Proyecto de Final de Carrera

(*Ingeniería Técnica en Informática de Gestión*)

Antecedentes y perspectivas de estudio en historia de la Criptografía

CURSO ACADÉMICO:	**2008-2009**
TUTOR:	**JORGE BLASCO ALÍS**
DIRECTOR:	**DIEGO NAVARRO BONILLA**

Alumno:

Xifré Solana, Patricia email: 100047481@alumnos.uc3m.es

Agradecimientos

A mi familia, especialmente que siempre han estado a mi lado, entre ellos a mis padres, que han sabido enseñarme lo bueno que es ser una persona con educación y me han apoyado y ayudado en cada momento.

A mi novio, por estar ahí, durante estos últimos meses tan duros y porque me ha motivado para poder escribir estas líneas y las que nos quedan.

A mis amigos, de fuera y dentro de la universidad que me han acompañado durante estos últimos años en la universidad, haciendo que se haya pasado muy rápido y conservando una amistad duradera.

A todos mis compañeros de clases y prácticas con los que he aprendido y me he enriquecido gracias a su sabiduría y confianza.

A los profesores de la Universidad que me han apoyado y ayudado con el proyecto.

Y por último, y no por ello menos importante, a mis tutores, Jorge Blasco Alís y Diego Navarro Bonilla, que me han apoyado durante todo el proyecto de fin de carrera y gracias a los cuales ha sido posible la realización del mismo; a Julio César Hernández Castro, quien iba a ser mi tutor hasta que tuvo que marcharse fuera del país y me puso en contacto con mis tutores anteriormente mencionados.

Contenido

Introducción 6
Objetivos del trabajo 8
Metodología seguida y fuentes empleadas 9
Estado de la cuestión 10
Principales pasos que ha dado la criptografía a lo largo de la historia 21
Criptografía Antigua 27
1) Procedimientos clásicos de cifrado 27
1.1 El ocultamiento de la información en las primitivas civilizaciones 28
1.2 La sistematización de los métodos de cifrado: La Antigüedad Clásica 30
1.3 Los primeros pasos: cifrado por sustitución y transposición 35
1.4 Ejemplos históricos de cifrado por sustitución y transposición 40
1.5 Condiciones del secreto perfecto 44
2) Edad Media. Islam: origen del criptoanálisis 48
2.1 Introducción al criptoanálisis 48
2.2 El Islam y el origen del criptoanálisis 50
2.3 Ataques a un Criptosistema 52
2.4 Ataque por fuerza bruta. Espacio de claves 55
2.5 Criptoanálisis básico 57
3) Edad Moderna 61
3.1 Criptografía en la Europa anterior al Renacimiento 61
3.2 La criptografía durante el Renacimiento 63
3.3 El Nomenclátor 68
3.4 Cifrados poli-alfabéticos 72
Criptografía Moderna 78
4) Edad Contemporánea 79
4.1 Cifrados Poligráficos 82
4.2 Ampliación de cifrados por Transposición 86
4.3 Criptografía de clave secreta 92
4.3.1 Arquitectura del cifrado en bloque y del cifrado en flujo 94
4.3.2 DES 105

4.3.2.1 Estructura e involución del DES 106
4.3.2.2 Manipulaciones en el DES 108
4.3.2.3 Expansión en el DES 109
4.3.2.4 Propiedades del DES 110
4.3.2.5 Seguridad del DES 111
4.3.3 AES 112
4.3.3.1 Estructura del AES 113
4.3.3.2 Transformación SubBytes e InvSubBytes 116
4.3.3.3 Transformación ShiftRows e InvShiftRows 118
4.3.3.4 Transformación MixColumns e Inv MixColumns 118
4.3.3.5 Transformación AddRoundKey e InvAddRoundKey 120
4.3.3.6 Esquema de clave en el AES 121
4.3.3.7 Seguridad del AES 121
4.4 La mecanización del secreto 122
Criptografía primera mitad del siglo xx: Guerras Mundiales 127
5) Criptografía en la primera Guerra Mundial 127
6) Criptografía en la segunda Guerra Mundial, el descifrado del Enigma y la barrera del idioma 138
Criptografía en la actualidad 153
7) Criptografía en clave pública 153
8) Criptografía para Internet 171
9) Protocolos criptográficos y firmas digitales 176
9.1 Firma digital 176
9.2 Firma digital del criptosistema RSA 183
9.3 Firma digital del criptosistema de ElGamal 184
9.4 Funciones Hash 185
10) La relevancia del cifrado 189
11) Un salto cuántico al futuro 194
12) Perspectiva técnica y legal de la criptografía frente al próximo milenio 214
Criptografía Española 217
Desarrollos interdisciplinares futuros 236
Resultados y Conclusiones 247
Gestión del proyecto 251
13) Medios técnicos empleados para el proyecto 251

14) Análisis económico para el proyecto 252
14.1 Presupuesto inicial 253
14.2 Coste final y análisis de desviación 255
Anexos y Bibliografía 256

Introducción

Criptografía es una palabra que viene del griego por la cual se entiende, el estudio de la ciencia que, mediante el tratamiento de la información, protege a la misma de modificaciones y utilización no autorizada, utilizando algoritmos matemáticos complejos para la transformación de la información en un extremo y la realización del proceso inverso en el otro.

Por ello, la criptografía, además de ser una disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado, garantizar su integridad, establecer su autenticidad y prevenir su repudio, tiene bases matemáticas actuales que son: teoría de números, teoría de la complejidad algorítmica, teoría de la información, estadística. Se distinguen la criptografía civil y la militar.

Con más precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias, el criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de la clave.

La criptografía, mediante el ocultamiento de la información proporciona:

■ Confidencialidad. Garantiza que sólo las personas autorizadas tienen acceso a la información.

■ Autenticación. Mecanismo para verificar que la información proviene del lugar indicado y que esta no ha sido modificada.

■ Integridad. Forma de detectar que la información no ha sido alterada por alguien no autorizado.

■ Control de Acceso. Restringir el acceso a la información.

■ No repudio. Servicio que garantiza la autoría del mensaje enviado.

A lo largo de la historia de la criptografía, se ha diferenciado entre: Precientífica ("Artística"), Científica (Shannon) y de clave pública (Diffie-Hellman).

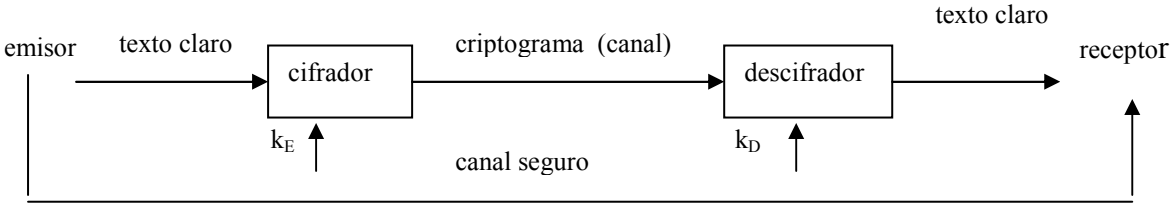
Básicamente, el objetivo de la criptografía es permitir la transmisión de información secreta por un canal público. Este problema de la comunicación segura fue de gran interés en la antigüedad y sigue considerándose vital en la actualidad, debido a los millones de ordenadores intercambiando constantemente información por Internet, una red pública al alcance de cualquiera y desde cualquier lugar del mundo.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

No obstante, la criptografía es una disciplina tan antigua como la propia escritura, que lógicamente se ha ido adaptando a los distintos canales de comunicación que la técnica ha proporcionado a lo largo de la historia: el papel, telégrafo, teléfono, la radio o las modernas redes de ordenadores. Su desarrollo ha sido siempre consecuencia de la lucha entre quienes diseñan códigos para ocultar información y quienes ingenian estrategias para romperlos. Una panorámica de esta disputa a lo largo del tiempo puede describir a la perfección una introducción a la criptografía, y eso es lo que se tratará de hacer en este documento.

En principio, la criptografía era prácticamente exclusiva de gobiernos y mandos militares, ya que éstos eran los únicos que necesitaban proteger sus comunicaciones. Dado el obligado secreto de los estamentos oficiales provocó que la criptografía sólo la conocieran unos pocos, entre los que raramente se encontraba alguien relacionado con el mundo universitario, sin embargo este aspecto ha cambiado radicalmente con la llegada del ordenador, gracias al cual se ha fomentado la demanda generalizada de protección de información, lo que ha despertado el interés de empresas y universidades por esta ciencia.

MODELO DE CRIPTOSISTEMA:



k_E : clave de cifrado
k_D : clave de descifrado

El ideal de la criptografía es dar con un criptosistema imposible de descifrar para quien no lo haya cifrado, lo cual supondría un pleno seguro de la confidencialidad de la información, y sin lugar a dudas el mayor de los avances en este campo.

Objetivos del trabajo

La intención es recorrer la historia de la criptografía desde los primeros pasos en la Antigüedad hasta nuestros días, en la era de Internet, estableciendo conclusiones hacia un futuro y haciendo un inciso para detenerse en la criptografía en España, presentando algunos métodos de cifrado que se emplearon en cada época y mostrando como fueron derrotados, al ser descifrados por el ingenio de los criptoanalistas, lo que anteriormente y en la actualidad obliga a sustituir dichos métodos por otros más complejos que sean prácticamente imposibles de descifrar.

Por último señalar la importancia de un apartado con independencia por si sólo de desarrollos interdisciplinares futuros, en el cual se plantea la colaboración con historiadores militares/diplomáticos con objeto de analizar documentos históricos que todavía permanecen cifrados en su original.

En definitiva, con el presente estudio, y con la mayor modestia posible, se pretende dar a conocer a los posibles lectores interesados este campo fascinante y complejo de la criptografía, a la vez que brindar la oportunidad de entrar en contacto con algunos métodos y servicios que tienen por principal objetivo mantener la seguridad y confidencialidad en la transmisión de mensajes, del mismo modo que los métodos desarrollados para romper la intimidad de tales comunicaciones.

Metodología seguida y fuentes empleadas

La dificultad, a la hora de realizar el presente estudio, radica en distinguir y manipular correctamente lo genérico de lo específico, no pudiendo encuadrarse ciertos métodos exactamente en unos determinados períodos históricos. Debido a ello, en el presente documento se ha elaborado una clasificación, que si bien sigue un orden cronológico, de forma personal (por parte del autor), se han establecido grandes apartados que recogen la mayor parte de esta disciplina a lo largo de la historia.

Evidentemente, la criptografía moderna goza de más extensión debido a la gran importancia que actualmente y en un futuro tiene y tendrá.

El proyecto consta de un conjunto de grandes bloques como son: la criptografía antigua (incluyendo en el mismo la antigüedad, la Edad Media y la Edad Moderna), que recoge el período comprendido desde que el hombre necesita enviar documentos escritos que sólo deben ser conocidos por su destinatario, hasta el siglo XVIII, que con el comienzo de la era contemporánea da lugar al siguiente gran bloque de criptografía moderna que se extiende hasta el siglo XX. La primera mitad del siglo XX se ha decidido incorporar como otro de estos grandes bloques debido a la relevancia que tuvo en las guerras mundiales. Finalmente la criptografía en la actualidad debe tratarse como otro bloque independiente. Por supuesto no podía faltar un apartado que hiciera referencia a lo que ha ocurrido en España.

Para terminar se ha decidido incluir un capítulo de Desarrollos interdisciplinares futuros, que como ya se ha mencionado en los objetivos del trabajo, se intentará plantear una colaboración con historiadores militares/ diplomáticos.

Las principales fuentes consultadas han sido algunas bibliotecas distinguiendo entre ellas la Biblioteca Nacional, la de la Universidad Carlos III, la de la Universidad Complutense y una o dos bibliotecas municipales. Además de ir al Centro de Documentación del Ministerio de Defensa (con grandes aportaciones para el proyecto) y una amplia gama de consultas de sitios Web así como una exhaustiva investigación en

todas y cada una de las Intranets correspondientes a los distintos organismos visitados en la obtención de información y material de investigación.

Estado de la cuestión

Hoy en día la información puede que sea uno de los bienes más preciados, o la desinformación una de las peores armas con las que atacar a alguien. Por lo que en la sociedad en la que vivimos se hace muy necesario la seguridad en las comunicaciones, y como principal exponente en Internet , ya que este método de comunicación es cada vez más utilizado, no sólo por estudiantes y comunidad universitaria, sino por empresas, particulares, y cada vez para realizar más cosas. Con lo cual cabe pensar que la criptografía será uno de los claros exponentes a tener muy en cuenta en el futuro de la informática, sobretodo a la velocidad que se implementan nuevas tecnologías, las cuales permiten el envío de información más valiosa y que puede comprometer mucho a los interlocutores en caso de que sea interceptada por otras personas. Lo cierto es que se trata de un mundo fascinante y que tiene muchas posibilidades de investigación.

Son muchos los expertos e investigadores unidos a las redes de investigadores y colegios invisibles de publicaciones los que en la actualidad están trabajando y desarrollando nuevas líneas de investigación dentro del campo de la criptografía. Dentro de esta gran lista destaca especialmente:

David Kahn, historiador estadounidense, periodista y escritor. Se ha dedicado casi exclusivamente a escribir acerca de la historia de la criptografía, de la inteligencia militar y de temas relacionados. Fue nombrado como doctor (DPhil) por la Universidad de Oxford en 1974 en el área de Historia Moderna de Alemania.

El primer libro de Kahn fue: *The Codebreakers*.(1) Supuso una novedad muy grande, máxime cuando por aquella época la criptografía en la segunda guerra mundial era considerado todavía un tema clasificado. Una de las ediciones inglesas de 1996 tiene un capítulo adicional con una recolección de los eventos acaecidos en criptología desde la

(1) publicado en 1967, fue considerado una obra maestra (y libro de referencia) en temas de historia de la criptografía. Finalista para el premio Pulitzer en el año 1968 dentro de la categoría de no ficción.

aparición de la primera edición, tal como el advenimiento de sistemas criptográficos populares tales como el PGP. Posteriormente ha desarrollado numerosos escritos sobre criptografía, tales como:

- Plaintext in the new unabridged: An examination of the definitions on cryptology en Webster's Third New International Dictionary (Crypto Press 1963).
- Cryptology goes Public (Council on Foreign Relations 1979).
- Notes & correspondence on the origin of polyalphabetic substitution (1980).
- Codebreaking in World Wars I and II: The major successes and failures, their causes and their effects (Cambridge University Press 1980).
- Kahn on Codes: Secrets of the New Cryptology (Macmillan 1984).
- Cryptology: Machines, History and Methods by Cipher Deavours & David Kahn (Artech House 1989).
- Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939-1943 (Houghton Mifflin 1991).
- Hitler's Spies: German Military Intelligence in World War II (Da Capo Press 2000).
- The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking (Yale University Press 2004).

Son de vital importancia en la actualidad criptográfica las redes de investigadores y colegios invisibles de publicaciones en las que se encuentran multitud de expertos que trabajan diariamente para ir dando grandes pasos dentro del mundo criptográfico gracias a sus escritos e investigaciones. Tales son:

Dr Jorge Ramió Aguirre, coordinador de la Red Telemática Iberoamericana de Criptografía y Seguridad de la Información (CriptoRed[(2)]). También profesor de la Universidad Politécnica de Madrid, su intención es establecer un flujo de cooperación con todos los países de Iberoamérica en materia de seguridad informática. En sus primeros tres meses de andadura, la Red contaba ya con más de 100 miembros, muchos

(2) Probablemente el portal en castellano dedicado a la Criptografía más conocido

de ellos profesores de reconocido prestigio, así como un buen número de universidades y centros de investigación. El objetivo, una comunidad científica virtual que difundirá en un sitio Web sus conocimientos y proyectos sobre seguridad informática. Sus escritos son básicamente electrónicos y últimamente ha actualizado su último Libro Electrónico de *Seguridad Informática y Criptografía en Diapositivas* Versión v 4.0.

Como experto en criptografía, y seguridad de la información, comentó el momento actual y las tendencias en materia de seguridad de la información en la novena edición del RECSI(3). A pesar del amplio abanico de temas presentados en las ponencias, uno de los que más resaltó en seguridad de la información debido a su carácter multidisciplinar, tal y como se esperaba, fue la de identificación, en sus vertientes documento nacional de identidad electrónico y sistemas de identificación por radiofrecuencia. Sí se echó en falta, y esto es algo que se viene arrastrando desde hace años, un mayor peso en propuestas innovadoras en gestión y análisis de riesgo.

Jeimy Cano. Miembro investigador de CriptoRed, e ingeniero de sistemas y computación de la universidad de Los Andes, Colombia, donde imparte cátedras relacionadas con delitos informáticos y computación forense, moderador de la lista de seguridad informática de la ACIS(4) y conferencista nacional e internacional en temas relacionados con seguridad informática, delitos informáticos y computación forense. En su conferencia presentada en el Día Internacional de la Seguridad de la Información (DISI 2006), organizado por la Cátedra UPM, y celebrado el 30 de noviembre en Madrid, dijo: "ellos -el crimen- sí están organizados, nosotros no". Las investigaciones de Jeimy Cano facilitan la labor de atrapar a los hackers, autores de ataques informáticos y de emprender acciones judiciales contra ellos.

También se encuentran el **MundoCripto** de **Jaime Suárez** y el **Taller de Criptografía** del profesor de la Universidad de Granada, **Arturo Quirantes**. Aunque existe una Asociación Española de Criptología, su Web parece ser que no se actualiza desde el año 2000.

(3) Reunión Española sobre Criptología y Seguridad de la Información celebraba en Barcelona (2007).
(4) Asociación Colombiana de Ingenieros de Sistemas

Una Web curiosa es **Cryptome,** quien publica documentos prohibidos por los gobiernos; inicialmente relativa a los algoritmos criptográficos pero que ha ido evolucionando para albergar todo tipo de información que alguna vez fue confidencial.

RSA Security convoca periódicamente retos de ruptura de algoritmos para evolucionar el tamaño de la longitud de las claves, el último ha sido el RSA-576.

Es de vital importancia todas las publicaciones llevadas a cabo por colegios invisibles de publicaciones y revistas. Especialmente y debido a su gran interés cabe señalar ***Cryptologica*****:** revista estadounidense trimestral que publica todos los aspectos relacionados con la criptografía. El primer volumen vio la luz en enero de 1977. Actualmente está dirigida por Taylor & Francis. Constituye una publicación única para los estudiantes interesados en todos y cada uno de los temas relacionados con criptología. Además patrocina una competición de artículos estudiantiles anual para animar el estudio de criptografía en los planes académicos. Greg Mellen Memorial patrocina becas para animar el estudio de criptología a los estudiantes.

No es una publicación gubernamental, sin embargo está revisada por el profesor Brian J. Winkel, Departamento de Ciencias Matemáticas, y la Academia Militar de los Estados Unidos (West Point).

Las áreas cubiertas incluyen la seguridad del ordenador, la historia, códigos y cifras, matemáticas, la ciencia militar, el espionaje, dispositivos de cifra, literatura, y lenguas antiguas. Los campos que abarca son la investigación y artículos expositivos, criptológicos, libros relacionados y la revista propiamente dicha. Sus artículos abarcan todas las áreas criptográficas.

Los artículos concernientes a criptosistemas y criptoanálisis matemático, aspectos de cifrado y descifrado, desafiando el código y la cifra, junto a los materiales históricos y memorias, así como las traducciones de contribuciones significativas son los más utilizados.

Los redactores que fundan la revista son David Kahn, Louis Kruh, Cifra A. Deavours, Departamento de Matemáticas, Universidad de Kean de Nueva Jersey, Unión NJ 07083 USA y Gregorio Mellen.

Cryptologica es la única revista en el mundo que trata con la historia, la tecnología, y el efecto impactante de inteligencia hoy en día: la inteligencia de comunicaciones. Esto promueve el estudio de todos los aspectos tanto técnicos como históricos y culturales relacionados con criptografía.

Los artículos de dicha revista han abierto muchos nuevos caminos en la historia de inteligencia. Han contado por primera vez como una agencia especial que preparó la información de descifrado para el Presidente Roosevelt, descrito las cifras de Lewis Carroll, revelado los detalles de la agencia de intervención de las conexiones telefónicas de Hermann Goering, publicado la metodología de algunos descifradores americanos de la segunda Guerra Mundial, expuesto como los descifradores de código americanos afectaron la estructura de las Naciones Unidas, traducido por una lado, las partes árabes de los primeros textos líderes mundiales sobre criptoanálisis y por otro del alemán un estudio de criptoanálisis nazi, así mismo, imprimió un artículo basado en un área hasta ese momento desconocida: El Frente occidental alemán de descifrado en la primera guerra mundial y muchos otros.

La revista publicó un discurso del jefe de la Agencia de Seguridad nacional de descifrado, la organización de cifrado y un análisis del estándar de cifrado de datos propuesto por el gobierno nacional. A su vez también editó artículos técnicos de análisis del criptosistema generado por máquinas de cifra, incluyendo la Enigma, además de relatar la solución de criptogramas históricos. Explicaron la base lingüística de la lengua navaja usada por cifradores en el océano Pacífico y comunicaciones digitales que pueden ocultar ilustraciones o imprimir con filigrana lo que autentica la fuente. Un artículo demostró la insuficiencia de cifras basadas en la música, entre otras cosas.

Además de esta importante revista, se pueden encontrar innumerables sitios Web y revistas digitales como la *revista digital universitaria* [5] o la *revista del Sur* [6] que con

(5) *revista.unam.mx*: http://www.revista.unam.mx/vol.10/num1/art01/int01-2.htm
(6) http://www.redtercermundo.org.uy/revista_del_sur/texto_completo.php?id=1198

mucha frecuencia dedican parte de sus paginas a publicar artículos interesantes sobre criptografía y sus actuales investigaciones.

Otras revistas de interés a cerca de criptografía son ***Intelligence and National Security*** estudiando con profundidad los ataques biológicos y no gubernamental, las principales dificultades encontradas en cuanto a seguridad por el departamento de inteligencia, analistas de inteligencia y fabricantes de política, y los beneficios y peligros de la tensión existente en las relaciones entre el servicio de inteligencia y el público en general, además de otros temas de gran interés. Habiendo otras muy similares tales como ***International Journal of Intelligence and Counterintelligence*** y ***Studies in Intelligence*** (www.cia.gov).

Es muy amplio y extenso lo referente a criptografía aplicada a la historia y tecnología militar. Existen muchos artículos en revistas que nos pueden dar una idea de cuáles son las líneas de investigación y proyectos que más interesan a los militares en cuanto a los temas de seguridad de la información y criptografía aplicada, todos ellos se encuentran detallados en los anexos al final de este proyecto, y son:

Criptografía aplicada a la informática. Obtenida en el centro de documentación del Ministerio de Defensa. Pertenece a un dossier sobre seguridad militar. Los aspectos de la seguridad de la información son tres: la seguridad física o control de acceso, la seguridad "Software" y la criptografía. Se analizan los tres aspectos pero sobre todo se hace hincapié en el último. Hay tres pasos por los que ha de pasar la información: procesamiento, almacenamiento y transmisión; en todos ellos dicha información es vulnerable, por lo que es importante estudiar todos los aspectos de seguridad en cada uno de ellos. Finalmente, se señala a los métodos criptográficos como las formas más seguras y efectivas.

La Seguridad en las Redes Militares de Telecomunicaciones. Nuevamente, este interesante artículo ha sido obtenido en el centro de documentación del Ministerio de Defensa, perteneciendo también al mismo dossier sobre seguridad militar. El objetivo de este artículo es mostrar como se lleva a cabo la protección de toda la señal electromagnética que proporcione información a un enemigo real o potencial así como cualquier documento una vez haya sido depositado en el ámbito de la red. Se estudia la

arquitectura general del sistema de seguridad y los principios básicos de la misma, así como las técnicas de cifrado y transmisión finalizando con la gestión de claves.

Nuevas tecnologías, nuevos retos para la defensa. Con este artículo se pretende introducir las bases de los sistemas de seguridad en la transmisión de la información a través de las redes de comunicaciones, así como hacer un estudio sobre el uso de la red como plataforma para el posible planteamiento de acciones que dan lugar a nuevas formas de conflicto.

El Instituto Politécnico Nacional se haya formado por un grupo de investigación dirigido por el doctor **Miguel Lindig Bos**, coordinador general de Servicios Informáticos, y el candidato a doctor **Víctor Silva García**, director del Centro de Innovación y Desarrollo Tecnológico en Cómputo, equipo que se ha propuesto resolver temas de investigación de gran interés, entre ellos el desarrollo de un algoritmo y una llave para utilizarla en Criptografía, constituyendo uno de los pocos, o quizá el único conjunto de científicos que trabajan en equipo en este área del conocimiento en México.

El sector que más se preocupa por llevar a cabo investigación en Criptografía es el militar, de ahí que sean las grandes potencias mundiales donde se realice la mayor parte de investigación en este campo. En 1977 la Criptografía pasó de una necesidad militar a una necesidad social y comercial. Paradójicamente, lo secreto se hizo público. Hoy en día existe la opción de utilizar criptosistemas para resguardar nuestra información civil.

La información que viaja a través del medio físico tiene que ir cifrada, porque significa dinero, y debe evitarse la posibilidad de intercepción y desciframiento. De ahí que sea necesario para el país desarrollar investigación en Criptografía, si no se quiere quedar rezagado, una vez más, en un área de la tecnología vital para los intereses nacionales de seguridad y soberanía.

La delincuencia informática parece que va más rápida que su seguridad. Dentro de 30 años, muchos de los secretos que guarda el mundo moderno bajo potentes algoritmos criptográficos, como los datos médicos o la información clasificada de los gobiernos, correrán un peligro real de saltar por los aires. La criptografía cuántica se

encargará de que su descifrado sea un juego de niños, susceptible de caer en manos de terroristas o criminales. Quien realizó tal profecía fueron, respetables investigadores como **Martin Hellman**, co-inventor de la criptografía de clave pública, y el criptólogo argentino **Hugo Scolnik**, durante sus intervenciones en el Día Internacional de la Seguridad de la Información en la Universidad Politécnica de Madrid.

Hellman y Scolnik sostienen que la criptografía cuántica está aún en un estado embrionario y hasta dentro de 30 años no se verán sus primeras aplicaciones prácticas, que romperán con facilidad los actuales sistemas de cifrado. Mientras tanto, ha empezado una carrera paralela para proteger la información que debería seguir siendo secreta cuando irrumpa la criptografía cuántica.

Hellman aseguró que está preocupado por si cae en malas manos. De momento, los investigadores trabajan en una de las pocas soluciones a su alcance: cifrar las cosas por duplicado, combinando criptografía simétrica y asimétrica, de forma que si la cuántica rompe la asimétrica, quede aún en pie la simétrica. El problema, dijo, "es que es muy caro, por lo que sólo puede usarse para información realmente valiosa".

Tal vez la conclusión más interesante que se puede extraer de la novena edición del RECSI, celebrada en Barcelona es que los grupos de investigación en España han aumentando y ampliado su horizonte, tanto en temática como en alcances internacionales. Sin tomar en cuenta aquellos profesionales y expertos de la seguridad informática en la empresa, industria y organismos del Estado que también investigan, estamos hablando que en España dentro de las universidades y centros de investigación existe un grupo superior a los 300 expertos, en su mayoría doctores, participando en decenas de proyectos de investigación. Un valor muy alto y que viene a poner de manifiesto el espectacular desarrollo que ha experimentado en nuestro país esta especialidad en los últimos 10 años.

De los expertos e investigadores que en la actualidad están trabajando y desarrollando nuevas líneas de investigación dentro del campo de la criptografía, conviene destacar algunos españoles y algunas líneas de investigación muy estudiadas y especialmente señalar a:

Juan Carlos Galende Díaz, doctor en historia por la universidad Complutense de Madrid y profesor titular del departamento de Ciencias y Técnicas Historiográficas de la facultad de Geografía e Historia, del que es actualmente su director, integrante de diferentes equipos de investigación nacionales e internacionales. Ha realizado diversos escritos como: Catálogo concordado de los repertorios bibliográficos de Hernando Colón, Diccionario Histórico de la Antroponimia Románica, Documentación epigráfica y paleográfica de interés científico-cultural e Histórico-social para la Comunidad de Madrid, La organización del espacio en la Corona de Castilla (1212-1369) etc. y autor de diversas monografías (Criptografía. Historia de la escritura cifrada, Diccionario general de abreviaturas españolas, La crisis del siglo XVIII y la Inquisición española, El caso de la Inquisición toledana (1700-1820), Antroponimia madrileña del siglo XVII, Historia y documentación...) y artículos de carácter paleográfico-diplomático, entre los que destacan los temas criptográficos, cronológicos, archivísticos, bibliotecarios, etc.

La entrega de un DNI electrónico (e-DNI) a la población es un hito importante dentro de la llamada Sociedad de la Información, que nos pone además a la vanguardia tecnológica en este ámbito. Dejando de lado el peliagudo tema de las funciones hash(7), que pasados ya dos años desde aquellos primeros ataques en serio a MD5(8) hoy se han generalizado a toda esa familia poniendo incluso en serio riesgo a SHA-1(9) y sigue sin haber una respuesta en forma de estándar mundial, siempre está en el aire la pregunta de porqué no se eligió para el eDNI curvas elípticas en vez de RSA(10), cuando todas las investigaciones apuntan a que será el nuevo estándar en cifrado de clave pública.

Expertos reunidos en Madrid apuestan por el doble cifrado para evitar el desvelamiento de información privada y secreta - Una empresa rusa vende servicios 'web' para distribución de código malicioso.

El riesgo de que la novedosa tecnología conocida como criptografía cuántica se use con fines perversos no es ninguna utopía, ya ha sucedido con los programas

(7) Construcción criptográfica empleada en muchas aplicaciones. Son usadas junto con los algoritmos de clave pública para cifrado y firma digital.
(8) Algoritmo utilizado para la autenticación de mensajes que verifica la integridad de la comunicación, autenticidad en el origen y puntualidad en el mensaje
(9) Algoritmo de funciones Hash Seguro
(10) Algoritmo de encriptación de clave pública.

informáticos, como demostró **Sergio de los Santos**(11). Ni los antivirus ni los cortafuegos protegen ya contra estos criminales que "han tomado la Web para distribuir sus códigos y también como parte de su infraestructura", refiriéndose a la Rusian Business Network, una empresa de San Petersburgo que vende servicios Web para distribución de código maligno y phishing.

El objetivo de la escuela **Lluis Santaló** 2005 es ofrecer una panorámica de las más recientes aplicaciones matemáticas en Criptografía. En la actualidad, las actividades humanas son cada vez más dependientes de las tecnologías de la información por lo que el concepto de seguridad informática juega un papel predominante en nuestra sociedad. Elementos tan cotidianos como tarjetas inteligentes, teléfonos móviles, compras por Internet o TV de pago son tan solo aspectos parciales de esta sociedad tecnológica en la que nos encontramos inmersos. Pero, detrás de cada uno de estos ejemplos, hay unos requerimientos específicos de seguridad que se cumplimentarán mediante la aplicación de soluciones criptográficas. Sin embargo, las aplicaciones criptográficas tropiezan con grandes dificultades matemáticas tanto en el diseño como en la implementación de criptosistemas seguros.

En dicha escuela se da una visión amplia de las tendencias actuales en criptografía tanto en la de clave secreta como de la de clave pública. Los cursos serán impartidos por expertos de reconocido prestigio dentro de la comunidad criptográfica internacional. La escuela cuenta además, con varias conferencias y mesas redondas.

Investigadores del Departamento de Lenguajes y Sistemas de Información e Ingeniería del Software de la Facultad de Informática de la Universidad Politécnica de Madrid (FIUPM) han desarrollado un prototipo de red metropolitana de criptografía cuántica que estará disponible en 2010 para ser implantada en cualquier red urbana de telecomunicaciones de España de la mano de Telefónica, la finalidad de este proyecto es alumbrar una nueva generación de soluciones de seguridad integrales, capaces de hacer frente a las actuales amenazas a la seguridad en las telecomunicaciones que presentan las redes convencionales.

(11) Consultor de seguridad de Hispasec Sistemas, que afirma "En el código malicioso hemos pasado del romanticismo al todo por la pasta, gente organizada que presta especial atención a atacar la banca en línea".

D. Carlos Jiménez, ingeniero superior de Telecomunicaciones en sus cinco especialidades por la UPM de Madrid. Creó la primera vacuna contra el virus "Viernes 13". En la actualidad es Director General de la empresa Secuware. Carlos Jiménez es Asesor del Gobierno español en temas de Seguridad Informática y ha desarrollado durante dos años el sistema de protección que actualmente tiene implantado el Ministerio de Defensa. Es considerado uno de los veinte mayores expertos mundiales en virus informáticos. Ha escrito numerosos artículos en revistas especializadas, participado en conferencias e impartido clases en diferentes universidades españolas y extranjeras.

José Ramón Soler y Fuensanta, Ingeniero en Informática por la Universidad Autónoma de Bellaterra y Doctor Ingeniero Industrial por la UNED. Hace varios años que empezó a trabajar sobre criptología habiéndole dedicado varios artículos en revistas especializadas, tanto españolas como extranjeras, y dos libros, siendo uno de ellos crucial en la historia de la criptografía de la guerra civil española; hablaremos de dicho libro en el apartado de criptografía española del presente proyecto**. Francisco Javier López-Brea Espiau**, Teniente Coronel del Ejército de Tierra y especialista en criptología del Ministerio de Defensa., es un gran estudioso de la criptología y su historia habiendo publicado artículos en revistas nacionales e internacionales y, siendo gran conocedor de los sistemas de cifrado mecánicos, es también autor del libro anteriormente mencionado.

Y junto a ellos podrían citarse un gran número de investigadores que están llevando a cabo diversas líneas de temas relacionados con la criptografía tanto internacional como nacional.

No podemos dejar de citar al **Centro Criptológico Nacional**, dependiente del Centro Nacional de Inteligencia, el cual cuenta con un equipo de respuesta ante incidentes de seguridad, cuya finalidad es mejorar el nivel de seguridad informática de la Administración pública española. El equipo se formó a principios del 2007 y participa en los principales foros de seguridad europeos y mundiales, en los que comparte información y objetivos, y debate sobre los nuevos avances en materia de ciberseguridad.

Este equipo se presentó en la consejería de Tecnología, Ciencia y Universidad del Gobierno de Aragón. El acto contó la presencia del director general de Tecnologías para la Sociedad de la Información del Gobierno de Aragón, **Miguel Ángel Pérez Costero**, y del subdirector adjunto del Centro Criptológico Nacional, **Luis Jiménez**, el cual dio a

conocer algunos de los recursos más importantes puestos a disposición de todas las administraciones públicas por parte de su centro para mejorar la seguridad de los sistemas y garantizar su funcionamiento eficaz al servicio del ciudadano. Entre estos, se encuentran el soporte y la coordinación en la resolución de incidentes producidos por 'phising', 'spam', ataques a servicios Web, captura de datos personales, denegación de servicio y destrucción de información.

Además, desde el Centro Criptológico Nacional también se avisa sobre vulnerabilidades, alertas y avisos de nuevas amenazas y se realizan análisis de códigos dañinos y de riesgos. También se imparten cursos de formación para el personal de toda la Administración y la evaluación y certificación de productos.

El subdirector adjunto del Centro Criptológico Nacional dijo que los ataques más comunes que se prevén para todo el año 2008 son el robo de información, la infección de los sistemas Windows y Unix por medio de 'troyanos orootkits'[(12)].

Otros problemas son la utilización de 'botnets' para realizar ataques de forma masiva, los ataques a servicios Web, el 'phishing' y el 'spam'. De entre ellos, y según Jiménez, los más preocupantes a día de hoy son los 'troyanos'.

La principal herramienta para dar soporte a estos servicios está constituida por el portal que ha desarrollado el Centro (www.ccn-cert.cni.es), que ofrece información actualizada diariamente sobre amenazas, vulnerabilidades, guías de configuración de las diferentes tecnologías, herramientas de seguridad, cursos de formación o indicaciones para mejores prácticas de seguridad.

Principales pasos que ha dado la criptografía a lo largo de la historia

El origen de la criptografía se remonta sin duda a los orígenes del hombre, desde que aprendió a comunicarse. Entonces, tuvo que encontrar medios de asegurar la confidencialidad de una parte de sus comunicaciones.

(12) herramienta que sirve para ocultar actividades ilegítimas en un sistema, una vez instalada, permite al atacante actuar con el nivel de privilegios del administrador del equipo

En el antiguo Egipto, la escritura jugó a veces ese papel. Sin embargo, el primer testimonio de uso deliberado de métodos técnicos que permitieran cifrar los mensajes viene de Grecia, sobre el siglo VI antes de Cristo, y se llama escítalo. Más tarde los ejércitos romanos utilizaron para comunicarse el cifrado de César. Además merece mención especial Sexto Julio Frontino, político del Imperio Romano, uno de los más importantes aristócratas de finales del siglo I. Es principalmente famoso por sus obras y tratados, especialmente por uno que habla de los acueductos de la ciudad de Roma. Durante su vida, Frontino escribió un tratado teórico sobre la ciencia militar, el cual se ha perdido. La obra que si ha perdurado, su *Strategemata*, es una colección de ejemplos de tácticas militares empleadas durante la hegemonía de los mundos griego y romano.

Después, durante cerca de 19 siglos, se asiste al desarrollo más o menos ingenioso de técnicas de cifrado experimentales donde la seguridad residía esencialmente en la confianza que quisieran darles los usuarios.

En el Islam destaca el sabio árabe conocido como Al-Kindi (801-873), importante filósofo y estudioso de las Ciencias. Autor de numerosos libros y uno de sus tratados más importantes, redescubierto el año 1987, en el archivo Sulaimaniyyah de Estambul, está relacionado con la criptografía y se titula *Sobre el desciframiento de mensajes criptográficos*.

La criptografía en Europa data de la edad media, El primer libro europeo que describe el uso de la criptografía fue escrito en el siglo XIII por el monje franciscano Roger Bacon, titulado *La Epístola sobre las obras de arte secretas y la nulidad de la magia,* en él se describen siete métodos distintos para mantener en secreto los mensajes. Por otro lado en el año 1379 Gabriele de Lavinde de Parma escribió el primer manual sobre criptografía. En 1563 el físico Giambattista Della Porta crea un sistema con la particularidad de cifrar bloques de dos en dos letras, el cual ha sido utilizado con éxito durante más de tres siglos. Fue el inventor del primer sistema literal de clave doble, o sea, la primera cifra en la cual el alfabeto cifrante muda cada letra. Este sistema poli alfabético era extremadamente robusto para la época, de modo que muchos consideran Della Porta como el "Padre de la criptografía moderna".

El desarrollo de los cifrados poli alfabéticos empezó con Leon Battista Alberti, que en 1568 publicó un manuscrito describiendo un disco de cifrado que define múltiples sustituciones, la contribución importante de Alberti es dar la posibilidad de cambiar el tipo de sustitución durante el proceso de cifrado. En 1586 Blaise de Vigenère generalizó el criptosistema de Julio Cesar utilizando todos los corrimientos posibles, esto también será analizado posteriormente.

En los años 1600, se comenzaron a dar soluciones a los criptosistemas existentes. En 1624 Augustus II, Duque Alemán, escribió el libro *Cryptomenytices et cryptographiae, libri IX*, en el que se dedicaba a la solución de varios criptosistemas. En 1663 en Roma, el jesuita Athanasius Kircher escribió el libro *Polygraphia nova et universalis*, el que consiste en una colección de criptosistemas usados en la época.

Para los años 1700, siguieron los tratados dedicados al criptoanálisis, en 1781, a causa de un concurso en Viena, se descubrieron 15 claves de los sistemas criptográficos de esa época.

A principios del siglo XIX Thomas Jefferson inventó una máquina constituida por 10 cilindros que estaban montados en un eje de forma independiente, en donde se colocaba el alfabeto y al girar los cilindros, quedaba cifrado el mensaje. En el siglo XIX, Kerchoffs estableció los principios de la criptografía moderna. Los algoritmos modernos usan una clave para controlar el cifrado y descifrado de los mensajes. Generalmente el algoritmo de cifrado es públicamente conocido y sometido a pruebas por parte de expertos y usuarios. Se acepta por lo tanto, la denominada hipótesis de Kerckhoffs, que establece que la seguridad del cifrado debe residir, exclusivamente, en el secreto de la clave y no en el del mecanismo de cifrado.

En la primera Guerra Mundial (1914-1918) los cifrados todavía eran hechos por diferentes asociaciones del alfabeto (cifrado por permutación) y los mensajes eran llevados por el hombre, usando medios de transporte muy lentos, de tal forma que había lugares a los cuales era imposible llevar el mensaje, como a barcos, aviones y submarinos, por lo que se comenzó a usar el teléfono, el telégrafo y la radio. Este último era fácil de transportar, lo que cambió radicalmente las comunicaciones; sin embargo, de este modo los mensajes eran también fácilmente interceptados. Esto justificó incrementar el uso de la criptografía.

Hasta 1918 los cifrados se hacían manualmente, lo que causaba muchos errores en el proceso de cifrar y descifrar, de tal modo que los criptógrafos comenzaron a crear máquinas para tales fines. Por ejemplo, en Estados Unidos desde 1861 hasta 1980 se registraron 1769 patentes relacionadas con la criptografía. A principios de los años 20 ya había un gran número de estas máquinas, dando gran seguridad en la transmisión de información. Esta década fue la edad de oro para las máquinas de cifrado. Una de las más populares fue la Enigma creada por el ingeniero alemán Arthur Scherbius. En Japón inventaron a Purple, en Estados Unidos tenían a SIGABA y la versión inglesa se llamó Typex. De igual forma en 1922, Arvid Damm crea la compañía Aktiebolget Cryptograph, que llegó a ser una de las más grandes proveedoras de equipo criptográfico de la época, no sólo para la industria militar sino también para bancos e industrias comerciales y de servicios.

En 1926 la marina alemana decidió comprar la máquina ENIGMA, que fue patentada hasta 1928, fecha en que Scherbius murió. Irónicamente en 1929 su invento se vendió a gran escala en todo el mundo. A finales de la segunda Guerra Mundial

De 1939-1945 se habían producido alrededor de 30,000 máquinas Enigma. No fue oficial, pero la fuerza aérea alemana era el más grande usuario con 20,000 del total de estas máquinas. Sin embargo la seguridad de los alemanes no sólo dependía de Enigma. En 1931 la firma Siemens Halske patentó un dispositivo de telecomunicaciones llamado Geheimschreiber, que fue usado durante y después de la segunda Guerra Mundial.

En 1948 y 1949 dos artículos de Claude Shannon, *Teoría Matemática de la Comunicación* y sobre *todo La Teoría de la Comunicación de los Sistemas Secretos* dieron los cimientos científicos a la criptografía borrando tanto vanas promesas como falsos prejuicios. Shannon probó que el cifrado de Vernam introducido algunas decenas de años antes, todavía llamado one time pad, era el único sistema incondicionalmente seguro. Sin embargo el sistema era impracticable.

Después de la guerra se inició el desarrollo de la electrónica y las computadoras. Criptosistemas con algoritmos más sofisticados fueron implementados en la transmisión de la información, pero aun eran usadas máquinas del tipo Enigma como la M-209 Converter o C-36 inventada por Boris Hagelin, la cual fue usada hasta principios de los

años 50 por la armada norteamericana. Como muchas otras actividades, la criptografía pasó a ser dominada predominantemente por quienes ganaron la guerra. Así se inició la nueva era de la criptografía electrónica. En la década de los 50, el panorama mundial estaba dirigido a otra etapa política, que conocemos como Guerra Fría. La hegemonía occidental se concentrada en Estados Unidos, su localización geográfica le permitió crecer económicamente, de tal modo que era un buen lugar para el desarrollo científico. Por ejemplo, un grupo de ex oficiales de la marina crearon a ERA (Engineering Research Associates), con el propósito de desarrollar e investigar lo que se refiere a la seguridad. Los proyectos Demon y Goldberg se dedicaron a hacer criptoanálisis en masa y a gran velocidad.

La necesidad política de penetrar los altos niveles soviéticos y del bloque del Este, hizo que Estados Unidos adoptara una mejor organización en el estudio de lo que llamaron Comunicación de Inteligencia (COMINT). Cuatro grupos de Estados Unidos se dedicaban a tal tarea, en particular al criptoanálisis: The Army Security Agency (ASA), The National Security Group, The Security Services of the Air Forces, y The Armed Forced Security Agency (AFSA). Por razones de eficiencia, el presidente Harry Truman decidió centralizar los servicios de COMINT, creando el 4 de Noviembre de 1952 la National Security Agency (NSA), que se encargaría de todos los aspectos de comunicación de inteligencia.

En Europa otras organizaciones como la North Atlantic Treaty Organization (NATO), desarrollaron tecnología para la seguridad en la información, con la finalidad de crear un dispositivo estándar, es decir, un equipo que sea utilizado por varios países, de esto resultó la KL-7 y KW-27.

Compañías como la International Bussiness Machines Corporation (IBM) crearon a principio de los años 60 un sistema llamado Harvest que contaba con una unidad de criptoanálisis de alta velocidad; asimismo en 1976 aparece la CRAY-1, la cual es una de las más veloces hasta la fecha, ésta cuenta con más de 200,000 circuitos integrados. Una de éstas fue adquirida por la NSA, para ser utilizada en el criptoanálisis.

A principios de los años 70, la criptografía estaba por iniciar la época de los circuitos integrados y el desarrollo en los algoritmos, concretamente, el uso de las

matemáticas modernas. Por ejemplo, en 1975 se publica la creación de IBM, el sistema Data Encryption Standard (DES), que ha sido uno de los más usados hasta la fecha.

Un año importante para la criptografía fue el de 1976, cuando W. Diffie y M. Hellman crean el concepto de Criptosistema de clave pública, es decir, un sistema donde la clave de cifrado se puede encontrar en un directorio público de usuarios; sin embargo, la clave de descifrado es diferente y no se obtiene fácilmente de la primera.

Poco más tarde, en 1978 se da a conocer el criptosistema de clave pública más seguro y usado hasta la fecha, el RSA. Sus inventores R. L. Rivest, A. Shamir y L. Adleman del MIT proponen la función de un sólo sentido que utiliza el exponente módulo un número entero n, producto de dos números primos y que tiene como seguridad la dificultad de factorizar a un número n de entre 100 y 200 dígitos. La necesidad de romper este criptosistema desarrolla la teoría de factorizar números grandes, cosa que después justifica la aparición de las curvas elípticas en criptografía.

Otro sistema que se ha mantenido hasta hoy, es el propuesto por T. ElGamal en 1984, que basa su seguridad en el problema del logaritmo discreto que aun no se ha podido resolver satisfactoriamente de manera rápida.

En la mayor parte del mundo existen centros de investigación en la seguridad de la información; por ejemplo, en 1988 se crea el European Institute for System Security, que entre sus objetivos está el desarrollar investigación en todos los campos que tengan que ver con la seguridad de la información, en particular con la criptografía. Varios de sus miembros son reconocidos matemáticos.

Muchas áreas de las matemáticas han podido ser usadas para crear criptosistemas, como los campos finitos y factorización de números enteros. Otros ejemplos son: en 1970 R. J. McEliece desarrolló un criptosistema de clave pública basado en códigos detectores - correctores de errores; en los años 80 V. Varadharajan propuso distintas estructuras de anillos que pueden ser aplicados en la generalización del sistema RSA; en 1984 Lidl y Müller proponen polinomios de permutación; en 1985, de forma independiente V. Miller y N. Koblitz usan la teoría de curvas elípticas, para crear criptosistemas, estas curvas fueron propuestas por Lenstra para factorizar números enteros; en 1988 J. Buchmann y H. Williams proponen usar campos cuadráticos reales e

imaginarios; en 1995 R. Scheidler y H. Williams usan campos ciclotómicos, etc. Otro tipo de protocolo propuesto recientemente por el grupo de la IBM usa la teoría de incertidumbre y se le conoce como criptografía cuántica.

Las universidades y compañías que actualmente se dedican a investigar y desarrollar tecnología en criptografía son: University of Waterloo, Massachusetts Institute of Technology (MIT), University of California in Berkeley, Stanford, University of Wisconsin in Milwaukee, the Royal Holloway University of London, y entre las compañías privadas están American Telegraph and Telephone (AT&T), Nippon Telegraph and Telephone (NTT), RSA Data Security, IBM, Siemens, Matsushita, Certicom, Thompson, etc. Pierre es profesor e investigador en la ENSTA (Ecole Nationale Supérieure de Techniques Avancées (Escuela Nacional Superior de Técnicas Avanzada). Su campo de investigación son los criptosistemas basados en la teoría de códigos correctores de errores. También existe un grupo de investigadores de la Universidad George Mason, de Virginia, que trabajan desde hace años en una herramienta capaz de detectar imágenes esteganografiadas en Internet. La novedosa ciencia, denominada esteganálisis, permite detectar información escondida en imágenes o archivos de sonido.

Para concluir, concebir sistemas criptográficos requiere sistemas con unos cimientos matemáticos suficientes que permitan proveer utilidades para medir y cuantificar su resistencia a eventuales ataques y, por qué no, encontrar el "Santo Grial" de la criptografía: el sistema incondicionalmente seguro.

Criptografía Antigua

1) Procedimientos clásicos de cifrado

Aunque los historiadores afirman que la criptografía está presente en todas las civilizaciones de la antigüedad, es conveniente resaltar que todos los ejemplos documentados que presentan son puntuales, ya que ninguna de estas civilizaciones utilizó de forma común la criptografía. Ningún imperio de aquella época se sirvió de dicha ciencia para enviar sus correspondencias confidenciales, sólo en contadas ocasiones hacían uso de ella.

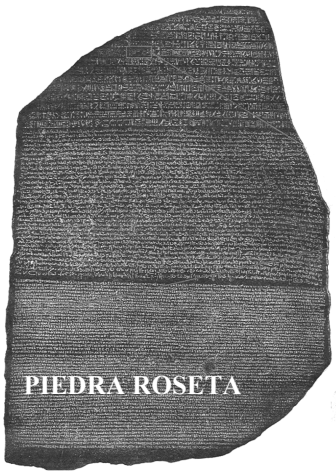
El uso regular de la criptografía comienza en la Edad Media, con los árabes, y en Europa durante el Renacimiento. En la antigüedad las pocas muestras de criptografía son muy simples, sin embargo es de vital importancia comenzar por dichas muestras, no sólo por curiosidad histórica, sino porque en ellas se encuentra la base de la criptografía que vendrá después.

1.1 El ocultamiento de la información en las primitivas civilizaciones

Cuestiones militares, religiosas y comerciales impulsaron desde tiempos remotos el uso de escrituras secretas. Las primitivas civilizaciones que tuvieron relevancia en la historia de la criptografía fueron las civilizaciones: egipcia, mesopotámica china e india.

CIVILIZACIÓN EGIPCIA. Escritura jeroglífica: aparece después de los 3000 A.C. y consiste en una escritura fonética que incluye ocasionalmente sema-gramas. Desaparece en el siglo IV D.C. prohibida por el Cristianismo y se sustituye pues, por la escritura copta.

La escritura jeroglífica representa los primeros precedentes de cifrado, el primer texto realmente relacionado con la criptografía del que se tiene conocimiento, procede precisamente del antiguo Egipto y data aproximadamente de 1900 A.C.; es un grabado en una piedra, la piedra Roseta, de la cámara principal de la tumba de un noble llamado Khnumhotep (noble del faraón Amenemhet) de la ciudad Menet Khufu, a orillas del Nilo. En el que se relatan los actos más relevantes de la vida de ese noble . En realidad la intención de este texto no era ocultar su contenido, que al igual que en los epigramas con jeroglifos no estaba previsto ocultar información, sino despertar el interés, realzar la figura del homenajeado y encumbrar al escriba.


PIEDRA ROSETA

CIVILIZACIÓN MESOPOTÁMICA: la escritura cuneiforme aparece aproximadamente en el año 3300 A.C. Los escribas de la antigua Mesopotamia, al igual que sus colegas egipcios, también cambiaban en ocasiones los signos cuneiformes de su escritura por otros con el fin de alterar la misma. Sin embargo y a diferencia de los egipcios, los escribas mesopotámicos si tuvieron intención de ocultar el significado de la escritura. Los primeros cifrados de esta cultura que se conservan son una tablilla de

arcilla en la que se escribió secretamente una fórmula para la barniz que se emplea en alfarería que seguramente era un valioso tesoro en aquella remota época, data aproximadamente 1500 A.C., además del empleo de signos cuneiformes inusuales y reemplazados por números en la firma y libro de claves.

CIVILIZACIÓN CHINA: Para los esbozos de ocultamiento usaban la esteganografía(13) de escritura en seda o papiro envuelto en cera. Esto constituye una curiosa forma de enviar secretamente mensajes, ya que el mensajero lo ocultaba en su propio cuerpo, tragándoselo.

Otra forma de llevar a cabo la ocultación de un mensaje mediante el método de esteganografía es ocultar el contenido del mismo en un canal de información, pero en paridad, esta técnica no se no se considera criptografía. Por ejemplo, mediante la esteganografía se puede ocultar un mensaje en un canal de sonido, una imagen o incluso en reparto de los espacios en blanco usado para justificar un texto. Este método no tiene porqué ser alternativo a la criptografía, siendo común que ambos métodos se utilicen de forma simultánea para dificultar aún más la labor del criptoanalista.

CIVILIZACIÓN INDIA: en la cual hubo un desarrollo temprano del cifrado, que se recoge en: Artha-Sastra (Libro del Estado) que contiene recomendaciones para los espías. Lolita-Vistara (Vida de Buda). Arthasastra, 300 A.C. es una criptografía para embajadores. Por último pero no menos importe, aunque resulte difícil de creer en el libro del Kamasutra, el cual recomienda para las mujeres el aprendizaje de 64 artes, cómo cocinar, saber vestirse, etc. La lista incluye también algunas menos obvias, como el ajedrez, la encuadernación de libros, etc. El número 45 de la lista es: mlecchita-vikalpa, el arte de la escritura secreta, preconizado para ayudar a las mujeres a ocultar los detalles de sus relaciones amorosas. Todo esto será la base de una de las descripciones más antiguas de codificación llevadas a cabo más tarde por el erudito brahmín Vatsyayana.

(13) disciplina que estudia los principios, métodos y medios de ocultar la existencia de mensajes mediante técnicas artesanales, tintas simpáticas o procesado de señales

CIFRADO DE KAMASUTRA

alfabeto:

A	D	H	I	K	M	O	R	S	U	W	Y	Z
V	X	B	G	J	C	Q	L	N	E	F	P	T

Texto en claro: **COMUNIDAD MYGNET**

Texto cifrado: **MQCESGXVX CPISUZ**

1.2 La sistematización de los métodos de cifrado: La Antigüedad Clásica

Las civilizaciones que tuvieron más relevancia en la antigüedad clásica en lo que a la criptografía se refiere fueron las civilizaciones: griega, romana y hebrea.

GRECIA CLÁSICA. La comunicación secreta se lograba, al igual que la antigua China mediante la ocultación de un mensaje, es decir, aplicando la técnica de esteganografía. La longevidad de la misma corrobora que ofrece un gran nivel de seguridad, pero padece de una debilidad fundamental y esta no es otra que en el caso de descubrirse el mensaje queda revelado automáticamente el contenido de la comunicación. Por eso, paralelamente al desarrollo de la esteganografía, se produjo la evolución de la criptografía, cuyo fin no es ocultar la existencia del mensaje, sino más bien su significado, un proceso que se conoce como codificación.

En Atenas el desarrollo del cifrado se debió a Homero(14), Herodoto(15) y a que también se desarrollo el primer manual con referencias a métodos de cifrado llamado, De la defensa de las Fortificaciones (siglo IV A.C.).

Herodoto, "el padre de la historia" en su libro *Las Historias* hizo una crónica de los conflictos entre Grecia y Persia, que él consideró como un enfrentamiento entre la libertad, los estados griegos y la esclavitud por parte de los persas opresores. Según Herodoto, fue el arte de la escritura secreta lo que salvó a Grecia de ser ocupada por

(14) En La Ilíada (título VI)
(15) En Los Nueve Libros de la Historia (título V. Histeio y título VII. Demarato

Jerjes, el despótico líder del los persas. Debido a que Demarato, un exiliado griego en Persia, grabó los planes persas en un par de tablillas de madera y después los cubrió con cera, ocultando así el mensaje. Ya en su destino, Gorgo, esposa del rey Leónidas adivinó que debajo de la cera debería esconderse algo escrito, gracias a lo cual las ciudades griegas se armaron a tiempo de derrotar a los persas. El mismo Herodoto narra la historia de Histaiaeo en la cual se afeita la cabeza a un mensajero para luego escribir el mensaje sobre su cuero cabelludo y posteriormente esperar a que le crezca el pelo, antes de remitir el mensaje a la persona deseada; de ésta manera el mensajero pudo viajar hasta su destino sin ser molestado, al afeitarse su cabeza fue capaz de mostrar al receptor el mensaje oculto. Obviamente esto fue posible en Grecia, ya que la rapidez en la recepción del mensaje no era el elemento principal.

Particularmente, en Esparta, en el siglo V A.C., el desarrollo del cifrado surgió con la invención del primer criptosistema para uso militar denominado la escítala lacedemonia(16). Se describe como un bastón (vara) redondo en el que se enrolla una cinta de pergamino larga y estrecha como una correa, sobre la cual se escribía el mensaje en forma longitudinal.

ESCÍTALA

Al desenrollar la cinta, las letras aparecían en otro orden, formando una secuencia sin sentido, por lo que era preciso que el receptor del mensaje dispusiera de otro bastón exactamente igual que el del emisor para recuperar el mensaje enrollándolo de nuevo en la cinta. Sin conocer el diámetro del bastón que había jugado el papel de clave, era imposible descifrar el mensaje.

El escritor Polybios (200-118 A.C.) describe un curioso sistema de transmisión de señales (Polibio) que se puede considerar como la primera "cifra" (modo de escribir con caracteres arbitrarios de tal manera que sólo la puede entender el que tenga la clave) histórica de sustitución y el precursor de los sistemas ADFGVX, cifra de los

(16) Desarrollado en la obra vidas paralelas de Plutarco

nihilistas y Bífida. Consta de una tabla (de 5×5) donde se escribe el correspondiente alfabeto:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

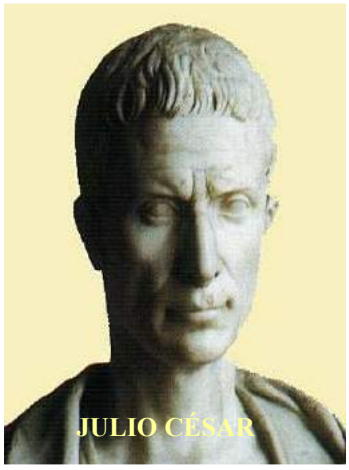
TABLA POLIBIO

Cada letra puede ser representada por dos números. Por ejemplo la letra a con el 11, siendo el primer número el identificador de la fila y el segundo el de la columna. Polybios sugería transmitir estos números por medio de señales luminosas procedentes de antorchas y así enviar mensajes desde largas distancias. Hay que dudar de la efectividad de este método en la transmisión de información, pero no cabe duda que su idea de representar letras por números fue tremendamente importante y estará presente a lo largo de toda la historia criptográfica. Además resulta muy interesante en este método la reducción en el número de caracteres finales, y la división de una unidad en dos partes manipulables separadamente. Lo que ha servido de base para otros sistemas de cifrado, es el caso del sistema Playfair.

ROMA CLÁSICA. Julio César en su guerra de las Galias envió mensajes a sus generales cambiando las letras latinas por las griegas. Utilizó la escritura secreta tan frecuentemente que Valerio Probo escribió un tratado entero a cerca del desarrollo del cifrado, el cual constituyó el primer libro de criptografía que ha desaparecido en la actualidad.

Gracias a la obra de Suetonio *Vidas de los Césares LVI* tenemos una descripción detallada del primer método algorítmico de cifrado: el método César, llamado así por su creador, el emperador romano Julio César (100 A.C.-44 A.C.). Dicho método consiste en una sustitución simple mono alfabeto. Se sustituye cada letra por la que se encuentra

tres posiciones más avanzadas en el orden del alfabeto haciendo una correspondencia cíclica para las últimas letras:



A B C D E F G H I K L M N O P Q R S T V X Y Z
d e f g h i k l m n o p q r s t v x y z a b c

Ejemplo de cifrado:

C I F R A D O T I P O C E S A R
f m i v d g r y m s r f h x d v

Tratamiento matemático:

Si asignamos a cada letra un número (A =00, B =01, C=02,.....Z=25), y consideramos un alfabeto de 26 letras, la transformación criptográfica en términos matemáticos se puede explicar bajo la siguiente fórmula de congruencias:

C≡ (M + 3) (mód 26)
M, corresponde a la letra del mensaje original
C, es la letra correspondiente a M pero en el mensaje cifrado.

CIFRADO

DESCIFRADO

C≡ (M - 3) (mód 26)
M, corresponde a la letra del mensaje original
C, es la letra correspondiente a M pero en el mensaje cifrado.

Aunque Suetonio sólo menciona un cambio del César de tres lugares, es evidente que al utilizar cualquier cambio comprendido entre 1 y 25 lugares, es posible generar 25 cifras distintas.

Obviamente, para descifrar basta con restar 3 al número de orden de las letras del criptograma.

LOS HEBREOS, cuyo desarrollo del cifrado se debe a las Sagradas Escrituras,

las cuales son sustituciones mono alfabéticas. Principalmente se distingue Atbash[17] Albam[18] y Atbah[19].

En el siglo VI A.C. en algunos textos antiguos figuran nombres de personas y ciudades que han sido transformados mediante la sustitución de unas letras por otras. Fundamentalmente se usaba el Atbash, que consiste en permutar la primera letra del alfabeto hebreo por la última y viceversa, análogamente la segunda por la antepenúltima, y así sucesivamente según la figura adjunta:

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Los caballeros templarios utilizaron este método criptográfico. Cuando fueron procesados y la orden fue desmantelada, una de las cuestiones que se utilizaron en su contra fue su adoración de "Baphomet". No se sabía muy bien qué o quién era pero se tomó como un ídolo o dios al que adoraban. Esta causa, junto con otras tan claras o tan "oscuras" como esta, acabaron con la Orden del Temple.

Algunos estudios posteriores han demostrado que si se aplica el atbash a la palabra "Baphomet", resulta la palabra "Sofía", que en griego significa "Sabiduría".

Otra sustitución similar muy utilizada fue el Albam, el la cual la primera letra se intercambiaba con la duodécima, la segunda con la decimotercera y así sucesivamente.

No obstante, no se observa ninguna razón para tal encriptación, quizás el motivo era simplemente dar un aire misterioso a los escritos. La siguiente imagen ilustra de un

(17) Jeremías: 25:26 51:41 51:1
(18) Isaías: 7:6
(19) Talmud

modo gráfico estas sustituciones mono alfabéticas:

La Cábala (s. XII-XIII) fue desarrollada en España. Hermenéutica de las escrituras hebreas: gema tría[20], temurah[21], notarikon[22] .

1.3 Los primeros pasos: cifrado por sustitución y transposición

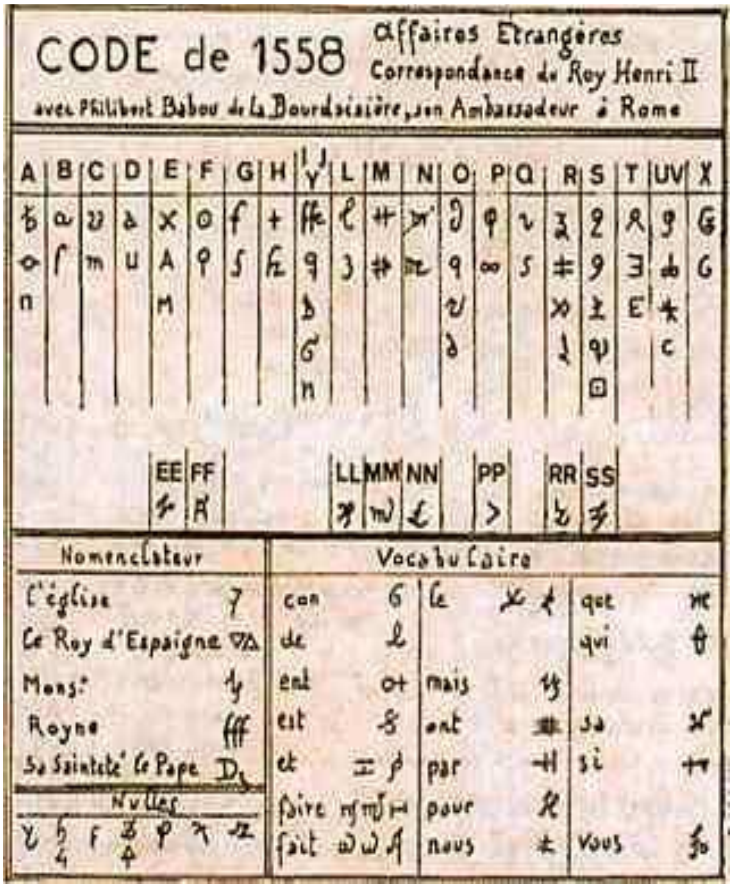
Los cifrados por sustitución y transposición fueron los métodos empleados por la mayoría de las civilizaciones mencionadas anteriormente. Debido a lo cual son dos procedimientos de cifrado básicos que se han ido repitiendo en épocas posteriores hasta llegar a nuestros días.

Sustitución: consiste en establecer una correspondencia entre las letras del alfabeto en el que está escrito el mensaje original y los elementos de otro conjunto, que puede ser el mismo o distinto alfabeto. De esta forma, cada letra del texto claro (texto que se pretende cifrar) se sustituye por su símbolo correspondiente en la elaboración del criptograma. En recepción, el legítimo receptor, que conoce asimismo la

(20) Sustitución de palabras por otras de igual valor numérico
(21) Sustitución anagramática
(22) Ocultación mediante acrósticos o viceversa

correspondencia establecida, sustituye cada símbolo del criptograma por el símbolo correspondiente del alfabeto original, recuperando así la información inicial.

Cifrado utilizado por Babeó, cifrado por sustitución



Transposición: consiste en barajar los símbolos del mensaje original colocándolos en un orden distinto, de manera que el criptograma contenga los mismos elementos del texto claro, pero colocados de tal forma que resulten incomprensibles. En recepción, el legítimo receptor, con conocimiento de la transposición, recoloca los símbolos desordenados del criptograma en su posición original.

Todos los procedimientos criptográficos clásicos se fundamentan en uno u otro principio, o bien en una superposición de ambos.

Al ser el cifrado por sustitución la forma más empleada en la antigüedad, se dedicará el resto de este apartado al mismo; mientras que la explicación y exposición de los cifrados por trasposición se pospondrán hasta el capitulo de criptografía moderna por ser en este momento donde gozaron de mayor difusión.

La definición dada para el método de sustitución es clara y sencilla, lo explica perfectamente; y permite extraer conclusiones de la seguridad que proporciona. Para ello, se presenta un criptosistema en el que se parte de dos alfabetos o colecciones de caracteres. Los textos a cifrar se contemplan como una secuencia de caracteres elegidos en el primer alfabeto, que se llama alfabeto en claro o llano. Los textos cifrados son así mismo sucesiones de caracteres del segundo alfabeto, llamado alfabeto de cifrado, La obtención del texto cifrado a partir del texto en claro se realiza mediante un proceso llamado algoritmo que depende de un dato fundamental: la clave. Dicha clave también es necesaria al receptor del mensaje para su descifrado.

En el cifrado por sustitución el alfabeto llano y el de cifrado tienen el mismo número de caracteres. Frecuentemente los dos alfabetos son el mismo, pero en general no tiene porqué ser así. Ahora cada signo del alfabeto llano se empareja con un único carácter del alfabeto cifrado. Habitualmente, esto se hace colocando en orden los caracteres del alfabeto llano y debajo de cada uno de ellos el signo del alfabeto cifrado con el que se empareja. En el cifrado de Julio César se ha dado un ejemplo de esto.

La clave en el método de sustitución es precisamente el modo en el que se empareja los caracteres de un alfabeto con los del otro. Tanto emisor como receptor deben conocer la clave. Para cifrar, el emisor reemplaza cada carácter del texto en claro por el carácter que tiene asociado en el alfabeto cifrado, según indica la clave. Para descifrar, el receptor del mensaje tiene que cambiar cada signo del texto cifrado por aquel del alfabeto llano que le corresponde. Además el formar claves a partir de palabras es un forma práctica, ya que facilita la memorización de la clave; pero no hay que confundir la clave con la palabra. La clave es, se reitera, el modo en el que se emparejan las letras del alfabeto llano y de cifrado.

Si un intruso recupera fácilmente la clave, se concluye que es capaz de hacerse con unas pocas líneas de texto pleno y su correspondiente cifrado, lo que se llama ataque con texto pleno. Sólo tiene que ir leyendo una a una las letras del texto en claro y cotejarlas con sus correspondientes del texto cifrado, de ese modo recupera la clave. Obtenida la clave, es fácil descifrar cualquier otro mensaje que se cifre con ella.

Pero la clave puede recuperarse también sin conocer texto pleno alguno. Esto se logra haciendo uso de la gran debilidad del cifrado por sustitución: cada letra del texto en claro se cifra siempre con el mismo signo del alfabeto de cifrado, lo que permite recuperar la clave a partir de unas cuantas líneas de texto cifrado mediante el llamado análisis de frecuencias, que es la técnica de criptoanálisis (más adelante hablaremos de ello) más antigua en la historia de la criptografía.

Para analizar un criptograma se deben llevar a cabo los siguientes pasos: lo primero es averiguar en qué idioma se ha escrito el mensaje en claro. Normalmente esto lo revela el contexto. Sin duda conocer quién ha escrito el texto o a quién va dirigido proporciona una pista fundamental, pero teniendo alguna pista, como por ejemplo que es una de las lenguas occidentales más habladas, se puede dejar la tarea de descubrir el idioma al análisis de frecuencias de la siguiente manera, se cuenta cuántas veces se repite cada signo: es decir, su frecuencia. Si el texto del criptograma hubiese sido formado eligiendo los caracteres de modo aleatorio, cada uno de ellos aparecería aproximadamente el mismo número de veces, las cuales se calcularían como el cociente entre el número total de signos que figuran en el texto y el número de signos diferente que hay. De no ser así, se puede comprobar que hay signos mucho más frecuentes que otros.

Lo mismo sucede con las letras de un idioma. Las palabras se forman uniendo sílabas que, por regla general, contienen una vocal y una o dos consonantes. Puesto que en el alfabeto latino las vocales son 5 y las consonantes 21 (22 si contamos la ñ), se explica que las vocales aparezcan más a menudo que muchas consonantes. Además ocurre que no todas las vocales o consonantes presentan la misma frecuencia.

Cuando se cifra un texto sustituyendo cada letra por otra o por un signo, se oculta su significado; pero no las frecuencias de las letras empleadas. La frecuencia de la letra del texto en claro es la misma que la frecuencia del carácter que lo sustituye. Por tanto los

signos que más abundan en el texto cifrado se han de corresponder con las letras de más frecuencia en el texto en clave. Esta es la idea esencial del análisis de frecuencias, el cual tiene ya más de mil años de antigüedad.

Después de todo esto se afirma que el primer paso para resolver un criptograma por sustitución es conocer las frecuencias de las letras de la lengua con la que se ha escrito el texto en claro. Seguramente casi todos los servicios secretos del mundo disponen de los datos de las frecuencias de las letras de mucho de los idiomas que se hablan en el mundo, en especial de las lenguas habladas en sus países vecinos. Pero no es necesario recurrir a esto, los libros de criptografía incluyen las frecuencias de las lenguas más populares. Y probablemente para cada idioma hay una dirección en Internet con las frecuencias de sus letras.

Así pues, se elabora una tabla con las frecuencias en tanto por ciento de cada letra para cada idioma que se quiera investigar, y se va analizando dicha tabla para descubrir el idioma. También se ha de tener en cuenta, no sólo las letra, sino cualquier otro signo, de manera que puedan intervenir los números, aunque son muy poco frecuente, salvo en texto especializados, los signos de puntuación, que suelen presentar una frecuencia intermedia, pero elevan el número de caracteres del alfabeto, y, por supuesto, merece una atención especial el espacio en blanco que se usa para separar las palabras. Es con diferencia el signo más frecuente. Por tanto el espacio en blanco suele tener una frecuencia en torno al 20% en los textos en claro. De todos modos existe la posibilidad de que el criptograma no contenga un signo de estas características, lo que implica automáticamente que el texto en claro se ha contraído sin espacios en blanco, lo cual es una buena idea para que descifrar el criptograma resulte más complejo.

Para proceder a descubrir el idioma se comparan las frecuencias del texto cifrado con las de la tabla confeccionada anteriormente, como lo que hay que comparar son listas de números, en matemáticas hay varias maneras de medir "la distancia" entre dos listas de números. La más utilizada es, sin duda, la suma de los cuadrados de las diferencias de sus números; es decir, se restan los primeros números de cada lista y el resultado se eleva al cuadrado. Seguidamente se hace lo mismo con los segundos, posteriormente los terceros y así sucesivamente. Finalmente se suman todas las cantidades calculadas, y esta

suma es la distancia. Por todo esto se procede entonces a calcular las distancias entre las frecuencias del texto cifrado y las frecuencias de las letras de cada uno de los idiomas.

Una vez que se sabe el idioma al pertenece el texto en claro, el siguiente paso es asociar las letras más frecuentes en ese idioma con los signos que más se repiten en la cifra y establecer las pertinentes conclusiones y deducciones.

Se ha de tener en cuenta que además de todo lo expuesto anteriormente, en un idioma, no sólo hay frecuencias de letras una a una, sino también bloques de dos letras (bigramas) y de tres letras (trigramas) que se repiten con bastante frecuencia, por lo que las estadísticas cuentan también dichos bloques, y nosotros debemos hacer los propio en nuestro criptograma a descifrar. Con un ordenador este proceso es inmediato, pero sin él es penoso. Con los datos obtenidos de estos cálculos se va descubriendo que símbolo del texto cifrado, se corresponde con que otro símbolo del texto en claro y así se va descifrando el criptograma.

Sin embargo, no se puede estar seguro de la validez total de las conclusiones. El argumento realizado es del todo correcto, pero no puede afirmarse lo mismo de las premisas. Éstas eran sólo las más probables. Se ha basado todo en el supuesto de que los símbolos más frecuentes en el idioma elegido se transforman en los signos más comunes del criptograma. Es lo más probable, pero no es seguro cien por cien. No obstante, enseguida se puede saber, contando las apariciones en el texto cifrado de los signos descubierto para restárselo a la suma total de signos que hay en el criptograma y ver que proporción se ha logrado descifrar, Si dicha proporción es alta, y todo es correcto, al restituir los signos por sus verdaderos símbolos, el texto en claro caerá por sí solo; si no se mostrarán incoherencias y se habrá de corregir algunas de las conclusiones anteriores.

1.4 Ejemplos históricos de cifrado por sustitución y transposición

Un ejemplo sencillo de cifrado por transposición consiste en escribir al revés las palabras de un texto. Cómo ejemplo histórico de cifrado por transposición se puede señalar la escítala lacedemonia, anteriormente mencionada en la civilización griega, en la cual ha de reseñarse que por el camino, la cinta de pergamino no era más que una sucesión de símbolos del alfabeto griego colocados en un orden ininteligible. Al colocar

de nuevo el destinatario la cinta alrededor de su propio bastón, aparecía el mensaje de origen.

Pero los demás ejemplos históricos que han sido presentados anteriormente en cada una de las civilizaciones, han sido cifrados por sustitución, que es sin duda la forma de comunicación secreta más empleada en la antigüedad. Algunos ejemplos históricos del cifrado por sustitución:

Cifrado de César (S. I A.C.). Sustituye la primera letra del alfabeto por la cuarta; la segunda por la quinta, y así sucesivamente con todas las demás estableciendo un ciclo con las últimas letras. Los términos matemáticos y un ejemplo ya está expuesto en un apartado anterior. La debilidad de este método radica en que la frecuencia de aparición de cada letra en el texto en claro se refleja exactamente en el criptograma. Conociendo la letra de mayor frecuencia en el tratamiento utilizado, queda automáticamente establecida la correspondencia.

Cifrado de Vigenère (1586). Es una generalización del cifrado anterior, con la particularidad de que la clave toma sucesivamente diferente valor. Ejemplo:

Mensaje:	PARIS	VAUT	BIEN	UNE	MESSE
Clave:	LOUPL	OUPL	OUPL	OUP	LOUPL
Criptograma:	AOLXD	JUJE	PCTY	IHT	XSMHP

En términos matemáticos:

$Y_i = (X_i \oplus Z_i)$ (mód 26)
Z_i = L, O , U, P, alternativamente
26 el número de letras del alfabeto

Se observa que a una misma letra en el texto en claro le pueden corresponder diferentes letras en el texto cifrado. La recuperación del mensaje original es análoga al procedimiento de César. Aunque el cifrado de Vigenère fue considerado seguro durante

siglos, el método Kasiski (incidencia de las coincidencias) publicado en 1863, consiguió romperlo.

La imagen siguiente muestra la tabla empelada en este código para el idioma inglés:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig- Tablero Vigènere para el alfabeto inglés

Cifrado de Beaufort (1710). Es una modificación del cifrado anterior, con la particularidad de que se suma la clave con la inversa de cada símbolo del texto en claro. Ejemplo:

Mensaje:	THIS	IS	THE	SAME	OLD	STUFF
Clave:	WIND	WI	NDW	INDW	IND	WINDW
Criptograma:	DBFL	OQ	UWS	QNRS	UCA	EPTYR

En términos matemáticos:

$Y_i = (Z_i \oplus (-X_i))$ (mód 26)
Z_i = W, I , N, D, alternativamente
26 el número de letras del alfabeto

En recepción, el procedimiento se repite de igual forma, obsérvese que el cifrado y descifrado se reduce a la misma operación. Este tipo de cifrado se conoce como cifrado recíproco o involutivo: F [F (texto claro)]= texto claro; aplicando dos veces la misma transformación F, se obtiene el texto original. Por otra parte, las debilidades de este método son las mismas que las del método Vigenère.

$X_\iota = (Z_i \oplus (-Y_i)) = (Zi \oplus (-Z_i) \oplus X_i)$ (mód 26)
Z = W, I , N, D, alternativamente
26 el número de letras del alfabeto

Cifrado de Vernam (1917). Representa el caso límite del cifrado de Vigenère. Emplea un alfabeto binario, pues inicialmente se utiliza para comunicaciones telegráficas haciendo uso del código Baudot (cinco dígitos binarios por carácter alfabético). La operación aritmética es la suma módulo 2, y la clave una secuencia binaria aleatoria de la misma longitud que el texto en claro. Ejemplo: para el mensaje original "come soon" en código ASCII se tiene:

Mensaje:	00011	01111	01101	00101	10011	01111	01111	01110
Clave:	11011	00101	01011	00110	10110	10101	01100	10010
Criptograma:	11000	01010	00110	00011	00101	11010	00011	11100

Para recuperar el mensaje original se suma nuevamente al criptograma la secuencia aleatoria, ya que adición y sustracción coinciden en la aritmética módulo 2. La originalidad del procedimiento Vernam radica en que la clave se utiliza solamente una vez, pues, en caso contrario, sucesivos criptogramas concatenados darían lugar a un cifrado tipo Vigenère.

El método Vernam fue utilizado durante la segunda Guerra Mundial por espías de diversas nacionalidades, a los que se les daba una secuencia binaria aleatoria con la recomendación de utilizarla para un único proceso de cifrado. En círculos criptográficos se creyó durante mucho tiempo en la seguridad total de este método, pero fue Shannon, en 1949, el primero en dar una prueba teórica de la misma.

Tras estos ejemplos, decir que hay más pero con los aquí mencionados puede uno hacerse una idea de cómo funciona claramente el cifrado por sustitución y como se las ingeniaron antaño para cifrar y descifrar mensajes con este tipo de cifrado.

1.5 Condiciones del secreto perfecto

Shannon definió sus condiciones de secreto perfecto partiendo de dos hipótesis básicas:

■ La clave secreta se utilizará solamente una vez, a diferencia de lo que sucedía en los métodos clásicos, en los que la clave era fija.

■ El enemigo criptoanalista tiene acceso sólo al criptograma; luego está limitado a un ataque sobre texto cifrado únicamente.

Basadas en estas dos hipótesis, Shannon enunció sus condiciones de secreto perfecto, las cuales pueden sintetizarse en:

Un sistema criptográfico verifica las condiciones de secreto perfecto si el texto claro X es estadísticamente independiente del criptograma Y, lo que en lenguaje probabilístico puede expresarse como:

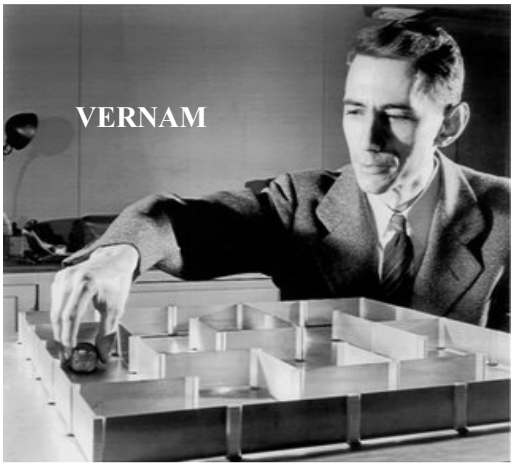
$$P(X = x \mid Y = y) = P(X = x)$$

Para todos los textos fuente $x = (x_1, x_2, \ldots x_M)$ y
Todos los posibles criptogramas $y = (y_1, y_2, \ldots y_N)$

Por lo tanto, la probabilidad de que la variable aleatoria X tome el valor x es la misma tanto si se conoce o no el valor tomado por la variable aleatoria Y, es decir empleando un lenguaje sencillo, esto equivale a expresar que la información sobre el texto claro aportada por el criptograma es nula. De tal forma que cualquier persona ajena no puede hacer una mejor estimación de X con conocimiento de Y que la que haría sin

su conocimiento, independientemente del tiempo y recursos computacionales de los que disponga para el procesado del criptograma.

Análogamente, y apoyándose en el concepto de entropía, Shannon determino la menor cantidad de clave necesaria para que pudieran verificarse las condiciones del secreto perfecto. Así pues, la longitud de la clave K tiene que ser, al menos, tan larga como la longitud del texto claro M:



$$K \geq M$$

La desigualdad se convierte en igualdad para el cifrado de Vernam.

Una vez conocidas las condiciones del secreto perfecto, la primera pregunta que nos surge es: ¿existen cifradores perfectos? La respuesta a esta pregunta es afirmativa como seguidamente se demostrará.

Consideremos un método de cifrado donde el texto claro, criptograma y clave tomen valores de un alfabeto L- ario

$$\{0, 1, \ldots, L\text{-}1\}$$

y en el que la longitud de la clave K, criptograma N y texto claro M coincidan entre sí

$$K = N = M$$

Entonces, el número de posibles textos claros, criptogramas y claves son iguales entre sí e iguales a L^M

Suponiendo:

■ La clave se elige de forma totalmente aleatoria;

$$P(Z = z) = L^{-M}$$
Para todos los L^{M} posibles valores z de la clave secreta

■ La transformación del cifrado es

$$Y_i = X_i \quad Z_i, (i = 1, \ldots., M)$$
donde $\oplus$ denota la adición modulo L, elemento a elemento

Fijado un texto fuente X = x, para cada posible valor de la clave

$$Z = z_j, (j = 1, \ldots, L^{M})$$

le corresponde únicamente un criptograma

$$Y = y_j, (j = 1, \ldots, L^{M})$$

Por consiguiente y de acuerdo con la primera condición, resulta sencillo ver que a un mismo texto claro X = x le puede corresponder con igual probabilidad cualquiera de los L^{M} posibles criptogramas, luego

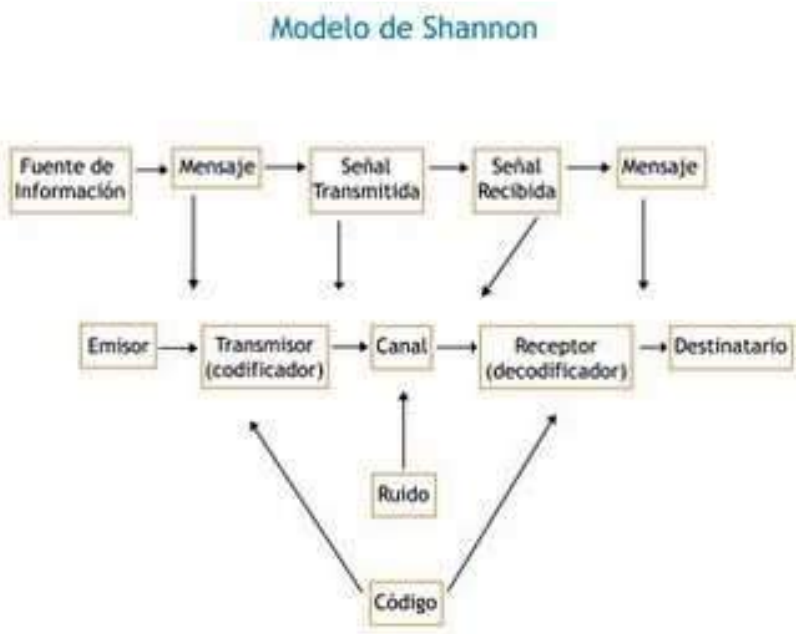
$$P(Y = y) = P(Y = y \mid X = x) = L^{-M}$$

Por tanto, la información que aporta el criptograma sobre el texto claro es nula, X e Y son estadísticamente independientes y la transformación módulo L verifica las condiciones de secreto perfecto.

Cuando particularmente L = 2, simplemente nos encontramos ante el cifrado Vernam.

Es importante resaltar que el tipo de cifrado módulo L brinda total seguridad respecto a la estadística del texto claro, lo cual es fundamental, ya que sería muy peligroso que la seguridad de un método de cifrado dependiera de la naturaleza estadística del lenguaje utilizado en el mensaje a cifrar.

Una vez planteadas y conocidas las condiciones de secreto perfecto de Shannon,



Podemos evaluar los métodos criptográficos que anteriormente hemos citado:

Cifrado de César. Utiliza una clave de longitud menor que el texto claro, la clave es fija y se reutiliza continuamente para cada letra del mensaje a cifrar. Por lo tanto, se ve claramente que este procedimiento no cumple las condiciones de Shannon, y consecuentemente la operación módulo 21 deja al descubierto en el criptograma la frecuencia de aparición de las letras del texto fuente.

Cifrado de Vigenere. La clave usada es más larga que en el método anterior, pero todavía sigue siendo más corta que la longitud del mensaje. Por otro lado, la clave no es una secuencia aleatoria, sino una palabra del lenguaje, sometida a sus reglas y características, que reutiliza sucesivas veces. Según las condiciones de Shannon, no constituye un método de cifrado perfecto, y si bien, se crea más dificultad que en el cifrado de César, el criptoanalista termina por encontrar alguna estrategia (método Kasiski) que le permita determinar la estadística del texto claro a partir del criptograma y, posteriormente, romper el criptograma.

Cifrado Vernam. La clave y el texto claro son de igual longitud, además dicha clave es una secuencia perfectamente aleatoria que solo se utiliza una vez. En este caso

podemos afirmar que se cumplen las condiciones de secreto perfecto de Shannon, ya que la suma módulo 2 con secuencia aleatoria ofrece un perfecto enmascaramiento del contenido y estadística del texto claro. Podría decirse que dentro del panorama criptográfico actual, el cifrado de Vernam es el único procedimiento incondicionalmente seguro, es decir el procedimiento con seguridad probada matemáticamente.

2) Edad Media. Islam: origen del criptoanálisis

2.1 Introducción al criptoanálisis

La criptología es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: criptografía y criptoanálisis. La criptografía se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial. El criptoanálisis, por su parte, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original. Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su criptoanálisis correspondiente

Criptoanálisis (del griego kryptós, "escondido" y analýein, "desatar") es el estudio de los métodos para obtener el sentido de una información cifrada, sin acceso a la información secreta requerida para obtener este sentido normalmente. Típicamente, esto se traduce en conseguir la clave secreta. En el lenguaje no técnico, se conoce esta práctica como romper o forzar el código, aunque esta expresión tiene un significado específico dentro del argot técnico.

Criptoanálisis también se utiliza para referirse a cualquier intento de sortear la seguridad de otros tipos de algoritmos y protocolos criptográficos en general, y no solamente el cifrado. Sin embargo, el criptoanálisis suele excluir ataques que no tengan como objetivo primario los puntos débiles de la criptografía utilizada; por ejemplo, ataques a la seguridad que se basen en el soborno, la coerción física, el robo, el keylogging y demás, aunque estos tipos de ataques son un riesgo creciente para la seguridad informática, y se están haciendo gradualmente más efectivos que el criptoanálisis tradicional.

Aunque el objetivo ha sido siempre el mismo, los métodos y técnicas del criptoanálisis han cambiado drásticamente a través de la historia de la criptografía,

adaptándose a una creciente complejidad criptográfica, que abarca desde los métodos de lápiz y papel del pasado, pasando por máquinas como Enigma(23) hasta llegar a los sistemas basados en computadoras del presente.

Los resultados del criptoanálisis han cambiado también: ya no es posible tener un éxito ilimitado al romper un código, y existe una clasificación jerárquica de lo que constituye un ataque en la práctica. A mediados de los años 70 se inventó una nueva clase de criptografía: la criptografía asimétrica. Los métodos utilizados para romper estos sistemas son por lo general radicalmente diferentes de los anteriores, y usualmente implican resolver un problema cuidadosamente construido en el dominio de la matemática pura. El ejemplo más conocido es la factorización de enteros.

El criptoanálisis ha evolucionado conjuntamente con la criptografía, y la competición entre ambos puede ser rastreada a lo largo de toda la historia de la criptografía. Las claves nuevas se diseñaban para reemplazar los esquemas ya rotos, y nuevas técnicas de criptoanálisis se desarrollaban para abrir las claves mejoradas. En la práctica, se considera a ambas como las dos caras de la misma moneda: para crear un sistema criptográfico seguro, es necesario tener en cuenta los descubrimientos del criptoanálisis. De hecho, hoy en día se suele invitar a la comunidad científica a que trate de romper las nuevas claves criptográficas, antes de considerar que un sistema es lo suficientemente seguro para su uso.

El criptoanálisis está íntimamente ligado a cada algoritmo de cifrado. Cuando alguien diseña un criptosistema, tiene que tener en cuenta todos los posibles ataques que éste puede sufrir, y que cada mecanismo de ocultación que implementa está respondiendo a un hipotético procedimiento de criptoanálisis.

No se puede hablar de un procedimiento general de criptoanálisis; cada algoritmo ha de ser atacado mediante un procedimiento adecuado a su estructura. No obstante, el usuario de un sistema criptográfico ha de tener presente que la robustez del algoritmo de cifrado no es el elemento definitivo en la seguridad; hay otros aspectos a tener en cuenta, principalmente la utilización del algoritmo y los protocolos con que se usa. Los algoritmos de cifrado utilizados actualmente resultan tan robustos y su rotura exige tal

(23) Máquina para cifrar utilizada por los nazis durante la Segunda Guerra Mundial

esfuerzo computacional, que resulta mucho más práctico, el atacar al protocolo o simplemente emplear métodos de espionaje tradicionales.

En la pasada guerra, Alemania tenía el equipo más formidable de criptoanalistas de todas las potencias en conflicto. Italia conseguía resultados parecidos sin criptoanálisis, le bastaba con robar información y claves en la fuente chantajeando, comprando y seduciendo a enemigos además de colocar micrófonos ocultos, oír a través de tabiques, etc. Recíprocamente, la criptografía italiana era igualmente débil, debido a que amigos y enemigos conocían sus claves.

Aunque la criptografía es muy antigua, no aparecen referencias documentadas sobre criptoanálisis. Los primeros procedimientos de criptoanálisis descritos se deben al oficial e instructor de mamelucos sirios y egipcios Alí Ibn ad Duraihim ben Muhammad al Mausili (1312-1361). Esencialmente recomendaba emplear procedimientos elementales de análisis basados en la redundancia del idioma analizado.

2.2 El Islam y el origen del criptoanálisis

La Edad de oro del Islam, también conocida como *Renacimiento islámico* data comúnmente a partir del siglo VIII hasta el siglo XIII. Durante este periodo, ingenieros, académicos y comerciantes del mundo islámico contribuyeron enormemente en aspectos como las artes, agricultura, economía, industria, literatura, navegación, filosofía, ciencias y tecnología, preservando y mejorando el legado clásico por un lado, y añadiendo nuevas invenciones e innovaciones propias.

Hay que hacer una mención especial a como se desarrolló la criptología en el Islam. La riqueza de la cultura islámica fue en gran medida el resultado de una sociedad rica y pacífica. Los califas abasíes estaban menos interesados en la conquista que sus predecesores, y en vez de ello, dirigieron sus esfuerzos a establecer una sociedad organizada y próspera. Los impuestos bajos fomentaron el crecimiento de los negocios, así como del comercio y la industria, mientras que las leyes estrictas redujeron la corrupción y protegieron a los ciudadanos. Todo ello se apoyaba en un eficaz sistema de gobierno, y a su vez, los gobernantes se apoyaban en la comunicación segura, lograda mediante el uso de la codificación. Además de cifrar los delicados asuntos de estado, está

documentado que los funcionarios protegían los archivos de los impuestos, demostrando un uso general y rutinario de la criptografía. Aún más evidencia de ello nos llega de muchos manuales administrativos, tales como el Adab al-Kuttab(24) del siglo x, que incluye secciones dedicadas a la criptografía.

Los gobernantes y funcionarios utilizaban generalmente un alfabeto cifrado que era simplemente una variación del orden del alfabeto llano, tal como lo describí antes, pero también usaban alfabetos cifrados que contenían otros tipos de símbolos. Por ejemplo, la *a* del alfabeto llano podía ser reemplazada por # en el alfabeto cifrado, la *b* podía ser reemplazada por +, y así sucesivamente. La cifra de sustitución mono alfabética es el nombre general que se da a cualquier cifra de sustitución en la que el alfabeto cifrado consiste en letras o en símbolos, o en una mezcla de ambos. Todas las cifras de sustitución que hemos visto hasta ahora pertenecen a esta categoría general.

Si los árabes se hubieran limitado a familiarizarse con el uso de la cifra de sustitución mono alfabética no merecerían una mención muy significativa en ninguna historia de la criptografía. Sin embargo, además de utilizar cifras, los eruditos árabes también eran capaces de destruirlas. De hecho, fueron ellos quienes inventaron el criptoanálisis, la ciencia de descifrar un mensaje sin conocer la clave. Mientras el criptógrafo desarrolla nuevos métodos de escritura secreta, es el criptoanalista el que se esfuerza por encontrar debilidades en estos métodos, para penetrar en los mensajes secretos. Los criptoanalistas árabes lograron encontrar un método para descifrar la cifra de sustitución mono alfabética, la cual había permanecido invulnerable durante muchos siglos.

El criptoanálisis no podía ser inventado hasta que una civilización hubiese alcanzado un nivel suficientemente sofisticado de erudición en varias disciplinas, incluidas las matemáticas, la estadística y la lingüística. La civilización musulmana constituyó una cuna ideal para el criptoanálisis porque el Islam exige justicia en todas las esferas de la actividad humana, y lograr esto requiere conocimiento. Todo musulmán está obligado a buscar el conocimiento en todas sus formas, y el éxito económico del califato abasí significó que los eruditos tuvieron el tiempo, el dinero y los materiales necesarios para cumplir con su deber. Se esforzaron por adquirir los conocimientos de las civilizaciones anteriores, obteniendo textos egipcios, babilonios, indios, chinos,

(24) El Manual de los Secretarios

parsis, sirios, armenios, hebreos y romanos, y traduciéndolos al árabe. En el año 815, el califa Al Mamún estableció en Bagdad la Bait al Hik-mah(25), una biblioteca y un centro de traducción.

A la vez que ganaba conocimiento, la civilización islámica fue también capaz de esparcirlo, porque había adquirido el arte de hacer papel de los chinos. La fabricación de papel dio lugar a la profesión de warraqin, (los que manejan el papel), máquinas fotocopiadoras humanas que copiaban manuscritos y suministraban a la creciente industria editorial. En su punto álgido, decenas de miles de libros se publicaban cada año, y en un solo suburbio de Bagdad había más de cien librerías. Junto a clásicos como *Los cuentos de las mil y una noches*, estas librerías vendían también libros de texto de todos los temas imaginables y contribuían a apoyar la sociedad más alfabetizada y culta del mundo.

Además de una mayor comprensión de temas seculares, el invento del criptoanálisis se basó también en el crecimiento de la erudición religiosa. Se establecieron importantes escuelas teológicas en Basora, Kufa y Bagdad, en las que los teólogos examinaban minuciosamente las revelaciones de Maho-ma, tal como aparecían en el *Corán*. Los teólogos tenían interés en establecer la cronología de las revelaciones, lo que hacían contando las frecuencias de las palabras contenidas en cada revelación. La teoría era que ciertas palabras habían evolucionado relativamente hacía poco, y por eso, si una revelación contenía un alto número de estas palabras más nuevas, indicaría que apareció después en la cronología. Los teólogos estudiaron también el Ha-dith, que consta de las afirmaciones diarias del Profeta. Los teólogos trataron de demostrar que cada aseveración era efectivamente atribuible a Maho-ma. Esto se hizo estudiando la etimología de las palabras y la estructura de las frases, para comprobar si textos particulares mostraban consistencia con los patrones lingüísticos del Profeta.

2.3 Ataques a un Criptosistema

Un criptosistema se puede atacar de muchas formas; la más directa sería la que hace uso únicamente del análisis del mensaje cifrado o criptograma. Se trata de un análisis pasivo. Pero en la realidad se pueden producir más ataques, apoyados en cierto

(25) Casa de la Sabiduría

conocimiento adicional o bien en cierto grado de intervención, en cuyo caso estaremos frente a un ataque activo.

Las posibilidades de éxito para atacar un criptosistema dependen en gran manera de las circunstancias que lo rodean y de la información de que se dispone. No es lo mismo atacar un criptosistema desconocido que uno conocido. El ataque a uno desconocido requiere en primer lugar, identificar o imaginarse cómo opera el algoritmo de cifrado. Por ello, los militares prefieren emplear sistemas exclusivos, no divulgados, cuya estructura y modo de trabajo se guarda celosamente. Pero esto puede ser un arma de dos filos; si la seguridad radica más bien en la ignorancia del sistema que en robustez intrínseca del algoritmo de cifrado, éste puede quedar comprometido si un oponente logra robar la información sobre su diseño. Hay ejemplos históricos de la posibilidad de reconstruir un sistema observando simplemente los mensajes cifrados, como fue el caso de la reconstrucción a ciegas por criptoanalistas estadounidenses de la máquina japonesa Purple.

A la hora de realizar un criptoanálisis, cuanta más información se posea, más fácil será dicha realización. Esencialmente, la importancia práctica del ataque depende de las respuestas dadas a las siguientes preguntas:

■ ¿Qué conocimiento y capacidades son necesarios como requisito?

■ ¿Cuánta información adicional secreta se deduce del ataque?

■ ¿Cuánto esfuerzo se requiere? (es decir, ¿cuál es el grado de complejidad computacional?)

Las situaciones más frecuentes para atacar se exponen a continuación en orden de facilidad creciente:

■ Sólo se conoce el criptograma. Es la situación más difícil, pero el ataque puede ser factible si se conoce o sospecha la lengua en que está escrito el mensaje.

■ Sólo se conoce el criptograma, pero éste va salpicado con partes en claro sin cifrar. Se apoya en que con toda probabilidad habrá palabras coincidentes en los fragmentos en claro y en el texto cifrado.

■ Se conocen varios criptogramas diferentes correspondientes al mismo texto en claro, cifrados con claves diferentes o vectores de inicialización.

■ Se conocen el criptograma y el texto claro correspondiente. Incluye el caso de que no se conozca enteramente el texto en claro, pero sí partes de él, o bien que se conozcan palabras probables.

■ Se conoce el criptograma correspondiente a un texto claro escogido por el criptoanalista, o bien se conoce el texto descifrado correspondiente a un criptograma elegido por el criptoanalista.

■ Se conoce el texto descifrado correspondiente a un criptograma elegido de forma adaptativa por el criptoanalista en función de análisis previos.

■ Se conoce la clave o al menos se puede limitar el espacio de claves posibles. Es el típico ataque a un sistema en el que las claves son elegidas manualmente por una persona; entonces éste suele elegir como clave palabras con sentido (fáciles de recordar), lo que hace disminuir tremendamente el número de claves utilizadas.

Estos tipos de ataque difieren evidentemente en la plausibilidad de que ocurran en la práctica. Aunque algunos son más probables que otros, los criptógrafos suelen adoptar un enfoque conservador y asumir el peor caso imaginable cuando diseñan algoritmos, razonando que si un sistema es seguro incluso contra amenazas tan poco realistas, entonces debería resistir al criptoanálisis en el mundo real también.

Todos estos casos pueden estar modulados por el hecho de que se conozca o no el criptosistema en uso, que es lo que supone la gran diferencia entre criptografía civil y estatal. Los ataque pueden ser clasificados:

■ Ruptura total: el atacante deduce la clave secreta

■ Deducción global: el atacante descubre un algoritmo funcionalmente equivalente para el cifrado y descifrado de mensajes, pero no obtiene la clave.

■ Deducción local (o de instancia): el atacante descubre textos planos ó cifrados adicionales a los conocidos previamente.

■ Deducción de información: el atacante descubre alguna información en el sentido de Shannon que no era conocida previamente.

■ Distinción del algoritmo: el atacante puede distinguir la información cifrada de una permutación al azar.

Complejidad: Los ataques se pueden categorizar por cantidad de recursos que requieren. Éstos pueden tomar la forma de:

■ Tiempo: el número de operaciones primitivas que deben ser realizadas. Esta categoría es bastante vaga; las operaciones primitivas podrían considerarse como instrucción básicas de computación, como una suma, una operación XOR, un desplazamiento bit a bit, etcétera, o como métodos de cifrado enteros.

■ Memoria: la cantidad de almacenamiento necesario para realizar el ataque.

■ Dato*s*: la cantidad de textos planos y cifrados necesaria.

En la criptografía académica, una debilidad o una ruptura en un algoritmo se definen de una manera bastante conservadora. Bruce Schneier resume esta posición de la siguiente manera: "Romper un cifrado simplemente significa encontrar una debilidad en el cifrado que puede ser explotada con una complejidad inferior a la de la fuerza bruta. No importa que la fuerza bruta pudiera requerir 2^{128} cifrados; un ataque que requiera 2^{110} cifrados se consideraría una ruptura... puesto de una manera simple, una ruptura puede ser tan sólo una debilidad certificacional: una evidencia de que el código no es tan bueno como se publicita″.

2.4 Ataque por fuerza bruta. Espacio de claves

Cuando un algoritmo es conocido, hay un ataque posible denominado de fuerza bruta, y que consiste en probar todas las claves. Estas formas de ataque obligan a varias precauciones por parte del usuario para no dar facilidades al oponente. Dichas precauciones son:

1 Cuando sea necesario repetir la transmisión de un mensaje cifrado, se hará con la clave original, para evitar el ataque número 3.

2 No se cifrará la información que ya es pública, para evitar el ataque número 4.

3 No se enviará la misma información en claro y en cifrado, aunque se haga por canales diferentes, para evitar el ataque número 4.

4 No se enviarán en una misma comunicación partes en claro y en cifrado, para evitar los ataques números 2 y 4.

5 Se evitará enviar mensajes cifrados, referentes a mensajes en claro recibidos del oponente, para evitar el ataque número 5.

6 Se elegirán las claves de forma aleatoria y carecerán de sentido, para no facilitar un ataque por fuerza bruta basándose en un diccionario reducido y así evitar el ataque número 7.

7 Se procurará incorporar de laguna forma la fecha y hora de producción de un mensaje a la clave, lo que asegura de cierta forma el cambio de clave con cada mensaje.

8 Las claves y algoritmos de cifrado, a ser posible, han de ser secretos y conocidos por un número reducido de personas, para evitar un ataque por fuerza bruta.

9 Se cambiarán las claves con la mayor frecuencia posible y se tratará de evitar el mismo uso de la misma clave con mensajes diferentes, para obligar al oponente que es capaz de romper el algoritmo recuperando la clave, a repetir el proceso de ataque con cada nuevo mensaje.

El ataque por fuerza bruta es el más elemental, cuando se conoce el algoritmo de cifrado y descifrado. Consiste en hacer una prueba exhaustiva con todas las claves posibles, para descifrar un criptograma. No es preciso poseer conocimientos de criptoanálisis, sólo disponer de tiempo y paciencia.

Si la cantidad de claves posibles es pequeña, el trabajo será corto, por el contrario, si la cantidad es muy grande, será largo. Esto lleva la concepto de espacio de claves siendo éste el número total de posibles claves que admite un criptosistema.

En último término, la seguridad de un criptosistema estará limitada por el espacio de claves; pero es posible que se puedan efectuar otros ataques más inteligentes, que reduzcan drásticamente el número de operaciones necesarias para su rotura.

Conviene resaltar que el secreto perfecto es teóricamente posible, ya que bastaría tener un sistema cuya distancia de unicidad fuera mayor que la longitud del mensaje. Se entiende por distancia de unicidad a la longitud de mensaje a partir de la cual, dado un criptograma y un algoritmo de cifrado determinado, tanto la clave como el mensaje claro quedan totalmente determinados. De tal forma que para mensajes de longitud inferior a dicha distancia siempre se podrán encontrar varios tríos de mensaje en claro + criptograma + clave, mientras que para mensajes con longitudes superiores a la distancia de unicidad sólo habrá una clave posible que dé lugar a un mensaje con sentido. Por lo tanto el secreto perfecto podrá alcanzarse mediante dos vías: con una clave cuya longitud sea igual a la del mensaje o con un mensaje aleatorio.

2.5 Criptoanálisis básico

Criptoanálisis clásico

Aunque la expresión criptoanálisis es relativamente reciente, fue acuñada por William F. Friedman en 1920, los métodos para romper códigos y cifrados son mucho más antiguos. La primera explicación conocida del criptoanálisis se debe al sabio árabe del siglo IX, Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi, en su Manuscrito para Descifrar Mensajes Criptográficos. Este tratado incluye una descripción del método de análisis de frecuencias[(26)].

Primera página de Un manuscrito para el descifrado de mensajes criptográficos, de Al-Kindi.

(26) Ibraham, 1992.

El análisis de frecuencias es la herramienta básica para romper los cifrados clásicos. En todas las lenguas conocidas, ciertas letras del alfabeto aparecen más frecuentemente que otras; por ejemplo, en español, las vocales son muy frecuentes, ocupando alrededor del 45% del texto, siendo la E y la A las que aparecen en más ocasiones, mientras que la frecuencia sumada de F, Z, J, X, W y K no alcanza el 2%. Igualmente, se pueden reunir estadísticas de aparición de pares o tríos de letras. El análisis de frecuencias revelará el contenido original si el cifrado utilizado no es capaz de ocultar estas estadísticas. Por ejemplo, en un cifrado de substitución simple (en el que cada letra es simplemente substituida por otra), la letra más frecuente en el texto cifrado sería un candidato probable para representar la letra "E".

El análisis de frecuencias se basa tanto en el conocimiento lingüístico como en las estadísticas, pero al volverse cada vez más complicadas los cifrados, las matemáticas se convirtieron gradualmente en el enfoque predominante en el criptoanálisis. Este cambio fue particularmente evidente durante la segunda Guerra Mundial, cuando los esfuerzos para romper los códigos del Eje requirieron nuevos niveles de sofisticación matemática. Más aún, la automatización fue aplicada por primera vez en la Historia al criptoanálisis, bajo la forma de los dispositivos Bomba y Colossus, una de las primeras computadoras.

Criptoanálisis moderno

RÉPLICA DE UN DISPOSITIVO BOMBE

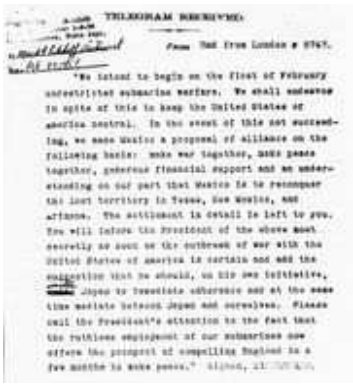
Aunque la computación fue utilizada con gran éxito durante la segunda Guerra Mundial, también hizo posibles nuevos métodos criptográficos que eran órdenes de magnitud más complejos que los utilizados hasta la fecha. Tomada como un todo, la criptografía moderna se ha vuelto mucho más impenetrable al criptoanalista que los métodos de pluma y papel del pasado, y parece que en la actualidad llevan ventaja sobre

los métodos del puro criptoanálisis. El historiador David Kahn escribió: "Son muchos los criptosistemas en venta hoy por parte de cientos de compañías comerciales que no pueden ser rotos por ningún método conocido de criptoanálisis". De hecho, en ciertos sistemas incluso un ataque de texto plano escogido, en el que un fragmento de texto plano seleccionado es comparado con su versión cifrada, no permite conocer el código para romper otros mensajes. En cierto sentido, entonces, el criptoanálisis está muerto. Pero éste no es el final de la historia. El criptoanálisis puede estar muerto, pero, mezclando mis metáforas, hay más de un modo de desollar un gato(27).

Kahn menciona a continuación las mayores posibilidades para la intercepción, la colocación de dispositivos grabadores (bugging), los ataques de canal lateral y la criptografía cuántica como sustitutos de los métodos tradicionales del criptoanálisis.

Kahn podría haberse apresurado demasiado al declarar al criptoanálisis muerto; aún no se han extinguido los cifrados débiles. En medios académicos, se presentan regularmente nuevos diseños, y también son rotos frecuentemente: el cifrado por bloques Madryga, de 1984, demostró ser vulnerable a un ataque con sólo texto cifrado disponible en 1998; FEAL-4, propuesto como sustituto para el algoritmo estándar de cifrado de datos DES fue demolido por una avalancha de ataques de la comunidad académica, muchos de los cuales no eran enteramente realizables en condiciones prácticas. En la industria, igualmente, los cifrados no están exentos de fallos: por ejemplo, los algoritmos AS/1, AS/2 y CMEA, usados en la industria de teléfonos móviles, pueden ser rotos en horas, minutos o incluso en tiempo real por equipo informático ampliamente disponible. En 2001, se demostró que el algoritmo WEP, utilizado para proteger redes Wi-Fi es susceptible de ser atacado mediante un ataque de clave relacionada.

El Telegrama de Zimmerman, descifrado



Los resultados del criptoanálisis

Los criptoanálisis exitosos han influido sin lugar a dudas en la Historia; la capacidad de leer los pensamientos, supuestamente secretos, o los planes de otros puede ser una ventaja decisiva, y nunca con mayor razón que en tiempos de guerra.

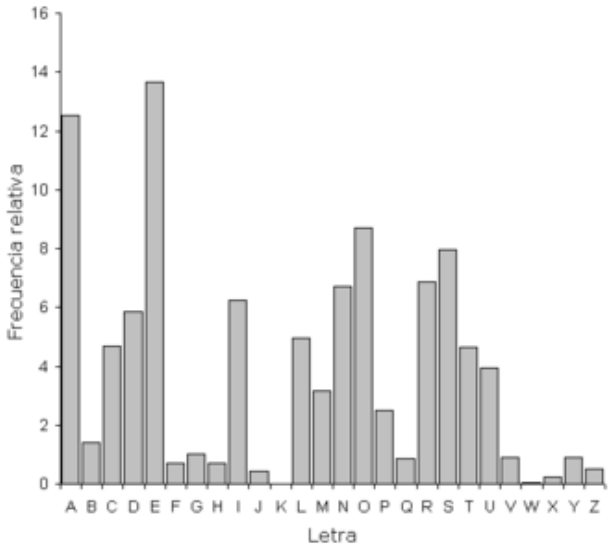
(27) Observaciones sobre el 50 Aniversario de la National Security Agency, 1 de noviembre, 2002

Por ejemplo, durante la primera Guerra Mundial, el descifrado del Telegrama de Zimmerman fue capital para la entrada de los Estados Unidos en la guerra. En la segunda Guerra Mundial, el criptoanálisis de los códigos alemanes, incluyendo la máquina Enigma y el código Lorenz, ha sido considerado desde un factor que apenas acortó la guerra en algunos meses en Europa, hasta un elemento crucial que determinó el resultado final. Los Estados Unidos también se beneficiaron del criptoanálisis del código japonés PURPLE durante la contienda.

Todos los gobiernos han sido conscientes desde antiguo de los potenciales beneficios del criptoanálisis para la inteligencia militar, tanto en lo puramente bélico como en lo diplomático, y han establecido con frecuencia organizaciones dedicadas en exclusiva al descifrado de códigos de otras naciones, por ejemplo GCHQ y NSA, organizaciones americanas todavía muy activas hoy en día. En 2004, surgió la noticia de que los Estados Unidos habían roto los códigos utilizados por Irán.

Cualquier mensaje en claro tiene unas propiedades estadísticas muy particulares, en cuanto a la frecuencia y asociación de letras, que lo diferencian totalmente de la distribución que presentaría un texto generado por un autómata de forma aleatoria. Cada idioma tiene una distribución estadística diferente y a priori es posible determinar combinaciones imposibles de letras y aquellas que son más probables y frecuentes.

Estudiando estas reglas se puede hacer un criptoanálisis heurístico, pero el verdadero análisis sistemático empieza con la aplicación de la Teoría de la Información.



Se define entropía, H(S), de una fuente de información como la cantidad media de información por símbolo emitido por ella. Su fórmula es:

$$H(S)= \sum P(s_i).\log_2 1/ P(s_i) \text{ bits/símbolo}$$

en donde $P(s_i)$ es la probabilidad de ocurrencia del símbolo s_i.

Cuando nos enfrentamos a un criptograma, la primera operación a realizar consistirá en un estudio estadístico para determinar su entropía. En función de ella se podrá determinar el tipo de cifrado. Si resulta que la entropía es igual a la máxima teórica, es decir, si coincide con la de un generador aleatorio, se podría tratar de un cifrado en flujo o en bloque. Pero si la entropía coincide con la de un idioma determinado, se tratará seguramente de una sustitución mono alfabética o de una transposición. Para distinguir entre ambas, será preciso analizar en detalle la distribución frecuencial de cada letra. En el caso de una transposición, la distribución la distribución estadística de cada una de las letras coincidirá con la habitual del idioma en cuestión, y la solución del criptograma consistirá en ordenar las letras. Si el perfil de la distribución estadística coincide con el idioma supuesto, pero no con la habitual de cada símbolo del idioma, pudiera tratarse de una sustitución mono alfabética. La solución se lograría haciendo coincidir los símbolos más frecuentes con las letras más comunes del idioma. En el caso de que la entropía presente valores comprendidos entre los habituales para un idioma y el correspondiente a una distribución uniforme, se tratará de un cifrado Poli alfabético, es decir, que a cada letra del mensaje claro le corresponderán diversas letras en el mensaje cifrado, normalmente dependiendo de la posición ocupada.

3) Edad Moderna.

3.1 Criptografía en la Europa anterior al Renacimiento

Fue probablemente el análisis textual del Corán, de motivación religiosa, lo que llevó a la invención de la técnica del análisis de frecuencias para romper los cifrados por sustitución monoalfabéticos, en algún momento alrededor del año 1000. Fue el avance criptoanalítico más importante hasta la segunda Guerra Mundial. Esencialmente, todos los cifrados quedaron vulnerables a esta técnica criptoanalítica hasta la invención del cifrado poli alfabético por Leon Battista Alberti (1465), y muchos lo siguieron siendo desde entonces.

La criptografía se hizo todavía más importante (secretamente) como consecuencia de la competición política y la revolución religiosa. Por ejemplo, en Europa, durante el Renacimiento, ciudadanos de varios estados italianos, incluidos los Estados Pontificios y la Iglesia Católica, fueron responsables de una rápida proliferación de técnicas criptoanalíticas, de las cuales muy pocas reflejaban un entendimiento (o siquiera el conocimiento) del avance de Alberti. Los cifrados avanzados, incluso después de Alberti, no eran tan avanzados como afirmaban sus inventores/desarrolladores/usuarios (y probablemente ellos mismos creían); puede que este sobre optimismo sea algo inherente a la criptografía, ya que entonces y hoy en día es fundamentalmente difícil saber realmente cómo de vulnerable es un sistema. En ausencia del conocimiento, son comunes las conjeturas y esperanzas, como es de esperar.

La criptografía, el criptoanálisis y la traición cometida por agentes y mensajeros en la conspiración de Babington, durante el reinado de la reina Isabel I de Inglaterra, provocaron la ejecución de María, reina de los escoceses. Un mensaje cifrado de la época de el hombre de la máscara de hierro(28) ha arrojado algo de luz (no definitiva, lamentablemente) sobre la identidad real de ese prisionero legendario y desafortunado.

La criptografía y su mala utilización estuvieron implicadas en la conspiración que condujo a la ejecución de Mata Hari y en la confabulación que provocó la ridícula condena y encarcelamiento de Dreyfus, ambos hechos acaecidos a principios del siglo XX. Afortunadamente, los criptógrafos también jugaron su papel para exponer las maquinaciones que provocaron los problemas de Dreyfus; Mata Hari, en cambio, fue fusilada.

Fuera del Medio Oriente y Europa, la criptografía permaneció comparativamente subdesarrollada. En Japón no se utilizó la criptografía hasta 1510, y las técnicas avanzadas no se conocieron hasta la apertura del país hacia occidente en los años 1860.

Aunque la criptografía tiene una historia larga y compleja, hasta el siglo XIX no desarrolló nada más que soluciones ad hoc(29) para el cifrado y el criptoanálisis. Ejemplos de lo último son el trabajo de Charles Babbage, en la época de la Guerra de Crimea,

(28) Descifrado poco antes del año 1900 por Étienne Bazeries
(29) Se usa pues para referirse a algo que es adecuado sólo para un determinado fin. En sentido amplio, *ad hoc* puede traducirse como «específico» o «específicamente».

sobre el criptoanálisis matemático de los cifrados poli alfabéticos, redescubierto y publicado algo después por el prusiano Fiedrich Kasiski. En esa época, el conocimiento de la criptografía consistía normalmente en reglas generales averiguadas con dificultad. Edgar Allan Poe desarrolló métodos sistemáticos para resolver cifrados en los años 1840. Concretamente, colocó un anuncio de sus capacidades en el periódico de Filadelfia Alexander's Weekly (Express) Messenger, invitando al envío de cifrados, que él procedía a resolver. Su éxito creó excitación entre el público durante unos meses. Más tarde escribió un ensayo sobre los métodos criptográficos que resultaron útiles para descifrar los códigos alemanes empleados durante la primera Guerra Mundial.

Proliferaron métodos matemáticos en la época justo anterior a la segunda Guerra Mundial(30).

3.2 La criptografía durante el Renacimiento

La resurrección del cifrado ocurrió durante El Renacimiento. Surgió la denominada expansión de uso del cifrado con la aparición del estado moderno, en el cuál se mantuvo una crisis de los métodos de sustitución por el conocimiento generalizado de las frecuencias de aparición de las letras y sílabas. Para solucionar este problema surgió la aparición de métodos alternativos, los cuales eran nuevos métodos de sustitución, nulos, silabarios (catálogo de sílabas en el que cada una aparece asociada al símbolo: números, voces, u otras sílabas) que la sustituye en un texto cifrado y nomenclátores (catálogo de nombres en el que cada uno aparece asociado a la palabra que le sustituye en un texto cifrado). Su inventor fue Lavinde (Secretario del antipapa Clemente VII en 1379) y se usó ampliamente durante 450 años.

Su evolución trajo pocas docenas de palabras (Lavinde) hasta miles de los zares. Lavinde asistió a la primera compilación europea de cifradores en 1739. Su eficiencia es pequeña y su resistencia ante compromisos es nula, ya que hay un reemplazamiento completo. Además, como sustitución a estos métodos surgió la aparición de nuevos métodos de sustitución poli alfabética y homofónica.

(30) Principalmente con la aplicación, por parte de William F. Friedman, de las técnicas estadísticas al desarrollo del criptoanálisis y del cifrado, y la rotura inicial de Marian Rejewski de la versión del Ejército Alemán del sistema Enigma.

Ejemplo de método de sustitución homofónica: Homófonos:

A = {03, 09, 11, 24, 27, 45, 54, 58, 62, 97}

C = {06, 29, 48, 63}

F = {23}

H = {52}

I = {04, 13, 19, 71}

M = {10, 15, 35, 99}

N = { 22, 42, 56, 67, 76, 84}

O = {05, 25, 35, 49, 81, 89, 94, 96}

S = {08, 12, 21, 53, 60, 74, 83}

T = {01, 61, 77, 92}

U = {17, 26, 98}

_ = {02, 07, 14, 20, 37, 41, 55, 57, 64, 68, 70, 73, 80, 87}

El ejemplo:
21 98 74 61 26 29 13 81 76 55 52 25 15 94 23 35 84 04 48 62

La Criptografía comenzó a progresar cuando los gobiernos de Europa Occidental comenzaron a utilizarla y la codificación comenzó a hacerse más popular principalmente en las comunicaciones entre embajadas.

Desde el siglo XIII, la escritura oculta fue practicada en varias republicas italianas, como Venecia o Florencia, y en la curia pontificia. Aunque aplicaban métodos muy sencillos, descubrieron un modo fácil para evitar el análisis de frecuencias: la permuta de una misma grafía por varios caracteres diferentes, añadiendo signos nulos. Será durante las centurias XIV y XV cuando se produzcan grandes progresos, en especial en Italia, puesto que los alquimistas y los científicos utilizaban esta costumbre para mantener en secreto sus descubrimientos. El preferido, y utilizado con mucha frecuencia, en la correspondencia diplomática moderna de índole confidencial es el "nomenclátor" o "tabla cifradora", compuesta por un alfabeto, casi siempre homofónico, y un conjunto de palabras o frases codificadas, representándose cada una de ellas por uno o más símbolos enigmáticos. Se puede afirmar que, en la centuria decimoquinta, la criptografía europea era una industria floreciente, pues nutrió su expansión durante el Renacimiento el resurgimiento de las artes, de las ciencias y de la erudición.

En la Edad Moderna se van a dar una serie de causas que provocan un auge de la disciplina criptográfica, entre otras el establecimiento con carácter permanente de

embajadas y secretarías de Estado, el incremento de las relaciones internacionales y, en consecuencia, la necesidad de asegurar el secreto de la correspondencia. Por este motivo, para evitar la lectura de la información y hacer más complicada su perlustración, se procede a complicar los métodos cifradores.

En 1518 Johannes Trithemius escribió el primer libro impreso de criptología. Inventó un método por el cual cada letra era representada como una palabra obtenida de una sucesión de columnas. La serie de palabras resultantes sería una oración legítima. Johannes Trithemius escribió, su *Steganographia*, la cual circuló como manuscrito por más de cien años, siendo copiada por muchas personas que deseaban extraer los secretos que se pensaba que contenía.

En 1526 la obra de Jacopo Silvestri discute seis métodos de cifras, inclusive la cifra de César para la cual él recomendaba el uso de un disco de cifragem. Su obra fue escrita para ser un manual práctico de criptología que claramente pretendía alcanzar un vasto círculo de lectores.

En el alfabeto-llave de Silvestri no poseía las letras v, w, y. En el disco, las tres marcas que suceden la Z representan: & para *et*; un símbolo usado comúnmente el latín medieval para significar *us* o uno a finales de palabras (ejemplo: plurib9 = pluribus), o con *con, cum* o cun en el inicio de palabras (ejemplo: 9pronto = concedo); un símbolo usado para *ron*, la terminación del genitivo latino (illo# = illorum). El zig-zag en el centro de la figura debe corresponder la una pequeña manivela para girar los discos móviles.

CIFRADO DE DISCO DE JACOPO SILVESTRI

En 1550, Girolamo Cardano escribió *Subtilitate libri XXI* esta obra famosa contiene información acerca del proceso de cifrado. La parrilla de Cardano consiste en una hoja de material rígido donde se encuentran, en intervalos irregulares, pequeñas aperturas rectangulares de la altura de una línea de escritura y de largura variable. El remitente escribe el texto en las aperturas, después retira la hoja y completa los espacios vacíos con letras cualesquiera. El destinatario pone la misma parrilla sobre el texto cifrado para leer el mensaje.

En 1551 John Dee (1527-1608), alquimista, astrólogo y matemático inglés trabajó con el alfabeto Enoquiano, también llamado lenguaje "Angelical". El alfabeto de este lenguaje arcaico estaba compuesto por 21 letras y fue descubierto por Dee y Edward Kelley. El lenguaje posee gramática y sintaxis propias. John Dee también posee una escritura cifrada que no fue quebrada hasta hoy.

En 1563, Della Porta escribió un texto sobre cifras introduciendo la cifra digráfica. Sugirió el uso de sinónimos y errores ortográficos para confundir a los criptoanalistas. Sus cuatro libros, tratando respectivamente de cifras arcaicas, cifras modernas, criptoanálisis y una lista de peculiaridades lingüísticas que ayudaban en la solución, compilaban el conocimiento sobre la criptografía de la época.

En 1580 François Viete (1540-1603), matemático francés, fue quien introdujo la primera notación algébrica sistematizada y contribuyó para la teoría de las ecuaciones. También fue uno de los mejores especialistas en cifras de todos los tiempos.

A finales del siglo XVI, el imperio español dominaba gran parte del mundo y, justamente por eso, los agentes españoles tenían que comunicarse usando una cifra mucho más intrincada. En la realidad, la cifra era compuesta por más de 500 caracteres, usados por el Rey Felipe II de España durante su guerra en defensa del Catolicismo Romano y de los hugonotes franceses. Algunos mensajes de soldados españoles fueron interceptados por los franceses y acabaron en las manos del rey Enrique IV de Francia. El rey entregó estos mensajes españoles a François Viete, con la esperanza de que él los descifrara. El matemático tuvo éxito y guardó el secreto cuando, después de dos años, los españoles descubrieron lo ocurrido. El rey Felipe de España, creyendo que una cifra tan compleja nunca pudiera ser quebrada, siendo informado de que los franceses conocían sus planes militares, fue a quejarse al Papa alegando que se estaba usando magia negra contra su país. El Papa, sin embargo, nunca creyó en esta historia.

En 1585 Blaise de Vigenère escribió un libro sobre cifras, incluyendo los primeros sistemas auténticos de texto claro y texto cifrado con auto-llave. Conforme Kahn, ambos fueron olvidados y reinventados a finales del siglo XIX. En 1586, Blaise de Vigenère publica su *Traicté des chiffres*, un tratado en el que discute muchas cifras, inclusive el sistema de la "auto-llave corriente", usada en algunas máquinas modernas para cifrar, y el así llamado método “Vigenère tableau”.

En el siglo XVIII surgió la Gran cifra (Luis XIV). Es una cifra mono alfabética mejorada, creada por los Rossignol en la que cada sílaba (y algún carácter ocasional) se representa por un número para dificultar el criptoanálisis un número concreto anula al anterior. En total maneja 587 números y fue un método olvidado tras la caída de la monarquía. Su desciframiento fue descubierto por Bazeries en 1893(31). El más notable fue la carta de Francois Louvois (ministro de la Guerra) a Luis XIV el cual desvela el misterio del "Hombre de la máscara de hierro", el general Bulonde que traicionó al Rey

Y en España, gracias a Felipe II se clasifican dos tipos de cifra que son
General en el que los mensajes eran entre secretarios de estado y de la guerra, virreyes, embajadores, gobernadores generales, etc. Particular en el que lo mensajes eran entre el rey o secretarios de estado o de la guerra con particulares. En la cifra general se lleva a cabo una sustitución homofónica en la que cada vocal son 3 homófonos y cada consonante son 2, o bien un silabario en el que cada sílaba son 2 números o un símbolo, o bien un nomenclátor que son 385 palabras frecuentes.

Los métodos de ocultación más usados son por medio de sustituciones lineales, es decir, de literales, numéricas, por notas musicales, simbólicas, nomenclátores, etc.; por transposición en la que cada sílaba son 2 números o un símbolo; y la esteganografía (anteriormente mencionada) mediante tintas simpáticas o escrituras microscópicas

Además merece especial mención en El Renacimiento el cifrado Pigpen (masónico), el cual es un cifrado de sustitución usado por los masones a partir del siglo XVIII, su origen se remonta a las Cruzadas del siglo XI-XIII

A	B	C
D	D	D
D	D	D

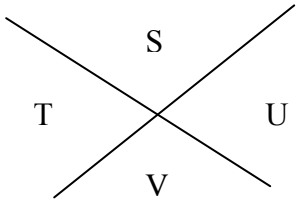
J.	K.	L.
M.	N.	O.
P.	Q.	R.

(31) 150 años después de su invención, tras 3 años de trabajos

Ejemplo del Cifrado Pigpen

Texto en claro: C i f r a d o p i g p e n

Texto cifrado:  etc.…



3.3 El Nomenclátor

Un nomenclátor es un catálogo de sustituciones donde, además de los signos que cambian a las letras, figuran otros que o bien son nulos(32) o reemplazan a bigramas, trigramas, palabras o incluso grupos de palabras.

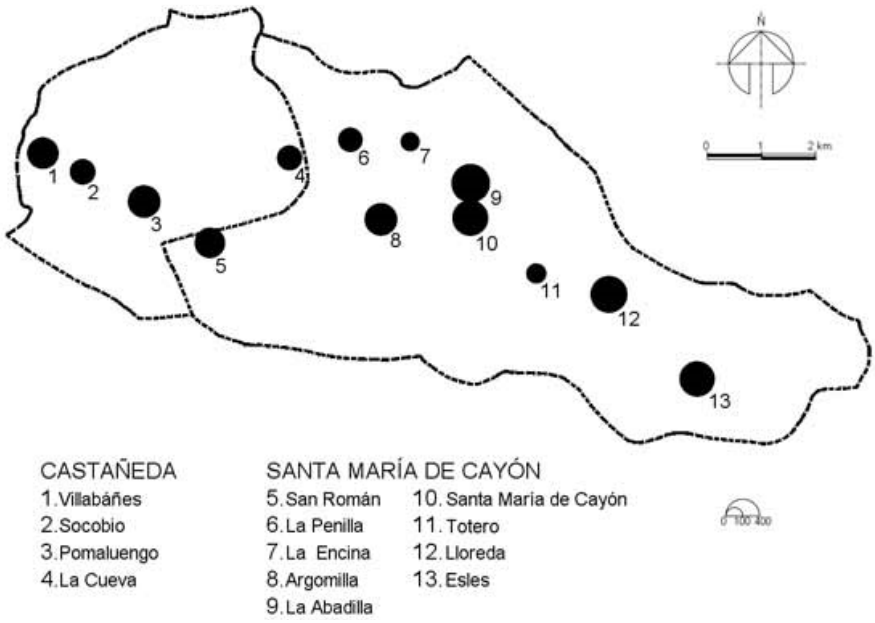
El nomenclátor fue el sistema de cifrado predominante hasta mediados del siglo XIX, hasta que el empleo del telégrafo en las comunicaciones obligó al diseño de otros criptosistemas más adecuados.

Como cualquier sustitución, un nomenclátor está comprometido si alguien es capaz de hacerse con texto en claro y correspondiente cifrado. La seguridad ante un ataque de texto cifrado depende del número de sustituciones que contenga, evidentemente. Un nomenclátor que presente sólo unas pocas sustituciones caerá ante un criptoanalista que disponga de suficiente texto cifrado y paciencia. Pero si contiene un número elevado de signos homófonos para las letras y en la lista de palabras del nomenclátor están todas aquellas de uso común en el contexto del mensaje, incluyendo los nombres propios; y si se dispone de un buen número de signos nulos que se dispersan adecuadamente por los textos cifrados, el criptoanálisis ante texto cifrado únicamente será dificilísimo, prácticamente imposible.

El nomenclátor será entonces un libro con unas cuántas páginas que, naturalmente, habrá que confeccionar y mantener en secreto. Esto también es muy

(32) Que no sustituyen a nada y se colocan en el texto cifrado con el propósito de dificultar el criptoanálisis.

difícil, de nuevo, casi imposible. Por ello, siempre estará comprometido ante la posibilidad de que algunos textos plenos caigan en manos enemigas.



POBLACIÓN DE HECHO, POR NÚCLEOS. CASTAÑEDA Y SANTA MARÍA DE CAYÓN, 1900. ELABORACIÓN PROPIA A PARTIR DE NOMENCLÁTOR DE LA POBLACIÓN, 1900

Los primeros nomenclátores de la Italia del siglo XV siguieron el modelo elaborado por Lavinde, con sustituciones sin homófonos y listas con muy pocas palabras. Paulatinamente fueron incorporando caracteres homófonos, primero para las vocales y después para las consonantes.

Los estados italianos más importantes disponían de departamentos dedicados al criptoanálisis. El más organizado fue el de Venecia, con policía secreta incluida. Venecia contó también con el mejor criptoanalista de la época, Giovanni Soro. Éste fue famoso por resolver varios cifrados a comienzos del siglo XVI. En Milán, el secretario de los duques de Sforza, Cicco Simonetta, fue un gran criptoanalista, suyo es el primer tratado dedicado exclusivamente al criptoanálisis en 1474. Y el Estado Vaticano contó con excelentes criptoanalistas que descifraron algunos de los nomenclátores de esa época, entre ellos los del monarca español Felipe II.

Pronto se comenzó a usar el nomenclátor, puesto que dicho sistema fue el único utilizado a partir del siglo XVI. Los nomenclátores de Carlos I fueron muy simples y

prácticamente rotos por los italianos. Cuando en 1566 Felipe II subió al trono, sabedor de la ineficiencia de las cifras españolas, mandó cambiarlas.

Felipe II usó diversos nomenclátores. Por un lado estaba la llamada cifra general, que era usada regularmente para comunicar con las embajadas en los diferentes países, se cambiaba cada cuatro años. Por otra parte, estaban las distintas cifras particulares que se empleaban con cada uno de los ministros y virreyes de las colonias americanas.

Los nomenclátores usados por Felipe II contienen ya un número importante de sustituciones, con objeto de elevar la seguridad mostrada por otros de épocas anteriores. Sin embargo, los nomenclátores de Felipe II también presentaban descuidos en su diseño que facilitaban su criptoanálisis.

No obstante, a pesar de sus deficiencias, los nomenclátores de Felipe II eran los más seguros de su época. No era fácil su cripotoanálisis con texto cifrado únicamente; aunque hubo quienes lo hicieron. Uno de ellos fue el francés François Viète. Éste resolvió varios nomenclátores usados por Felipe II.

La historia de la criptografía nos lleva en el siglo XVII a la Francia de Luis XIII gobernada por el cardenal Richelieu. Su eminencia tomó a su servicio a un joven experto en criptografía, Antoine Rossignol, con el doble encargo de resolver los criptogramas interceptados a los enemigos de Francia y diseñar las propias cifras francesas. Aunque esto no era lo habitual en la criptografía de estado, en la cual, por regla general, las personas que confeccionaban los nomenclátores no practicaban el criptoanálisis, y ello explica las deficiencias en seguridad que presentaban algunas cifras. Como criptoanalista, Rossignol resolvió numerosos criptogramas entre los que se encuentran algunos interceptados a los hugonotes y que dieron clara ventaja a las fuerzas católicas de Richelieu en las guerras de religión del siglo XVII.

En esta época, los nomenclátores que se empleaban habían aumentado varios cientos el número de sustituciones con el objetivo de incrementar la seguridad. Este elevado número de sustituciones hizo necesario el uso de números en el alfabeto de cifrado convirtiendo, de este modo, los textos cifrados en secuencias numéricas. Pero para no complicar los procesos de cifrado y descifrado, los nomenclátores se

confeccionaban de tal modo que había una correlación entre el orden alfabético de las palabras y el orden natural de los números que las reemplazaban.

Los nomenclátores franceses elaborados por Rossignol no presentaban esta inseguridad de correlación, ya que se elegían de modo aleatorio. Para facilitar el cifrado y descifrado, los nomenclátores comprendían dos partes, es decir, eran como un diccionario bilingüe. En una parte, la que se utilizaba en el cifrado, se ordenaban alfabéticamente las letras, palabras, y a continuación se escribía el número que las cambiaba. En la otra parte, empleada en el descifrado de mensajes, los números se disponían en su orden habitual y al lado figuraba la porción de texto en claro al que sustituían. Este modelo de nomenclátor se impuso en todo el mundo al final del siglo XVIII.

A pesar de su robustez, las cifras francesas de aquella época fueron rotas por el inglés John Wallis, el cual después de su actividad matemática se dedicó a la criptografía, cuyos logros más notables fueron los despachos franceses de Luis XIV.

A comienzos del siglo XVIII tiene lugar en muchos países europeos la creación de departamentos secretos destinados al criptoanálisis de las cartas interceptadas, los cuales fueron llamados las cámaras negras. La primera en crearse fue la Cabinet Noir francesa, pero la mejor fue, sin duda alguna, la Geheime Kabinets-Kanzlei, situada en Viena. Allí las cartas eran abiertas, copiadas y selladas otra vez sin evidencia alguna de este proceso. Las copias de los documentos cifrados se sometían al criptoanálisis, cuyos éxitos estaban garantizados debido a la calidad de los criptoanalistas. Uno de tales triunfos fue la ruptura de las cifras de Napoleón.

La violación de la correspondencia diplomática fue practicada con el mayor descaro. Es comprobado por una anécdota que incluye David Kahn en su libro *The Codebrakers.*

Las cámaras negras austriaca y francesa cerraron sus puertas en 1848, mientras que la inglesa cerró cuatro años después. La causa principal de cierre fue que por aquella

época el telégrafo cambió el modo de enviar mensajes. No hay razón alguna para mantener departamentos secretos encargados de transgredir las cartas privadas cuando su contenido viaja por públicos hilos conductores. Lo que sí es seguro es que el telégrafo acabó con la historia del nomenclátor.

Nadie ha dado nunca un método genérico para criptoanalizar un nomenclátor a partir de texto cifrado exclusivamente. Una idea de cómo se llevó a cabo ese criptoanálisis nos la pueden dar historiadores como Gustave Adolph Bergenroth. Este prusiano del siglo XIX dedicó los últimos años de su vida a resolver nomenclátores utilizados por la Corona española en los siglos XVI y XVII. Bergenroth abrió un camino que le permitió recuperar las 83 sustituciones del nomenclátor.

Uno de los ejemplos más divulgados de criptoanálisis de antiguos textos corresponde a la conocida como la Gran Cifra de Luis XIV. La popularidad de la Gran Cifra se debe a que la persona que lo resolvió concluyó con una conjetura sobre la identidad del hombre de la máscara de hierro. La gran cifra fue rota por un experto criptoanalista del ejército francés, el comandante Etienne Bazeries que fue capaz de descifrar el difícil puzzle de los Rossignol en tres largos años. Y así concluyó la teoría a cerca de la identidad del hombre de la máscara de hierro, la cual no ha sido aceptada por los historiadores.

3.4 Cifrados poli-alfabéticos

A finales del siglo XV y durante la siguiente centuria, mientras el nomenclátor era el único método de cifrar que se seguía en la práctica, aparecieron unas publicaciones en las que se mostraron otras formas de hacer criptografía. Estos nuevos métodos arrancan del cifrado por sustitución, pero lo hacen empleando una sustitución diferente en el cifrado de cada letra. Haciendo esto, una misma letra del alfabeto en claro se transforma en cada ocasión en un signo distinto del alfabeto de cifrado y se inutiliza así el citado análisis de frecuencias dando la impresión de que se manejan múltiples alfabetos.

Por lo general, un criptosistema poli alfabético que gestione claves de forma eficiente proporciona una seguridad mucho mayor que la de un nomenclátor, aunque éste contenga un gran número de signos. Pero a pesar de ello, las diplomacias y ejércitos desconsideraron los nuevos métodos y el nomenclátor continuó gobernando el mundo de

las cifras hasta bien entrado el siglo XIX. Probablemente porque los responsables de manejar cifras en estas organizaciones descubrieron el principal inconveniente de los cifrados poli alfabéticos: un pequeño error cometido durante el proceso de cifrado puede imposibilitar la decodificación, algo que no sucedía con el nomenclátor. Y por ello los sistemas poli alfabéticos no fueron habituales hasta que, entrado el siglo XX, la técnica hizo posible eliminar tales errores mecanizando la codificación y decodificación.

El primer cifrado poli alfabético lo dio a conocer uno de los máximos exponentes del Renacimiento italiano Leone Battista Alberti (1404-1472) siendo el responsable del primer cifrado de disco e inventor de la sustitución poli alfabética. Empezó a interesarse por la criptografía gracias a su amistad con Leonardo Dato, secretario encargado de las cifras del Papa. Fruto de ese interés fue un manuscrito de 25 páginas titulado *Modus scribendi in jiferas*, escrito en 1466. En él figuara un cifrado que resulta poli alfabético porque lo giros del disco menor traen sustituciones, todas diferentes.

El funcionamiento de este y todos los cifrados poli alfabéticos que se verán a continuación es extenso, por ello queda la opción de consultar en los libros y referencias de sitios Web mencionados en la bibliografía para los muy interesados.

CRIPTOSISTEMAS: Sustitución poli alfabética:

Tabla para posiciones pares

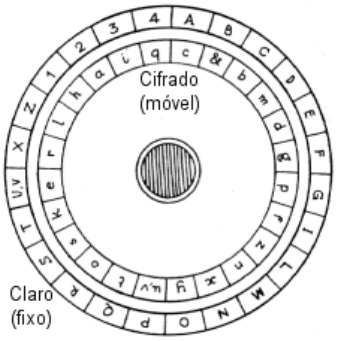
A B C D E F G H I J K L M N Ñ O P Q R S T U VWX Y Z

a e i m p t x b f j n q u y c g k ñ r v z d h l o s w

Tabla para posiciones impares

A B C D E F G H I J K L M N Ñ O P Q R S T U VWX Y Z

n r w b g l p u z e j ñ s x c h m q v a f k o t y d i



Los dos discos de Alberti

SUSTITUCIÓN POLIALFABÉTICA: Ejemplo

S U S T I T U C I O N P O L I A L F A B E T I C A

v k v f f f d w f h y m g ñ f n Q l a r p f j w a

Alberti creía irrompible su cifrado siempre que permaneciera secreto el orden de las letras del disco móvil. Naturalmente esto no es así. La idea de los discos es muy interesante y será aprovechada más adelante por otros criptólogos, pero no lo es el modo en el que Alberti los utiliza. Aún así, el cifrado de Alberti es mucho más seguro que los nomenclátores empleados en su época y tiene el método, como ya se ha mencionado anteriormente, de ser el primer cifrado poli alfabético de la historia de la criptografía.

El siguiente cifrado fue concebido por el monje benedictino alemán Johannes Trithemius. Este prolífico escritor contempló la criptografía como parte de lo esotérico, tema por el que tenía gran interés y al que dedicó los ocho volúmenes que componen su *Steganografía,* escrito en 1499, fue un libro famoso que circuló en forma manuscrita por todo Europa y terminó siendo prohibido por la iglesia Católica en 1609. En él figuran también algunas formas de criptografía, materia a la cual consagró un libro de seis tomos que tituló *Poligrafía,* en 1508.

Es evidente, que el cifrado anterior es tan vulnerable como simple, pero va inspirar a otros diseñadores de cifras durante toda la historia de la criptografía. Un de estas cifras es la que aparece en un folleto titulado *La cifra del Sig.* Giovan Batista Belaso, escrito en 1553, que utiliza la tabla de Trithemius conjuntamente con una clave. El siguiente ejemplo lo demuestra:

CLAVE: BELASOBLASOBELASOBEL
TEXTO CLARO: CIFRADOPOILALFABETICO
TEXTO CIFRADO: dnqrsrptwlbomklbyhkgw

Para simplificar, en este ejemplo la clave ha constado de una única palabra. Belaso propuso emplear claves formadas por varias palabras fáciles de recordar. También recomendó variar la clave frecuentemente y ello hace que Belaso sea el primer autor que diseño un criptosistema en el que las claves cambian periódicamente.

Más o menos al mismo tiempo que Belaso, el físico y matemático Girolamo Cardano (1523-15) empleó el método de la rejilla que fue usado por Richelieu (Luis XIII). Este aurota sugiere emplear la tabla de Trithemius usando como clave el propio

texto en claro y cifrando cada una de sus palabras con el principio del mismo, según muestra el siguiente ejemplo:

CLAVE:	SIC	SICE	SICERGOEL
TEXTO CLARO:	SIC	ERGO	ELEMENTIS
TEXTO CIFRADO:	lre	yais	ytgqxthnd

Cuando se usa el mismo texto en claro como clave, se denomina autoclave. El empleo de autoclaves es una idea muy interesante, utilizada actualmente en algunos criptosistemas que se implementan en el ordenador. Naturalmente, el autoclave de Cardano es demasiado simple, pero es el primero que recoge la historia de la criptografía.

La siguiente obra que se destaca es *De Furtivis Literarum*, escrita en 1563 por el napolitano Giovanni Battista Della Porta (1538-1615). La cual analizó los métodos de cifrado, presentando en su cifrado Porta, la primera sustitución digráfica. Sus cuatro volúmenes recogen toda la criptografía hecha hasta esa época, incluidas las numerosas aportaciones del autor. Porta ideó cifrados de diversa índole que hacían uso de discos giratorios o tablas.

Los 11 alfabetos de Giovanni Battista Della Porta

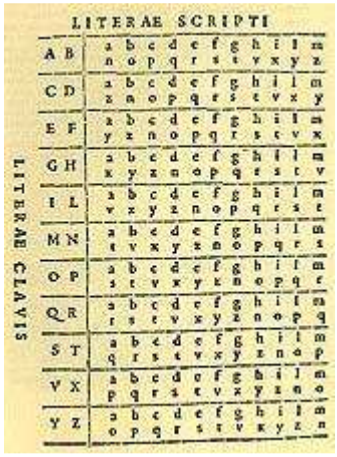
CIFRADO DE PORTA
ab
A B C D E F G H I L M
N O P Q R S T U V Y Z
cd
A B C D E F G H I L M
Z N O P Q R S T U V Y
A B C D E F G H I L M
ef
Y Z N O P Q R S T U V
gh
A B C D E F G H I L M
V Y Z N O P Q R S T U
il
A B C D E F G H I L M
U V Y Z N O P Q R S T
mn
A B C D E F G H I L M
T U V Y Z N O P Q R S

El físico italiano Giambattista Della Porta fue el inventor del primer sistema literal de llave doble, o sea, la primera cifra en la cual el alfabeto cifrante muda cada letra. Este sistema poli alfabético era extremadamente robusto para la época, de modo que muchos consideran Della Porta como el "Padre de la criptografía moderna". Della Porta inventó su sistema en 1563 y esta cifra fue utilizada con éxito por más de tres siglos. Caracteristicas.

La cifra Della Porta empleó 11 alfabetos diferentes y reversibles que él designó por AB, CD, EF, etc. que pueden ser vistos en la figura al lado. El principio es el mismo del desplazamiento circular visto en la Cifra de Bellaso.

op
A B C D E F G H I L M
S T U V Y Z N O P Q R
qr
A B C D E F G H I L M
R S T U V Y Z N O P Q
A B C D E F G H I L M
St
Q R S T U V Y Z N O P
uv
A B C D E F G H I L M
P Q R S T U V Y Z N O
yz
A B C D E F G H I L M
O P Q R S T U V Y Z N

LA CIFRA DELLA PORTA



Ejemplo:

CLAVE: PORTAPORTAPORTAPORT

TEXTO CLARO: DEFVRTIVISLILITERARVM

TEXTO CIFRADO: xyyeebpdnfqpcvesmdp

El autor del siglo XVI que más fama cobró en la historia de criptografía es el francés Blaise de Vigenère (1523-1596), mencionado en capítulos anteriores. Diplomático de la corte francesa en Roma desde los 26 años, decide abandonar esa ocupación a los 47 y dedicarse exclusivamente a sus estudios y escritos. Entre éstos el que interesa aquí es el voluminoso *Traicté des chiffres*, publicado en 1585, y en el que además de la materia indicada en el título, se tratan cuestiones de alquimia, magia y otras artes ocultas. Entre los numerosos cifrados que aparecen en su libro, describe uno poli alfabético que él mismo denominó "le chiffre indéchiffrable" y que la criptografía actual lo conoce como cifrado de Vigenère, del que ya se ha hablado con anterioridad.

En realidad éste no es sino la cifra propuesta por Belaso, empleando una tabla similar a la de Trithemius pero no necesariamente con las letras de los alfabetos dispuestas en el orden habitual, sino siguiendo otras ordenaciones convenidas entre el emisor y el receptor. Curiosamente la tabla de este cifrado equivale a un disco como el ideado por Alberti.

Por tanto, la diferencia entre el cifrado de Alberti y el de Vigenère, lo que hace al segundo mucho más seguro que el primero, es el número de claves que se maneja en caso. En el de Alberti la clave se reduce a una letra elegida entre 24 posibles, las que convienen el emisor y el receptor para casar los discos y en el otro hay una infinidad, puede ser un grupo de palabras de cualquier longitud. De hecho el propio Vigenère recomendaba, al igual que Belaso emplear claves larga, que además, convenía variar frecuentemente. Otra posibilidad que contempló fue el uso de autoclaves.

Con Vigenère concluye la lista de autores renacentistas que recomiendan los cifrados poli alfabéticos como alternativa al nomenclátor en el reinado del país de las cifras. A mediados del siglo XIX, los ejércitos europeos demandaron otras formas de cifrado que dieran protección a sus recién estrenadas comunicaciones telegráficas. Esta fue la oportunidad de los viejos cifrados poli alfabéticos, que al fin alcanzaron la gloria deseada por sus creadores. Es evidente que los cifrados anteriores caen fácilmente ante un ataque con texto claro.

En 1863, un veterano del ejército prusiano, el mayor Friedrich Wilhelm Kasiski, da el primer paso hacia el criptoanálisis de los cifrados poli alfabéticos dentro de un libro titulado *Die Geheimschiften und die Dechiffrirkunst*(33) Este primer paso es encontrar la longitud de la clave empleada. En consecuencia, si en un criptograma hay bloques repetidos, la longitud de la clave debe dividir al máximo común divisor de las distancias entre fragmentos iguales.

No obstante, el problema de encontrar la longitud de la calve se resuelve de un modo definitivo mediante el llamado índice de coincidencia de un texto, concepto introducido por Kasiski en la década de los años veinte. Se define como la probabilidad de que dos de sus letras elegidas al azar coincidan.

$$IC = \frac{f_a\,(f_a - 1) + f_b\,(f_b - 1) + \ldots + f_z\,(f_z - 1)}{n\,(n - 1)},$$

donde $f_a, f_b, \ldots, f_z$ son las frecuencias de las letras y n es la longitud del texto, es decir, el número de letras que tiene.

(33) La escritura secreta y el arte del desciframiento.

Si hubiésemos extraído un texto de gran tamaño, las frecuencias de sus letras estarían muy próximas al patrón de frecuencias de nuestro idioma, entonces el índice de coincidencia del texto sería prácticamente igual a la suma de los cuadrados de los números en español. Cuando ciframos un texto por sustitución, las frecuencias de sus letras se mantienen en el texto cifrado resultante, y, en consecuencia, el índice de coincidencia también. Pero si se emplea un sistema poli alfabético, entonces resulta una distribución de frecuencias parecida a la de un testo aleatoria, ya que las frecuencias más altas del texto en claro se reparten entre varias letras del criptograma.

Al tener una pareja de texto se denomina índice de coincidencia mutua al aplicado para ellos, y es la probabilidad de que al elegir una letra en cada texto, ambas coincidan:

$$ICM = \frac{f_a\, g_a + f_b\, g_b + \ldots + f_z\, g_z}{n\, m} \quad ,$$

donde $f_a, f_b, \ldots, f_z$ son las frecuencias de las letras, n es la longitud del texto, $g_a, g_b, \ldots, g_z$ las frecuencias del otro texto y m su longitud.

Este índice no varía si ambos textos se cifran mediante una misma sustitución, pero si se cifra cada texto con una sustitución diferente, el IC baja. Por tanto el ICM sirve para averiguar si dos textos han sido cifrados con una misma sustitución.

Por último se ha de definir el concepto de simetría de la posición, la cual afirma que la distancia entre dos letras dadas es constante en todas sus filas.

Francis Bacon (1561-1626) dijo: *"una cifra perfecta no debe ser trabajosa de escribir ni de leer, debe ser imposible de descifrar"*.

Criptografía Moderna

Dos hechos significativos marcan un punto de inflexión en el mundo de la criptografía. El primero de ellos, los estudios realizados por Claude Shannon sobre la teoría de la información y criptología (1948), desde ese momento, la criptología deja de ser considerada como un mero arte rodeado de un cierto aire de misterio y en algunos

casos de escepticismo, para ser tratada como una rama más de las matemáticas. El segundo hecho es la publicación de un artículo realizado por Whitfield Diffie y Martin Hellman (1976) en el que proponen un nuevo método de cifrado, creando criptosistemas de clave pública.

A la vista de todo lo expuesto, podría afirmarse, siendo coherentes, que la criptografía clásica abarca desde los tiempos inmemoriales hasta los años de la posguerra, es decir, hasta la mitad del siglo XX. El adjetivo de clásicas, en contraposición al de criptosistemas modernos, se debe tanto a las técnicas utilizadas en las primeras, básicamente operaciones de sustitución y transposición de caracteres, con o sin clave pero siempre unido al concepto de clave secreta, como al uso de máquinas dedicadas a la cifra. En el caso de los sistemas modernos, éstos hacen uso, además de lo anterior, de algunas propiedades matemáticas como, por ejemplo, la dificultad del cálculo del logaritmo discreto o el problema de la factorización de grandes números, unido esto a la representación binaria de la información. No obstante, muchos sistemas modernos y que en la actualidad se siguen utilizando se basan en conceptos que podríamos dominar clásicos como son los de transposición y sustitución con una clave privada, si bien en estos sistemas la operación se realiza sobre una cadena de bits y no sobre caracteres.

La criptografía moderna (la cual también sigue vigente hoy en día, por lo que no sería incorrecto llamarla criptografía en la actualidad) queda dividida en dos grandes bloques según la relación existente entre clave de cifrado y de descifrado: criptografía de clave privada o criptografía de clave pública.

4) Edad Contemporánea

En 1844, el americano Samuel F.B. Morse transmitió el primer mensaje telegráfico entre las ciudades de Baltimore y Boston, mostrando así al mundo la posibilidad de enviar comunicaciones instantáneas desde largas distancias, lo que supuso una revolución en el desarrollo de la criptografía. Los primeros usuarios del nuevo invento fueron particulares dedicados al mundo de los negocios que lo emplearon para sus transacciones comerciales.

Las compañías telegráficas garantizaban la plena confidencialidad, aunque había un motivo de preocupación, el elevado coste de los mensajes, que era proporcional a su longitud. Surgió entonces una necesidad de reducir en lo posible el tamaño de los telegramas, sin que ello supusiera una pérdida de datos, lo que da paso a la aparición en el mercado de los llamados códigos comerciales telegráficos. Éstos eran amplios repertorios de palabras y frases enteras ordenadas alfabéticamente, y su lado las correspondientes series de números o letras que las reemplazaban. Así pues, un código comercial es un enorme nomenclátor que, a diferencia de éste, su fin no es cifrar un texto, sino producir otro más corto y, en consecuencia, más barato al ser telegrafiado. Estos códigos no proporcionaban ninguna seguridad en la comunicación, ya que eran públicos, pero el simple hecho de carecer de sentido el texto resultante proporcionaba una privacidad suficiente para la mayoría de los usuarios del telégrafo.

El primer código comercial fue publicado al año siguiente de la demostración de Morse. Su autor, el abogado Francis O.J. Smith, era precisamente el agente promocional del propio Morse. Al de Smith le siguieron cientos de códigos comerciales por todo el mundo, cuyo uso se prolongó hasta la segunda Guerra Mundial. El telégrafo fue usado también por gobiernos, diplomáticos y militares. Hacia 1860, los libros de códigos habían sustituido ya el viejo nomenclátor, aunque si se deseaba una mayor seguridad, se cifraba el código resultante.

En criptografía se distinguen dos clases de códigos, los ordenados o de una parte, y los desordenados o de dos partes. Los ordenados [34] son aquellos en los que tanto las palabras de texto en claro, como las series de números que las reemplazan van ambas ordenadas, mientras que en los desordenados no se sigue esta correlación. Estos últimos requieren dos partes, en una van ordenadas alfabéticamente las palabras de texto en claro y se usa para codificar, mientras que en la otra parte, el orden lo siguen las series de números o letras y sirve para descodificar.

Todos los códigos comerciales eran de una sola parte, ya que son más fáciles de elaborar, los oficiales, en cambio, los había tanto de una parte como de dos. Los códigos oficiales solían incluir homófonos para las palabras más frecuentes, con objeto de dificultar su criptoanálisis.

El impacto del telégrafo en la criptografía militar fue todavía mayor, puesto que las órdenes a las tropas era imprescindible cifrarlas debido a que resultaba sencillo interceptar las comunicaciones militares que viajaban a través de los hilos telegráficos. Los libros de códigos no eran adecuados para este menester, ya que si caían en manos enemigas, tras la rendición de una unidad, se comprometía la totalidad de las comunicaciones y había que editar y distribuir un nuevo código.

Era necesario emplear diferentes métodos de cifrado, los cuales debían ser fáciles de manejar en campaña y altamente seguros. Además era obligado que esta seguridad dependiese únicamente de una clave que pudiese variar rápidamente y de modo que, aunque el enemigo tuviese constancia del criptosistema empleado, el desconocimiento de la clave impidiese el descifrado de los mensajes. Los métodos de cifrado destinados a ser empleados en el frente fueron llamados cifras de campo. Los cifrados poli alfabéticos eran ideales para utilizar como cifras de campo, especialmente el de Vigenère o alguna de sus variantes, de hecho éstos fueron los que se utilizaron en los primeros días del telégrafo, hasta que, en 1863, el oficial del ejército prusiano Kasiski dio a conocer un método de criptoanálisis para la sustitución poli alfabética que desaconsejó su uso, por lo que se hizo necesario idear otros modos de cifrado.

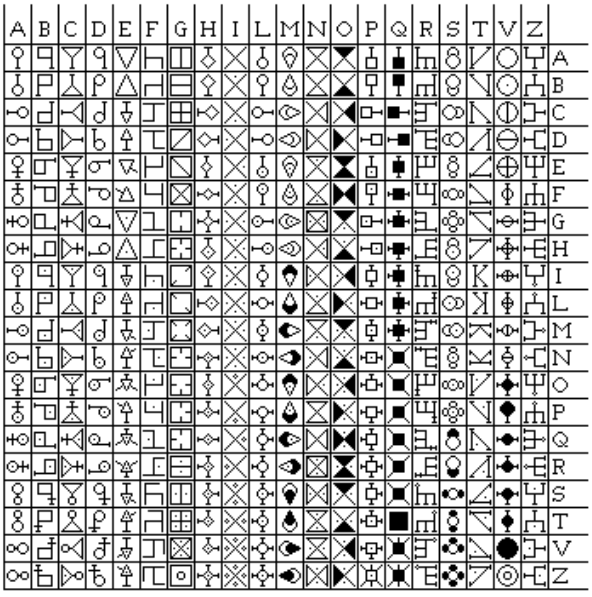
(34) Si el código es ordenado basta con una de las partes para codificar y descodificar, gracias la doble orden

4.1 Cifrados Poligráficos

Los nuevos criptosistemas que fueron empleados como cifras de campo responden en su mayoría a dos modelos que contemplan los actuales libros de criptografía y que se denominan, respectivamente, cifrados poligráficos y cifrados por transposición.

En un criptosistema poligráfico los textos en claro se dividen en bloques con igual número de letras, a continuación, cada uno de estos bloques se reemplaza por otro de signos del alfabeto de cifrado, siguiendo las reglas que indique el criptosistema y haciendo uso de la clave. La concatenación de los bloques que resultan es el texto cifrado. Los bloques de texto en claro no tienen porqué tener la misma longitud que los del texto cifrado, aunque es común que suceda, dicha longitud suele ser un número pequeño; si es dos, el cifrado se dice digráfico, si es tres, trigráfico, etc.

Hay que señalar que el primer criptosistema criptográfico que se conoce data de 1563, el cual fue dado a conocer por Porta en su libro *De Furtivis Literarum,* siendo un cifrado digráfico. El primer criptosistema poligráfico diseñado para servir como cifra de campo data de 1854, su autor Charles Wheatstone, le dio el nombre de cifrado Playfair, el cual fue utilizado por el ejército del gobierno británico como cifra de campo en la primera Guerra Mundial, entre otras. También lo emplearon varias armadas como cifra de emergencia en la segunda Guerra Mundial.



Cifrado digráfico de Porta

La cifra Playfair es un criptosistema digráfico. Se parte de un cuadrado dividido e 25 casillas y en él se disponen las letras del alfabeto ordenadas como disponga la clave. Añadiendo una palabra clave a la matriz de cifrado se consigue una mayor seguridad, la clave se coloca al comienzo de la matriz quitando las repeticiones y a continuación el resto de las letras del alfabeto.

Matriz de Playfair. Por ejemplo, palabra clave VERANO AZUL letra nula X

V	E	R	A	N
O	Z	U	L	B
C	D	F	G	H
I/J	K	M	P	Q
S	T	W	X	Y

Para cifrar, en el texto en claro se suprimen los espacios en blanco y los signos de puntuación, seguidamente se divide el texto en pares de letras, insertando una letra nula entre dos letras iguales cuando éstas estén en el mismo para, o al final del texto si queda una letra suelta.

TEXTO CLARO: COMPRUÉBALO TÚ

CON LA LETRA NULA: CO MP RU EB AL OT UX

TEXTO CIFRADO: IC PQ UF NZ LG ZS LW.

Cada pareja de letras se transforma en otro par de letras de texto cifrado en función de las tres posibilidades siguientes:

- Si las dos letras no están en la misma fila ni columna, se cambia cada letra por la que está en su misma fila, pero en la columna de la otra letra.
- Si las dos letras se encuentran en la misma fila, se sustituye cada una de ellas por la que se encuentra a su derecha. En caso de ser la última de su fila, se reemplaza por la primera de dicha fila.
- Si las letras se localizan en la misma columna, se reemplaza cada una de ellas por la que está debajo. En caso de ser la última de su fila, se reemplaza por la primera de dicha fila.

Era costumbre agrupar el texto cifrado en bloques de cinco letras e insertar un espacio en blanco entre dos bloques: 'ICPQU FNZLG ZSLW'.

El descifrado de la cifra Playfair es similar al cifrado, con la diferencia de que en los casos 2 y 3 anteriores hay que reemplazar las letras por las que se encuentran a la izquierda o arriba, respectivamente. Como puede observarse cifrar y descifrar es relativamente sencillo.

La clave es cada una de las diferentes formas de colocar las 25 letras en el cuadrado, lo que implica que el número total de claves es el factorial de 24, debido a que hay diferentes claves que dan lugar al mismo cifrado, y por ello se reduce del factorial de 25 al de 24.

Otros sistemas digráficos más fáciles de utilizar, y a la vez, más seguros son los que describimos a continuación:

Doble Playfair o cifra de los dos cuadrados en la que se consideran dos cuadrados de 25 casillas y en cada uno de ellos se colocan las letras del alfabeto conforme indique la clave. Este método fue utilizado por los alemanes en la segunda Guerra Mundial, aunque con alguna variante consistente en comenzar dividiendo el mensaje en grupos de un mismo número de letras. Seguidamente el primer grupo se coloca encima del segundo, el tercero sobre el cuarto, y así sucesivamente. En verdad ello provoca que este modo de cifrar sea un doble cifrado. La división del texto en claro en grupos de un mismo número de letras y la posterior disposición de esto grupos según se ha indicado, equivale a efectuar una reordenación de las letras, lo que conlleva una transposición. Una vez sometido el texto en claro a dicha transposición, el resultado se vuelve a cifrar con el método de los dos cuadrados, lo que implica, como es de esperar, el aumento de la fortaleza del criptosistema empleado.

En 1859 Chase, publicó el interesante criptosistema en el que se parte de un rectángulo dividido en 30 casillas dispuestas en tres filas y diez columnas, en ellas se colocan las letras del alfabeto en el orden que determine la clave. Para que no queden casillas vacías, se amplia previamente el alfabeto con algunos signos (uno puede ser el espacio en blanco) hasta conseguir un total de 30 elementos, tantos como casillas. Las tres filas del rectángulo se enumeran como 1,2 y 3; las diez columnas de 0 a 9. Cada letra del alfabeto tiene asociada un par de números, los de la fila y columna a la que pertenece

llamados coordenadas. A continuación el texto en claro se divide en bloques con un número de letras acordado entre el emisor y el receptor.

El proceso de descifrado consiste en seguir el camino inverso. La calve de este criptosistema es el modo de disponer las 30 letras del alfabeto en las casillas del rectángulo, siendo el número de claves distintas el factorial de 30.

El criptosistema Chase nunca fue usado en la práctica, a pesar de que reúne las dos condiciones buscadas que debían presentar las cifras de campo: facilidad en su uso y seguridad. Su fortaleza radica en la idea de representar las letras del alfabeto por los dos números que se han llamado coordenadas.

El siguiente criptosistema es el llamado nombre de cifra bífida, ideado en 1895 por el francés Félix Marie Delastelle. Los trabajos de Delastelle. Y el de otros criptólogos como Bazeries, Kerckhoffs, Valerio,… hicieron de la criptografía francesa la mejor de su tiempo.

Cifrado de Delastelle.

	1	2	3	4	5
1	A	L	B	T	R
2	O	S	C	D	E
3	F	G	H	I	J
4	K	M	N	P	U
5	V	W/Q	X	Y	Z

En virtud del esquema proporcionado por el cuadrado, cada letra viene representada por un para de números entre 1 y 5.

El proceso de cifrado requiere que el texto en claro sin espacios en blanco ni signos de puntuación, se divida en bloques de una longitud acordada entre emisor y receptor.

Cada bloque proporciona dos números que se escriben uno a continuación del otro, y después se dividen en pares de números (las coordenadas de las letras).

El descifrado sigue exactamente el mismo proceso, pero en orden inverso. La calve es la manera en que se colocan las 25 letras en el cuadrado, lo que hace que el número de posibles claves sea el factorial de 25.

Los cifrados poligráficos anteriormente presentados caen sin mucha dificultad ante un ataque con texto pleno, lo que conlleva un cambio frecuente de la clave. Se trata

de criptoanalizar textos conociendo exclusivamente el texto cifrado y, naturalmente, el criptosistema empleado. Esto resulta posible sólo en ocasiones mediante el método de la palabra probable, debido a el empleo de un vocabulario muy concreto, y, en consecuencia, reducido por parte de los cargo militares.

Si no hay conocimiento del criptosistema utilizado, las siguientes observaciones en el texto cifrado elevarían considerablemente la probabilidad de su certeza:

■ En un criptosistema poligráfico la longitud de los bloques que componen los textos cifrados deben ser un divisor del número total de sus letras.
■ Ninguno de los bigramas que componen el texto cifrado contiene dos letras iguales.
■ No puede haber más de 25 letras distintas en el texto cifrado, ya que éste es realmente el número de letras del alfabeto utilizado.
■ En el texto cifrado figuran algunos bigramas junto con sus inversos. En los textos en claro suele haber algunos bigramas que tanto ellos como sus inversos son frecuentes, y como los cifrados digráficos conservan la frecuencia de los bigramas, se explica así, esta cuarta observación.

4.2 Ampliación de cifrados por Transposición

Esta forma de cifrado hace su aparición en la historia de la criptografía muy pronto, en el siglo V A.C., con el escítalo espartano, pero su presencia es totalmente marginal hasta que, a mediados del siglo XIX, la criptografía militar ve en las transposiciones la cifra de campo ideal. La razón de ello está en la sencillez de los procesos de cifrado y descifrado. En contrapartida, la seguridad que ofrecen los cifrados por transposición es inferior a la de los poligráficos, claro que esto no se supo hasta que no fueron sometidos a la acción de los criptoanalistas en la primera Guerra Mundial.

Los métodos de transposición realizan un intercambio de posiciones de los componentes del texto siguiendo un patrón preestablecido, de esta manera el mensaje resultante es ininteligible. Una característica no muy recomendable de estos métodos es el acarreo de errores a lo largo del documento cifrado. Existen varias maneras de realizar este reajuste, la más común es la de hacer la trasposición por columnas, aunque puede escogerse cualquier forma geométrica y forma de recorrido.

Se produce una transposición con sólo escribir el texto en claro, escribiendo de derecha a izquierda. Por ejemplo, uno de los métodos de cifrado empleado por el ejército confederado en la guerra de Secesión Americana fue el conocido como rail fence que consiste en escribir primero en zigzag en dos o más renglones.

```
E     I     N     Z
 S R T E   Z G   A
  C     O     I     G
```

El texto cifrado es: EINZSRTEZGACOIG

Más posibilidades se presentan si la escritura de texto en claro forma una figura geométrica regular como, por ejemplo, un cuadrado. Podemos producir múltiples criptogramas reescribiendo las letras de diversos modos (por columnas, filas, filas al revés, en diagonal,…).

En definitiva, no hay límites a las maneras de diseñar cifrados por transposición, pero aún siendo simple el proceso de cifrado, de los ejemplos anteriores, en él pueden distinguirse dos fases, en la primera escribimos el texto en claro (únicamente las letras) siguiendo un determinado diseño que, por lo general, conduce a formar una figura geométrica, mientras que en la segunda se obtiene el texto cifrado reescribiendo las letras según el modo convenido entre el emisor y el receptor del mensaje. Para descifrar, el receptor deberá deshacer los dos pasos anteriores.

Al haber infinidad de criptosistemas por transposición, se van a presentar seguidamente algunos de los más característicos. En todos ellos se emplea nuestro alfabeto español de 27 letras, por lo que ignoramos los espacios en blanco y los signos de puntuación que contengan los textos en claro.

El más sencillo y más recurrido ha sido el denominado transposición de columnas, por está razón se solía usar en combinación con otro cifrado de distinta categoría como una sustitución. En el método de transposición por columnas se escribe el mensaje en columnas debajo de la palabra clave y a continuación se escogen las columnas por orden posicional o alfabético. En el caso de que queden celdas sin ocupar, se rellenan con caracteres nulos que no puedan entorpecer la lectura correcta del mensaje original Si bien es un método sencillo, fue utilizado hasta la II guerra mundial. En la transposición de columnas se parte de una clave que consta de un entero n y una

reordenación de los números 1, 2, 3…,n. En la práctica, estos datos se obtienen considerando una palabra o grupo de palabras, el entero n es el número de letras que tiene y la reordenación referida la proporciona el orden alfabético de sus n letras. Por ejemplo, consideramos la palabra de 5 letras 'KAIRO' y colocamos debajo de sus letras el número que corresponde al orden alfabético:

K	A	I	R	O
3	1	2	5	4

Se obtiene la clave formada por el entero n=5 y esta reordenación de los 5 primeros números: 3, 1, 2, 5, 4. Fijada la clave, el texto en claro se dispone formando un rectángulo con exactamente n columnas y el texto cifrado se obtiene al escribir secuencialmente las columnas en el orden proporcionado por la clave:

TEXTO CLARO: REUNIÓN EN EL CUARTEL

CLAVE: KAIRO

TEXTO CIFRADO: ENCEUEULROLTIERNNA

K	A	I	R	O
3	1	2	5	4
R	E	U	N	I
O	N	E	N	E
L	C	U	A	R
T	E	L		

También puede seguirse el estándar de agrupar las letras en bloques de cinco, tal como se hacía en la práctica para evitar errores telegráficos:
ENCEU EULRO LTIER NNA

Para descifrar el mensaje, el receptor del mismo, ha de contar primero con el número de letras de que consta, 18 en este caso. Seguidamente hay que dividir 18 entre n (el número de columnas, 5 en nuestro caso) y así se obtiene 3 como cociente y 3 también como resto, lo que indica que las tres (resto) primeras columnas del rectángulo cuentan con cuatro letras y las dos restantes con tres. Teniendo esto en cuenta, el receptor ha de rellenar las columnas con el texto cifrado siguiendo el orden determinado por la clave recuperando así, el mensaje en claro.

En este ejemplo, para facilitar la labor, la clave tenía pocas letras, lo que puede facilitar el trabajo del criptoanalista, mientras que otra con muchas puede ser difícil de memorizar. Así pues, un buena elección práctica oscilaría entre 7 y 25 letras. Todas las transposiciones que se llevaron a la práctica fueron criptoanalizadas a partir de texto cifrado únicamente. Dentro de esta categoría de cifrado, la transposición de columnas presenta una seguridad intermedia.

Lo difícil de su criptoanálisis es descubrir el número de columnas e identificarlas, obtener después su orden correcto es más sencillo. Para no facilitar esta tarea, la última fila del rectángulo debe quedar siempre incompleta, si da la casualidad de que la fila se llena, han de añadirse algunas letras nulas al final del texto en claro para que este continúe en una nueva pero incompleta fila.

La seguridad aumenta notablemente si se efectúa una doble transposición de columnas, en la cual, habitualmente la segunda transposición está regida por la misma clave que la primera, aunque puede utilizarse otra distinta. Este método es uno de los cifrados por transposición más seguros que hayan sido puestos en uso. Fue la cifra de campo preferida por muchos ejércitos hasta la primera Guerra Mundial, entre ellos el alemán y el americano; también estuvo presente en la segunda Guerra Mundial.

El siguiente criptosistema es el de transposición de los nihilistas rusos, por ser usado por este grupo anarquista que surgió en la Rusia zarista e n la segunda mitad del siglo XIX. Las claves son las mismas que en la transposición de columnas, pero el proceso de cifrado es más complicado. El primer paso consiste en dividir el texto en claro en fragmentos de n^2 letras y formar cada unos de ellos encuadrado nxn. A continuación, se reescriben los cuadrados reordenando sus columnas de acuerdo con el orden determinado por la clave. Seguidamente se repite la misma operación en las filas de cada cuadrado y así se obtiene el cifrado final.

El receptor del mensaje deberá seguir el proceso inverso para recuperarlo, es decir, partir el texto cifrado en trozos de n^2 letras, escribir cada uno en un cuadrado nxn y deshacer los reordenamientos de filas y columnas en los cuadrados. Tendrá que prestar atención con el último cuadrado, para que las casillas que resulten vacías sean las correctas.

Un curiosos criptosistema que fue publicado en 1885 por Julio Verne en su novela *Matías Sandorff* recibe el nombre de rejilla giratoria porque la clave es un cuadrado dividido en cuadrículas sin repetir ninguna. Su origen se remonta al menos al siglo XVIII. En la confección de la rejilla giratoria, la selección de las cuadrículas agujereadas se hace siguiendo la estrategia de dibujar un cuadrado 6x6 y numerando sus cuadrículas dividiendo el cuadrado en otros cuatro cuadrados de nueve casillas cada uno. Al rotar 90 grados, cada uno de estos cuatro cuadrados se traslada a otro adyacente de forma que cada una de sus cuadrículas va a parar a aquella con igual número. En consecuencia, si se quiere que cada cuatro giros sucesivos de 90 grados se descubran todas las celdillas una única vez, se ha de perforar nueve de ellas sin hacerlo en dos con el mismo número. Esta argumentación permite también contar cuantas rejillas 6x6 diferentes pueden construirse. Puesto que se ha de elegir una de las cuatro casillas con el número 1, otra de las cuatro con el número 2 y así sucesivamente, hay 4^9 maneras diferentes de hacerlo, ahora bien, como una misma rejilla puede estar en cuatro posiciones distintas y cada una de ellas corresponde a una selección diferente de los nueve agujeros, el número anterior ha de dividirse por 4 quedando así 4^8 rejillas 6x6 diferentes.

En general, el número de rejillas distintas de dimensión nxn con n par, n= 2k, es 4 elevado a k^2-1, pero también pueden considerarse rejillas nxn con n impar, en cuyo caso n= 2k+1 y el número de rejillas diferentes será 4 elevado a $k^2 + k - 1$.

Para descifrar un mensaje cifrado con una rejilla giratoria, el legítimo receptor ha de seguir otro proceso [(35)].

Se ha de señalar que los procesos de cifrado y descifrado pueden ser intercambiados, consiguiéndose así otra manera de usar la rejilla giratoria. Además se ha de notar que, al igual que ocurría en transposición de los nihilistas, el cifrado en la rejilla se inicia dividiendo el texto en claro en fracciones de igual longitud que luego son reordenadas de la misma manera. En general, los criptosistemas por transposición, cuyo método de cifrado cumple tal característica se denominan regulares.

(35) este proceso es algo largo, por lo que para los muy interesados se puede consultar en los libros y sitios Web expuestos en la bibliografía

Por otro lado, es fácil determinar si un criptosistema ha sido cifrado por transposición, como no es más que una reordenación de un cierto texto en claro, las frecuencias de sus letras se mantienen en el criptograma, y por ello deben seguir en patrón de frecuencias de las letras del idioma en el que está escrito el texto lo que implica, que un simple análisis de frecuencias permite averiguar si el texto ha sido cifrado por transposición. Lo que es tan sencillo es concretar, a partir de los criptogramas exclusivamente, que cifrado por transposición ha sido empleado.

No obstante, si se dispone de varios criptogramas con exactamente la misma longitud, no es necesario averiguar antes que tipo de transposición lo ha generado para que el criptoanálisis pueda comenzar. En este caso, el simple y efectivo método de los múltiples anagramas descubre los textos en claro.

En 1878 tres aficionados al criptoanálisis(36) descifraron varios telegramas confirmando que el partido Demócrata Americano compró votos en las conflictivas selecciones presidenciales celebradas dos años antes. En esta ocasión, el método de cifrado empleado con los comprometedores telegramas fue una transposición de palabras en lugar de letras, además de reemplazar previamente los nombres propios y las palabras más significativas por otros términos.

El método de los múltiples anagramas también es aplicable a las transposiciones regulares, aunque no se disponga de varios criptogramas con el mismo número de letras. Para poder hacerlo, el criptoanalista debe conocer el periodo, entendiendo por éste la longitud de los fragmentos en los que inicialmente se han partido los textos en claro. El problema está en que no hay método alguno para calcular el mencionado periodo a partir de los criptogramas únicamente.

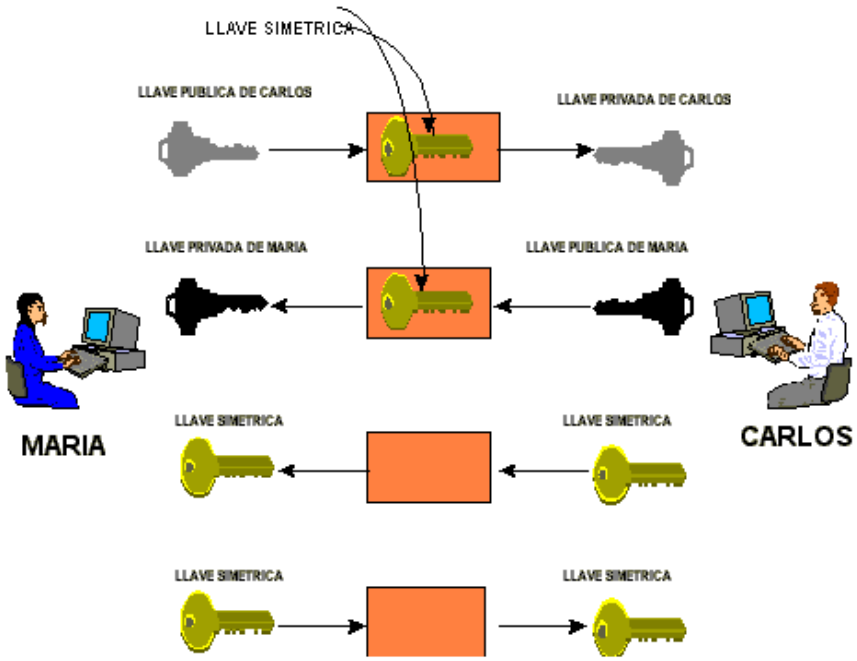
En general, cualquier transposición regular cuyo periodo varíe entre unos pocos valores es atacable mediante anagramas, independientemente de lo complicado que sea su proceso de cifrado, lo que implica que las transposiciones regulares son menos seguras que las irregulares.

(36) Los editores del *New York Tibune* John Hassard y William Grosvernor por un lado, y el matemático Edward Holden por otro lado.

4.3 Criptografía de clave secreta

También llamada de clave simétrica, es aquella que emplea la misma clave k tanto para cifrar como para descifrar. Presenta el inconveniente de que para ser empleada en comunicaciones, la clave k debe poseerla tanto el emisor como el receptor, para lo cual es necesario que se pueda transmitir la calve de forma segura.

Se dice que un sistema de cifrado de clave secreta es seguro si ningún ataque conocido de menor complejidad que la búsqueda exhaustiva sobre el espacio de claves ofrece mejores resultados que ésta.



La seguridad depende del emisor y el receptor. Existen dos operaciones para cifrar transposición y sustitución distinguiendo dos tipos de cifrado de clave secreta o simétrica cifrado en bloque y cifrado en flujo.

Cifrados en bloque. Los criptosistemas basados en cifrados en bloque dividen el mensaje a cifrar en diversos fragmentos, por lo general de longitud fija, y aplican a cada uno de ellos una transformación criptográfica. La mayoría de estos algoritmos se basan en los conceptos de confusión y difusión inicialmente propuestos por Shanon, los cuales se utilizan para anular la redundancia de la fuente.

Un buen mecanismo de confusión hará demasiado complicado extraer relaciones estadísticas entre el texto en claro, el texto cifrado y la clave. Por su parte la difusión trata de repartir al máximo la influencia de cada bit del mensaje original entre el mensaje cifrado.

Lo que en realidad se hace para conseguir algoritmos fuertes, sin necesidad de almacenar tablas enormes, es intercalar la confusión, que implica sustituciones simples con tablas pequeñas con la difusión, que implica permutaciones. Esta combinación se conoce como cifrado de producto. La mayoría de los algoritmos se basan en diferentes capas de sustituciones y permutaciones, denominadas Red de Sustitución-Permutación.

Algunos ejemplos de cifrado en bloque son:

DES: algoritmo de cifrado que emplea una clave de 56 bits de longitud para cifrar los 64 bits del texto en claro y así obtener un criptosistema de igual longitud. Esté basado en dos operaciones lógicas XOR y operaciones de sustitución y permutación que se repiten en 16 rondas o iteraciones(37).

IDEA: opera con bloque de información de 64 bits y claves de 128 bits. El cifrado consiste en ocho vueltas elementales y una transformación de salida. La seguridad está basada en operaciones lógicas XOR, sumas (módulo 2^{16}) y multiplicadores (módulo $2^{16}+1$).

RC5: sistema de cifrado diseñado por R Rivest para RSA Data Security Inc. El método no es público ni está patentado, sino que es un secreto industrial. Este cifra bloques de longitud variable y tiene un número variable de vueltas. Las operaciones básicas en él realizadas son la operación lógica XOR, la suma modular, así como rotaciones y desplazamientos de bits. El análisis exhaustivo para el caso particular de 15 vueltas con bloques de cifrado y claves de 64 bits, indica que la ruptura del mismo requiere un total de 2^{68} 2exp68 textos en claro, lo cual garantiza su seguridad ya que no puede haber más de 2^{64} de dichos textos.

(37) Lo veremos con más detalle en el capítulo 4.3.2

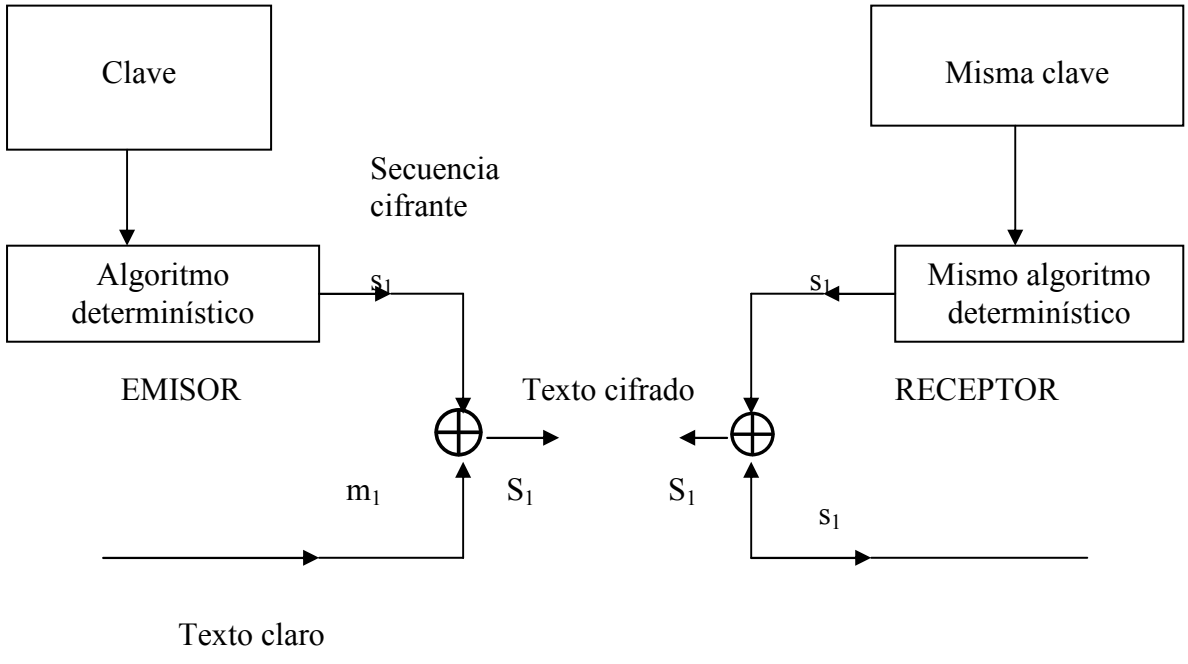
Rijndael: a partir de octubre del año 2000 ha sido adoptado como Estándar Avanzado de cifrado (AES). Es un sistema de cifrado de bloques diseñado para manejar longitudes de clave y de bloque variables, ambas comprendidas entre los 128 y 156 bits(38).

Cifrados en flujo. Los sistemas del cifrado en flujo dividen el sistema a cifrar en caracteres (cuya longitud es mejor que los bloques), para posteriormente cifrar cada carácter aplicando una función que varía con el tiempo cuya dependencia temporal está regida por las variables que definen el estado del sistema. Así pues, después del cifrado de cada carácter, el sistema evoluciona a un nuevo estado de acuerdo con una determinada regla. Como consecuencia de ello sucede que caracteres idénticos poseen por lo general cifrados diferentes, lo que contribuye a aumentar la seguridad del sistema.

4.3.1 Arquitectura del cifrado en bloque y del cifrado en flujo

Los actuales cifradores de flujo no son más que un cifrado de Vigenère en el que la longitud de la clave tiende a infinito.

En la práctica se utiliza el método de cifrado en flujo, cuyo esquema fundamental se encuentra representado en la siguiente figura:



(38) Lo veremos con más detalle en el capítulo 4.3.3

El emisor A, con una clave corta (secreta) y un algoritmo determinístico (público), genera una secuencia binaria (s_1) cuyos elementos se suman módulo 2 con los correspondientes bits de texto claro m_1, dando lugar a los bits de texto cifrado c_1. Esta secuencia c_1 es la que envía a través de un canal público.

En recepción, B, con la misma clave y el mismo algoritmo determinístico, genera la misma secuencia cifrante (s_1), que suma modulo 2 con la secuencia cifrada (c_1), dando lugar a los bits de texto claro m_1. Fácilmente se ve, que el cifrado en lujo es asimismo una involución, pues el procedimiento de cifrado es idéntico al de descifrado.

Por otro lado, como la secuencia cifrante se ha obtenido a partir de un algoritmo determinístico, el cifrado en flujo ya no se considera secuencias perfectamente aleatorias, sino solamente pseudoaleatorias. No obstante, todo lo perdido en cuanto a seguridad, por no cumplirse en rigor las condiciones de Shannon, se gana en viabilidad práctica a la hora de utilizar este procedimiento de cifrado. Por lo tanto, la única información que han de compartir emisor y receptor es la clave secreta, cuya longitud oscila entre 120-250 bits.

Actualmente, los bits de clave se suelen hacer llegar a ambos destinatarios mediante un procedimiento de clave pública, de tal forma que cuando ambos disponen ya de la clave, se procede a aplicar el esquema tradicional del cifrado de flujo.

En cuanto a los generadores pseudo aleatorios de secuencia cifrante, es importante señalar que resulta muy difícil evaluar cuando una secuencia binaria es suficientemente segura para ser utilizada en Criptografía, puesto que no existe un criterio general y unificado que lo certifique. Sin embargo, se señalan una serie de requerimientos generales que toda secuencia cifrante ha ce cumplir para su correcta aplicación al procedimiento de cifrado de flujo.

Período de la secuencia cifrante ha de ser al menos tan largo como la longitud del texto a cifrar. En la práctica, se generan secuencias con periodos del orden de 10^{38} o superiores.

Distribución de ceros y unos para una secuencia aleatoria, debe cumplir que diferentes muestras de una determinada longitud han de estar uniformemente distribuidas a lo largo de toda ella.

En toda secuencia binaria, se denomina racha de longitud K a una sucesión de K dígitos iguales entre dos dígitos distintos.

La función auto correlación AC(K) de una secuencia periódica de periodo T se define como:

$$AC(K) = (A - D) / T$$

donde A y D representa respectivamente el número de coincidencias y no coincidencias entre la secuencia considerad y ella misma desplazada cíclicamente K posiciones.

Si K es múltiplo de T, la auto correlación está en fase y AC(K) =1, pero si esto no se cumple, entonces la auto correlación está fuera de fase y AC(K) toma valores comprendidos en el intervalo (-1, 1).

Golomb formula tres postulados que una secuencia binaria finita debe satisfacer para poder ser denominada secuencia pseudo aleatoria

■ En cada periodo de la secuencia considerada, la diferencia entre unos y ceros no debe exceder la unidad.

■ En cada periodo de la secuencia considerada, la mitad de las rachas tiene una longitud igual a 1, la cuarta parte tiene longitud igual a 2, la octava parte tiene una longitud igual a 3 y asi sucesivamente. Igualmente, para cada una de las longitudes anteriores habrá el mismo número de rachas de ceros que de unos.

■ La auto correlación AC(K) fuera de fase es constante para todo valor de K.

Una secuencia finita que verifique estos tres postulados se denomina secuencia PN (Pseudo-Noise) y goza de todas las propiedades de una secuencia binaria con distribución uniforme.

Aparte de estos postulados, las distribuciones χ^2 y los métodos espectrales constituyen una buena guía para el estudio de las propiedades de pseudoaleatoriedad de una secuencia dada.

La medida de la imprevisibilidad de una secuencia es su complejidad lineal y el algoritmo para calcularla es el algoritmo de Massey-Berlekamp.

Es importante que se cumpla el principio de facilidad de implementación, es decir, la secuencia tiene que ser fácil de generar con medios electrónicos para su aplicabilidad en el proceso real de cifrado/descifrado.

Algunos de los métodos más simples y conocidos para la generación de secuencias pseudoaleatorias son:

Generadores basados en congruencias lineales. Basado en relaciones de recurrencia.

Boyar demostró que las secuencias obtenidas a partir de congruencias lineales no eran criptográficamente seguras.

Una variante de este procedimiento consiste en generar la secuencia cifrante a partir de algunos bits de la representación binaria. Aunque criptográficamente hablando, tampoco constituye un procedimiento seguro.

Registros de desplazamiento realimentados. Constituido por etapas y una función de realimentación que permite expresar cada nuevo elemento de la secuencia en función de los n elementos anteriores,

El período de la secuencia producida dependerá del número de etapas del registro y de las características de la función. Lógicamente, el máximo período que puede alcanzar una secuencia será 2^n para el caso de un registro de n etapas.

La clave para este tipo de generadores está constituida por el contenido inicial del registro y/o el conocimiento de la función de realimentación. Dependiendo de si la función es o no lineal, así será, respectivamente, el registro de desplazamiento realimentado.

Registros de desplazamiento realimentados no linealmente (NLFSR). Presentan el problema de no existir un método sistemático para su análisis y manipulación. Efectivamente, las secuencias generadas por estos registros pueden tener ciclos pequeños que se repiten indefinidamente a lo largo de todas ellas, lo que criptográficamente hablando es peligroso. Por otro lado, estos generadores son difíciles de implementar para una generación rápida de secuencias cifrantes.

Registros de desplazamiento realimentados linealmente (LFSR). Son uno de los dispositivos más importantes para la generación de secuencias pseudoaleatorias. Su modelación e implementación electrónica son sencillas. Y naturalmente, el estado inicial tiene que ser distinto del estado todo ceros, para evitar la secuencia idénticamente nula. Por lo tanto, el mayor número de estados diferentes será $2^n - 1$.

Todo registro de desplazamiento realimentado linealmente tiene asociado un polinomio de realimentación de grado n.

Se distinguen varios tipos:

■ Generadores con polinomio de realimentación factorizable. La longitud de la secuencia depende del estado inicial y el máximo período T verifica $n \leq T < 2^n - 1$, pudiendo aparecer períodos secundarios que son divisores de T.

■ Generadores con polinomio de realimentación irreducible. La longitud de la secuencia no depende del estado inicial y el período T es un divisor de $2^n - 1$.

■ Generadores con polinomio de realimentación primitivo. La longitud de la secuencia no depende del estado inicial y el período T es $2^n - 1$.

Estos generadores son los que ofrecen una secuencia de período máximo $2^n - 1$, luego son los más recomendables para su aplicación criptográfica.

Existen algoritmos para la determinación de polinomios primitivos con coeficientes binarios. La secuencia generada por un registro de desplazamiento de polinomio primitivo se denomina secuencia de "máxima longitud" o abreviadamente, "m-secuencia".

Las m-secuencias cumplen las condiciones exigibles a una secuencia cifrante en cuanto a período, distribución estadística y facilidad de implementación. Sin embargo, constituyen un fracaso absoluto en lo concerniente a la complejidad lineal, ya que conociendo 2n dígitos consecutivos de una secuencia de este tipo, resulta muy fácil predecirla. Y por lo tanto se conocería el estado del registro en un determinado instante y su esquema de realimentación.

Cualquier secuencia periódica puede ser generada por un LFSR no singular. La longitud del mínimo (más corto) registro de desplazamiento realimentado linealmente que es capaz de generarla, recibe el nombre de complejidad lineal. En la práctica, el algoritmo de Massey-Berlekamp determina la longitud, esquema de realimentación y contenido inicial del LFSR que genera la secuencia considerada.

La principal característica del filtrado no lineal es la dificultad que presenta a la hora de analizar, y especialmente de acotar, el valor de la complejidad lineal de la secuencia resultante. La mejor estrategia para abordar este problema se centra en la búsqueda de clases de funciones cuyas secuencias de salida tengan garantizada una complejidad lineal elevada. Como ejemplo ilustrativo puede señalarse el trabajo de Rueppel[39], en el que se concluye que, para valores de n en el rango n=250, la probabilidad de elegir un filtrado no lineal con complejidad lineal máxima está próxima a la unidad.

(39) R. A. Kueppel, Analysis and Design of Stream Ciphers, Springer – Verlag, New York, 1986

Los principios de diseño par secuencias generadas a partir de un filtrado no lineal, son:

■ Utilizar un registro de desplazamiento realimentado linealmente de polinomio primitivo para obtener un gran período y buenas características estadísticas.

■ Incluir varios términos de cada orden hasta el orden máximo para conseguir una buena confusión.

■ Escoger un orden K de la función que permita obtener una complejidad lineal cercana al valor máximo, es decir, K = n/2.

■ Incluir un término lineal para conseguir unas buenas propiedades estadísticas.

■ Hacer que la clave determine algunos términos de la función no lineal.

No obstante, aún siguiendo estos criterios en la elección del filtrado, la dificultad principal en el manejo de estas transformaciones sigue siendo su dificultad de análisis.

De entre todas las técnicas de generación de secuencias cifrantes a partir de varios registros de desplazamiento realimentados linealmente, pueden destacarse tres grandes grupos:

■ Generadores de secuencia basados en una combinación no lineal de varios registros de desplazamiento.

■ Generadores de secuencia multivelocidad

■ Generadores de secuencia con desplazamiento irregular de alguno de sus registros.

En los generadores de secuencia basados en una combinación no lineal de varios registros de desplazamiento, las salidas de los LFSRs integrantes constituyen las entradas a la función no lineal. El ejemplo más representativo de este grupo es el generador de

Geffe, el cual consiste en una combinación de tres registros de desplazamiento, donde el primero de ellos LFSR1 actúa como selector y las otras dos secuencias de LFSR2 y LFSR3, a_2 (t) y a_3 (t), respectivamente, se combinan de forma aleatoria mediante un conmutador que selecciona una u otra secuencia en función de los bits de a_1 (t), secuencia generada por LFSR1. La debilidad de este generar estriba en la alta probabilidad de coincidencia que existe entre la secuencia de salida y las secuencias a_2 (t) y a_3 (t).

Todos los generadores descritos anteriormente tienen como característica común que todos sus registros se desplazan simultáneamente a cada impulso de reloj. Además, algunos de sus registros integrantes pueden desplazarse a distintas velocidades, lo cual abre nuevas posibilidades en la generación de secuencias cifrantes. El ejemplo más significativo de este tipo de generadores es el generador multivelocidad de Massey – Rueppel, el cual consta de dos registros de desplazamiento que funcionan a distinta velocidad. El registro de n etapas trabaja a una velocidad $d \geq 2$ veces más rápida que el registro de m etapas, siendo $n \geq m$. El factor de velocidad d es variable y se usa como parte de la clave. Si ambos registros tiene polinomio de realimentación primitivo y además se cumple que el máximo común divisor de n y m es igual a la unidad e igualmente el máximo común divisor de d y $(2^n - 1)$ también es igual a la unidad, entonces la secuencia de salida tiene complejidad lineal. El carácter bilineal de la expresión matemática, que lo representa, permite un ataque por consistencia lineal, ya que conociendo los polinomios de realimentación, el criptoanalista puede determinar el factor de velocidad d y el contenido inicial de ambos registros.

La principal característica de los generadores de secuencia con desplazamiento irregular es que la secuencia de salida de un registro controla el funcionamiento del reloj de los registros subsiguientes. En este caso, el ejemplo representativo lo constituye el generador de Beth – Piper en el que la entrada al reloj del LFSR2 está controlada por la secuencia de salida del LFSR1, de tal manera que el LFSR2 cambia su estado en cada instante t solo si a_1 (t) =1.Aunque la complejidad de este generador pueda llegar a ser muy grande (proporcional a 2^n) su seguridad es mínima.

Una versión fortalecida del generador Beth – Piper la constituye el generador en cascada de Gollmann, el cual consta de una serie de m LFSRs con polinomios de

realimentación primitivos de grado n, El registro LFSRi está controlado por todos los LFSRj con j < i, según el esquema de Beth – Piper.

El generador Shrinking es de secuencia binaria muy sencilla y cuenta con buenas propiedades criptográficas. Consta de dos LFSRs, un registro de control LFSR1 que diezma irregularmente la secuencia producida por el otro registro LFSR2. En la literatura especifica se han descrito varios ataques contra este generador, sobresaliendo el ataque por consistencia lineal, que requiere una búsqueda exhaustiva sobre todos los estados del registro LFSR1. Recientemente se ha detectado un nuevo ataque que está basado en el concepto de probabilidad posterior de los bits individuales del registro LFSR1, que permite reconstruir los estados iniciales de ambos registros sin tener que recorrer los de LFSR1 y con una complejidad computacional significativamente menor que la de los ataques previamente conocidos.

Finalmente, se puede concluir que un buen generador de secuencia cifrante debe satisfacer simultáneamente un cúmulo de requisitos independientes entre si. Todos los Generadores considerados en este estudio verifican las condiciones de período largo y buena distribución estadística, pero no todos ellos cumplen de igual modo el requerimiento de complejidad lineal.

Respecto a los ataques criptoanalíticos, resulta interesante señalar que, aunque teóricamente son posibles en la práctica su viabilidad depende del orden de magnitud de los parámetros utilizados en el generador bajo estudio. Por lo que no siempre se podrá romper un criptosistema con los procedimientos encontrados en la literatura.

El diseño de generadores de secuencia cifrante se plantea como un desafío continuo diseñador – criptoanalista, en el que ciertos generadores van sucumbiendo, pero son rápidamente sustituidos por otros nuevos que pretenden ser invulnerables.

Por consiguiente, y tras la visión general realizada sobre el cifrado de flujo, queda patente que se trata de un método rápido y eficaz en un mundo en el que cada vez hay más necesidad de proteger la información. De todas formas no existe un criterio unificado que dictamine si la secuencia cifrante utilizada está suficientemente próxima a una secuencia aleatoria que sería la única en garantizar la perfecta seguridad del método.

Tampoco existe un procedimiento sistemático para criptoanalizar estos generadores, cada uno requiere un tratamiento especial en función de sus características, y aunque la labor del criptoanalista radica, precisamente, en encontrar dependencias estadísticas o relaciones algebraicas entre las diferentes subsecuencias. Nunca puede asegurarse que un generador de secuencia cifrante sea intrínsecamente bueno, a veces, la fortaleza de un generador se fundamenta simplemente en que no se ha sabido aplicar el criptoanálisis adecuado o bien en que nadie se ha parado a criptoanalizarlo.

Es importante resaltar que, aunque la criptografía de clave pública esté en auge, los procedimientos matemáticos que engloba son tan lentos y laboriosos que los viejos cifrados bit a bit permanecen vigentes, a pesar de sus detractores. Y la rapidez de ejecución del cifrado en flujo es y será siempre la mejor garantía de su vigencia.

Cifrado en bloque es aquel en el que se cifra el mensaje original agrupando los símbolos en grupos (bloques) de dos o más elementos. Algunos sistemas de cifrado, como el poligráfico y el de transposición, son ejemplos de cifrado en bloque.

En un cifrado moderno en bloque se cumple:

■ Cada símbolo se cifra de manera dependiente de los adyacentes.

■ Cada bloque de símbolos se cifra siempre de igual manera, independientemente del lugar que ocupe en el mensaje.

■ Dos mensajes originales iguales, cifrados con la misma clave, producen siempre mensajes cifrados iguales.

■ Para descifrar parte de un mensaje no es preciso descifrarlo completamente desde el principio, basta con hacerlo desde el bloque que interese.

En cuanto a la arquitectura del cifrado en bloque, cabe señalar que todos ellos se componen de cuatro elementos:

■ Transformación inicial. Puede tener una o dos funciones, la primera consiste en aleatorizar los datos de entrada (para ocultar bloques de datos de todo ceros o unos, etc.),

careciendo de significación criptográfica si no depende de la clave, como sucede en el DES. La segunda función, solamente presente en algunos criptosistemas, como el RC5 e IDEA, tiene significación criptográfica, dificultando ataques por análisis lineal o diferncial, en este caso es función de la clave.

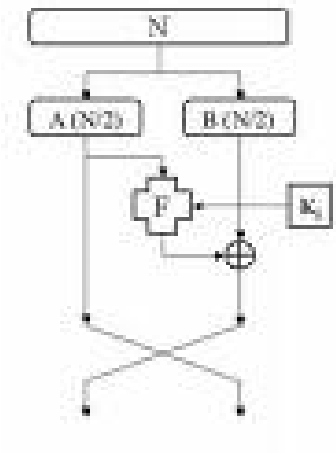
■ Una función criptográficamente débil iterada r veces o vueltas. Las vueltas intermedias consisten en una función no lineal complicada de los datos y la clave, que puede ser unidireccional (DES) o no (IDEA, RC5). Dicha función no lineal puede estar formada por una sola operación muy compleja o por la sucesión de varias transformaciones simples.

Las vueltas intermedias se enlazan por sumas módulo 2 bit a bit con datos que proceden de la transformación inicial o de las vueltas precedentes. De esta forma se facilita que se produzca una involución cuando se repite el proceso de forma idéntica pero eligiendo las claves de descifrado en orden inverso, obteniéndose así los datos de partida.

Las vueltas intermedias no han de formar grupo para que el conjunto de varias pasadas sucesivas con sus subclaves correspondientes no sean equivalentes a una pasada única con una subclave diferente, lo cual sería un desastre.

■ Transformación final. Sirve para que las operaciones de encriptación y desencriptación sean simétricas. Cuando las vueltas de encriptación son de una sola operación, separadas por sumas módulo 2 bit a bit (DES, RC5), esta transformación se limita a realizar la operación inversa de la transformación inicial. No obstante, en los sistemas donde las vueltas de encriptación acaban con una operación que afecta a todos los bits del bloque, la transformación de salida debe realizar tanto la función inversa de esta operación como la inversa de la transformación inicial

Red de Feistel



■ Algoritmo de expansión de clave. Tiene por objeto convertir la clave de usuario, normalmente de longitud limitada entre 32 y 256 bits, en un conjunto de subclaves que pueden estar constituidas por varios cientos de bits en total. Conviene que sea unidireccional y que el conocimiento de una o varias subclaves

intermedias no permita deducir las subclaves anteriores o siguientes. Además, ha de vigilaese que las subclaves producidas no constituyan un pequeño subconjunto monótono de todas las posibles.

Los cifrados de Feistel son aquellos criptosistemas en los que el bloque de datos se divide en dos mitades y en cada vuelta de encriptación se trabaja, alternativamente, con una de las mitades. Pertenecen a este tipo los criptosistemas LUCIFER, DES, LOKI, y FEAL.

4.3.2 DES

En 1973, el NBS(40) organizó un concurso solicitando un algoritmo de encriptación para la protección de datos de ordenador durante su transmisión y almacenaje. En 1974, la corporación IBM presentó, entre otras, una propuesta inspirada en su sistema LUCIFER, que, convenientemente modificada, dio lugar al Data Encrytion Standard (41), abreviadamente llamado DES. La aprobación y modificación de la propuesta se hizo bajo la supervisión de la NSA (42).

En cualquier caso, la longitud de clave del DES es bastante modesta lo cual la hace desaconsejable en el actual desarrollo de la informática

El DES es un algoritmo de cifrado en bloque con una longitud de bloque de 64 bits (ocho símbolos ASCII) y una longitud de clave de 56 bits, lo que equivale a que existan $2^{56} = 7{,}2 \cdot 10^{16}$ claves diferentes.

La norma exige que el DES se implemente mediante un circuito integrado electrónico. En el año 1981, ANSI (43) adoptó el DES con el nombre de Data Encryption Algorithm, abreviadamente DEA, para no tener que realizar la implementación con circuito integrado y poder ser programado en un ordenador.

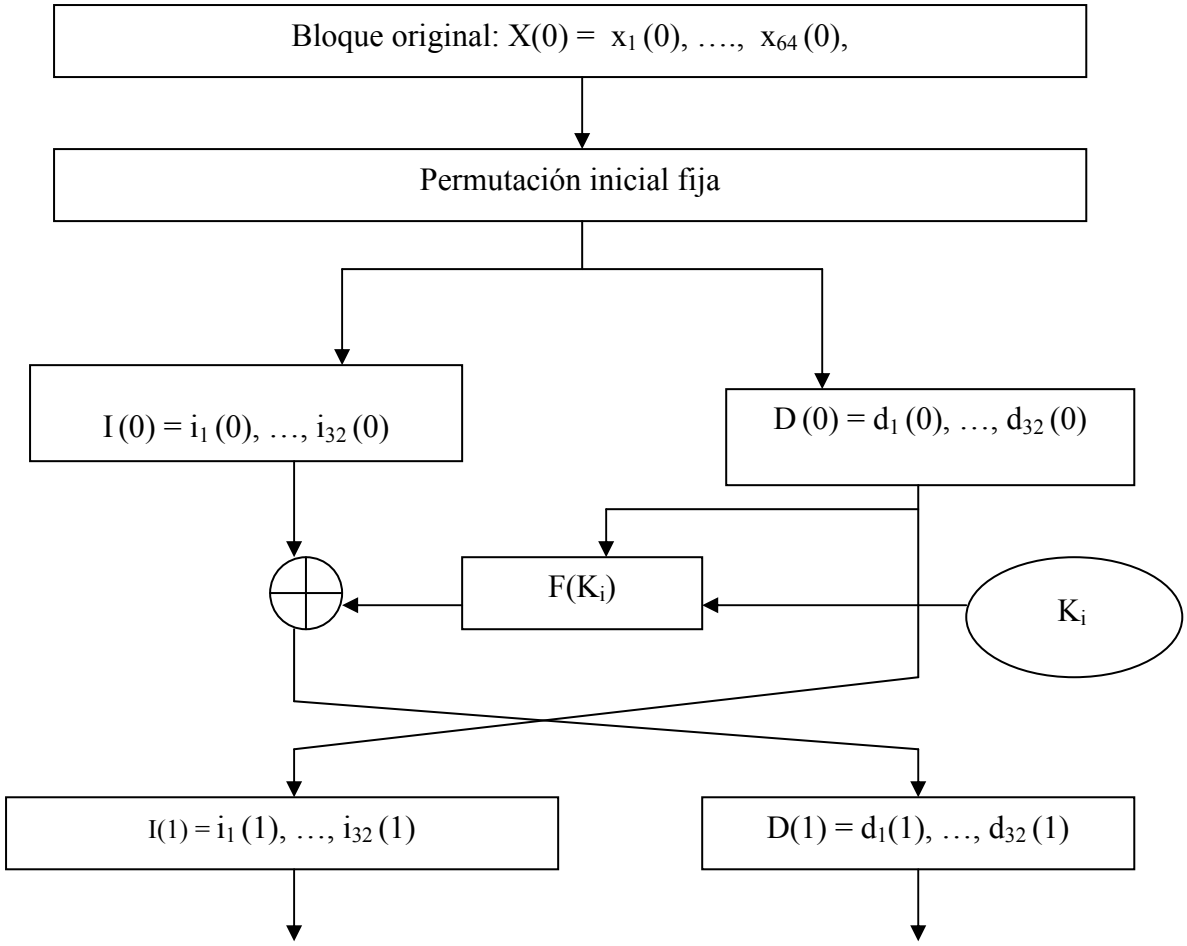
No resulta difícil conseguir versiones software del DEA en servidores FTP de Internet.

(40) National Bureau of Standards, USA
(41) Norma de encriptación de datos
(42) National Security Agency, USA
(43) Americam National Standars Institute, USA

4.3.2.1 Estructura e involución del DES

Estructuralmente hablando, el DES trabaja alternativamente sobre las dos mitades del bloque a cifrar. Primeramente se hace una permutación inicial fija y, por tanto, sin valor criptográfico. Seguidamente se divide el bloque en dos mitades, la derecha y la izquierda. Posteriormente se realiza una operación modular que se repite 16 veces, dicha operación consiste en sumar módulo 2 a la parte izquierda con una función $F(K_i)$ de la parte derecha, gobernada por la clave K_i. Finalmente se intercambian las partes derecha e izquierda.

El siguiente esquema representa el inicio y la primera vuelta de la estructura DES

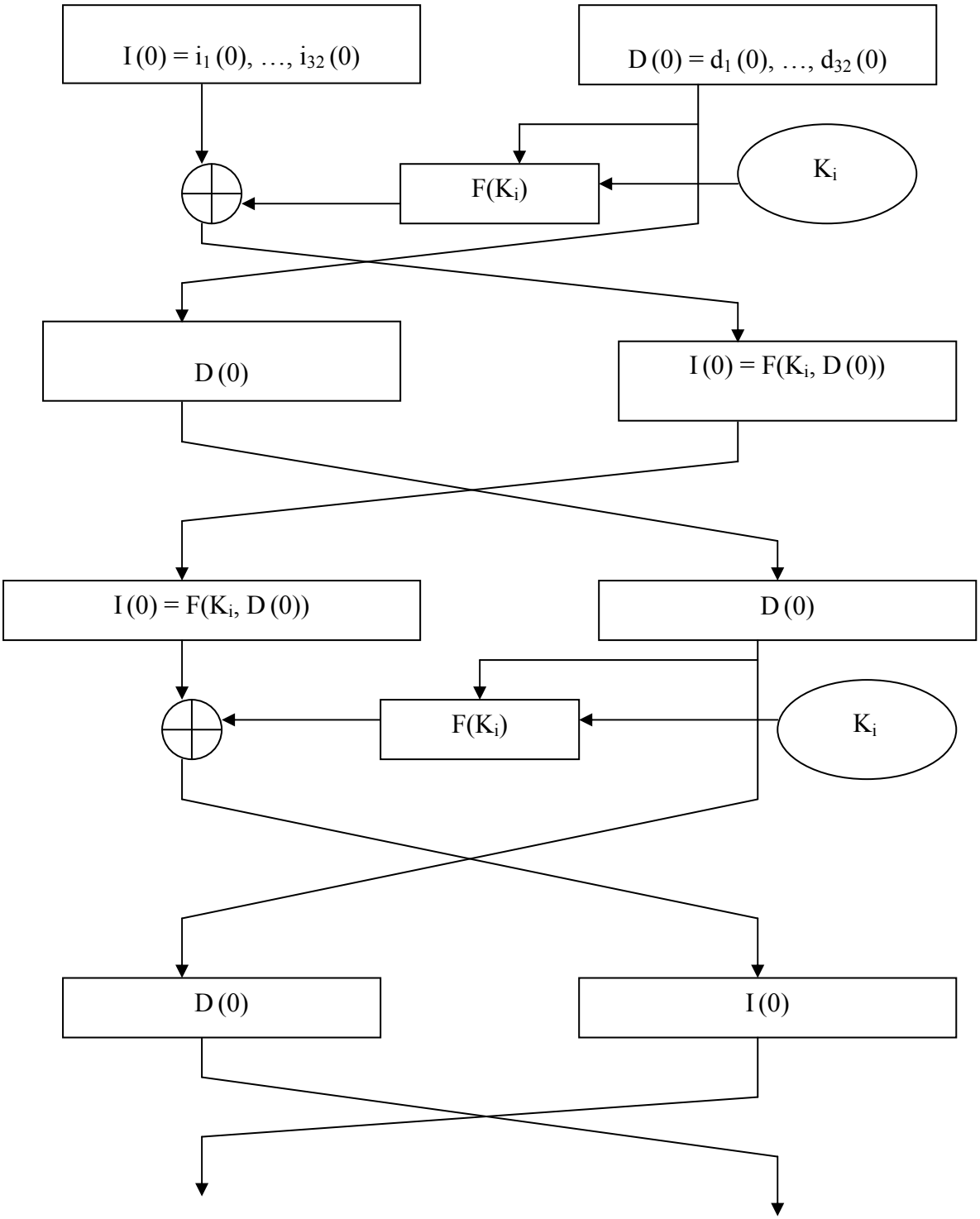


En la vuelta número 16 se omite el intercambio, pero se remata el algoritmo con una permutación final que es la inversa de la inicial

Para descifrar el DES basta con repetir la operación modular, que es una involución, es decir, su aplicación repetida dos veces conduce a los datos originales. Es

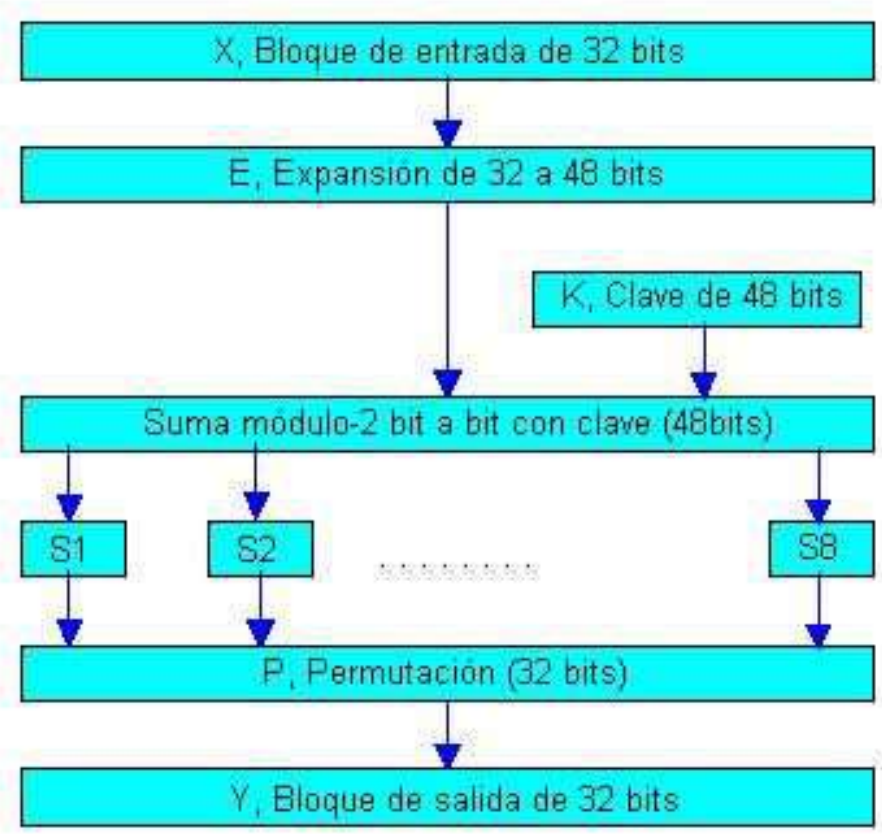
evidente que no es preciso invertir la función F sino repetirla. Esto permite que dicha transformación sea una función de un solo sentido, empleando operaciones no lineales.

El siguiente esquema representa los pasos de la involución en el DES:



4.3.2.2 Manipulaciones en el DES

La función F descrita es un conjunto de operaciones que se combinan según el siguiente esquema.



Estructura de la función F en DES

La primera manipulación consiste en fabricar un vector de 48 bits a partir de los 32 bits iniciales mediante una expansión lineal, expuesta en la siguiente tabla

Izquierda	32	1	2	3	4	5	4	5	6	7	8	9
Centro izda	8	9	10	11	12	13	12	13	14	15	16	17
Centro dcha	16	17	18	19	20	21	20	21	22	23	24	25
Derecha	24	25	26	27	28	29	28	29	30	31	32	1

Los bits originales aparecen en rojo, mientras que los bits añadidos están representados en azul (por problemas de presentación, aparecen cuatro filas, que han de considerarse correlativas).

Después se combina la clave local de 48 bits con el vector anterior por suma de módulo 2 bit a bit, consiguiéndose otro vector de 48 bits, que se divide en ocho grupos de seis bits. Cada uno de estos grupos entra en cada una de las ocho funciones denominadas en el esquema anterior como "cajas S". Siendo dichas cajas las responsables de la no-linealidad del DES. En cada caja entran s6is bits, pero sales solo cuatro. Además, las cajas S están elegidas de forma que la sustitución producida no sea afín ni función lineal de la entrada y los bits sobre los que se hace la sustitución son los cuatro centrales.

En cada caso hay cuatro sustituciones posibles, dependiendo del valor de los bits laterales. Cuando se cambia un solo bit de la entrada, resultan cambiados por lo menos dos bits de la salida

Los principios para la elección de las cajas S jamás han sido revelados, y es información clasificada por el gobierno de los Estados Unidos.

Finalmente, se pasa la información por una "caja P", la cual es una permutación lineal fija (expuesta en la siguiente tabla), elegida de modo que la difusión de bits sea máxima a lo largo del bloque de 32 bits.

El bloque	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
Se cambia por	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

4.3.2.3 Expansión en el DES

Aunque en el DES de manejan claves de 64 bits, la primera operación que se realiza es su reducción a 56 bits, eliminando un bit de cada ocho, seguidamente se reordenan los bits restantes. Operación que carece de significación criptográfica.

A continuación se generan los 16 subclaves necesarias en 16 vueltas de algoritmo. Cada subclave está compuesta por 48 bits, Hay que tener en cuenta, que durante el descifrado se toman en orden inverso al de cifrado.

Para generar las subclaves, en primer lugar se divide la clave de 56 bits en dos mitades de 28 bits. Seguidamente, las mitades se permutan circularmente hacia la izquierda uno o dos bits dependiendo de la vuelta. Resultando

Vuelta afectada	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Número de bits	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Tras las rotaciones se unen de nuevo las mitades, obteniéndose, otra vez, 16 grupos de 56 bits. Finalmente, se procede a seleccionar 48 bits de cada grupo para formar las 16 subclaves mediante una operación denominada "permutación con compresión". Los bits elegidos son iguales para todas las subclaves.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Permutación con compresión final de la clave de 56 bits

4.3.2.4 Propiedades del DES

Las propiedades fundamentales son:

■ Dependencia entre símbolos. Cada bit del texto cifrado es una función compleja de todos los bits de la clave y todos los bits del texto original.

■ Cambio de los bits de entrada. Un cambio de un bit en el mensaje original produce el cambio del 50%, aproximadamente, de los bits del bloque cifrado.

■ Cambio de los bits de clave. Un cambio de un bit de la clave produce, aproximadamente, el cambio de la mitad de los bits del bloque cifrado.

■ Claves débiles. Existen cuatro claves débiles que producen un cifrado fácil de descifrar, debido a que todas las claves parciales K1 a K16 son iguales. Además, existen 28 claves semidébiles que, igualmente, producen un mensaje cifrado fácil de descifrar, esta vez debido a que solo se producen dos o cuatro subclaves parciales diferentes. Por este motivo, cuando se elige una clave al azar, es fundamental asegurarse de que no se ha producido una de estas claves.

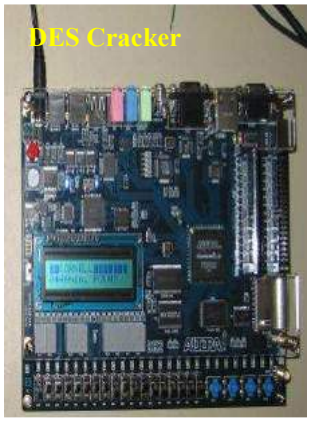
■ Un error en la trasmisión de un texto cifrado se propaga a todo el bloque del que forma parte, produciendo, consecuentemente, un conjunto de errores del descifrado de 64 bits.

4.3.2.5 Seguridad del DES

Teóricamente el algoritmo de Vernam es indescriptible. Sin embargo, no existe ninguna prueba que garantice la indescifrado, en la práctica, de un algoritmo cifrado, lo único que existe son demostraciones de que ciertos algoritmos son vulnerables.

La opinión generalizada es que el DES es un excelente sistema de cifrado, ya que hasta hace muy poco, nadie ha demostrado ser capaz de reventar un DES. Su único problema es que su espacio de claves resulta excesivamente reducido para el actual estado del arte de la tecnología electrónica.

El primer ataque especializado para el DES ha sido el Criptoanálisis diferencial, el cual consigue recuperar la clave del DES a cambio de un considerable esfuerzo computacional, que obliga al análisis de una cantidad ingente de parejas de textos claros y sus correspondientes cifrado.



En la actualidad, el sistema de ataque al DES más eficaz es el DES Cracker, una máquina que data de mayo de 1998, capaz de probar todas las claves del DES en nueve días, o lo que es lo mismo, el tiempo medio que requiere para encontrar una clave es de cuatro días y medio.

La construcción de una máquina similar no está al alcance de un particular, pero si a la de cualquier gobierno u organización. Por lo tanto, desde esta fecha quedo patente que el DES ya no era tan seguro y debería prescindirse de él en beneficio de algoritmos con un espacio de claves considerablemente mayor.

A partir de ese año se ha utilizado el Triple-DES [(44)], como solución transitoria mientras se desarrollaba un nuevo estándar, el AES, publicado en noviembre de 2001.

4.3.3 AES

En 1996, el NIST[(45)] dio los primeros pasos para la creación de un Estándar de Cifrado Avanzado (Advanced Encryption Standard) que de forma abreviada se conoce como AES. Su objetivo fue desarrollar una especificación para encontrar un algoritmo de cifrado que sustituyera al anticuado DES, de tal forma que el nuevo algoritmo fuese capaz de proteger la información sensible de los ciudadanos y del gobierno hasta bien entrado el siglo XXI.

Dado que se desea que el estándar pueda utilizarse por lo menos hasta el año 2060, debió realizarse una elección conservadora. Ante los últimos avances teóricos en computación, es licito pensar que si se llegasen a construir computadores cuánticos totalmente operativos, los problemas de números hoy considerados irresolubles en un tiempo razonable, como la factorización o los logaritmos discretos, se podrán resolver más rápidamente, quebrantando definitivamente la seguridad de los algoritmos criptográficos con longitudes de claves actuales.

Para llevar a cabo el proyecto, se reunió a diversos diseñadores. Finalmente, el 2 de octubre de 2000, el NIST anunció el algoritmo ganador: el Rijndael o AES, propuesto por los belgas Vincent Rijmen y Joan Daemen.

El AES es un cifrador que opera con bloques de longitud igual a Nb palabras de 32 bits. Estos valores de Nb pueden ser 4,6 y 8; por otro lado, la longitud de clave es de Nk palabras de 32 bits e igualmente los valores de Nk pueden ser 4, 6 y 8. Por lo tanto, las longitudes de clave y bloque pueden ser de 128, 192 ó 256 bits.

(44) http://www.tropsoft.com/strongenc/des3.html
(45) National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología

El AES es fácilmente adaptable a cualquier longitud de bloque y/o clave múltiplo de 32 bits.

4.3.3.1 Estructura del AES

Se trata de un cifrador iterado, relativamente sencillo, que emplea funciones invertibles y opera con bloques enteros y bytes en vez de bits.

Estado, el resultado obtenido en cada paso del algoritmo, es un conjunto de tantos bits como la longitud del bloque. Los bits adyacentes se agrupan de ocho en ocho, formando bytes, y éstos en una tabla cuadrada de cuatro filas y Nb columnas (cuatro para el caso particular de este estándar.

Al principio del algoritmo se copian los bytes de entrada en_i que estaban numerados correlativamente en la tabla de Estado.

BYTES DE ENTRADA ESTADO BYTES DE SALIDA

en_0	en_4	en_8	en_{12}
en_1	en_5	en_9	en_{13}
en_2	en_6	en_{10}	en_{14}
en_3	en_7	en_{11}	en_{15}

→

$s_{0,0}$	$s_{4,0}$	$s_{8,0}$	$s_{12,0}$
$s_{1,0}$	$s_{5,0}$	$s_{9,0}$	$s_{13,0}$
$s_{2,0}$	$s_{6,0}$	$s_{10,0}$	$s_{14,0}$
$s_{3,0}$	$s_{7,0}$	$s_{i11,0}$	$s_{15,0}$

→

sal_0	sal_4	sal_8	sal_{12}
sal_1	sal_5	sal_9	sal_{13}
sal_2	sal_6	sal_{10}	sal_{14}
sal_3	sal_7	sal_{11}	sal_{15}

En el esquema anterior, se ilustra el proceso de cifrado completo, que consta de tres etapas:

- Una transformación inicial
- Nr -1 vueltas regulares
- Una vuelta final.

La transformación inicial consiste en una suma módulo 2 (XOR) de los primeros 128 bits de la clave con el mensaje claro.

El número de vueltas Nr es función de la longitud de clave :

- Nr = 10 para clave de 128 bits.
- Nr = 12 para clave de 192 bits.
- Nr = 14 para clave de 256 bits.

La generación de subclaves se obtiene a partir de la clave inicial mediante un algoritmo de expansión, denominado, Key expansión, y una regla de selección para cada vuelta.

El número total de bits de las subclaves es iguala la longitud del bloque por el número de vueltas más uno. Por ejemplo, para un bloque de 128 bits y 10 vueltas, el número de bits total de las subclaves es:

128 x 11 = 1408 bits ó 176 bytes.

Para el mayor bloque posible, 256 bits con 14 vueltas de cifrado, el número total de bits para el total de subclaves es:

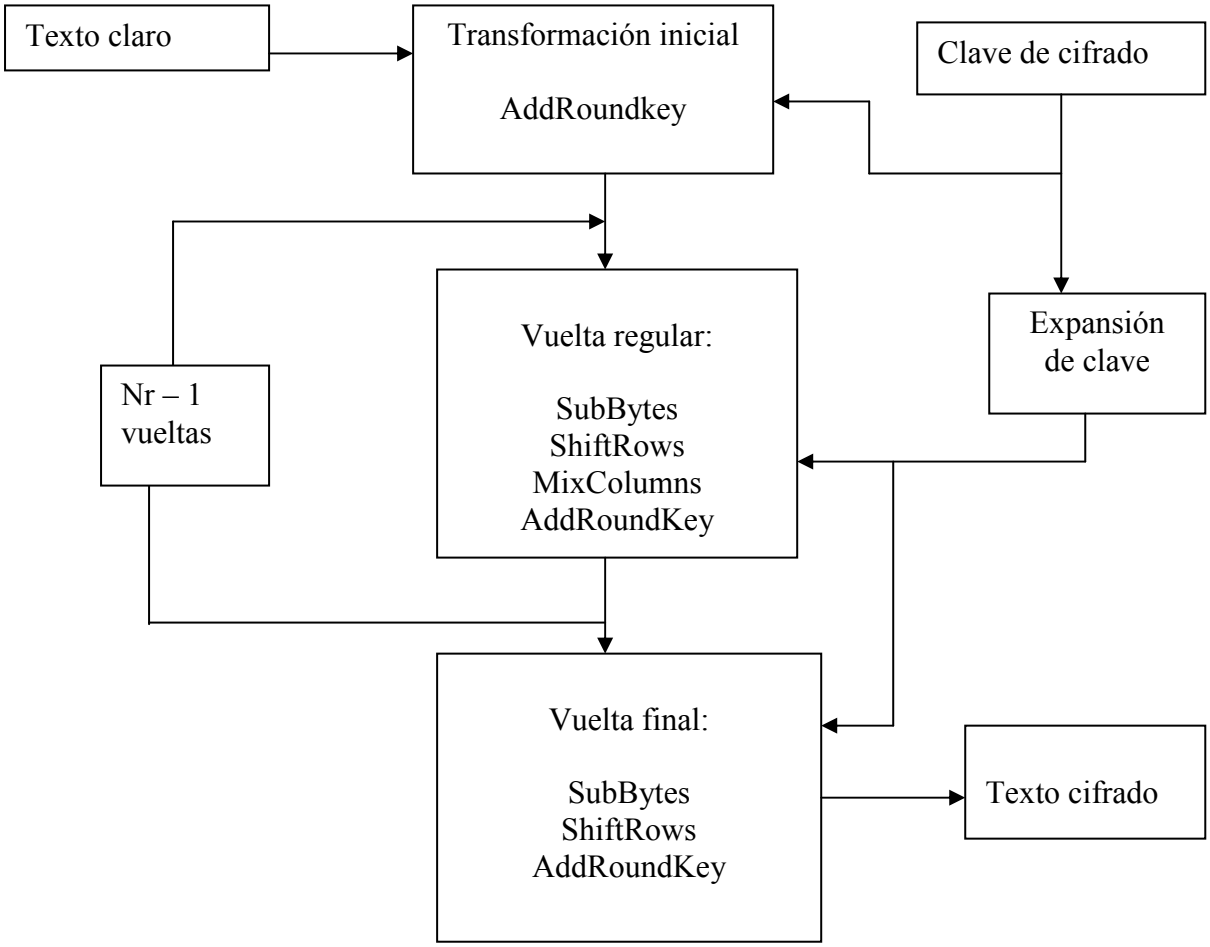
256 x 15 = 3840 bits ó 480 bytes.

La clave de cifrado, de 16, 24 ó 32 bytes se transforma en una clave expandida mediante una función, denominada Key expansión, para obtener los bits necesarios, anteriormente descritos. Sabiendo que una palabra es un vector de 4 bytes, y suponiendo que la clave inicial fuera 128 bits, se obtendría que la clave expandida contiene 44 palabras para cifrar bloques de 128 bits y 120 palabras para cifrar bloques de 256 bits.

Las subclaves para cada vuelta se obtiene de la Key expansión mediante la regla: la primera subclave consiste en las primeras Nb palabras, la segunda son las siguientes Nb palabras, etc.

La clave expandida se obtiene siempre de la clave de cifrado inicial, no se especifica nunca y y no existen restricciones para la misma que, lógicamente, ha de mantenerse secreta.

El esquema siguiente corresponde al esquema general del AES:



La transformación que tiene lugar en cada vuelta regular de cifrado está compuesta, a su vez, por cuatro transformaciones diferentes:

■ SubBytes: sustitución no lineal de bytes (función solamente del Estado).

■ ShiftRows: desplazamiento de las filas del Estado cíclicamente, con diferentes saltos (función del Estado).

■ MixColumns: mezcla de columnas (función del Estado).

■ AddRoundKey: suma módulo 2 (XOR) con la subclave de vuelta correspondiente (función del Estado y la subclave).

La vuelta final es casi igual a las vueltas regulares , debido a que no se aplica la transformación MixColumn, por lo tanto en la vuelta final solo se sufren tres transformaciones: SubBytes, ShiftRows y AddRoundKey.

El descifrado se realiza efectuando las operaciones inversas de las empleadas en el cifrado, en orden inverso al utilizado, las cuales se irán colocando en cada transformación.

4.3.3.2 Transformación SubBytes e InvSubBytes

Se aplica a todos y cada uno de los bytes del Estados. Consiste en una única caja S, similar a las del DES.

El número de bits de entrada y salida es idéntico. Además, constituye una aplicación biunívoca, por lo que es sencillamente invertible.

Por consiguiente, su fin es introducir una no-linealidad en el proceso.

A diferencia del DES, en el nunca se revelaron las razones del diseño de las cajas S, lo que invita a sospechar posibles trampas ocultas, los autores del AES dan una fórmula matemática para su construcción, orientada a cumplir con los siguientes criterios:

■ Minimizar la correlación entre la entrada y la salida.

■ Minimizar la probabilidad de propagación de diferencias

■ Maximizar la complejidad de la expresión algebraica de la transformación.

La siguiente tabla presenta la caja S en formato hexadecimal:

b

a	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	f5	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Para la construcción de dicha tabla, primero se halla la inversa multiplicativa del byte a transformar, en GF(2^8) módulo ($x^8 + x^4 + x^2 + x + 1$), tomando sus bits como los coeficientes de un polinomio en GF(2^8). Excepcionalmente, el byte {0 0} se trasforma en sí mismo. Finalmente, se efectúa una transformación afín en GF(2), definida por la siguiente tabla:

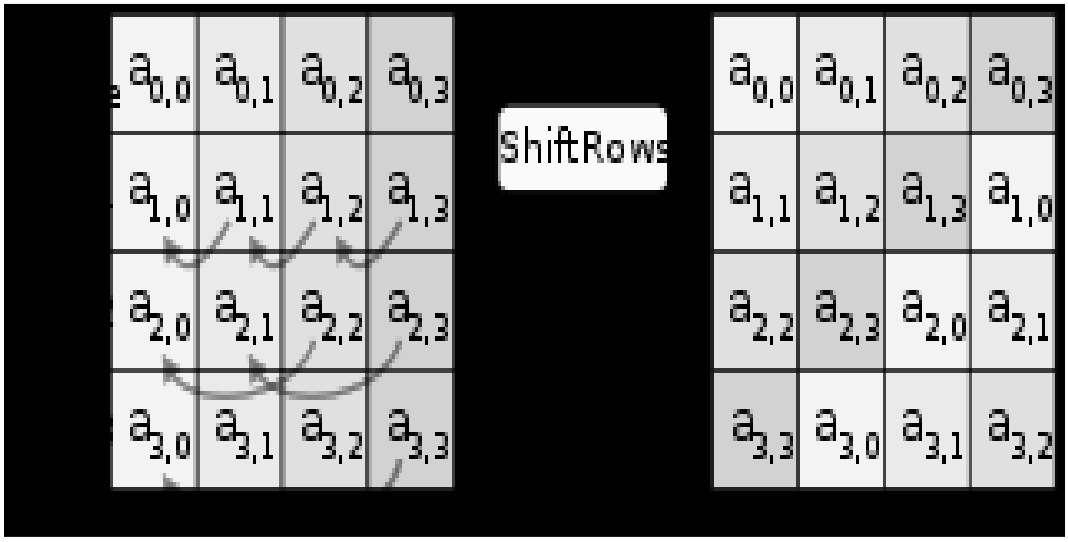
$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

donde a_i son los valores de entrad y b_i los valores de salida.

En la operación de descifrado (InvSubBytes) se invierte la transformación interpretando la tabla anterior en sentido inverso, aunque sería más cómodo y ágil construir y utilizar una tabla inversa.

4.3.3.3 Transformación ShiftRows e InvShiftRows

En este caso se permutan cíclicamente los contenidos de las filas del Estado.



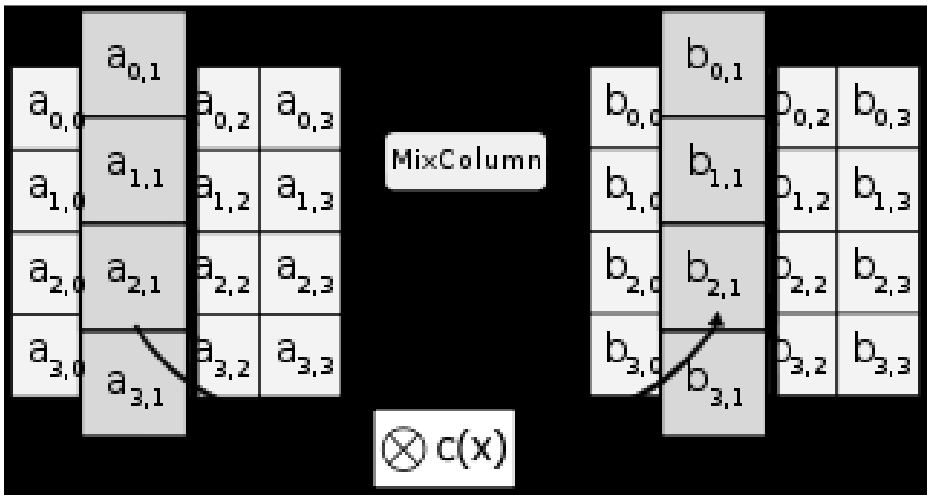
La primera fila permanece invariable, mientras que las restantes se desplazan cíclicamente a la izquierda uno, dos y tres lugares, respectivamente.

Esta transformación ayuda a conseguir la difusión, volviéndose resistente a los ataques diferenciales.

En la operación de descifrado (InvShiftRows) se invierte la transformación dejando la primera fila invariable, mientras que las restantes se desplazan cíclicamente a la derecha uno, dos y tres lugares, respectivamente.

4.3.3.4 Transformación MixColumns e Inv MixColumns

Esta Transformación opera sobre el Estado columna a columna.



Consiste en multiplicar cada columna por una matriz de la forma:

$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \otimes \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix}$$

donde $a_{i,j}$ y $b_{i,j}$ son los valores del Estado de la columna j antes y después de la transformación, respectivamente, estando los coeficientes de la matriz expresados en código hexadecimal.

Cada byte es tratado como un polinomio en GF(2^8), lo que implica que los bits que lo componen sean considerados como coeficientes de un polinomio, más que como números.

En todos los casos, si el resultado tiene más de ocho bits, se reduce módulo $(x^8 + x^4 + x^2 + x + 1)$.

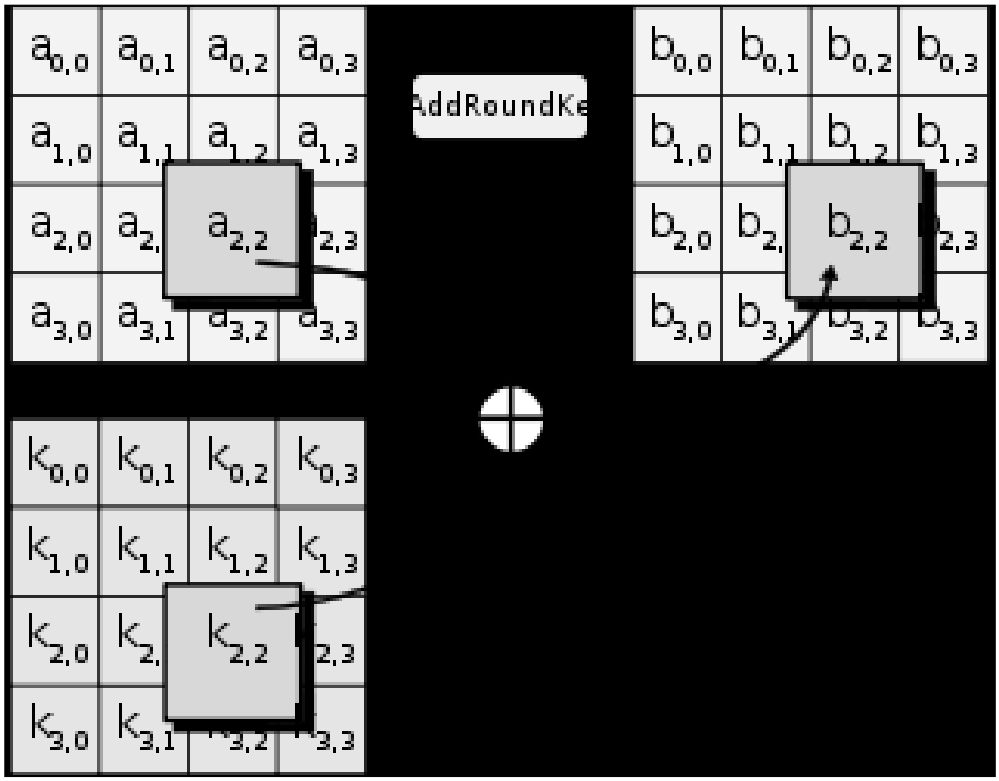
En la operación de descifrado (InvMixColumns) se invierte la transformación operando sobre el Estado, columna por columna. Consistiendo en multiplicar cada columna por una matriz de la forma:

$$\begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \otimes \begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ a_{3,j} \end{bmatrix}$$

donde $b_{i,j}$ y $a_{i,j}$ son los valores del Estado de la columna j antes y después de la transformación inversa. Análogamente los coeficientes de la matriz están expresados en código hexadecimal.

4.3.3.5 Transformación AddRoundKey e InvAddRoundKey

En esta transformación se suman módulo 2 (XOR) los bits del Estado y los bits de la subclave de vuelta Kr correspondiente.



En la operación de descifrado (InvAddRoundKey) se invierte la transformación restando módulo 2 (XOR) los bits de la subclave de vuelta correspondiente de los bits de Estado.

4.3.3.6 Esquema de clave en el AES

Debido a que la longitud de clave en el AES puede ser de 128, 192 ó 256 bits, es necesario generar muchas subclaves a partir de ella: la subclave inicial, más Nr subclaves de vuelta, cada una de ellas de cuatro palabras de 32 bits. Las subclaves requeridas se generan por derivación de la clave de cifrado mediante un procedimiento de expansión, cuyo esquema (46) varia en función de la longitud de la clave de cifrado.

Como ya se adelanto anteriormente, dada una clave de cifrado k, la expansión de clave en AES se realiza construyendo una secuencia W de Nb (Nr + 1) palabras W_i de 32 bits, con la de 192 bits se generan 52 palabras de 32 bits y con la de 256 bits se generan 60 palabras de 32 bits

En todos los casos, las Nk palabras de la clave constituyen las primeras Nk palabras de la clave expandida W_0 …….. W_{Nk-1}.

Si las palabras de la clave expandida se alinean en filas de longitud Nk, se aprecia que las nuevas palabras se fabrican a partir de la suma módulo 2, bit a bit, de la palabra anterior y la palabra situada inmediatamente encima, con la excepción de la primera columna de todos los esquemas y de la cuarta columna del esquema para Nk = 8.

4.3.3.7 Seguridad del AES

El margen de seguridad, en este método de cifrado, es difícil de medir, debido a que el número de rondas cambia con el tamaño de clave, siendo de 10 rondas para llaves de 128 bits, 12 rondas para llaves de 192 bits, y 14 rondas para llaves de 256 bits. Hasta el año 2005, los mejores ataques conocidos son sobre versiones reducidas a 7 rondas para llaves de 128 bits, 8 rondas para llaves de 192 bits, y 9 rondas para llaves de 256 bits.

Algunos criptógrafos muestran preocupación sobre la seguridad del AES. Ellos manifiestan que el margen entre el número de rondas especificado en el cifrador y los mejores ataques conocidos es muy pequeño. Así pues, existe el riesgo recae de que sea posible encontrar alguna manera de mejorar los ataques y de ser así, el cifrado podría ser roto.

(46) Una representación graficadle esquema de clave en AES para 128,192 y 256 se puede encontrar en la bibliografía adjuntada

En el contexto criptográfico se considera "roto" un algoritmo si existe algún ataque más rápido que una búsqueda exhaustiva (ataque por fuerza bruta).

Otra preocupación recae sobre la estructura matemática de AES. A diferencia de la mayoría de cifradores de bloques, AES tiene una descripción matemática muy ordenada, y aunque todavía, no ha llevado a ningún ataque, algunos investigadores están preocupados porque futuros ataques quizá encuentren una manera de explotar dicha estructura. Sin embargo, ésta tiene la ventaja de ser bastante simple, lo cual facilita su análisis de seguridad durante el tiempo especifico en el proceso de desarrollo de AES.

Por lo tanto, puede concluirse que, en principio, el margen de seguridad del AES es adecuado.

4.4 La mecanización del secreto

A finales del siglo XIX, la criptografía estaba en desorden desde que se acabo con la seguridad de la cifra de Vigenère. Los criptógrafos habían estado buscando una nueva cifra que logrará restablecer la comunicación secreta, para así, utilizar el recién inventado, telégrafo, sin que las comunicaciones fueran descifradas. Por otro lado, el físico italiano Marconi invento una forma de telecomunicación, todavía, más poderosa, que hizo, aún más apremiante, la necesidad de comunicación segura.

Marconi no tardo en transmitir y recibir pulsaciones de información entre distancias de hasta 2,5 kilómetros. Había inventado la radio, la cual tenía la gran ventaje de no necesitar cables, ya que la señal viajaba por el aire. En 1896, buscando respaldo económico para su idea, Marconi emigró a Gran Bretaña, donde obtuvo su primera patente. Continuando con sus experimentos, aumentó el alcance de sus comunicaciones por radio. Al mismo tiempo, comenzó a buscar aplicaciones comérciales, señalando las dos ventajas principales de la radio: hallarse exenta de construir las costosas líneas de telégrafo y poseer el potencial de enviar mensajes entre lugares que de otra forma se mantendrían aislados.

En 1942 los físicos del momento descubrieron la ionosfera, la cual actúa como un espejo, permitiendo que las ondas de radio reboten en ella además de rebotar en la

superficie de la Tierra, por lo que los mensajes de radio pueden llegar a cualquier parte del mundo tras una serie de rebotes entre la ionosfera y la Tierra.

Por todas estas razones, la radio permitía coordinar una flota sin importar donde se hallasen los barcos, análogamente, también permitía que los generales dirigiesen sus campañas manteniéndose en contacto continuo con las batallones. Sin embargo, la característica principal de la radio es, también, su mayor debilidad militar, debido a que los mensajes llegarán, inevitablemente, tanto al enemigo como al receptor, por lo que la codificación fiable se convirtió en algo imprescindible.

Entre los años 1914 y 1918, primera Guerra Mundial, no surgieron grandes descubrimientos, tan sólo un catálogo de fracasos criptográficos, no porque los creadores de código no crearán cifras nuevas sino porque una a una fueron descifradas.

Desde que se resolvió la cifra Vigenère en el siglo XIX, los descifradores habían mantenido ventaja sobre los codificadores. Hasta que, hacia el final de la primera guerra mundial, cuando ya los criptógrafos estaban desesperados, unos científicos estadounidenses llevaron a cabo un avance extraordinario, comprobando que la cifra Vigenère podía utilizarse como base para una forma nueva y más exitosa de codificación, de tal forma que la nueva cifra podía ofrecer una seguridad perfecta.

La principal debilidad, como ya se ha comentado anteriormente, de la cifra Vigenère es su naturaleza cíclica. Pero ¿qué ocurriría?, si la clave fuese más larga de las cinco letras que tiene, es decir, si la clave fuese tan larga como el mensaje. Entonces, la técnica criptoanálista desarrollada por Babbage y Kasiski[47] no funcionará. Sin embargo, aparece como problema que el criptógrafo debe crear una clave muy larga, es decir, si el mensaje tiene cientos de palabras, la clave necesita tener cientos de letras. Por lo que se intento basarla en, por ejemplo, la letra de una canción ó elegir un libro cualquiera y basar la clave en una serie de nombres al azar (si el libro es de ornitología en nombres de pájaros, etc.). Finalmente, se comprobó que semejantes claves son fundamentalmente defectuosas, ya que la inseguridad surge porque la clave está formada por palabras con sentido

(47) http://en.wikipedia.org/wiki/Kasiski_examination y http://homepage.cem.itesm.mx/rogomez/CursoCriptoTec/babbage.html

Este nuevo sistema de criptoanálisis comienza con la suposición de que el texto cifrado contiene algunas palabras corrientes.

En 1918 los criptógrafos comenzaron a experimentar con claves que carecían de estructura, obteniéndose de este modo una cifra indescifrable.

Al final de la primera Guerra Mundial, el comandante Joseph Mauborgne, jefe de la investigación criptográfica del ejercito de Estados Unidos, introdujo el concepto de la clave aleatoria, es decir, una clave que no constaba de una serie de palabras reconocibles, sino de una serie de letras mezcladas al azar. Abogó por el uso de estas claves aleatorias como parte de la cifra de Vigenère para proporcionar un nivel de seguridad sin precedentes.

La primera fase del sistema de Mauborgne era compilar un gran cuaderno consistente en cientos de hojas de papel, en las que en cada una de ellas había una clave única formada de líneas de letras reunidas al azar. Existían dos copias del cuaderno, una para el receptor y otra para el emisor, de tal forma que para codificar un mensaje, el emisor aplicaría la cifra de Vigenère usando la primera hoja de papel del cuaderno como clave. Mientras que el receptor puede descifrar fácilmente el texto cifrado usando la clave idéntica e invirtiendo la cifra de Vigenère. Una vez enviado, recibido y descifrado el mensaje con éxito, tanto el emisor como el receptor romperán la hoja del libro utilizada para no volver a ser usada. Cuando se codifica el siguiente mensaje se usa la siguiente clave aleatoria del cuaderno, que también posteriormente será destruida y así sucesivamente. Debido a que cada clave se utiliza una, y sólo una, vez, el sistema se conoce con el nombre de "la cifra de cuaderno de uso único", la cual vence todas las debilidades previas.

Sí un mensaje es interceptado, el primer obstáculo para el criptoanalizador es que, por definición, en una clave aleatoria no hay repetición, de modo que el método de Babbage y Kasiski no puede penetrar en la cifra de cuaderno único. Como alternativa, podrá intentar colocar una palabra "prueba" en varios lugares y tratar de deducir el trozo correspondiente a la clave. Sin embargo, aunque esta palabra funcionase, el criptoanalista no puede saber si la palabra de prueba está o no en el lugar correcto.

Evidentemente probando todas las claves posibles, cosa que está completamente fuera de las posibilidades humanas y mecánicas, el criptoanalista encontraría el mensaje correcto, pero también surgirían todos los mensajes incorrectos. Por consiguiente, el criptoanalista sería incapaz de distinguir el correcto de todos los demás.

Por lo tanto, la seguridad de la cifra de cuaderno único se debe enteramente a que la secuencia de las letras de la clave es por completo aleatoria. De hecho, se puede probar matemáticamente que es imposible que un criptoanalista descifre un mensaje codificado con una cifra de cuaderno de uso único. En otras palabras, la cifra de cuaderno de uso único no es meramente considerada indescifrable, como sucedía con la cifra Vigenère en el siglo XIX, sino que es en realidad absolutamente segura. Así pues, dicha cifra ofrece garantía de secreto, considerándose el "Santo Grial" de la criptografía.

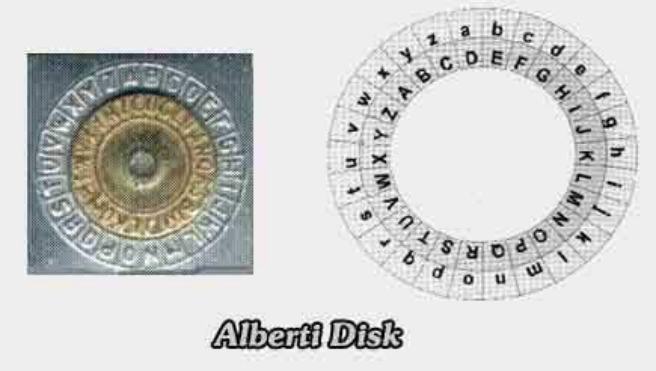
No obstante, la cifra de cuaderno de uso único no pudo ser utilizada en el calor de la batalla, es más, no se ha usado casi nunca, debido a que, y aunque teóricamente es perfecta, en la práctica, padece dos dificultades fundamentales, primero y especialmente el problema de poder crear grandes cantidades de claves aleatorias. Los criptógrafos se han dado cuenta que crear una clave aleatoria requiere muchísimo tiempo, esfuerzo y dinero. Por eso las mejores claves aleatorias se crean utilizando procesos físicos naturales, como la radioactividad, que se sabe que exhibe una conducta verdaderamente aleatoria. Sin embargo, esto no resulta práctico para la criptografía cotidiana. Además, en el caso de que pudieran crearse suficientes claves aleatorias, todavía quedaría por resolver la segunda dificultad, que no es otra que su distribución.

Otro factor a tener en cuenta, es que el uso generalizado del cuaderno de uso único llenaría el campo de batalla de mensajes y contables, pero es importante resaltar que no deben emplearse atajos, es decir, emplear claves iguales para mensajes distintos con el fin de evitar este problema. Otro problema es, el hecho de que, si el enemigo captura un solo juego de claves, todo el sistema de comunicaciones se vería comprometido.

Ante estos problemas los criptógrafos de la época se vieron obligados a abandonar el lápiz y el papel, y sacar partido de la tecnología más avanzada para codificar mensajes. Ya que el uso del cuaderno de uso único es factible para personas que necesitan una comunicación ultrasegura y pueden permitirse mantener los enormes costes de creación

y distribución segura de las claves. En ejemplo actual de uso de cifra de cuaderno único es la línea directa entre los presidentes de Rusia y de Estados Unidos.

La primera máquina criptográfica es el disco de cifras(48), inventado en el siglo XV por el arquitecto italiano León Alberti, uno de los padres de la cifra poli alfabética, puede ser considerado un modificador que toma cada letra de texto llano y lo transforma en otra cosa. El modo de operación descrito hasta ahora es sencillo, y la cifra resultante es muy fácil de descifrar, pero dicho disco puede ser utilizado de manera más compleja. Alberti sugirió cambiar la posición del disco durante el mensaje, lo que de hecho genera una cifra poli-alfabética en vez de mono-alfabética.



El disco de cifras acelera la codificación y reduce los errores comparado con realizar la codificación mediante el cuadro Vigenère.

La característica principal, resultante al utilizar el disco de cifras de esta forma, es el hecho de que el disco cambia su modo de cifrar durante la codificación, y aunque este nivel extra de complicación hace que la cifra sea más difícil de descifrar, no la convierte en indescifrable, ya que se trata simplemente de una versión mecanizada de la cifra Vigenère, la cual ya fue desentrañada por Babbage y Kasiski. No obstante, quinientos años después de Alberti, una reencarnación más compleja de su disco de cifras conduciría a una nueva generación de cifras, una índole de magnitud más difícil de descifrar que nada de lo usado previamente.

En 1918 el inventor alemán Arthur Scherbius y su íntimo amigo Richard Ritter fundaron la compañía "Scherbius y Ritter", una innovadora empresa de ingeniería. Entre sus proyectos se encontraba uno consistente en sustituir el lápiz y papel de los inadecuados sistemas de criptografía empleados en la primera guerra mundial por una forma de codificación que sacará partido de la tecnología del siglo XX, es decir,

(48) Explicado en el capítulo 3.4 de cifrados poli-alfabéticos

desarrolló una maquinaria criptográfica que era esencialmente una versión eléctrica del disco de cifras de Alberti. Dicho invento, denominado "Enigma", muy empleada durante la segunda Guerra Mundial, se convertiría en el más temible sistema de codificación de la Historia.

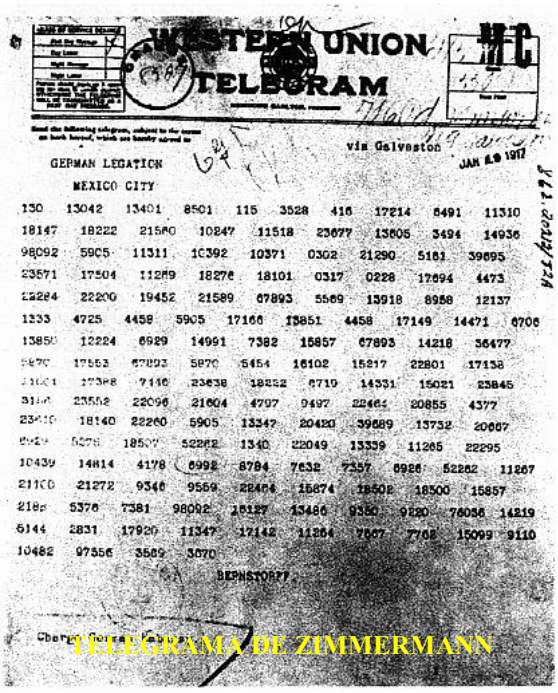
Criptografía primera mitad del siglo XX: Guerras Mundiales

5) Criptografía en la primera Guerra Mundial

Durante aquellos tiempos tan convulsivos, las naciones en Europa disponían de cables telegráficos transatlánticos para, mediante los mismos, establecer sus comunicaciones con otros países al otro lado del océano Atlántico. Los especialistas ingleses, sin embargo, habían logrado inutilizar desde el inicio de la guerra dichas comunicaciones. Por ello el ministro de asuntos exteriores germano, Zimmermann, no tenía mas remedio que utilizar una solución "puente", es decir, enviaba los mensajes a países neutrales, con los que previamente había establecido un acuerdo, cual es el caso de Suecia y el propio Estados Unidos (contra el que más tarde iba a conspirar) y de allí, los envíos se realizaban a las embajadas americanas que determinaba Alemania.

En 1917, el embajador de Alemania en Washington, Johann Von Bernstorff, recibió un telegrama de Zimmermann, en el que se podían leer una serie de instrucciones para la delegación germana en México. Para garantizar que el envío iba a llegara a su destinatario, lo hizo por duplicado, siendo el otro país receptor del mensaje, Suecia. Al tercer día de la recepción del mensaje original Bernstorff, hizo lo propio con su homónimo en México.

La diplomacia alemana usaba una serie de codificaciones para este menester y ello permitía que los mensajes llegaran cifrados a su destinatario. Estos códigos no eran sino una amplísima variedad de cifras. El telegrama enviado de Berlín a Washington iba cifrado según el código que se podía identificar con el número 0075. El enviado por el embajador alemán en Washington al de México por el código 13042. ¿Por qué se cambió el código de un país al otro? Sencillamente, porque la embajada de Alemania en México no utilizaba el código 0075.



El **Telegrama Zimmermann** [49] tal y como fue enviado por el embajador alemán en Washington al embajador en México. Cada palabra cifrada fue enviada en un grupo de cuatro o cinco números, usando un libro de códigos.

El mensaje Zimmermann proponía la alianza entre México y Alemania. El gobierno germano intentaría, permanecer neutral con Estados Unidos, pero si esto fallaba, se sugería al gobierno mexicano, su unión a la causa alemana, sin reservas, atacando a los Estados Unidos. Alemania se comprometía a ofrecer asistencia económica y a devolverle a México los territorios de Texas, Nuevo México y Arizona, que México había perdido en la Guerra México-Estados Unidos debido a los Tratados de Guadalupe-Hidalgo en 1848.

Por otra parte, tanto el cable de Estados Unidos como el de Suecia, estaban intervenidos, ya que ambos discurrían por el Reino Unido. Una vez que los ingleses hubieron obtenido los dos mensajes alemanes, dirigidos a Suecia y Estados Unidos, los enviaron a un órgano de análisis criptográfico, la llamada Sala 40[50]. Allí, los criptoanalistas Montgomery y Gray se pusieron a la tarea de descifrar los mensajes, determinaron que era el 0075 y que había sido puesto en servicio 6 meses antes, pero sólo pudieron recuperar el mensaje parcialmente, debido a su novedad. Lo que si lograron averiguar era quién iba a ser el destinatario final del mensaje, la embajada alemana en México. Como ambos expertos sabían que en México no utilizaban el código 0075, dedujeron que Bernstoff había enviado otro código. Recuperaron una transcripción

(49) http://es.wikipedia.org/wiki/Telegrama_Zimmermann
(50)Agencia de cifras del Ministerio de Marina británico durante la primera guerra mundial. Llamada así por la oficina en que se alojaba inicialmente.

del envío desde Estados Unidos y ahí fue donde pudieron descifrar por completo el mensaje.

El telegrama fue publicado en los periódicos estadounidenses. Al principio, mucha gente dudo de la veracidad del mismo. Muchos pensaban que era una argucia del servicio secreto inglés para arrastrar al coloso americano a la guerra, naturalmente en su favor, pero el propio Zimmermann admitió que él mismo lo había cursado. El presidente Wilson llevó al Congreso de su país, una declaración de guerra contra Alemania.

El grave problema del telegrama fue, desde un principio un sistema erróneo de cifrado, es decir, el fallo es utilizar libros de código. En principio, el sistema puede ser correcto si se mantiene en secreto este libro, basándose en el elevado número de sustituciones que suele catalogar. Lo malo es que los usuarios sólo usan un número bastante reducido, ya que el lenguaje que debe usar es muy restringido. De este modo, al llevar a la práctica el libro de códigos, se reduce todo a un nomenclátor, como los que se utilizaban antiguamente. Además dado que los criptoanalistas poseen mucho texto cifrado con el mismo código, esto es suficiente para traducir al idioma común unos pocos cientos de palabras diferentes que suelen ser utilizadas. Así fueron recuperados en la 40 los códigos involucrados en el telegrama en cuestión. Nunca dispusieron de un ejemplar de tales libros.

También fue seleccionado este método, código de libros, por la armada alemana para sus comunicaciones ya que suponían que, al igual que sus colegas de otro ejércitos, esta era una forma segura al no disponer nadie de sus códigos. Solamente tardaron un mes los expertos británicos en obtener la traducción. El llamada código Magdeburgo, constaba de palabras de cuatro letras en las que primera y cercera eran consonantes y las otras dos vocales (de esa forma se podía pronunciar cada palabra del código). Además, los alemanes después de codificar mediante este sistema los textos, los cifraban con lo que creían acrecentar la seguridad. Para ello se realizaba una sustitución mono alfabética, reemplazando las vocales por vocales y las consonantes por consonantes (el texto seguía pudiéndose pronunciar). Una vez sabido esto, el criptoanalista podía averigua la clave de la sustitución viendo que algunas palabras del código presentaban mayor frecuencia que otra en virtud del contexto de aquello que se pretendía enviar, es decir del mensaje. Otra

herramienta que facilitaba la tarea, era el diseño del código, repitiendo esta tarea cada vez que se cambiaba la clave, cada tres meses cuando la guerra comenzó y acortándose cada vez más hasta llegar a hacerlo cada media noche en 1916.

El mismo código era empleado en naves de superficie y en submarinos, pero el método de cifrado ulterior, era una transposición de columnas. La clave se cambiaba con muy escasa frecuencia y también, en este caso, los británicos accedieron a las instrucciones dadas a los submarinos alemanes, ya que disponían de los códigos.

Estos códigos mencionados no fueron los únicos descifrados por los ingleses que, al final de la guerra, reconocieron haber traducido unos quince mil mensajes.

En cuanto los ingleses, la Royal Navy también uso códigos para proteger sus comunicaciones radiotelegráficas. Sus libros contenían una gran variedad de palabras y grupos de ellas codificadas con números de cinco dígitos, incluyendo muchos homófonos. Pero lo que más llama la atención es el empleo de polífonos: un mismo número de código puede tener distintos significados (tres, en los códigos ingleses). Para distinguir un polífono de otro que no lo fuese, al polífono se anteponían y posponían las letras A, B y C, mientras que al otro código solo se posponían.

Por ejemplo el descifrado correcto del mensaje:

13901 01581 47869

con el código

A 01581 B Municionamiento

B 01581 A 4 de julio

C 01581 B Alemán

- 13901 C Visto

A 47689 B Príncipe de Gales

B 47689 C Crucero

C 47689 A Miércoles

es: Visto Crucero Alemán

La armada inglesa no cifraba el código resultante, ya que toda la seguridad estaba basada en las características de sus libros de códigos, que están entre los mas complejos que se hayan escrito jamás. Los alemanes no penetraron nunca en este lenguaje, al menos hasta 1916, cuando crearon un servicio de interceptación.

De todos los criptoanlistas de los tiempos de la guerra, los franceses fueron los más eficaces. De la misma manera que los ingleses de la habitación 40 pudieron descifrar los códigos alemanes en el terreno de la diplomacia y la armada alemanas, los franceses de Le Bureau du Chiffre hicieron lo propio con los códigos empleados por los ejércitos de tierra alemanes. Este organismo creado a finales del XIX, contaba al comenzar la primera Gran Guerra con un equipo de criptoanalistas formados con el curso de La Cryptographie Militaire de Auguste Kerchoffs (siendo sus escritos los que proporcionaron, a los franceses, una guía excepcional de los principios del criptoanálisis). Fue precisamente en este clima de guerra, cuando el holandés, que paso la mayor parte de su vida en Francia, Kerckhoffs que también había creado y desarrollado una red de escuchas radiotelegráficas, por todo el territorio galo. Por ello, no es de extrañar que, antes de replegarse, los franceses tuviesen instrucciones de inutilizar completamente las líneas telegráficas. De esta manera se forzaba al ejército alemán a emplear la radio, siendo estos mensajes capturados y posteriormente analizados criptográficamente. El plan fue un éxito

La vigilancia de los franceses contrastaba fuertemente con la actitud de los alemanes, que entraron en guerra sin contar con una oficina criptográfica militar. Cada nueva cifra ideada volvía temporalmente impotentes a los criptoanalistas, pero la inteligencia francesa, incluso si el mensaje era indescifrable, proporcionaba información del mismo mediante el análisis de tráfico [51], cosa muy valiosa ante nuevas cifras.

Al iniciarse la guerra, el ejército de tierra alemán utilizaba una cifra de campo que se denominaba "ÜBCHI", y era una doble transposición de columnas. La única solución para resolver aquel sistema y en ese periodo de tiempo, era el de los múltiples anagramas, que funciona con cualquier cifrado por transposición, pero necesita dos o más criptogramas cifrados con la misma clave y de la misma longitud, lo cual implica un

(51)Procedimiento de seguimiento de mensajes empleado por la vigilancia francesa para deducir potencialmente el destino y origen del mismo.

proceso muy lento, aunque con paciencia se van recuperando los textos en claro; el siguiente paso es descubrir la clave haciendo uso de dicho textos claros

Los expertos alemanes variaban la clave cada diez o quince días, que es un tiempo demasiado largo para el tráfico de mensajes existentes. Como, por otra parte, la mayoría de los textos contenían mensajes que se aproximaban a las cien letras, no era difícil encontrar dos de ellos con la misma longitud. A finales de 1914, los alemanes introdujeron un nuevo método de cifrado, tras el anuncio aparecido en la prensa francesa, bastante indiscreto, de que los mensajes germanos estaban siendo descifrados.

Sin embargo, el nuevo sistema de cifrado era peor que el anterior. Consistía en un cifrado Vigenère con clave ABC, seguido de una transposición de columnas. El nuevo método fue llamado por los franceses ABC. Tan sólo un mes mas tarde, se ideo un método para criptoanalizarlo a partir del texto cifrado únicamente. ABC estuvo en vigor hasta mayo del año siguiente. En ese momento la guerra se volvió estática y se caracterizó por el uso de trincheras, por lo que no había apenas movimientos de tropas. Con ello se redujo considerablemente el número de mensajes enviados, dándose el caso de que algunos se enviaban claros.

Más tarde siguió la cifra ABCD, algo más prolija. Primero se cifraba el texto en claro, utilizando el sistema Vigenère con clave abcd pero de forma intermitente, y a continuación se procedía a transponer las columnas. . La clave de dicha transposición gobernaba también las intermitencias en el cifrado Vigenère previo. Tan sólo tardaron los franceses dos semanas en romper este nuevo cifrado, que dejo de ser utilizado por lo alemanes en abril de 1916.

Una serie de cifrados poli alfabéticos reemplazaró este sistema. Pero eran tan poco eficaces que con frecuencia confundían tanto a los cifradores como a los descifradores. Se abandonó y regreso al modelos por transposición. Esta vez, los alemanes emplearon rejillas giratorias, una cada semana, que tampoco pudieron burlar a los criptoanalistas franceses. Después, el ejercito alemán recurrió a los códigos.

Durante este tiempo los ingleses utilizaron su cifra Playfair, empleándola en todos los frentes. Sus aliados franceses, hicieron uso de una cifra basada en las transposiciones de columnas, pero con una curiosa variante: antes de escribir secuencialmente las

verticales, se escriben algunas diagonales que parte de ciertas letras de la primera fila y cuya especificación exacta forma también parte de la clave

De esta forma, el texto cifrado comienza con las diagonales especificadas, primero las que parten hacia la derecha, después las que toman como sentido la izquierda, respetando su orden numérico. Tras las diagonales, van las columnas, según el orden prefijado por la clave.

¿Por qué se utilizaban las diagonales? Sencillamente para romper la uniformidad en las longitudes de las columnas, hecho en que se basa el criptoanálisis de las transposiciones de columnas. Pese a lo que se pudiera pensar, este sistema no añade una cuota de seguridad a la doble transposición de columnas que utilizaban los alemanes cuando la guerra estalló (su cifra ÜBCHI). Tampoco lo es el famoso Playfair británico. Sin embargo, tanto el método francés como el inglés no fueron interpretados por los alemanes hasta que pasaron tres años desde el inicio de la guerra, que fue cuando Alemania (1916) creó su propia oficina de criptoanálisis, la Abhorchdienst y, lógicamente, desarboló los códigos de los aliados.

Con los ejércitos inmovilizados en sus refugios subterráneos, el medio de comunicación ideal se convirtió en el teléfono. . Pero en el frente, el enemigo intervenía los cables telefónicos. Como consecuencia de esta intervención, los aliados no tuvieron más remedio que cifrar sus conversaciones, mediante unos códigos especiales que se llamaron "códigos de trinchera".

Eran cuadernos pequeños en los que estaban escritos unos pocos cientos de palabras codificadas con dos o tres letras. Dichos vocablos eran frecuentes en las comunicaciones militares, con un significado esencial para que el mensaje pudiera ser entendido con claridad. Se hallaban agrupados por categorías como infantería, artillería, números, lugares, verbos, etc. Cuando una orden militar era cursada por teléfono, las palabras clave se reemplazaban por su homólogo código con lo que el enemigo no entendía nada del mensaje. Sin embargo, estos códigos presentaban un problema y es que podían caer con mucha facilidad en manos del enemigo, al encontrarse muy cerca de sus líneas. Por este motivo los códigos de trinchera, se cambiaban con relativa frecuencia. Los primeros fueron diseñados por los franceses a comienzos del año 1916 y pronto se sumaron a ellos

los británicos, tras experiencias terribles, e incluso los americanos cuando llegaron a Europa a principios de 1917.

Los códigos de trinchera, solamente eran útiles a la finalidad para la que habían sido diseñados, es decir, no eran eficaces en las comunicaciones radiotelegrafiadas. Los británicos, tras constatar que los criptoanalistas germanos había roto sus cifras, emplearon a partir de 1916 códigos con un repertorio de varios miles de palabras y cifrando mas tarde, para dar mayor seguridad al mensaje. Aún así, el servicio de analistas germanos penetró en numerosas ocasiones en tales comunicados. De nuevo, fue obligado cambiar los códigos con cierta frecuencia, para evitar que cayeran en poder del enemigo. En el caso americano, el más diligente, se modificaban cada mes. Y ya al final de la guerra utilizaron un código que no necesitaba ser escrito en ningún libro: el lenguaje nativo de los indios Choctaw, que formaba parte del ejército americano en el viejo continente. Ello no obedeció a ninguna estrategia criptográfica premeditada, sino que fue algo improvisado. Durante la segunda Guerra Mundial, los americanos volvieron a utilizar este sistema a través de sus soldados aborígenes, en su lucha contra los japoneses. En esta ocasión, se emplearía la lengua navaja.

En la primavera de 1918, el jefe del estado mayor germano, Erich Von Ludendorff, había preparado en secreto una gran ofensiva.

Como era evidente, el factor sorpresa sería irrelevante si los aliados interceptaban las comunicaciones alemanas previas al gran ataque. Para evitarlo, el mando alemán renunció al empleo de códigos y se decidió por las cifras de campo. En esta ocasión se escogió una nueva, de entre varias candidatas. Una que los propios criptoanalistas alemanes no pudieron descifrar. Estudios posteriores demuestran que fue la cifra de campo mas segura que jamás se emplearía en la primera gran guerra. La llamaron GEDEFU 18 o cifrado ADFGX, diseñada por el coronel Fritz Nebel.

En el cifrado ADFGX [52] se comienza disponiendo las letras en un cuadrado de 25 casillas, según el orden que indique la clave. Las cinco filas y columnas de este cuadrado no van numeradas del uno al cinco, sino que en su lugar se emplearon las letras A, D, F, G, X (de ahí el nombre del cifrado). Por ejemplo:

(52) introducida el 5 marzo de 1918, justo antes de la gran ofensiva alemana del 21 de marzo, la cual será desarrollara en el capitulo correspondiente

	A	D	F	G	X
A	f	r	i	t	z
D	n	e	b	l	a
F	c	d	g	h	k
G	m	o	p	q	s
X	u	v	w	x	y

En este ejemplo la letra "a", tiene coordenada DX y así sucesivamente. La razón de utilizar las letras A, D, F, G y X en lugar de números del uno al cinco tiene que ver con el empleo del código Morse, ya que en dicho código, los números tienen una representación parecida, pero la de las letras anteriores es suficientemente distinta y permite corregir los errores de la transmisión. De esta manera, el código Morse de tales letras se muestra a continuación: **A: ._ D: _ . . F: .._ G: _ _ . X: _ . ._**

Para cifrar, cada letra del texto en claro se sustituye por su par de coordenadas. Supongamos que deseamos cifrar el texto claro "Se necesitan municiones":

S E N E C E S I T A N M U N I C I O N E S

GX DD DA DD FA DD GX AF AG DX DA GA XA DA AF FA AF GD DA DD GX

La secuencia obtenida no es el texto cifrado, sino que antes hay que someterla a una transposición de columnas con otra clave que, por ejemplo, puede ser la "Ludendorff", formando primero el correspondiente rectángulo:

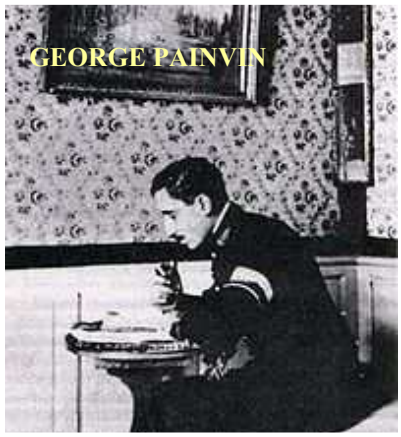
L	U	D	E	N	D	O	R	F	F
6	10	1	3	7	2	8	9	4	5
G	X	D	D	D	A	D	D	F	A
D	D	G	X	A	F	A	G	D	X
D	A	G	A	X	A	D	A	A	F
F	A	A	F	G	D	D	A	D	D
G	X								

y a continuación las columnas son colocadas secuencialmente en el orden que determina la clave:

DGGA AFAD DXAF FDAD AXFD GDDFG DAXG DADD DGAA XDAAX.

Siendo esto último el resultado final, es decir, el texto cifrado, teniendo en cuenta que en la realidad no llevaría espacios en blanco, lo cual lógicamente ayudaría al criptoanalista a desentrañar la clave. Los alemanes comenzaron a utilizar este método en 1918. Al ver esto los franceses, decidieron enviar estos mensajes a su mejor criptoanalista, Georges Painvin que comprobó que la presencia de exactamente cinco letras distintas en los criptogramas, concluía que se trataba de un cifrado tomográfico en el que cada letra del alfabeto en claro se debía reemplazar por una de las veinticinco parejas que pueden formarse con las cinco letras distintas. Tras varios días de un trabajo agotador, la única nueva conclusión que obtuvo fue que los germanos cambiaban la clave a diario, ya que así lo indicaba la frecuencia de las letras.

La ofensiva comenzó y también comenzaron a prodigarse, en gran medida, los mensajes alemanes, siendo dos de ellos los que llamaron la atención del criptógrafo francés.



Painvin observó que en cada cinco o seis letras había dos o más coincidentes, siendo esto totalmente lógico, puesto que es lo que sucede cuando ciframos mediante transposición de columnas dos textos con una misma cabecera. Al formar con los textos el rectángulo correspondiente y después escribir secuencialmente las columnas, la coincidencia de los mensajes se traslada a las primeras letras de las columnas. Consecuentemente, Painvin había logrado descubrir el método de cifrado que seguía a la sustitución tomográfica, usan transposición de columnas en cada texto. El francés ya tenía identificadas las columnas, lo cual supone la parte mas compleja del criptoanálisis de una transposición de columnas ya que lo que queda después se relativamente sencillo,

colocar las columnas en su orden correcto, para lo que se emplean los bigramas y trigramas mas frecuentes del idioma empleado.

Sin embargo, en este caso la sustitución tomográfica previa, imposibilita esta técnica. Lo primero que hizo el galo fue no darse por vencido fijándose en el número de letras de los mensajes. Las columnas con más letras son las situadas a la izquierda en el rectángulo que ha de formarse para efectuar la transposición. Sus números son entonces los primeros en el orden que determina la clave, aunque no en ese orden necesariamente. Y finalmente, las restantes columnas deben situarse a la derecha del rectángulo. Paivin ya tenía una primera aproximación al orden de las columnas determinado por la clave, siendo esa información toda la que podía ser extraída e insuficiente para recuperar la clave. Por fortuna, entre los demás mensajes recuperados ese día, también había dos de ellos con un final común, coincidencia que permitía identificar sus columnas. El genio del francés fue mas allá, al considerar el resto de los mensajes del mismo día, localizando en cada uno de ellos columnas, de ahí formó pares de letras, realizando un análisis de frecuencias que confirmaba que Painvin iba por el buen camino. Comprendió que como la longitud de la clave era par, dos claves distintas daban lugar al mismo cifrado, lo cual significa que, fijada una de ellas, la otra se obtiene cambiando filas por columnas en el cuadrado 5X5 que determina la sustitución tomográfica de la primera fase del cifrado y, después reemplazando las letras en lugar impar por sus consecutivas par en la clave que gobierna la transposición de columnas. Consecuentemente, bastaba con recuperar una de ellas.

El análisis de frecuencias que Painvin efectuó con unas columnas le hizo notar que aquellas situadas en lugares impares, presentaban frecuencias similares de cada una de las letras A, D, F, G y X, pero diferentes de las columnas que eran colocadas en lugar par, lo cual permitió descubrir la paridad del resto de las columnas, siendo el paso siguiente emparejar cada columna impar con su consecutiva par. Las frecuencias de los pares de letras que resultan en cada una de las dos asociaciones candidatas determinarán cuál es la correcta, es decir, aquella que más se parezca a la distribución de frecuencias del alemán. La parte difícil del criptoanálisis ya estaba hecha. El resto era sólo cuestión de paciencia y tiempo. Y por fin, el 26 de abril, Painvin, concluyó este criptoanálisis que había iniciado tres semanas antes.

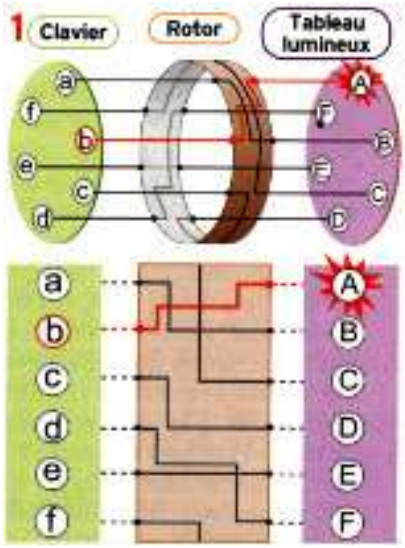
De repente, el 1 de junio los mensajes ADFGX incorporaron una sexta letra, la "V", lo cual implicaba que los alemanes habían diseñado otro cuadrado, esta vez, de 6X 6 con el fin de incluir los dígitos del 0 al 9. Naturalmente esto no fue comunicado al criptoanalista francés, aunque lo sospechó rápidamente y, al día siguiente de sus sospechas, ya había descifrado los mensajes cifrados con el nuevo modelo; además en aquellas fechas, eran inminentes ataques germanos que, de triunfar, pondrían Paris en manos del enemigo. Los mensajes descifrados revelaron que dichos ataques iban a tener lugar sobre la línea francesa entre Montdidier y Compiègne. En efecto, el 9 de junio quince divisiones alemanas se lanzaron sobre un ejército francés que les estaba esperando, con lo cual fueron aniquiladas. Muy pocas veces más contaron los aliados con la ventaja de conocer los planes del enemigo. De hecho, los franceses sólo recuperaron diez claves ADFGVX alemanas durante toda la guerra. Painvin no logró encontrar una solución general para esta cifra alemana.

La primera Guerra Mundial, marcó un punto de inflexión en la historia de la criptografía militar, ya que antes de que sobreviniera, únicamente el ejército francés contaba con oficiales especialistas en códigos y cifras y después de que pasara, todos los ejércitos crearon unidades especializadas en Criptografía. Por otra parte, en la lucha que mantuvieron diseñadores de cifras y códigos con sus adversarios criptoanalistas es clara la victoria de estos últimos. A pesar de la gran variedad de códigos y cifras que se emplearon, el triunfo de los criptoanalistas fue contundente, pero no hay que olvidar que contaron con un par de ayudas inestimables: la primera, la gran cantidad de texto que proveían las interceptaciones telegráficas y, sobre todo, la radio, la segunda, mas importante, la falta de una seria instrucción criptográfica en las personas que manejaban la información encriptada. Pero a pesar de tan humillante derrota, los creadores de cifras no se desanimaron, volviendo una y otra vez a la lucha y esta vez no sólo armados con papel y lápiz, sino también con máquinas electromecánicas.

6) Criptografía en la segunda Guerra Mundial, el descifrado del Enigma y la barrera del idioma

La segunda Gran Guerra no tendrá sólo, un gran tránsito de comunicaciones, sino también que dichas transmisiones se harán de formas más sofisticadas, siendo las comunicaciones basadas en el teléfono y la radio ya habituales en todos los ejércitos. La Guerra Civil Española será el banco de pruebas de muchos criptosistemas y durante la

Gran Guerra se inventa la mayor máquina criptográfica hasta entonces conocida, la máquina Enigma, que fue ofrecida al gobierno alemán por sus fabricantes: Arthur Scherbius y Richard Ritter que la patentaron en 1918. Esta máquina consiste básicamente en un teclado similar al de la máquina de escribir, resultando que al pulsar cada letra, aparece otra en una consola y que simultáneamente, y según las versiones, se va escribiendo en una tira de papel que va saliendo por un lateral.



Vista interior de la Enigma

El funcionamiento no se diferencia mucho del codeógrafo de Alberti, pero en versión eléctrica, ya que al pulsar una tecla, la corriente eléctrica entra en una pieza cilíndrica por la base, que está dividida en 26 sectores, uno por cada letra. En el interior del cilindro un entramado de cables la desvía para salir por la otra base que también está dividida en 26 sectores, uno por cada letra, saliendo la corriente por una letra cualquiera, diferente de la inicial. Esta pieza cilíndrica es fundamental para la misión de la Enigma y su nombre es "el modificador" que, si permanece estático, da como resultado una sustitución mono alfabética, dependiendo únicamente del cableado del modificador y de la posición en que está colocado (26 posibilidades). Pero la Enigma tenía varias características para hacerla inexpugnable: en primer lugar, el modificador a cada pulsación de la tecla tenía acoplado un motor y giraba un poco, hasta la siguiente letra, para hacer la siguiente sustitución no con el mismo alfabeto sino con otro, consecuentemente la sustitución se hacía poli alfabética.

La segunda característica era que no sólo tenía un modificador, sino tres, en su versión normal, cinco para mensajes entre la inteligencia alemana y hasta diez en la que se codificaban los mensajes del propio Hitler. Y una tercera característica para añadir seguridades que los modificadores eran extraíbles e intercambiables. Además de esta cota de seguridad, los inventores añadieron un nuevo dispositivo, el clavijero que consiste en 26 clavijas, una por cada letra, dispuestas en dos filas, de tal amera que si dos clavijas se unían mediante un cable, la máquina automáticamente permutaba una letra por otra en todos sus mensajes, admitiendo la máquina hasta un máximo de seis cables uniendo doce letras. Además para poder descodificar con la misma máquina, se añadió una pieza nueva llamada "el reflector" que estaba colocada detrás de los modificadores y que hacía que escribiendo los mensajes codificados, fuera la electricidad en sentido contrario a través de los modificadores y el mensaje a pareciera descodificado.

La rotación del modificador es la característica más importante del diseño Scherbius. Sin embargo, la máquina tiene una debilidad obvia: teclear una misma letra seis veces hará que el modificador vuelva a su posición original y teclear una misma letra una y otra vez repetirá el mismo patrón de codificación

En general, los criptógrafos se han mostrado deseosos de evitar la repetición, porque conduce a la regularidad y la estructura en el texto cifrado, que son los síntomas de una cifra débil. No obstante, dicho problema se puede mitigar introduciendo un segundo disco modificador, ya el patrón de codificación no se repite hasta que el segundo modificador vuelve a estar como al principio, lo que requiere seis revoluciones completas del primer modificador, o la codificación de 6 x 6, es decir, de 36 letras en total. Dicho de otro modo, hay 36 disposiciones de los modificadores distintas, lo que equivales a cambiar entre 36 alfabetos cifrados, que con un alfabeto de 26 letras, la máquina de cifras cambiaría entre 26 x 26, es decir, 676 alfabetos cifrados. De modo que combinando los modificadores, a veces también llamados rotores, es posible construir una máquina de codificación que cambia continuamente entre diferentes alfabetos cifrados. Además, todo esto se lleva a cabo con gran eficiencia y exactitud, gracias al movimiento automático de los modificadores y a la velocidad de la electricidad.

Normalmente puede considerarse a la máquina Enigma desde el punto de vista de un sistema general de cifras, y las posiciones iniciales son lo que determina los detalles

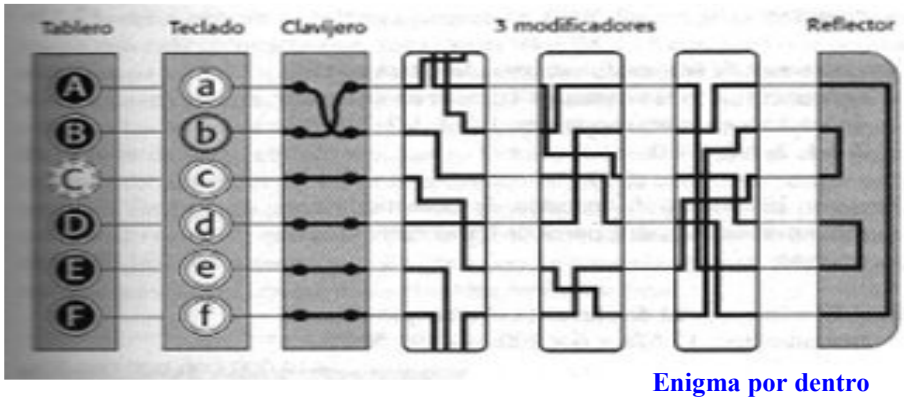
exactos de la codificación, es decir, las posiciones iniciales determinan la clave. Generalmente, las posiciones iniciales vienen dictadas por un libro de códigos, que enumera la clave para cada día y que se encuentra disponible para todos los que forman parte de la red de comunicaciones. No hay que olvidar que distribuirle libro de códigos es una labor que requiere tiempo y esfuerzo, pero como sólo se necesita una clave para cada día, podría paliarse este contratiempo, acordando enviar un libro de códigos que contenga 28 claves una vez cada cuatro semanas.

Para descifrar el mensaje, es necesario que el receptor disponga de otra máquina Enigma y una copia del libro de códigos que contenga la posición inicial de los modificadores para ese día. Obviamente nunca debe permitirse que la clave y el libro de códigos que la contienen caigan en manos ajenas a la red de comunicación, ya que sin el libro de códigos es necesario probar todas las claves para intentar descifrar el mensaje.

En poco tiempo Scherbius decidió mejorar la seguridad de su invento aumentando el número de disposiciones iniciales y, de esta forma, el número de claves posibles. Se podría haber aumentado la seguridad añadiendo más modificadores, ya que cada nuevo modificador aumenta el número de claves con un factor de 26, pero esto también aumentaría el tamaño de la máquina. Por eso, para evitar este contratiempo, añadió dos nuevos rasgos:

■ Poder sacar los modificadores y que fueran intercambiables. Como la disposición exacta de los modificadores es crucial tanto para la codificación como para la descodificación, el que pueda disponerse de seis maneras diferentes los tres modificadores aumenta el número de claves o el número de posiciones iniciales posibles, con un factor de seis.

■ Insertar un clavijero entre el teclado y el primer modificador, el cual permite que el emisor inserte cables que tienen el efecto de intercambiar algunas de las letras antes de que entren en el modificador.

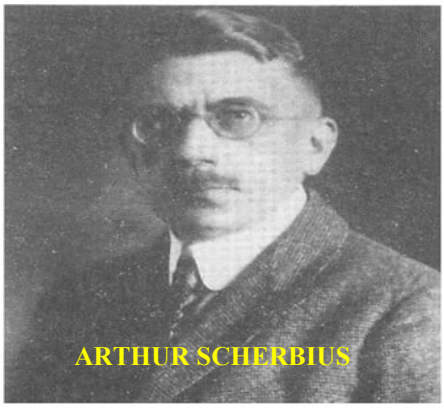


Enigma por dentro

De esta forma, el operador de la Enigma disponía de seis cables, lo que implica que se podían intercambiar seis pares de letras, dejando 14 letras sin conectar y sin modificar. Las letras intercambiadas por el clavijero forman parte de la disposición de la máquina, de modo que se deben especificar en el libro de códigos. Mientras el emisor y el receptor estén de acuerdo sobre la posición de los cables del clavijero, el orden de los modificadores y sus respectivas orientaciones, todo lo cual lo especifica la clave, podrán codificar y descodificar mensajes muy fácilmente. Sin embargo, un interceptor ajeno que no conozca la clave tendrá que probar cada una de las 10.000.000.000.000.000 claves posibles para descifrar el texto, algo que está totalmente fuer del alcance de cualquier criptoanalista.

En definitiva, combinando los modificadores con el clavijero, Scherbius protegió su máquina contra el análisis de frecuencia y al mismo tiempo la dotó de un número enorme de claves posibles.

Scherbius creía que la Enigma era inexpugnable y que su fortaleza criptográfica crearía una gran demanda. Ofreció la máquina de cifras tanto al ejercito como al mundo de los negocios, proporcionando diferentes versiones para cada mercado. Sin embargo, el elevado coste de la máquina desalentó a los compradores potenciales. Aunque, también es verdad, que el ejercito alemán estaba lo suficientemente asustado como para apreciar el valor de la máquina Enigma, gracias a dos documentos británicos: "The World Crisis"[53] ("La



(53) http://www.cripto.es/Enigma/boletin_Enigma_16.htm y http://www.kirjasto.sci.fi/churchil.htm

crisis mundial") de Winston Churchill, publicado en 1923, incluía un dramático relato de cómo los británicos habían obtenido valioso material criptográfico alemán. Igualmente en 1923, la Marina Real británica publicó su historia oficial de la primera guerra mundial, que reiteraba el hecho de que la interceptación y el criptoanálisis de las comunicaciones alemanas habían dado una clara ventaja a los aliados. El ejército alemán inició una investigación sobre como evitar los fiascos criptográficos de la primera guerra mundial y concluyó que la máquina Enigma ofrecía la mejor solución. Así pues, en 1925 Scherbius comenzó la fabricación en serie de Enigmas, que entraron al servicio del ejercito alemán al año siguiente, y que posteriormente fueron utilizadas por organizaciones gubernamentales y estatales como, por ejemplo, los ferrocarriles. El invento de Scherbius proporcionó al ejército alemán el sistema de criptografía más seguro del mundo y al estallar la segunda guerra mundial sus comunicaciones estaban protegidas por un nivel de codificación sin precedentes. A veces, pareció que la máquina Enigma tendría un papel vital para conseguir la victoria nazi, pero, en vez de ello, al final formo parte de la perdición de Hitler. El inventor no vivió lo suficiente para ver los éxitos y los fracasos de su máquina de cifras.

La clave de la Enigma consistía en tres letras que conocían emisor y receptor y que hacían mención a las posiciones iniciales de los tres modificadores, y ese fue, precisamente, uno de sus puntos flacos, la clave y su distribución por un ejército muy extendido geográficamente.. De manera casi simultánea a la Enigma, otros fabricantes construyeron máquinas similares en Holanda (Alexander Koch), Suecia (Arvid Damm) y Estados Unidos (Edward Hebern), pero eran muy costosas, en cuanto a su proceso de fabricación y sólo pudieron venderse unas cuantas. Sin embargo, el gobierno alemán tenía otros planes de futuro al darse cuenta de los desastres cometidos durante la primera Guerra Mundial. Consideraron que la Enigma era inexpugnable y se comenzó la fabricación en serie, entrando en funcionamiento en 1926 y sorprendiendo desagradablemente a los criptoanalistas británicos de la sala 40, a los norteamericanos y a los franceses que no acertaban a comprender aquella cifra, intentando desenmarañar aquella máquina, pero sin éxito alguno. En esta época existía un país que no se podía permitir el lujo de que las comunicaciones alemanas fuesen fluidas: Polonia, que se acababa de formar como estado independiente y geográficamente se encontraba entre Alemania y al URSS, lo que propició que en aquella época tuviera una eficiente Caja Negra: el Biuro Szyfrow.

Este organismo estaba dirigido por el capitán Maksymilian Ciezki y venía de una guerra con la Unión Soviética, por lo que sus criptoanalistas se hallaban bien entrenados, ya que durante el año de guerra con URSS habían descifrado la nada despreciable cifra de cuatrocientos mensajes enemigos.

El órgano polaco, llegó incluso a comprar una Enigma alemana y destriparla para averiguar sus secretos, pero desgraciadamente sólo tuvieron acceso a la variedad civil, no a la militar. Como tampoco los criptoanalistas franceses fueron capaces de descifrar la Enigma, recurrieron a otros caminos, como el de fotografiar, por parte de un agente francés en 19131, dos documentos sobre la construcción de la Enigma, suministrados por un rencoroso oficial alemán expulsado del ejército germano, siendo estos documentos archivados por el servicio de espionaje francés que no los debió considerar vitales, pero que fueron remitidos a Polonia, gracias a un acuerdo entre ambos países. Gracias a ellos una réplica de la Enigma fue construida, en su versión militar, con lo cual comenzó el ataque al cifrado alemán.

El Biuro Szyfrow aprendió que cada principio de mes, el ejército alemán distribuida un nuevo libro de códigos, en el que venía escrito explícitamente lo que llamaban la clave del día. Y aprendieron también que el ejército alemán para añadir seguridad a su máquina, utilizaba lo que llamaban la clave de mensaje, la cual consistía en una posición inicial diferente de los modificadores para cada mensaje que se codificaba con la Enigma. Sabiendo la clave de día, cada soldado que emitía con la Enigma ponía el clavijero en posición, los modificadores en orden y la posición inicial de dichos modificadores; pero antes de empezar a emitir el mensaje, escribía tres letras cualesquiera, lo que constituía la clave de mensaje. Seguidamente el emisor movía los modificadores a esa posición recién inventada y ya emitía el mensaje. Con el fin de evitar errores, la clave de mensaje se repetía dos veces.

El receptor, tenía su máquina con la clave de día, recibía primero las seis letras que formaban la clave del mensaje, y cambiaba los modificadores a la posición indicada; de

tal forma que el mensaje que comenzaba a recibir tras las seis letras, podía ser descifrado con esa nueva posición.

La clave del mensaje tenía una gran fuerza, ya que era inventada por el emisor en ese instante y no figuraba escrita en ningún libro de claves. La Enigma parecía una máquina verdaderamente inexpugnable.

El Biuro Szyfrów organizó un curso de criptografía e invitó a veinte matemáticos, los cuales prestaron juramento de silencio. Todos ellos procedían de la universidad de Poznan, situada al oeste del país, y que a pesar de no tener mucho prestigio formó parte de Alemania hasta 1918, por lo que todos los matemáticos dominaban el alemán. De inmediato Marian Rejewski , con su trabajo en solitario, destacó en criptografía y está considerado como una de las mentes más lúcidas para la criptografía de todos los tiempos, ya que fue él quién con medios muy limitados descifró la máquina de criptografía más potente antes de la existencia del ordenador. Para lo cual, Rejewski se centro en lo poco que tenía, aunque la Enigma poseía clave de día y clave de mensaje, la clave de mensaje era independiente en cada mensaje, pero la clave de día era la misma durante todo el día y además con esa clave de día siempre se cifraban tres letras que se repetían dos veces. Rejewski sabía que la repetición era la perdición de cualquier cifra, por pequeña que fuera esa repetición. Cada día, tomaba esas seis primeras letras de todos los mensajes posibles; mirando la primera y la cuarta, sabía que una letra desconocida se convertía primero en cierta letra y después se convertía en otra. Así al terminar el día, aunque desconocía cual era la clave del día, si comprobaba que las claves de cada mensaje generaban relaciones.

Esto es lo que en matemáticas se llama una permutación [(54)], como el número total de permutaciones de un conjunto de n elementos viene dado por n!, Rejewski sabía que existía 26! permutaciones, o sea, 403.214.611.270.000.000.000.000.000 posibilidades diferentes, dependiendo de la clave del día.; pero también sabía que en toda permutación es fácil encontrar lo que se llama un ciclo con una longitud determinada. Además observó un detalle importantísimo, y es que esos ciclos no dependen de las posiciones

(54) permutación es una reordenación de un conjunto

del clavijero, con lo cual una tarea sobrehumana se había convertido en un problema que sólo era difícil.

El clavijero es la pieza que más posibilidades da a la Enigma, pero sólo sustituye seis letras por otras seis letras y por lo tanto es una simple sustitución mono alfabética de pocas letras, fácil de descifrar. Este largo y arduo trabajo llevado acabo por Rejewski está considerado como uno de los mayores logros de toda la historia de la criptografía, llego hasta tal punto su eficacia que contraatacó construyendo una máquina que tenía archivos cíclicos y longitudes de estos, de tal forma que probaba todas las posibles claves que podían tener en una máquina Enigma, de manera que sólo tecleando ciclos y longitudes, aquella máquina daba la clave de día de la Enigma, dicha máquina recibió el nombre de bomba. La bomba tenía adosada una Enigma, y así probaba candidatos a claves de las que cumplían la condición de número de ciclos y longitudes de ciclo hasta dar con la clave.

La máquina tenía seis partes, en total eran seis bombas cada una de ellas con una disposición de modificadores y simultáneamente se buscaba la clave de día. Con las bombas se podía encontrar la clave de día en unas dos horas. A las doce de la noche, cada día, el ejercito alemán cambiaba las claves de día. A esa hora, empezaba el trabajo de las bombas.

De todas formas todo es trabajo fue inútil, el jefe del Biuro Szyfrów, Guido Langer, sabía las claves con antelación, el espía francés que paso los planos de la Enigma, también estuvo pasando los libros de claves durante siete años de duro trabajo de Rejewski; pero nunca dijo nada, pretendía tener a su equipo en plena forma para cuando ya no dispusiera de las claves.

En 1938, el ejercito alemán empezó a dudar de la eficacia de sus comunicaciones con la Enigma y decidió aumentar el nivel de seguridad. Cada operador de la Enigma recibió dos nuevos modificadores, con lo que ya disponía de cinco modificadores para tres ranuras donde colocarlos. Además, el clavijero que unía doce letras para cambiar seis letras entre sí, paso a tener veinte, con lo que se tenían diez letras intercambiadas entre sí. Estos cambios en la Enigma hicieron que las posibilidades de cifras diferentes se multiplicaran por 2000. La bomba de Rejewski que constaba de seis máquinas

conectadas a seis Enigmas, ahora necesitaría conectar 60 máquinas, y las sustituciones que producía el clavijero, ahora serían más, casi de todo el alfabeto. Rejewski no tenía medios para continuar luchando, pero había demostrado a todas las potencias europeas que la Enigma no era indescifrable.

En 1939, el gobierno polaco preveía que su país sería invadido, para salvaguardar todo el trabajo de Rejewski, el jefe del Biuro Szyfrów, citó en Varsovia a los jefes de las Cajas Negras de Francia y Gran Bretaña, en donde fueron informados de todo. El 1 de septiembre de 1939, Hitler invade Polonia y comienza la segunda Guerra Mundial, pero el equipote descifradores de la Sala 40 del ejército británico, está preparado. La Sala 40 fue renovada casi en su totalidad, accedieron matemáticos que hasta entonces casi no había, su nombre fue cambiado por el de GC&CS(55), cambio su sede a Bletchley Park y al frente de la misma fue colocad Alastair Denniston. Casi inmediatamente los criptoanalistas de Bletchley Park, dominaron las técnicas polacas. Además inventaron las suyas propias, una de esas técnicas fue lo que se denominan los cillis. Ya se ha dicho que la clave de mensaje de la Enigma eran tres letras cualesquiera, lógicamente hay muchas posibilidades, pero en la práctica, es difícil elegir muchas veces seguidas tres letras al azar. No es raro imaginar que un operador que tiene que inventarse constantemente tres letras al azar, para cada uno de los mensajes que emita, al final, intenta que sean fáciles, de esta forma se pierde parte del azar y por consiguiente parte de la potencia de la Enigma. Es importante resaltar que los cillis no son fallos de la máquina sino fallos humanos.

Sin duda Alan Turing (1912-1954), último director de Bletchley Park fue su figura más destacada. Turing fue un matemático interesado sobre todo en lógica, encargado de la inteligencia militar británica, pero sobre todo es conocido por ser la primera persona que concibe los fundamentos teóricos de un extraño aparato llamado ordenador. En 1937 publicó el articulo: "On Computables Numbers", en el que sienta los cálculos matemáticos en términos de una máquina que con un protocolo adecuado pueda realizarlos. En dicho articulo define lo que llamo la Máquina de Turing, máquina diseñada para realizar un protocolo de actuación de forma rápida e infalible. Pero Turing

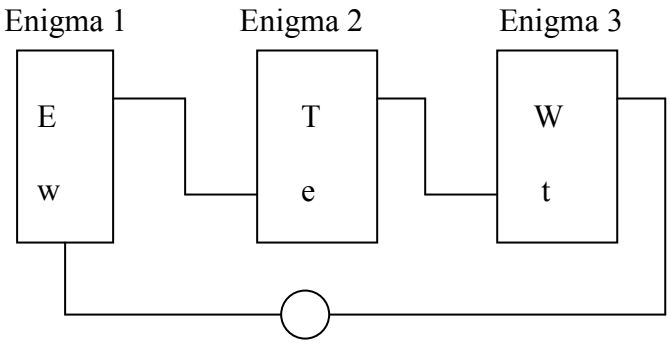
(55) Goverment Code and Chipre School

fue más allá, y define lo que llamó la Máquina Universal, una máquina capaz de diseñar y controlar los protocolos de actuación de las máquinas de Turing. La máquina Universal está considerada como el primer antecedente teórico del moderno ordenador. Por primera vez, se concibe la utilidad de una máquina programable. El articulo de Turing tuvo una gran influencia y dió lugar a una ciencia nueva, una ciencia basada en la posibilidad de que los cálculos puedan enseñarse a una máquina. Esta nueva disciplina certifica fue denominada "Computer Sciences", lo cual provocó la aparición de la palabra computer, en español computador, mientras que la nueva disciplina recibió el nombre de Informática y el aparato que realizaba dichas operaciones ordenador. La diferencia es importante, para unos es ordenar información, para otros realizar cálculos.

Para descifrar la Enigma, Turing aprovechó lo que en criptografía se denomina un puntal(56). Turing observó que todos los días a las 6,00 hrs, el ejército alemán emitía un mensaje y dedujo que era un informe meteorológico, por tanto en algún lado debía contener la palabra alemana que designa al tiempo atmosférico: wetter. Así pues, como sabía que gracias al reflector, la Enigma tenía la propiedad de que ninguna palabra quedaba invariable. Turing buscaba por el principio del mensaje, donde encajar wetter, ya que estas letras son muy frecuentes en alemán. Siempre tenía varias opciones, pero en casi todas ellas se encontraba lo que él llamaba un rizo, con esta palabra, Turing denominaba a una transformación, parecida a las estudiadas por Rejewski, de tal forma que si en una determinada posición de los modificadores, wetter se ha transformado en ETDWIK, se habrá producido un rizo: w se transforma en E, la e se transforma en T y la segunda t se transforma en W. Turing imaginó una Enigma con una determinada posición de modificadores, llamémosla P en la que w se transforma en E, otra Enigma en la que e se transforma en T, esta segunda Enigma, tendrá la misma posición P pero contados los modificadores desplazados una posición, a la que llamaremos la posición P+1, y finalmente, una tercera Enigma en la que t se transforma en W, esta Enigma tendrá la posición P+3. Las tres Enigmas, tendrán las misma posiciones pero desplazadas. Teniendo las tres Enigmas, para comprobar que están en condiciones bastará, poner un cable que salga de la E de la primera Enigma, y entré en la segunda

(56) Puntal es una palabra del texto original que es conocida.

Enigma en la e; un cable que salga de la T de la segunda y entré en la t de la tercera; finalmente, se coloca un cable que cierre el circuito con una bombilla para comprobar que se ha conseguido, dicho cable irá desde la w inicial hasta la W final.



Así si se mueven los modificadores automáticamente, sólo habrá que esperar a que la bombilla se encienda para encontrar la posición buscada. Además este circuito ignora al clavijero, tenga las posiciones que tenga, aparecerá la posición correcta.

Pero, evidentemente, esa palabra no era el único puntual que se podía conocer, por lo tanto unió cada una de las letras de salida de la primera Enigma con cada una de las letras de entrada de la segunda; y cada letra de salida de la segunda, con cada letra de entrada de la tercera; y posteriormente cerrar todos los circuitos añadiendo bombillas. El resultado fue una inmensa máquina repleta de bombillas a la que también llamó bomba, bastando en la bomba de Turing poner en la primera los modificadores en una posición, la segunda en la misma pero todas las posiciones desplazadas un lugar y la tercera con los modificadores dos lugares más desplazados, seguidamente, tuvo que esperar que se encendiera alguna bombilla, y como los modificadores cambiaban la posición cada minuto, se tardaba unas cinco horas en encontrar la clave.

Sin embargo, puede ocurrir que no se tuvieran los tres modificadores correctos de los cinco posibles, la solución fue tener sesenta bombas funcionando simultáneamente que cubrían todas las posibilidades; quedando aún el clavijero, que de nuevo se limitaba a una sustitución mono alfabética de alguna de las letras.

El conocer un puntual fue tan importante para la descodificación de la Enigma que en los días decisivos de la guerra, cuando no se conocía ninguna palabra del mensaje original, se optaba por una determinada posición de latitud y longitud, palabras que aparecerían en los próximos mensajes.

La Enigma, en sus diferentes modelos, no fue la única máquina de codificación que se utilizó durante la segunda Guerra Mundial; el ejército japonés utilizó una máquina que los norteamericanos descifraron y que llamaban Purple, el ejército británico utilizó una máquina llamada TipeX y los militares estadounidenses utilizaron una máquina llamada SIGABA. Las máquinas de los ejércitos aliados nunca fueron descifradas, ya que los ejércitos enemigos confiaban demasiado en sus cifras y no apostaron nunca por descifrar las máquinas enemigas. Aunque el ejército estadounidense tenía su SIGABA, esta forma de codificación por escrito les parecía muy lenta, por lo que buscaron otra solución.

SIGABA

Mientras los descifradores británicos estaban descifrando la cifra Enigma alemana y alterando el curso de la guerra en Europa, los descifradores norteamericanos estaban teniendo una influencia igualmente importante en los acontecimientos del área del Pacífico desentrañando la máquina de cifras japonesa conocida como Purple (Púrpura).

Aunque la Purple y la Enigma fueron finalmente descifradas, ofrecieron bastante seguridad cuando fueron puestas en práctica inicialmente y supusieron verdaderos desafíos para los criptoanalistas norteamericanos y británicos. De hecho, si la máquinas de cifras anteriores hubieran sido utilizadas correctamente sin claves de mensaje repetidas, sin restricciones en las posiciones del clavijeros y en las disposiciones de los

modificadores, y sin mensajes estereotipados que causaban puntuales, es bastante posible que nunca hubieran sido descifradas hasta el momento.

La verdadera fuerza y potencial de las máquinas de cifras la demostraron la máquina TipeX (o tipo X) y la máquina de cifras SIGABA (o M-143-C), siendo dichas máquinas más complejas que la Enigma y usadas correctamente, por los que permanecieron indescifradas durante toda la guerra. Los criptógrafos aliados tenían confianza en que las complejas máquinas de cifras electromecánicas podían garantizar la comunicación segura; sin embargo, éstas no son la única manera de enviar mensajes seguros debido a que una de las formas de codificación más seguras utilizadas en la segunda guerra mundial era también una de las más simples.

A comienzos de 1942, el ingeniero Philip Johnston, hijo de un misionero protestante, que había crecido en una reserva de indios navajos, estudió y elaboró un sistema de comunicación basado en el lenguaje navajo. Este código era oral, por tanto rápido y difícil de estudiar su frecuencia, aunque de todas formas se añadieron varios sinónimos para cada palabra y homófonos. Su idea era que cada batallón tuviera operadores de radio de esta tribu; se tomó concretamente esta tribu porque a pesar de ser la más numerosa en los EE.UU. era la menos alfabetizada y además su idioma era ininteligible para otros indios americanos. También se adaptó el léxico militar y los nombres de varios países. Dicho código fue considerado un éxito.

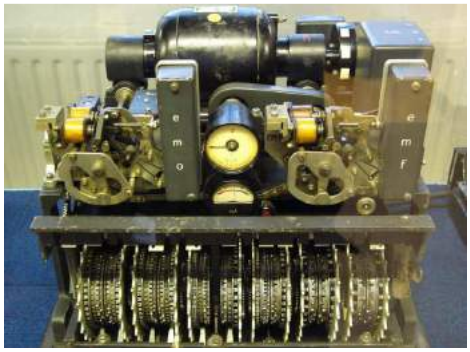
La impenetrabilidad del código navajo se debía al hecho de que el navajo pertenece a la familia de lenguas na-dené, que no tiene ninguna conexión con ninguna lengua asiática o europea. A pesar de sus puntos fuertes, el código navajo tenía defectos importantes. Pese a dichos defectos, en total hubo 420 mensajeros de código navajo, y aunque su valentía como combatientes se reconoció, su papel especial en proteger las comunicaciones era información clasificada, puesto que el gobierno le prohibió hablar sobre su trabajo, y su contribución única no se hizo pública. Los navajos fueron ignorados durante décadas, hasta que finalmente en 1968, el código navajo fue desclasificado. Sin embargo, el mayor tributo al trabajo de los navajos es el simple hecho de que su código es uno de los poquísimos de toda la historia que nunca fue descifrado. El teniente coronel Seizo Arisue, jefe de la inteligencia japonesa, admitió que, aunque

habían descifrado el código de las fuerzas aéreas norteamericanas, no consiguieron tener ningún éxito con el código navajo.

código navajo


Seizo Arisue

Durante la segunda guerra mundial existía otra cifra que se utilizaba para los mensajes del propio Hitler: la cifra Lorenz. Ésta se llevaba a cabo con otra máquina llamada Lorenz SZ4, que era similar a la Enigma pero más compleja. Esta máquina fue descifrada en Bletchley Park por los descifradores John Tiltman y Bill Tutte. Las bombas no fueron suficientes para descodificar esta cifra, no eran lo suficientemente rápidas ni flexibles, siendo esta cifra descodificada con otra máquina llamada el Colossus, que fue diseñado por el matemático Max Newman siguiendo la idea de la máquina Universal de Turing y fue construido por Tommy Flowers, quién tras diez meses acabó su construcción el 8 de diciembre de 1943. El Colossus era considerablemente más rápido que las bombas y está considerado como el primer ordenador programable de la historia.



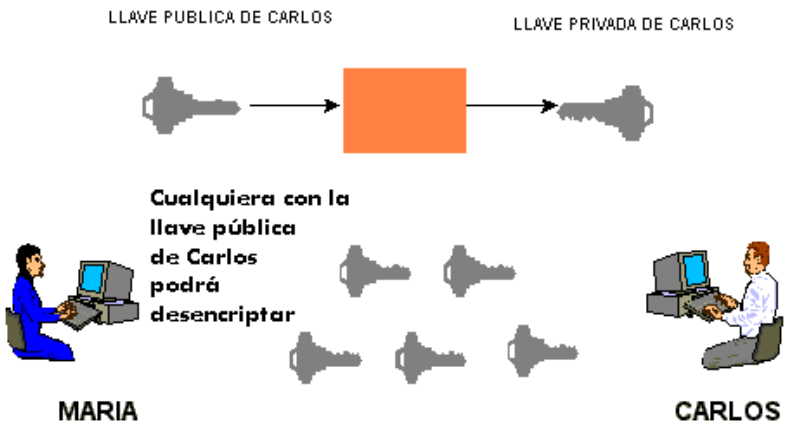
Máquina alemana de cifrado de Lorenz, usada en la segunda Guerra Mundial para el cifrado de los mensajes para los generales de muy alto rango

Tras la segunda Guerra Mundial, todo el material de Bletchley Park fue considerado alto secreto por el gobierno británico quién ordenó que todas las máquinas allí utilizadas fueran destruidas; pero tecnológicamente había llegado el momento, ya se tenían todos los medios y las ideas suficientes para la construcción del ordenador.

Criptografía en la actualidad

7) Criptografía en clave pública

La criptografía asimétrica (también llamada criptografía de clave pública) es una criptografía que se basa en utilizar dos claves: una pública, conocida por todo el mundo y una privada, en poder de una única persona. Estas cifras invariablemente utilizan en problemas matemáticos difíciles como base para su seguridad, así que un punto obvio de ataque es desarrollar métodos para resolver el problema. La seguridad de una criptografía de dos claves depende de cuestiones matemáticas de una manera que no se aplica a la criptografía de clave secreta, y recíprocamente conectan el criptoanálisis con la investigación matemática en general de nuevas maneras.



La manera más rápida de acceder a la comunicación cifrada no es a través del criptoanálisis, sino hacerse con la calve, para lo que en contra sólo existe una solución y es cambiar la clave frecuentemente. Lo habitual es que una de las partes que va a mantener comunicación cifrada elija la clave y lo notifique a la otra. Se plantea así un antiguo problema en criptografía basado en la distribución de claves .Una manera de resolver este problema puede ser:

- Una de las partes: A escoge una clave y cifra empleando otra clave que sólo A conoce.

■ B cifra este resultado una segunda vez, también con una clave que sólo B conoce. El mensaje doblemente cifrado se devuelve a A.

■ A retira su clave particular y remite de nuevo el mensaje a B

■ Por último, B retira también la suya y ya ambos conocen la clave común.

De este modo, A ha comunicado a B una clave común de forma segura por un canal que no necesita serlo. Este idea es interesante sin duda y resuelve el problema de distribución de claves, pero antes se quiere solucionar otro problema que es que la clave común cifrada ha de transmitirse tres veces lo que implica la incógnita por parte de cada una de las dos partes implicadas de que cada mensaje recibido es auténtico, es decir, no ha sido transmitido por un intruso además de la incógnita de cómo realizar esta idea en la práctica.

La repuesta a estas cuestiones y a otras muchas relacionadas, se encuentra dentro de la criptografía en clave pública. En dicha criptografía, con la clave pública se cifran los mensajes y con la privada se descifran. De este modo cualquiera puede cifrar mensajes y transmitirlos al receptor conocedor de la clave privada que es el único que será capaz de entenderlos.

La primera publicación que incluye este revolucionario concepto criptográfico fue un artículo escrito por Whitfield Diffie y Martin Hellman, titulado "New Directions in Cryptograflhy" y publicado en 1976. En él se presentan las nociones básicas de la criptografía en clave pública, se plantean algunos problemas que con ella se resuelven y se describe el primer criptosistema perteneciente a esta nueva rama de la criptografía. Sus autores mencionan también el trabajo de Ralph Merkle, quien había llegado a la misma idea de clave pública. No obstante, aunque se considera a estos tres investigadores americanos loa padres de la criptografía en clave pública, es probable que esta idea fuera desarrollada antes en el seno de todopoderosas organizaciones gubernamentales dedicadas a las tareas criptográficas.


Whitfield Diffie


Ralph Merkle


Martin Hellman

La criptografía de clave pública presenta una ventaja sobre la criptografía de clave secreta. Si *n* personas desean comunicarse mediante un criptosistema de clave secreta, cada una de ellas debe disponer de una clave diferente para cada persona del grupo. Por tanto hace falta poder generar en total *n(n-1)* claves. Teniendo en cuenta que *n* puede ser del orden de varios millares, será necesario generar ficheros de varios millones de claves. Además, añadir un miembro al grupo no es sencillo, ya que habrá que generar otras *n* claves para que el nuevo miembro pueda comunicarse con los demás integrantes del grupo, y después distribuir las nuevas claves a todo el grupo. Por contra, en el caso de un criptosistema asimétrico, se guardan las *n* claves públicas de los miembros del grupo en un directorio. Para añadir un miembro, basta conque ponga su clave pública en el directorio.

La seguridad en criptografía asimétrica es un problema mucho más delicado que en la simétrica, ya que el único dato no público es la clave que sirve para el descifrado. Además no es fácil reunir seguridad y efectividad en un cifrado en clave pública y solamente unos pocos de los numerosos criptosistemas que han sido propuestos lo han logrado. Otra característica distintiva de los algoritmos asimétricos es que, a diferencia de los ataques sobre criptosistemas simétricos, cualquier criptoanálisis tiene la oportunidad de usar el conocimiento obtenido de la clave pública. Los algortimos asimétricos se diseñan en torno a la conjeturada dificultad de resolver ciertos problemas matemáticos. Si se encuentra un algoritmo mejorado que puede resolver el problema, el criptosistema se ve debilitado. Por lo general estos algoritmos están basado en las llamadas funciones unidireccionales definiendo a las mismas como funciones que transforman una variable x en otra y si dada x, el cálculo de y se puede realizar en

tiempo polinomial [57] y además, dada y, el cómputo de una x que produce tal y es un problema intratable [58].

En realidad, el interés de la criptografía de clave pública es el de ocuparse de muchos problemas de seguridad, y ofrecer una gran flexibilidad. Lo que permite entre otras cosas encontrar soluciones a los problemas de autentificación:

Estableciendo el concepto de función unidireccional con un ejemplo. Fijada una lista de r enteros positivos $m_1 \ldots m_r$, a cada bloque de r bits $b_1 \ldots b_r$ se le asocia la suma

$$S = b_1 m_1 + \ldots + b_r m_r$$

Se define función unidireccional a la que a cada bloque r bits le hace corresponder la suma S, el cálculo de S a partir del bloque de bits es inmediato efectuando r-1 sumas como mucho y ello se realiza con un algoritmo lineal. Pero dada una suma S, recuperar un bloque de bits que la produce es un problema intratable famosamente conocido como problema de la mochila. Naturalmente para observar la intratabilidad de este problema hay que considerar valores de r que no sean pequeños, tales como $r > 100$.

Un criptosistema asimétrico diseñado a partir de una función unidireccional basa su seguridad en el problema intratable asociad a esta función, por tanto se trata de que su criptoanálisis sea equivalente a resolver dicho problema. Al mismo tiempo, la rapidez de su vía directa, esto es, el cálculo de y a partir de x, puede ser empleada en los procesos de cifrado y descifrado.

Sucede que el problema de la mochila es fácil de resolver si los enteros forman una sucesión súper creciente, lo que significa que cada entero es mayor que la suma de los anteriores. Luego en el criptosistema de Diffie-Hellman y Merkle (también llamado de la mochila) se parte de una sucesión de enteros súper creciente, considerando además

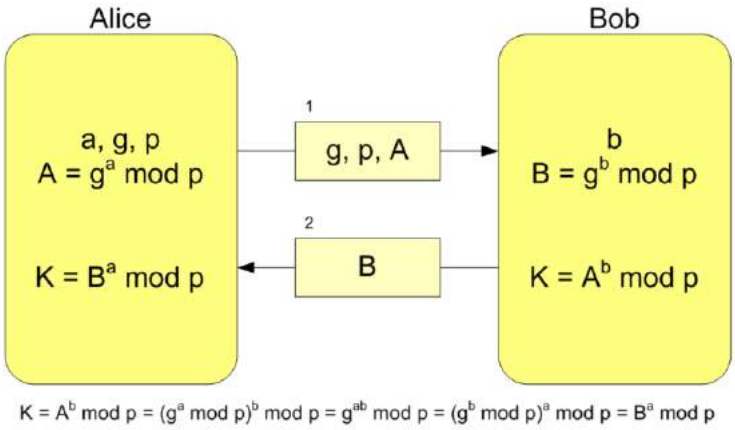
(57) Un algoritmo se ejecuta en tiempo polinomial si existe cierto entero k tal que si los datos de entrada tienen una longitud de n bits, entonces el algoritmo se ejecuta en un número de pasos próximo a n^k.

(58) Un problema que se resuelve mediante un algoritmo que corre en tiempo polinomial es de clase P, análogamente si tal algoritmo no es polinomial es NP. Los problemas NP que no son P (puesto que se cree que ambas clases no coinciden) son los denominados problemas intratables, es decir, aquello para los que no se conocen algoritmos polinomial es que los resuelvan y que además, se sospecha que tales algoritmos no existen.

otros dos enteros, el módulo (mayor que la suma de todos los enteros de la sucesión) y el multiplicador, primo con el módulo (el máximo común divisor de ambos enteros es 1).

La sucesión súper creciente, el módulo y el multiplicador constituyen la clave privada que sólo conoce el receptor de los mensajes. Seguidamente consideramos la aritmética modular(59) pero fijando ahora como módulo de esa aritmética el módulo de la clave privada, además por otro lado como el multiplicador es primo con el módulo tiene inverso para el producto, multiplicando dicho inverso por cada uno de los términos de la sucesión súper creciente que forma parte de la clave privada. Se obtiene así una sucesión $\{t_1 \ldots t_n)$ que ya no es súper creciente, la cual es precisamente la clave pública que conoce todo el mundo.

Para cifrar con ella un mensaje que se supone codificado en binario, el emisor lo divide en bloques de 8 bits ($b_1 \ldots b_8$) y los reemplaza por la suma: **$S = t_1 b_1 + \ldots + t_n b_8$**



He aquí un ejemplo: Clave pública: {257, 576, 390, 399, 417, 515, 463, 350}
Texto claro: 01001101 10001110 00110011 ↓ S ↓ S ↓ S Texto cifrado: 45456 22284 20485
Para la clave privada: módulo: 700 multiplicador: 79 inverso: 319

Para descifrar, el receptor del mensaje debe usar la aritmética módulo el de la clave privada y multiplicar S y el otro miembro de la elución anterior por el multiplicador. Se obtienen así otra ecuación, en la que figuran los enteros de la sucesión súper creciente.

(59) Las operaciones con aritmética modular se realizan recurriendo a las operaciones habituales de enteros y sustituyendo el resultado por el resto de dividirlo entre el módulo

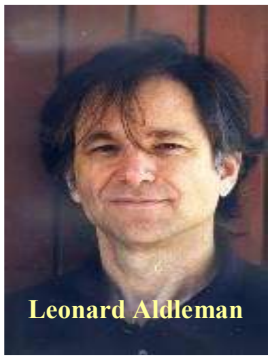
A partir de ella, el receptor puede recuperar el bloque de bits de la manera explicada antes.

Cuando Merkle, Diffie y Hellmandieron a conocer su criptosistema, propusieron utilizar mochilas a partir de 256 enteros. Con tal cantidad, un computador capaz de comprobar un billón de posibles soluciones por segundo tardaríamos de 10^{53} años en comprobarlas todas. Basándose en este hecho, Merkle, Diffie y Hellman creyeron que su criptosistema era seguro y, con el fin de obtener beneficios de su trabajo, lo patentaron en 1980, aunque obtuvieron poco de esta patente debido a que Adi Shamir logró criptoanalizarlo tan sólo un par de años después mostrando que era posible recuperar en tiempo polinomial la clave privada partir de la clave pública y de los textos cifrados.

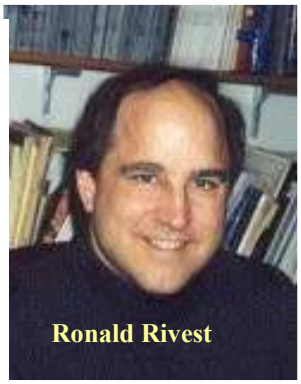

Adi Shamir

La seguridad del protocolo Diffie-Hellman depende de la dificultad de calcular un logaritmo discreto. En 1983, Don Coppersmith encontró una manera más rápida de calcular logaritmos discretos (dentro de ciertos grupos), y por tanto obligando a los criptógrafos a utilizar grupos más grandes, o diferentes tipos de grupos.

En agosto de 1977, la famosa revista *Scientific American* incluía una breve descripción del criptosistema de clave pública más usado en la actualidad denominado RSA, nombre que se forma con las iniciales de los apellidos de sus creadores: Ronald Rivest, Adi Shamir, y Leonard Aldleman, los cuales


Leonard Aldleman

Fundaron en 1982 la compañía RSA Data Security, con objeto de publicar las aplicaciones de su criptosistema que resultó ser un gran negocio debido a que RSA está basado en el problema de factorización de enteros. Basta elevar la cantidad de dígitos del número a factorizar, de 10 a 50 para que el número de operaciones requeridas sea inalcanzable para cualquier ordenador anterior y actual.


Ronald Rivest

El problema de la factorización de enteros proporciona la siguiente función unidireccional, la que a un par de números primos p y q le hace corresponder su producto n= p.q siendo unidireccional porque el cálculo de n a partir de p y q es rápido y se puede

llevar a cabo con un algoritmo casi lineal, por el contrario recuperar los primos p y q factorizando n es un problema intratable soportando en dicho problema el criptosistema RSA.

Se parte de dos primos p y q, distintos y suficientemente grandes para que una vez calculado n resulte imposible su factorización a quien desconozca p y q y se calcula también el llamado indicador de Euler, que en este caso toma el valor $\Phi=(p-1)(q-1)$ además de considerar la aritmética modular módulo Φ, seguidamente se fija un entero positivo $e< \Phi$ se calcula d, su inverso, a continuación se destruye tanto Φ como los enteros p y q que no volverán a utilizarse y que comprometen la seguridad del criptosistema. Los números n y e constituyen la clave pública (denominándose, respectivamente módulo y exponente) y el entero d es la clave privada.

Para cifrar, los textos en claro han de suponerse sucesiones de números enteros positivos menores que n , por lo que si estuviera dicho texto en binario, puna forma sencilla de conseguir lo propuesto es dividir el texto en bloques de k bits, siendo k tal que $2^k \leq n$, y considerar el número binario que determina cada bloque, considerando de nuevo la aritmética modular con módulo n t transformando cada uno de los números (B) que compone el texto en claro en otro número C de acuerdo con la ecuación $C=B^e$. La sucesión de estos números C es el texto cifrado que se transmite.

He aquí un ejemplo: Clave pública: p=257; q=307; n=78899; e=101
Texto claro: 0100000101001101 1000111001000100 0101001101000001 Numeros B: 16717 36412 21249 ↓ B^{101} ↓ B^{101} ↓ B^{101} Numeros C: 45456 22284 20485
Para la clave privada: d=37229 módulo: n indicador de Φ mayor entero k= 16

Para descifrar, el receptor del mensaje recupera de nuevo los números B calculando las potencias C^d dado que $B=C^d$.

Los números considerados en nuestro ejemplo son pequeños para facilitar el cálculo, pero en la práctica, los enteros que se utilizan tienen un tamaño mínimo de 256 bits (77 dígitos) y no es raro llegar incluso a los 1024 bits (308 dígitos). Usar RSA con números de este tamaño requiere superar dos dificultades, la primera, manejar y operar estos números de un modo eficiente, además el cómputo de potencias modulares es lento y, como consecuencia de ello, el cifrado con RSA también lo es siendo al menos más lento que con cualquiera de los algoritmos de cifrado simétrico presentados con anterioridad. El otro problema es la generación de la clave, concretamente la búsqueda de dos números primos arbitrariamente grandes porque, aunque hay suficiente números primos del tamaño que se desee, encontrar dos de ellos sólo es posible si se implementa en el ordenador un algoritmo que permita decidir si un número dado es primo.

La razón de emplear números de tamaño semejante no es otra que la de impedir que un criptoanalista logre factorizar el módulo de n, porque de ser así el cálculo de Φ y después la clave privada se hace de forma inmediata, por lo que impedir factorizar el módulo de n es vital para la seguridad de RSA. Para factorizar un módulo RSA, el algoritmo más rápido que se conoce es el método de la cifra cuadrática descubierto en 1985 (para enteros de hasta 116 cifras) y para enteros de más de 116 cifras es preferible el método de la criba del cuerpo numérico descubierto en 1993.

Además de una factorización del módulo, otro ataque posible es el descubierto por M. Wiener en 1989, el cual dio un algoritmo que permite encontrar la clave privada d cuando ésta no supera la raíz cuarta del módulo n y los primos p y q verifican que el máximo común divisor de p-1 y q-1 es pequeño. Por tanto, como esta segunda condición suele ocurrir muy frecuentemente si los primos p y q se eligen aleatoriamente, conviene considerar claves privadas con un número de dígitos muy próximo al módulo. También se han descubierto otros escenarios muy particulares en los que la seguridad del RSA está comprometida, uno de ellos es el denominado ataque contra un módulo común, que tiene lugar cuando se emplean dos o más claves que comparten un mismo módulo, por lo que si un mismo mensaje es cifrado con dos de estas claves, el texto en claro se puede recuperar a partir de las claves públicas y los criptogramas. Por otro lado como es posible factorizar el módulo conociendo la clave privada, basta conocer una clave

privada para poder calcular todas las demás que compartan el mismo módulo. No obstante, todos estos peligros son fáciles de eludir y, sin temor a una equivocación, se puede afirmas que hoy en día RSA es un criptosistema seguro.

Ahora bien, un avance en la factorización tendría un impacto claro en la seguridad de RSA. En 1980, se podía factorizar un número de 50 dígitos con un coste de 10^{12} operaciones elementales de computación. Para 1984 la tecnología en algoritmos de factorización había avanzado hasta el punto de que se podía factorizar un número de 75 dígitos con las mismas 10^{12} operaciones. Los avances en la tecnología de computación también han provocado que estas operaciones se puedan realizar en un tiempo mucho menor. La Ley de Moore predice empíricamente que las velocidades de computación continuarán aumentando. Las técnicas de factorización podrían mostrar un desarrollo parecido, pero con gran probabilidad dependerán de la capacidad y la creatividad de los matemáticos, ninguna de las cuales ha sido nunca satisfactoriamente predecible. Número de 150 cifras como los utilizados en RSA han sido factorizados. El esfuerzo fue mayor que el mencionado anteriormente, pero no estaba fuera de los límites razonables para un ordenador moderno. Al comienzo del siglo XXI, los números de 150 cifras ya no se consideran suficientemente grandes como clave para RSA. Números de varios cientos de dígitos se siguen considerando demasiado difíciles de factorizar en 2005, aunque los métodos probablemente continuarán mejorando con el tiempo, obligando a los tamaños de clave a mantener el ritmo de crecimiento o a desarrollar nuevos algoritmos.

El cómputo de potencias modulares se realiza mediante un algoritmo que, aunque lento, corre en tiempo polinomial, por el contrario el cálculo de x a partir de y es un problema intratable, denominado problema de los logaritmos discretos, el cual sirvió de base a Diffie y Hellman para dar una solución al problema de la distribución de claves, en la cual, en primer lugar, las dos partes interesadas en una clave común, llamense A y B, deben convenir en un primo p y un base a de los logaritmos módulo p. Una de las partes, digamos A, elige secretamente un entero x y computa $y=a^x$, dato que transmite a B. Análogamente, B elige de modo secreto otro entero u, calcula $v=a^u$ y lo comunica a A. Con v y x, A calcula $K=v^x$ y B también puede obtener este mismo K con su entero secreto u y el dato y que A le ha transmitido, lo que implica

$$\mathbf{Y^u=(a^x)^u=(a^u)^x=v^x=K}$$

La clave común es este entero K que sólo A y B conocen. Lo más significativo de este algoritmo es que tanto el primo p como la base a no necesitan ser secretos, dado que aunque se intercepten y y v, el cálculo de x ó u requiere resolver logaritmos discretos, lo que es un problema intratable. Y sin x ó u la clave K no puede ser calculada, por lo que A y B han intercambiado una clave segura por un canal inseguro sin necesitar mantener previamente una reunión privada.


Taher ElGamal

Unos años después, en 1985, Taher ElGamal propuso un criptosistema basado también en el problema de los logaritmos discretos. Se parte de un primo p y se considera la aritmética modular, módulo p eligiendo a continuación dos enteros positivos aleatorios a y x, ambos menores que p, calculando $y=a^x$ módulo p. Los tres enteros p, a, y constituyen la clave pública y x es la clave privada.

Para cifrar, los textos en claro han de contemplarse como sucesiones de números enteros positivos menores que p, consiguiéndose como antes, dividiendo en bloques de k bits, siendo k tal que $2^k \leq p$, considerando así el número binario que determina cada bloque. Entonces, para cada uno de los números B que compone el texto en claro se elige aleatoriamente un entero positivo E<p y se calcula $C_1=a^E$ y $C_2=B.y^E$. El par de números C_1 Y C_2 es el transformado de B y la sucesión de estos pares es el texto cifrado que se transmite.

He aquí un ejemplo: Clave pública: p=70001; a=35791; y=54093; e=101
Texto claro: 0100000101001101 1000111001000100 0101001101000001
Numeros B: 16717 36412 21249
Numeros E: 45981 11037 64159
$C_1=a^E$ $C_2=B.y^E$ $C_1=a^E$ $C_2=B.y^E$ $C_1=a^E$ $C_2=B.y^E$ Par C_1 Y C_2: 41073 5298 14594 58065 17737 57206
Para la clave privada: x=59925 mayor entero k= 16

Para descifrar, el receptor del mensaje recupera de nuevo los números B calculando $C_2.C_1^{-x}$.

La seguridad del criptosistema ElGamal radica en que como x es el logaritmo discreto de y en base a, encontrar esta clave privada x es un problema intratable. No obstante, al igual que ha ocurrido con la factorización de enteros, los algoritmos encontrados recientemente han hecho que el cálculo de logaritmos discretos sea un problema "menos intratable". Sin entrar en detalles, para que el criptosistema sea seguro, p debe tener al menos 512 bits (155 dígitos) y ser un primo fuerte [(60)].

Dado un cuerpo K, se llama curva elíptica sobre K a la curva plana sobre K definida por la ecuación:

$$\mathbf{Y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a \in K.,\ i = 1,\ldots,6}$$

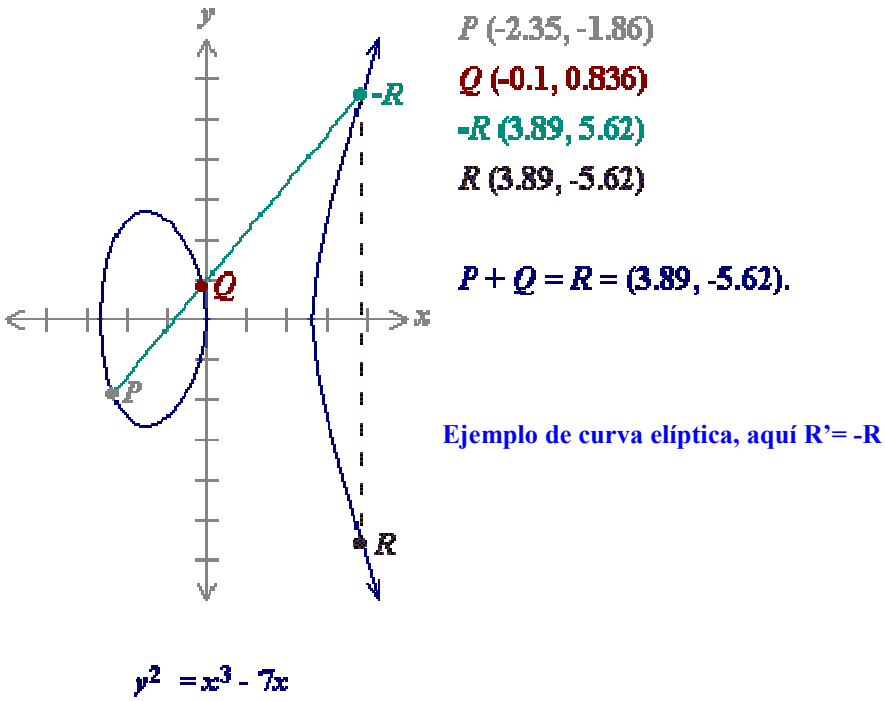
Un a curva elíptica es un tipo especial de curva algebraica plana que tiene la propiedad de que los puntos que yacen en ella forman un grupo abeliano aditivo [(61)].

Sea E una curva elíptica definida sobre el cuerpo finito GF (q), siendo q un primo o la potencia de un primo p^r. Dados dos puntos P, Q pertenecientes a E, la recta PQ corta a E en tres puntos (por ser la ecuación de tercer grado) en P, en Q y en otro punto R', de tal manera que se define la suma de los puntos en E como P+Q=R, siendo R el punto de la curva simétrico a R'.

De esta forma, la multiplicación que se ha efectuado en los grupos anteriores aquí se transforma en la suma de puntos, mientras que la exponenciación anterior aquí se transforma en el producto de un número de GF (q) por un punto de la curva. Por otra parte, se ha probado que el logaritmo discreto para curvas elípticas es tan difícil de resolver como sobre otros grupos del mismo tamaño, así pues, estas curvas se han utilizado para implementar los criptosistemas basado en el logaritmo discreto (Diffie-Hellman y ElGamal), con la seguridad, pero con la ventaja de utilizar claves de

(60) p-1=2.q, con q otro número primo.
(61) En matemáticas, un grupo abeliano, también llamado grupo conmutativo es aquel en el que el orden de los factores no altera el producto. Un grupo abeliano es aditivo cuando se escribe utilizando el símbolo + para su operación binaria

longitudes más pequeñas, lo que requiere menos memoria de ordenador y elementos hardware de tamaño más reducido.



Ejemplo de curva elíptica, aquí R'= -R

Si E es una curva elíptica sobre un cuerpo finito GF (q) y P es un punto de E, entonces el problema del logaritmo discreto en E (de base B) es: dado un punto P perteneciente a E, encontrar un entero x perteneciente a GF (q) tal que x.B=P. Así para definir el protocolo análogo al de ElGamal sobre una curva elíptica, E, se elige un punto de la curva, P, y se selecciona un entero aleatorio a, de modo que la clave privada es el entero a y la clave pública es el punto de la curva a.P.

Otra de las ventajas de utilizar curvas elípticas es que cada usuario puede elegir una curva elíptica diferente, utilizando el mismo cuerpo base, lo que permite, por tanto, que todos los usuarios utilicen el mismo hardware, además de que la curva elíptica elegida puede cambiarse periódicamente para mayor seguridad.

Si en lugar de considerar un cuerpo finito en entero con p se selecciona de enteros con n, siendo n= p.q, p y q primos, se está analizando actualmente la posibilidad de implementar criptosistemas análogos al RSA sobre estas curvas elípticas.

Los criptosistemas presentados son sólo una muestra de los muchos que han sido propuestos desde 1976, tales como el de Rabin, el de McElice, etc. sin embargo, los descritos son los más significativos.

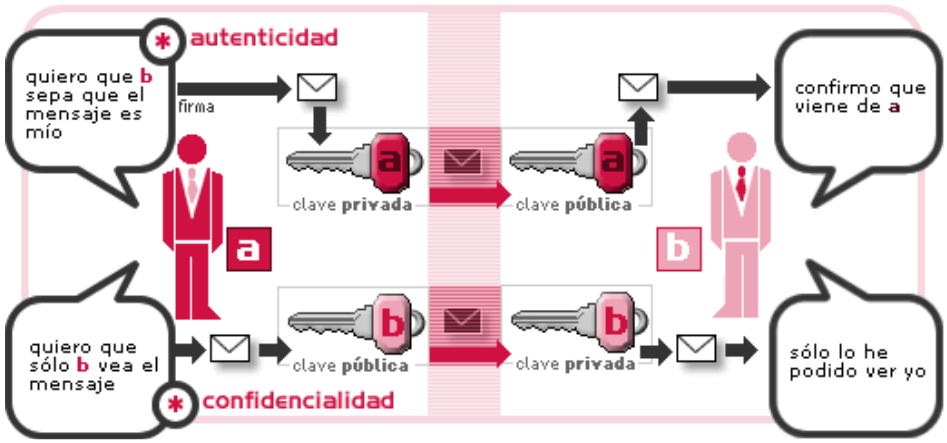
Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para los algoritmos simétricos se considera segura una clave de 128 bits, para los asimétricos (exceptuando los basados en curvas elípticas) se recomiendan claves de al menos 1024 bits. Además, la complejidad de cálculo que comportan estos últimos, los hace considerablemente más lentos que los algoritmos de cifrado simétrico. En la práctica los métodos asimétricos se emplean generalmente para codificar la clave de sesión (simétrica) de cada mensaje o transacción particular.

Las aplicaciones de la criptografía de clave pública son mucha y variadas describiéndose algunas de ellas a continuación:

Autenticación de un mensaje. Dejando al margen el objetivo específico de la criptografía de proporcionar comunicaciones seguras sobre canales inseguros, existen también otras aplicaciones tales como la intimidad y la firma digital de las que hablaremos en posteriores capítulos. Pero otro requerimiento fundamental en las transmisiones criptográficas es que los mensajes resulten fiables, es decir, que exista la seguridad de que nadie pueda modificar parte alguna del contenido del mensaje transmitido, por lo que la primera aplicación de la criptografía es la autenticación del mensaje.

Generalmente se consideran dos clases diferentes de criptoanálisis en las transmisiones criptográficas, los cuales son los pasivos o escuchas y los activos o tramperos. Mientras que los primeros se limitan a interceptar la transmisión y procuran descifrar el mensaje o la clave, los segundos intentan introducir información en la transmisión, con lo que el mensaje enviado se modifica. Los esquemas de autenticación tienen por objeto detectar la presencia de tramperos en la transmisión, asegurando dicho protocolo la intimidad de los mensajes supuesto que ningún espía conoce la clave utilizada. No obstante, un trampero puede desconocer la clave secreta utilizada por dos parte integrantes y, sin embargo, conocer pares de mensajes y sus correspondientes

textos cifrados, hecho que puede permitir introducir piezas de textos cifrados en la transmisión.



Por otra parte, con respecto a los criptosistemas de clave pública, el proceso de firmar digitalmente un mensaje permite asegurar la autenticación del mismo, por lo que en el caso de que el mensaje obtenido a partir de firma digital no coincida con el mensaje recuperado por medio de la clave privada del destinatario, éste debe ser rechazado, lo que implica el consiguiente rechazo de su autenticación.

Concluyendo, para falsificar un mensaje o una parte del mismo utilizando un criptosistema de clave pública, es necesario falsificar tanto el mensaje como la firma correspondiente al mismo, lo cual obliga a conocer la clave privada del remitente del mensaje.

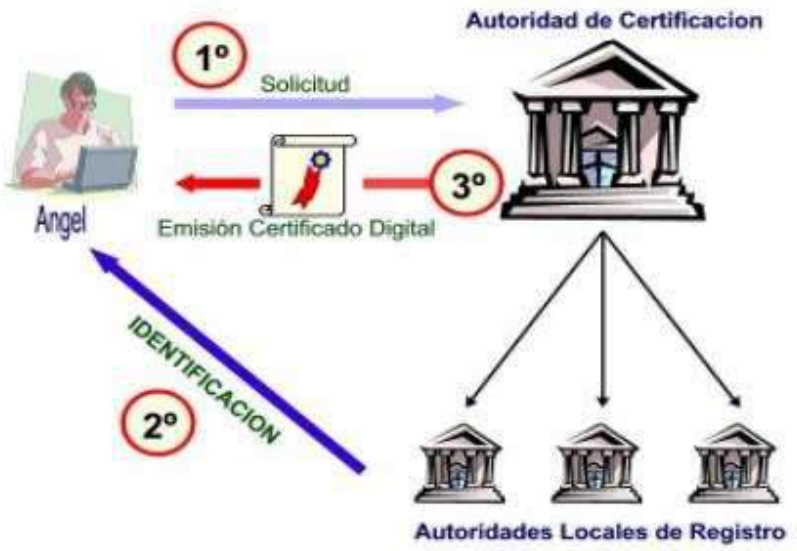
Identificación del usuario. Generalmente, el acceso a una red se lleva a cabo mediante la identificación del usuario por un password, lo que supone que éstos están almacenados en el ordenador y, por tanto, son accesibles. Una forma de evitar que alguien pueda acceder a dichos passwords y conocerlos, es permitir al ordenador que valide el password de un usuario pero que no lo almacene, para lo cual se puede utilizar una función unidireccional de tal modo que el ordenador no almacene los passwords, sino las imágenes de los mismos por medio de dicha función unidireccional.

No obstante, todavía existe un momento en el que los password son accesibles; dicho momento es mientras el ordenador los guarda en memoria y efectúa los cálculos para comprobar la identificación. Así pues, el remedio sería que el ordenador nunca conociera el password del usuario lográndolo con el protocolo basado en la

identificación amigo o enemigo de la segunda Guerra Mundial en el que, cada usuario elige una clave aleatoria de algún criptosistema de clave pública y revela al ordenador el algoritmo de cifrado, mientras que programa en su terminal el algoritmo de descifrado. Cada vez que el ordenador desee confirmar la identidad de un usuario, genera un mensaje aleatorio, lo cifra y lo envía al usuario, el cual, lo descifra y lo devuelve al ordenador, quien lo compara con el mensaje original. El problema que presenta este protocolo es que permite la identificación de la terminal, no del usuario, y por ello el remedio sería utilizar un password para la terminal y el protocolo anterior para la red.

Al margen de la cuestión que acabamos de señalar, existe un procedimiento que permite asegurar la identificación de un usuario ante terceras personas, lo que se trata recurriendo a autoridades de certificación (CA), la cuales son organismos centrales que expiden certificados a los usuarios validando en el proceso sus claves. Así, cuando un usuario desea participar en un red de comunicaciones, selecciona sus claves, pública y privada y solicita un certificado de autenticación de modo que pueda exhibirlo como garantía de que la clave pública le pertenece, estando firmado dicho certificado con la clave privada de la autoridad de certificación.

Con los requisitos anteriores, si un usuario tiene que identificarse ante otro al enviar un mensaje, le enviará, además del mensaje y la firma correspondiente, su certificado como propietario de esa clave pública, entonces el receptor del mensaje verificará el certificado mediante la clave pública de la autoridad de certificación que haya firmado el certificado, y posteriormente, confiando ya en la clave pública del remitente, verificará la firma digital del mensaje.



Lanzamiento de una moneda por teléfono. Problema catalogado como imposible. Alicia y Bernardo se han divorciado y viven en dos ciudades diferentes, ellos quieren decidir quién se queda con el coche lanzando una moneda al aire mientras hablan por teléfono, pero, dado que con este planteamiento, si Bernardo elige el resultado del lanzamiento antes de que Alicia lance la moneda, Alicia podría hacer trampa; y, por otra parte, si Alicia lanza la moneda y luego Bernardo elige el resultado, el que puede hacer trampa es Bernardo; con lo que se trata de encontrar un protocolo de modo que ninguno de los dos pueda hacer trampa.

Una posible solución sería determinar un procedimientos sería que Alicia no pudiera lanzar la moneda después de oír la hipótesis de Bernardo, y de modo que Bernardo no sea capaz de conocer el resultado del lanzamiento antes de decir su hipótesis. Este planteamiento que parece desembocar en un problema imposible se puede resolver mediante el siguiente protocolo:

■Alicia y Bernardo se ponen de acuerdo y eligen una función unidireccional sobre un conjunto X con igual número de pare e impares, f: X $\longrightarrow$ Y.

■Alicia elige un número aleatorio x de X, calcula f(x) = y, y anuncia el valor de y a Bernardo.

■Bernardo supone si x es par o impar y dice su hipótesis a Alicia.

■ Alicia descubre el valor de x elegido y ambos comprueban que, en efecto f(x) = y.

De este modo, se resuelve si Bernardo acertó o no con su hipótesis sobre la paridad de x y, por tanto, si se queda o no con el coche. Con dicho protocolo, la posibilidad de hacer trampas es muy remota, siendo la única posibilidad para ello que la función no se elija correctamente debido a que no sea biunívoca, con lo que Alicia podría conocer dos valores diferentes de x que dieran la misma imagen por f, pero de modo que esos dos valores tuvieran distinta paridad, desembocan en hacer trampa; por otra parte, Bernardo podría hacer estimaciones probabilísticas sobre la paridad de los valores de x computando la función f elegida.

Hay otro protocolo que permite resolver el problema anterior recurriendo a los residuos cuadráticos en lugar de a las funciones unidireccionales, el cual utiliza números enteros de Blum, que son números enteros producto de dos números primos, ambos congruentes con 3 módulo 4, hecho que se basa en que tales números poseen la propiedad de que sólo una de las raíces cuadradas de un residuo cuadrático módulo n vuelve a ser residuo cuadrático. El protocolo es el siguiente:

■ Alicia elige aleatoriamente un entero de Blum, n, y un elemento x de Z_n^* Calculando, seguidamente, el valor de $y = x^2$ (módulo n) y el de $z = y^2$ (módulo n) comunicándole a Bernardo el valor de z.

■Bernardo anuncia si cree que y es par o impar.

■Alicia descubre x e y a Bernardo y le convence de que n es un entero de Blum.

■ Bernardo comprueba entonces que $y = x^2$ (módulo n) y que $z = y^2$ (módulo n).

En definitiva, Alicia da a Bernardo un residuo cuadrático, z, módulo un entero de Blum, y Bernardo tiene que decidir si su raíz cuadrada principal, y, es par o impar con lo que es imposible que ninguno de los dos haga trampa.

Transferencia inconsciente. Una parte A posee un secreto que quiere transferir a otra parte B, pero de modo que, después de ejecutado el protocolo, la probabilidad de que B haya recibido el mensaje sea del 50% y, además, que A no sepa si B ha

conseguido el secreto. Para concretar, supongamos que A quiere transferir inconscientemente a B el secreto de la factorización de un número n como producto de dos números primos grandes, esta situación no hace perder generalidad al problema, pues el secreto puede estar cifrado mediante el criptosistema RSA, para que el conocimiento de la factorización del número permita conocer el secreto. A continuación vemos los pasos necesarios para ello:

■B elige un número x y dice a A el valor de x^2 (módulo n).

■A (que conoce la factorización de n = p.q) calcula las cuatro raíces cuadradas de x^2 (módulo n) y hace conocer una de ellas a B.

■B comprueba si la raíz cuadrada conseguida en el paso 2 es congruente con una raíz cuadrada (módulo n), en cuyo caso B no obtiene ninguna información que no supiera ya. En caso contrario, B tiene dos raíces cuadradas diferentes del mismo número módulo n y, por tanto, es capaz de factorizar n; por otra parte, A no tiene forma de saber en cual de las dos situaciones se encuentra B.

Firma de un contrato. Permite que A y B puedan firmar un contrato simultáneamente en una red, de modo que ninguna de las partes pueda romper el protocolo y disponer de la firma de la otra parte sin haber firmado el contrato. El principal problema que se presenta al formar contratos es que cualquiera que sea la primera parte que firma el contrato es el primer responsable. Para conseguir una responsabilidad simultánea, se procede:

■ A construye el número n_A como producto de dos primos grandes, y B procede de forma similar con n_B.

■ A envía a B un contrato firmado (con su firma digital) en el que asegura que el contrato es válido si B sabe como factorizar n_A, procediendo B de forma análoga con n_B.

■ Una vez que cada parte ha leído el contrato firmado y ha verificado la firma digital de la otra parte, se intercambian los factores de n_A y n_B, por el protocolo de intercambio de secretos.

Correo con acuse de recibo. En este caso, A envía un correo a B, de modo que B obtiene el correo sólo si A obtiene un recibo de B. Supongamos que el correo con acuse de recibo que A desea enviar a B es m y que E_A es el cifrador de de clave pública de tipo RSA de A. El siguiente protocolo se basa en el hecho de que B puede obtener el correo m si es capaz de factorizar n_A:

■ A construye n_A como producto de dos primos grandes y se lo envía a B.

■ B construye n_B como producto de dos primos grades y se lo envía a A, junto con el acuerdo firmado de que si A puede factorizar n_B, entonces B factoriza n_A y obtiene cualquier correo m que esté cifrado por E_A: E_A (m).

■ A continuación, A y B se intercambian los factores por le protocolo de intercambio de secretos.

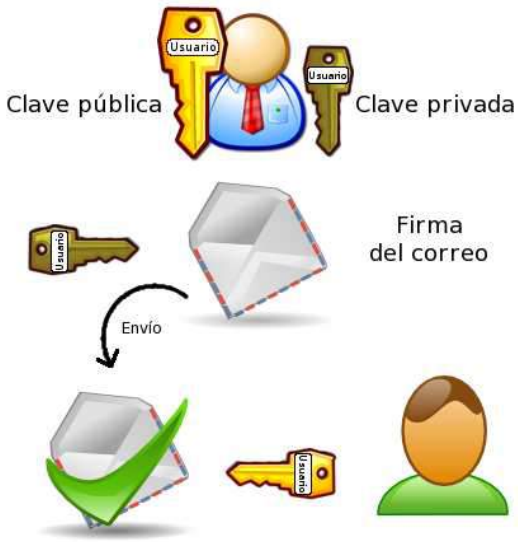
Obsérvese que el recibo de A incluye el contenido del correo m.

Las aplicaciones anteriores son sólo una muestra de todas las que hay, sin embargo existen otras muchas aplicaciones criptográficas tales como **póker por teléfono, secreto dividido, descubrimiento parcial de secretos (problema del millonario), venta de secretos, esquema electoral, descubrimiento mínimo, intercambio de secretos, computación con datos cifrados, canales subliminales, protección de software, …**, que para los muy interesados se detallan en los libros de la bibliografía de esta proyecto.

8) Criptografía para Internet

A finales de 1955, Presper Eckert y John Mauchly, de la universidad de Pensilvania, concluyeron la construcción de lo que muchos consideran el primer ordenador electrónico: ENIAC (Electronic Numerical Integrator And Computer). La primera tarea que llevo a cabo fueron unos cálculos de Física Nuclear que suponían 100 años de trabajo de una persona y en los que el ENIAC empleo sólo 2 horas, podía efectuar 5000 sumas ó 360 multiplicaciones en un segundo. Actualmente, en el mundo hay varios cientos de millones de ordenadores, de peso y tamaño cada vez más reducido, que son capaces de realizar más de un millón de operaciones por segundo y, lo que es

más importante, cómo pueden ser programados para realizar cualquier tarea están cada vez más presentes en un mayor número de actividades humanas.



Usando nuestra clave pública comprueba la firma

Indudablemente, y como era lógico, la criptografía se vio afectada por la llegada de los ordenadores. En primer lugar, en el modo de hacerla, ya que un ordenador puede ser programado para implementar cualquiera de los métodos de cifrado descritos hasta ahora, así como las máquinas de rotores descritas y por supuesto los métodos de criptoanálisis. No es difícil imaginar que si muchos criptosistemas fueron derrotados sin emplear un ordenador, con él no tienen ninguna posibilidad. Sin embargo, también, sería iluso pensar que la llegada de los ordenadores ha dado ventaja a los criptoanalistas frente a los diseñadores de código. Por el contrario, en el ordenador es posible implementar nuevos criptosistemas que proporcionan una seguridad muy superior a los cifrados clásicos. Por consiguiente, los fundamentos de los nuevos criptosistemas arrancan del modo en que se representa la información en los ordenadores, aunque internamente se representan del mismo modo: mediante números, números binarios.

Un número binario(62) es una secuencia de bits y todos los ordenadores operan internamente con números binarios por lo que cualquier información que procesen ha de transformarse antes en una sucesión de números binarios mediante la asignación de un número a cada dato básico de información, empleando para ello un código. Así pues, un texto escrito con un cierto alfabeto se puede transformar en una secuencia binaria

(62) http://es.wikipedia.org/wiki/Binario

haciendo corresponder a cada letra del alfabeto el número binario que figure en el código utilizado al efecto. Hasta hace muy poco, tal código era el habitualmente famoso ASCII (American Standard Code for Information Interchange) de 8 bits. En la actualidad, se ha desarrollado un nuevo código estándar de 16 bits, el Unicode, el cual es una extensión del ASCII que incluye numerosos juegos de caracteres: griego, árabe, cirílico, chino, japonés, símbolos matemáticos, etc., con 16 bits hay lugar para 2^{16} = 65536 signos diferentes.

TABBLA DE ASCII DE 8 BITS

DEC	HEX	OCT	CHAR	DEC	HEX	OCT	CH	DEC	HEX	OCT	CH	DEC	HEX	OCT	CH
0	0	000	NUL	32	20	040		64	40	100	@	96	60	140	`
1	1	001	SOH	33	21	041	!	65	41	101	A	97	61	141	a
2	2	002	STX	34	22	042	"	66	42	102	B	98	62	142	b
3	3	003	ETX	35	23	043	#	67	43	103	C	99	63	143	c
4	4	004	EOT	36	24	044	$	68	44	104	D	100	64	144	d
5	5	005	ENQ	37	25	045	%	69	45	105	E	101	65	145	e
6	6	006	ACK	38	26	046	&	70	46	106	F	102	66	146	f
7	7	007	BEL	39	27	047	'	71	47	107	G	103	67	147	g
8	8	010	BS	40	28	050	(	72	48	110	H	104	68	150	h
9	9	011	TAB	41	29	051	)	73	49	111	I	105	69	151	i
10	A	012	LF	42	2A	052	*	74	4A	112	J	106	6A	152	j
11	B	013	VT	43	2B	053	+	75	4B	113	K	107	6B	153	k
12	C	014	FF	44	2C	054	,	76	4C	114	L	108	6C	154	l
13	D	015	CR	45	2D	055	-	77	4D	115	M	109	6D	155	m
14	E	016	SO	46	2E	056	.	78	4E	116	N	110	6E	156	n
15	F	017	SI	47	2F	057	/	79	4F	117	O	111	6F	157	o
16	10	020	DLE	48	30	060	0	80	50	120	80	112	70	160	p
17	11	021	DC1	49	31	061	1	81	51	121	Q	113	71	161	q
18	12	022	DC2	50	32	062	2	82	52	122	R	114	72	162	r
19	13	023	DC3	51	33	063	3	83	53	123	S	115	73	163	s
20	14	024	DC4	52	34	064	4	84	54	124	T	116	74	164	t
21	15	025	NAK	53	35	065	5	85	55	125	U	117	75	165	u
22	16	026	SYN	54	36	066	6	86	56	126	V	118	76	166	v
23	17	027	ETB	55	37	067	7	87	57	127	W	119	77	167	w
24	18	030	CAN	56	38	070	8	88	58	130	X	120	78	170	x
25	19	031	EM)	57	39	071	9	89	59	131	Y	121	79	171	y
26	1A	032	SUB	58	3A	072	:	90	5A	132	Z	122	7A	172	z
27	1B	033	ESC	59	3B	073	;	91	5B	133	[	123	7B	173	{
28	1C	034	FS	60	3C	074	<	92	5C	134	\	124	7C	174	|
29	1D	035	GS	61	3D	075	=	93	5D	135	]	125	7D	175	}
30	1E	036	RS	62	3E	076	>	94	5E	136	^	126	7E	176	~
31	1F	037	US	63	3F	077	?	95	5F	137	_	127	7F	177	DEL

Hoy en día, prácticamente la totalidad de los hogares de los llamados países desarrollados tienen a su disposición un ordenador personal, y de ellos raro es el que no dispone de la herramienta Internet para realizar sus comunicaciones, investigaciones, etc. Las comunicaciones vía Internet a través del correo electrónico a desbancado al correo tradicional, dicha situación ha provocado cierta incertidumbre sobre la seguridad de la información y comunicaciones y creado, en cierta medida, la necesidad de utilizar la cifra en todas nuestras actuaciones, para gozar de cierta tranquilidad.

¿En qué situaciones o ámbitos es recomendable que toda la información transmitida electrónicamente entre dos actores fuera cifrada? No es necesario o al menos no recomendable para nuestra salud mental caer en este tipo de paranoias. Podemos pensar que todo lo que nos intercambiamos a través de Internet se está recolectando... y es así, es verdad que existe la red Exelon... pero de ahí a cifrar todos nuestros correos creo sería caer precisamente en esa paranoia.

Pero aquí hay que saber diferenciar los ámbitos de trabajo. Cifrar todo mi correo personal no tendría sentido, algunos mensajes tal vez sí, pero si trabajo por poner un ejemplo en el Ministerio de Defensa y uso mi cuenta de correo corporativa, posiblemente sí sería lógico que muchos de mis mensajes fuesen cifrados y firmados. Y aquí entramos en un terreno cuyo debate estará siempre abierto: ¿nos interesa más la confidencialidad (secreto) de la información o su autenticidad e integridad?

Como lo definen las denominadas políticas de seguridad, dependiendo del entorno en que nos movamos primará una más que la otra. Aunque ambas tienen importancia, si hubiese que elegir entre las dos en el mundo de Internet y las redes, hoy me inclinaría por la de autenticidad e integridad a través de certificados digitales e infraestructuras de clave pública.

El correo electrónico es una postal digital, que no asegura la confidencialidad. Pero los sistemas criptográficos bien diseñados si pueden garantizar el secreto de la correspondencia.

El correo electrónico llega a todos los hogares y empresas vía Internet con velocidad deslumbrante, pero también es muy sencillo ser victima potencial de los escuchas electrónicos. La forma de reforzar el carácter reservado de estas transmisiones es cifrarlas, manipulando y enrevesado la información con el fin de volverla ininteligible para todos, excepto para el destinatario.

Desde los años ochenta el desarrollo de algoritmos refinados y de equipos informáticos económicos ha puesto al alcance de cualquier persona sistemas criptográficos muy potentes, cuya seguridad es de nivel militar. Es de esperar que los continuos avances técnicos doten a dichos sistemas de una mayor resistencia llegando incluso a poder volverles invulnerables al descifrado de claves.

Hasta hace muy poco tiempo, la NSA poseía el monopolio de la técnica de encriptación, especialidad que era mantenida en celoso secreto. En 1976 Whitfield Diffie y Martin E. Hellman, profesores de la universidad de Stanford, publicaron el articulo "New Directions in Cryptography" donde exponían abiertamente la noción de criptografía de clave pública, lo cual supuso un cambio radical es el panorama de la criptografía. De tal forma, que el los años sucesivos a dicha publicación se ha desarrollado y florecido una vigorosa comunidad criptográfica en las universidades y empresas, no solo de Estados Unidos, sino de todo el mundo. Por otro lado, la creciente popularidad de Internet y la preocupación general por la seguridad de las comunicaciones en dicho medio, ha intensificado la tendencia. Algunos de los mejores cifrados y sistemas de claves están siendo desarrollados por criptógrafos pertenecientes a universidades o empresas privadas repartidas por todo el globo y es la propia NSA la que se ve obligada a adquirir esos productos comerciales para atender parte de sus necesidades criptográficas.

En los criptosistemas tradicionales se usa una sola clave tanto para la encriptación como para la descodificación. Tales sistemas simétricos exigen que la clave sea trasmitida por un canal seguro. Pero, si ya hay un canal seguro, ¿Qué necesidad hay de llevar a cabo una encriptación? Al ser eliminada esta limitación por Diffie y Hellman, se produjo una expansión de la criptografía. La clave pública permite la comunicación sin necesidad de un medio secreto de envío de claves. Tales sistemas asimétricos se fundamentan en un par de claves que son distintas, aunque complementarias. Cada clave descifra el mensaje que la otra cifra, pero el proceso no es reversible. Por lo tanto, una de las claves (clave pública) puede hallarse al alcance de muchos, mientras que la otra (clave privada) sólo está en manos de su poseedor.

Los principales algoritmos de clave pública son el de Diffie-hellman y el método RSA (explicado y desarrollado en un capítulo posterior). Variantes del primero son el

estándar de firma digital del Instituto Nacional de Pesos y Medidas, ElGamal y los métodos basados en curvas elípticas.

Los sistemas criptográficos de clave pública sirven, además, para la certificación de mensajes, es decir, el receptor puede comprobar la identidad del remitente. Evidentemente, toda esta encriptación y descodificación exige diversos cálculos matemáticos. Pero existen programas, como el PGP, apto para ordenadores personales, capaces de automatizar el proceso.

La criptografía de clave pública presenta dos graves limitaciones:

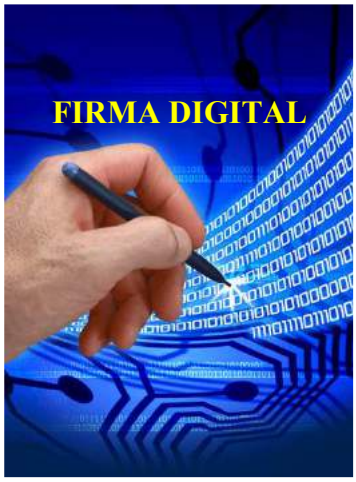
■ Relativa lentitud, lo cual hace que sea poco práctica a la hora de codificar mensajes grandes.

■ En ocasiones permite que aparezcan en el mensaje patrones que sobrevivan al proceso de encriptación, siendo tales pautas detectables en el texto, lo que hace que la técnica sea vulnerable de análisis criptográfico o criptoanálisis.

En definitiva, la codificación de gran tamaño suele estar encomendada a cifras simétricas, más rápidas y seguras, estando limitada la criptografía de clave pública a la pequeña, aunque esencial función, de intercambio de las claves simétricas

9) Protocolos criptográficos y firmas digitales

9.1 Firma digital



El concepto de firma digital, fue introducido por Diffie y Hellman en 1976 y básicamente es un conjunto de datos asociados a un mensaje que permiten asegurar la identidad del firmante y la integridad del mensaje.

El nacimiento de la firma electrónica se debe sin duda a la necesidad de una respuesta técnica segura para poder realizar la conformidad o el acuerdo de voluntades en una transacción electrónica (comercio electrónico, e-adminstración, etc.).

En consecuencia, la firma digital es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor y que no ha existido ninguna manipulación posterior de los datos (integridad).

Las firmas digitales, protocolos para envío de mensajes, pueden clasificarse en:

■ Implícitas: están contenidas en el propio mensaje

■ Explícitas: son añadidas como una marca inseparable del mensaje

■ Privadas: permiten identificar al remitente sólo para alguien que comparte un secreto con el mismo.

■ Públicas (o verdaderas): permiten identificar al remitente ante cualquier persona a partir de información públicamente disponible.

■ Revocables: el remitente puede, posteriormente, negar que la firma digital en cuestión le pertenece.

■ Irrevocables: el receptor puede probar que el remitente escribió el mensaje.

Es de vital importancia que las firmas digitales sean fáciles de hacer, fáciles de verificar y difíciles de falsificar; para lo cual, en muchas ocasiones, y con el fin de evitar un ataque contra las firmas por sustitución, donde el posible atacante hace uso de un viejo mensaje, se incluye un número de secuencia del mensaje o un sello temporal.

Ya que un usuario puede utilizar un criptosistema de clave pública para firmar digitalmente un mensaje, es conveniente distinguir entre rúbrica de un usuario y su firma digital. Tal distinción se basa en el doble proceso que se lleva acabo para la elaboración de la firma digital.

Ventajas de la firma digital: autenticación, imposibilidad de suplantación, integridad, no repudio, auditabilidad, confidencialidad de la información intercambiada entre las partes. Otra ventaja de la firma digital es su portabilidad, es decir, la firma digital puede ser realizada en diferentes puntos del mundo, de forma simultánea y sin necesidad de testigos.

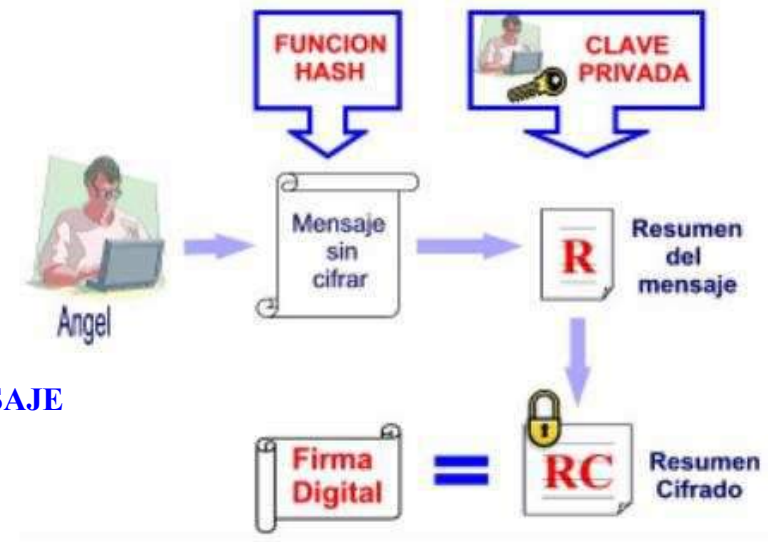
Desventajas de la firma digital. Quizá la más notable desventaja actual de la firma digital en contra de la firma autógrafa, es que la primera no es valida legalmente aun en muchos países. Parece ser que esto obedece a una transición natural de esta nueva

tecnología, que por lo tanto existe un rechazo en su aceptación a pesar de los grandes beneficios que proporciona. Otra desventaja visible de la firma digital, es que su seguridad depende de la clave privada, es decir, que si la clave privada se compromete por alguna causa, entonces, se compromete la seguridad de la firma digital, esto quiere decir que puede ser usada por individuos y eventos no autorizados

Se denomina rúbrica de un usuario correspondiente a un mensaje a otro mensaje que sólo él puede elaborar a partir de su clave privada y del mensaje que desea firmar, mientras que se llama firma digital a la encriptación de la rúbrica y que es enviada por medio del canal inseguro.

Si A desea firmar digitalmente el mensaje m, envía el mensaje cifrado c al usuario B, y para firmarlo digitalmente se procede:

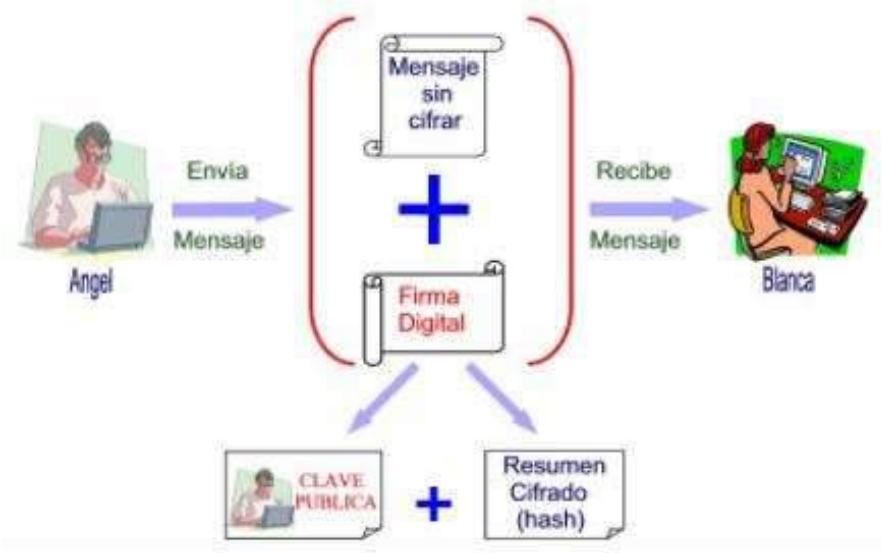
■ A calcula su rúbrica cifrando el mensaje a enviar con su clave privada: $r = f_a^{-1}(m)$. Es evidente que r es la rúbrica de A para el mensaje m, pues es el único que puede generarla.
■ Seguidamente, A determina su firma para el mensaje m sólo con encriptar, con la clave pública de B, la rúbrica que acaba de determinar: $s\text{-}= f_b(r) = f_b(f_a^{-1}(m))$.



FIRMA DE MENSAJE

Una vez que B recibe o recupera el mensaje m debe proceder a la verificación de la firma digital de A, siguiendo los siguientes pasos:
■ B determina la rúbrica de A para el mensaje recibido calculando: $f_b^{-1}(s) = f_b^{-1}(f_b(r)) = r$, por medio de su clave privada.

■ Seguidamente, B comprueba que: $f_a(r) = f_a(\ ^{f}{}_{a}^{-1}(m)) = m$.



VERIFICACIÓN POR EL RECEPTOR DE LA FIRMA DIGITAL DEL MENSAJE.

El agosto de 1991, el NIST(63) propuso un estándar para firma digital: Digital Signatura Standard, abreviadamente DSS, y su correspondiente algoritmo: Digital Signatura Algorithm, abreviadamente DSA(64), solicitando comentarios públicos para la adopción del estándar propuesto. El objetivo que perseguían era proporcionar a las oficinas gubernamentales de los Estados Unidos una forma estándar de firmar las comunicaciones cuando ello fuera necesario.

El DSA propuesto en la elección de los parámetros para DSS es una variante del protocolo de ElGamal(65) consta de los siguientes pasos:

(63) Nacional Institute of Standard and Technology (Instituto nacional de Estándares y tecnología de los Estados Unidos.
(64) Ampliamente detallado en los libros citados en la bibliografía de este proyecto
(65) Explicado con detalle en su correspondiente apartado 9.3.

■ Cada usuario elige los parámetros:

- p: un número primo con $2^{1023} < p < 2^{1024}$.
- q: un divisor primo de p – 1, con $2^{159} < q < 2^{160}$.
- g: un generador del único subgrupo cíclico de $\mathbf{Z}_p^*$ de orden q.
- su clave privada, x, un entero aleatorio con $0 < x < q$.
- su clave pública y, $y = g^x \pmod p$.

■ Suponiendo que H: $\mathbf{M} \rightarrow \mathbf{Z}$ la función hash(66) SHA – 1, y que el mensaje a firmar es m, la firma digital se elabora:

- se selecciona un entero aleatorio k para cada mensaje, con $0 < k < q$
- se calcula el valor de $r = (g^k \pmod p) \pmod q$.
- se resuelve la congruencia: $H(m) \equiv - x \cdot r + k \cdot s \pmod q$ para s.

La firma digital para el mensaje m es la pareja (r,s).

■ Para verificar la firma se procede:

- se calcula $w \equiv s^{-1} \pmod q$.
- se calculan $u_1 \equiv H(m) \cdot w \pmod q$ y $u_2 \equiv r \cdot w \pmod q$.
- se calcula $v \equiv (g^{u_1} \ y^{u_2} \pmod p) \pmod q$.
- se comprueba que $v = r$.

Para ver cómo funciona la verificación, basta notar que de la congruencia anterior se tiene: $w \cdot H(m) + x \cdot r \cdot w \equiv k \pmod q$, donde $w \equiv s^{-1} \pmod q$, o $u_1 + x \cdot u_2 \equiv k \pmod q$. Finalmente, elevando g a $u_1 + x \cdot u_2$, se tiene:

$$\mathbf{r = (g^{u_1} \ y^{u_2} \pmod p) \pmod q}$$

Al igual que la firma digital de ElGamal, la firma del NIST se puede extender a un grupo cíclico de orden q.

La elección de los parámetros de la firma digital DSS se leva a cabo del siguiente modo:

■ Se genera el número primo q repitiendo la elección aleatoria de un número impar q con $2^{159} < q < 2^{160}$ y comprobando su primalidad hasta que q sea primo.

(66) Explicado con detalle en su correspondiente apartado 9.4.

■ Seguidamente, se genera el primo p repitiendo la elección aleatoria de un número entero n con

$$\frac{2^{1023} - 1}{2q} < n < \frac{2^{1024} - 1}{2q}$$

hasta que $p = 2n \cdot q + 1$ sea primo.

■ Finalmente, se genera un elemento g de orden q del grupo $\mathbf{Z}_p^*$ repitiendo la elección aleatoria de un entero h con $1 < h < p - 1$ y computando $g = h^{(p-1)/q}$ hasta $g \neq 1$

El NIST alega como ventajas para su propuesta de firma digital estándar:

■ La seguridad del DSS propuesto está basada en la dificultad del problema del logaritmo discreto en $\mathbf{Z}_p^*$.

■ La ventaja de trabajar en un subgrupo de $\mathbf{Z}_p^*$ es que los tamaños de las firmas son menores.

■ El DSS no puede ser utilizado, de forma obvia, para la encriptación, lo cual para algunos resulta más un inconveniente que una ventaja.

Análogamente, es interesante plasmar las críticas más señaladas a esta propuesta:

■ El tamaño de los parámetros p y q resulta insuficiente para una adecuada seguridad. Se supone que el NIST permitirá una mayor flexibilidad en la elección de tales parámetros.

■ Se requiere la generación de un número aleatorio k de 160 bits para firmar cada uno de los mensajes.

■ La seguridad alegada con relación a que determinar logaritmos en un subgrupo cíclico de orden q necesita determinar logaritmos en $\mathbf{Z}_p^*$ es sólo una hipótesis, dado que el que en la actualidad no se conozcan algoritmos para calcular logaritmos en un subgrupo cíclico de un grupo finito dado, no significa que no se puedan determinar.

■ Requiere mayor trabajo que el necesario para firmar digitalmente un mensajes si se utiliza el criptosistema RSA.

El DSS, junto con su algoritmo, el DSA, es sólo una parte de un proyecto más amplio propuesto por el NIST y la NSA, conocido con el nombre Capstone, el cual pretende desarrollar un estándar de Criptografía de clave pública del gobierno estadounidense, y consta de cuatro componentes:

■ Un algoritmo de encriptación de datos en masa, llamado Skipjack y que no es público.

■ Un estándar para la firma digital (DSS) y un algoritmo de firma digital (DSA).

■ Un protocolo de cambio de clave (aún no ha sido anunciado).

■ Una función hash (Secure Hash Standard, SHS) con su correspondiente algoritmo (Secure Hash Algorithm, SHA – 1).

Todas las partes de Capstone tiene una seguridad de 80 bits, y todas las claves implicadas tienen la misma longitud: 80 bits. Las primeras implementaciones de este proyecto se han cristalizado en el chip llamado Clipper. Este tipo de chip permite cifrar, mediante el algoritmo Skipjack, mensajes bajo los supuestos del proyecto Capstone. Igualmente, Clipper ha sido propuesto como estándar por el gobierno americano, de modo que todas las comunicaciones internas gubernamentales se harían con este chip, así como cualquier comunicación de quien desee hacer negocios con el gobierno.

Un documento electrónico firmado es equivalente a un documento en papel y firmado a mano que se publica en un tablón de anuncios. La firma electrónica es uno de los aspectos más importantes de la criptografía porque permite realizar muchas transacciones por Internet, evitando desplazamientos y pérdidas de tiempo. De hecho en España, a la firma electrónica aplicada sobre datos consignados en forma electrónica, se le otorga la equivalencia funcional con la firma manuscrita en virtud de la ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Quizás la aplicación más conocida en España es la posibilidad de entregar la declaración de la renta en formato electrónico por Internet. Para ello el usuario se identifica ante el servidor Web de la Agencia Tributaria mediante su certificado digital, y luego entrega el documento electrónico de la declaración firmada con su clave privada.

Otro ejemplo son ciertas peticiones que se realizan mediante formularios en la Web, que si se firman electrónicamente tiene la misma validez que una petición presencial. El correo electrónico también puede beneficiarse de los algoritmos de firma

electrónica para poder enviar mensajes firmados que tiene la misma validez que una carta firmada, y evitando los problemas de falsificación del remite del correo. Por último, un aspecto en el que se va más despacio son las transacciones bancarias, las cuales ganaría en nivel de seguridad si se realizasen firmadas digitalmente.

En la práctica no se suele cifrar toda la información del documento con la clave privada, ya que resulta muy pesado computacionalmente, sino que resulta mucho más eficiente (tanto para el emisor como para los receptores) obtener un resumen del documento mediante algoritmos HASH(67) y luego cifrar exclusivamente el código obtenido.

9.2 Firma digital del criptosistema RSA

Para enviar la firma digital del mensaje m con el criptosistema RSA, el supuesto usuario A, cuya clave pública es (n_a, e_a) y cuya clave privada es d_a, debe realizar los siguientes pasos:

■ Cálculo de su rúbrica encriptando el mensaje mediante su clave privada: $r \equiv m^{d_a} \pmod{n_a}$

■ Determinación de su firma digital sólo con cifrar con la clave pública de B la rúbrica anterior: $s \equiv r^{e_b} \pmod{n_b}$.

El mensaje firmado que A envía a B es la pareja formada por (c,s), siendo c el criptograma correspondiente al mensaje m. Evidentemente, sólo A puede determinar la rúbrica anterior, ya que es el único que conoce d_a.

Para que B pueda verificar que la firma corresponde a A, sólo debe comprobarse que:

■ $s^{d_b} \pmod{n_b} \equiv (r^{e_b} \pmod{n_b})^{d_b} \pmod{n_b} \equiv r^{e_b d_b} \pmod{n_b} = r$.

■ $r^{e_a} \pmod{n_a} \equiv m^{d_a e_a} \pmod{n_a} = m$.

Cuando quiere llevarse a cabo la firma digital de un mensaje, ha de tenerse en cuenta que para elaborar la rúbrica r, el mensaje m debe estar dentro del rango de encriptación de n_a. Así pues, la longitud del mensaje m no sólo debe ser menor que n_b

(67) Hay un apartado de firma digital dedicado a esto.

para ser cifrado, sino que también debe ser menor que n_a para que se pueda determinar la rúbrica del remitente. Por otro lado, la rúbrica que se obtiene al cifrar con la clave privada del remitente debe estar dentro del rango de encriptación de n_b, puesto que para calcular la firma digital hay que reducir módulo n_b. En caso contrario, es decir, si $r > n_b$, la rúbrica debe ser troceada en bloques y cifrar cada uno de los mismos.

Este análisis puede llevarse fácilmente a cabo si el mensaje ha de enviarse a una única persona; pero si se trabaja dentro de una red y un usuario desea comunicarse con diferentes usuarios d la misma, sería muy conveniente determinar un proceso que permitiera no tener que llevar a cabo el análisis anterior para cada uno de los mensajes que cualquiera desease enviar. La forma de evitar dicho inconveniente la propusieron Rivest, Shamir y Adleman mediante un protocolo orientado a una red de comunicaciones que permitía realizar el envío de un mensaje a muchos usuarios conectados a una red. El citado protocolo consta de los siguientes pasos:

■ Se elige un umbral h (por ejemplo, $h \approx 10^{199}$)

■ Cada usuario U publica dos pares de claves públicas: (n_u, e_u) y (l_u, f_u), el primero de ellos para ser utilizado en el cifrado de mensajes, y el otro, para ser utilizado en la verificación de la firma.

■ Los módulos de cada uno de los usuarios deben verificar la condición: $l_u < h < n_u$

Con estas condiciones, en el envío de un mensaje firmado del usuario A al B, bastará dividir el mensaje en bloques y verificar que dichos bloques del mensaje m cumplen la condición: $0 < \min \{l_u\}$. Tras lo cual, el usuario A utiliza la clave pública de B: (n_b, e_b) para cifrar el mensaje m, y para elaborar su rúbrica usara su clave privada g_a correspondiente a su clave pública para firmar digitalmente los mensajes (l_a, f_a)

El ataque contra el protocolo de firmar digitalmente un mensaje con el criptosistema RSA es el mismo que el que debería llevarse a cabo para romper el propio criptosistema, dado que en ambos casos las operaciones que se realizan son las mismas.

9.3 Firma digital del criptosistema de ElGamal

El esquema diseñado por ElGamal[(68)] para firmar digitalmente un mensaje sigue el siguiente formato:

(68) El Esquema de firma ElGamal es un esquema de firma digital basado en la complejidad del cálculo del logaritmo discreto. Más información en http://es.wikipedia.org/wiki/Esquema_de_firma_ElGamal

■ Generar, por parte del usuario A, un número aleatorio h tal que cumpla: mod (h, p – 1) = 1

■ Calcular, por parte del usuario A, el elemento $r \equiv a^h \pmod p$.

■ Resolver, por parte del usuario A, la congruencia $m \equiv a \cdot r + h \cdot s \pmod{p - 1}$.

La firma digital del usuario A para el mensaje m es el par (r,s).

Para que el receptor de dicho mensaje m compruebe la firma digital del usuario A debe efectuar:

■ B calcula $r^s \equiv (a^h)^s \pmod p$ y $(a^a)^r \pmod p$.

■ Igualmente, B debe calcular $(a^a)^r \cdot (a^h)^s \pmod p$ y comprobar que es igual a $a^m \pmod p$.

En el caso de pretender conseguir la falsificación de una firma del usuario A en el mensaje m, un escucha tendría que resolver la ecuación $a^m = (a^a)\, r \cdot r^s$ con las incógnitas r y s. Si al intentar resolver dicha ecuación se llevase a cabo la fijación de r para tratar de resolver la ecuación en s resultante, aparecería un problema de logaritmo discreto; mientras que si la incógnita fijada fuera la s y se tratase de resolver la ecuación resultante en este caso, lo que aparecería sería una congruencia exponencial mixta, para la que no hay algoritmo conocido. Este problema se conoce como el Problema de la firma digital de ElGamal (ESP).

9.4 Funciones Hash

Normalmente, los problemas que suelen presentarse a la hora de implementar en la práctica un criptosistema son que los criptosistemas de clave pública generalmente se cifran de forma mucho más lenta que los criptosistemas de clave secreta. Además, los esquemas de firma digital suelen ser muy lentos y, en ocasiones, la longitud de la firma suele ser similar o mayor que el propio mensaje que se firma. Pero, la necesidad de firmar mensajes y el hecho no deseable de que la longitud de la firma sea extensa, hace pensar en la conveniencia de buscar una solución a este problema, la cual consiste en utilizar las llamadas funciones hash antes de firmar un mensaje.

Una función hash (función picadillo) es una función computable que aplica a un mensaje m de tamaño variable, una representación de tamaño fijo del propio mensaje: H(m), que es llamado su valor hash. Por lo tanto las funciones hash se definen como:

$$\mathbf{H: : M \rightarrow M,\ H(m) = m'}$$

En general, h(m) es mucho menor que m

Por otro lado, las funciones hash también pueden utilizarse para determinar el resumen de un documento y hacer público dicho resumen, sin revelar el contenido del documento del que procede el mensaje.

Se dice que una función hash es unidireccional si dicha función hash H es tal que para cualquier mensaje m′ es difícil encontrar un mensaje m tal que m′ = H(m). No es más que una función hash que es también una función unidireccional.

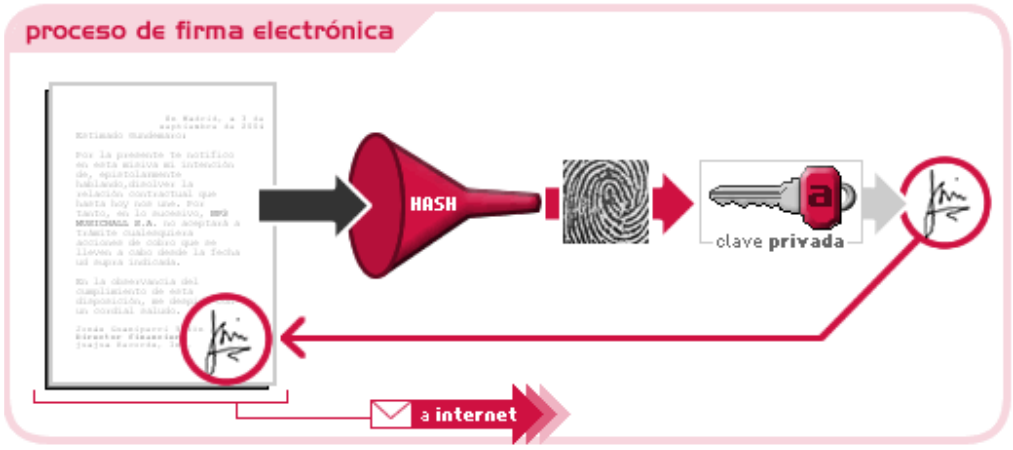
Las funciones hash unidireccionales, también llamada función resumen es difícil de invertir. En este tio de funciones al valor H(m) se le suele llamar el resumen de m, y puede pensarse como una hulla dactilar del mensaje largo m.

Una vez definidas las funciones hash, el problema señalado anteriormente respecto a la longitud de la firma digital se resuelve si en lugar de firmar el mensaje completo m se firma el resumen del mensaje; esto es, se firma H(m).

De esta forma, un usuario A que desee enviar el mensaje m a un usuario B, junto con su firma, lo que hará será enviar el mensaje cifrado; $c = f_b(m)$, y como firma enviará la rúbrica obtenida a partir del resumen H(m) cifrada. Por tanto, determinará:

■ La rúbrica para el resumen del mensaje es: $r = f_a(H(m))$.

■ A continuación determinará la firma digital para la rúbrica anterior: $s = f_b(r) = f_b(f_a^{-1}(H(m)))$.

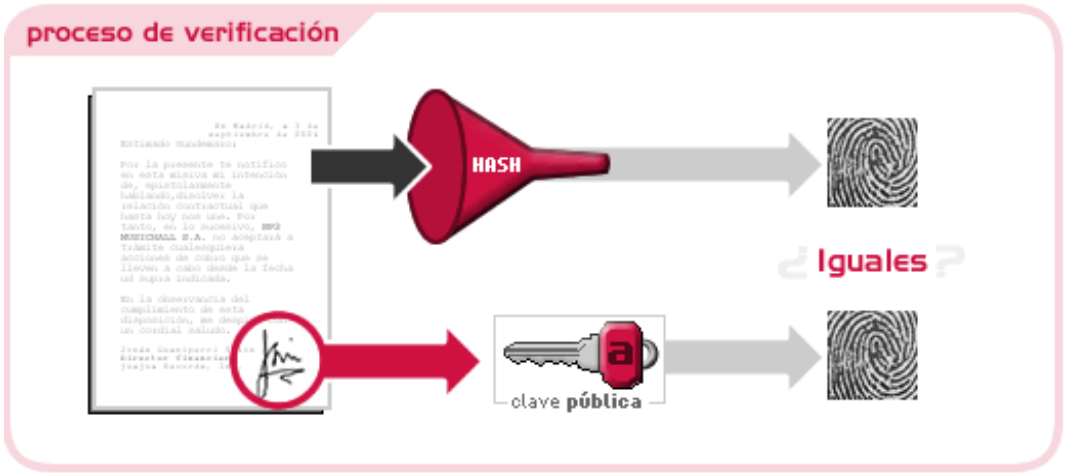


El usuario B recuperará el mensaje como es habitual, terminando m sin más que calcular $f_b^{-1}(c)= f_b^{-1}(f_b(m))=m$ y validará la firma de A:

■ Calculando la rúbrica de A para el resumen del mensaje m: $r=f_b^{-1}(s)= f_b^{-1}(f_b(r))$.

■ A continuación determinará el resumen del mensaje m, $H(m)= f_a(r)= f_a(f_a^{-1}(H(m)))$.

■ Por último, comprobará que el mensaje obtenido coincide con el valor de la función pública H sobre el mensaje recibido.



Es habitual que en lugar de considerar las funciones hash definidas de M en M, se considere que el valor de H(m) pertenezca a los números enteros, para lo cual bastará con cifrar el resumen obtenido H(m) mediante la clave privada del usuario. Así una función hash se define como sigue:

H: M ⟶ Z, H(m)=n

Hay que hacer notar que, dado que el criptosistema ElGamal determina la firma digital de una forma algo diferente al procedimiento general descrito anteriormente, la utilización de la función hash se lleva a cabo en el último paso del protocolo ya descrito; es decir, cuando se resuelve la congruencia, por tanto el último paso se modifica como sigue:

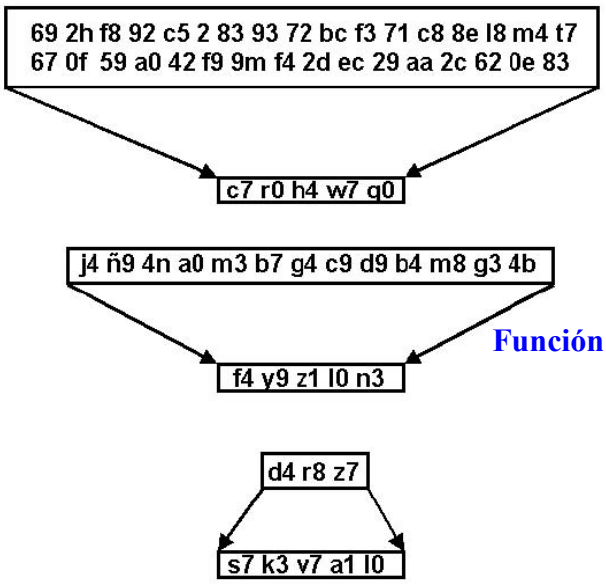
A resuelve la congruencia: $H(m) \equiv a.r + h.s \pmod{\phi(n)}$.

La elección de una función hash para ser utilizada a la hora de firmar digitalmente mensajes debería llevarse a cabo de modo que sea lo suficientemente segura para su uso criptográfico, debiendo ser difícil encontrar un mensaje m cuyo resumen sea un valor dado; además de ser difícil poder encontrar mensajes distintos que proporcionen el mismo resumen. Por otra parte, la longitud del resumen debería ser lo suficientemente larga como para evitar una investigación exhaustiva a una escucha.

El ataque contra una firma digital puede llevarse a cabo por dos medios. El primero consiste en atacar el procedimiento matemático en el que se basa el método de la firma, y el segundo en atacar la función hash utilizada para crear el resumen del mensaje. Por ello, es aconsejable elegir un método para firmar digitalmente y una función hash que requieran esfuerzos comparables para ser rotos.

Las funciones hash más utilizadas con propósitos criptográficos son las llamadas MD2, MD4 y MD5[(69)] propuestas por Rivest y la función SHA-1[(70)]. Las funciones MD producen resúmenes de 128 bits, y la SHA-1, de 160 bits. El único ataque que se conoce contra ellas es el de la investigación exhaustiva.

(69) Message Digest, MD
(70) Secure Hash Algorithm.



Función Hash sha-256 genera una salida de 256 bits

10) La relevancia del cifrado

A la vista de todo lo anteriormente expuesto, se concluye este capitulo con los resultados obtenidos de un estudio publicado en el National Encryption Survey en 2006, acerca de la relevancia del cifrado y su uso generalizado en organizaciones con sede en Estados Unidos.

La principal conclusión obtenida fue que el uso del cifrado se encuentra lejos de su consolidación Efectivamente, el cifrado de información en las organizaciones aún no ha encontrado su lugar entre las prácticas generalizadas de protección, pese a que aquéllas que las incluyen entre sus medidas de salvaguarda confían mucho más en la integridad de sus ficheros personales y sensibles. El estudio demostró que sólo un 4,2% de las compañías incluyen el cifrado en su plan global de seguridad y las que si lo usan, esgrimen como motivo fundamental de ello, la preocupación ante el robo de datos durante un incidente de seguridad y la consiguiente perdida de prestigio, por encima de políticas de cumplimiento.

Dicho estudio, llevado a cabo por el Instituto Ponemon, bajo el patrocinio de una compañía clásica en la materia, "PGP Corporation "tenía como objetivo, evaluar el grado de integración de las técnicas de cifrado en las empresas con sede en EEUU y la percepción que tienen los profesionales sobre su importancia y uso. El informe, también,

abordaba cuestiones como que área es la responsable de obtener e implementar el cifrado, los usos más comunes y las razones que llevan a usarlo, que tipo de datos deben ser protegidos y el nivel de confianza de los participantes en el uso del cifrado a la hora de proteger la información confidencial, personal o sensible.

El estudio constató que los profesionales especializados en seguridad informática y privacidad tienen mayor confianza en los programas de seguridad de sus organizaciones cuando se emplea el cifrado como parte de su plan de implementación en toda la organización.

El 55% de las empresas que utilizan el cifrado de documentos tiene como finalidad la prevención de brechas de seguridad, mientras que el 40% lo hace para proteger la imagen o la reputación de la empresa, el resto argumentaba como motivos: el cumplimiento con la ley Sarbanes-Oxley(71) y evitar tener que notificar a proveedores y empleados la perdida de datos tras un incidente. Por lo tanto, el uso del cifrado a la hora de almacenar o transmitir información es discrecional y dispar, de tal forma que en orden descendente las prioridades en las organizaciones son:

- Cifrar documentos confidenciales que atañen al negocio.
- Las grabaciones que contienen propiedad intelectual o información sensible sobre clientes.
- La información contable y financiera.
- La información que atañe a empleados.

Así pues, el objetivo buscado por la mayoría de empresas e instituciones a la hora de cifrar su información es enviar de forma segura documentos electrónicos de carácter confidencial a otro sistema o ubicación, son muy pocas las que cifran datos en un dispositivo de almacenamiento informático como un servidor o un ordenador portátil y menos aún las que efectúan cifra de archivos o cintas de respaldo de carácter confidencial antes de enviarlas a centros externos de almacenamiento.

(71) http://www.interamericanusa.com/articulos/Leyes/Ley-Sar-Oxley.htm

Una de las aplicaciones más extendidas de las técnicas de cifrado está en la comunicación en modo seguro del navegador de Internet, es decir, cuando el usuario pone https en lugar de http; estableciendo una conexión https el navegador solicita la clave pública del servidor y luego se establece la comunicación mediante algoritmos simétricos. En el caso del correo electrónico cifrado, se sigue el estándar S/MIME que se basa en las normas PKCS#7. Análogamente se aplican cifrados simétricos con claves autogeneradas y luego dichas claves se cifran con algoritmos asimétricos.

Los documentos más sensibles a ser cifrados según la mayoría de las empresas son aquéllos que atañen al negocio, seguidos de cerca por los que contienen información sobre la propiedad intelectual y de clientes. Considerándose menos necesarios de cifrar los sujetos a la información contable y financiera, así como los referidos a los empleados. Entre las cinco categorías de información personal acerca de clientes , consumidores o empleados que ha de ser cifrada se encuentran la información sanitaria, la orientación sexual, el número de la Seguridad Social, miembros de la familia, etc. Alcanzando menos relevancia las direcciones de correo, teléfono y dirección postal, formación académica, etc.

Las normativas y reglamentos con más peso a la hora de tomar la decisión de cifrar información resultaron ser las regulaciones de varios estados norteamericanos y las leyes federales sobre notificación de brechas en la seguridad y pérdida de datos.

Con anterioridad a 1970, la criptografía era demasiado complicada y costosa para su uso diario, pero esto quedo solucionado tras la invención de la clave pública y el microprocesador. Por un lado, la utilización de claves de cifrado públicas y privadas propuestas en 1976 por Diffe, Hellman y Merkle preparó el camino para el uso generalizado de criptografía muy potente. Por otro lado, los microprocesadores rápidos, cada vez más asequibles, dan al usuario medios para realizar los cálculos que este tipo de criptología requiere.

Igualmente, el establecimiento de comunicaciones electrónicas por redes de ordenadores crea la necesidad de preservar el carácter confidencial de las conversaciones y transacciones. La criptografía ofrece una solución a este tipo de problema, y al iniciarse los años noventa, se disponía de criptografía muy efectiva. Pero, también, se

suscitó un acalorado debate político. En Estados Unidos, la administración pretende restringir el uso del cifrado de datos porque teme que delincuentes y espías aprovechen esta técnica para sus torcidos propósitos. La NSA(72) temía no poder descifrar los mensajes de posibles espías y terroristas, por otro lado, el FBI(73) estaba obsesionado con el uso que los delincuentes podían hacer de la criptografía. Por lo que, en los últimos años, ambos organismos han presionado al gobierno de Estados Unidos para que reglamente las técnicas de cifrado y han abogado por mantener las actuales restricciones sobre exportación de soporte informático para criptografía de gran potencia. Sin embargo, esto no es ni será nunca una solución, puesto que a través de Internet pueden encontrarse y de forma gratuita programas criptográficos. Por consiguiente, no es una buena táctica arrinconar un hallazgo técnico por evitar el mal uso que puedan hacer de el unos delincuentes, además, dado que la criptografía proporciona muchos benéficos a la sociedad y que es fundamental para la protección de datos, resulta paradójico que se pretenda crear una sociedad más segura promoviendo leyes que obstaculicen la seguridad al intentar impedir la difusión de sus nuevos avances, Lo lógico será dictar leyes que ayuden a controlar a los individuos desaprensivos que utilizan la criptografía para hacer el mal, de la misma manera que no se prohíbe la venta de cuchillos aunque algunas personas puedan usarlos para cometer asesinatos.

En algún momento se ha optado por soluciones de compromiso, que permitieran utilizar por doquier una criptografía potente, aunque dejando a la policía y servicios de seguridad del estado la facultad de descifrar los mensajes cuando tuvieren la preceptiva autorización legal. En un caso típico, se enviaría junto con cada mensaje una versión cifrada de la clave con la que se ha cifrado ese mensaje. De tal forma que un centro de recuperación de claves autorizado por la policía podrá valerse de una clave maestra directa para descifrar la clave del mensaje, y ésta a su vez se utilizará para descifrar el propio mensaje. No obstante, parece ser que estos sistemas no satisfacen a nadie porque han sido muy fáciles de burlar. Los espías y delincuentes pueden modificar los programas criptográficos para invalidar las facilidades de recuperación de claves, o

(72) Agencia nacional de Seguridad. Encargada de vigilar las comunicaciones electrónicas alrededor del mundo.
(73) Oficina Federal de Investigación de los Estados Unidos

sencillamente tomar de Internet otros programas alternativos. La recuperación de la clave sería, además, muy costosa. Alguien tendría que financiar la ceración, dotación de personal y mantenimiento de los centros dedicados a esa labor. A largo plazo, sin embargo, se pagaría un precio más importante y sutil por el desgaste de la confianza en el Gobierno.

Los sistemas de recuperación de claves, también, tienen riesgos inequívocos para la seguridad. El punto más débil del sistema son las mismas claves maestras, que se convertirán en blanco de espías, delincuentes e incluso funcionarios corruptos. Si éstos lograrán penetrar en un centro de recuperación de claves y robarán una clave maestra de cifrado, podrían descifrar las comunicaciones de Internet y, entonces, millones de datos secretos de empresas, personas y gobiernos quedarían expuestos al robo.

En 1993, El Congreso pidió al Consejo de Investigación Nacional que estudiase la política de Estados Unido sen materia de criptografía. En 1996, se publicó un excelente informe con las siguientes conclusiones:

■ Al hacer balance, las ventajas de una mayor difusión de la criptografía superan a las desventajas.
■ No debe prohibirse por ley la venta ni el empleo de cualquier forma criptográfica dentro de los Estados Unidos.
■ Los controles aplicados a la exportación de criptografía deberán relajarse progresivamente pero no suprimirse.

Los miembros del Consejo de Investigación coincidieron en que la prohibición de la criptografía no sujeta a reglamentación sería incontrolable. No obstante, se sigue haciendo presión a favor de la recuperación de claves y de no relajar los controles de exportación a menos que la clave de recuperación se agregue a los programas exportados.

Sólo con el paso del tiempo, se facilitará la introducción de criptografía potente, cuya reglamentación será cada vez más difícil.

Las consecuencias económicas de la política actual quedan cada vez más claras y con todas estas medidas Estados Unidos se arriesga a perder su liderazgo en la industria de la programación debido a su restrictiva política de exportación.

Finalmente, la capacidad de establecer conversaciones privadas es un derecho democrático esencial. Efectivamente, la democracia se apoya en que los ciudadanos puedan expresar libremente sus opiniones sin temor de ser vigilados ni reprendidos, y ese principio ha de regir tanto en el ciberespacio como en el mundo real, por lo tanto, sí se restringieran los derechos a utilizar la criptografía, esto significaría un claro retroceso en la democracia.

11) Un salto cuántico al futuro

Durante dos mil años, los creadores de cifras han luchado por preservar secretos, mientras que los descifradores se han esforzado por revelarlos. Ha sido siempre una carrera reñida, en la que los descifradores contraatacaron cuando los creadores de cifras parecían ir en cabeza y los creadores de cifras inventaron nuevas y más potentes formas de cifrado cuando los métodos previos se vieron comprometidos. La invención de la criptografía de clave pública y el debate político en torno al uso de la criptografía nos trae al momento presente, y es evidente que los criptógrafos están ganando la guerra de la información. En el momento actual, se vive en una dorada criptografía debido a que es posible crear cifras que están realmente fuera del alcance de todas las formas conocidas de criptoanálisis. Sin embargo todas las cifras que se consideran indescifrables, tarde o temprano han sucumbido al criptoanálisis.

Predecir los avances futuros de cualquier tecnología es siempre una tarea precaria, pero con las cifras es particularmente arriesgada. No sólo se tiene que adivinar que descubrimiento reserva el futuro, sino que también se ha de adivinar que descubrimientos reserva el presente, puesto que puede que haya avances extraordinarios escondidos tras el velo del secreto gubernamental. A continuación se examinarán unas pocas de las ideas futuristas que pueden aumentar o destruir la privacidad en el siglo XXI dando lugar a dos enfoques, el primero considera el futuro del criptoanálisis y una idea en particular que podría permitir que los criptoanalistas descifraran todas las cifras actuales; en cambio, el segundo considera la posibilidad criptográfica más apasionante, un sistema que tiene el potencial de garantizar una privacidad absoluta.

El futuro del criptoanálisis. A pesar de la enorme potencia de RSA y otras cifras modernas, los criptoanalistas aún pueden desempeñar un valioso papel a la hora de recoger inteligencia, hecho demostrado sabiendo que los criptoanalistas están más solicitados que nunca antes en la historia.

Sólo una pequeña fracción de la información que fluye por el mundo está cifrada con seguridad y el resto está mal cifrada o totalmente sin cifrar, debido a que el número de usuarios de Internet está creciendo rápidamente y, sin embargo, muy pocas de estas personas toman precauciones adecuadas en lo referente a la privacidad.

Incluso si los usuarios emplean la cifra RSA correctamente, los descifradores todavía pueden hacer muchas cosas para obtener información de los mensajes interceptados, éstos continúan utilizando viejas técnicas de criptoanálisis tales como el análisis de tráfico. Un avance más reciente es el denominado ataque de tempestad, que trata de detectar las diferentes señales electromagnéticas emitidas por un ordenador cada vez que se teclea una letra. Lo cual permitirá ínter codificado. Para defenderse de los ataques de tempestad existen ya compañías que proveen material protector que se puede usar para revestir las paredes de una habitación e impedir el escape de señales electromagnéticas.

Otros ataques incluyen el uso de caballos de Troya, de tal forma que Y podría diseñar un virus que infecte el software PGP y se instales silenciosamente en el ordenador de X para que cuando X utilice su clave privada para descifrar un mensaje, el virus despierte anote dicha clave para que la siguiente vez que X conecte con Internet, el virus enviaría escondida la clave privada a Y permitiéndole descifrar todos los mensajes siguientes enviados por X. El caballo de Troya, otro truco de software, conlleva que Y diseñe un programa que aparentemente funciones como un producto de codificación genuino, pero que en realidad traiciona al usuario. Una variante del caballo de Troya es un software de codificación completamente nuevo que parece seguro, pero en realidad contiene una puerta trasera, algo que permite a sus diseñadores descifrar los mensajes de todo el mundo.

Aunque el análisis de tráfico, los ataques de tempestad, los virus y los caballos de Troya son técnicas útiles para recoger información, los criptoanalistas son conscientes de

que su verdadero objetivo es encontrar una forma de romper la cifra RSA, la piedra angular de la codificación moderna, por lo que si se proponen desafiarla tendrán que realizar un gran avance teórico o tecnológico. Los criptoanalistas han intentado encontrar un atajo para factorizar (lo que sería un gran avance teórico), un método que reduzca drásticamente el número de pasos necesarios para encontrar p y q, pero hasta ahora todas sus tentativas han acabado en fracaso.

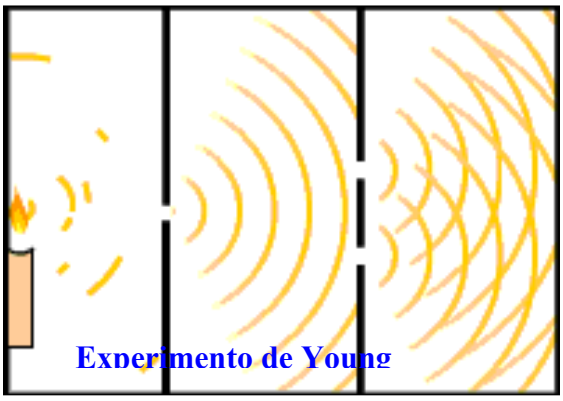
$25 = 5^2$
$180 = 2^2 3^2 5$
$81 = 3^4$
$78439 = 78439$
$225 = 3^2 5^2$
$65980394 = (2)(29)(67)(16979)$

Factorización

Sin mucha esperanza de un gran avance teórico, los criptoanalistas se han visto obligados a buscar una innovación tecnológica. Los chips de silicona seguirán siendo cada vez más rápidos con el paso de los años, aumentando al doble su velocidad aproximadamente cada dieciocho meses, pero esto no es suficiente para causar un impacto verdadero en la velocidad de la factorización dado que, los criptoanalistas necesitan una tecnología que sea billones de veces más rápida que los ordenadores actuales, por lo que están anhelando una forma radicalmente nueva de ordenador: el ordenador cuántico. Si los científicos pudieran construir un ordenador cuántico, sería capaz de realizar cálculos a una velocidad tan tremenda que haría que un superordenador moderno pareciera un ábaco roto.

Para explicar los principios de la informática cuántica,(74) resulta útil remontarse a finales del siglo XVIII y observar el trabajo de Thomas Young, quien realizó el primer gran avance en el desciframiento de los jeroglíficos egipcios.

(74) Niels Bohr, uno de los padres de la mecánica cuántica afirmó: cualquiera que pueda contemplar la mecánica cuántica sin sentir vértigo es que no la ha comprendido, Se basa en ideas potencialmente extrañas.


Experimento de Young

En su experimento realizado en 1799, Young había hecho brillar una luz sobre una mampara en la que habría dos estrechas aberturas verticales; en una pantalla situada a cierta distancia detrás de las aberturas, Yong esperaba ver dos rayas brillantes, proyecciones de las aberturas. En vez de ello, observó que la luz se desplegaba desde las dos aberturas y formaba un patrón de varias rayas de luz y rayas oscuras sobre la pantalla; dicho patrón lo había desconcertado, pero más adelante pudo explicarlo: Young comenzó suponiendo que la luz era un tipo de onda y si la luz emanaba de las dos aberturas se comportaba como las ondas, y fue descubriendo una compresión más profunda de la verdadera naturaleza de la luz publicando posteriormente "La teoría ondulatoria de la luz", un clásico sin antecedentes entre los artículos de física.

Hoy día sabemos que la luz se comporta efectivamente como una onda, pero sabemos que también puede comportarse como una partícula; que percibamos la luz como una onda o como una partícula depende de las circunstancias, y esta ambigüedad de la luz se conoce como la dualidad onda-partícula. Mencionando también que la física moderna considera que un rayo de luz consta de innumerables partículas individuales, conocidas como fotones, que presentan propiedades como de onda, por lo que se puede interpretar el experimento de Young en términos de fotones que se desbordan por las aberturas y luego reaccionan entre sí al otro lado de la mampara.

Hasta ahora no hay nada de particular en el experimento de Young, sin embargo, la tecnología moderna permite a los físicos repetir el experimento de Young utilizando un filamento que es tan tenue que emite fotones únicos de luz. Con sólo un fotón pasando cada vez por las aberturas no esperaríamos ver el patrón rayado observado por Young, porque ese fenómeno parece depender de que dos fotones atraviesen simultáneamente aberturas diferentes y se mezclen al otro lado. En vez de ello, se podría esperar ver sólo dos rayas de luz, que serían simplemente la proyección de las aberturas de la mampara; sin embargo, por una razón extraordinaria, incluso con fotones únicos el

resultado sobre la pantalla sigue siendo un patrón de rayas de luz y oscuridad, igual que si los fotones hubieran estado mezclándose.

Este extraño resultado desafía el sentido común, puesto que no hay manera de explicar el fenómeno en función de las leyes clásicas de la física, la cual puede explicar las órbitas de los planetas o la trayectoria de una bala de cañón, pero no puede describir completamente el mundo de lo verdaderamente diminuto, como la trayectoria de un fotón, por lo que para explicar semejantes fenómenos de los fotones, los físicos recurren a la teoría cuántica, una explicación de cómo se comportan los objetos a nivel microscópico. Sin embargo, incluso los físicos cuánticos no se pueden poner de acuerdo sobre cómo interpretar este experimento tendiendo a dividirse en dos bandos opuestos, cada uno con su propia interpretación.

El primer bando propone una idea conocida como superposición en la cual se comienza afirmando que sólo se sabe con seguridad dos cosas sobre el fotón, que sale del filamento y que va a dar a la pantalla. Todo lo demás es un completo misterio incluido si el fotón pasó por la abertura izquierda o por la derecha. Debido a que la trayectoria del fotón es desconocida, los superposicioncitas adoptan el peculiar punto de vista de que, de laguna forma, el fotón pasa por las dos aberturas simultáneamente, lo que le permite inferir consigo mismo y crear el patrón rayado que se observa en la pantalla. Los argumentos se basa en que no se sabe si el fotón pasó por la abertura izquierda o por la derecha, de modo que se asume que pasó por las dos aberturas al mismo tiempo, dado que si no se sabe lo que está haciendo una partícula, entonces puede hacer cualquier cosa posible simultáneamente. Cada posibilidad se denomina un estado, y cómo el fotón cumple ambas posibilidades, se dice que está en una superposición de estados. En cambio, el anticuado punto de vista clásico del fotón (debe haber pasado por una de las dos aberturas y simplemente no se sabe por cuál) a pesar de ser mucho más sensato que el punto de vista cuántico, no puede explicar el resultado final. La teoría cuántica establece que una superposición reúne todas las posibilidades y sucede sólo cuando se pierde de vista un objeto siendo una manera de describir ese objeto durante un período de ambigüedad.

El segundo bando cuántico se basa en la interpretación de los mundos múltiples, la cual afirma que al salir del filamento el fotón tiene dos opciones, pasar por la abertura

izquierda o por la derecha y en es preciso momento el universo se divide en dos universos, en un universo el fotón pasa por la abertura izquierda y en el otro universo pasa por la abertura derecha interfiriendo estos dos universos de alguna forma entre sí, explicando así el patrón rayado. Los seguidores de este bando creen que cada vez que un objeto tiene el potencial de entrar en uno de entre varios estados posibles, el universo se divide en muchos universos, de modo que cada potencial se realiza en un universo diferente denominándose multiverso.

Independientemente del bando adoptado, la teoría cuántica es una filosofía desconcertante; a pesar de ello, a demostrado ser la teoría científica más práctica y con más éxito jamás concebida. Además de su capacidad única para explicar el resultado del experimento de Young, la teoría cuántica explica satisfactoriamente muchos otros fenómenos, siendo la única teoría que permite a los físicos calcular las consecuencias de las reacciones nucleares en las centrales eléctricas, explicar el milagro del ADN, explicar cómo brilla el sol, y sólo ella se puede utilizar el láser que lee los CD, por lo tanto se vive en un mundo cuántico.

De todas las consecuencias de la teoría cuántica, la más importante tecnológicamente es potencialmente el ordenador cuántico, puesto que además de eliminar la seguridad de todas las cifras modernas, el ordenador cuántico anunciaría una nueva era de potencia informática. Uno de los pioneros de la informática cuántica es David Deutsch, un físico inglés que comenzó a trabajar con ese concepto en 1984, el cual estaba convencido de que los ordenadores deberían obtener

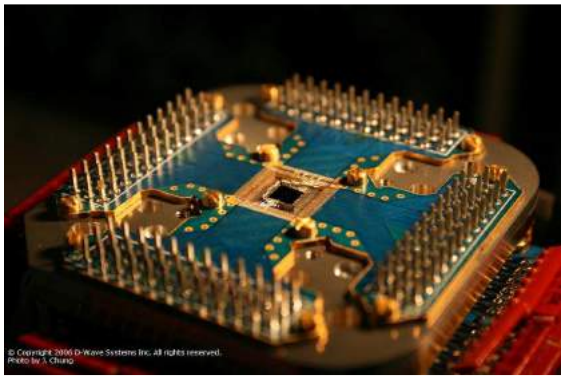
Las leyes de la física cuántica, porque las leyes cuánticas son más fundamentales. En el nivel microscópico, dichas leyes se nos muestran en su verdadero misterio y un ordenador construido para sacar partido a estas leyes se comportaría de una manera drásticamente nueva. En un artículo

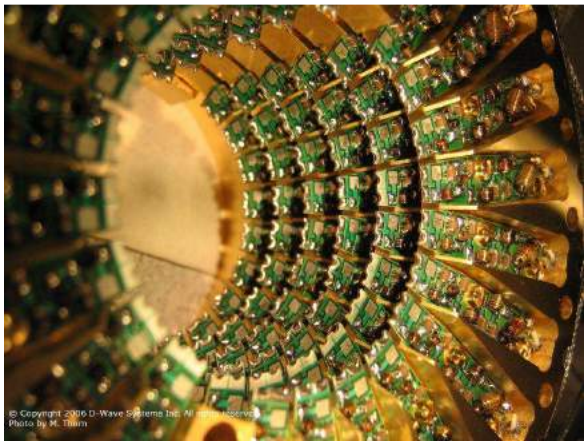
David Deutsch

publicado en 1985 describió su visión de un ordenador cuántico que funcionaría de acuerdo a las leyes de la física cuántica, en particular, explicó en que se diferenciaba su

ordenador cuántico de un ordenador corriente. Sea cual sea la interpretación de la teoría cuántica, el ordenador cuántico puede tratar dos preguntas al mismo tiempo sacando partido a las leyes de la física cuántica.

Una forma de representar los números es en términos de partículas giratorias, puesto que muchas partículas fundamentales poseen un giro inherente y pueden girar hacia el este o el oeste. Una secuencia de estas partículas representa una





ordenador cuántico

secuencia de 1s y 0s, o un número binario. Un ordenador cuántico desafía el sentido común. Ignorando los detalles por un momento , un ordenador cuántico se puede considerar de dos maneras diferentes,

Dependiendo de qué interpretación cuántica se prefiera. Algunos físicos consideran el ordenador cuántico como una única entidad que realiza el mismo cálculo simultáneamente con 128 números; otros lo consideran como 128 entidades, cada una de ellas en un universo diferente y cada una realizando sólo un cálculo. La informática cuántica es tecnología de La zona oscura.

Como un ordenador cuántico funciona con 1s y 0s que están en una superposición cuántica se denominan bits cuánticos o qubits(75). La ventaja de los qubits queda aún más de manifiesto cuando se consideran partículas.

Sacar partido a efectos cuánticos podría dar lugar a ordenadores cuánticos de una potencia inimaginable. Por desgracia cuando Deutsch creó su visión de un ordenador cuántico a mediados de los años ochenta, nadie podía imaginar como construir una máquina sólida, práctica, con esas características. Uno de los mayores obstáculos era

(75) Término creado por Schumacher en 1995, como abreviatura de quantum bit, bit cuántico.

mantener una superposición de estados a lo largo de todo el cálculo, debido a que un átomo disperso que infiriese con una de las partículas giratorias rompería la superposición llevándola a un solo estado, haciendo que fracasara el cálculo cuántico. Otro problema era que los científicos no sabían como programar un ordenador cuántico y, por tanto, no estaban seguros de qué tipo de cómputos podría ser capaz de realizar. Sin embargo en 1994, Peter Shor logró definir un programa útil para un ordenador cuántico, siendo la noticia extraordinaria para los criptoanalistas dado que el programa de Shor definía una serie de pasos que un ordenador cuántico podía seguir para factorizar un número gigante, justo lo que se requería para romper la cifra RSA; desgraciadamente, Shor no podía demostrar su programa de factorización porque todavía no existía nada parecido a un ordenador cuántico.

$ax + ay + az = a(x + y + z)$

$x^2 - y^2 = (x + y)(x - y)$

$x^2 + (a + b)x + ab = (x - a)(x + b)$

$x^2 + 2xy + y^2 = (x - y)^2$

$x^2 - 2xy + y^2 = (x - y)^2$

$acx^2 + (ad + bc)xy + bdy^2 = (ax + by)(cx + dy)$

$x^3 + y^3 = (x + y)(x^2 - xy + y^2)$

$x^3 - y^3 = (x - y)(x^2 - xy + y^2)$

Factorización

Factorizar:

$p_1(x) = x^3 - 10x^2 + 25x$

$p_2(x) = 3x^3 + 18x^2 + 27x$

$p_3(x) = 4x^3 - 36x$

$p_4(x) = 4x^4 + 16x^3 + 16x^2$

Solución:

1) $p_1(x) = \square \cdot (x^2 - 10x + \square) = \square \cdot (\square)^2$

2) $p_2(x) = \square \cdot (x^2 + \bigcirc x + 9) = \square \cdot (\square)^2$

3) $p_3(x) = \square \cdot (x^2 - \bigcirc) = \square \cdot (x + 3) \cdot (\square)$

4) $p_4(x) = \square x^2 \cdot (x^2 + \square x + 4) = \square x^2 \cdot (\square)^2$

Después, en 1996, Lov Grover descubrió otro poderoso programa, el cual es una forma de buscar una lista a una velocidad increíblemente alta, lo que puede que no suene particularmente interesante hasta que uno se da cuenta de que eso es exactamente lo que se quiere para descifrar una cifra DES, dado que su ruptura implica necesariamente buscar una lista de todas las claves posibles para encontrar la correcta. Un ordenador que utilice el programa de Grover podría encontrar la clave en menos de cuatro minutos.

Es una mera coincidencia que los dos primeros programas para ordenador cuántico que se han inventado hayan sido exactamente lo que los criptoanalistas habían puesto en primer lugar en su lista de deseos. Aunque los programas de Shor y Grover produjeron un optimismo enorme entre los descifradores, hubo también una inmensa frustración, porque todavía no existía algo como un ordenador cuántico operativo que pudiera hacer funcionar estos programas. Aunque varios avances recientes han subido la

moral de los investigadores, puede decirse que la tecnología sigue siendo notablemente primitiva.

Sólo el tiempo dirá si se pueden superar los problemas para construir un ordenador cuántico, y de ser así, cuándo. Mientras tanto, lo único que se puede hacer es especular sobre el impacto que tendría en el mundo de la criptografía. Desde los años setenta, los creadores de cifras han llevado una clara delantera en la carrera contra los descifradores, gracias a cifras como DES y RSA; según se entra en el siglo XXI, más y más comercio se llevará a cabo en Internet, y el mercado electrónico dependerá de cifras fuertes para proteger y verificar las transacciones financieras. Según la información se convierte en la mercancía más valiosa del mundo, el destino económico, político y militar de las naciones dependerá de la fortaleza de las cifras.

Por consiguiente, el desarrollo de un ordenador cuántico totalmente operativo pondría en peligro nuestra privacidad personal, destruiría el comercio electrónico y demolería el concepto de la seguridad nacional, en otras palabras, haría peligrar la estabilidad del mundo.


Ordenador cuántico

Aunque aún está en pañales, la informática cuántica presenta una amenaza potencial al individuo, los negocios internacionales y la seguridad global.

Aplicaciones de la computación cuántica al criptoanálisis. Los ordenadores cuánticos son potencialmente útiles para el criptoanálisis. Debido a que los estados cuánticos pueden existir en una superposición (es decir, estar entrelazados), es posible un nuevo paradigma computacional, en el que un bit no representa tan sólo los estados 0 y 1, sino cualquier combinación lineal de estos. Peter Shor de los Laboratorios Bell probó la posibilidad, y varios equipos han demostrado uno u otro aspecto de la computación cuántica en los años transcurridos desde entonces. Por el momento, sólo se ha demostrado una muy limitado prueba de posibles diseños. No hay, a fecha de 2006, una perspectiva creíble de un ordenador cuántico real y utilizable.

Sin embargo, de construirse un ordenador cuántico, muchas cosas cambiarían. La computación en paralelo sería probablemente la norma, y varios aspectos de la criptografía cambiarían.

En particular, dado que un ordenador cuántico sería capaz de realizar búsquedas de claves mediante fuerza bruta extremadamente rápidas, tamaños de clave considerados hoy en día más allá de los recursos de cualquier atacante por fuerza bruta quedarían al alcance de este ataque. Los tamaños de clave necesarios para quedar más allá de la capacidad de un ordenador cuántico serían considerablemente más grandes que los actuales. Algunos escritores de divulgación han declarado que ningún cifrado permanecería seguro de estar disponibles los ordenadores cuánticos. Otros aseguran que simplemente añadiendo bits a las longitudes de las claves evitará los ataques de fuerza bruta, incluso con ordenadores cuánticos.

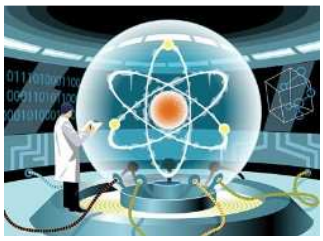
Una segunda posibilidad es que el aumento en capacidad computacional pueda hacer posibles otros ataques de búsqueda de claves, más allá de la simple fuerza bruta, contra uno o varios de los algoritmos actualmente inexpugnables. Por ejemplo, no todo el progreso en la factorización de números primos se ha debido a una mejora de los algoritmos. Una parte se debe al incremento del poder computacional de los ordenadores, y la existencia de un ordenador cuántico en funcionamiento podría acelerar considerablemente las tareas de factorización. Este aspecto es bastante predecible, aunque no claramente. Lo que no puede ser anticipado es un avance en el campo teórico que requiera la computación cuántica, que pudiera hacer realizables ataques actualmente impracticables o incluso desconocidos. En ausencia de un método para predecir estos avances, sólo nos queda esperar.

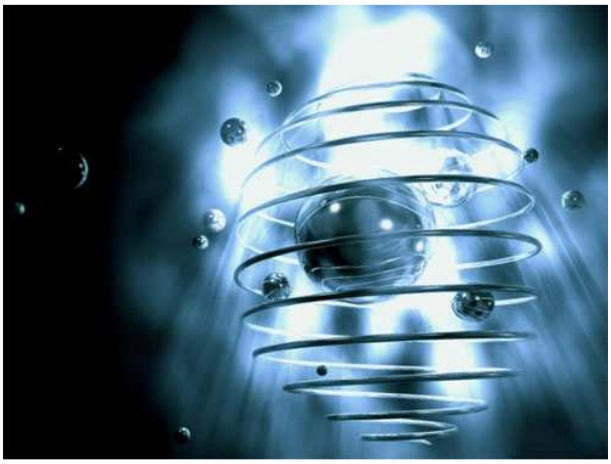
Se desconoce si existe un método de cifrado en tiempo polinómico que requiera un tiempo exponencial para su descifrado, incluso para un ordenador cuántico.

La criptografía cuántica. Mientras los criptoanalistas esperan la llegada de los ordenadores cuánticos, los criptógrafos están ocupándose de su propio milagro tecnológico: un sistema de cifrado que restableciera la privacidad, incluso si tuviera que hacer frente a la fuerza de un ordenador cuántico. Esta nueva forma de codificación es fundamentalmente diferente a cualquiera de las que se conocen anteriormente, ya que ofrece la esperanza de una privacidad perfecta, lo que en otras palabras quiere decir, que

este sistema nos tendría ningún defecto y garantizaría una seguridad absoluta para toda la eternidad. Además, de basarse en cifrado en flujo usando fotones como bits, se fundamenta en la teoría cuántica, la misma que constituye el fundamento de los ordenadores cuánticos.

Los ordenadores cuánticos nos miran desde la vuelta de la esquina



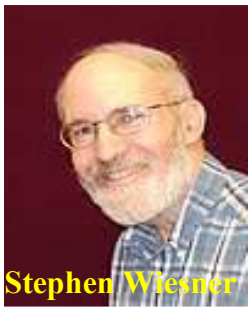


Nueva forma de probar los componentes ópticos que podrían algún día usarse para construir ordenadores cuánticos. Técnica mucho más simple que las pruebas convencionales porque usa una luz láser estándar, en lugar de depender de la creación de fotones en estados cuánticos especiales.

Mientras la teoría cuántica constituye la inspiración para un ordenador que podría descifrar todas las cifras actuales está también en el centro de una nueva cifra indescifrable denominada criptografía cuántica.

La historia de la criptografía cuántica se remonta a una curiosa idea desarrollada a finales de los años sesenta por Stephen Wiesner, el cual el cual acababa de inventar el concepto del dinero cuántico, que tenía la gran ventaja de ser imposible de falsificar.

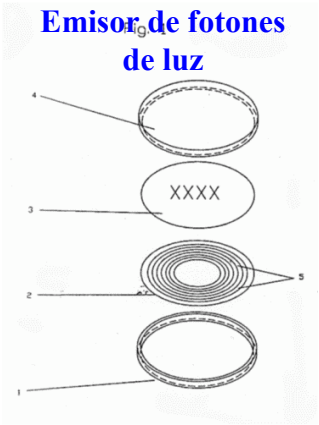
El dinero cuántico de Wiesner se basaba enormemente en la física de los fotones. El ángulo de vibración se conoce como la polarización del fotón, y una bombilla genera fotones con todas las polarizaciones, lo que significa que algunos fotones vibrarán hacia arriba y abajo, otros de un lado a otro y otros en ángulos intermedios.



Stephen Wiesner

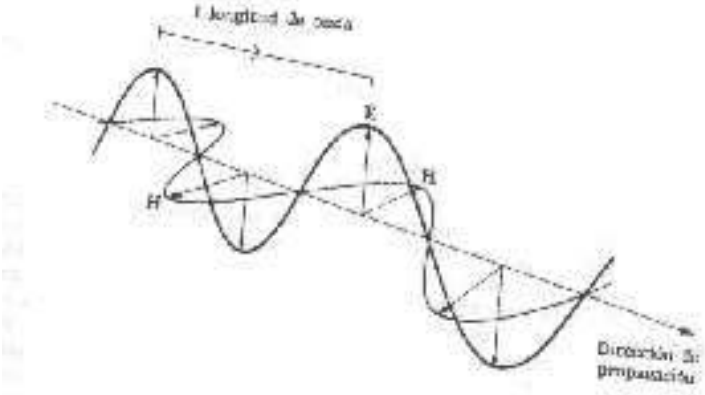
Colocando un filtro, conocido como Polaroid, en la trayectoria de los fotones, es posible asegurar que el rayo de luz que sale se compone de fotones que vibran en una dirección particular; en otras palabras,

todos los fotones tienen la misma polarización. Cualquier fotón que ya esté polarizado en la misma dirección del filtro Polaroid pasará automáticamente por él sin modificarse y los fotones que estén polarizados perpendicularmente al filtro quedarán bloqueados. Los fotones polarizados diagonalmente están en un dilema cuántico cuando afrontan un filtro Polaroid vertical, es puro azar, la mitad de ellos quedará bloqueada y la otra mitad pasará, y los que pasen estarán reorientados con una polarización vertical.



Wiesner planeó usar la polarización de los fotones para crear billetes de dólar que nunca pudieran ser falsificados, debido a la idea de que dichos billetes contuvieran 20 trampas de luz, diminutos aparatos que son capaces de capturar y retener un fotón. El banco emisor puede identificar cada billete según su secuencia de polarización y su número de serie impreso, y guardaría una lista maestra de los números de serie y las correspondientes secuencias de polarización.

La luz se polariza en ejes ortogonales



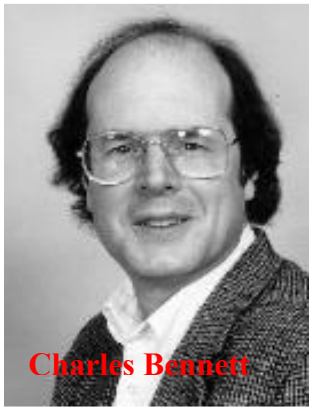
Para crear una falsificación eficaz, el falsificador debe usar un billete genuino como muestra, precisar de alguna manera sus 20 polarizaciones y luego duplicar el billete, reproduciendo el número de serie y cargando las trampas de luz de forma adecuada. Sin embargo, precisar las polarizaciones de los fotones es una tarea notoriamente difícil, y si el falsificador no puede precisarlas exactamente en el billete de muestra no puede esperar duplicarlas. El problema del falsificador es que debe utilizar la

orientación correcta del filtro Polaroid para identificar la polarización de un fotón, pero no sabe que orientación usar porque no conoce la polarización del fotón.

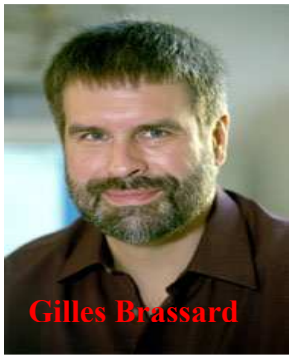
La dificultad de precisar fotones es un aspecto del principio de incertidumbre, desarrollado por el físico alemán Werner Heisenberg en los años veinte, el cual sostiene que es lógicamente imposible precisar todos los aspectos de un objeto particular con toda exactitud, lo que en nuestro caso se traduce diciendo que es imposible precisar todos los aspectos de los fotones que hay en las trampas de luz, siendo este principio otra extraña consecuencia de la teoría cuántica.

Por tanto, se llega a la conclusión de que el dinero cuántico es una idea brillante, siendo también una idea totalmente inviable. Para empezar, los ingenieros no han creado todavía la tecnología para atrapar fotones en un estado polarizado particular durante un período de tiempo lo suficientemente largo, incluso si existiera la tecnología resultaría demasiado caro ponerla en práctica.

Parecía que sólo había una persona que compartía el entusiasmo de Wiesner por el dinero cuántico; se trataba de un viejo amigo llamado Charles Bennett, en quien Wiesner confió que apreciaría el dinero cuántico y le entregó una copia de su manuscrito. A Bennett le fascinó inmediatamente el concepto y lo consideró una de las ideas más bellas que había visto.

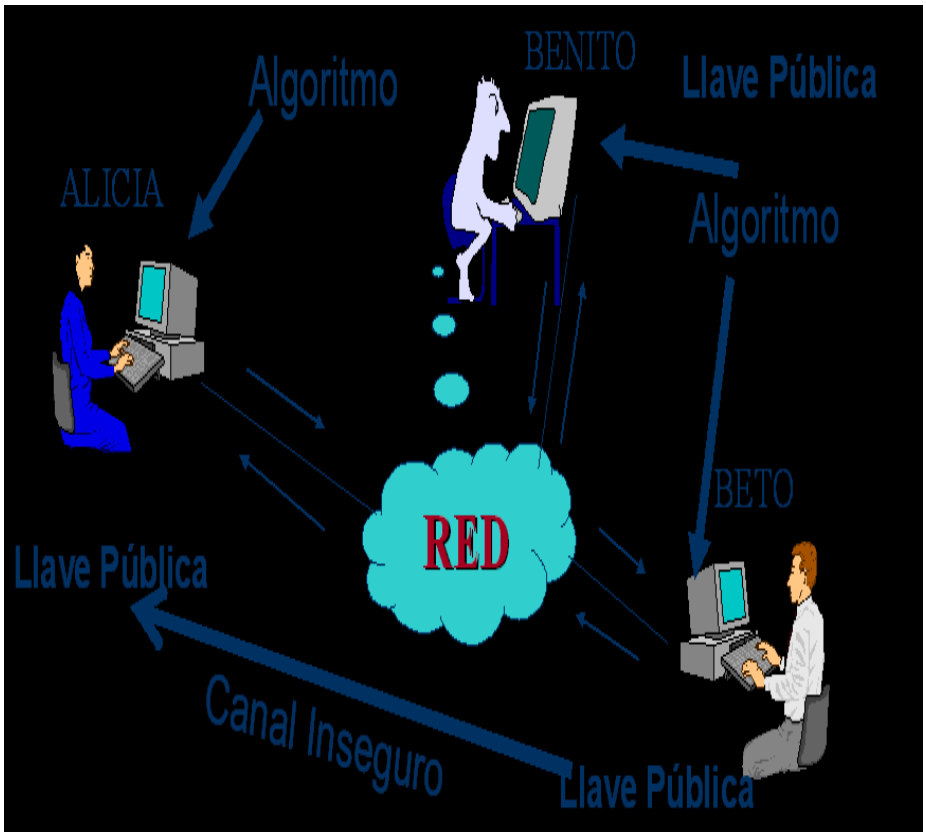

Charles Bennett

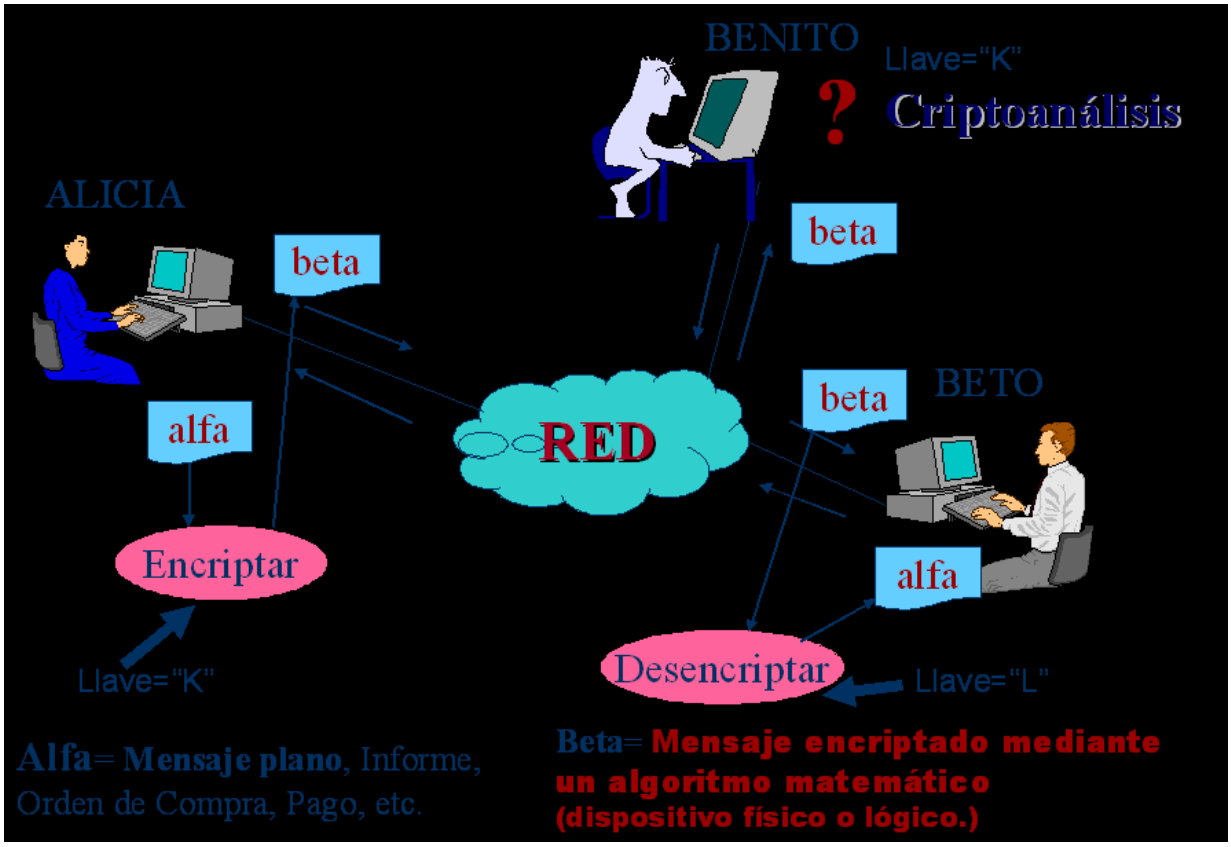
Un día, Bennett le explicó el concepto del dinero cuántico a Gilles Brassard, un científico de la informática. Bennett y Brassard, poco a poco empezaron a ver que la idea de Wiesner podría tener una aplicación en criptografía.

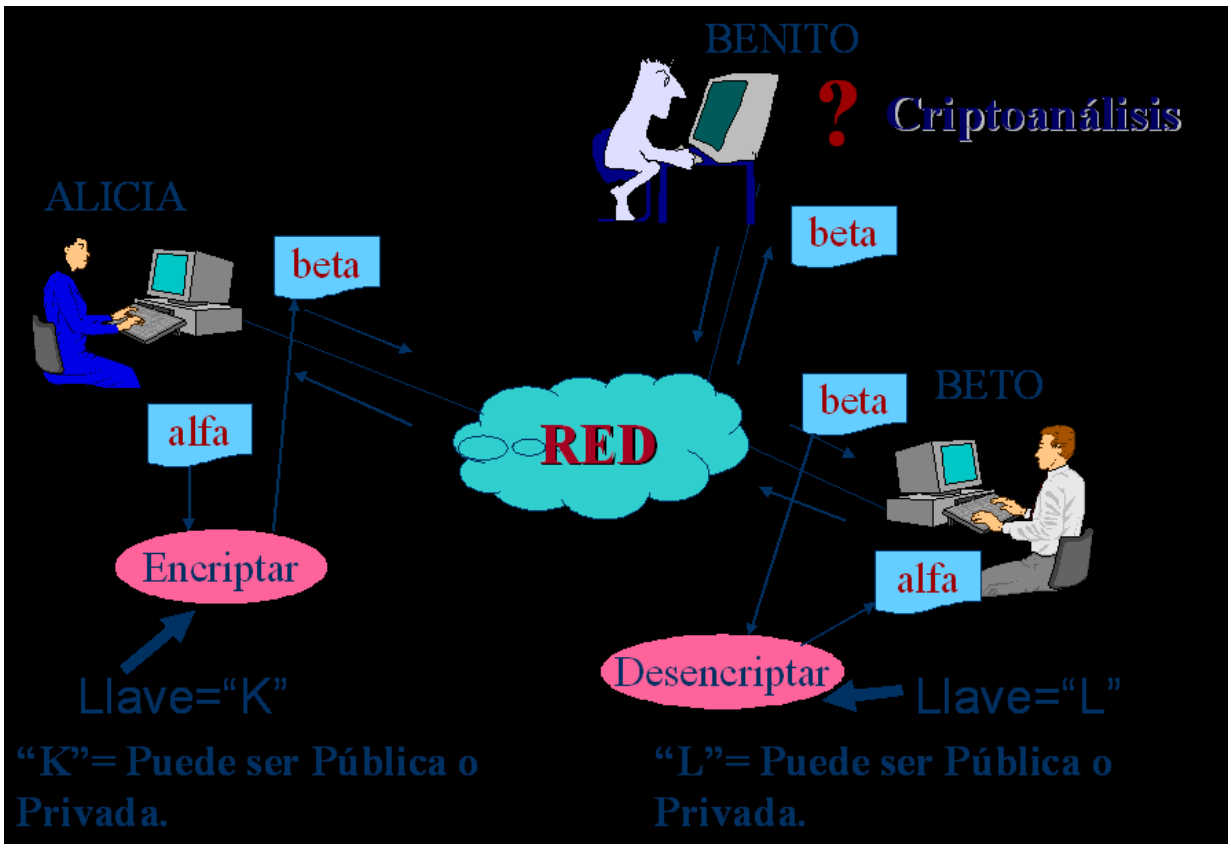

Gilles Brassard

Para que Y descifre un mensaje cifrado entre X y Z, primero debe interceptarlo, lo que significa que de laguna manera debe percibir con exactitud el contenido de la transmisión. El dinero cuántico de Wiesner era seguro, porque resultaba imposible percibir con exactitud las polarizaciones de los fotones atrapados en los billetes.

Bennett y Brassard comenzaron a crear un sistema, el cual parece tener algunos rasgos agradables. Y no puede estar segura de estar interceptando con exactitud el mensaje cifrado, de modo que no puede tener esperanzas de descifrarlo; sin embargo, el sistema tiene un problema grave y aparentemente insuperable: Z se encuentra en la misma situación que Y, en cuanto a que no tiene ninguna manera de saber que esquema de polarización está utilizando X para cada fotón, de modo que también él interpretará erróneamente el mensaje. La solución obvia al problema es que X y Z se pongan de acuerdo en el esquema de polarización que usarán para cada fotón; de alguna forma X tiene que hacer llegar de manera segura a Z la lista de los esquemas de polarización. Por supuesto X podría cifrar dicha lista utilizando una cifra de clave pública como RSA y luego transmitírsela a Z.




BENITO
Llave="K"
?
Criptoanálisis
ALICIA
beta
beta
beta
BETO
alfa
RED
Encriptar
alfa
Llave="K"
Desencriptar
Llave="L"
Alfa= Mensaje plano, Informe, Orden de Compra, Pago, etc.
Beta= Mensaje encriptado mediante un algoritmo matemático (dispositivo físico o lógico.)


BENITO
?
Criptoanálisis
ALICIA
beta
beta
beta
BETO
alfa
RED
Encriptar
alfa
Llave="K"
Desencriptar
Llave="L"
"K"= Puede ser Pública o Privada.
"L"= Puede ser Pública o Privada.

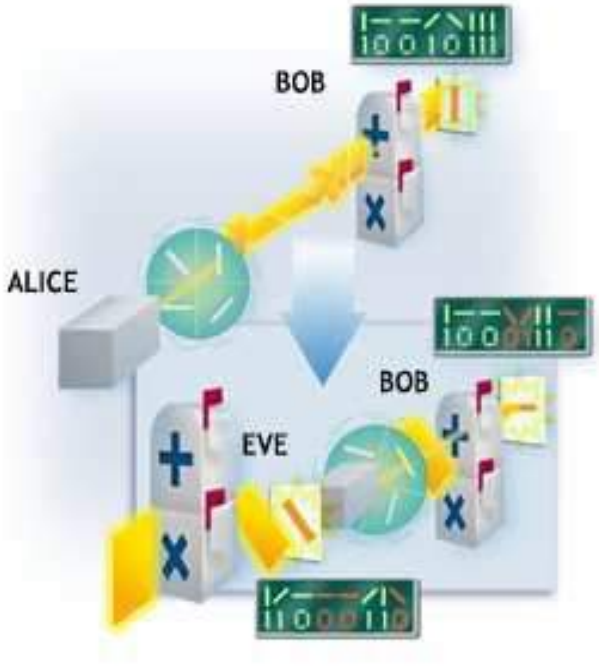
Sin embargo imaginamos que estamos en una era en la que RSA ha sido descifrada, quizá a raíz del desarrollo de poderosos ordenadores cuánticos, debido a que el sistema de Bennett y Brassard tiene que ser autosuficiente y no depender de RSA. Durante meses trataron de pensar una forma de solucionar el problema de la distribución de la clave. Entonces en 1984, en un momento de ¡eureka! Crearon la criptografía cuántica, la forma más segura de criptografía jamás concebida. Su receta para la criptografía cuántica requiere tres fases preparatorias que no conllevan enviar un mensaje cifrado pero permiten el intercambio seguro de una clave que luego se puede usar para cifrar un mensaje.

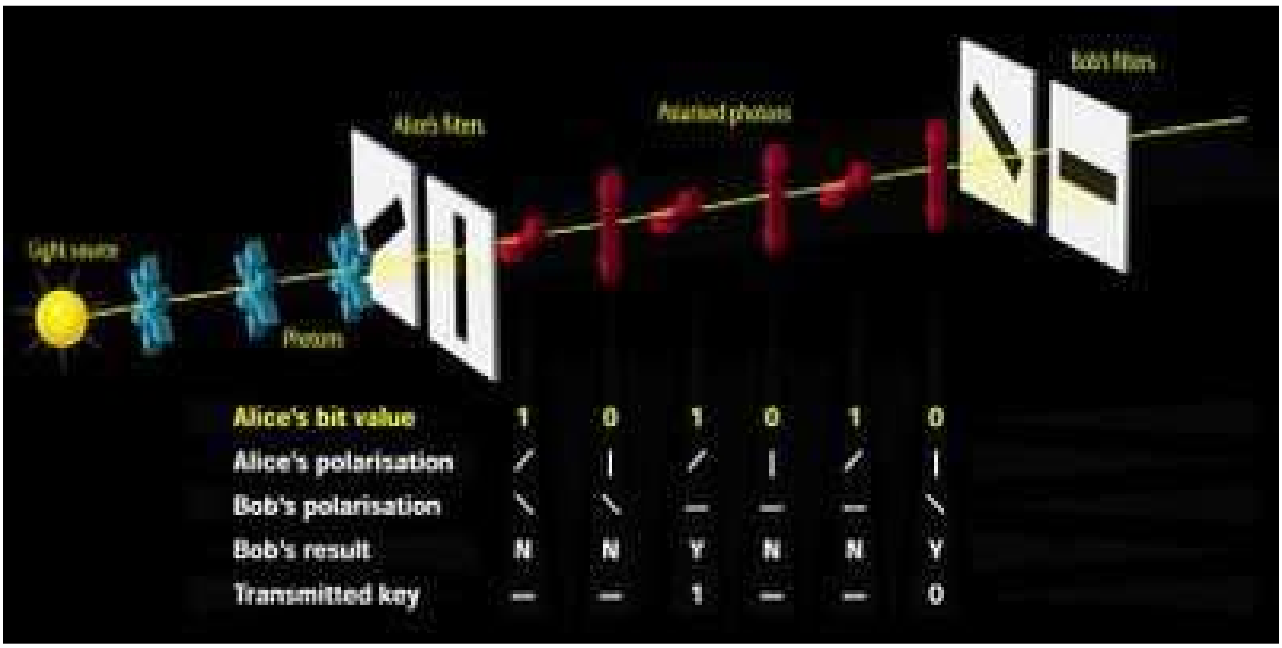
■ Fase 1. X comienza por transmitir una secuencia aleatoria de 1s y 0s utilizando una elección aleatoria de esquemas de polarización rectilíneos (horizontal y vertical) y diagonales.

■ Fase 2. Z tiene que precisar las polarizaciones de estos fotones, pero como no tiene ni idea de qué esquema de polarización ha usado X para cada uno de ellos alterna aleatoriamente. Si Z usa el detector erróneo, puede interpretar erróneamente el fotón de X.

■ Fase 3. Hasta el momento, X ha enviado una serie de 1s y 0s, y Z ha detectado algunos de ellos correctamente y otros erróneamente, por lo que para aclarar la situación, X llama por teléfono a Z en una línea corriente y poco segura y le dice que esquemas de polarización utilizó para cada fotón, pero no le dice cómo polarizó cada fotón; Z le dice entonces en que ocasiones ha adivinado el esquema de polarización correcto. Finalmente, X y Z ignoran todos los fotones para los que Z utilizó el esquema erróneo y se centran tan sólo en aquellos para los que se adivinó el esquema correcto, por lo que de hecho se ha generado una secuencia más corta de bits, que se compone solamente de las mediciones correctas de Z.

Estas tres fases han permitido a X y Z establecer una serie común de dígitos, siendo la propiedad crucial de esta secuencia aleatoria, porque se deriva de la secuencia inicial de X, que es en sí misma aleatoria; además las ocasiones en las que Z utiliza el detector correcto son también aleatorias, por lo que la secuencia acordada no constituye ningún mensaje, pero podría servir como clave aleatoria. Por fin puede comenzar el verdadero proceso de cifrado seguro.





Esta secuencia aleatoria acordada puede utilizarse como clave para una cifra de cuaderno de uso único absolutamente indescifrable. Previamente, el único problema con la cifra de cuaderno de uso único era la dificultad de distribuir de una manera segura las series aleatorias, pero el plan de Bennett y Brassard resuelve este problema. X y Z han

acordado un cuaderno de uso único y las leyes de la física cuántica no permiten que Y lo intercepte con éxito.

Otra manera de entender la criptografía cuántica es considerándola desde el punto de vista de una baraja de cartas (76) en vez de fotones polarizados. Cada carta tiene un valor y un palo, y normalmente, se puede mirar una carta y ver tanto el valor como el palo al mismo tiempo.

La criptografía cuántica permite que X y Z acuerden una clave, que Y no puede interceptar sin cometer errores; además dicha criptografía tiene una ventaja adicional: ofrece a X y Z una manera de descubrir si Y está escuchan subrepticiamente, debido a que su presencia en la línea se evidencia porque cada vez que mide un fotón se arriesga a alterarlo, y estas alteraciones les resultan obvias a X y Z. La revisión de errores se lleva a cabo después de las tres fases preliminares, y para entonces X y Z deberían tener secuencias idénticas de 1s y 0s.

Para resumir, la criptografía cuántica es un sistema que garantiza la seguridad de un mensaje dificultando que Y pueda leer con exactitud una comunicación entre X y Z, teniendo además la ventaja añadida de que si Y intenta escuchar subrepticiamente, X y Z podrán detectar su presencia. Por tanto, la criptografía cuántica permite que X y Z intercambien y acuerden un cuaderno de uso único con completa privacidad para luego utilizarlo como clave para cifrar un mensaje. El procedimiento tiene cinco fases básicas:

■ Fase 1. X envía a Z una serie de fotones y Z los precisa.

■ Fase 2. X le dice a Z en qué ocasiones los midió correctamente.

■ Fase 3. X y Z desechan las mediciones que Z realizó erróneamente y se centran el la que hizo correctamente para crear un para idéntico de cuadernos de uso único.

■ Fase 4. X y Z prueban la integridad de sus cuadernos de uso único revisando algunos de los dígitos.

(76) Para verlo detalladamente consultar la bibliografía adjunta de este proyecto, dado que esta información se encuentra en uno de los libros.

■ Fase 5. Si el proceso de verificación es satisfactorio pueden usar el cuaderno de uso único para cifrar un mensaje; si la verificación revela errores saben que los fotones estaban siendo interceptados por Y, por lo que necesitan empezar de nuevo desde el principio.

Catorce años después de que el artículo de Wiesner sobre el dinero cuántico hubiera sido rechazado por las revistas científicas había inspirado un sistema de comunicación absolutamente seguro, dando por tanto alivio Wiesner porque por fin su trabajo está siendo reconocido.

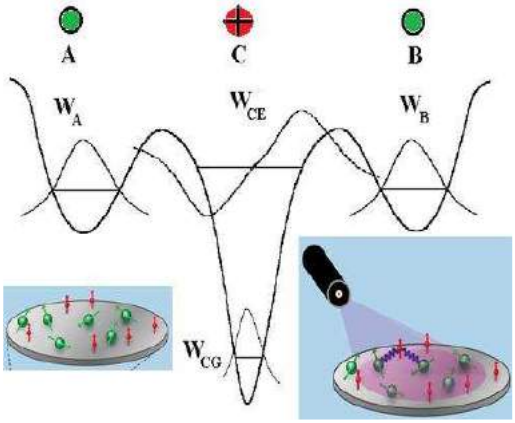
Los criptógrafos recibieron la criptografía cuántica de Bennett y Brassard con entusiasmo; sin embargo muchos experimentadores alegaron que el sistema funcionaba bien en teoría, pero que fracasaría en la práctica, basándose en que creían que la dificultad de tratar con fotones individuales haría que el sistema resultara imposible de poner en práctica. A pesar de las críticas Bennett y Brassard estaban convencidos de que se podría hacer que la criptografía cuántica funcionara, teniendo tanta fe en su sistema que no se molestaron en construir el aparato.

Sin embargo, en 1988 Bennett comenzó a reunir los componentes que necesitaría para un sistema criptográfico cuántico y tomó un estudiante de investigación John Smolin, para que lo ayudara a montar el aparato, se propusieron la tarea de intentar enviar fotones polarizados de un lado al otro de la habitación, para luego precisarlos. Un ordenador denominado X controla la transmisión de fotones y un ordenador denominado Z decidía que detector debía utilizarse para precisar cada fotón. Tras horas, Bennett presenció el primer intercambio criptográfico cuántico en el que X y Z lograron enviar y recibir fotones, discutieron los esquemas de polarización que había usado X, desecharon los fotones que Z había precisado utilizando el detector erróneo y acordaron un cuaderno de uso único consistente en los fotones restantes. El experimento de Bennett había demostrado que dos ordenadores, X y Z, se podían comunicar en absoluto secreto, siendo un experimento histórico, a pesar del hecho de que los dos ordenadores estuvieran a una distancia de sólo 30 cm.

Desde el experimento de Bennett, el desafío ha sido construir un sistema criptográfico cuántico que opere entre distancias útiles, no siendo esta tarea nada insignificante, puesto que los fotones no viajan bien. Un medio más eficaz para transmitir fotones es a través de una fibra óptica y recientemente los investigadores han logrado utilizar esta técnica para construir sistemas criptográficos cuánticos que operan a través de grandes distancias. Un grupo de científicos han comenzado de nuevo a experimentar con la criptografía cuántica a través del aire, siendo su objetivo final crear un sistema criptográfico cuántico que pueda operar a través de satélites; si esto se pudiera conseguir permitiría la comunicación global absolutamente segura. Hasta ahora, han logrado transmitir una clave cuántica a través del aire a una distancia de 1 km.

La criptografía cuántica ya ha dejado de ser futuro, para ser presente. La pregunta es ¿hemos conseguido la seguridad perfecta? Pues la respuesta es: sí y no.

Teóricamente la definición es perfecta, la cuestión es que los aparatos no lo son, y existen por tanto problemas; por ejemplo, la existencia de pulsos con más de un fotón, combinado con pérdidas en el canal y errores de los receptores, permitiría a un intruso romper el esquema. Actualmente se plantean varias alternativas para superar esta restricción, utilizando fuentes ideales de fotones con satélites de órbita baja o repetidores cuánticos. Los satélites de órbita baja tienen el problema que deben funcionar como un centro fiable, en el cual los usuarios se deberían fiar de que nadie accede a su información. Por otro lado, están los repetidores cuánticos, que no necesitan centros fiables ni límites de distancia; su problema radica en que actualmente su viabilidad tecnológica es lejana.

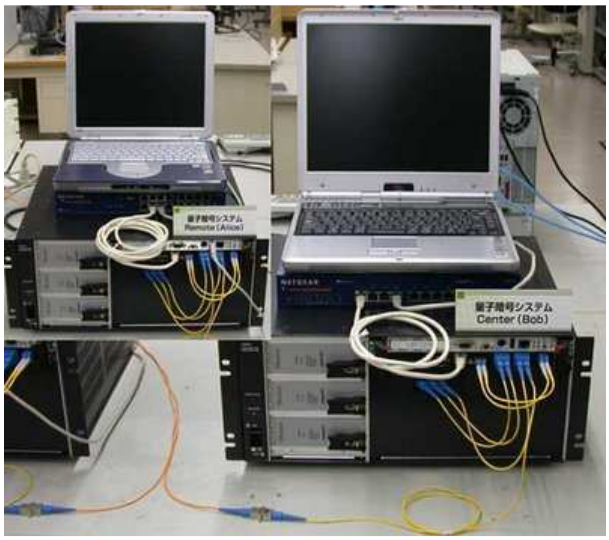


Computación cuántica

Los expertos en seguridad se preguntan cuánto se tardará en convertir la criptografía cuántica en una tecnología práctica. En esto momentos, contar con la

criptografía cuántica no supondría una ventaja, porque la cifra RSA ya no da acceso a una codificación de hecho indescifrable; sin embargo si los ordenadores cuánticos se convierten en realidad, RSA y todas las demás cifras modernas serán inútiles, y la criptografía cuántica se convertirá en una necesidad. La carrera está en marcha, la pregunta realmente importante es si la criptografía cuántica llegará a tiempo de salvarnos de la amenaza de los ordenadores cuánticos, o si habrá un intervalo sin privacidad, un período entre el desarrollo de los ordenadores cuánticos y la llegada de la criptografía cuántica. Hasta ahora la criptografía cuántica es la tecnología más avanzada, siendo el experimento suizo con fibras ópticas, la demostración de que sería viable construir un sistema que permita la codificación segura entre instituciones financieras de una misma ciudad, cosa que ocurre en la actualidad.

En definitiva, la criptografía cuántica marcaría el fin de la batalla entre los creadores de cifras y los descifradores siendo los primeros los claros vencedores.



12) Perspectiva técnica y legal de la criptografía frente al próximo milenio

Posiblemente, aunque quizás de manera inadvertida para gran parte de la humanidad, pero veloz e inexorablemente, estamos empezando a traspasar el umbral de una nueva era, caracterizada por una creciente importancia de la información y un uso masivo y voraz de la misma, que, indudablemente, va a transformar radicalmente todas las bases sobre las que se cimientan nuestras arcaicas sociedades para alumbrar unas nuevas denominadas, con toda justicia, sociedades de la información. Dichas sociedades

requieren, y requerirán, garantías de que la base sobre la que se asientan la información es fiable y confiable.

La seguridad de la información está llamada a jugar un papel insustituible en todo el conjunto de nuevas aplicaciones y servicios, como teletrabajo, telemedicina, tele- educación, tele-administración, comercio electrónico, dinero electrónico, etc.

Ahondando ya en este campo, destaca dentro de él una disciplina capital que, si bien ha venido usándose desde tiempos ancestrales, con el advenimiento de las nuevas sociedades ha visto acrecentarse espectacularmente el interés por la misma, naturalmente se esta hablando de la criptografía, la cual considerada desde la antigüedad clásica como el medio por excelencia para la preservación de la confidencialidad de las informaciones, sobre todo las de origen militar y diplomático. Y, que lógicamente, desde la década de los setenta, conforme se iba incrementando el interés por la misma, ha ido ampliando su campo de ampliación en cuanto a la protección de la confidencialidad hasta abarcar, en estos últimos años, el mantenimiento de la integridad de los datos, la acreditación de la identidad de sus fuentes y la imposibilidad de su repudio.

Consecuencia del aumento de interés experimentado por este campo de la seguridad de la información es la confusión que actualmente reina en el mismo, y que se podría catalogar como "crisis de crecimiento", caracterizada por la aparición interrumpida de nuevos algoritmos de cifrado, técnicas criptográficas y protocolos de uso de éstas y, finalmente, por el replanteamiento que los estados e instituciones internacionales se están haciendo acerca de la utilización indiscriminada y descontrolada que se esta haciendo de estos potentísimos procedimientos de protección de sus datos.

Algunos países, como Francia, habían procedido a legislar tanto el uso interno de las técnicas de cifrado como la importación y exportación de tales productos, mientras otros, principalmente Estados Unidos hacían lo propio con las exportaciones. Del mismo modo, es frecuente hallar gobiernos que distinguían entre productos de cifrados destinados a preservar la integridad, o la autentificación , o ambas, del remitente de informaciones incluyendo la firma digital y productos destinados a proteger la confidencialidad. Así, a menudo, los poderes ejecutivos son más proclives a permitir el manejo sin trabas de técnicas criptográficas destinadas al mantenimiento de la integridad

y autenticidad, que hacer lo propio respecto de aquellas otras dirigidas a ocultar la información.

La irrupción de nuevos procedimientos comerciales y económicos, como el correo electrónico, están contribuyendo a la, denominada por los economistas, globalización de la economía, lo cual induce a los gobiernos de los estados más avanzados a plantearse la promulgación de leyes, que, poniendo coto al empleo indiscriminado y descontrolado de estas potentísimas técnicas de encubrimiento de la información, no suponga un freno a la citada globalización.

Como consecuencia del interés europeo en el desarrollo de la llamada sociedad global de la información, en 1997 elaboró la Comunicación: Towards a European Framework for Digital Signatures and Encryption, en donde se ponen las bases de lo que en la actualidad aparece como Directiva, al menos en lo que respecta a la firma digital

Análogamente, dentro del marco europeo, la Institución Europea de Normalización de las Telecomunicaciones (ETSI) prepara un estándar especifico acerca de la TTP(77), y el Consejo de Europa, en su guía sobre el delito informático, ha alertado sobre el peligro del uso indiscriminado de la criptografía, que dificulta de forma creciente las investigaciones policiales, por el empleo generalizado que hace de dichas técnicas la delincuencia internacional.

En un ámbito más universal, ISO(78) trabaja en una norma de firma digital, al igual que la ONU que también prepara el suyo. Quizás la iniciativa más notable, con diferencia, sea la de la OCDE(79), que en 1996 comenzó a elaborar una Guía de principios criptográficos, concluida y publicada en 1997.

Prácticamente todos los estados norteamericanos tienen muy avanzados sus borradores o incluso ya han aprobado las correspondientes leyes. De hecho, fue Utah el primer territorio del mundo en dotarse de una disposición legal de tal naturaleza. En todo caso, la primera propuesta de limitar el uso de las técnicas criptográficas se debe al presidente Clinton, que en 1993 lanzó la iniciativa presidencial conocida como

(77) Trusted Third Parties. Más información en **http://en.wikipedia.org/wiki/Trusted_third_party**
(78) International Organization for Standardization. Más información en **http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_para_la_Estandarizaci%C3%B3n**
(79) Organización para la cooperación y el Desarrollo económico. Más información en **http://es.wikipedia.org/wiki/OCDE**

Clipper-chip. Ésta imponía el algoritmo de cifrado Skipjack, implementado en un dispositivo físico, que incorporaba un mecanismo de claves custodiadas, lo que a su vez suponía el establecimiento de TTP's, pero con la peculiaridad de que éstas serían concretamente dos : Ministerio de Comercio y el de Justicia. Sin embargo, ante la fuerte reacción contraria que suscitó, la administración estadounidense ha relajado su posición en los dos aspectos más cuestionables: admitiendo otras TTP (no por fuerza gubernamentales) y permitiendo otros algoritmos de cifrado, incluso implementados en software siempre que:

- Incorporen el procedimiento de claves a prueba de intrusiones
- El algoritmo programado no sea clasificado
- Instrumenten un mecanismo que trasmita frecuentemente la clave de sesión cifrada y la clave obtenida de las custodiadas.

Para los equipos criptográficos así construidos quedaría sin efecto las disposiciones que limitaban la exportación de los productos criptográficos que admitiesen claves de más de 40 bits.

Criptografía Española

Poco se ha escrito es España sobre materia criptográfica, la primera obra de criptografía se adjudica a Juan Tritheme, monje benedictino del monasterio español en la diócesis de Myence, el cual gobernó hasta 1506, en el que fue nombrado abad de San Jaime de Wurhtbourg, y en donde murió en 1516. También, puede encontrarse alguna documentación en la Biblioteca Universal de la Paleografía española del P. Burriel..

El uso de la escritura cifrada con clave existe desde los primeros tiempos de nuestra era. Juan Bouquero y Contius tenían sus alfabetos que desfiguraban con el cambio de letras, Pedro Massio y Antonio Venero empleaban las iniciales de los nombres, Gesualdo y Juan Bautista Porta formaban sus alfabetos con las iniciales de los oficios y dignidades, además Casio Severo, Christophoro Songolio y Antonio Maliabechi, bibliotecario del Gran Duque de Florencia, dieron origen a las verdaderas claves sustituyendo cada letra por un número.

Muñoz y Rivero, en su *Paleografía Visigoda*, nos habla, también, de la correspondencia cifrada y presenta como testimonio un documento atribuido a San Jerónimo.

Diferentes son los sistemas de que los autores de criptografía nos dan cuenta, como se ha explicado sobradamente a lo largo de este estudio. Igualmente, se ha resaltado que la formación de una clave no es difícil, puesto que no se sujeta a reglas fijas y sólo depende de la mayor o menor pericia del amanuense en la combinación de signos, lo realmente complicado es obtener una cifra que resulte prácticamente indescifrable y por otro lado, también, resulta extremadamente complejo llevar a cabo el descifrado de un documento, faltando la clave. Hay quien asegura que todo texto cifrado, por difícil que sea, llegará a traducirse sin necesidad de la clave; opinión que tiene muchos detractores, porque si bien es verdad que el abecedario sencillo y aún el silabario pudiera descifrarse a fuerza de combinaciones, no se alcanzaría el mismo resultado con los nombres y palabras completas, cuando éstas tienen cada una un signo especial.

Algunas cifras, sobre todo las generales de Felipe II (ya detalladas en capítulos anteriores), en que los nombres se encuentran por cientos y es raro que una persona, por hábil que sea, pueda descubrir la palabra equivalente de cada uno de estos signos. Se cuenta que la Reina Isabel I de Inglaterra tenía a su servicio un cortesano llamado maestre Phelipe, hombre muy experto en estas materias, a quien encargaba el descifrado de los documentos que caían en su poder, y merced a su habilidad fueron descifrados los correos que en 1620 remitió el Conde Oñate para el Archiduque Alberto, consiguiendo enterarse de cuanto trataba en Roma el Conde de Olivares con el Papa Sixto V, pero que nunca pudo llegar a poner en claro la mayor parte de los nombres.

El escollo principal con el que los investigadores que manejan papeles de Estado tropiezan continuamente, es la correspondencia cifrada tan abundante en esta sección. Existen muchísimos documentos aún sin descifrar, a pesar de los grandes trabajos llevados a cabo en esta materia, cuyo resultado se ha dado al público en la colección de 112 volúmenes de documentos inéditos, además de otros particulares, como el del Sr. Conde de Valencia de Don Juan, que descifro la correspondencia de don Luis de Requesseno siendo gobernador de Flandes; el barón Kesoin, que para escribir su *Historia de Bélgica* hubo de descifrar los despachos del Duque de Alba, don Antonio de Guarras

y don Juan de Speo, durante la embajada de estos en Inglaterra y el gobierno de Flandes, entre otros.

Todos los documentos de la sección de Estado son de vital importancia a la hora de elaborar nuestra propia historia, por lo que resulta fundamental interpretarlos fielmente para resolver muchas cuestiones históricas aún en el aire.

Los documentos cifrados recogidos en los archivos generales del Estado no alcanzan más allá de los Reyes Católicos. Dicha colección de claves de los siglos XV al XVIII comprende más de 400 y resulta un poderoso auxiliar para el investigador que trate de estudiar con detenimiento la correspondencia diplomática de esta época, y muy especialmente los intrincados negocios en que intervinieron Felipe II, don Juan de Austria y el Duque de Alba. Esta época constituye, prácticamente, el principio de criptografía en España por la gran variedad de cifras utilizadas.

El primer acto de gobierno de Felipe II fue ordenar la formación de claves. Así vemos que en la carta dirigida desde Bruselas a su tío el emperador Fernando, con fecha 24 de mayo de 1556 dice que ha vuelto a cambiar la cifra que usaba Carlos V para comunicarse con sus ministros de Italia y de otras parte, no sólo por ser antigua, sino por estar totalmente divulgada y no ser buena para los negocios. Será durante este periodo cuando la utilización de claves en la comunicación alcanzó su punto álgido.

En el siglo XVII decae notablemente el uso de las claves. Siguen las claves generales con muy pocas variantes, y se encuentran bastantes particulares compuestas tan sólo de abecedario en francés o italiano.

En el siglo XVIII desaparece toda la elegancia, la uniformidad y belleza antes empleada en la construcción de claves. Algunas son muy caprichosas con la sustitución de palabras por signos de ejecución laboriosa y difícil, otras en las que el abecedario está representado por la siete notas musicales en sus diferentes valores; la del Duque de Sessa, compuesta por 49 abecedarios y la de Juan Bautista de Tessis, que consta de 161 encasillados, conteniendo cada uno las 10 cifras arábigas con sus correspondientes palabras, que se representan en la cifra por el número del encasillado y el que acompaña a la palabra.

Como ya se ha explicado con anterioridad, la esteganografía, al contrario que la criptografía, pretende ocultar el mensaje, una vez descubierto éste, el contenido del mismo puede ser leído. Esta es la técnica que suelen utilizar los espías para enviar sus mensajes por métodos tradicionales. Por ejemplo, son bien conocidas las propiedades del zumo de limón cuando se utiliza como si fuera tinta; dicha técnica era la utilizada por Zumalacárregui para comunicarse con Don Carlos en las guerras Carlistas. Otra de las formas de ocultar los mensajes es cambiar el valor de las palabras por otras de apariencia totalmente inocente e insertarlas en una carta, como hacían para comunicarse secretamente la Agrupación Guerrillera de Levante en la posguerra, al igual que varias personalidades republicanas en el exilio.

Sin lugar a dudas, la época más importante para la criptografía en España se corresponde con la Guerra Civil (1936-1939), tanto durante sus prolegómenos, como durante su desarrollo y finalmente durante el periodo conocido como la posguerra.

No se pude hacer un estudio sobre la criptografía en la guerra civil española sin tener en cuenta toda la labor llevada a cabo, sobre este tema, por los autores José Ramón Soler Fuensanta y Francisco Javier López-Brea Espiau que se encuentra perfectamente reseñada en su magnífico libro: *Soldados sin Rostro: Los servicios de Información, espionaje y criptografía en la Guerra Civil Española,* Barcelona, Inédita. José Ramón Soler y Fuensanta, Ingeniero en Informática por la Universidad Autónoma de Bellaterra y Doctor Ingeniero Industrial por la UNED ha mostrado un gran interés por la historia de los servicios de información, y en particular la criptología. Hace varios años que empezó a trabajar sobre el tema habiéndole dedicado varios artículos en revistas especializadas, tanto españolas como extranjeras, y un libro, aparte del anteriormente citado. Francisco Javier López-Brea Espiau, Teniente Coronel del Ejército de Tierra y especialista en criptología del Ministerio de Defensa., es un gran estudioso de la criptología y su historia habiendo publicado artículos en revistas nacionales e internacionales y, siendo gran conocedor de los sistemas de cifrado mecánicos, es un experto en el funcionamiento de las máquinas Enigma.

En los primeros meses de1937 se lleva a cabo la reorganización del ministerio de Estado y los servicios de información dependientes del mismo. Para ello se crea, por

orden del 11 de marzo de dicho año, el Gabinete Político y Diplomático, organismo del que dependerá todo lo relacionado con el servicio de información y cifra y, dentro de él, el SIDE(80) encargado de los servicios de espionaje y contraespionaje en Europa. La dirección del SIDE recayó sobre Anselmo Carretero Jiménez.

José Frade Mendiboure, trabajador del Ministerio de Estado desde 1926 y que en agosto de 1936 era jefe de cifra del Ministerio de Estado, propuso que Anselmo Carretero Jiménez fuera destinado a la sección de cifra. La creación de un Gabinete Criptográfico que regulase el caos en cuestiones de cifra, en el que estaba sumido el gobierno de la Republica y las legaciones diplomáticas, era algo urgente.

Los servicios de escucha y descifrados nacionalistas, principalmente italianos y alemanes, estaban muy contentos por la falta de cuidado en temas de cifra que se producían en las representaciones de la Republica en el extranjero.

No sólo existía una pésima gestión en todo lo relacionado con la cifra, sino que además en noviembre de 1936 es robado en Berlín uno de los códigos, el 166, lo cual obliga al Ministerio de Asuntos Exteriores a ordenar a los embajadores no utilizar dicho código. Aunque también, es justo reconoce que el robo de tales códigos fue común por parte de ambos bandos al principio de la guerra. El mismo mes los republicanos se hacen con el código de los nacionalistas y os telegramas descriptazos gracias a esta acción son rápidamente enviados a Valencia. De todas maneras la disciplina criptográfica en las Embajadas y representaciones en el extranjero de la Republica fue deficiente desde el principio. En diciembre de 1936 en una circular directa a las representaciones en el extranjero, el Gobierno de Valencia tuvo que recomendar la máxima atención en el cifrado de telegramas. Ante tantos problemas, en agosto de 1937 se crea el Gabinete Criptográfico del Ministerio de Estado, el cual estará formado por dos secciones, la de claves, encargada de la creación, almacenamiento, control y distribución de las claves del Ministerio y la de la cifra, encargada del cifrado y descifrado de mensajes. El personal de las dos secciones estaría formado por:

(80) Servicio de Información Diplomático y Español

Sección de Claves	Sección de Cifra
Jefe de	Sección
Dos Cripotografos oficiales	Dos Redactores de cifra
Dos Auxiliares Criptógrafos	Dieciocho Oficiales de cifra
Cinco Auxiliares nmecanógrafos	Dos Archiveros registradores
	Seis Auxiliares mecanógrafos

La seguridad en temas de cifra a pesar de la reorganización, seguía siendo uno de los principales problemas del Ministerio del Estado. Los problemas relativos a la cifra no llegaron a solucionarse en toda la guerra. Pero, la seguridad no era el único problema, existía una gran descoordinación en las Legaciones republicanas. Teóricamente la URSS ayudó mucho a la Republica, pero en realidad pretendían llevar la guerra más a favor de Stalin y vendieron a los republicanos armas malas y caras que tuvieron que pagar con oro.


TELEGRAMA OFICIAL

VALENCIA

J A E N.

Jefe sector Granada.-

su telegrama cifrado ayer 21 horas clave Unión 1 [illegible] en V (ene en uve) resulta completamente indescifrable. Pedir y ordena encargado cifra exquisito cuidado este trabajo evitar retrasos y pérdida tiempo. Repito o reconviene Estación Telegráfica atención servicio con el grupo fucsia con justo aparatos.

F.E.C.H.O.

27 Octubre 1936
Telegrama enviado al jefe del Sector Granada (republicano): "su telegrama cifrado ayer….. resulta indescifrable"
(Fuente: Archivo sobre la Guerra Civil, Salamanca)

Los mensajes secretos no sólo son propios de ambientes militares y diplomáticos, a veces la gente común deben ocultar su información, como ocurrió, por ejemplo, con algunas mujeres del campo de Ibiza que al principio de la guerra, en el trabajo llevaban una enagua de color verde si todo estaba normal o una de color fucsia si había guardias o voluntarios nacionalistas. Y justo en este punto, es donde entra en juego la criptografía, la cual permite asegurar la seguridad de las comunicaciones. Con la aparición de la radio, los mensajes podían circular libremente, lo cual puso de manifiesto la importancia de la criptografía.

Las secciones de escucha se encargan de interceptar el mensaje, definiendo a su vez, que unidad operativa esta transmitiendo y desde donde, así como otras muchas

cuestiones dependiendo de la afluencia de las mismas o de su silencio; realizando, de esta forma, todo un estudio sobre las formas de comunicación, el cual se conoce como análisis de tráfico. Una vez obtenidos los mensajes cifrados, estos son enviados a la sección de criptoanálisis o contracifra. No hay que olvidar, que el criptoanálisis pretende obtener el contenido del mensaje sin conocer el método o un parámetro auxiliar necesario para descifrar el criptograma y a este proceso se le conoce con el nombre de descifrar el mensaje, en contraposición a descifrar un mensaje que es lo que hace el receptor autorizado del mismo para obtener el mensaje original.

Durante la Guerra Civil, los encargados de realizar las tareas de análisis de información por ambos bandos era la Sección Segunda del Estado Mayor, los cuales realizaban los resúmenes y enviaban la información resultante del análisis a los responsables de la operación.

Quizás, sea importante hacer notar la diferencia que existe entre las cifras y los códigos; mientras las primeras son formas de manipular el mensaje mediante una serie de transformaciones, sustituciones de letras por símbolos u otras letras, cambio de orden de las mismas, para lograr convertir un mensaje en algo teóricamente inteligible para una persona que no las conozca; un código es, básicamente, un diccionario en el que se asocian palabras o frases completas a palabras o grupos de letras. Para aumentar la seguridad, siempre puede cifrarse con una cifra un mensaje que ha sido cifrado con un código, esta operación recibe el nombre de supercifrado, y es una operación muy común en los ambientes diplomáticos y navales. El procedimiento normal con el que se lleva a cabo un supercifrado es con una simple suma sin acarreo (método muy utilizado por la marina nacionalista al principio de la guerra). Dado que la posibilidad de coordinarse era difícil, al principio de la guerra, se optó por utilizar un código Perea con una nueva numeración de páginas y sin recifrar, para más adelante, una vez restablecida la normalidad criptográfica, añadirse las tablas de supercifrado.

DE SALAMANCA A/E C Y (probable Ifni)
El Coronel jefe estado mayor del aire al jefe aeródromo
C L A V E " I "
Por mediacion señora de capitan R U G I A N O notifiquen
a señora de capitan S O M P A N Y fallecimiento de este en
accidente ocurrido Talavera haciendole presente mi sentido
pesame/.
Descifrado a las 11 horas del 11 dic 1936
(casi descubierta la clave " I " por este gabinete de cifra)
(Hoy dia 11 dic. 1936)
SECCION DE INFORMACION
11 DIC 1936
A las Horas
GABINETE DE CIFRA

11 diciembre 1936
Mensaje nacional captado por los republicanos (muestra que no deben mandarse mensajes cifrados sólo en parte)
(Fuente: Archivo sobre la Guerra Civil Española).

Un código presenta como ventaja sobre una cifra el hecho de que al no existir ningún tipo de relación en él dificulta mucho la labor del criptoanálista. Como desventaja presenta el hecho de tener que manejar un libro de códigos, que puede llegar a ser muy voluminoso, y que no es fácilmente reemplazable. Como caso especial, puede citarse los denominados códigos de trinchera, cuya característica esencial es ser muy reducidos y orientados a un uso muy específico. Estos códigos vieron su nacimiento en la primera guerra mundial y fueron ampliamente utilizados en la guerra civil española por su facilidad de uso, y porque reducían mucho el mensaje, con lo que se evitaba la posible detección del emisor. Existen varios ejemplos muy representativos de estos: la clave Bous[81], la clave Bertrán Musitu[82] y el último ejemplo lo vemos en la aviación republicana, la cual utilizaba un código para informar sobre la aviación enemiga y la actuación de la aviación propia a través de una serie de partes cifrados con unas reglas predeterminadas que utilizaban a su vez una serie de tablas de sustitución para el cifrado.

No obstante, si ha de mencionarse un método de cifrado por excelencia en la Guerra Civil Española, éste es sin duda la tabla de homófonos y una variación de ella, el sistema de cinta o sistema español, la cual consiste en llevar a cabo una sustitución simple de un símbolo por otro, como por ejemplo en la clave Violeta[83], donde se sustituía la letra del alfabeto superior por su equivalente inferior.

(81) Utilizada para las comunicaciones cifradas de los Bous de las Fuerzas Navales del Cantábrico de la Marina de Guerra Republicana. Dicha clave consta de nueve páginas pero utiliza un máximo de tres letras para representar todas las posibles situaciones en que se puede encontrar la embarcación.
(82) sistema de cifrado rápido para emisión de mensajes mediante radios clandestinas que evitaba la detección de la estación y la consecuente eliminación de la emisora.
(83) clave de régimen interior para comunicados de importancia entre compañías y el mando del Batallón 415 de la Brigada Mixta 104, durante la Guerra Civil Española.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	Ñ
x	ñ	u	t	v	z	h	k	e	a	d	o	r	y	m	c	i	l	j	b	o	f	q	g	n	s

El hecho de que las letras L y U tengan como equivalencia la "o" no es un error tipográfico, sino que ya aparecía de esta forma en la transcripción que hizo el SIPM de la clave. En realidad una de las dos "o" tendría que ser una "p" pero estos errores eran más frecuentes de lo que puede parecer. Por lo tanto, según este método, la palabra OBUS se escribiría MÑOJ.

Lo normal es que en un mensaje aparezcan unas letras con más frecuencia que otras, por ejemplo la letra E aparece más veces que la Z y por lo tanto, en un mensaje cifrado, éstas tendrán un mayor número de representaciones, lo cual da lugar a una tabla de homófonos de dicho mensaje. Como ocurre por ejemplo en la clave X[84]. Donde, como según se aprecia en la siguiente tabla, la A puede representarse por el 10, el 30 o el 69, lo que hace más difícil el descriptazo.

COPIA DE LA CLAVE HERMIDA EMPLEADA POR LA BRIGADA MIXTA Nº104.

415 BATALLON

CLAVE VIOLETA

(1) A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.

(2) x.ñ.u.t.v.z.h.k.e.a.d.o.r.y.m.c.i.l.j.b.

(1) U.V.X.Y.Z.Ñ.

(2) o.f.q.g.n.s.

NOTA: Esta clave de régimen interior se cree para uso de las comunicaciones de importancia entre las Compañías y el Mando del Batallón.
Las cifras necesariamente deberán ser consignadas en letras.-Las columnas pueblanas con el signo (1) corresponden al alfabeto.-Las columnas sucesivas con el signo (2) corresponden en su equivalencia en clave.-

Hay un sello en tinta en el costado derecho en forma de triangulo que dice.-Brigada Mixta 104.-Batallón 415.Dentro del triangulo:Mayoría.-

Fecha desconocida
Clave Violeta usada por la República,
y capturada por el bando nacional
(Fuente: Archivo Militar de Ávila)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
			01			09		03	08			07			02			05			06				04
10	14	15		17			13			19	12			18			16			11					
					29								27			22			20			23	26	25	
30			31			35		37	33			34			32			36			38				39
	49	40		48	46		45			42				44			43			47			41		
											51		50			53			56			58		54	
69	67			66			65		63		61			60		62			64		68				
		79	70		71	72		75		77		74	73		76		78								
																		89		81		85	87	86	82

(84) Clave que usaba el buque mar Cantábrico para sus comunicaciones con la estación de Méjico, las estaciones costeras de Santander o Bilbao, la escuadra o el Gobierno.

Para formar la tabla de homófonos de este método, se utilizaban números de dos cifras del 10 al 99 totalmente desordenados y colocados al azar, sin embargo, en los sistemas usados durante la guerra civil ésta limitación se cambia en algunos casos y se elimina en otros llegándose a representar todos los números de dos dígitos, aunque en general se solía utilizar alguno de ellos como punto.

Junto con la tabla de homófonos, el método de cifrado más utilizado, pese a su antigüedad y poca seguridad, durante la Guerra Civil Española, fue el sistema manual de cifrado conocido como de cinta móvil. Su origen data de finales del siglo XIX y la primera vez que aparece documentado es en el libro *Método Oficial de Guerra* de Carmona. Poco después aparece en un texto de telegrafía militar de Losada con el nombre de método español. Según Carmona el método era utilizado en la época de su publicación por todos los Ministerios exceptuando el de Estado; Losada, por su parte, afirma que es el procedimiento adoptado en España para cifrar los escritos oficiales. El criptógrafo de cinta móvil consiste en una tabla de homófonos como la clave X a la que se añaden dos filas, una en la que figura el alfabeto en orden normal y en la otra se introduce una cinta móvil con un alfabeto doble totalmente aleatorio. En el diseño original la cinta pasa a través de dos ranuras a ambos lados de la tarjeta donde está ubicada la clave y justo debajo del alfabeto claro, tal como muestra el siguiente esquema.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
B	E	W	T	R	S	M	Q	Y	U	I	O	P	A	N	D	F	G	H	J	K	L	Ñ	Z	X	C	V	B	E
	10		20		30		32		41		01		92		87		99		45		26		25		76		37		
		02		62		13		27		63		05		14		61		07		22		21		09		12			
	11		03		15		34		29		35		37		24		36		38		23		39		40		69		
		04		18		28		49		51		54		19		06		08		58		64		71		70			
	33		31		50		32		16		44		52		55		56		59		60		65		72		75		
		47		17		48		42		43		46		53		57		66		68		74		78		80			
	67		73		81		84		83		85		91		79		90		77		82		88		89		86		

El alfabeto solía generarse mediante la utilización de una palabra clave. Durante la guerra surgieron algunas variaciones sobre este sistema, quizás, las más importantes fueron la utilización de más de una cinta móvil y completar la clave con pequeños repertorios de códigos.

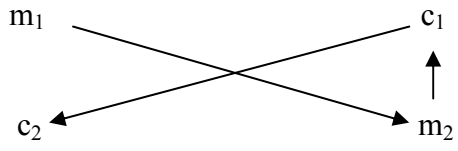
Para cifrar ambos comunicantes debían ponerse de acuerdo en la colocación de la cinta móvil, para ello indicaban el par de letras, la primera del alfabeto normal y la

segunda de la cinta para posicionarla correctamente. Posteriormente se procedía a cifrar utilizando el alfabeto marcado en la cinta como alfabeto base y escogiendo cualquiera de los números de la columna debajo de la letra a cifrar como texto cifrado. Si bien el secreto depende de ir variando los números usados como cifra, lo cierto es que muy frecuentemente eran empleados los mismos números para representar las letras. Por ejemplo para cifrar la frase METODO DE CINTA con este método y según la tabla reseñada anteriormente, resultaría:

M	E	T	O	D	O	D	E	C	I	N	T	A
13	10	20	01	87	35	24	11	76	63	14	03	92

Recientemente, y en contra de lo que se pensaba, los historiadores Domingo Blasco y Francisco Cabrera descubrieron que el método de Playfair también fue muy utilizado durante la guerra. Este método fue, con ampliaciones y algún cambio, muy empleado hasta la segunda guerra mundial, debido a su sencillez y a su fácil adaptación a cualquier entorno. Dicho método consiste en formar una tabla cuadrada de 5x5 elementos en los que se introducen las letras del alfabeto, utilizándose la misma celda para "I" y la "J", y análogamente para la "U" y la "V". Para crear la tabla se usa una palabra clave que sólo conocen las dos personas que se van a mandar los mensajes. En primer lugar se colocan las letras correspondientes a dicha palabra, sin que haya repeticiones, y posteriormente se colocan el resto de las letras del alfabeto hasta completar la tabla. Una vez confeccionada la tabla de cifrado se divide el texto a cifrar en grupos de dos letras consecutivas comprobando que no existe ningún par de letras iguales. En caso de que esto suceda, se inserta un nulo, es decir, una letra al azar que no produzca confusión en el contenido del mensaje. Concluido este paso se procederá según las siguientes reglas:

■ Si las letras a cifrar están en diagonal, el par cifrado será el formado por las letras que formen la diagonal de los otros dos vértices del rectángulo, de modo que si m_1, m_2 es el par del mensaje y c_1, c_2 el correspondiente par del cifrado, el proceso de cifrado sería de la forma:



■ Si las dos letras a cifrar están en la misma horizontal, el par cifrado estará formado por las letras a la derecha de ambas, siendo la primera columna la que sigue a la última y la última la que antecede a la primera.

■ Si las dos letras a cifrar están en la misma vertical, el par cifrado estará formado por las letras de debajo de ambas, siendo la primera fila la que sigue a la última y la última la que antecede a la primera.

El proceso de descifrado es simplemente llevar a cabo los pasos anteriores en sentido inverso. Así por ejemplo, si se quisiera cifrar la frase ATACAD AL AMANECER con la clave DINAMITA. El procedimiento a seguir sería: en primer lugar, como ya se ha dicho, crear la tabla.

D	I/J	N	A	M
T	B	C	E	F
G	H	K	L	M
O	P	Q	R	S
U/V	W	X	Y	Z

Seguidamente se divide el texto en pares de letras que son las que se usarán para cifrar.

Texto en claro	AT	AC	AD	AL	AM	AN	EC	ER
Texto cifrado	DE	NE	MI	ER	MD	MA	FE	LY

También se usaron frecuentemente durante la guerra civil el método Gronsfeld(85) y una variante del cifrado de Polibio. El primero, sencillo pero poco seguro, usaba como clave ocho números cada uno de los cuales indicaba el número de letras del alfabeto que debía desplazarse el mensaje original. Por ejemplo, si quiere cifrarse la palabra MANDAMOS y se utiliza como clave el número 2468 1357, se cogerá la letra que está dos posiciones antes de la M, es decir, la K; luego la letra que ocupa cuatro posiciones antes de la A, ósea, la W ya que al haber finalizado el alfabeto empleamos como primer desplazamiento la Z, y así sucesivamente. De tal forma que el cifrado final quedaría:

M	A	N	D	A	M	O	S
K	W	H	V	Z	J	K	M

(85) Contra este criptosistema no se puede usar ni el método de fuerza bruta ni el estudio de las frecuencias de las letras del texto, pues altera la frecuencia de una misma letra. La E se ha cifrado de varias formas distintas.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0:	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
1:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
2:	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
3:	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	F	G	H
4:	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
5:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
6:	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
7:	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
8:	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
9:	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C

El segundo, tenía por base generar una tabla con tres filas de diez columnas. La primera fila no tenía numeración y la segunda y tercera filas se numeraban respectivamente con dos de los números no utilizados en las columnas de la primera fila. Las columnas se numeraban con una puntuación de dos dígitos del cero al nueve.

El proceso de cifrado consistía en poner una palabra de ocho o menos letras diferentes en la primera fila, en dicha palabra se eliminaban las letras repetidas y el resto, hasta completar el alfabeto, se disponían en las dos filas siguientes. El cifrado es similar al de Polibio [(86)], pero aquí las letras pueden codificarse como uno o dos números.

Por ejemplo si tenemos el mensaje "Atacar al amanecer", la clave fusil y las columnas generadas por el siguiente orden

	8	3	0	2	4	6	1	7	5	9
	F	U	S	I	L					
5	A	B	C	D	E	G	H	J	K	M
1	N/Ñ	O	P	Q	R	T	V	X	Y	Z

(86) Inventado hacia 150 a. C. por el historiador Polibio, Se trata de un algoritmo trivial, donde cada letra del alfabeto es reemplazada por las coordenadas de su posición en un cuadrado. Es un caso particular de transposición mono-alfabética. Este tipo de código no resiste a un análisis de frecuencias. Más información en http://es.wikipedia.org/wiki/Cuadrado_de_Polibio

El mensaje cifrado sería 581658058145845859581854505414. El descifrado es sencillo, ya que si el dígito inicial es un cinco o un uno sabemos que es el carácter que viene representado por dos dígitos, en caso contrario solo por uno.

Una de las pocas claves de trasposición utilizadas en la guerra fue usada por el PSOE. El cifrado consistía en una trasposición de columnas, en uno de los documentos consultados, el orden utilizado era 4,2,9,17,10,3,11,12,1,5,8,13,16,7,6,15,14. Es decir, que el mensaje se dividía en 17 columnas en las cuales se iban cogiendo las letras en el orden que marcaba la columna. Por ejemplo, en el caso de querer cifrar, la ya utilizada frase ATACAR AL AMANECER, disponemos las letras debajo de la casilla correspondiente a su posición y, al tener sólo 16 letras, le añadimos un nulo, una letra que no de lugar a confusión en el mensaje. Para ello escogemos la letra V; una vez hecha esta operación, vamos cogiendo las letras en el orden marcado por la puntuación, es decir, la que está en la posición 4 en primer lugar, la que está en la posición 2 en el segundo lugar y así sucesivamente.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A	T	A	C	A	R	A	L	A	M	A	N	E	C	E	R	V

El mensaje cifrado resultante sería: CTAVMAANAALERAREC

Evidentemente, durante la guerra civil, ambos bandos se apresuraron a organizar sus servicios de información y preparar sus claves. Los primeros días fueron caóticos para los dos bandos, ya que carecían de disciplina criptográfica, y además, utilizaban las mismas claves. El mismo almirante Pascual Cervera y Cervera [87] afirmo en un artículo de la *revista general de la Marina* "....en esta materia estábamos, tanto los nacionales como los rojos, en mantillas".

Sí se añade a la ignorancia, la laxitud, por decirlo de alguna manera, con la que se tenía al principio de la guerra la disciplina criptográfica, o lo que es lo mismo, las normas de seguridad en la cifra, no es difícil imaginar que el descifrado por parte del enemigo era previsible y habitual. No es que no existiera una reglamentación adecuada en cuestión de cifra, es que el personal estaba mal preparado para una guerra moderna y

(87) Director de los primeros grupos de criptoanálisis de la marina nacionalista en Cádiz.

no se valoraba la importancia del cifrado. La normalización en cuestión de cifra fue lenta, debido principalmente a un problema de definición de fuerzas y frentes.

En cuanto a la utilización de máquinas de cifra, la más básica era sin duda la Clave Norte, la cual era un dispositivo de cifrado mecánico ya anticuado para la época. Estaba formado por dos ruedas dentadas, con un número de dientes diferentes en cada una, cuarenta la izquierda y treinta y siete la derecha, y diferente tamaño, 10,5 centímetros de diámetro exterior y 10 centímetros de diámetro interior la izquierda por 9,7 y 9,2 respectivamente la derecha. Ambas ruedas se encontraban encima de dos círculos, el de la izquierda de cartulina que se cambiaba con una cierta frecuencia y en el que se encontraba el alfabeto cifrado, y el de la derecha, metálico, en el que se encontraba el alfabeto en claro, con algunas letras repetidas. En la rueda de la izquierda había un agujero, a continuación de las letras y en la parte inferior, que es por donde se veía el resultado del cifrado.

El bando nacional no tardo en usar la máquina Enigma (ya descrita en el apartado de la segunda Guerra Mundial), la cual les fue proporcionada por los alemanes. Además, existe constancia de la utilización de máquinas Kryha, la cual fue desarrollada en 1924 por Alexander Von Kryha .Obtuvo un gran éxito comercial y se uso masivamente, estuvo en activo hasta mediados de los años cincuenta.

El bando nacionalista estaba asesorado por los alemanes e italianos en términos de cifra, sin embargo, el bando republicano no se quedó atrás, llegando a disponer de una eficiente gestión criptográfica, al menos en el ambiente militar, gracias al asesoramiento soviético. En las unidades del ejército se usaban códigos con supercifrado, las tablas del mismo cambiaban cada semana o cada diez días como mucho, desgraciadamente no ocurrió lo mismo con el resto de las instituciones.

Como ya se ha mencionado los primeros mensajes, eran rápidamente captados y descifrados por ambos bandos, los cuales tomaron conciencia, en seguida, de la importancia de los datos que podían obtenerse de la escucha y la descriptación. Sin embargo, el bando nacionalista fue el que saco mejor partido de esto, ya que rápidamente organizó sus centros de escucha y descriptado adjuntos a sus Servicios de Información y, sobre todo, centralizó la información obtenida en aras de una mayor eficacia. Gran parte

de este merito fue de D. Antonio Sarmiento León-Troyano, que se encargo de organizar los servicios de escucha, cifra y contracifra y de la colaboración en esta materia con los alemanes e italianos.

El número de claves capturadas al ejército republicano por el bando nacional fue enorme debido, principalmente, a que el ejército republicano no fue homogéneo, lo que propició, sobre todo al principio de la guerra, la laxitud en ciertas prácticas, entre ellas las del uso de la criptografía. La distribución de claves fue muy deficiente, siendo muy frecuente el tener que repetir el mensaje por no disponer de la nueva clave. Además, hubo claves con una duración excesiva para la protección de comunicaciones de alto nivel. No obstante, la mayoría de estos problemas se fueron solucionando a medida que transcurría la guerra, pero en contra partida, para cuando eso ocurrió los servicios nacionales de descriptazo disponían ya de un nivel excelente y de gran experiencia acumulada. Otro de los problemas de los que adolecía también el servicio de criptografía de la República era la falta de un repositorio centralizado de claves, problema que no llego a solucionarse nunca. Sin embargo, es importante destacar que en el bando republicano hubo excelentes profesionales en cifra y contracifra, y que las normas de seguridad, al menos en los últimos años de la guerra y en los estamentos militares superiores, fueron escrupulosamente seguidas.

El descifrado tiene una importancia fundamental en el Servicio de Información Militar. Los servicios de escucha y de descifrado son sólo una parte de este servicio, ya que no hay que fiarse exclusivamente de los datos obtenidos de las escuchas o descriptazos, puesto que se puede estar sufriendo intoxicaciones informativas realizadas por el enemigo para desorientar a nuestras propias fuerzas. Una aplicación especial, aunque no es la prevista inicialmente en un servicio de escucha y descriptazo, es la comprobación de nuestras propias claves, el cercioramiento de su utilidad e incluso para la introducción de espías en el bando contrario. Los servicios de escucha se encargan principalmente de la captación de mensajes tanto en claro como cifrados, análisis de tráfico, y ubicación de las fuerzas enemigas a través de sus comunicaciones. Por lo tanto, los dos servicios, escucha y contracifra, son complementarios, pudiendo ocurrir, a veces, que el segundo se nutre de la información que proporciona el primero y ambos aportan información al Servicio de Información Militar.

El personal dedicado al criptoanálisis debe estar dotado de paciencia, perseverancia, imaginación, suficientes conocimientos y sobre todo mucha suerte, ya que la mayoría de los sistemas que se pretenden forzar se consideran muy seguras y en muchas ocasiones se rompen gracias a un error cometido por el usuario, una mala gestión de claves o un seguimiento deficiente de las normas de seguridad.

En el bando nacional, el proceso seguido para el descifrado comenzaba con la captación del mensaje o mensajes cifrados por parte de un grupo de escuchas. Estos eran apuntados en impresos especiales y remitidos al grupo de criptoanalistas; si se trataba de una clave conocida, se procedía a su descifrado y su remisión al Servicio de Información, en caso contrario los especialistas intentaban el descriptazo. Cuando no se conoce la clave, el descriptazo es claramente conflictivo y de gran complejidad; normalmente se necesita la ayuda de varios expertos, que mediante cruces de información, un archivo adecuado y, como ya se ha dicho, paciencia, perseverancia y mucha suerte, puede que consigan romper el código o la cifra. Una vez rota la clave, se almacenaba en un repertorio de claves y se enviaba la noticia al General Francisco Franco, el cual, en caso de no poseerla, solicitaba su remisión por un método seguro. El proceso comenzaba con la identificación de las unidades u organismos implicados, como el emisor y destinatario del mensaje. A partir de este conocimiento se puede determinar la clave utilizada, si se conoce, o sino usar "cuñas", es decir, palabras probables que ayuden a descifrar el mensaje. Normalmente, para evitar ese problema, los emisores y destinatarios de los mensajes solían estar codificados e incluso podían tener más de un valor de código.

En cuanto al bando republicano, contó con la ayuda soviética en cuestiones de cifra y contracifra, aunque no tan pronto como la que los italianos y alemanes dieron al bando nacional. Los codificadores debían realizar las operaciones de cifrado y descifrado de los asesores soviéticos. El cifrado lo realizaba una persona distinta del que transmitía la información, esquema común en los ejércitos de la época ya que el que conocía el mensaje no podía transmitirlo y el que lo transmitía no lo conocía. De todos los especialistas rusos llegados a España, F. M. Ogaryshev, G. K. Mucha y Z. V. Berezin fueron los más importantes. Su función principal fue la organización de la captación de mensajes transmitidos entre las tropas nacionales y el cuero de ejército italiano. Al principio su contribución fue modesta, ya que tenían la dificultad de trabajar en un idioma muy desconocido, pero poco a poco este problema se fue superando. Las

comunicaciones que no podían ser descifradas eran enviadas a Moscú, donde un grupo de especialistas los estudiaban e intentaban su descifrado. Los especialista soviéticos, también, se encargaron de formar el personal del Negociado de Criptografía de la Sección de Información del Estado Mayor Central de la República. Dicho Negociado estaba formado por un par de subnegociados, el primero de cifra y claves, dedicados respectivamente al cifrado y descifrado de mensajes y a la creación de cifras y material de cifra, y el segundo de criptografía que, paradójicamente, se dedicaba al criptoanálisis.

Una ayuda inestimable, para ambos bandos, fue la descripción de las redes de comunicaciones enemigas. Una vez definidas las estaciones de radio, sus longitudes de onda, identificadores y horarios de emisión, era más fácil establecer los nuevos identificadores en el caso de cambio y, en consecuencia, ayudar a determinar las personas que aparecen en la comunicación.

Algún autor ha mencionado que la criptografía ha matado más gente que la bomba atómica. Es posible ya que el conocimiento de los planes enemigos antes de que se ejecuten es de un valor inestimable. Concretamente, en la Guerra Civil Española, la información proporcionada por los descifrados permitió obtener una ventaja estratégica de primer orden al bando nacional al disponer de una información privilegiada sobre la situación de las fuerzas enemigas, su composición, sus intenciones y sus carencias. En otros casos, el conocimiento de las claves del bando contrario logró capturar material e impedir el revituallamiento del enemigo. Por otro lado, los descifrados también podían servir para modelar la estrategia a seguir.

Sería fácil criticar las descoordinaciones, fallos y graves errores que sufrieron ambos bandos en cuestiones criptográficas. Sin embargo, hay que tener en cuenta que en la distancia todo parece fácil, pero había que estar allí.

La República dispuso desde el principio de mucha más gente dispuesta a arriesgar su vida, pero no supo, o no pudo dada su permanente falta de recursos, aprovechar el caudal humano a su favor. El modelo soviético no era fácilmente exportable a España, ni era probablemente el más adecuado. Evidentemente, se necesitaba un único servicio de espionaje y contraespionaje que canalizará la información provenientemente tanto del territorio nacional, como del extranjero, su

creación hubiera supuesto un aprovechamiento indudable de recursos y hubiera redundado en una mayor eficacia. Pero, mal podían asesorar los soviéticos en este aspecto cuando la falta de recursos había sido una lacra perenne de sus propios servicios, lo que hacía que se orientasen más a la delación y al miedo como herramientas de contraespionajes que a la investigación. La República tampoco supo ver la gran importancia que podían tener unos servicios de información en el exterior, quizás por la falta de personas adecuadas para dirigirlo, quizás por la división de estos. Finalmente, dos de los errores más importantes, siempre hablando de servicios de información, espionaje y contraespionaje, fueron la poca importancia dada al Norte de África y el poco uso que se hizo de los guerrilleros.

El bando nacionalista lo tuvo mejor en el aspecto humano desde el principio. El personal que estaba en su bando era profesional de las armas, y, al ser ellos los alzados en armas, la mayoría de la gente que se unía a sus filas era concordante con sus ideas. Por otro lado, la ayuda alemana e italiana fue determinante, por su capacitación técnica en cuestiones de información, muy superior a la española al principio de la guerra. También hay que destacar el acierto de unificar todos los servicios de información en uno, evitando las injerencias entre ellos y dotándolos de una visión única.

La aparición de la radiotelegrafía a finales del siglo XIX y su amplia utilización a partir del siglo XX significo una revolución en las comunicaciones. A partir de ese momento era posible la transmisión de información a grandes distancias y de una forma muy rápida. Pero, también, su facilidad de difusión implicaba una gran facilidad de intercepción, con lo que su principal ventaja se convertía al mismo tiempo en su principal inconveniente. España, aunque en los siglos XV y XVI fue una potencia criptológica de primer orden, y, a pesar de haber dado a la historia uno de los mejores libros de criptografía, en los años treinta no disponía de una disciplina criptográfica estricta ni métodos de cifrados adecuados para la época. Por lo que se hizo imprescindible la intervención de potencias extranjeras, para ambos bandos, en cuestiones criptográficas.

Tras la Guerra Civil española, la evolución de la criptología en España se ha tratado de manera conjunta a la del resto de las naciones en sus respectivos apartados.

Desarrollos interdisciplinares futuros

Como se ha desarrollado a lo largo de este proyecto, la criptología ha jugado un papel fundamental a lo largo de todos los tiempos. Su utilización estaba principalmente encadenada a temas de defensa, militares y bélicos. En la actualidad, la criptología sigue siendo imprescindible con relación a estos temas ,ya que desgraciadamente las guerras y conflictos militares siguen existiendo, pero además ha vuelto sus ojos a todo tipo de temas relacionados la comunicación.

De todos es sabido que la evolución de los ordenadores ha sido muy rápida, y que la mayoría de los hogares tienen un ordenador, así mismo los usuarios de Internet se cuentan por millones y puede afirmarse que casi todos los jóvenes (cada vez más jóvenes) tienen varias cuentas de correo electrónico, un teléfono móvil y desde luego casi todos aspiran al teléfono WAP. Por lo que, evidentemente, el uso de la criptología es y será imprescindible para todo el mundo de la comunicación y seguridad.

La utilización de la criptología en masa y para temas diferentes de los propiamente bélicos está creando muchas dificultades, no sólo las técnicas propiamente dichas sino también otras muy importante de origen legal e incluso moral. El estado actual de las cosas en critografía es un encarnizado debate entre los partidarios de la libertad absoluta para codificar todos los mensajes, cada uno con su propio código y los que son partidarios de controlar las comunicaciones para poder salvaguardar a la sociedad de todo tipo de delincuentes: terroristas, asesinos, ladrones, etc.

En un lado de esta contienda se encuentran la mayoría de los gobiernos de los países, sobre todo después de lo ocurrido en Nueva York el 11 de septiembre de 2001, casi todos ellos tienen medios para rastrear las comunicaciones buscando palabras o expresiones determinadas. El sistema más potente de rastreo pertenece a los Estados Unidos y se llama Echelon, el cual busca en correos electrónicos, faxes, llamadas telefónicas, etc. tratando de encontrar una serie de palabras concretas como pueden ser: "asesinar", "Bin Laden", etc., pero si no cuentan con el método o no pueden hacerlo sencillamente lo legislan. En España, desde octubre de 1992 existe la Asociación Española de Criptología y Seguridad de la Información, la cual fue fundada por Lorenc Huguet (actual Rector de universidad en Baleares), amparo Fúster y Dolores de la Guía

(ambas del CSIC), además el 8 de abril de 1998 se aprobó la Ley General de Telecomunicaciones que en su articulo 52 sobre cifrado en las redes y servicios de telecomunicaciones se legisla que el cifrado es un instrumento de seguridad de la información, pero entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de notificar bien a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, a efectos de su control de acuerdo con la normativa vigente. Del mismo modo el 27 de junio de 2002 se aprobó la Ley de Servicios de la Sociedad de la información y el Comercio Electrónico que obliga a los servidores a guardar copia de todos los correos electrónicos que difundan durante al menos seis meses. En septiembre de ese mismo año la Unión Europea, bajo la presidencia de Dinamarca, debatió y aprobó una ley por la que los servidores de toda Europa deberán almacenar los correos electrónicos durante todo un año.

En el otro lado se encuentra la mayoría de los usuarios que piden privacidad absoluta. Entre todos ellos destaca Phill Zimmermann, ingeniero informático que lidera a nivel mundial la privacidad y el cifrado personalizado, que ha diseñado un sistema de cifrado llamado PGP (Pretty Good Privacy), el cual distribuye gratuitamente desde junio de 1991 por Internet para que todo el mundo tenga su propia codificación. Dicho sistema se basa en un cifrado llamado IDEA, que es similar a DES. La idea de PGP es codificar el mensaje con IDEA, pero para evitar ataques, simultáneamente al mensaje, el emisor también manda la clave de IDEA, codificada mediante RSA. Además de esto, la clave utilizada no se hace de forma consciente por el emisor, sino que la genera el propio ordenador según los movimientos aleatorios del ratón. Para añadir a todo esto más seguridad, Phill Zimmermann, ha añadido a PGP la posibilidad de la firma digital, llevada a cabo por el sistema ElGamal, en los mensajes. Evidentemente, este sistema ha causado muchos problemas a su autor con el gobierno de su país y ha sido acusado por el FBI de traficante de armas por exportar PGP vía Internet.

En España en 1996 aparece el primer boletín de criptografía, PGP Megazine, fundado por José Manuel Gómez y que en el año siguiente, 1997, se convierte en Kriptopolis.com, la página Web de criptografía más visitada en España.

Las tres grandes ideas de los últimos años en criptografía: intercambio de claves de Diffe-Hellman-Merkie, clave asimétrica RSA y Lucifer, han abierto nuevas líneas de investigación que van dando su fruto.

Dentro del intercambio de claves se han estudiado varios protocolos muy operativos como:

- Protocolo de autentificación de sello temporal.
- Protocolo de autentificación con números aleatorios.
- Protocolo de autentificación con números aleatorios y funciones unidireccionales.
- Protocolo de rana habladora, Meyer y Matyas en 1982.
- Protocolo Needham-Schroeder en 1987.
- Protocolo de Otway-Rees modificado en 1987.
- Protocolo de Kerberos.

Desde la aparición de Lucifer por Feistel, se ha investigado en la misma línea, dando lugar a lo que se denomina cifrados en bloque o cifrados de Feistel, los más utilizados son: LOKI (1990), Feal (1988), PEES (1990) y de este IDEA (1991), RC5 (1994). Aunque el más usado es el DES (1976) y de este DEA (1981) que es el habitual de codificación, a pesar que se sospecha que la NSA tiene alguna puerta falsa para descifrar los mensajes. No es un método infalible, pero nadie ha conseguido descifrarlo, se cree que la única forma de atacarlo es probando todas las claves posibles. Por supuesto, al ser muy lento no se usa para mensajes grandes sino sólo para pequeños mensajes: claves de otros mensajes, firmas electrónicas, identificaciones, contraseñas, etc.

El futuro de la informática parece que apunta a corto plazo por lo que se llama ordenador paralelo, ordenador con un procesador que puede realizar varias funciones a la vez. En estos momentos, el procesador, hace operaciones muy rápidas, pero de una en una, se está intentando, imitando al cerebro humano, que el procesador realice operaciones diferentes en diferentes zonas. También parece que está muy cerca el biochip, chip que se basa en moléculas orgánicas sensibles a la corriente eléctrica y que posiblemente puedan injertarse en seres vivos.

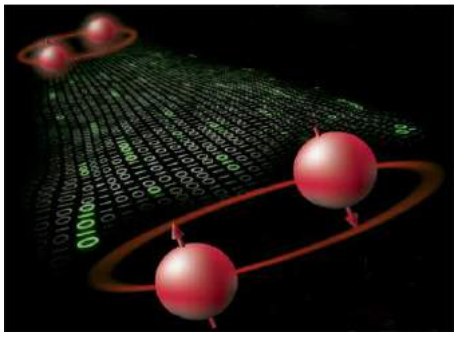
A más largo plazo, el mundo de la informática camina hacia los ordenadores cuánticos, niveles subatómicos, quizás ordenadores ópticos y velocidad de la luz. Pero lo que es indudable es que serán ultrarrápidos.

Lo que es evidente es que viendo las máquinas que actualmente están en el mercado, o las que algunos tienen, supongo que será probable que algunos gobiernos ya tengan ordenadores que los usuarios tendremos dentro de diez o quince años.

En cuanto al futuro de la criptografía, cualquier idea sobre el mismo es casi imposible de imaginar, lo que si puede conocerse son las actuales corrientes de investigación y comprobar los puntos y aspectos que más posibilidades tiene de llegar a desarrollarse. Lo que si es cierto es que cada país seguirá una línea de investigación diferente, de las cuales solo tendremos noticias, dentro de muchos años, cuando sean inútiles. En principio parece que una línea de actuación puede ir hacia la luz polarizada.

Fernando Acero expone en su bitácora un nuevo método de cifrado, basado en resistencias eléctricas que, a todas luces, parece ser más seguro y sencillo que la criptografía cuántica, a la par que más seguro y confiable. El autor, que habla muy bien de este método, pone en duda, no obstante, las razones que llevan a pensar que la criptografía cuántica está "tocada" puesto que este método es un paso adelante (¿o atrás?, por su sencillez) a las técnicas de cifrado cuántico de "toda la vida".

En un artículo aparecido en Physical Review Letters se explica un método por el cual se pueden romper los sistemas criptográficos basados en los principios de la mecánica cuántica. Dicho método se basa en permitir que el flujo de datos interactúe con un estado cuántico que viaja hacia atrás en el tiempo. Es decir, se usa la teoría general de la relatividad para alterar un sistema cuántico.



No son excesivas las investigaciones que se están realizando sobre criptografía cuántica. En Japón tienen un sistema en pruebas, y en Boston (Estados Unidos) existe un desarrollo similar cuya titularidad es del DARPA, el organismo cuyos avances en los años sesenta dieron origen a Internet.

En cuanto a España, se está trabajando en toda la línea de encriptación cuántica. La criptografía española se ha propuesto llevar a cabo una lucha desaforada contra los ciber delincuentes. Los teléfonos móviles de última generación se parecen cada vez más a un ordenador en miniatura, lo que significa que están amenazados por los mismos peligros, como virus, *spam* o ataques de ciber delincuentes. Para evitarlo, el reto para las compañías de software es mantener la seguridad de los terminales y las aplicaciones pero, sobre todo, las redes por las que circula la información, tanto inalámbricas como por cable. Así pues, el futuro está en la encriptación o criptografía cuántica, una tecnología que se remonta a los años ochenta y cuya segunda generación ya está aquí.

Como ya se ha explicado en el capítulo de criptología cuántica de este proyecto, la tecnología quantum key exchange (intercambio de claves cuánticas) se basa en un complejo protocolo mediante el cual el emisor y el receptor intercambian información en qubits (de quantum bits o bits cuánticos) codificados en fotones, lo que permite acordar entre las partes una clave con seguridad garantizada y virtualmente invulnerable.

En palabras de Christian Monyk, uno de los responsables del proyecto europeo SECOQC (Desarrollo de una Red Global para la Comunicación Segura Basada en la Criptografía Cuántica), "la información que se transporta puede leerse sólo una vez y ningún fisgón puede descifrar las claves sin ser descubierto". La tecnología permite refrescar infinidad de veces por segundo las claves con las que se transmite la información.

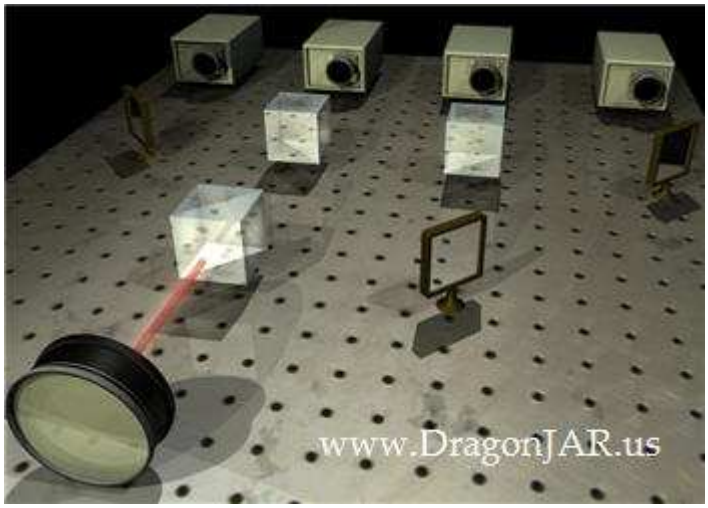
Esta teoría puede parecer ciencia ficción, pero podría estar en marcha en 2010 si se cumplen las previsiones de Vicente Martín, profesor de la Facultad de Informática de la Universidad Politécnica de Madrid y director del Grupo de Investigación en Información y Computación Cuántica. Martín y su equipo han desarrollado una red metropolitana basada en criptografía cuántica, la primera de las tres que existen en el

mundo que puede desplegarse sobre las redes ya existentes, por lo que “el desarrollo y aplicación de la tecnología es más barata con el mismo nivel de seguridad", dice Martín.

El proyecto cuenta con un presupuesto de 31 millones de euros y está apoyado por un consorcio de 12 empresas y 15 organismos públicos de investigación. De momento, “se prevé que los primeros usuarios sean organismos interesados en contar con alta seguridad, como el Ejército, el Gobierno, los bancos o empresas que necesiten seguridad extra", predice Martín. Telefónica, que lidera el consorcio de empresas investigadoras, ya está implantando una nueva red a base de fibra óptica pasiva que permitirá introducir en su interior corrientes de qubits que convivirían con los fotones de las telecomunicaciones convencionales, sin provocar interferencias.

Por ahora, sin embargo, la única posibilidad de que los ciber delincuentes no intervengan un teléfono móvil son los antivirus específicos. Según Gabriel Agatiello, de la compañía de seguridad Trend Micro, "los teléfonos cada vez almacenan más información sensible y, por eso, ya existen tecnologías de cifrado del dispositivo móvil". En todo caso, hay voces discordantes: según un informe de la compañía alemana de seguridad informática G-Data, las alertas sobre virus en móviles son desproporcionadas.

La delincuencia informática parece que va más rápida que su seguridad. Dentro de 30 años, muchos de los secretos que guarda el mundo moderno bajo potentes algoritmos criptográficos, como los datos médicos o la información clasificada de los gobiernos, correrán un peligro real de saltar por los aires. La criptografía cuántica se encargará de que su descifrado sea un juego de niños, susceptible de caer en manos de terroristas o criminales. Quien realizó tal profecía no fue un simple agorero, sino respetables investigadores como Martin Hellman, co inventor de la criptografía de clave pública, y el criptólogo argentino Hugo Scolnik, durante sus intervenciones en el Día Internacional de la Seguridad de la Información en la Universidad Politécnica de Madrid.



Hellman y Scolnik sostienen que la criptografía cuántica está aún en un estado embrionario y hasta dentro de 30 años no se verán sus primeras aplicaciones prácticas, que romperán con facilidad los actuales sistemas de cifrado. Mientras tanto, ha empezado una carrera paralela para proteger la información que debería seguir siendo secreta cuando irrumpa la criptografía cuántica. Hellman aseguró que está preocupado por si cae en malas manos. De momento, los investigadores trabajan en una de las pocas soluciones a su alcance: cifrar las cosas por duplicado, combinando criptografía simétrica y asimétrica, de forma que si la cuántica rompe la asimétrica, quede aún en pie la simétrica. El problema, dijo, es que "es muy caro, por lo que sólo puede usarse para información realmente valiosa".

El riesgo de que esta novedosa tecnología se use con fines perversos no es ninguna utopía, ya ha sucedido con los programas informáticos, como demostró Sergio de los Santos, consultor de seguridad de Hispasec Sistemas: "En el código malicioso hemos pasado del romanticismo al todo por la pasta, gente organizada que presta especial atención a atacar la banca en línea". Como ejemplo de su creciente poder, mostró fotos de una lujosa fiesta en Praga que reunió a algunos de estos nuevos criminales.

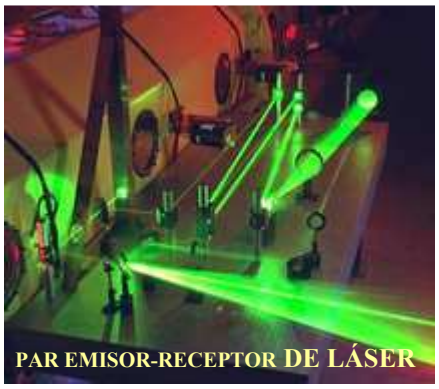
Según De los Santos, los ciber delincuentes "funcionan como una industria, el código que producen es muy bueno y sofisticado, optimizando los recursos para obtener mayores beneficios". Ni los antivirus ni los cortafuegos protegen ya contra estos criminales que "han tomado la Web para distribuir sus códigos y también como parte de

su infraestructura", refiriéndose a la Rusian Business Network, una empresa de San Petersburgo que vende servicios Web para distribución de código maligno y phishing.

Una muestra de la sofisticación de esta industria es la familia de troyanos Sino Wall, explicó De los Santos: "Una vez te has infectado, el troyano queda latente, vigilando tus hábitos de navegación. Cuando detecta que has visitado algo interesante, por ejemplo un banco, envía esta información cifrada al criminal, que decide si es un objetivo apetecible y si tiene algún código malicioso específico para él. Si se da el caso, lo instala en tu máquina para que robe tus claves".Otra muestra de la complejidad de estos troyanos es su funcionamiento modular, de forma que el mismo pueda servir para diversas funciones, al gusto del criminal: enviar correo basura, bombardear redes o infectar otros ordenadores. Además, detectan el navegador que está usando su víctima y descargan troyanos específicos para aprovechar los agujeros de este programa. Fernando Acero, de Hispalinux, añadió: "Si tu ordenador está infectado con un troyano, hará las operaciones que quiera con tu DNI electrónico".

El director de la Agencia Española de Protección de Datos, Artemi Rallo, ofreció otro ejemplo de mal uso de la tecnología: el trabajador que instala en el ordenador de su oficina un programa de intercambio de archivos y lo configura mal, de forma que abre al acceso público la base de datos de la empresa, con información privada de miles de personas. "Ya ha habido una sanción y habrá otras, algunas por datos más sensibles", anunció Rallo. El director de la agencia se quejó de que "no hay información sobre los riesgos que plantean las herramientas tecnológicas, ni tampoco conciencia ciudadana sobre privacidad". Y preguntó al público: "¿Cuántos ciudadanos pulsan la cláusula de privacidad de la Web que visitan?: uno de cada 10.000. Nadie quiere perder ni tres segundos en conocer los riesgos a que se expone".

Por lo tanto, en un futuro próximo, la computación cuántica nos permitirá descifrar, de manera relativamente fácil, la información cifrada con los métodos actuales. Sin embargo, otra aplicación de la física cuántica, la criptografía cuántica, nos permitirá usar nuevas formas de cifrado que resultarán virtualmente indescifrables. Su aplicación práctica está más cerca gracias a una investigación del laboratorio Cavendish de la Universidad de Cambridge. Sus desarrollos hacen viable la comunicación de banda ancha en canales cifrados cuánticamente.


PAR EMISOR-RECEPTOR DE LÁSER

La mayoría de sistemas de cifrado actuales se basan en la utilización de combinaciones numéricas para ocultar la información. Utilizan problemas matemáticos difíciles de resolver por los ordenadores actuales, como descomposiciones de números primos muy grandes. Esas combinaciones numéricas son tan complejas que garantizan que la información no pueda ser descifrada. Aunque esto no es estrictamente cierto. Simplemente, esas claves son suficientemente complejas como para garantizar que no pueden descifrarse en un cierto período de tiempo, lo suficientemente largo como para ser consideradas seguras.

La física cuántica dice que no se puede medir un sistema sin alterarlo, ya que con el mismo acto de medirlo ya lo estamos alterando de alguna manera. La criptografía cuántica se basa en ese principio para cifrar la información. Si alguien intenta leer el mensaje sin la clave correcta, la información se destruye en el proceso, emulando la idea de Leonardo DaVinci en su criptex.

Como normalmente se utilizan los fotones de luz como vehículo de información, los cuales se polarizan mediante filtros, haciendo que vibren en una dirección determinada, y se envían, la única manera de leer la información de esos fotones es hacerla pasar por filtros que estén orientados del mismo modo en que fueron enviados. Por consiguiente, sólo hay una oportunidad de leer la información contenida en un fotón. Ya que, el mismo acto de filtrarlo altera su estado de vibración, así que la información se pierde si el filtro no es el correcto. Si alguien intenta interceptar los fotones para descifrarlos, al no conocer la combinación de filtros adecuada nunca tendrá acceso a la información. Además, al intentar leer los fotones los estará corrompiendo, de forma que el receptor original verá las alteraciones provocadas por el intruso y sabrá de su presencia. Lo cual hace de este sistema el idóneo para la seguridad.

Una razón por la que aún no hay una aplicación práctica extendida de esta tecnología es que la comunicación debe hacerse por un canal cuántico limpio, que no altere los fotones durante el viaje. De momento se ha conseguido probar un canal válido

para este tipo de comunicación de unos 150Km de largo usando fibra óptica. Una distancia semejante se ha alcanzado probando comunicaciones entre satélites en órbita, donde la densidad de la atmósfera es tan tenue que casi no altera los fotones. Por otro lado, además, se requiere que se efectúen avances en la tecnología necesaria para transmitir la señal, tanto en la tecnología necesaria en el emisor para codificar y enviar la señal, así como en el receptor para recibir y descodificar la información. Hasta ahora era necesario usar sistemas criogénicos y combinaciones complejas de dispositivos ópticos avanzados. Sin embargo, los técnicos del laboratorio Cavendish de la Universidad de Cambridge han desarrollado un par emisor-receptor que resuelve en gran medida este problema. Han creado un sistema que utiliza un láser atenuado como emisor de fotones, y un detector compacto de fotodiodos como receptor. Ambos son capaces de trabajar a altas velocidades. Según su estudio, utilizando estos dispositivos sería viable la comunicación de banda ancha de alta seguridad en canales de fibra óptica.

Todd Brun de la Universidad del Sur de California en Los Ángeles y sus colegas han encontrado una manera de usar los estados definidos por la formulación de Deutsch para decodificar los mensajes cifrados cuánticamente. Un mensaje típico sería enviado como una serie de partículas, cada una de las cuales puede estar en tres estados diferentes: "cero", "uno" y "superposición" (una combinación de "cero" y "uno"). El receptor mide cada partícula pero necesita información adicional posterior del emisor para distinguir los estados que son superposiciones de los que no lo son. Sin embargo podría haber un escucha capaz de distinguir según se está produciendo la transmisión, digamos, entre un "cero" y una "superposición", podría interceptar el mensaje y también enviar partículas al receptor que imitasen las originales, evitando, de esta forma, la detección. Evidentemente, esto no sería posible sin un conocimiento avanzado del estado original. No obstante estas amenazas existen y una forma de resolverlas viene dada por la física teórica, ya que, dichas amenazas a la seguridad de las transmisiones basadas en criptografía cuántica sólo las resolverá una teoría cuántica de la gravitación.

Por otro lado, parece ser que un equipo de científicos ha logrado demostrar que la tele-clonación cuántica es posible. En esencia, esto consistiría en conseguir varias copias remotas de un haz láser, incluyendo los estados entrelazados de los fotones que lo integran. De confirmarse, este hallazgo permitiría realizar escuchas en una línea protegida mediante criptografía cuántica. Ya que bastaría clonar el haz de partículas y

direccionar uno de los clones a su destino legítimo, a la vez que usamos el otro para escuchar la línea, sin ningún peligro de ser descubiertos...

En esencia, el trabajo de un criptólogo consiste en buscar problemas imposibles (o muy difíciles) de resolver, como el de conocer el estado completo de una partícula sin alterarla, y buscar mecanismos para que aquellos que pretendan acceder de forma no autorizada a la información se vean obligados a enfrentarse al mismo. Esta es una diferencia esencial con la mayor parte de las ramas de la Ciencia, que suelen buscar soluciones a los problemas, y que generalmente se muestran especialmente incómodas frente a las cuestiones no resueltas. Es muy peligroso aventurarse a predecir cómo evolucionará este tema; si realmente esta -u otra- novedosa técnica acabará con este tipo de criptografía prácticamente antes de haber nacido, o todavía quedan resquicios en la Física Cuántica adecuados para pergeñar nuevos métodos de protección de la información. Lo que sí parece que está quedando cada vez más claro es que, si ramas de la ciencia tan ampliamente conocidas y estables como las Matemáticas, todavía nos sorprenden de vez en cuando al utilizarlas como base para desarrollar nuestros algoritmos de protección de la información, confiar en propiedades del mundo físico que apenas conocemos parece, cuando menos, aventurado. De cualquier modo, hoy por hoy y en un futuro próximo, el hecho de que se haga viable la criptografía cuántica es una buena noticia para entes tan importantes como los gobiernos o la banca, puesto que la confidencialidad de las comunicaciones es básica para ellos. Y de esta forma se apaciguarán sus recelos ante la llegada de los computadores cuánticos, que podrían suponer una amenaza para su seguridad. Este hecho también puede favorecer las inversiones y las apariciones de proyectos en este campo.

Por último me queda señalar las principales tecnologías que cambiarán el mundo en el siglo XXI:

Wireless Sensor Networks
Injectable Tissue Engineering
Nano Solar Cells
Mechatronics
Grid Computing
Molecular Imaging

Nanoimprint Lithography

Software Assurance

Glycomics

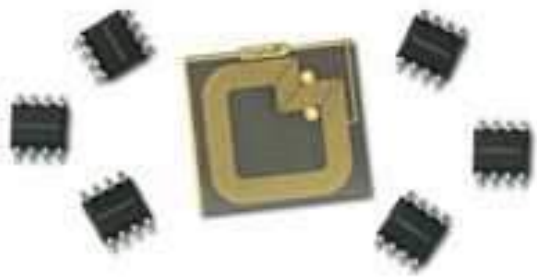
Quantum Cryptography

Resultados y Conclusiones

Por ser este un proyecto puramente investigativo, no se han obtenido resultados numéricos mediante una experimentación. Pero sí es muy importante resaltar algunos hechos y datos que determinan la bondad de los principales puntos del proyecto.

La seguridad informática es mucho más que criptografía; es gestión, auditoría, normativas, legislación, análisis de riesgos, protección de redes, protocolos, protección de datos personales, sistemas de identificación, metodologías, hardware, etc. y personas. Y al final, todo suele romperse por el punto más débil, el ser humano. Opino que la e-confianza se alcanza solamente si todos estos apartados se llevan a buen puerto, en especial el factor humano, la concienciación. Hoy por hoy, la seguridad absoluta en las comunicaciones no existe, por lo que la criptografía es únicamente capaz de poner barreras más menos difíciles de franquear para poder considerar dos campos bien diferenciados al hablar de la seguridad ofrecida por la criptografía: seguridad de los operadores y seguridad de los protocolos.

Chip CryptoCompanion para ofrecer seguridad criptográfica en sistemas embebidos



La seguridad de los operadores criptográficos se considera violada cuando ha sido posible obtener la clave secreta del sistema distinguiéndose:

■ Seguridad incondicional: es la ofrecida por los métodos de cifrado para los que se puede demostrar que no existe posibilidad de conocer la clave aún conociendo el método de cifrado, llamándose cifrados perfectos.

■ Seguridad computacional: es la ofrecida por aquellos métodos de cifrado tales que no existe capacidad de cálculo suficiente para obtener su clave secreta asociada, definida dicha seguridad de acuerdo con la teoría de la complejidad algorítmica, los conocimientos matemáticos actuales y las prestaciones de los ordenadores.

■ Seguridad probable: es la ofrecida por aquellos métodos de cifrado que aún sin estar basados en principios matemáticos de seguridad demostrable, no han podido ser violados pese a los continuados esfuerzos para conseguirlo, los cuales suelen utilizar técnicas especiales para el barajado de información mediante operaciones lineales y no lineales de bits, de forma que el esfuerzo computacional necesario para romper el sistema se presupone razonablemente superior a la capacidad de cálculo del atacante.

■ Seguridad condicional: es la ofrecida por todos los demás métodos, es decir, por aquellos procedimientos de cifrado diseñados con fines específicos y para los que la dificultad de violación es siempre muy superior a la supuesta capacidad de un eventual atacante.

En la seguridad de los protocolos, cualquiera de ellos puede ser vulnerable si no está bien diseñado y sus posibles debilidades matemáticas no han sido analizadas. En este caso, es posible que la violación del protocolo pueda incluso llevarse a cabo sin necesidad de encontrar la clave secreta del operador que lo genera, es decir, el protocolo puede ser vulnerable aun a pesar de utilizar un operador criptográfico seguro. Por todo ello, la seguridad de los protocolos es un parámetro difícil de definir, puesto que cada uno de ellos tiene características propias, las cuales ofrecen en cada caso la posibilidad de llevar a cabo gran diversidad de ataques.

Hay una cuestión crucial que se ha de tener en cuenta a la hora de cifrar un mensaje: ¿clave pública o clave secreta? La criptografía de clave pública aporta solución a muchos más problemas que la criptografía de clave secreta, surgiendo entonces la pregunta de cuál es la utilidad de los cifrados simétricos. Existen dos razones fundamentales para escoger un cifrado simétrico como el DES o el AES: por una parte, la mayoría de los sistemas de cifrado de clave pública son muy lentos; por ejemplo RSA es varios centenares de veces más lento que AES implementándose en software y es completamente imposible implementarlo en hardware; actualmente donde la velocidad de transmisión de la información constituye un punto crucial, el algoritmo de cifrado no

puede ser el factor limitante. Por otro lado, desde el punto de vista de la seguridad, hay problemas relativos a la estructura misma de los sistemas de cifrado de clave pública.

El tamaño de las claves necesario en criptografía de clave pública para asegurar una seguridad satisfactoria es mayor que el tamaño de claves en criptografía de clave secreta. En realidad, la noción y la importancia del tamaño de la calve para asegurar la seguridad no tiene sentido más que en el caso de la calve secreta. De hecho, esos sistemas se basan en la hipótesis de que los únicos posibles ataques son los llamados ataques exhaustivos (o por fuerza bruta) que consisten en enumerar todas las claves posibles.

Por el contrario, en el caso de clave pública, el tamaño de la clave no tiene sentido más que cuando se considera el mismo sistema. De hecho, por ejemplo el sistema RSA de 512 bits es mucho menos seguro que el sistema AES de 128 bits. La única medida válida para evaluar un criptosistema de clave pública es la complejidad del mejor ataque conocido. La mayor diferencia es que jamás se está al abrigo de ataques teóricos. Muy recientemente un grupo de investigadores ha conseguido factorizar un número de 512 bits, lo que trae como consecuencia que para tener una seguridad suficiente para los próximos años, se aconseja generalmente utilizar números de 1024 bits.

En cifrado, es mejor entonces utilizar algoritmos de clave secreta cuando sea posible, por lo que una solución aceptable es el compromiso elaborado por Zimmerman para concebir PGP. El principio de cifrado es: supongamos que X y Z desean comunicarse de manera íntegra, utilizando un algoritmo de clave secreta (siendo este algoritmo IDEA en el caso de PGP); X y Z se ponen de cuerdo sobre la clave secreta por un protocolo de intercambio de claves; este tipo de protocolos utiliza propiedades de criptografía de clave pública. Después se comunican utilizando el algoritmo IDEA que es público. Una vez que su conversación ha terminado, rechazan la clave de esa sesión.

Tal sistema combina las ventajas de los dos tipos de criptografía; de modo que para concluir se establece que lo más seguro es utilizar los algoritmos de clave secreta en los cifrados, habiendo previamente cifrado la calve con algún algoritmo de clave pública, debido a que en general, se considera que la mayor debilidad se encuentra en el protocolo de intercambio de claves.

Por la nebulosa que le rodea y la posibilidad de sumirnos en un mundo de ciencia ficción, los ordenadores cuánticos generan mucha polémica. Hay evidencia y se puede comprobar por los resultados publicados en congresos e Internet que se han logrado interesantes desarrollos científicos relativos a la computación cuántica con decenas de bits, y que ello podría significar un verdadero crack en el mundo de la criptografía.

De existir aparatos con esas características pero trabajando con centenares o miles de bits, traería como consecuencia inmediata que toda la seguridad criptográfica que hoy conocemos se quedaría en papel mojado.

De todas maneras, no nos engañemos, la seguridad actual es sólo probabilística: alguien puede dar con la clave privada del Banco de España en un segundo, algo tan simple como acertar un número de unos 320 dígitos, que sería la clave privada del certificado digital de esa entidad... pero esa probabilidad es tan pequeña que confiamos en la seguridad del sistema.

La criptografía cuántica es un sistema de cifrado indescifrable. Puede que esto parezca una afirmación bastante exagerada, sobre todo a la luz de anteriores afirmaciones similares. En diferentes momentos de los últimos dos mil años, los criptógrafos han creído que la cifra mono alfabética, la cifra poli alfabética y las cifras de máquina como la Enigma eran indescifrables. En cada uno de estos casos se demostró posteriormente que los criptógrafos estaban equivocados porque sus afirmaciones se basan meramente en el hecho de que la complejidad de las cifras superaba el ingenio y la tecnología de los criptoanalistas en un determinado momento de la historia. Con la

perspectiva del tiempo, se puede ver que los criptoanalistas descubrirían inevitablemente una forma de descifrar cada cifra o de desarrollar la tecnología que la descifraría.

Sin embargo, la afirmación de que la criptografía cuántica es segura es cualitativamente diferente de todas las afirmaciones anteriores, siendo dicha criptografía no sólo de hecho indescifrable, sino absolutamente indescifrable. La teoría cuántica, la teoría de más éxito en la historia de la física, significa que es imposible que Y intercepte con exactitud la clave de cuaderno de uso único establecida entre X y Z, Y ni siquiera puede tratar de interceptar la clave de cuaderno de uso único sin que X y Z adviertan su espionaje. En realidad, si un mensaje protegido por la criptografía cuántica fuese descifrado alguna vez, esto significaría que la teoría cuántica es errónea, lo que tendría implicaciones desastrosas para los físicos; se verían obligados a reconsiderar su comprensión de cómo funciona el universo en su nivel más fundamental.

Si se pueden construir sistemas criptográficos cuánticos que operen entre grandes distancias, la evolución de las cifras se detendrá habiendo llegado la búsqueda de la privacidad a su fin. Habrá disponible una tecnología que garantice las comunicaciones seguras a los gobiernos, el ejército, las empresas y el público, habiendo ganado los creadores de cifras la guerra que han mantenido a lo largo de toda la historia de la criptografía con los descifradores. La única cuestión que queda es si los gobiernos nos permitirían usar esa tecnología haciéndose dichos gobiernos la pregunta siguiente: ¿cómo regular la criptografía cuántica para que enriquezca la Era de la Información sin proteger a los criminales?

Gestión del proyecto

Se tratará de establecer una relación entre el esfuerzo intelectual realizado y los distintos costes tanto directos como indirectos que se han producido a lo largo del proyecto.

13) Medios técnicos empleados para el proyecto

En la realización del proyecto ha sido necesario utilizar varias herramientas tanto de software como de hardware. Seguidamente se muestra un listado con los medios tanto físicos como lógicos que han sido necesarios para el desarrollo del proyecto:

- Herramientas hardware
  - Portátil Toshiba S A 80-131 2.0 Ghz. 0,5 Gb RAM, 30 Gb. Disco duro.
  - Ordenador sobremesa hp Dual Core 2.4Ghz. 2Gb RAM, 140 Gb d duro.
- Harramientas software
  - Sistema Operativo Microsoft Windows XP.
  - Microsoft Office 2003 Professional.
  - Microsoft Office PowerPoint 2003 Professional
  - Navergador Mozilla Firefox versión 2.0.0.14.

14) Análisis económico para el proyecto

En esta sección se pretende realizar un análisis económico detallado del coste que ha supuesto la realización del presente proyecto. Debido a que el proyecto es puramente investigativo no se puede realizar un análisis tan detallado como en otros proyectos, por lo que se procederá a hacer una estimación del coste requerido para dicho proyecto estableciendo para ello el presupuesto inicial previsto, para más adelante contrastarlo con el presupuesto final y poder analizar las posibles desviaciones.

Para la realización de los presupuestos se ha utilizado la metodología de estimación de costes que a continuación se detalla:

- Recursos humanos: la forma de medir los recursos humanos utilizados son las horas/hombre. Para ello se ha llevado a cabo un control semanal de las horas dedicadas al proyecto.
- Herramientas software: para las herramientas software que se han utilizado se ha de contabilizar el precio de adquisición o alquiler, aplicando si procede el correspondiente prorrateo.
- Herramientas hardware: para las herramientas software que se han utilizado se ha de contabilizar el precio de adquisición o alquiler, aplicando si procede el correspondiente prorrateo.
- Costes indirectos: dentro de este grupo se incluyen los costes de utilización de las redes de comunicaciones, los costes de fotocopias, así como costes de transporte. La forma de medir estos costes es realmente compleja porque no se ha llevado a cabo un control explícito de los mismos, por lo que se estiman como un porcentaje de los costes directos.

14.1 Presupuesto inicial

A continuación se detalla cada uno de los recursos utilizados (pertenecientes a los cuatro grupos de recursos que se han descrito) indicando los costes asociados a los mismos.

■ Costes de personal. En la tabla que se muestra a continuación se encuentra desglosado el coste por hora imputada a cada fase del proyecto; debido a que este es un trabajo exclusivamente de investigación, dichas fases no son el ciclo de vida del proyecto sino más bien la fase de investigación propiamente dicha, la fase de transcripción del proyecto y la fase de revisión.

El cálculo necesario para obtener el número de horas realizadas en cada fase se obtiene de la multiplicación de los días necesarios para completarla por el número de horas que se ha trabajado cada día. Debido a que no todos los días se ha dedicado una jornada completa de 8 horas por motivos principalmente de estudio de asignaturas se calcula una aproximación de unas 5 horas trabajadas por día. Por ejemplo, el cálculo necesario para obtener el número de horas trabajadas en la fase de investigación es 105 días x 5 horas/día = 525 horas.

Es importante resaltar que existen dos trabajadores en el proyecto. El autor del mismo, que se encarga de realizar todas las tareas que se han planificado y el tutor que interviene en la fase de revisión. Para la contabilización de las horas se ha tenido en cuenta tanto las horas invertidas por el autor como las invertidas por el tutor.

La multiplicación del coste por hora entre las horas necesarias para completar una fase dan el coste total (en €) parcial de cada fase. El precio del coste por hora se ha obtenido mediante una estimación de los precios publicados en la A.L.I. (Asociación de doctores, Licenciados e Ingenieros en informática), de tal forma que la investigación se asemeja con la documentación, la transcripción y la revisión con la implantación.

Fase	Horas estimadas	Coste (€/Hora)	Coste total (en €)
Investigación	525	12	6300
Transcripción	75	12	900
Revisión	50	12	600

Por consiguiente el coste total de personal asciende a: **7800 €**

■ Costes de Hardware. La siguiente tabla refleja los equipos de hardware que fueron necesarios para la realización del proyecto:

Hardware	Coste sin I.V.A. (€)	Vida útil estimada (meses)	Tiempo de uso en proyecto (meses)	Coste imputable al proyecto sin I.V.A. (€)
Portátil Toshiba	900	54	4	66,6
Sobremesa hp	1200	60	4	80

Por consiguiente el coste total de hardware asciende a: **146,6 €**

■ Costes de software. La siguiente tabla refleja el software que ha sido necesario para la elaboración del proyecto. La única herramienta software que no aparece en esta tabla es la del navegador Mozilla firefox, debido a que la tasa de conexión a Internet se incluye en los costes indirectos y Mozilla es software gratuito de libre distribución.

Software	Coste sin I.V.A. (€)	Vida útil estimada (meses)	Tiempo de uso en proyecto (meses)	Coste imputable al proyecto sin I.V.A. (€)
Microsoft Windows XP	0 (Licencia incluida en el ordenador)	Indefinida (estimada 60 por vida útil)	4	0
Microsoft Office 2003 Professional	575,80	Indefinida (estimada 60 por vida útil)	4	38,38
Microsoft Office PowerPoint 2003 Professional	529,7	Indefinida (estimada 60 por vida útil)	4	35,31

Por consiguiente el coste total de software asciende a: **73,69 €**

■ Costes indirectos. Los costes indirectos se estiman como un porcentaje de los costes directos debido a la dificultad para su contabilización. Dentro de estos costes se incluyen el coste de conexión de la red eléctrica, red de comunicaciones de área local, gastos de fotocopias, gastos de desplazamiento, etc. Para este proyecto, se estima que los costes indirectos son un 20% de los directos.

En la tabla expuesta a continuación se refleja un resumen de los costes totales imputables al proyecto, acorde a los subtotales calculados en los apartados anteriores:

Concepto	Coste sin I.V.A. (€)
Coste de personal	7800
Coste de hardware	146,6
Coste de software	73,69
Total costes directos (TCD)	8020,29
Costes indirectos (20% TCD)	1604,06
Coste total (sin I.V.A.)	**9624,35 €**

Al ser un proyecto puramente investigativo, lo único que se podría pensar para obtener un beneficio es vender el propio proyecto como fuente de información al cliente, por lo que no tienen mucho sentido establecer un presupuesto para dicho cliente incluyendo en él el I.V.A. y el beneficio que se obtendría.

14.2 Coste final y análisis de desviación

A continuación se muestra la tabla que contiene el coste asociado a la planificación real del coste de personal. Las principales divergencias con la planificación inicial residen en el empleo real de los recursos.

Fase	**Horas estimadas**	**Coste (€/Hora)**	**Coste total (en €)**
Investigación	560	12	6720
Transcripción	85	12	1020
Revisión	47	12	564

Por consiguiente el análisis de la desviación es:

Total costes de personal (presupuesto real)	**8304 €**
Total costes de personal (presupuesto inicial)	**7800 €**
Diferencia con respecto planificación	**+ 504**

Como se puede observar en la planificación real se emplearon más recursos que los planificados inicialmente (cosa lógica en un proyecto investigativo) para las fases de investigación y transcripción, lo que ha supuesto un aumento en el número de horas y por lo tanto un aumento del coste parcial de dichas fases, lo cual arroja un resultado de un coste superior, aunque en la fase de revisión se ha empleado una duración menor a la prevista inicialmente. De todas maneras, a la vista de estos resultados, puede afirmarse que no existe una diferencia significativa en el precio total del proyecto.

Anexos y Bibliografía

Anexo1:

Nuevas Tecnologías, Nuevos Retos para la Defensa

La importancia de la información y su uso masivo en la sociedad y en las Fuerzas Armadas hace que la seguridad de su transmisión tome un papel fundamental. Antes el problema era aumentar la capacidad de transmisión para disponer de más datos, hoy en día es necesario ser cauto y analizar los contenidos de la información a transmitir.

La apertura y libre uso de las redes de comunicación como Internet o las Intranets proporcionan un gran medio de comunicación que no sólo facilita su uso legitimo, sino también para el planteamiento y preparación de acciones que van más allá de la legalidad.

Desde el punto de vista de las Fuerzas Armadas la seguridad de la información es de vital importancia, por lo que es preciso adoptar sumo celo en el uso de las nuevas tecnologías de la información tanto en su uso en acuartelamientos y bases militares como en Sistemas de Mando y Control.

Cuando se habla de seguridad en tecnologías de la Información no se debe olvidar que la misma está sustentada en la criptografía. La fuerza de la criptografía es la medida en tiempos y recursos que se requieren para convertir un texto original en otro cifrado y viceversa. El auge de la criptografía se debe:

■ Aumento de la velocidad de cálculo gracias a la aparición de los ordenadores.

■ Mejora e innovación de algoritmos matemáticos que ayudan a definir sistemas criptográficos estables y seguros.

■ Necesidad de seguridad por el aumento del uso de las redes de comunicación.

Internet está siendo el motor de cambio más importante de nuestro tiempo, cada día que pasa el hombre se hace más dependiente de Internet e igualmente se ha convertido en una parte integral de las infraestructuras militares y civiles. Es paradójico, que Internet naciera para reducir el peligro de pérdida de información que ocasionaría un

ataque nuclear soviético a los EEUU y sin embargo, esa red de redes pronto se ha convertido en su principal preocupación.

El ciberterrorismo se está convirtiendo en uno de los puntos más preocupantes para los responsables de la seguridad de todos los países desarrollados. En 1996 el director de la CIA, John Deutch testificó que los ataques de hackers eran considerados como la segunda amenaza más peligrosa a los EEUU. Cuanto más sofisticado es el estado, más dependiente es de las computadoras y de las tecnologías de la información y más vulnerable a los ataques informáticos bélicos, como virus, códigos malignos y software de hackers.

En el ciberespacio es difícil diferenciar un ataque terrorista de cualquier otro. En el incidente denominado "Solar Sunrise" los sistemas militares de los EEUU fueron atacados electrónicamente y alguien desde un ordenador en los Emiratos Árabes Unidos parecía ser la fuente. Sin embargo, lo que estaba siendo atacado eran los sistemas sin clasificar logísticos, administrativos y de contabilidad esenciales para la gestión y despliegue de fuerzas militares. Dicho ataque fue llevado a cabo en el mismo momento en que se consideraba una acción militar contra Irak por su falta de cumplimiento con los equipos de inspección de la ONU. El primer momento de los ataques hizo sospechar que se tratará de un ataque informático en masa por parte de una nación hostil. Pero resulto que dos adolescentes de California bajo la dirección de un sofisticado pirata informático israelí, también adolescente, habían orquestado el ataque con herramientas de hacker disponibles en Internet.

Para clasificar como ciberterrorismo un ataque, éste debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo; ataque que deriven en muertes, explosiones, contaminaciones atmosféricas, etc. Está suficientemente probado que los grupos terroristas están utilizando Internet para coordinar operaciones y con fines propagandísticos y además a bajo coste. Del mismo modo, es sabido por todos que Al Qaeda estaba investigando métodos para realizar ataques informáticos, sus agentes visitaron muchos sitios Web, frecuentados por los hackers adolescentes, descargándose herramientas y preparando estrategias sobre como introducirse en las redes informáticas. Igualmente, llevaron a cabo una vigilancia de las redes informáticas que ayudan al funcionamiento de las redes

eléctricas, suministro de agua, de transportes y comunicaciones de los EEUU y dichas vigilancias se hicieron desde ordenadores situados por todo el mundo.

Los ciber ataques, independientemente del origen de la amenaza tienen una serie de características comunes. Los estudiosos del arte de la guerra empiezan a considerar el llamado ciberespacio como un nuevo escenario, donde ya se gestan nuevos actores y nuevas formas de conflicto

Algunos autores establecen grandes diferencias, dentro de los nuevos modelos de conflicto, en el ámbito de las nuevas tecnologías de la información entre guerra en red y la ciber guerra. La primera de ellas se plantea como conflictos de carácter social e ideológico entre naciones y sociedades, sostenidos en parte, por medios de comunicación propios de Internet. Su objetivo es dañar o modificar todo aquello que una parte de la sociedad sabe o cree saber sobre el mundo. Por otro lado, la ciber guerra pasa a un nivel de carácter militar, incluyendo los sistemas de mando y control del adversario, sus sistemas de información e inteligencia, así como sus sistemas de distribución y por tanto, la ruptura del sistema de toma de decisiones.

En el proyecto de investigación que se está llevando a cabo en MADOC/DIVA, la ciber guerra se ha considerado dentro del ámbito de la guerra de mando y control. La C2W (guerra de mando y control) viene definida por la actividad de la seguridad de las operaciones, la decepción, las operaciones psicológicas, la guerra electrónica y la destrucción física, mutuamente apoyado por la información, para ocultar ésta, influir, degradar o destruir la capacidad de mando y control del adversario, mientras que protege contra tales acciones las capacidades de mando y control propia.

Esta lucha por el control de las fuentes de información, lejos de favorecer la fortaleza informática, incide en la vulnerabilidad e inconsistencia de los sistemas de seguridad civiles y militares, nacionales e internacionales, por ello la seguridad informática y el sistema de telecomunicaciones es, y deberá seguir siendo, objeto de investigación y deben estar sujetas a un diseño de política de protección de los dispositivos y redes de información. Resulta, entonces, de vital importancia delimitar que información sensible debe ser reservada y cifrada y cuales son los riesgos y amenazas que pueden afectar a los sistemas de seguridad. Debe ser por tanto una prioridad el

establecimiento y extensión de medios, protocolos, sistemas y estrategias de organización de la información adecuadas a las nuevas condiciones de estructuración de las infraestructuras y sistemas de seguridad.

Anexo2:

La Seguridad en las Redes Militares de Telecomunicaciones

El objetivo principal de las redes de telecomunicaciones militares es transportar la información necesaria para la acción coordinada entre los diversos órganos que participan en la Defensa Nacional. La necesidad de proteger la información militar tendrá siempre un rasgo específico: la naturaleza de la amenaza.

Mientras las agresiones a las redes civiles tienen objetivos concretos, son realizadas con medios limitados y se producen aleatoriamente en el tiempo; los ataques a las redes militares son coordinados, cuentan con los medios nacionales hostiles y se multiplican en las épocas de crisis o guerra. Ese es el motivo por el que la seguridad de las redes de telecomunicación militar debe tratarse como un hecho cualitativa y cuantitativamente diferenciado.

El tema de seguridad que más preocupa a los militares es proteger toda señal electromagnética que proporcione información a un enemigo real o potencial, y todo documento, una vez haya sido depositado en el ámbito de la red, es decir, desde que el remitente lo presenta para su transmisión hasta que es entregado al destinatario. En consecuencia, serán consideradas las amenazas que ataquen directamente contra este objeto, y así quedaran excluidas otras, como el espionaje tradicional o el ataque por la fuerza a las estaciones, etc.

Existen distintas modalidades de seguridad frente al tipo de amenaza presente:

■ Seguridad física impidiendo el acceso a todas las personas no autorizadas.

■ Seguridad de Comunicaciones (COMSEC), conjunto de técnicas y dispositivos que ocultan el contenido informático de la comunicación, incluyendo todo el campo del cifrado.

■ Seguridad de Transmisión (TRANSEC), conjunto de técnicas y procedimientos para resistir o evadirse de las acciones de guerra electrónica o de inteligencia. Que se realicen sobre la señal transmitida.

■ Seguridad de Emisiones (EMSEC) protege la información de aquella que pudiera inferirse de emisiones radiadas de forma no intencionada.
■ Seguridad Informática (COMPUSEC) protege los sistemas informáticos del acceso de usuarios no autorizados y del ataque por técnicas típicamente informáticas.
■ Protección Nuclear, conjunto de dispositivos destinados a proteger los equipos del impulso electromagnético que se origina por la explosión en la atmósfera de ingenios nucleares.

Para que un plan de seguridad sea eficaz es necesario elaborar un plan de seguridad de comunicaciones que coordine todos estos aspectos tan diversos. La seguridad por si misma constituirá un subsistema, pues cuenta con una organización, unos medios humanos, medios materiales y unos procedimientos que le dan identidad propia. De tal forma que se define red segura como parte de la red general en la que se han adoptado las medidas y se han incorporado los medios necesarios para garantizar la protección de la información.

La arquitectura del subsistema de seguridad se configura en dos niveles, uno de gestión con órgano de mando y control y otro de red con un conjunto de áreas seguras y unos enlaces entre ellas que deben ser protegidos.

El subsistema de seguridad y, en particular, la red segura deben ser concebidos de acuerdo con unos principios esenciales. El cifrado es el aspecto de seguridad que más curiosidad despierta. Existen dos modelos genéricos de cifrado: el cifrado analógico y el cifrado digital. El empleo de uno u otro dependerá de la técnica empleada en la red y, sobre todo, del grado de seguridad requerido. Debido a la mejora en el grado de seguridad que ofrece la cifra digital, el empleo de las técnicas analógicas queda reducida a los casos de fuente y red analógicas. Cuando, además, las conversiones que exigiría la cifra digital, ocasionen molestias no aceptadas por el usuario o cuando la diferencia de coste no se justifique por la importancia de la información que se ha de cifrar (caso altamente improbable en aplicaciones militares). Debe añadirse que los clásicos retrasos y limitaciones de velocidad en las conversiones que constituían una objeción a la cifra digital han sido considerablemente mejorados con las técnicas tipo "vocoder".

La aplicación del cifrado a las comunicaciones presenta, asu vez, dos modalidades claramente diferenciadas:

■ Cifrado de enlaces: cifrado de canal ("channel encryption") y cifrado de grupo ("bula encryption"). La información es cifrada en su recorrido entre dos nodos consecutivos de la red, ya sea la de un canal de transmisión o la de varios canales. En cada nodo, la información es descifra a la recepción y cifrada de nuevo para su transmisión al nodo siguiente. Exige:

- Las tramas múltiples han de ser digitales
- La información permanece en claro en todos los nodos.
- Cuando no se conoce a priori la ruta que seguirá la información, la cifra debe extenderse a todas las rutas posibles

■ Cifrado extremo a extremo o de usuario (end to end encryption). El cifrado de la información se realiza en el equipo Terminal del usuario remitente y circula en modo seguro a través de la red, hasta ser descifrada en la Terminal del destinatario .Exige:

- Cifra únicamente el contenido informático.
- El coste es muy alto porque el número de equipos de cifrado es igual al número de usuarios a asegurar.
- La gestión de claves se complica por el número y dispersión de usuarios.
- Parte de la operación (paso de claro a cifra) queda bajo la responsabilidad del usuario, por lo que los descuidos y errores pueden multiplicarse.
- Las técnicas de cifrado y las conversiones originan retrasos y distorsiones.

En las redes extensas con numerosos usuarios que deban comunicarse todos con todos en modo seguro, la generación, distribución, empleo y cambio de las claves, elemento esencial del grado de seguridad del cifrado, es un problema complejo. Los métodos más utilizados son:

■ Generación y distribución previa con calendario fijado para los cambios, o por mutuo acuerdo entre corresponsales.

■ Estación central que asigna una clave para cada comunicación en el momento de establecerse.

■ Algoritmos de clave-pública que fraccionan la clave de cada usuario en una parte conocida públicamente (utilizada para cifrar los mensajes que le son dirigidos), y una parte privada (utilizada por el propio usuario para descifrarlos).

Anexo3:

Criptografía aplicada a la informática.

Toda la información a la que tiene acceso la sociedad está sometida a amenazas y riesgos de diversos grados, directamente relacionados con su valor económico, político y estratégico. Por supuesto, cualquier tratamiento de información implica ciertos riesgos calculados pero existen otros no evaluados. Por lo tanto, al hablar de seguridad es imprescindible evaluar todos los aspectos de la misma.

■ Seguridad física y control de accesos. En los últimos años se ha tomado conciencia en todo el país, de la importancia de la seguridad física y control de accesos por lo que se han creado multitud de empresas expertas en protección física.

■ Seguridad software. Todos los fabricantes de ordenadores proporcionen sus medios de protección contra el acceso de de personas no autorizadas, mediante palabras de paso. Por lo que mediante este modo, se controla el acceso a la utilización del terminal.

■ Seguridad criptográfica. Consiste en realizar un cifrado de la información, mediante unas claves y un algoritmo lo suficientemente complejo, para impedir que la información sea inteligible para cualquier persona que no disponga del mismo algoritmo y claves de cifrado. Si bien cifrar una información resulta sencillo, el hacerlo de una forma totalmente segura que suponga una garantía del más alto nivel, da lugar a la complejidad existente en los equipos criptográficos.

■ Estados de vulnerabilidad de la información. Se trata de dar soluciones para asegurar la información en los tres estados de procesado en que pueda encontrarse.

■ Almacenamiento de la información. Es el estado en el cual, la información permanece durante más tiempo. La forma de asegurar la información almacenada, está basada en medidas de seguridad física en los accesos donde ésta se almacena y en el tratamiento criptográfico de dicha información.

■ Transmisión de la información. Es el proceso en el cual más fácilmente puede desviarse la información, por lo que resulta totalmente necesario utilizar métodos criptográficos para conseguir un elevado grado de seguridad.

■ Métodos criptográficos: "Soft-Hard". Actualmente, hay dos formas básicas de cifrar la información: métodos "software" y métodos "hardware".Para conseguir un cifrado de alta calidad, ha de utilizarse un algoritmo muy complejo y con unas claves de longitud suficientemente elevada. Todo ello requiere realizar gran cantidad de operaciones, en las cuales un procesado por métodos software emplearía un tiempo excesivamente elevado. Por otra parte, utilizar la capacidad de procesado del ordenador para el cifrado de la información no resulta rentable.

En el proceso de transmisión de la información, las velocidades de transmisión utilizadas limitan el uso de métodos software y por lo tanto, hay que ceñirse a la utilización de cifradores de tipo hardware.

Todo ello hace que el uso de cifrado software sea cada día menor y que la gran mayoría de las aplicaciones criptográficas actuales estén implantadas en equipos criptográficos por hardware.

■ Criptografía en el almacenamiento de la información. La gran proliferación de los ordenadores personales ha ocasionado que sea necesario almacenar ciertos ficheros de información en forma cifrada.

El equipo criptográfico DPC 300 de Técnicas de Cifra, S.A., está especialmente diseñado para esta aplicación. Se utiliza especialmente con ordenadores personales y sirve para fichar un fichero específico y almacenarlo en uno nuevo. Los ficheros, una vez cifrados, pueden ser almacenados o transmitidos/recibidos a través de un sistema estándar de comunicaciones.

Igualmente, el DPC-3000 proporciona la capacidad de introducir y almacenar las claves criptográficas. Estas claves se introducen mediante un fichero desde el teclado, y se almacenan en una memoria RAM, situada en la tarjeta cifradora.

El DPC-3000 consiste en una tarjeta de cifrado y en un disquette con el software de aplicación necesario. Todo el proceso de cifrado se realiza por hardware en la tarjeta cifradora, así se evita la utilización de memoria del ordenador y se obtiene una velocidad de cifrado muy alta.

La tarjeta cifradora se instala en el bus de expansión del PC y dispone de su propio microprocesador, generador de claves y memorias de su almacenamiento.

El software se utiliza solamente como interface con el usuario y dispone de tres programas: el de cifrar un fichero, el de descifrar un fichero y el de gestión de claves.

El resultado del proceso son ficheros cifrados con una determinada clave, que contienen caracteres que no pueden ser sacados por impresora ni por pantalla.

■ Criptografía en la transmisión de información. El mayor riesgo en la filtración de información se produce durante su transmisión a través de la red de comunicaciones.

Existen varios métodos de transmisión de la información entre los que se distinguen: método a través de la red de télex, método mediante el telefax, método a través de las redes de datos.

■ Télex. La serie XMP de Técnicas de Cifra, S.A., proporciona la seguridad necesaria en las comunicaciones de mensajes a través de la red télex. Son terminales criptográficos independientes que incorporan todas las funciones de cifrado/descifrado y transmisión/recepción.

■ Con la aparición de nuevos equipos de comunicaciones, la red de télex tiende a desaparecer y está siendo sustituida progresivamente por la comunicación vía teléfax, mucho más rápida.

Actualmente, a menudo se puede seguir más de cerca la actividad de una organización, interviniendo su línea de teléfax, en vez de intervenir el teléfono.

La solución a este problema se obtiene mediante los cifradores de teléfax. El cifrador de teléfax DEL-7000 es un equipo compacto de alto nivel de seguridad, que

cifra los datos que van saliendo del teléfax a la línea de comunicaciones, mediante un proceso "bit" a "bit", no propagador de errores.

La introducción de claves se realiza desde un inyector de claves, externo a la unidad. Dispone de cuatro tipos diferentes de claves: básicas, de mensaje, de cliente y de familia, lo cual le da una máxima seguridad y una gran flexibilidad en su gestión.

■ Datos. La comunicación entre ordenadores puede establecerse de forma sincrónica o asincrónica.

Las comunicaciones sincrónicas se utilizan para transmitir información a gran velocidad. Las velocidades normales son hasta 512 KBPS, 1024 KBPS y 2048 KBPS. Los cifradores de datos sincrónicos de la serie DEL-7000, proporcionan seguridad del más alto nivel en comunicaciones de este tipo. Mediante un cifrado totalmente "hardware" y un equipo de pequeñas dimensiones, se puede cifrar información sincrónica incluso a velocidades como las anteriormente mencionadas.

Las comunicaciones asincrónicas se utilizan normalmente en canales que no soporten velocidad tan alta como las anteriores. Las velocidades típicas son 1200 BPS, 2400 BPS, hasta 19200 BPS. Los cifradores asincrónicos DEL-7010 de Técnicas de Cifra, realizan el cifrado en este tipo de comunicaciones hasta las velocidades máximas, permitidas en estos canales. Poseen las mismas características de sencillez y seguridad que todos los equipos de la serie DEL.

Actualmente se utiliza cada vez más, la transmisión de información a través de la red pública X.25 (BERPAC).

Por consiguiente, proteger la información mediante métodos de seguridad física, acceso "software" y criptográfica, es una necesidad vital en los tiempos actuales. Y, por supuesto, los métodos criptográficos proporcionan la forma más efectiva de conseguir un alto nivel de seguridad en los estados más vulnerables de la información: su almacenamiento y transmisión.

- **Libros:**

Singh, Simon, (2000). *Los códigos secretos*, Barcelona: Debate. [1]

Fuster-Sabater, A y Otros, (2000). *Técnicas criptográficas de protección de datos*, Madrid: Ra-Ma. [2].

Soler Fuensanta, José Ramón y Francisco Javier López-Brea-Espiau (2008), *Soldados sin rostro: los servicios de información, espionaje y criptografía en la Guerra Civil Española*. Barcelona: Inédita. [3].

Heiberg, Morten y Ros-Agudo Manuel, (2006). *La trama oculta de la guerra civil*, Barcelona: Crítica. [4]

Ortega-Triguero Jesús J., López-Guerrero, Miguel-Ángel y García-del-Castillo-Crespo, Eugenio C., (2006). *Introducción a la criptografía. Historia y actualidad*, Cuenca: Ediciones de la universidad de Castilla- La Mancha. [5]

Alcocer-y-Martínez, Mariano, (1934). *Criptografía española*, Madrid: Sn. [6]

Román-Sánchez, José-Antonio, (2002). *La escritura secreta: breve historia de la criptografía*, Málaga: I.E.S. Nuestra señora de la victoria. [7]

Ramió-Aguirre, Jorge. *Libro electrónico: Seguridad Informática*, cuarta edición versión v32, Universidad Politécnica de Madrid. [8]

Ministerio-de-Defensa, Centro-Superior-de-Información-de-Defensa, (1997). *Glosario de términos criptología*, Tercera edición, Madrid: Ministerio de Defensa, Secretaria General Técnica. [9]

Huecas-y-Carmona, Cesáreo, (1897-1898). *Escritos cifrados al alcance de todos: clave silabica para comunicarse en el lenguaje cifrado*, Segunda edición España: [s.n.], [s.a.]. [10].

REFERENCIAS:

[1] Consultado especialmente para los puntos referenciados en el índice como: el punto 4.4: la mecanización del secreto, el punto 6: Criptografía en la segunda Guerra Mundial, el descifrado del Enigma y la barrera del idioma y el punto 11: un salto cuántico al futuro. Además se ha utilizado para consultas generales en todo lo referente a criptografía antigua.

[2] Consultado especialmente para los puntos referenciados en el índice como: el punto 4: edad contemporánea, sobre todo el punto 4.3 criptografía de clave secreta, el punto 4.3.2: DES y el punto 4.3.3: AES, el punto 7: criptografía en clave pública y el punto 9:

protocolos criptográficos y firmas digitales. Además se ha utilizado para consultas generales en todo lo referente a criptografía antigua, particularmente en los procedimientos clásicos de cifrado (sustitución y transposición) y en lo referente al criptoanálisis.

[3] Consultado especialmente para el punto referenciado en el índice como: criptografía española, en particular el período comprendido entre los años 1936-1939: la guerra civil.

[4] Consultado especialmente para el punto referenciado en el índice como: criptografía española, en particular el período comprendido entre los años 1936-1939: la guerra civil.

[5] Consultado especialmente para los puntos referenciados en el índice como: el 3.3: Nomenclátor, el 3.4 cifrados poli-alfabéticos, el 4.1 cifrados poligráficos y el punto 5: criptografía en la primera Guerra Mundial. Además se ha utilizado para consultas generales en todo lo referente a criptografía moderna y para el punto 7: criptografía en clave pública.

[6] Consultado especialmente para el punto referenciado en el índice como: criptografía española, particularmente el el período anterior a la guerra civil.

[7] Ha sido utilizado para consultas generales de la mayoría de los apartados del proyecto.

[8] Consultado especialmente para los puntos referenciados en el índice como: criptografía en la actualidad, sobre todo el punto 9 de protocolos y formas digitales.

[9] Ha servido para llevar a cabo una consulta en la clarificación de conceptos concernientes a la criptografía.

[10] Ha sido utilizado para consultas generales de la mayoría de los apartados del proyecto.

- **Artículos en revistas:**

Ribagorda, Arturo, (1998). "Perspectiva técnica y legal de la criptografía frente al próximo milenio", *Novática,* nº 134, páginas 5-8. [1].

Dávila, Jorge, (febrero 2008). "32 años de criptografía asimétrica y de clave pública", *SIC,* nº 78, páginas 102-104. [2].

Zimmermann, P.R, (1998). "Criptografía para Internet", *Investigación y ciencia*, nº 267, páginas 74-79. [3].

Informe de National Encryption Survey (abril 2006). "La relevancia del cifrado y su uso generalizado en organizaciones lejos de su consolidación", *SIC,* nº 69, páginas 22-24. [4].

Delgado, Vera, (2006). "Aplicaciones prácticas de la criptografía", *Anales de mecánica y electricidad*, ISSN 0003-2506, Vol 83, Fasc 2, páginas 10-16. [5].

Delgado, Vera, (2006). "Introducción a la criptografía: tipos de algoritmos", *Anales de mecánica y electricidad*, ISSN 0003-2506, Vol 83, Fasc 1, páginas 42-46. [6].

Castillo-Chamarro, José- Miguel (junio 2004). "Nuevas tecnologías, nuevos retos para la defensa" *Memorial de Artillería*, nº 1, páginas 71-81. [7].

Jarauta-Sánchez, Javier (octubre 1990). "Criptografía aplicada a la informática", *Ejército*, nº 609, páginas 62-66. [8].

Manzanedo-Martínez, Antonio (octubre 1990). "Seguridad en las redes militares de telecomunicaciones", *Ejército*, nº 609, páginas 54-58. [9].

Gallego-Serra, Fermín (octubre 1988)."El secreto de las comunicaciones en la segunda guerra mundial: "la operación ULTRA"", *Revista española de Defensa*, nº 8, páginas 62-63. Permitió desvelar los sistemas alemanes de cifra arrojando nuevas luces sobre el conflicto. [10].

Soler, José-Ramón, (2005). "Un Centro de Escucha y Descifrado en la Guerra Civil Española" Fuensanta y López-Brea-Espiau, Javier, (Junio de 2005). *Revista Española de Historia Militar 59*, páginas 189-198. [11].

Gordillo-Courcières, José-Luis, (Abril 1994). "La captura del Mar Cantábrico", *Historia y Vida 313.,* páginas 107-114. [12].

Soler-Fuensanta, José-Ramón (Julio 2004). "Mechanical cipher systems in the Spanish Civil War", *Cryptologia,* Vol. XXVIII, nº 3, páginas 265 - 276. [13].

Soler-Fuensanta, José-Ramón y López-Brea-Espiau, Javier, (2005). "Los hombres que nunca existieron", *Revista Española de Historia Militar* nº 64, páginas 134-141. En ésta se dan los nombres de las personas que formaban el grupo de descifrado del Estado Mayor de la República y probables nombres del grupo Camazón. [14].

REFERENCIAS:

[1] Consultado especialmente para el punto referenciado en el índice como: Perspectiva técnica y legal de la criptografía frente al próximo milenio.

[2] Consultado especialmente para el punto referenciado en el índice como: punto 7: criptografía en clave pública.

[3] Consultado especialmente para el punto referenciado en el índice como: punto 8: criptografía para Internet.

[4] Consultado especialmente para el punto referenciado en el índice como: punto 10: la relevancia del cifrado.

[5] Consultado de forma general para todas las aplicaciones prácticas de la criptografía, particularmente de la de clave pública.

[6] Consultado de forma general para los ámbitos de la criptografía en los que se van definiendo y codificando los distintos tipos de algoritmos.

[7], [8], [9] Consultado para todos los temas relacionados con el apartado referenciado en el índice como criptografía actual.

[10] Consultado especialmente para el punto referenciado en el índice como: punto 6: Criptografía en la segunda Guerra Mundial, el descifrado del Enigma y la barrera del idioma.

[11], [12], [13] Consultado especialmente para el punto referenciado en el índice como: criptografía española, concretamente en el período de la guerra civil.

[14] Consultado especialmente para el punto referenciado en el índice como criptografía actual, en concreto a lo ocurrido en España.

- **Artículos en revistas digitales:**

Morales, Raúl (12 Noviembre 2008). "España contará en 2010 con una red metropolitana de criptografía cuántica", Facultad de Informática de la Universidad Politécnica de Madrid. [1]. URL correspondiente:
http://www.tendencias21.net/Espana-contara-en-2010-con-una-red-metropolitana-de-criptografia-cuantica_a2725.html

Martínez, Eduardo (15 Junio 2003). "La criptografía cuántica rompe la barrera de los 100 kilómetros". [2]. URL correspondiente:
http://www.tendencias21.net/La-criptografia-cuantica-rompe-la-barrera-de-los-100-kilometros_a179.html

Gutiérrez, César (11 Octubre 2008). "Se implementa la primera red protegida con criptografía cuántica". [3]. URL correspondiente:
http://www.tendencias21.net/Se-implementa-la-primera-red-protegida-con-criptografia-cuantica_a2624.html

Martínez, Yaiza (02 Febrero 2008). "Tele transportan un qubit fotónico a 7 metros conservando su información". [4]. URL correspondiente: http://www.tendencias21.net/Teletransportan-un-qubit-fotonico-a-7-metros-conservando-su-informacion_a2048.html

Piacente, Pablo-Javier (15 Abril 2009). "El desarrollo de los ordenadores cuánticos depende de un nuevo software de control", Facultad de Informática de la Universidad Politécnica de Madrid. [5]. URL correspondiente: http://www.tendencias21.net/El-desarrollo-de-los-ordenadores-cuanticos-depende-de-un-nuevo-software-de-control_a3167.html

REFERENCIAS:
[1], [2], [3], [4], [5] Consultado especialmente para el punto referenciado en el índice como: punto 11: un salto cuántico al futuro.

• Revistas y revistas digitales:

Velasco, Fernando y Navarro, Diego (Diciembre 2008- Mayo 2009). *Inteligencia y Seguridad*: *revista de análisis y perspectiva,* Ed: Fernando Velasco y Diego Navarro nº 5. Primera publicación periódica en España en materia de Inteligencia. Cátedra Servicios de Inteligencia y Sistemas Democráticos (URJC). Instituto Juan Velázquez de Velasco de Investigación en Inteligencia (UC3M); Plaza y Valdés. [1].
Ciberp@is, revista editada por El país. URL correspondiente:
http://www.ciberpais.elpais.es/
Soler-Fuensanta, José-Ramón, (2004). *Missatges Secrets*, España: Mediterrania. Eivissa. URL correspondiente: http://dialnet.unirioja.es/servlet/libro?codigo=92127

• Internet:

http://www.Kriptopolis.com (accedida en junio 2009).
http://www.cripto.es/Enigma.htm (accedida en abril 2009).
http://www.mundocripto.com (accedida en mayo 2009).

http://rinconquevedo.iespana.es/rinconquevedo/criptografia/criptografia.htm (accedida en marzo 2009).

http://wwwvectorsite.net/ttcode4.html#m1 (accedida en febrero 2009).

http://www.philzimmermann.com/ (accedida en abril 2009).

http://www.microasist.com.mx/noticias/en/ampen1402.shtml (accedida en febrero 2009).

http://www.marketingycomercio.com/_numero14/00abr_firmadigital.htm (accedida en mayo 2009).

http://www.htmlweb.net/seguridad/varios/firma_juridico.html (accedida en junio 2009).

http://www.neoteo.com/criptografia-la-maquina-Enigma-y-la-segunda-guerra.neo (accedida en mayo 2009).

http://seguridaddescifrada.blogspot.com/2008/06/la-criptografa-gan-la-segunda-guerra.html (accedida en marzo 2009).

http://aldea-irreductible.blogspot.com/2008/07/la-aventura-de-la-historia-mensajes.html (accedida en abril 2009).

http://www.latinoseguridad.com/LatinoSeguridad/Reps/Cripto1.shtml (accedida en mayo 2009).

http://www.hezkuntza.ejgv.euskadi.net/r43573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf (accedida en marzo 2009).

http://serdis.dis.ulpgc.es/~iicript/PAGINA%20WEB%20CLASICA/CRIPTOGRAFIA/POLIALFABETICAS/cifra%20de%20la%20porta.htm (accedida en abril 2009).

http://mx.geocities.com/valdesmarrero/cripto_grafia.html (accedida en abril 2009).

http://es.tldp.org/LinuxFocus/pub/mirror/LinuxFocus/Castellano/May2002/article243.shtml (accedida en febrero 2009).

http://criptografia-nosotras.blogspot.com/2008/05/los-criptoanalistas-rabes.html (accedida en febrero 2009).

http://www.taringa.net/posts/info/1881049/Santo-Grial-de-la-criptograf%C3%ADa.html (accedida en marzo 2009).

http://www.criptored.upm.es/investigacion/informe.htm (accedida en mayo 2009).

http://www.criptored.upm.es/paginas/investigacion.htm (accedida en marzo 2009).

http://www.netfocus.es/es/EMPRESA/SALA_DE_PRENSA/ENTREVISTA_CRIPTOGRAFIA_Y_SEGURIDAD_DE_LA_INFORMACION/ (accedida en junio 2009).

http://www.bibliotecapleyades.net/ciencia/esp_ciencia_manuscrito05.htm (accedida en abril 2009).

http://www.mat.ucm.es/~iluengo/Santalo05.html (accedida en mayo 2009).

http://www.virusprot.com/Col13.html (accedida en febrero 2009).
http://www.tendencias21.net/informatica/La-primera-red-metropolitana-de-criptografia-cuantica-estara-disponible-en-Espana-en-2010_a94.html (accedida en abril 2009).
http://www.cripto.es/informes/info026.htm (accedida en junio 2009).
http://www.virusprot.com/Col12.html (accedida en marzo 2009).
http://www.virusprot.com/Recomen1.html (accedida en marzo 2009).
http://www.periodistasenlinea.org/modules.php?op=modload&name=News&file=article&sid=1721 (accedida en mayo 2009).
http://criptografiaurjc.blogspot.com/2008/03/historia-moderna.html (accedida en abril 2009).
http://www.dma.fi.upm.es/java/matematicadiscreta/Aritmeticamodular/criptografia.html (accedida en junio 2009).
http://www.dean.usma.edu/math/pubs/cryptologia/ (accedida en marzo 2009).
http://www.revista.unam.mx/vol.10/num1/art01/int01-2.htm (accedida en junio 2009).
http://www.redtercermundo.org.uy/revista_del_sur/texto_completo.php?id=1198 (accedida en febrero 2009).
https://observatorio.iti.upv.es/resources/new/2655 (accedida en marzo 2009).
http://www.securitybydefault.com/2009/03/es-segura-la-criptografia-en-la.html (accedida en abril 2009).
http://www.cazarabet.com/lalibreria/fichas5/soldadossinrostro.htm (accedida en marzo 2009).
http://juanchox.blogspot.com/2009/05/la-criptografia-cuantica-mas-cerca.html (accedida en mayo 2009).
http://www.tendencias21.net/La-criptografia-cuantica,-mas-cerca_a3250.html (accedida en mayo 2009).
http://www.laflecha.net/canales/seguridad/criptografia-cuantica-el-futuro-de-la-seguridad (accedida en abril 2009).
http://www.etsit.upm.es/arbol-denoticias.html?tx_ttnews[tt_news]=108&cHash=e64fe1b19b (accedida en marzo 2009).
http://www.kriptopolis.org/el-fin-de-la-criptografia-cuantica (accedida en marzo 2009).
http://www.jadbp.org/node/21 (accedida en abril 2009).
http://images.google.es/imgres?imgurl=http://es.geocities.com/gce_euzkadi/imagenes/fotos/cifras/bou_cifra8.jpg&imgrefurl=http://es.geocities.com/gce_euzkadi/paginas/cifra.ht

ml&usg=__srMM6qKjQE4QFZChASedr-1KCLk=&h=404&w=283&sz=14&hl=es&start=21&sig2=5-2aUFctIj_blTFFckGJRw&tbnid=mFIWM6DJ55jIMM:&tbnh=124&tbnw=87&prev=/images%3Fq%3Dcriptografia%2Btransposici%25C3%25B3n%26gbv%3D2%26hl%3Des%26sa%3DG&ei=C8YTStOuNNnF-Qb-_p2tDw (accedida en junio 2009).

http://images.google.es/imgres?imgurl=http://www.telefonica.net/web2/akiv/scytaleruedа.gif&imgrefurl=http://historiasconhistoria.es/2007/06/28/mensajes-cifrados-de-la-antiguedad.php&usg=__DZCekt4Hhzgx2wWPrXxVMCYk5Eo=&h=255&w=257&sz=27&hl=es&start=39&sig2=aPsRZJprPbEoh-FamK1k5g&tbnid=9b835i0t90kZPM:&tbnh=111&tbnw=112&prev=/images%3Fq%3Dcriptografia%2Btransposici%25C3%25B3n%26gbv%3D2%26ndsp%3D21%26hl%3Des%26sa%3DN%26start%3D21&ei=l8gTStLHE9LN-QbLlIGVDw (accedida en junio 2009).

http://images.google.es/imgres?imgurl=http://www.kriptopolis.org/images/qubit.jpg&imgrefurl=http://www.kriptopolis.org/criptografia-y-dinero-cuantico&usg=__muncshFfTs076ldmYTp6KslR4cU=&h=265&w=187&sz=13&hl=es&start=1&sig2=tmhJKCZkbxoTb9WxoKadrg&tbnid=HyBBwSsF1tSiMM:&tbnh=112&tbnw=79&prev=/images%3Fq%3Ddinero%2Bcu%25C3%25A1ntico%26gbv%3D2%26hl%3Des%26sa%3DG&ei=d8s3StaIFcWZ_AaCkaXbDQ (accedida en mayo 2009).