ETSIT UPM

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN

Isdefe

Cuadernos
Cátedra
ISDEFE-UPM

4

Criptología y Seguridad

Jorge Dávila Muro

Criptología y Seguridad

Jorge Dávila Muro

Primera edición: Diciembre 2008

Edita:
Fundación Rogelio Segovia para el
Desarrollo de las Telecomunicaciones
Ciudad Universitaria, s/n
28040-Madrid

Imprime:
E.T.S.I. de Telecomunicación
Universidad Politécnica de Madrid
Ciudad Universitaria, s/n
28040-Madrid
Diseño de cubierta y
maquetación: Rocio Ortega

ISBN (13): 978-84-7402-352-7
ISBN (10): 84-7402-352-1
Depósito Legal: M-42946-2008

Índice

Presentación	3
Prefacio	7
¿Qué es la criptografía?	7
La cifra	8
Etapas de la criptografía	9
El principio de la criptografía clásica	10
La ocultación en los textos sagrados	12
Los primeros usos militares	13
La criptografía en la diplomacia y el buen gobierno	16
Los imperios de Oriente	17
Criptografía medieval y renacentista	19
El Barroco y los maestros de espías	26
La era moderna	30
El telégrafo y la popularidad del cifrado	35
El nacimiento del criptoanálisis moderno	38
El siglo XX y las máquinas de cifrado	42
El cifrado perfecto	46
Telegramas cifrados e intercepciones inconfesables	47
La máquina Enigma	51
La guerra en el Pacífico	52
Máquinas para el criptoanálisis	56
La guerra fría y el proyecto Venona	59
La teoría de la información y de los sistemas secretos	68
La guerra de Corea	70
Diecisiete años de espionaje para el Kremlin	72
La guerra de Vietnam	75
En las costas del Sinaí	78
Capturando la máquina	79
ARPANET y la semilla del nuevo escenario	80
El DES y la criptografía civil	81
El nuevo siglo y el *Advanced Encryption Standard*	86
La era digital y primeros límites para la criptografía civil	88

La Web 89
El PGP 90
El PGP de código abierto 92
Retos y resistencia del algoritmo RSA 93
El SSL y las comunicaciones Web cifradas 95
Primeros ciber-delitos 96
El nacimiento de las funciones *hash* 97
La quimera de la protección de contenidos multimedia 98
La criptografía de clave pública 100
El RSA y otros algoritmos asimétricos 104
Limitaciones a la criptografía civil 107
El algoritmo RC4 y las conexiones Wi-Fi 109
Evaluaciones criptográficas internacionales 112
Ascenso y caída de las funciones *hash* 114
Criptografías cuánticas 116
El declive de la función SHA-1 120
El criptoanálisis moderno y la inseguridad GSM 123
El análisis de tráfico 124
Algunos sistemas nacen muertos 126
La longitud de las claves y su evolución con los niveles de seguridad 127
¿Qué problemas quedan por resolver en la criptrografía actual? 128
Epílogo 132
ANEXO 133
La criptografía y la seguridad en el 7º Programa Marco europeo y en el Plan Nacional Español 135
Organismos y departamentos de la Administración Pública con competencia en temas criptográficos 143

Presentación

En la Sociedad de la Información en la que vivimos, la mayor parte de la información que es gestionada se transmite, se procesa o se almacena en algún momento en un sistema de información y comunicaciones. Sin embargo, la enorme y creciente complejidad tecnológica de los sistemas de información y comunicaciones dificulta la comprensión de los conceptos de seguridad y protección de la información. Se da la paradoja de que cada vez hay más personas que conocen y usan las tecnologías de la información y, sin embargo, cada vez hay menos que tengan un conocimiento profundo de las mismas.

Por ello, damos la bienvenida a este trabajo del profesor Jorge Dávila, por su loable intento de dar a conocer y divulgar conceptos complejos como los relativos a la criptología y a la seguridad.

Podemos definir la Seguridad de las Tecnologías de la Información (TIC) como la capacidad de los sistemas que utilizan dichas tecnologías (sistemas que denominamos de información y comunicaciones) para resistir, hasta un determinado nivel de confianza, accidentes o acciones maliciosas que pueden comprometer la confidencialidad, integridad, autenticidad y disponibilidad de la información que manejan. También, y no menos importante, el concepto de seguridad de las tecnologías de la información abarca la capacidad de protección de la integridad y disponibilidad de los propios sistemas de información y comunicaciones.

Los productos de seguridad son aquellos que forman parte de los sistemas de información y comunicaciones y que proporcionan al sistema la capacidad de protección de la información. Su función es singularmente importante porque, en definitiva, los productos de seguridad de las TIC son los que hacen posible que un sistema, inseguro, pueda ser usado de forma segura manteniendo todas sus funciones esenciales.

Dentro de los productos de seguridad tienen un papel muy destacado los productos criptológicos, papel que viene dado por las singulares características que tiene la Criptología. La Criptología, tal como a lo largo de este libro se pone de manifiesto, es capaz de proporcionar soluciones para mantener la confidencialidad y la integridad de la información, para proporcionar autenticación, evitar el no-repudio y registrar las acciones ejecutadas sobre un sistema. Los productos criptológicos no son más que implementaciones específicas, adaptadas a diversos entornos y servicios, de las funciones que proporciona la Criptología y por ello, hoy en día, no se concibe un sistema de información que no incorpore funciones y mecanismos de seguridad fundamentados en un algoritmo criptológico.

El autor de la monografía, el profesor Jorge Dávila, es un especialista muy conocido en el mundo de la seguridad de las tecnologías de la información y las comunicaciones, con el que el personal del Centro Criptológico Nacional contrasta habitualmente opiniones y pareceres sobre cuestiones técnicas. Experto conocedor de los secretos que esconde la ciencia criptológica, es autor habitual y prolífico de artículos y comentarios en importantes revistas del sector de la seguridad.

El profesor Dávila ha hecho un excepcional trabajo de divulgación científica en la presente monografía. En algo más de cien páginas, revisa toda la evolución histórica de la ciencia criptológica, sin perder detalle de las diferentes fases por las que ha pasado y apuntando cuáles serán las líneas futuras de su desarrollo. Por ello, estamos seguros de que el presente trabajo satisfará las expectativas tanto de los lectores menos versados en la materia, que buscan una conocimiento genérico en su primera aproximación al mundo de la criptografía, como a los más experimentados, que dispondrán de una perspectiva histórica detallada, lo que les permitirá responder a muchos de los interrogantes actuales del mundo de la seguridad de las tecnologías de la información y las comunicaciones, en general, y del desarrollo criptológico, en particular.

Finalmente, sólo nos queda agradecer y felicitar tanto a Isdefe como a la Universidad Politécnica de Madrid por esta iniciativa, conscientes como somos de que la divulgación de la cultura de la seguridad es un camino arduo y difícil, en el que el Centro Criptológico Nacional no puede ni quiere caminar solo, sino colaborando con empresas e instituciones como las ya citadas, para hacer posible que los beneficios de la Sociedad de la Información lleguen a todos.

D. Alberto Saiz Cortés
Secretario de Estado-Director
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL

"Es dudoso que el género humano logre crear
un enigma que el mismo ingenio humano no sea capaz
de resolver"
Edgar Allan Poe

Prefacio

Códigos, cifras, señales y lenguas secretas han estado ocultando el contenido y significado de algunas comunicaciones durante siglos, independientemente de si su transmisión se ha hecho por medios orales o escritos, mediante gestos o por canales electrónicos. Aunque el origen de esta actividad no está claro, quizás por su mismo amor al secreto y a la confidencialidad, lo que si está claro es que su existencia, sus métodos y sus propósitos no siempre han permanecido ocultos. De hecho, en nuestros días, la preocupación de la sociedad global por los temas de la confidencialidad y de la protección de la información ha desenterrado viejos fantasmas y mitos. La seguridad en general, y la de la información en particular, ha venido a extender y popularizar métodos criptológicos que en otros tiempos solo eran propios de iglesias, monarcas, príncipes, diplomáticos, subversivos y militares, por no mencionarlos a todos.

¿Qué es la criptografía?

La criptografía es el arte de escribir algo que no puede entender nadie, a menos que se tenga la correspondiente clave. La palabra criptografía proviene del griego κρυπτος (kryptos = oculto), de γραφειν (grafein = escribir) y del sufijo *-ia que* es el utilizado para crear sustantivos abstractos. Así pues, la criptografía es algo que se refiere a la escritura y su cualidad de permanecer oculta[1].

Una definición menos lingüística del término criptografía se refiere al arte o ciencia de cifrar y descifrar la información utilizando técnicas complejas que hagan posible el intercambio seguro de mensajes transformados que sólo pueden ser leídos por aquellas personas a quienes van dirigidos. Para hablar con un poco más de precisión, cuando esta área de conocimiento es tratada como una ciencia, entonces deberíamos hablar de la criptología, ya que ésta engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el criptoanálisis. Esta

[1]De esa misma raíz griega que indica algo "oculto, secreto, engañoso", es de donde derivó también la palabra gruta y, a partir de ésta, grotesco. Más tarde surgiría cripta como cultismo del término gruta.

última actividad siempre ha estado íntima y antagónicamente relacionada con aquella, ya que estudia los métodos que se utilizan para "romper" la seguridad de los textos que hayan sido cifrados con el objetivo de recuperar la información original que contienen, y hacer esto en ausencia de la clave oportuna.

La cifra

Otro término muy castellano utilizado para referirse al curioso arte de ocultar intencionadamente el significado de los mensajes escritos es el de "cifra". En principio, una cifra es cualquier número o dígito y, como bien sabemos, a su vez, un número puede tener varios dígitos o cifras. Se conocen diversos sistemas de numeración, y cualquiera conoce la existencia de caligrafías distintas, como la árabe y la latina, por ejemplo, para representar a los números, pero también hay números que representan letras como es el caso de la escritura hebrea.

El nombre que designa los números viene del árabe "*sifr*" que (رفص) en su momento sólo representaba al número cero[2] , el número vacío, y que después paso a referirse a todos los números. En latín medieval existió la palabra "*cifra*", y el lenguaje codificado viene del término italiano "*cifra*" (pronunciado como "*chifra*", en castellano). La primera aparición del cero se verificó en Babilonia en el siglo III antes de nuestra era y, mucho después, apareció también entre los mayas; sin embargo, la cultura occidental debe el cero a los habitantes de la India que ya lo representaban con un círculo en el siglo V, y lo llamaban "*sunja*", que significa "*vacío*" en sánscrito. Esta palabra dio lugar al "*sifr*" árabe, pero hubo que esperar hasta el siglo VIII de nuestra era para que el "*sunja*" entrara en el mundo árabe.

---

[2]La palabra "cero" viene de la palabra "*zero*" a través del frances *zéro*, que a su vez proviene del lenguaje romance veneciano y este del italiano a través de una deformación de *zephirum* (latín): *zephirum*→*zefiro*→*zefro*→*zero*. El término *Zephirum* fue el nombre que le dio el matemático italiano Fibonacci[1] en su obra *Liber Abaci* (Libro del Ábaco) en 1202. Leonardo de Pisa (1170-1250) también conocido como Fibonacci lo tomó del árabe "*sifr*" (رفص) , que significa "*vacío*". El matemático y astrónomo persa Al-Khwārizmī usó la palabra *sifr* en su obra *Al-ğabr* (*Álgebra*; es decir, la *Reducción*) escrita en el año 825. Los árabes tomaron el concepto del cero de la India en el año 773 y los hindúes lo llamaban "*sunja*", en sánscrito. El matemático indú Brahmagupta (598-668) explica el concepto del cero en su libro *Brahmasphutasiddhanta (La apertura del universo)* escrito en el año 628, como el resultado de restar a un número el valor de él mismo. Los mayas también descubrieron el cero y lo usaban en su calendario que era un sistema a base de 60.

Etapas de la criptografía

La historia de la criptografía abarca muchos miles de años. Podemos decir que el periodo clásico de la criptografía se extiende desde sus orígenes hasta el final de la Primera Guerra Mundial, y dentro de este periodo los algoritmos se realizaban a mano, con lápiz y papel, o con la ayuda de sistemas mecánicos relativamente sencillos.

En el periodo comprendido entre las dos guerras mundiales, los sistemas de cifrado empiezan a sofisticarse y se convierten en máquinas electromecánicas que, llegada la Segunda Guerra Mundial, juegan un papel decisivo en el desarrollo de la contienda. Terminado el derramamiento de sangre en 1945, no con ello desaparecen las tensiones militares y sociales, por lo que la criptografía sigue jugando un papel relevante durante lo que se conoce como la Guerra Fría, y ésta se basa en sistemas, todavía electromecánicos, cada vez más sofisticados. Sin embargo, todo esto cambiará irreversiblemente con la llegada de los microcontroladores, la electrónica integrada, la era digital y el final de la década de los setenta.

Durante el periodo clásico e incluso durante la Guerra Fría, las técnicas criptográficas utilizadas estaban a la altura de los hombres, pero después, a principios del siglo XX, las cosas cambiaron radicalmente y la complejidad de los algoritmos y de los sistemas utilizados adoptó magnitudes astronómicas. El abandono de los sistemas clásicos se produjo cuando, en 1922, se inventaron los complejos sistemas electromecánicos denominados teleprinters, teletypewriters o teletipos[3] simplemente.

---

[3]Teletype es una marca comercial de la compañía Teletype Corporation con sede en Skokie, Illinois, EEUU, hicieron la primera instalacion commercial de telégrafo impreso en la Compañía Postal y de Telégrafos de Boston y New York en 1910. El teletipo se hizo popular con los ferrocarriles, y la Associated Press adoptó esta compañía en 1914 como su servicio de telegrafía. Morkrum se unió con su competidor E.E. Kleinschmidt para formar Morkrum-Kleinschmidt Corporation, que pronto fue rebautizada como Teletype Corporation. Esta compañía fue absorbida por la AT&T en 1930.

El circuito teletipo estaba normalmente unido a una perforadora de papel y a un lector de la misma (http://homepages.cwi.nl/~dik/english/codes/punched.html), permitiendo reenviar los mensajes recibidos a través de otro circuito. Sobre esta tecnología se construyeron complejas redes de comunicación militar y comercial. Los operadores podían leer la prioridad o urgencia del mensaje e incluso, si era necesario, alimentar con esa cinta calificada como "FLASH PRIORITY" un lector de otro teletipo cuando todavía estaba saliendo de la perforadora original. El tráfico de rutina tenía que esperar horas para su distribución a destino final.

Hasta la década de los años setenta, la criptografía y el criptoanálisis han sido propios de entornos eminentemente militares y del mundo de las comunicaciones diplomáticas, por lo que su uso y desarrollo era un derecho que se reservaban para si los gobiernos de las naciones. Sin embargo, en la década de 1970 dos hechos cruciales lanzaron la criptografía al mundo civil, uno de ellos fue la publicación por parte del NIST de Data Encription Estándar (DES), y el otro, la invención de la Criptografía de Clave Pública.

El principio de la criptografía clásica

La aparición de la escritura data de, al menos, 3.100 años antes de nuestra era. La escritura vino de manos de los sumerios que inventaron lo que hoy se conoce como escritura cuneiforme. Muchos años atrás, unos 4.000 años antes de nuestra era se había producido la gran aportación de los egipcios: la invención de la escritura jeroglífica. Sin embargo, habría que esperar 1.500 años hasta que los fenicios desarrollaran la idea de un alfabeto, y simplificasen considerablemente las reglas de la escritura. Con la aparición de ésta, la Humanidad se dota de la capacidad de memoria que aporta la letra escrita.

El uso más antiguo que se conoce y que pueda estar relacionado con la criptografía podemos observarlo en un conjunto de jeroglíficos tallados en un monumento egipcio del Imperio Antiguo. Este monumento se encuentra en la ciudad de Nemet Khufu, y en él aparece lo que se conoce como la Inscripción[4] de Khnumhotep II[5] que es, quizás, el primer criptograma de la historia. El monumento data del año 1.900 a.C., y se construyó para albergar la tumba del nomarca[6] en Beni Hasan. El escriba encargado de decorar su sala con una oda a las virtudes de su señor decidió utilizar un código sencillo de sustitución jeroglífica, cambiando algún que otro símbolo por uno de sus sinónimos menos conocidos. Este escriba no utilizó un sistema de cifrado propiamente dicho, simplemente cambió algunos jeroglíficos de aquí y de allá[7], principalmente al final de los documentos.

---

[4]Para una transcripcion al inglés ver http://nefertiti.iwebland.com/texts/khnumhotep.htm

[5]**Khnumhotep II** (*1890 a. C.*) Nomarca de la Dinastía XII, (Reino medio) durante el reinado del faraón Amenemhat II, cuyo mausoleo y tumba están en Beni Hassan.

[6]**Nomarca** en el Antiguo Egipto era un cargo de gobernador que estaba al frente de comunidades organizadas llamadas nomos. El cargo era designado por el faraón aunque se sabe que en determinadas épocas se hizo hereditario. A veces había grandes roces y conflictos entre el poder de los nomarcas y el del faraón.

[7]En particular, en las últimas 20 columnas de la inscripción 222, en la que se habla de los monumentos edificados por el nomarca.

Lo interesante de estas alteraciones de las reglas de escritura es que cualquier observador podía, en poco tiempo, figurarse cuál era la lectura correcta de las transcripciones. Entonces, ¿por qué lo hizo?.

Hay varias posibilidades, pero desgraciadamente nunca sabremos la verdad. Es posible que los egipcios quisiesen preservar, ante el observador casual, el secreto de ciertos rituales religiosos. Haciendo que los textos religiosos fuesen difíciles de leer conseguirían hacer misteriosa su religión, y eso siempre ha dado importantes réditos a la casta sacerdotal. Otra interpretación más sencilla es que el escriba tan sólo quisiese dar una apariencia formal a sus escritos y, por ultimo, también podría tratarse de una decisión personal del escriba que habría querido impresionar al lector mostrando cómo él podía escribir a un nivel mas elevado. En este caso, se trataría de un curioso acto de vanidad transcendental. Este sería otro de los usos y finalidades que también tiene la criptografía en tiempos modernos[8].

Un poco más tarde, alrededor del año 1.500 antes de nuestra era, mientras los fenicios inventan el alfabeto, en Mesopotamia se utilizaba la criptografía para proteger secretos más mundanos. En una tablilla de tan sólo 7 x 5 cm encontrada en las riveras del rio Tigris, tenemos el más antiguo ejemplo del uso del cifrado como protección de una fórmula para vitrificar la cerámica de barro. En este caso, lo que se pretende proteger es algo con un valor netamente comercial, que nada tenia que ver con gobiernos, ejércitos o iglesias. El cifrado consistía, una vez más, en utilizar signos cuneiformes en sus valores silábicos menos comunes para intentar ocultar su significado real del mensaje y con él, la fórmula.

En la escritura cuneiforme, los pictogramas o los dibujos representando cosas concretas fueron la base de esa escritura. Los primeros pictogramas se parecían a los objetos que representaban, pero tras su uso repetido y el paso del tiempo, estos símbolos empezaron a simplificarse y a hacerse más abstractos. Estas marcas se volvieron afiladas, en forma de cuñas como la cabeza del punzón que las producía, y ya podían referirse a sonidos o a conceptos abstractos.

[8]Ver el caso de los mensajes enviados a periódicos de San Francisco, por el asesino en serie conocido como el Asesino del Zodiaco.

La ocultación en los textos sagrados

Entre los años quinientos y seiscientos antes de nuestra era, los escribas hebreos compusieron el Libro de Jeremías, en donde se mencionan varios nombres de personas y de lugares que habían sido deliberadamente "ocultados" en la biblia hebrea utilizando una cifra muy peculiar. En concreto, יבק בל *Lev Kamai* (51:1) es la versión Atbash de מידשכ *Kasdim* (*Caldeos*), y ששך *Sheshakh* (25:26; 51:41) es la versión de לבב *Bavel* (*Babilonia*). El uso del cifrado Atbash siempre ha sido asociado con metodologías exotéricas del misticismo judío aplicadas al estudio de los textos religiosos al igual que lo que ocurre con la Cábala. (en hebreo,קַבָּלָה , y significa *recibir*). El cifrado Atbash[9] es un código que sustituye la primera letra del alfabeto, *aleph*, por la última, *tav*, la segunda, *beth*, por la penúltima, *shin*, y así sucesivamente hasta que se alcanza el centro del alfabeto. Esta cifra es una de las pocas que se utilizan en hebreo. Atbash es un cifrado por sustitución monoalfabética en el que cada letra del alfabeto del criptograma realmente representa a otra.

El uso de la criptografía por parte de iglesias e instituciones religiosas tiene una larga tradición en lo que a la protección de sus misterios se refiere, ya que éstos, en muchas ocasiones, han resultado ofensivos para la cultura dominante o para las autoridades políticas del momento. Quizás, el ejemplo mas conocido sea el famoso "Número de la Bestia" del Libro de las Revelaciones, también conocido como "El Apocalipsis", del Nuevo Testamento cristiano[10]. La cifra 666 podría ser el criptograma que oculta una peligrosa referencia. Algunos estudiosos creen que era una referencia velada al Imperio Romano o, mas en concreto, a su emperador Nerón, ducho en la persecución de los primeros cristianos. Esta referencia iba dirigida a los iniciados (a quienes "*tienen la clave para entender*") y evitar que llamase la atención de las autoridades. Al menos para los escritos del cristianismo, gran parte de la necesidad de esas técnicas de ocultación desaparecieron con la conversión pactada de Constantino y la adopción del cristianismo como la religión oficial del Imperio Romano.

---

[9]ATBASH adquiere su nombre del hecho de que, en esa cifra, la A se transforma en T, la B en Sh, y así sucesivamente, por tanto ATBSh, y de ahí, ATBASH.

[10]Apocalipsis 13:18 "*Y aquel que tenga inteligencia que calcule el número de la Bestia, pues es el número de un hombre, y ese número es el 666*".

Al igual que muchas otras traducciones hechas en aquellos tiempos, el Nuevo Testamento se tradujo de los Textus Receptus[11] bizantinos que estaban escritos en griego. Por otra parte, el Antiguo Testamento se tradujo del texto masorético hebreo, y los textos apócrifos fueron traducidos del Septuagint (LXX); *la Biblia de los Setenta*[12] o alejandrina, escrita en griego vulgar en la ciudad de Alejandría. La Biblia alejandrina es la traducción más antigua, del hebreo al griego, del antiguo testamento y su confección se inició en el año 250 a.C.y no se terminó hasta un siglo después, en el año 150 a.C.

En los manuscritos griegos, el número llamado "*de la bestia*" se representa en forma numérica como "χξς", y algunas veces, literalmente como "seiscientos sesenta y seis", (ἑξακόσιοι ἑξήκοντα ἓξι *hexakoosioi hexékonta hex*). El registro mas antiguo que se conoce de ese fragmento es el papiro 115 de los encontrados en la ciudad egipcia de Oxyrhynchus, y en él da un número ligeramente diferente, el 616, como "χις".

Los primeros usos militares

Se sabe que en la Grecia Clásica, en el siglo quinto antes de nuestra era, se utilizaban métodos criptográficos para proteger informaciones. Un ejemplo de ello es el Scitalo lacedemónico[13]. Un scitalo (en griego *σκυτάλη*, *bastón*) es una herramienta utilizada para poner en práctica un sencillísimo cifrado que consiste en transponer las letras que componen el mensaje. La herramienta en sí consta de un cilindro con una tira de piel enrollada longitudinalmente a su alrededor en la que se escribe el mensaje a enviar.

Al desenrollar la tira del cilindro o bastón todas las letras del mensaje siguen escritas en la cinta pero su orden relativo y sus posiciones actuales no parecen ser las correctas, por lo que el mensaje que resulta de la lectura lineal de la cinta es incomprensible. Se dice que los griegos en general, y lo espartanos en particular, utilizaban esta cifra para comunicarse durante las campañas militares en las que participaban.

---

[11]Llamados así porque *Textus Receptus* → ***textum*** *ergo habes, nunc ab omnibus* ***receptum*** → textum y receptum → textus receptus.

[12]El nombre de Setenta se debe a que la tradición judia, transmitida en la Epístola de Aristeas, atribuye su traducción a 72 sabios judíos (seis de cada una de las doce tribus) en 72 días. Esta tradición toma su origen en la gematría, una técnica exegética que da valores numéricos interpretativos a los nombres, en la que el siete equivale a la perfección.

[13]**Lacedaemon**, o **Lakedaimon**, (en griego **Λακεδαιμων** o **Λακεδαιμωνία**) es el nombre correcto con el que se denominaba al estado espartano y así aparece en las obras de Tucídides.

El receptor del mensaje utiliza otro bastón con el mismo diámetro que el utilizado para escribir el mensaje, y en él enrolla la cinta de piel escrita que ha recibido. Al repetir exactamente la misma operación que realizó el remitente, el destinatario podrá leer un mensaje coherente e idéntico al que se envió. Este método tiene la ventaja de que es rápido y esta libre de errores, algo muy conveniente cuando uno está inmerso en el campo de batalla; sin embargo, su seguridad es muy reducida y se puede "romper" fácilmente.

El historiador Herodoto de Halicarnaso (484-425 a.C.) menciona también el envío de mensajes secretos físicamente ocultos dentro de tablillas de cera y madera, o como tatuajes hechos en la cabeza de un esclavo de confianza que se ocultaban cuando a éste le volvía a crecer el pelo, Aunque éstos no son ejemplos propiamente dichos de las prácticas criptográficas, puesto que el mensaje se envía sin modificar, si no resultan detectados son mecanismos que permiten la transmisión segura y confidencial de los mensajes. Estas técnicas se engloban dentro de lo que se conoce como esteganografía.

La esteganografía es el arte de escribir mensajes ocultos de tal modo que nadie, a excepción del destinatario pretendido del mensaje, puede darse cuenta de la existencia del mensaje. La esteganografía es, en cierto modo, antagonista de la criptografía ya que esta última trata de ocultar el significado del mensaje pero no ve problema en que se conozca la existencia del mismo. El término esteganografía viene de la famosa obra de Johannes Trithemius titulada *Steganographia*, escrita en 1499 y publicada en Frankfurt en 1606.

Según Herodoto, Demarato, rey espartano entre los años 515 y 491 a.C., envió a las ciudades griegas un aviso acerca del próximo ataque de los persas escribiendo su mensaje en una tablilla de madera, para luego ocultarlo cubriéndolo con cera y así simular que se trataba de una tablilla de escritura sin utilizar (*tabula rasa*). La tabilla recubierta de cera era un instrumento muy popular como material reutilizable para la escritura.

Otro ejemplo esteganográfico clásico lo encontramos con Histiades, un tirano que debía su puesto a Darío I el Grande, rey de Persia, quien había conquistado Mileto y otras ciudades de la Jonia en Asia menor. A Histiades no le gustaba vivir en la ciudad de Susa, e hizo planes para recuperar su poder en Mileto instigando la que se conoce como la Revuelta en Jonia, que constituyó el primer gran conflicto entre persas y griegos y la piedra de toque para las guerras entre ambos pueblos que vendrían después. En el 499 a.C., Histiades afeitó la cabeza de su esclavo más fiel, y le tatuó un mensaje en la cabeza, y luego esperó a que le creciese el pelo. Después

el esclavo fue enviado a encontrarse con Aristágoras, yerno de Histiades y, por aquel entonces Tirano de Mileto, para que este afeitara la cabeza del esclavo y poder así leer el mensaje, en el que se le instaba a revolverse contra los persas. Aristágoras, siguió las instrucciones de Histiades, y con la ayuda de atenienses y eretrianos, atacaron y quemaron la ciudad de Sardis, capital persa de la Jonia.

Los romanos también conocían algo de criptografía y ejemplo de ello son la cifra de César y sus variaciones. El cifrado César recibe su nombre de Julio Caesar (100-44 a.C.) quien, de acuerdo con el historiador Caius Suetonius Tranquillus, (69-140), la utilizó, con un desplazamiento a la izquierda de tres posiciones, para proteger sus mensajes de carácter militar[14]. Aunque César es el protagonista del primer uso registrado de este método de sustitución, se conocen otras cifras del mismo tipo que también han sido utilizadas. Uno de los usuarios de dicha cifra fue el emperador Augusto[15], aunque lo hizo con un desplazamiento hacia la derecha de una letra, y sin realimentar de forma cíclica el alfabeto[16].

Hay evidencias de que Julio César también utilizaba algunos sistemas de ocultación más complicados[17]; esto es conocido por unos comentarios de Aulus Gellius, autor y gramático latino, posiblemente de origen africano y ciudadano de Roma, quien en una de sus obras hace referencia a un tratado, hoy perdido, sobre las cifras presentes en la epístolas de César.

---

[14]"*Si él tenía algo confidencial que decir, lo escribía en cifra, es decir, cambiando el orden de las letras del alfabeto, de modo que no se pudiese reconocer ni una palabra. Si alguien quiere descifrar eso, y obtener su significado, deberá sustituir la cuarta letra del alfabeto, es decir la D, por una A y asi sucesivamente con todas la letras*." - Suetonius, De Vita Caesarum, Divus Iulius 56. Ver http://www.fordham.edu/halsall/ancient/suetonius-julius.html

[15]Concretamente nos referimos al emperador Caius Iulius Caesar Octavianus (23 de septiembre 63 adc - 19 de agosto 14 dc), heredero político de Julio César.

[16]"*Cuando escribía en cifra, ponía una B por cada A, una C por cada B, y con el resto de letras seguía el mismo principio, utilizando AA para sustituir a la X*." - Suetonius, De Vita Augustorum, Divus Augustus 88. Ver http://www.fordham.edu/halsall/ancient/suetonius-augustus.html

[17]*De notis litterarum, quae in C. Caesaris epistulis reperiuntur; deque aliis clandestinis litteris ex vetere historia petitis; et quid skytale sit Laconica.*
Libri sunt epistularum C. Caesaris ad C. Oppium et Balbum Cornelium, qui res eius absentis curabant. In his epistulis quibusdam in locis inveniuntur litterae singulariae sine coagmentis syllabarum, quas tu putes positas incondite; nam verba ex his litteris confici nulla possunt. Erat autem conventum inter eos clandestinum de commutando situ litterarum, ut in scripto quidem alia aliae locum et nomen teneret, sed in legendo locus cuique suus et potestas restitueretur; quaenam vero littera pro qua scriberetur, ante is, sicuti dixi, conplacebat, qui hanc scribendi latebram parabant. Est adeo Probi - Aulus Gellius, Noctium Atticarum Liver XVII 9.1-5.

Es imposible conocer el grado de eficacia que podían tener estas medidas de ocultación del significado real de los mensajes, pero es muy probable que sus cifrados fueran razonablemente seguros, no solo por el hecho de que sólo algunos pocos enemigos de César realmente sabían leer, sino por la ausencia, por aquel entonces, de técnicas de criptoanálisis.

La criptografía en la diplomacia y el buen gobierno

En otro lado del mundo, en la India, la criptografía era un arte bien conocido desde la antigüedad. De hecho, en el tan mencionado Kamasutra[18] se recomienda a los amantes el uso de técnicas de ocultación, entre ellas las que hoy consideraríamos como criptográficas, para poder comunicarse sin ser descubiertos.

En la primera parte de Kamasutra, en el capítulo tercero se listan sesenta y cuatro artes y se presentan así:

> "*El hombre debería estudiar el Kama Sutra y las artes y ciencias subordinadas a esto [....] Incluso las jóvenes criadas deberían estudiar este Kama Sutra, junto con sus artes y ciencias, antes de casarse, y después deberían continuar haciéndolo con el consentimiento de sus maridos*''.

Esas artes claramente no son para un gobierno, o de mero interés académico sino, más bien, para practicarlas los legos. En esta lista de artes, en las posiciones 44 y 45 se puede leer:

> *44. - El arte de entender las escrituras en cifra, y la escritura de las palabras de un modo particular.*
>
> *45. - El arte de hablar cambiando las formas de las palabras. Esto se puede hacer de varios modos. Algunos hablan cambiando el principio de las palabras, otros añadiendo letras innecesarias a cada sílaba de una palabra, y así de muchas otras formas.*

[18] **Kama** (काम **kāma**) es una palabra en sánscrito que tiene el significado general de "deseo" carnal y no carnal, e "intención" junto a los significados específicos de "placer" y "amor (sexual)". Utilizado como nombre propio se refiere a Kama, el dios hindú del amor.

La criptología en la antigua India no se queda en un juego de amantes sino que, en su versión criptoanalítica, asciende al grado de instrumento de gobierno con la publicación de un manual, el Arthasastra, que se adelanta en algunos siglos a la obra del renacentista Niccolo di Bernardo dei Machiavelli.

El Arthasastra (*Arthaśāstra*) es un tratado sobre la administración pública, la política, la económica y la estrategia militar. La confección del Arthasastra se hizo entre los siglos segundo y cuarto de nuestra era[19].

El Arthasastra defiende el modelo de un gobierno autocrático construido sobre una economía sólida y eficiente. Este manual discute la ética de la economía y las funciones y obligaciones de un rey. El Arthasastra también trata los temas de la sociedad del bienestar y de la ética colectiva que mantiene unida a la sociedad. De acuerdo con este manual, un Rajarshi es alguien que, además de tener un elevado auto-control, y de cultivar su intelecto de modo contínuo, también "*tiene sus ojos bien abiertos a través del uso de espías*", y de cualesquiera técnicas que le permitan conocer el contenido de comunicaciones, secretas o no, que se den dentro de su reino.

Los imperios de Oriente

Fuera de Europa, tras el fin de la edad de oro musulmana, llevado a cabo por los mongoles, la criptografía permaneció, en términos relativos, subdesarrollada. Por otro lado, la criptografía en Japón parece no haber existido hasta el año 1510, y las técnicas realmente avanzadas solo aparecieron después de que el país se abriese a Occidente en la década de 1860.

No hay indicios que permitan confirmar la existencia de la criptología en Japón antes del periodo de los estados guerreros[20](*senkokujidai*), durante el cual se cree que Uesugi Kenshin[21] y Oda Nobunaga utilizaban cifras

[19]Mabbett, I. W.: "*The Date of the* (*Arthaśāstra*)'. Journal of the American Oriental Society 84 (2). pp. 162-169. April 1964. ISSN 0003-0279.

[20]El periodo **Warring States period** (戦国時代 *sengoku jidai*?) fue un tiempo de revuelta social, intriga política, y conflicto militar casi constante que duro desde mediados del siglo quince hasta principios del siglo diecisiete.

[21]**Uesugi Kenshin** (上杉 謙信 1530-1578) fue un señor feudal ("daimyo" significa "gran nombre") que gobernó en la provincia de Echigo durante el periodo Sengoku en Japón. El fue uno de los muchos poderosos señores del periodo Sengoku. Su fama proviene de su agudeza táctica en el campo de batalla, de su legendaria rivalidad con Takeda Shingen, de su experiencia militar, de su estrategia y de su creencia en el dios de la guerra Bishamon. De hecho, muchos de sus seguidores y otros creían que el era el avatar de Bishamonten, y le llamaron Kenshin Dios de la Guerra.

sencillas basadas en sustituciones sencillas. En el contexto de la historia mundial de la criptografía, este despertar es muy tardío si se tiene en cuenta que los pueblos del Mediterráneo habían utilizado sistemas de cifrado basados en transposiciones y sustituciones unos 1.500 años antes de que Uesugi naciese.

El sistema de cifrado utilizado por Uesugi era, básicamente, una sustitución sencilla utilizando lo que se conoce como la Tabla de Polibius[22]. El alfabeto japonés Iroha contiene cuarenta y ocho letras, por lo que se utiliza un cuadrado de siete por siete, con una celda dejada en blanco, para colocarlo. Las filas y las columnas están etiquetadas con un número o una letra. Cada letra del texto en claro es sustituida por sus coordenadas en esa tabla para así componer el criptograma.

Poco se sabe acerca de las medidas que el gobierno japonés tomó durante el periodo Meiji (1868-1912), periodo en el que Japón inició su modernización, para proteger sus comunicaciones; sin embargo, del periodo que siguió, el periodo Taishō (1912-1926), hay algo más de información, aunque realmente no es hasta la llegada del periodo Showa (marcado por el gobierno del Emperador Hirohito 1926-1989), cuando la armada imperial japonesa realmente decide mejorar activamente sus habilidades criptológicas.

---

[22]El **tablero de Polibius** es un artefacto inventado por el historiador griego clásico Polibius, descrito en su obra "*Historias*" (Hist. X.45.6 ff.), para fraccionar los caracteres de un texto en claro y poder así representarlos mediante un conjunto menor de símbolos. Polibius no pudo imaginar lo util que sería su enfoque para la telegrafía; él sugirió que los símbolos podrían ser representados usándolos por pares dentro de un conjunto de antorchas. También se ha utilizado el tablero, en la forma de "knock code", para enviar mensajes entre prisioneros dando golpecitos en las conducciones metálicas o en las paredes. Se dice que este método lo utilizaron los prisioneros nihilistas de los Zares de Rusia, y también por los prisioneros americanos en la guerra de Vietnam. Realmente puede señalizarse de muchas formas diferentes (flashes, señales sonoras, tambores, señales de humo, etc.) y es más fácil de aprender que el código Morse, aunque es algo menos eficiente que otros códigos mas complejos. En criptografía, el tablero de Polibius no es especialmente seguro, incluso si se utiliza con una sustitución alfabética, sin embargo ofrece la posibilidad de fraccionar un símbolo en varios símbolos del criptograma, por lo que es un componente de varios sistemas de cifrados clásicos como son el sistema ADFGVX, el código de los Nihilistas, y la cifra bífida inventada en 1901 por Félix Delastelle, que combina el tablero de Polibius con una transposición y utiliza el fraccionamiento para conseguir difusión.

En dicha época los japoneses mejoraron rápidamente sus habilidades en criptografía clásica pero, ese crecimiento se frenó porque el enemigo al que combatían, China, también utilizaba sistemas criptográficos clásicos desde mediados de los años treinta (del siglo veinte). Esto dio a la armada imperial nipona la falsa impresión de que sus esfuerzos ya habían merecido la pena y no había por qué continuar en ellos. Las habilidades que tan buen servicio les habían dado en la guerra continental con China serían de muy limitado efecto durante la Segunda Guerra Mundial, en la que Japón se enfrentó a varios enemigos y todos ellos muy al día en lo que a técnicas criptológicas se refiere.

Criptografía medieval y renacentista

Al igual que ocurre con los textos sagrados hebreos, el Corán[23] también ha sido objeto de un detallado análisis de los textos que los constituyen, y quizás fuese este estudio lo que condujo a la invención del análisis de frecuencias como técnica esencial para la ruptura de cualquier cifrado por sustitución monoalfabética; esto ocurría alrededor del año mil de nuestra era.

Esencialmente, todas las cifras basadas en sustituciones de las letras del mensaje por otras letras o símbolos cualesquiera resultaban vulnerables ante esta técnica de análisis. En occidente, esta situación de desventaja de los sistemas de cifrado frente a los criptoanalistas duró hasta que se inventaron, alrededor de 1465, las cifras polialfabéticas por parte del humanista italiano León Battista Alberti (1404-1472). Aunque usualmente se conoce a Alberti como el padre de los cifrados polialfabéticos, revisiones recientes de las contribuciones hechas por los árabes a la criptografía[24] han desvelado que, según el contenido de un manuscrito hallado recientemente, el mundo árabe ya tenía conocimiento de tales cifras polialfabéticas quinientos años antes de que Alberti las propusiese.

---

[23]El **Corán** (en árabe: القرآن *al-qur'ān* , literalmente "*la recitación* ") es el texto religioso central del Islam. Los musulmanes creen que el Corán es el libro de guia divina y la dirección para la humanidad, y consideran el texto en su árabe original como una transcripción literal de la palabra de dios, revelada a Mahoma durante un periodo de 23 años y ven en el Corán la revelación final de dios a la humanidad.

[24]Ibrahim A. Al-Kadi : T*he origins of cryptology: The Arab contributions*, Cryptologia, 16(2). April 1992. pp. 97-126.

Ismail al-Kindi[25], que escribió el libro titulado "*Risalah fi Istikhraj al-Mu'amma*" (*Manucrito sobre el Descifrado de Mensajes Criptográficos*) alrededor del año 800 de nuestra era, fue el primero en describir algunos cifrados polialfabéticos, así como en hacer una clasificación de los cifrados, la fonética y la sintaxis árabe y, lo que es más importante, describió el uso de diferentes técnicas estadísticas para el criptoanálisis, y dio la primera descripción de lo que hoy se conoce como "Análisis de Frecuencias". Además de estos descubrimientos, su obra contiene aportaciones sobre probabilidad y estadística que son ochocientos años anteriores a las de maestros como Pascal y Fermat.

Entre mediados del siglo quince y el final del primer cuarto del siglo XVI aparece un misterioso libro ilustrado que hoy en día se conoce como el Manuscrito de Voynich, y cuya característica más sobresaliente es que su contenido es del todo incomprensible. Se cree que fue escrito, entre los años 1450 y 1520, por un autor desconocido y con una escritura y en un lenguaje también desconocido. Desde el principio, el Manuscrito de Voynich ha sido estudiado con gran interés por muchos criptógrafos profesionales y aficionados, y todos ellos han fracasado en el intento de saber qué dice esa obra. Esta resistencia a ser leído hace de este manuscrito uno de los objetos mas curiosos de la historia de la criptología, aunque hay también quien piensa que se trata de un engaño muy elaborado, y que solo contiene símbolos arbitrarios.

Este manuscrito recibe su nombre del librero y bibliófilo polaco-lituano, Wilfrid Michael Voynich, quien lo compró a los jesuitas de Villa Mondragone, cerca de Roma, en el año 1912. Desde el año 2005, ese manuscrito tiene la signatura MS 408 de la Biblioteca Beinecke de libros y manuscritos raros de la Universidad de Yale.

En el año 1466, León Battista Alberti (1404-1472), un polifacético humanista renacentista italiano, inventó el cifrado polialfabético. Alberti recibió la mejor educación que en aquellos momentos podía tener un noble italiano. Entre 1414 y 1418 estudió a los clásicos en la escuela de Gasparino Barzizza en Papua y, posteriormente, completó su educación en la Universidad de Bolonia, donde estudió leyes y se doctoró en 1428. A principios de la década de 1430, fue a Roma a trabajar para la curia papal.

---

[25]Ya'qub ibn Is?aq al-Kindi (en árabe: يعقوب بن اسحاق الكندي) (801-873), también conocido en Europa por la versión latinizada de su nombre **Alkindus**, fue un árabe musulman polifacético: filósofo, científico, astrólogo, astrónomo, químico, matemático, músico, médico, y físico. Al-Kindi fue el primer musulmán de los filósofos peripatéticos, y entre sus numerosas aportaciones, es bien conocido por sus esfuerzos para introducir la filosofía griega en el mundo árabe, y por ser pionero en criptografía y física.

Después de profesar los votos, fue enviado a administrar el Priorato de San Martino a Gangalandi en el barrio de Lastra a Signa, en Florencia. Alberti fue también inspector papal de monumentos, y asesoró al Papa Nicholas V.

La primera cifra polialfabética que hizo pública, fue inventada por Alberti y en ella utilizaba un cifrado César para cifrar el mensaje, pero cambiaba a un alfabeto distinto cuando le parecía oportuno e indicaba este hecho en el criptograma escribiendo la primera letra del nuevo alfabeto en mayúsculas. Alberti también desarrolló un método y un artefacto mecánico de cifrado, descritos en su tratado de 1467, que revolucionaron la criptografía occidental de su época.

La cifra de Alberti consiste en dos discos de metal, uno fijo y otro móvil, unidos por un mismo eje sobre el que el disco interior puede rotar. Alrededor del disco exterior están escritas en minúsculas las letras del alfabeto latino pero omitiendo la *H*, la *K*, y la *Y*, ya que Alberti las consideraba superfluas. En el disco exterior también se incluían los números del 1 al 4 para ser utilizados con un libro de códigos que contuviese frases y palabras preseleccionadas a las que se les habrían asignado valores con esos cuatro dígitos. Alberti diseño su sistema de cifrado teniendo en mente a los cortesanos y diplomáticos.

El disco interior contiene, desordenado al azar, el alfabeto latino en mayúsculas y la partícula latina et. Alberti pensó que su cifra era irrompible, y esta suposición se basaba en sus investigaciones sobre el análisis de frecuencias, que es el método de ataque más efectivo para el descifrado de criptogramas obtenidos por sustitución monoalfabética.

Los estudios de Alberti en criptología eran solo un interés pasajero, pero a sugerencia de su amigo Leonardo Dato, secretario del Papa, Alberti decidió investigar el cifrado y eventualmente publicó un libro sobre esa materia, a pesar de la irrelevancia de este tratado para su obra arquitectónica y pictórica.

El principio de cambiar de alfabeto de sustitución continua e indefinidamente fue un gran avance; una implementación sencilla de este principio y fácil de aplicar dio como resultado unos sistemas polialfabéticos que fueron bastante difíciles de romper. De hecho, no fue hasta mediados del siglo XIX con los trabajos secretos de Babbage (1791-1871) durante la Guerra de Crimea, y los de Friedrich Kasiski (1805-1881), cuando las sustituciones polialfabéticas dejaron definitivamente de ser seguras.

Un poco después de Alberti, hubo otro gran personaje para la criptografía que es conocido como Johannes Trithemius. En realidad, se llamaba Johann Heidenberg (1462-1516), y había nacido en la ciudad alemana de Trittenheim, junto al rio Mosela; fue abad y estudioso del ocultismo y tuvo una gran influencia en la evolución posterior de las corrientes ocultistas europeas.

Estudió en la Universidad de Heidelberg y regresando un día de la universidad a su casa, en 1482, le sorprendió una tormenta de nieve por lo que se refugió en la abadía benedictina de Sponheim cerca de Bad Kreuznach. No conocemos sus razones pero el hecho es que decidió quedarse allí y un año después fue elegido abad de esa comunidad con sólo veintiún años de edad. En su mandato transformó la abadía que pasó de ser un lugar pobre, indisciplinado y ruinoso a convertirse en un centro de aprendizaje. La biblioteca de la abadía, que tenía cincuenta libros cuando Trithemius ingresó, llegó a contener más de dos millares de ejemplares. Sin embargo, sus esfuerzos no fueron recompensados con elogios, y su reputación como mago no favoreció su aceptación dentro de la ortodoxia católica. Con el tiempo, aumentaron las diferencias con la comunidad del convento y eso le llevó a presentar su dimisión en 1506, cuando decidió aceptar la oferta del obispo de Würzburg, Lorenz von Bibra (obispo desde 1495 hasta 1519), para convertirse en el abad de *Schottenklöster*[26] en la ciudad del mismo nombre, y allí se quedó hasta el final de sus días. Entre sus alumnos mas conocidos estaban Heinrich Cornelius Agrippa (1486-1535) y Paracelsus (1493-1541).

Johannes Trithemius, en un libro publicado en 1518, después de su muerte, dio a conocer una cifra polialfabética de clave progresiva. A diferencia de la clave de Alberti, que cambia de alfabeto a intervalos aleatorios, Trithemius cambiaba de alfabeto con cada letra del mensaje. Él empezó con una tabula recta, un cuadrado que contiene veintiséis alfabetos[27]. Cada alfabeto era el mismo de arriba pero desplazado una posición a la izquierda, y volviendo a empezar con la A después de haber llegado a la Z. La idea de Trithemius era cifrar la primera letra del mensaje utilizando el primer alfabeto, de modo que A se transforma en B, B en C, etc. La

[26]**Schottenklöster** (significa *Scottish monasterios* en alemán, singular: *Schottenkloster*) es el nombre aplicado a la fundaciones monásticas de misioneros irladeses y escoceses en la Europa continental, particularmente de los monasterios benedictinos en Alemania, que a principios del siglo trece se reunieron en una congregación cuyo abad general era el del Monasterio de los Escoceses en Regensburg.

[27]Trithemius, escribía en latín, por lo que su versión original de la Tabula Recta sólo contenía 24 alfabetos.

segunda letra del mensaje debía cifrarse con el segundo alfabeto, y así sucesivamente. El disco de Alberti implementa el mismo esquema si se rota una posición del disco interior después de cada uno de los cifrados o descifrados.

La cifra de Trithemius es de solución trivial, y la implementación de Alberti mediante su máquina no es mucho más difícil de romper. En ambos casos, la clave progresiva no está suficientemente protegida frente a ataques. Incluso la implementación que hizo Alberti de su cifrado polialfabético es bastante fácil de romper ya que la letra escrita en mayúsculas es el indicio más importante para su criptoanálisis. Durante los siglos posteriores se perdió en el olvido el significado real del uso de múltiples alfabetos para la sustitución, y los diseñadores de cifrados se concentraron más en oscurecer el modo de elección de unos pocos de esos alfabetos, repitiéndolos si era preciso, y no se daban cuenta de que podían aumentar la seguridad de todo el sistema utilizando simplemente muchos más alfabetos, llegando incluso a no repetir nunca ninguno de ellos.

La obra más famosa de Johannes Trithemius es la titulada *Steganographia*, que fue escrita en 1499 y publicada en Frankfurt en 1606, y en 1609 la iglesia católica la colocó en su *Index Librorum Prohibitorum*. Este libro está compuesto por tres volúmenes y, en una primera lectura, parece tratar de conjuros y del uso de la magia negra para, en concreto, utilizar a los espíritus para poderse comunicar a largas distancias. Desde la publicación en 1606 de las claves de descifrado de los dos primeros volúmenes, se sabe que dicha obra trata realmente de criptografía y esteganografía. Hasta hace poco, del tercer volumen se pensaba que era un tratado de magia, pero recientemente se ha comprobado que las formulas "mágicas" que contenía, realmente eran textos encubiertos con más contenido criptográfico en su fondo. Este trabajo es el que ha dado nombre al moderno campo de la esteganografía.

Otras obras de Trithemius incluyen la *De Laude Scriptorum* (*En alabanza a los escribas*) escrita en 1492 e impresa en 1494, *De septum secundeis (Las siete Inteligencias Secundarias)* de 1508, una historia del mundo basada en la astrología; *Annales Hirsaugiensis*[28] de 1514, y su *Polygraphia* de 1518.

---

[28]Annales Hirsaugiensis. Su título completo es: ANNALES HIRSAUGIENSIS...COMPLECTENS HISTORIAM FRANCIAE ET GERMANIAE, GESTA IMPERATORUM, REGUM, PRINCIPIUM, EPISCOPORUM, ABBATUM, ET ILLUSTRIUM VIRORUM, ("*Los anales de Hirsau...incluyendo la historia de Francia y Alemania, las hazañas de emperadores, reyes, príncipes, obispos, abades, y hombres ilustres* ". Hirsau fue un monasterio cercano a Württemberg, cuyo abad encargó el trabajo en 1495, pero su confección en dos volúmenes duró hasta 1514 (trabajo con 1400 páginas). Este libro se imprimió por primera vez en 1690 y algunos le consideran el primero de los libros humanistas en Alemania.

Los conocidos como *Cipher Manuscripts*[29] fueron escritos siguiendo el esquema de la cifra de Trithemius (el Alfabeto Tebano[30]), un sencillo cifrado por sustitución monoalfabética que Trithemius describe en su libro *Polygraphia*. Esos manuscritos en cifra fueron utilizados para fundar en 1888 la Orden Hermética del Dorado Amanecer, una sociedad secreta masónica que tuvo una gran influencia en la sociedad inglesa durante la era Victoriana y en el ocultismo europeo moderno.

Entrados en el siglo XVI, nos encontramos con Blaise de Vigenère (1523-1596), un diplomático y criptógrafo francés. El cifrado de Vigenère se llama así porque, incorrectamente, se atribuyó a él su invención en el siglo XIX. Vigenère nació en la villa de Saint-Pourçain, y a la edad de 17 años entró en el servicio diplomático, en el permaneció durante los siguientes treinta años, retirándose en 1570. Cuando sólo tenía 22 años fue enviado a la Dieta de Worms como secretario, y más tarde entró al servicio del Duque de Nevers. En 1549 fue a Roma en una misión diplomática que duró dos años, y regresó de nuevo en 1566. En ambos viajes, Vigenère entró en contacto con libros de criptografía y con criptógrafos. En su retiro, Vigenère escribió veinte libros, entre los cuales destacan un *Traicté de Cometes, un Traicté de Chiffres* (1585) y un *Traicté du Feu et du Sel* (1608). En su libro *Traicté de Chiffres* el autor describe la cifra de autoclave que había inventado y que, realmente, fue la primera cifra de este tipo cuya ruptura no es trivial.

El mal denominado Cifrado de Vigenère es un método de cifrado que utiliza una serie de diferentes cifras de Cesar dependiendo de las letras de una palabra clave. Esta es la versión más sencilla de un cifrado por sustitución polialfabética. El cifrado de Vigenère ha sido reinventado repetidas veces. Originalmente fue descrito por Giovanni Battista Bellaso en su libro "*La cifra del Sig. Giovan Battista Bellaso*". Esta cifra es bien conocida porque es fácil de entender y de utilizar, además de parecer irrompible para los neófitos.

Giovanni Battista Bellaso nació en el seno de una antigua y noble familia de Brescia, Italia, en el año 1505 y en 1534 estudió en la Universidad de Pádova donde se laureó en derecho civil en el año 1538. Mas tarde, en el año 1549 fue a Roma para entrar al servicio del Cardenal Duranti, luego pasó al servicio del Cardenal Rodolfo Pio, con el que compartiría su pasión por la experimentación científica y por la criptografía; en esa misma ciudad conoció a Blaise de Vigenère. En 1553 Bellaso publicó en Venecia su libro

[29]Ver http://www.hermetic.com/gdlibrary/cipher/

[30]Ver http://en.wikipedia.org/wiki/Theban_alphabet

titulado "*La Cifra del Sig. Giovan Battista Bellaso*"[31]. Dos años después publicó en Brescia la obra "*Novi et singolari modi di cifrare*" y en 1564, también en Brescia, publicó el libro titulado "*Il vero modo di scrivere in cifra*".

Bellaso era un hombre con gusto por la investigación e interesado por las matemáticas, que se dedicó a la escritura secreta en una época en la que estos artes gozaban de gran reconocimiento en todas las cortes italianas, independientemente de si eran divinas o humanas. Bellaso, un poco por pasión y un poco por necesidad, experimentaba con nuevos sistemas de cifrado para su práctica profesional cotidiana como secretario, y fue él quien dio con un método que ha hecho historia y al que se le ha considerado indescifrable durante cuatro siglos. En el primero de sus tres opúsculos cuenta como había tenido muchos años de práctica cuando estaba al servicio del cardenal Duranti.

Blaise de Vigenère recuerda a Bellaso como parte del séquito del cardenal Rodolfo Pio de Capri en el año 1549, y le atribuye la invención de la cifra polialfabética con clave lateral, e incluso la invención de la *tabla recíproca* hoy conocida como "Tabla Della Porta". En 1564 Bellaso acusó a Della Porta de plagio por haber impreso la tabla recíproca sin citarle como verdadero inventor de la misma.

Fue Bellaso el primero en proponer que se identificase la serie de alfabetos individuales puestos en juego durante un cifrado polialfabético mediante un verso convenido, además de sugerir varios modos de formar los alfabetos cifrantes con la finalidad de liberar a los comunicantes de la necesidad de intercambiarse discos o tablas precompiladas. El método de Bellaso es claramente polialfabético y, a diferencia de la cifra de León Battista Alberti, este sistema es estrictamente periódico, aunque el uso de uno o varios versos lo puede hacer bastante seguro, incluso cuando las tablas fuesen de dominio público.

El segundo libro de Bellaso, "*Novi et singolari modi di cifrare de l'eccellente dottore di legge Messer Giovan Battista Bellaso nobile bresciano… Stampati per Lodovico Britannico in Brescia. 20 decembre 1555*", continuación del primero, contiene una tabla que se construye desplazando la segunda mitad del alfabeto de un modo regular y, a la hora de cifrar, los alfabetos y la secuencia de letras indicadoras son mezcladas según una palabra clave previamente acordada, que puede ser distinta para cada destinatario.

---

[31]El 21 de julio del año 1553 ve la luz en Venecia la obra "*La cifra del Sig. Giovan Battista Bellaso, gentil'huomo bresciano, nuovamente da lui medesimo ridotta à grandissima breuità & perfettione*", escrita por Giovan Battista Bellaso y dedicada al polígrafo Girolamo Ruscelli.

En 1564 aparece en Brescia y con los tipos de Giacomo Britannico apodado "*il Giovane*", la obra titulada "*Il vero modo di scrivere in Cifra con facilità, prestezza, et securezza di Misser Giovan Battista Bellaso, gentil'huomo bresciano*", dedicada al cardenal Alessandro Farnese. Este tratado es el epílogo y la lógica continuación de los dos trabajos precedentes. Los alfabetos que forman la tabla que aparece en dicho texto son generados nemotécnicamente mediante el uso de una palabra clave, por otra parte, incoherente. El cifrado puede hacerse palabra a palabra, con o sin letras indicadoras y la periodicidad aumenta respecto a otros métodos propuestos por el mismo autor. La idea esencial era la de utilizar varios alfabetos desordenados y una palabra o un verso que actúe como clave secreta.

Los alfabetos recíprocos al estilo Bellaso son obviamente mas débiles que los alfabetos completamente aleatorios propugnados por el método de Alberti; sin embargo, las claves largas y la aperiodicidad pueden hacer que el trabajo de rotura de la clave sea verdaderamente difícil, como queda de manifiesto probando a resolver alguno de los ejercicios propuestos[32] en su opúsculo por el propio Bellaso. Su sistema autocifrante puede considerarse superior al atribuido a Vigenère por la simple razón de que la elección del alfabeto se hace, en parte, con el texto en claro, y en parte de forma progresiva, rompiendo así la cadencia regular típica del sistema de Vigenère.

El Barroco y los maestros de espías

En pleno siglo XVI, aparece otro de los personajes clave que son necesarios para entender el papel que puede llegar a jugar la criptografía en la vida de las sociedades; se trata de Francis Walsingham (1532-1590) que ha pasado a la historia como el maestro de espías de la reina Isabel I de Inglaterra. Admirador de Niccolo Machiavelli, a Walsingham se le recuerda como uno de los mas hábiles tejedores de redes de espías de la historia, y como un excelente maestro en el uso de intrigas y engaños para defender a la corona inglesa. Walsingham es uno de los padres de los modernos servicios de inteligencia[33].

---

[32]Se ha llegado a afirmar que Bellaso había anticipado la ley de la caída isocrona de los cuerpos de Galileo escribiendo en su tratado de 1564: "*La ragione perche lassando cadere da alto à basso due palle, una di ferro, l'altra di legno, cosí presto cada in terra quella di legno, como quella di ferro*". Este es el enunciado de siete de los retos propuestos para ser solucionados por el lector y que deberían contener la explicación del enunciado dado en claro.

[33]**Inteligencia** es información valiosa por su actualidad y relevancia, mas que por su detalle o precisión -en contraste con "*datos*" que típicamente se refieren a informaciones o valores precisos o particulares, o a"*hechos*" que normalmente se refiere a información verificada.

En el ámbito del contraespionaje, Walsingham estuvo detrás del descubrimiento de los complots de Throckmorton[34] y Babington para eliminar a la reina Elizabeth I, y así devolver a Inglaterra al catolicismo poniendo en el trono a la reina Mary de los escoceses.

En noviembre de 1583, después de varios meses de vigilancia, Walsingham mandó arrestar a Throckmorton y le extrajo, bajo tortura, una confesión en la que admitía haber conspirado con el embajador español en Londres Bernardino de Mendoza y otros, en contra de la reina Isabel I. El complot proponía la invasión de Inglaterra y Escocia desde el continente y la sublevación de los católicos del interior. Throckmorton fue ejecutado en el año 1584 y Mendoza expulsado de Inglaterra.

En este caso la Reina Mary no fue acusada pero Walsingham estaba muy preocupado por la influencia que ésta tenía tanto dentro como fuera de Inglaterra, por lo que se propuso eliminarla. El complot conocido como de Babington, fue el resultado mas claro de esa determinación. Walsingham infiltró a sus agentes entre los miembros de la comunidad católica inglesa y fomentó sus divisiones internas.

El nombre de esta conspiración se lo debe al del conspirador Anthony Babington (1561-1586), un joven noble católico de Derbyshire. Fue John Ballard, un cura jesuita y agente católico, el que reclutó a Babington y lo convenció para que se involucrara en un complot para destronar o asesinar a la reina Isabel I, y sustituirla por la católica reina de Escocia. En diciembre de 1585, Walsingham arrestó a Gilbert Gifford, un confidente de los conspiradores que le dio la llave para poder desmantelar esa conspiración.

Gilbert Gifford nació en Staffordshire en el año 1560, y su padre era John Gifford, un rebelde católico que se negaba a aceptar los estándares establecidos por la iglesia de Inglaterra. Gifford fue ordenado diácono en 1585. En su tiempo como estudiante, Gifford se hizo amigo de John Savage, estudiante que ya estaba involucrado en el complot de Babington. En octubre de 1585 Gifford abandonó el colegio de Rheims y fue a París,

[34]**Francis Throckmorton** (1554-1584) fue un conspirador católico contra la reina Isabel I de Inglaterra. Era hijo de Sir John Throckmorton y sobrino de Sir Nicholas Throckmorton, uno de los diplomáticos de Isabel I y su embajador en Francia. En 1580, se entrevistó con descontentos católicos ingleses asilados en España y Francia, y a su vuelta a Inglaterra en 1583, actuó como intermediario para las comunicaciones entre los que apoyaban la causa católica en el continente, la Reina Mary prisionera y el embajador español Bernardino de Mendoza. Un registro de su casa dió suficientes pruebas incriminatorias y, después de ser torturado, confesó su implicación en un complot para eliminar a la reina y restaurar la iglesia católica en Inglaterra. Aunque Throckmorton mas tarde se retractó de su confesión, fue condenado por alta traición y ejecutado en 1584.

donde se entrevistó con Thomas Morgan, un agente de la reina Mary, y con Charles Paget, otro conspirador. A su regreso a Inglaterra en diciembre fue arrestado y llevado a Londres para ser interrogado por Walsingham. Después del arresto, Gifford accedió a colaborar como agente doble. Mientras trabajaba para Walsingham, Gifford llevaba mensajes entre la Reina Mary y sus seguidores permitiendo así que los mensajes fuesen interceptados por Walsingham.

En el mes de julio de 1586, Gifford entregó el primer mensaje remitido por Mary a Anthony Babington. La carta de la reina prisionera decía que tenía partidarios suyos en París. La respuesta de Babington a Mary fue que él tenía un centenar de seguidores dispuestos a colaborar en la liberación de Mary, y que en la conspiración contaba con seis amigos personales que se encargarían de su liberación. En el mensaje, Babington, un católico, desveló sus sentimientos contra Isabel I, a la que describía como una usurpadora a la vez que proclamaba que él y muchos otros estaban libres de la obediencia a la reina Isabel I debido a la excomunión de ésta por parte del Papa Pio V en 1570.

Los mensajes entre Mary y Babington estaban codificados mediante un nomenclátor o libro de códigos, que utilizaba símbolos para representar algunas palabras y frases comunes y también tenía sustituciones para representar a las letras (23 símbolos para la sustitución de letras y 36 caracteres para palabras y frases). El mensajero los pasaba de contrabando dentro y fuera de la prisión, ocultos dentro de los tapones de un barril de cerveza que un cervecero cercano entregaba y recogía. Los sirvientes de la reina Mary debían recoger los mensajes de los barriles de cerveza y poner en sus tapones huecos los mensajes de respuesta.

Walsingham tenia identificada la conspiración y estuvo intentando aclarar cuales eran las identidades de los seis conspiradores que formaban el núcleo central del complot. Cada mensaje entre Mary y Babington primero era leído por Walsingham, copiado en la escuela de espías de éste, y enviado a su destino intacto. La escuela de espías de Walsingham decodificó cada mensaje por prueba y error empezando por las sustituciones de letras y utilizando la frecuencia de los caracteres más comunes hasta que se obtenía un texto legible, y el resto se adivinaba por el contexto hasta que todo el documento era compresible. Después de que se descubriera en que consistía la cifra, los mensajes interceptados eran leídos en el mismo día que se copiaban. Cada mensaje era devuelto en condiciones tales que no mostraba evidencia de que hubiese sido ya leído y copiado.

En Julio de 1586, Babington propuso a Mary que Isabel I fuese asesinada, y hacía referencia a una invasión desde España, y a que tenía un plan para

librarla de su prisión. Según ese mensaje, el Emperador Felipe II había prometido enviar una expedición militar a Inglaterra cuando la reina Isabel I no estuviera ya en el poder. En un mensaje fechado en el mes de julio de 1586 también se explicaba cuáles eran los preparativos para matar a Walsingham y a Lord Burghley, por aquel entonces Primer Ministro de Isabel I. Con esos mensajes Walsingham ya tenía la evidencia que necesitaba para implicar a la reina de los escoceses, aunque aún le faltasen las identidades de los seis conspiradores.

En la última carta de Mary a Babington, le agradecía sus esfuerzos por liberarla y derrocar a Isabel I, Walsingham decidió intervenir en ese punto y le pidió a Thomas Phelippes[35], un experto en descifrar cartas, falsificar textos manuscritos y en romper y reparar sellos sin que se notara, que añadiese una coletilla a la carta original preguntando cuál era la identidad concreta de los seis conspiradores. Babington recibió la nota falsificada y el mensaje, pero nunca contestó con los nombres de los conspiradores.

Poco después Babington fue arrestado mientras buscaba un pasaporte para ir a entrevistarse con Felipe II en España. A pesar de no haber contestado, las identidades de los seis conspiradores fueron descubiertas por otros medios, y todos ellos fueron arrestados el 15 de agosto de 1586. Con las pruebas obtenidas en la intercepción epistolar fue fácil juzgar, condenar y conseguir la ejecución de la reina de los escoceses en 1587.

Ya en el siglo XVII y siguiendo todavía en suelo inglés, aparece otro personaje análogo a Walsingham, aunque esta vez dicho personaje no estaba allí para proteger a la corona inglesa. Se trata de John Wilkins (1614-1672), un clérigo ingles y, curiosamente, la única persona que ha dirigido tanto la Universidad de Oxford como la de Cambridge. Se casó con la hermana de Oliver Cromwell, Robina, y fue el primer secretario de la Royal Society of London desde su primera reunión en 1660 y fue Obispo de Chester desde 1668 hasta su muerte.

En el año 1641, Wilkins publicó un tratado anónimo titulado "*Mercury, or The Secret and Swift Messenger*". Esta pequeña y clara obra sobre criptografía fue de lo más oportuna y un verdadero regalo para los diplomáticos y líderes que habrían de actuar en las inminentes guerras civiles británicas (1642-1646 y 1648-1649) entre puritanos parlamentaristas *(roundheads*)

---

[35]**Thomas Phelippes** (1556-1625) era un falsificador y agente de inteligencia. Sirvió principalmente a las órdenes de Sir Francis Walsingham, durante el reinado de Isabel I de Inglaterra, descifrando códigos utilizados en las conspiraciones contra ella. Se le recuerda por haber sido quien puso la coletilla en la carta de la reina Mary a Babington.

y monárquicos (*roytalists*) que apoyaban al rey Carlos I y a su estirpe. En 1648, Wilkins fue nombrado director del Wadham College de Oxford, y bajo su mandato el colegio prosperó extraordinariamente. Aunque apoyaba a Oliver Cromwell, había mantenido el contacto con los monárquicos más cultivados, quienes le entregaban sus hijos para su educación. En 1656, se casó con Robina Cromwell y en 1659, poco antes de su muerte, Oliver Cromwell hizo las gestiones pertinentes para que nombrasen a su cuñado director del Trinity College de Cambridge, nombramiento que fue confirmado por el sucesor de Cromwell como Lord Protector de Inglaterra, su hijo Richard Cromwell.

La era moderna

Hasta finales del siglo XVIII, las comunicaciones sólo podían realizarse mediante mensajeros que fuesen de un sito a otro transportando personalmente la información de origen a destino. Sin embargo, en 1792 Claude Chappe puso en funcionamiento la primera línea de comunicación a largas distancias basándose en el uso de semáforos.

Un semáforo o telégrafo óptico es un aparato para transportar información a través de señales visuales entre torres y mediante palas móviles, ventanas en una matriz, mediante banderas utilizadas a mano, etc. La información se codifica según la presencia y la posición de los elementos mecánicos. Otros ejemplos de telegrafía óptica los constituyen el sistema internacional de banderas de señalización marítima, las lámparas de Aldis, y los heliógrafos. Las redes de semáforos precedieron al telégrafo eléctrico, y eran mucho más rápidos que los mensajeros a caballo para llevar un mensaje a largas distancias, y también mucho más caro y menos privado que el sistema eléctrico que lo reemplazaría mas tarde. La distancia entre semáforos repetidores está determinada por la orografía y por el tiempo (visibilidad).

Claude Chappe (1763-1805) fue un inventor francés que en 1792 demostró la utilidad práctica del sistema de semáforos que luego se expandiría por Francia y que fue el primer sistema práctico de telecomunicaciones. Chappe nació en Brûlon, Francia, y era nieto de un barón frances. Se había dedicado al servicio de la iglesia, pero perdió su cargo durante la Revolución Francesa. Él y sus cuatro hermanos desempleados decidieron desarrollar un sistema práctico de estaciones repetidoras de semáforos, posibilidad considerada desde la antigüedad pero nunca realizada hasta ese momento.

Ignace Chappe (1760-1829), hermano de Claude, era miembro de la Asamblea Legislativa durante la revolución y con su ayuda, la asamblea

apoyó la propuesta de construir una línea de repetidores desde París a Lille (quince estaciones cubriendo 193 km), para transmitir partes de guerra.

Los hermanos Chappe determinaron experimentalmente que los ángulos de un segmento eran más fáciles de ver que la presencia o ausencia de paneles. Su diseño final tenía dos brazos conectados por un travesaño horizontal. Cada brazo tenía siete posiciones, y el travesaño horizontal tenía cuatro más permitiendo expandir un código con 196 combinaciones distintas. Los brazos eran de uno a nueve metros de largo, negros y equilibrados con contrapesos, y se movían sólo con dos manivelas. Pronto se vió que el uso de lámparas montadas sobre los brazos no eran adecuadas para poder utilizar los semáforos durante la noche. Las estaciones repetidoras se colocaron distantes entre sí de 12 a 25 kms., y cada estación tenía un telescopio que apuntaba hacía arriba y abajo en la líneas de repetidores.

En 1792 se transmitió con éxito el primer mensaje entre París y Lille. En 1794 la línea de semáforos informó a los parisinos de la captura de Condé-sur-l'Escaut[36] a los Austrias menos de una hora después de haber ocurrido la victoria. Se construyeron otras líneas y el sistema fue copiado por otros estados europeos; Napoleón lo utilizó para coordinar sus ejércitos y su imperio.

En 1824 Ignace Chappe intentó aumentar el interés en el uso de los semáforos utilizándolos para la transmisión de mensajes de carácter comercial, sin embargo, los empresarios y financieros se resistieron. Veintidós años más tarde, en 1846, el gobierno francés apostó por unas nuevas líneas de telégrafo eléctrico. Muchos contemporáneos advirtieron lo fácil que era el sabotaje y la interrupción del servicio dado lo sencillo que era cortar el cable. A pesar de ello, esta nueva tecnología dio al traste con el futuro de las comunicaciones ópticas en el siglo XIX.

Saliendo del viejo continente, al final del siglo XVIII aparecieron los primeros indicios de actividad criptográfica en las por entonces colonias inglesas de América. Estos indicios llegaron de manos de Thomas Jefferson (1743-1826), tercer presidente de los Estados Unidos de Norteamérica (1801-1809), y principal autor de la Declaración de Independencia de Filadelfia (1776), además de ser uno de los padres fundadores de los EEUU por su apoyo a las tesis del republicanismo.

---

[36]**Condé-sur-l'Escaut** es una comuna francesa situada a 12 km al noroeste de Valenciennes, a 51 km de Lille, a 90 km de Bruselas y a 239 km de París. La villa se encuentra en la confluencia de los rios la Haine y l'Escaut.

Mientras servía como Secretario de Estado (1790-1793) de George Washington, Thomas Jefferson desarrolló un ingenioso sistema y método para codificar y decodificar mensajes. Durante la Revolución Americana, Jefferson había utilizado mensajeros para llevar cartas con informaciones sensibles, pero el uso de códigos se volvió parte esencial de su correspondencia cuando fue representante de América en Francia (1784-1789), ya que el sistema de correos europeo abría y leía todas la cartas que pasaban a través de él.

El disco de Jefferson es un sistema de cifrado que utiliza 36 ruedas, cada una de ellas con todas las letras del alfabeto marcadas en su canto, y siguiendo un orden aleatorio. El invento de Jefferson tuvo lugar en 1795 pero no llegó a ser suficientemente conocido, por lo que cayó en el olvido hasta que fue reinventado un siglo después por el comandante Étienne Bazeries, el conquistador de la Gran Cifra[37]. Después de esta segunda invención, este sistema fue utilizado por el ejército americano desde 1923 hasta 1942 con el nombre de M-94. La segunda versión de esta misma invención es lo que se denomina el Cilindro de Bazeries.

---

[37]**La Gran Cifra** fue un nomenclator desarrollado por una familia de criptógrafos franceses conocidos como los Rossignol (Antoine, Bonaventure y Antoine-Bonaventure Rossignol), que sirvieron a la corona francesa como criptógrafos. Este nomenclator era muy bueno en su clase, de ahí su nombre; tenía reputación de irrompible y, de hecho, incluso después de caer en desuso, algunos mensajes de los archivos franceses, diplomáticos en apariencia, son completamente ilegibles.

La cualidades como criptógrafo de Antoine Rossignol se hicieron bien conocidas cuando, en 1626, se capturó una carta cifrada a un mensajero que salía de la ciudad de Réalmont, controlada por lo hugonotes y sitiada por el ejército francés. Esta carta decía que los sitiados no serían capaces de aguantar por mucho más tiempo, y al final del mismo día en que dicha carta fue capturada, Rossignol ya la había descifrado. Los franceses devolvieron la carta con el mensaje descrifrado adjunto, lo que forzó a los sitiados a rendirse. Él y su hijo Bonaventure Rossignol pronto fueron elevados a puestos importantes de la corte.

Juntos, padre en hijo, desarrollaron un código que utilizaba 587 números diferentes que era tan robusto que resistió el criptoanálisis durante siglos hasta la llegada del comandante Étienne Bazeries, quien fue capaz de romperla en 1893, al darse cuenta de que cada número representaba una sílaba francesa en lugar de una letra como ocurría habitualmente en los códigos de la época. Brazeries imaginó que un secuencia de números que se repetían, 124-22-125-46-345, quería decir "les ennemis" y a partir de esa suposición fue capaz de deshacer el secreto de toda la cifra.

En una de las cartas descifradas por Bazeries aparece una posible solución al misterio del hombre de la máscara de hierro. Esa carta se refería a un general llamado Vivien de Bulonde que tenía que atacar el pueblo italiano de Cuneo pero, en lugar de ello, huyó, facilitando así la llegada de los Austrias y, consecuentemente, poniendo en serio peligro el éxito de toda la campaña francesa en Piamonte. La carta descifrada decía así:

Étienne Bazeries (1846-1931) fue un criptoanalista militar francés que estuvo en activo entre 1890 y la Primera Guerra Mundial y de él escribió el historiador David Kahn lo siguiente: "*el gran pragmático de la criptología. Sus contribuciones teóricas irrelevantes, pero el fue uno de los mas grandes criptoanalistas naturales que la ciencia ha tenido*" (Kahn 1996, p244).

Aparentemente, Bazeries se interesó por la criptografía a través de la solución de criptogramas aparecidos en las columnas de anuncios personales de los periódicos, y pronto aplicó su experiencia criptoanalítica al ámbito militar cuando, en 1890, resolvió mensajes cifrados con el sistema oficial de transposición del ejercito francés, lo que obligó al Ministerio de la Guerra a cambiar y adoptar un nuevo sistema. En un esfuerzo por promover la reforma dentro de los sistemas del gobierno y aumentar la seguridad nacional, Bazeries se dedicó a descubrir las debilidades de los sistemas franceses de cifrado. En 1891, ya habían corrido noticias sobre su talento, y empezó a trabajar en la Sección de Cifra del Ministerio de Asuntos Exteriores. Bazeries continuó su trabajo criptoanalítico en ese puesto incluso después de ser licenciado del ejército en 1899, ayudando en la resolución de las cifras militares alemanas utilizadas durante la Primera Guerra Mundial. Sin embargo, muchas de las recomendaciones de Bazeries al gobierno francés y que iban dirigidas a mejorar los sistemas de cifra oficiales, se toparon con una burocracia interminable y muchos desaires, lo cual terminó convirtiéndose en una fuente continua de frustración dentro de una carrera ilustre[38]. Bazeries se retiró en 1924, a la edad de setenta y ocho años. Su libro de 1901 titulado "*Les Chiffres secrets dévoilés*" (*Cifras Secretas Desveladas*) se considera una referencia básica en la literatura sobre criptografía.

El cilindro de Bazeries consiste en un conjunto de 20 a 30 discos numerados, con un alfabeto distinto grabado en el canto, y con un agujero en el centro para que puedan ser apilados sobre un mismo eje. Los discos son

---

> *"Su Majestad conoce mejor que cualquier otra persona las consecuencias de este acto, y tambien sabe de cuan profundamente nuestro fracaso en tomar la plaza perjudicará nuestra causa, u fallo que debe subsanarse durante el invierno. Su Majestad desea que usted arreste inmediatamente al General Bulonde y le haga conducir a la fortaleza de Pignerole, donde será encerrado en una celda con guardia nocturna, y donde se le permitirá caminar por el patio durante el día con una máscara".*

[38]Ver Candela, Rosario, *The Military Cipher of Commandant Bazeries*. New Cork. Cardanus Press, 1938.

removibles y pueden ser montados en el eje siguiendo cualquier orden. El orden en el que se ponen los discos puede considerarse la clave de cilindro de Bazeries, y el destinatario y remitente deben poner los discos exactamente en el mismo orden.

Una vez que se han ensartado los discos correctos en el orden correcto, el usuario puede rotar cada disco hasta que la frase del texto que se quiere cifrar aparezca en una línea. Luego, el remitente puede copiar cualquier otra línea de texto como criptograma. El destinatario del mensaje simplemente tiene que poner los discos en el orden correcto, escribir el mensaje cifrado en una de las líneas, y luego buscar en las restantes generatrices del cilindro hasta reconocer una línea con sentido que será la del texto en claro. Hay una probabilidad extremadamente baja de que haya dos líneas con mensajes legibles y con sentido, pero esto sería detectado por el propio generador del cifrado al elegir el criptograma. Este sistema es bastante seguro incluso frente al criptoanálisis moderno, especialmente si el mensaje es corto y el orden de las letras en los cantos de los discos no son conocidos por el atacante. Según se hagan más largos los mensajes, más fácil será aplicar el análisis de frecuencias y encontrar patrones que rompan el código.

Otro ejemplo importante del efecto de la criptografía en el devenir de la historia lo podemos encontrar en la denominada Guerra Peninsular o Guerra de Independencia que enfrentó a la alianza de España, Portugal y Reino Unido contra Francia en el suelo de la península Ibérica durante las guerras napoleónicas. La guerra empezó cuando los ejércitos franceses ocuparon España en 1808 y duró hasta que la "coalición de los seis" venció a Napoleón en 1814.

Ya sabemos que la liberación de España es una de las primeras contiendas modernas en las que se hizo uso de la guerra de guerrillas a gran escala, y que su éxito, en parte, fue debido a las guerrillas españolas y a la incapacidad de los grandes ejércitos de Napoleón Bonaparte para pacificar a los habitantes de los territorios ocupados, pero también algo tuvo que ver la habilidad criptoanalítica de los aliados.

En esa guerra resalta el papel jugado por George Scovell (1774-1861), un miembro de la intendencia de la Armada británica que estaba destinado en la península ibérica durante la Guerra de Independencia española. La historia le recuerda por su papel crucial en la ruptura de los códigos utilizados por la fuerzas francesas durante dicha contienda. Como dotado lingüista que era, se le asignó un equipo de colaboradores pertenecientes a varias nacionalidades que habían sido reclutados por sus conocimientos de los hechos locales y por sus habilidades lingüísticas. Este equipo

desarrolló un sistema bastante eficaz para interceptar y descifrar las comunicaciones francesas. En la primavera de 1811, el ejército francés empezó a utilizar un código basado en una combinación de 150 números, y que fue conocido como el Código del Ejército Portugués; Scovell rompió ese código en dos días.

Al final de 1811, un nuevo código llamado el Gran París fue enviado a todos los oficiales del ejército francés. Se basaba en 1400 números y derivaba de un código diplomático del siglo XVIII que añadía figuras sin sentido al final de las cartas. En diciembre de 1812, cuando una carta de José Bonaparte enviada a Napoleón fue interceptada, Scovell pudo descifrar lo suficiente para enterarse de los planes y operaciones concretas que iban a realizar los franceses. La información conseguida fue vital para la victoria del general Wellington sobre los franceses en la ciudad de Vitoria el 21 de junio de 1813.

El telégrafo y la popularidad del cifrado

Aunque realmente no contribuyó al desarrollo de la criptografía, si es necesario mencionar a Joseph Henry (1797-1878), científico escocés naturalizado americano que, entre otras cosas, fue el primer secretario de la Smithsonian Institution. Durante su vida, fue considerado por sus compatriotas como uno de los más grandes científicos americanos desde Benjamin Franklin. Henry, mientras construía electroimanes, descubrió el fenómeno electromagnético de la auto-inductancia y de la inductancia mutua, a la vez que Faraday hacía los mismos descubrimientos en Europa, pero fue Henry el primero en publicar sus resultados. Los trabajos de Henry sobre los relés electromagnéticos fueron las bases del telégrafo eléctrico inventado en 1837 simultáneamente por William Fothergill Cooke y Charles Wheatstone en Inglaterra, y por Samuel Morse en los Estados Unidos. La llegada del telégrafo revolucionó los sistemas de transmisión de la información, ampliando así el ámbito de la criptografía a todas aquellas actividades que iban a fluir a través de sus claves. Además de crear el telégrafo de un solo hilo, Morse fue co-inventor, con Alfred Vail, del famoso código que lleva su nombre: el Código Morse.

Aunque la criptografía durante muchos siglos se mantuvo en los entornos que le eran propios, como los militares, diplomáticos, subversivos, etc., el siglo XIX vino a sacarla de los mismos, ampliando su reducido nicho gracias a los intereses comerciales que hacían uso del telégrafo y, además, la criptografía saltó al ámbito de la población civil gracias a las obras literarias de Poe.

Edgar Allan Poe (1809-1849) fue un poeta, autor de novelas, editor y crítico literario norteamericano, y uno de los dirigentes del Movimiento Romántico norteamericano. Aunque es mas conocido por sus macabros cuentos de misterio, Poe fue realmente uno de los pioneros de las historias cortas, y padre indiscutible de las ficciones detectivescas y de la ciencia ficción[39]. Poe siempre tuvo interés en el campo de la criptografía; de hecho, llegó a colocar un anuncio de sus habilidades como descifrador en el periódico *Alexander's Weekly (Express) Messenger* de Filadelfia, y en él invitaba a sus lectores a que le retasen con todo tipo de cifrados, que él encontraría el modo de resolverlos[40]. Su éxito creó un cierto grado de agitación pública durante varios meses[41]. En el mes de julio del año 1841, Poe publicó un ensayo titulado "*Some Words on Secret Writing*" en la revista *Graham's Magazine*, de la que era uno de sus críticos destacados, y su editor en el periodo 1841-1842. Habiéndose dado cuenta del interés del público en este tipo de artes, Poe escribió la famosa narración titulada "*The Gold-Bug*"[42] en la que incorporaba el análisis de cifrados como elemento estelar de la historia[43].

El éxito de Poe en la criptografía se sostuvo no tanto por sus conocimientos en ese campo, sino por su conocimiento del mundo y de la cultura periodística de su época. Sus afiladas capacidades analíticas, que eran evidentes a la luz de sus historias de detectives, le permitieron ver que el público en general era ampliamente ignorante de cuales eran los métodos con lo que se podía resolver un criptograma sencillo, y utilizó esta percepción en beneficio propio[44]. La sensación que creó Poe con este tinglado

[39]Stableford, Brian: *Science fiction before the genre*. The Cambridge Companion to Science Fiction. Edward James y Farah Mendlesohn Eds. Cambridge University of Press, pp 18-19. 2003.

[40]Morelli, R.: *Edgar Allen Poe and Cryptography*. Historical Cryptography. 2002, disponible en http://starbase.trincoll.edu/~crypto/historical/poe.html

[41]Silverman, Kenneth: *Edgar A. Poe: Mournful and Never-ending Remembrance*. New York Harper Perennial, 1991. p. 152-3.

[42]"***The Gold-Bug***" es una historia corta que se desarrolla en Sullivan's Island, Carolina del Sur y que incluye el descifrado de un mensaje secreto y el hallazgo de un tesoro. La historia fue publicada por primera vez en *Philadelphia Dollar Newspaper* en junio de 1843 después de que Poe ganase un concurso literario organizado por ese periódico; el premio que recibió fue de 100 dólares. El criptograma misterioso era:

53‡‡†305))6*;4826)4‡.)4‡);806*;48†860))85;1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*4)88*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

[43]Rosenheim, Shawn James: *The Cryptographic Imagination*. Baltimore. Johns Hopkins University Press. 1997. pp. 2, 6.

[44]Dukes, Daniel W.: *The Legend of Poe the Cryptographer*. The Poe Perplex, disponible en http://www.usna.edu/EnglishDept/poeperplex/cryptop.htm

criptoanalítico jugó un papel esencial a la hora de popularizar el uso y publicación de criptogramas en los periódicos y revistas[45].

Poe ha tenido una prolongada influencia en la criptografía más allá del que causara en el público a lo largo de su vida. William Friedman, el mas destacado criptólogo norteamericano, estaba muy influido por Poe. El interés inicial de Friedman por la criptografía vino tras leer en su adolescencia "*The Gold-Bug*", aunque luego se centró en el descifrado de máquinas japonesas como PURPLE que tuvieron un papel importante en el escenario de la Segunda Guerra Mundial.

Además de imaginar el telégrafo, Charles Wheatstone (1802-1875) fue un científico británico e inventor de varios avances científicos de la era victoriana, entre los que cabe destacar una especie de pequeño acordeón de mano, que se conoce como concertina inglesa, el estereoscopio (artefacto que muestra imágenes tridimensionales), y el cifrado Playfair. Sin embargo, Wheatstone es más conocido por sus contribuciones al desarrollo de lo que hoy se conoce como Puente de Wheatstone, originalmente inventado por Samuel Hunter Christie, y que se utiliza para medir una resistencia eléctrica desconocida.

El cifrado Playfair o cuadrado Playfair es una técnica manual de cifrado simétrica y fue la primera cifra de sustitución digrámica. Este esquema fue inventado en 1854 por Charles Wheatstone, pero lleva el nombre del Lord Playfair porque fue este último quien más promovió su uso. En este sistema se cifran simultáneamente pares de letras (*digramas*), en lugar de utilizar las letras independientes como ocurre en una sencilla cifra de sustitución. El cifrado Playfair es bastante más complejo que el de Vigenère que, por aquel tiempo, estaba en uso. El cifrado Playfair es significativamente más difícil de romper ya que el análisis de frecuencias no funciona en este caso. Es cierto que todavía se puede hacer el análisis de frecuencias, pero hay que hacerlo sobre los 676 ($26^2 = 676$) posibles digramas de un alfabeto con 26 letras (monogramas). El análisis de frecuencias es posible cuando se trabaja con digramas, pero es más trabajoso y requiere mucho más material criptográfico si se quiere tener algún éxito.

El cifrado Playfair fue rechazado por el Ministerio de Asuntos Exteriores británico por su aparente complejidad operativa. Cuando Wheatstone se ofreció a demostrar que tres de cada cuatro niños de una escuela próxima podrían aprender a utilizarlo en menos de quince minutos, el secretario

[45]Friedman, William F.: *Edgar Allan Poe, Cryptographer* en la obra On Poe: "*The Best from American Literature*". Durham, NC. Duke University Press, 1993. p. 40-1

del Foreign Office le respondió[46], "*Eso es muy posible, pero nunca logrará enseñárselo a los agregados consulare*s".

Sin embargo, el código Playfair fue utilizado con propósitos bélicos por las fuerzas británicas involucradas en la Segunda Guerra de los Boers, y en la Primera Guerra Mundial, y también por los australianos durante la Segunda Guerra Mundial. La razón de este extendido uso de Playfair es que se trata de una cifra razonablemente rápida y su uso no requiere equipos especiales. Un escenario típico del uso del cifrado Playfair sería el de proteger información importante, pero no crítica, durante una batalla. Para cuando los criptoanalistas enemigos hubiesen podido romper la clave y dar con el mensaje en claro la información sería inútil para ellos. Playfair no ha vuelto a ser utilizado por las fuerzas militares debido al advenimiento de los sistemas digitales de cifrado. Ahora se considera que Playfair es un código inseguro para cualquier propósito. La primera solución publicada de la cifra Playfair fue descrita en un panfleto de diecinueve páginas escrito por el teniente Joseph O. Mauborgne[47], publicado en 1914.

La cifra Playfair utiliza una tabla de 5 por 5 conteniendo hasta 25 letras, y una palabra clave o frase secreta. Memorizar la palabra clave y cuatro sencillas reglas es todo lo que se necesita para poder cifrar y descifrar. Como muchas cifras premodernas, la de Playfair puede ser rota fácilmente si se dispone de suficiente criptograma. Conseguir dar con la clave es bastante inmediato cuando se conocen tanto el criptograma como su correspondiente texto en claro. Pero cuando sólo se conoce el criptograma, el criptoanálisis por fuerza bruta implica buscar a través del espacio de claves coincidencias entre las frecuencias de ocurrencia de los digramas (pares de letras) del criptograma y la frecuencia de ocurrencia de los digramas en el lenguaje que se supone que está escrito el mensaje original.

El nacimiento del criptoanálisis moderno

El reinado de las cifras polialfabéticas como inaccesibles para los criptoanalistas se terminó con las aportaciones de Charles Babbage y Friederich W. Kasiski.

---

[46]Literalmente: "*That is very possible, but you could never teach it to attachés*".

[47]En la historia de la criptografía, **Joseph Oswald Mauborgne** (1881-1971) fue co-inventor del cifrado basado en *one-time pads* con Gilbert Vernam que trabajaba en Bell Labs.

Charles Babbage (1791-1871), matemático, filósofo e ingeniero mecánico inglés, fue el primero a quien se le ocurrió la idea de construir un computador programable. Partes del mecanismo original construido por él se encuentran expuestas en el Museo de la Ciencia de Londres[48]; en el año 1991 se construyó, a partir de los diseños originales, un ejemplar completo de la máquina diferencial de Babbage y resultó que funcionaba perfectamente. Construida con las tolerancias propias del siglo XIX, el éxito de la máquina completa indica que la máquina de Babbage hubiese funcionado si se hubiese terminado.

Además de sembrar, sin éxito, las bases de los futuros ordenadores programables, Babbage también tuvo resultados notables en criptografía al conseguir romper el cifrado de autoclave de Vigenère, al que se denominaba "*the undecipherable cipher*". Los descubrimientos de Babbage fueron utilizados por las fuerzas militares británicas en diferentes campañas, y no fueron publicados hasta varios años después. En aquel momento se vio la coincidencia de los resultados de Babbage y los del oficial prusiano Friedrich Kasiski, que también los había obtenido de manera independiente.

El Mayor Friedrich Wilhelm Kasiski (1805-1881) fue un oficial de la Infantería de Prusia del Este, criptógrafo y arqueólogo. Kasiski nació en Schlochau, Prusia Oeste (ahora Czluchow, Polonia). En el año 1863, Kasiski publicó un libro con noventa y cinco páginas sobre criptografía y titulado "*Die Geheimschriften und die Dechiffrierkunst*" ("*Escritura secreta y el arte de descifrarla* "). Esta fue la primera publicación de un procedimiento para atacar, con éxito prácticamente asegurado, los cifrados basados en sustituciones polialfabéticas y, en particular, al cifrado de Vigenère.

El método de Kasiski se basa en el análisis de las distancias que hay entre fragmentos iguales que se repiten a lo largo del texto cifrado; tal análisis puede dar indicios sobre cuál es la longitud de la clave utilizada en el cifrado polialfabético. La hipótesis sobre la que se basa este análisis es que las repeticiones que aparecen en un criptograma se deben a una de dos posibles causas: (1) o son coincidencias fortuitas y su distribución sería homogénea sobre toda la longitud del criptograma, (2) o son el resultado de repeticiones presentes en el texto en claro y que aparecen alineadas de la

[48]**The Science Museum** se encuentra situado en Exhibition Road, en el barrio de South Kensington, en Londres SW7, y es una parte importante de National Museum of Science and Industry (NMSI) y constituye una de las atracciones turísticas de la ciudad (Muy recomendable).

misma manera con la clave secreta de cifrado que se repite. En este segundo caso, la distancia entre repeticiones deberá ser un múltiplo entero de la longitud de la clave que se repite iterativamente a lo largo de todo el texto. Analizando los factores de las distancias entre repeticiones podemos obtener indicios sobre cuál es la longitud de la clave empleada en el proceso de sustitución polialfabética. A esta técnica se la conoce como Análisis de Kasiski.

La importancia del trabajo criptoanalítico de Kasiski no fue apreciada en su justa medida en el tiempo en que éste se produjo, y al no ser seducido por lo vítores de sus contemporáneos, Kasiski decidió dedicarse a la arqueología que era lo que realmente le llamaba la atención. Los últimos años de su vida los pasó en la ciudad de Neustettin (Szczecinek) y, como dice David Kahn, "*Kasiski se murió el 22 de Mayo de 1881 y, con toda seguridad, lo hizo sin saber la gran revolución que causó en la criptología*".

A finales del siglo XIX se empiezan a vislumbrar las reglas que permitirían realmente afrontar la tarea de crear nuevos sistemas de cifrado razonablemente seguros. En este afán nos encontramos con las aportaciones de un peculiar lingüista y criptógrafo holandés, el Dr. Auguste Kerckhoffs (1835-1903), que enseñó lenguas en reputadas instituciones francesas. Kerckhoffs estudió en la Universidad de Lieja y después de un periodo de tiempo en el que enseñó en escuelas de Holanda y Francia, se hizo profesor de lengua alemana en la Escuela de Altos Estudios Comerciales de París.

Su fama la debe a dos ensayos que publicó, durante el año 1883, en "*Le Journal des Sciences Militaires*" titulados "*La Cryptographie Militaire*"[49]. Esos artículos revisaban cuál era el estado del arte en la criptografía militar de aquellos tiempos, y ponían de manifiesto que era necesario mejorar considerablemente las capacidades francesas en tales actividades.

Kerckhoffs también incluyó en sus artículos varios consejos y reglas prácticas, además de seis principios[50] para el diseño de nuevas cifras. De esos seis, el más importante es el que dice que "*El diseño de un sistema*

[49]Auguste Kerckhoffs, *La cryptographie militaire*, Journal des sciences militaires, vol. IX, p. 5-83, Jan. 1883, pp. 161-191, Feb. 1883. disponible en http://www.petitcolas.net/fabien/kerckhoffs/

[50]Las **seis reglas de Kerckhoffs** son: [1] El sistema deberá ser, si no teóricamente irrompible, al menos irrompible en la práctica. [2] El diseño de un sistema no debería requerir el secreto y el compromiso del sistema no deberá ser un inconveniente para los corresponsales. [3] La clave deberá ser memorizable sin necesidad de notas y deberá ser fácil cambiarla. [4] Los criptogramas deberán ser transmisibles por telégrafo. [5] El aparato o documentos relacionados deberán ser portables y operados por una sola persona. [6] El sistema deberá ser sencillo, y no requerirá de una larga lista de reglas ni supondrá estrés mental.

no debería requerir el secreto y el compromiso del sistema no deberá ser un inconveniente para los corresponsales", y que se conoce como Principio de Kerckhoffs. La seguridad del sistema sólo debe reposar sobre el secreto de la clave, y no sobre el secreto de ninguna otra parte del sistema. Esta máxima fue reformulada por Claude Shannon muchos años después, diciendo que "*el enemigo conoce el sistema*". Estas afirmaciones contrastan con las de aquellos que creen que se puede llegar a la seguridad ocultando el sistema mismo y/o su uso.

De acuerdo con el principio de Kerckhoffs, la mayor parte de la criptografía civil se hace utilizando algoritmos públicos y bien conocidos, lo cual contrasta con el hecho de que los sistemas empleados para proteger la información gubernamental o militar clasificada, a menudo se mantienen en secreto[51]. Siguiendo la línea aperturista, Eric Raymond extiende este principio al software de código abierto diciendo: "*Cualquier diseño de software de seguridad que no asuma que el enemigo posee el código fuente, realmente no merece la pena; por tanto, nunca confíes en el software de código propietario*". Aunque han pasado más de ciento veinte años desde que se hizo esta sabia afirmación, todavía hay quienes creen que pueden mantener en secreto el algoritmo de sus generadores de licencias, de sus sistemas multimedia, etc.

Aún sin haber dado cuenta de todos los hechos acontecidos en el siglo XIX, y con objeto de ver cuáles han sido los impactos de la criptografía sobre la vida pública, quizás convenga recordar la historia de lo que se conoce como los cifrados de Beale. Los criptogramas de Beale son un conjunto de tres documentos, de los cuales uno de ellos pretende indicar donde está enterrado un tesoro de oro y plata cuya cuantía alguien ha estimado en treinta millones de dólares actuales. Los otros dos documentos describen el contenido del tesoro, y listan los nombres de los diferentes propietarios de tan codiciable tesoro.

La historia de estos tres criptogramas empezó en un panfleto de 1885 en el que se detallaba que un tesoro había sido enterrado por un hombre llamado Thomas Jefferson Beale en un lugar secreto del estado de Virginia, EEUU, en 1820. Beale confió una caja conteniendo los mensajes cifrados[52] a un tabernero de Lynchburg llamado Robert Morriss cerca de Montvale en Bedford County, y luego desapareció, para nunca más ser visto. El tabernero entregó los tres documentos a un amigo antes de morir, y ese amigo se dedicó los siguientes veinte años a encontrar el

[51]Ver sistemas de cifrado de la NSA en http://en.wikipedia.org/wiki/NSA_encryption_systems

[52]Ver http://www.simonsingh.com/Beale_Treasure_Ciphers.html

modo de descifrar dichos mensajes, y, utilizando una edición particular de la Declaración de Independencia de los Estados Unidos como clave para construir un libro de códigos, el amigo sólo fue capaz de resolver uno de los mensajes, el segundo criptograma, en el que se dan detalles del tesoro enterrado e información muy genérica sobre su localización. Al final, el amigo se rindió e hizo públicas las cartas y los criptogramas mediante un panfleto de 1885 titulado *The Beale Papers*. No hubo explicación alguna sobre qué condujo a la solución del segundo criptograma, lo que nos hace pensar que quizás hubo información suplementaria que hoy se ha perdido. Sin embargo, todavía quedan pendientes de dilucidar los contenidos de los otros dos criptogramas; el primero y el tercero. Desde la publicación del panfleto, se han hecho cierto número de intentos de descifrar estos dos criptogramas y así poder encontrar el tesoro prometido, pero todos han fallado[53].

El siglo XX y las máquinas de cifrado

Antes de terminar el siglo XIX se produce lo que se dio en llamar el Asunto Dreyfus, que fue un escándalo político que dividió en dos a Francia. El asunto Dreyfus se refiere a una falsa acusación de traición a un capitán de artillería por un supuesto paso de secretos militares a los alemanes a través de su embajada en París. El Capitán Alfred Dreyfus, era un joven oficial de artillería y además judío; para su acusación se llevó a cabo un conjunto inusual de instigaciones y obstrucciones claras del funcionamiento de la justicia francesa, todo ello siguiendo las indicaciones de las más altas instancias del ejército galo. Este escándalo duro varios años, y no terminó hasta que el honor del acusado fue completamente reivindicado.

Durante la Primera Guerra Mundial, Holanda permaneció neutral y como ciudadana holandesa, Margaretha Zelle, también conocida como Mata Hari, podía cruzar libremente las fronteras nacionales. Para evitar los campos de batalla, sus viajes a Francia los hacía a través de España y las islas británicas, y sus continuos desplazamientos llamaron la atención a más de uno. Mata Hari era una cortesana con buenas relaciones entre los oficiales aliados de más alto rango. En un interrogatorio realizado por oficiales de la inteligencia Británica (MI5), ella admitió que trabajaba como agente para el ejército francés, aunque más tarde no ratificó esta declaración. No está claro si Mata Hari mintió para parecer más misteriosa, o si realmente las autoridades francesas la tenían en nómina pero, si fuese este último el caso, nunca lo reconocerían.

[53]Ver http://www.elonka.com/UnsolvedCodes.html

En el mes de enero de 1917, el agregado militar alemán en Madrid mandó mensajes por radio a Berlín describiendo lo útiles que estaban resultado las actividades de un espía alemán con nombre en código H-21. Los servicios de inteligencia franceses interceptaron los mensajes y, de la información que contenían fueron capaces de identificar al agente H-21 con Mata Hari. Lo curioso es que tales mensajes se habían cifrado con un código que la inteligencia alemana sabía que ya había sido roto por los franceses. Esto hace pensar que los mensajes fueron concebidos de modo que, si ella era de hecho un agente francés, los alemanes lograrían así desenmascararla como un agente doble y conseguir neutralizarla.

El 13 de febrero de 1917, Mata Hari fue arrestada en la habitación de su hotel en París. Se la llevó ante los tribunales y fue acusada de espiar a favor de los alemanes y de, consecuentemente, causar la muerte a millares de soldados franceses. Se la declaró culpable de los cargos y fue fusilada el 15 de octubre de 1917, a los 41 años de edad. Hay teorías que apoyan la tesis de que los franceses utilizaron su procesamiento y ejecución para distraer la atención de otros hechos que ocurrían en el frente.

Es muy probable que Mata Hari no fuera un doble agente sino que, dado que era una cortesana, seguramente fuera utilizada como chivo expiatorio por parte del jefe del contraespionaje francés, Georges Ladoux, quien era el responsable de reclutar a Mata Hari como espía francés, y quien luego más tarde fue también arrestado por ser un agente doble. Los datos de este caso son bastantes vagos y habrá que esperar a que los documentos oficiales se desclasifiquen ya que estos fueron clasificados por un siglo, periodo que se cumple el próximo año 2017.

A principios del siglo XX, los cifrados de mas alta seguridad se hacían utilizando máquinas electromecánicas, por lo que la tarea de los criptoanalistas se volvió mucho mas ardua que en etapas anteriores. Varios de los grandes éxitos del criptoanálisis de la primera mitad del siglo XX vinieron de la mano de William Frederick Friedman (1891-1969), un criptólogo norteamericano que dirigió la división del Servicio de Inteligencia y Señales de la Amada norteamericana (*Signals Intelligence Service*) en la década de 1930, y que siguió en servicio hasta la década de los cincuenta. Al final de los años treinta, subordinados suyos dirigidos por Frank Rowlett consiguieron rompen el cifrado japonés PURPLE, lo que les permitió abrir los secretos diplomáticos japoneses durante la Segunda Guerra Mundial.

Durante la década de 1920 ganaron mucha popularidad una variada serie de máquinas de cifrar que eran, casi todas, eran el resultado de conectar un teletipo a un cierto circuito eléctrico sencillo. Un ejemplo pionero de estos artilugios es la Máquina de rotores de Hebern, diseñada en los EEUU

en 1915 y patentada[54] en 1919 por Edward Hebern. Este sistema ofrecía tal seguridad y su uso era tan sencillo que Hebern convenció a sus inversores de que pronto todas las compañías tendrían una de esas máquinas y las utilizarían profusamente. Sin embargo, su compañía quebró cuando terminó la primera guerra europea, y Hebern terminó en prisión acusado de manipulación del mercado bursátil.

Al igual que Hebern, Friedman también pensaba que las nuevas máquinas de rotor terminarían siendo importantes, y dedicó cierto tiempo a analizar la máquina de Hebern. Durante algunos años, Friedman concretó algunos principios de análisis, e identificó algunos problemas que son comunes en la mayoría de los diseños de máquinas basadas en rotores. Dentro del conjunto de características que resultan peligrosas están aquellos casos en los que los rotores que avanzan una posición con cada pulsación de tecla, es decir, el rotor más rápido, el que avanza con cada pulsación, se coloque en cualquier extremo de la serie de rotores. En este caso, si se consigue interceptar suficiente criptograma y aplicando un método estadístico estándar conocido como el test Kappa, o el Índice de Coincidencia, Friedman demostró que podía, con mucho trabajo, romper cualquier cifra generada por esa máquina.

Friedman utilizo su comprensión de las máquinas de rotores para desarrollar otras máquinas alternativas que eran inmunes a sus propios ataques. La mejor de todas fue la máquina SIGABA[55], que llegó a ser la máquina de cifrado de mas alta seguridad de los Estados Unidos durante la Segunda Guerra Mundial. Esta máquina fue inventada conjuntamente por Friedman y Frank Rowlett, el joven matemático contratado por Friedman que logró romper el cifrado PURPLE.

En la historia de la criptografía el **97-shiki obun inji-ki** (九七式欧文印字機) ("*Sistema 97 Máquina de Imprimir para Caracteres Europeos*", 1937) o **Angoki Taipu-B** (暗号機タイプB) ("*Máquina de Cifrado Tipo B*", 1937), con nombre en código PURPLE para los Estados Unidos, fue una máquina de cifrado para mensajes diplomáticos que utilizó el Ministerio de Asuntos Exteriores japonés durante la Segunda Guerra Mundial. La máquina se basaba en el uso de conmutadores por pasos como los utilizados por los antiguos teléfonos rotatorios. La información obtenida de su descifrado recibió el nombre en código Magic.

---

[54]Ese mismo año también presentaron sus patentes otros fabricantes como Arvid Gerhard Damm, Arthur Scherbius y Hugo Alexander Koch.

[55]También conocida como ECM Mark II o Converter M-134 por el ejército de los USA, o CSP-888/889 por la Armada, y una versión modificada se llamó CSP-2900. Es una máquina que utiliza un sistema electromecánico de rotores para cifrar y descifrar los mensajes.

El nombre en código PURPLE se refiere al color de las carpetas utilizadas por los criptoanalistas para guardar el material obtenido en sus análisis; había una máquina Red utilizada por el Ministerio de Asuntos Exteriores japonés, por lo que "Purple" era el siguiente color que en ese momento estaba disponible. Los japoneses también utilizaron otros sistemas anteriores como fueron Coral y Jade (en uso entre 1942 y 1944) pero PURPLE fue el sucesor y la mejora de ambas.

La nueva cifra demostró ser difícil de romper. La unidad criptológica de la Marina (OP-20-G) y el SIS pensaron que podía estar relacionada con máquinas japonesas anteriores por lo que el SIS decidió estudiarla. Después de varios meses buscando patrones en los criptogramas de PURPLE, un equipo del SIS, dirigido por Friedman y Rowlett, encontró el modo de reconstruir la máquina, lo cual supuso un hecho extraordinario. PURPLE, a diferencia de la máquina Enigma alemana o del diseño de Hebern, no utilizaba rotores, sino selectores por pasos como las que se utilizaban en las centralitas telefónicas electromecánicas conmutadas. Leo Rosen del SIS construyó una máquina y, como se descubrió posteriormente, utilizó un modelo de conmutador por pasos idéntico al que habían utilizado los japoneses. Así, a finales de 1940, el SIS había construido un ejemplar exacto de la máquina PURPLE sin haber visto nunca una de ellas.

Con las máquinas duplicadas y con la comprensión de su funcionamiento, el SIS pudo descifrar el cada vez mas intenso tráfico de señales japonés. Una de esas intercepciones fue el mensaje dirigido a la embajada japonesa en Washington, en el que se ordenaba al embajador (el 7 de diciembre de 1941) negociaciones con los EE. UU. El mensaje dio una clara indicación de que se quería impedir la guerra, y fue entregado en el Departamento de Estado de los EE. UU. sólo unas horas antes del ataque a Pearl Harbor.

En 1941 y debido a un ataque de nervios atribuido al agotamiento que le causó el trabajo contra la máquina PURPLE, Friedman fue hospitalizado. Mientras tanto, un equipo de cuatro hombres: Abraham Sinkov y Leo Rosen del SIS, y los tenientes Prescott Currier y Robert Weeks de la Armada norteamericana OP-20-G[56], visitaron las instalaciones británicas de la

[56]**OP-20-G** o "*Office of Chief Of Naval Operations (**OP**NAV), **20**th Division of the Office of Naval Communications, G Section / Communications Security*", fue el grupo de la armada norteamericana dedicado a la inteligencia, a las señales y al criptoanálisis durante la Segunda Guerra Mundial. Su misión era interceptar, descifrar, y analizar las comunicaciones navales de los barcos japoneses, alemanes e italinos. Además el OP-20-G también copiaba mensajes diplomáticos de muchos gobiernos extranjeros. El mayor esfuerzo de todas las secciones iba dirigido contra Japón e incluía romper el libro "Azul" de códigos navales inicialmente utilizado por los japoneses. Esto fue posible interceptando y localizando a los emisores en el Océano Pacífico, en el Atlántico y en los mismos EE. UU. Continentales, e interceptando también las actividades de una escuela japonesa para radio operadores de cifrado telegráfico situada en el propio Washington D.C.

"*Government Code and Cypher School*" en Bletchley Park. Los visitantes entregaron a los británicos una máquina PURPLE y, a cambio, recibieron detalles sobre el diseño de la máquina Enigma y de cómo los británicos la habían descifrado.

En aquel momento, cuatro años antes de que se terminase la guerra, norteamericanos y británicos ya conocían con detalle los artefactos que utilizaban sus enemigos para proteger sus comunicaciones mas sensibles. Sin duda, los aliados supieron encontrar los modos de determinar qué claves se estaban utilizando en cada momento y, con ello, escuchar lo que sus enemigos preparaban para luego sorprenderles. Esta secreta ventaja fue, para muchos, decisiva a la hora de cómo se resolvería la guerra. Lo que si es cierto es que alemanes y japoneses terminaron rindiéndose.

El cifrado perfecto

Gilbert Sandford Vernam (1890-1960) fue un ingeniero de los Laboratorios Bell de la AT&T quien, en 1917, inventó un cifrador en flujo y mas tarde fue co-inventor de lo que se conoce como cifrado *One-Time Pad*.

Vernam propuso un teletipo cifrador en el que una clave previamente preparada y mantenida en una cinta de papel, se combina carácter a carácter con el texto en claro que se quiere proteger, y así producir su correspondiente criptograma. Para descifrar ese criptograma es necesario utilizar exactamente la misma clave volviéndola a combinar, en sentido inverso, carácter a carácter, obteniéndose el texto en claro original. Más tarde, Vernam trabajó para la Postal Telegraph Co., y pasó a ser empleado de la Western Union cuando ésta adquirió la anterior en 1943. Sus últimos trabajos fueron sobre sistemas automáticos de interruptores para redes de teletipos.

La función de mezcla especificada por Vernam en la US Patent 1.310.719, concedida el 22 de Julio de 1919, es la operación binaria XOR, aplicada a los impulsos o bits individuales que se utilizan para codificar los caracteres del mensaje según el código Baudot de los teletipos. Como dijo la National Security Agency (NSA) norteamericana en su día, "*quizás esta sea una de las patentes mas importantes en la historia de la criptografía*"[57].

[57]Ver http://www.nsa.gov/publications/publi00017.pdf: "*In 1919 he was granted a patent, perhaps one of the most important in the history of cryptography*".

Poco después, Joseph Mauborgne, por aquel tiempo capitán de la US Army Signal Corps, propuso que, además, la cinta de papel con la clave contuviese información aleatoria. Las dos ideas, cuando se combinan, dan automáticamente lo que se conoce como cifrado *One-Time Pad*, aunque ninguno de ellos utilizó ese nombre. Este sistema fue patentado a mediados de la década de 1920.

En 1919 el Ministerio de Asuntos Exteriores de la Alemania de Weimar adoptó el uso manual del cifrado *One-Time Pad* para la protección de cierto tráfico. Como el problema era tener suficiente clave, ésta se proporcionaba a los agentes en forma de pequeños librillos u otros objetos diminutos fáciles de transportar y ocultar. En tales objetos se escribía cuidadosamente el material secreto y único que constituía la clave para una futura transmisión. El procedimiento más conveniente para asegurar el uso único y el secreto de la clave era, después de haber cifrado un mensaje, destruir la fuente quemándola. Durante la Guerra Fría, el KGB normalmente entregaba a sus agentes el material de clave impreso en finas hoja de papel que químicamente había sido transformado en nitrocelulosa, de modo que podían arder rápidamente sin dejar cenizas.

Claude Shannon trabajando también en los Laboratorios Bell probó, con sus trabajos durante la Segunda Guerra Mundial, que el cifrado *One-Time Pad* es irrompible. Estos resultados fueron publicados mas tarde, en octubre de 1949. Este fue el primer y único sistema de cifrado para el que existe tan poderosa prueba. El uso correcto del sistema OTP daría al traste con cualquier posible éxito criptoanalítico, por lo que el eterno antagonismo estaría resuelto a favor del secreto. Sin embargo, las cosas no son tan sencillas y, además, de la seguridad del sistema de cifrado, también hay que evaluar la seguridad del modo se usarlo, por lo que siempre hay sitio para la esperanza (criptoanalítica).

Telegramas cifrados e intercepciones inconfesables

Un ejemplo claro de cómo los sistemas cifrados pueden cambiar la historia lo tenemos en el denominado Telegrama de Zimmermann. Así se le llama a un telegrama codificado que fue enviado por el Secretario de Asuntos Exteriores del Imperio Germánico, Arthur Zimmermann, el 16 de enero de 1917, al embajador alemán en Méjico, Heinrich von Eckardt, a finales de la Primera Guerra Mundial.

Ese telegrama daba instrucciones al embajador para que se presentase ante el gobierno mejicano y le hiciese la propuesta de formar una alianza militar germano-mejicana contra los EE. UU. Si los mejicanos se decidían a apoyar a los alemanes en la guerra, a Méjico se le asignaría el territorio

"cedido" a los Estados Unidos de Norteamérica después de la Guerra USA-Méjico (New México, Texas, y Arizona). El mensaje fue interceptado y decodificado por los británicos y su contenido entregado a los americanos, lo que les sirvió de excusa para entrar en la guerra. El gobierno del presidente mejicano Venustiano Carranza estudió la posibilidad de retomar el mando de sus anteriores territorios y llego a la conclusión de que no sería posible o incluso deseable por varias razones. Carranza rechazó formalmente las propuestas de Zimmermann el 14 de abril, tiempo en el que los EE.UU. declararon la guerra a Alemania.

El telegrama fue interceptado a tiempo y fue descifrado en extensión suficiente como para hacerse una idea de lo que decía por los criptógrafos Nigel de Grey, William Montgomery y el Almirante William R. Hall de la unidad de Inteligencia Naval conocida como "Room 40"[58]. Esta lectura fue posible porque el código que utilizaba la Oficina de Asuntos Exteriores alemana había sido parcialmente criptoanalizado utilizando, entre otras técnicas, mensajes en claro capturados y un libro de códigos, de una versión anterior de esa cifra, a Wilhelm Wassmuss, diplomático alemán que actuaba en el Oriente medio, y al que también se le conoció como "*el Lawrence de Arabia alemán*" o "*Wassmuss de Persia*".

El gobierno británico, que quería mostrar a los norteamericanos el telegrama, se encontró ante un dilema: si utilizaban públicamente el telegrama, los alemanes sabrían que su código había sido roto; y si no lo hacían perdían una oportunidad de oro para arrastrar a los Estado Unidos a la guerra[59]. Había además otro problema: no podían, sin más, enseñarle el telegrama al gobierno de los Estados Unidos. Por su importancia, el mensaje fue enviado desde Berlín al embajador alemán en Washington, Johann von Bernstorff, para su ulterior transmisión al embajador alemán en México, von Eckardt, y esto se hizo por tres rutas distintas. Los británicos obtuvieron el telegrama por una de ellas. En aquellas fechas, los americanos habían dado gentilmente acceso a Alemania a su propio sistema de telégrafo diplomático como prueba de buena voluntad del presidente Woodrow Wilson y dentro de su iniciativa de paz.

---

[58]La **Room 40**, formalmente la **NID25** fue la habitación en el almirantazgo en donde se llevó a cabo, en un principio, el esfuerzo criptoanalítico británico durante la primera Guerra Mundial. Ver Patrick Beesly, "*Room 40: British Naval Intelligence, 1914-1918*". New York: Harcourt, Brace, Jovanovich, 1982 ISBN 0-15-178634-8.

[59]El telegrama fué enviado durante un tiempo en el que los sentimientos anti-alemanes en la población norteamericana eran especialmente altos debido a la muerte de 128 ciudadanos norteamericanos en barcos británicos hundidos por los ataques de submarinos alemanes.

Por su parte, los alemanes no tenían miedo de utilizarlo ya que sus mensajes estaban cifrados y porque, en aquellos tiempos, los Estados Unidos, por principios, no leían la correspondencia diplomática de otros países y, además, porque, a diferencia de Gran Bretaña, los norteamericanos no tenían ninguna capacidad criptoanalítica. El telegrama fue desde la embajada norteamericana en Berlín a Copenhague y luego a través de un cable submarino a los EEUU, pasando a través de Inglaterra, donde fue interceptado. Para los británicos, revelar la fuente del telegrama a los Estados Unidos sería como admitir que tenían pinchadas las líneas americanas de comunicación diplomática.

El telegrama hasta Washington fue cifrado utilizando el código 7500, un código nuevo y mas difícil que los anteriores. Sin embargo, la embajada en Méjico todavía no lo tenía por lo que la embajada alemana en Washington tuvo que recodificar y retransmitir el mensaje utilizando un código más antiguo, el 13040 o 13042, ambos bien conocidos por los interceptores británicos.

El gobierno británico imaginó que la embajada alemana en Washington enviaría el mensaje hacia la embajada en Méjico a través del sistema comercial de telégrafo y, por tanto, debería existir una copia del mismo en las oficinas del telégrafo público en Ciudad de Méjico. Si los británicos pudieran hacerse con una copia allí, podrían pasársela al gobierno de los Estados Unidos directamente, diciendo que la habían obtenido mediante espionaje en Méjico. Así pues, contactaron a uno de sus agentes en México, conocido como Mr. H., quien sobornó a un empleado del telégrafo para que le diese copia de dicho mensaje. En su autobiografía, Sir Thomas Hohler, el embajador británico en México en aquellos tiempos, dice haber sido él el agente Mr. H. Para mayor goce de los criptoanalistas británicos, el mensaje enviado desde Washington a México fue protegido con la misma cifra que aparecía en el libro de códigos de Wassmuss por lo que fue completamente descifrado.

El telegrama fue entregado al Ministro británico de Asuntos Exteriores, quien a su vez contactó con el embajador norteamericano en Inglaterra y le entregó el telegrama el 23 de febrero de 1917; dos días después estaba encima de la mesa del presidente norteamericano Woodrow Wilson y Estado Unidos entró en la Primera Guerra Mundial.

Inicialmente casi todo el mundo creyó que se trataba de una falsificación de los servicios de inteligencia británica para meter a América en la guerra dentro del bando aliado. Esta opinión, que no se limitaba a grupos pacifistas y pro-alemanes, fue reforzada por diplomáticos alemanes y mejicanos, y por algunos periódicos norteamericanos, especialmente los

del imperio mediático del magnate William Randolph Hearst. Como consecuencia de todo ello, el 29 de marzo de 1917, Arthur Zimmermann dio una rueda de prensa confirmando el texto del telegrama, y así cortó las especulaciones sobre su autenticidad.

En octubre de 2005, se publicó en la prensa que se había descubierto una transcripción mecanográfica genuina del descifrado original del telegrama de Zimmermann. Se cree que dicho documento es el que se le enseñó al embajador americano en Londres en 1917. Escrito a mano por el Almirante Hall en la parte superior del documento se puede leer: "*This is the one handed to Dr Page and exposed by the President*". Ya que muchos de los documentos secretos de este incidente diplomático fueron destruidos, se pensaba que el original del descifrado se había perdido para siempre.

Aunque los americanos no tenían mucha experiencia criptoanalítica a principios del siglo XX, pronto se pusieron manos a la obra; su primer gran éxito se produjo durante la Conferencia Naval de Washington. Este evento consintió en una conferencia diplomática organizada por la administración del presidente norteamericano Warren G. Harding que se celebró en Washington entre el 12 de noviembre de 1921 y el 6 de febrero de 1922. La conferencia se celebró bajo los auspicios de la Liga de las Naciones, y en ella participaron nueve países con intereses en el Océano Pacífico y el Este asiático; curiosamente, la Unión Soviética no fue invitada. Ésta fue la primera conferencia internacional desarrollada en territorio de los Estados Unidos y también fue la primera conferencia de la historia en donde se trató del desarme multilateral.

Las posturas americanas fueron predominantes todo el tiempo, entre otras cosas, porque interceptaban y descifraban las instrucciones secretas que daba el gobierno japonés a su delegación. Esos mensajes ponían de manifiesto cual sería la relación naval mínima que aceptaría Tokyo; y los negociadores norteamericanos utilizaron ese conocimiento para presionar a los japoneses y empujarlos hasta sus límites. Este éxito del gobierno de los EEUU fue uno de los primeros construido sobre sus esfuerzos criptológicos y de espionaje, y su consecuencia más directa fue la proliferación y mayor importancia de ese tipo de agencias dentro de la administración americana[60].

[60]Ver http://www.fas.org/irp/agency/inscom/trail.pdf

Herbert Osborne Yardley (1889-1958) fue un criptólogo americano conocido por ser el autor del libro "*The American Black Chamber*" publicado en 1931. El titulo de su libro se refiere a la organización criptográfica, el MI-8[61], que Yardley fundó y dirigió inmediatamente después de terminar la Primera Guerra Mundial. Bajo la dirección de Yardley, los criptoanalistas de la Black Chamber americana rompieron los códigos diplomáticos japoneses que se usaron en la Conferencia Naval de Washington. Más tarde, Yardley también ayudó a los nacionalistas chinos a romper los códigos de los japoneses, y trabajó brevemente para el gobierno canadiense ayudándoles a poner en pie una unidad criptológica.

En 1929, el Secretario de Estado de los Estados Unidos Henry L. Stimson[62] decide terminar con las actividades criptoanalíticas y cerrar la "Black Chamber" del Departamento de Estado diciendo que "*los caballeros no leen el correo de los demás" (Gentlemen do not read each other's mail*) aunque más tarde se retractó de esa opinión.

La máquina Enigma

Lo que comúnmente se conoce como La máquina Enigma fue un artefacto diseñado para el cifrado y descifrado de mensajes secretos. Más correctamente, Enigma fue una familia de máquinas electromecánicas de rotores que están íntimamente relacionadas entre sí, y que se concretaban en una cierta variedad de modelos diferentes.

---

[61]El MI-8 fue disfrazado de compañía comercial, con sede en Nueva York, que se dedicaba a producir y vencer códigos y cifras para usuarios del mundo empresarial y de los negocios; sin embargo, estaba financiada conjuntamente por el ejército y el Departamento de Estado de los EE. UU. y su verdadera misión era poner en claro las comunicaciones secretas, principalmente diplomáticas, de otras naciones.

[62]**Henry Lewis Stimson** (1867-1950) era un político americano que fue Secretario de Guerra, Gobernador General de las Filipinas, y Secretario de Estado. Era conservador republicano, y un abogado muy conocido de la ciudad de Nueva York. Su fama se debe principalmente a haber sido Secretario de Guerra, teniendo bajo su control el ejército y las fuerzas aéreas, durante la Segunda Guerra Mundial, y fue elegido para dicho cargo por su actitud agresiva frente a la Alemania Nazi. Se las arregló para reunir y entrenar a doce millones de soldados y pilotos, para comprar y llevar a los campos de batalla el 30 % de la producción nacional así como para construir y luego utilizar la bomba atómica.

Las máquinas Enigma fueron utilizadas comercialmente desde principios de la década de 1920 y, a partir de entonces, también fueron utilizadas por servicios gubernamentales y militares de algunas naciones, siendo el caso más famoso el de la Alemania Nazi de antes y durante la Segunda Guerra Mundial. El modelo militar alemán, la Wehrmacht Enigma, es a la que comúnmente se refieren las citas cuando se limitan a mencionar el nombre de Enigma.

La máquina tiene mucha notoriedad porque los criptólogos de los Aliados fueron capaces de descifrar un gran número de mensajes generados con ese modelo de máquina. El descifrado fue posible gracias a los trabajos llevados a cabo en 1932 por los criptógrafos Marian Rejewski, Jerzy Rózycki y Henryk Zygalski en el denominado "Cipher Bureau"[63] (Biuro Szyfrów) polaco. A mediados de 1939 los métodos de reconstrucción de la máquina y los de descifrado fueron entregados por Polonia a Inglaterra y Francia. La información obtenida a través de esta fuente, con nombre en código ULTRA, fue una ayuda muy significativa para el bando aliado durante toda la guerra.

Aunque el cifrado Enigma presentaba algunas debilidades criptográficas, en la práctica fue su combinación con otros factores importantes tales como los errores de los operadores, errores de procedimiento, y máquinas o libros de códigos ocasionalmente capturados, lo que hizo realmente posible que los Aliados fuesen capaces de descifrar las comunicaciones Enigma.

La guerra en el Pacífico

Durante la Segunda Guerra Mundial, la Armada japonesa utilizó varios códigos y cifras, algunos más efectivos que otros. El más y mejor conocido era el denominado JN-25, cuyo criptoanálisis permitió a los americanos la victoria en Midway.

JN-25 es el nombre dado por los criptoanalistas al esquema de comunicación de mando y control más seguro que utilizaba la Armada Imperial Japonesa durante la Segunda Guerra Mundial, y su referencia numérica se debe a que era el vigésimo quinto sistema naval japonés identificado. Se trataba

[63]El Gabinete de Cifra polaco tuvo éxitos notables frente a la criptografía soviética durante la Guerra Polaco-Soviética de 1919 a 1921, lo que ayudó así a mantener la independencia polaca que se había conseguido como consecuencia de la Primera Guerra Mundial. A principios de diciembre de 1932, esta unidad fue capaz de romper el cifrado Enigma alemán de entonces y también de superar las cada vez mas complejas estructuras y operaciones de las versiones dotadas de panel de permutación (*plugboard*) de las nuevas máquinas Enigma, que serían las mas utilizadas por Alemania durante la inminente guerra mundial.

de un código de cifrado, que producía tráficos radiotransmitidos de grupos de cinco números. Fue frecuentemente revisado a lo largo de su vida activa, y cada nueva versión requería un criptoanálisis prácticamente *ad initio*. Cada cierto tiempo se introducían nuevos libros de códigos y también se renovaban los libros de supercifrado, algunas veces de forma simultánea. En particular, el JN-25 fue cambiado, curiosamente, antes del ataque a Pearl Harbor, el primer día de diciembre de 1941. Esa misma fue la versión del código JN-25 que estaba suficientemente rota a finales de mayo de 1942 como para poner en alerta a los EE.UU. y facilitar así su victoria en la batalla de Midway.

Los británicos, australianos, holandeses y americanos cooperaron para atacar el código JN-25, y empezaron justo después del ataque a Pearl Harbor. La armada japonesa no volvió a entrar en batalla hasta finales de 1941, por lo que hubo poco tráfico con el que trabajar. Las discusiones y órdenes internas de la Armada japonesa generalmente viajaban por rutas más seguras que la radio, como son los mensajeros o la entrega directa mediante naves de la misma Armada. Aunque hay abierta discrepancia entre distintos autores, el grado de éxito en el criptoanálisis del código JN-25 utilizado justo antes de diciembre de 1941 no era superior a un 10% en el momento del ataque. El tráfico JN-25 aumentó inmediatamente después del inicio de la guerra naval a finales de 1941 y proporcionó la información criptográfica necesaria para llegar a tener éxito en la descodificación, tanto de la versión en uso como de las que siguieron, del código denominado JN-25.

El esfuerzo norteamericano estaba dirigido desde Washington por el Comando de Señales e Inteligencia de la Armada, llamado OP-20-G. Su sede estaba en Pearl Harbor, en las instalaciones de la Unidad de Inteligencia de Combate de la Armada (Estation HYPO). Con el apoyo de la estación de escucha CAST situada en las Filipinas, y con la ayuda de los británicos de Hong Kong y luego de Singapur, se montó un ataque a la edición del código JN-25 que entró en servicio el 1 de diciembre de 1941 que tuvo un gran éxito. Todos juntos hicieron progresos importantes hasta principios de 1942 y para ello utilizaron lo que llamaron "chuletas" (cribs), en el sentido académico de tal término, y que no eran sino pares conocidos de texto en claro y su correspondiente criptograma. Gracias a las formalidades muy frecuentes en los mensajes japoneses, tales como *"Tengo el honor de informar a su Excelencia…"* además del uso de títulos formalizados y con estilo bien conocido, era posible imaginar que ciertos tipos de textos estaban presentes en determinadas posiciones del mensaje, saludos al principio y despedidas al final, etc., y así probar con un par texto en claro - criptograma. Este es el método criptográfico clásico conocido como de *palabra probable*.

Hay que recordar que la ruptura de la cifra PURPLE (también llamada AN-1) en 1940 no había permitido conocer nada de las comunicaciones militares. La cifra Purple era utilizada por el Ministerio de Asuntos Exteriores para sus comunicaciones diplomáticas más seguras, y no tenía ninguna relación criptográfica con ninguna versión del código militar JN-25, ni con ningún otro sistema de cifrado del ejercito japonés durante la guerra del Pacífico. En la época de la entrada en guerra, el ejército nipón no se fiaba suficientemente de su propio Foreign Office como para hablarles de sus códigos. El tráfico JN-25 estaba limitado a comunicaciones militares, principalmente operacionales, de las que el enemigo o cualquier otro podrían inferir informaciones estratégicas o tácticas.

El 18 de abril de 1943 y para elevar la moral de sus tropas después de la derrota de Guadalcanal, el Almirante de la flota nipona Isoroku Yamamoto decidió hacer una inspección a lo largo del Pacífico Sur. El 14 de abril de ese año, los criptoanalistas de la Inteligencia Naval norteamericana, con nombre de código "Magic", interceptaron y descifraron un mensaje en el que se daban detalles muy concretos y precisos del viaje que habría de realizar el Almirante de la Flota Imperial, Yamamoto. En tal mensaje se incluían los tiempos de salida y llegada y los puntos que iba a visitar, así como los números y tipos de aviones que le iban a transportar y acompañar en su periplo. Yamamoto, según el itinerario revelado, volaría desde Rabaul a Ballalae Airfield, en una isla próxima a Bougainville en las Islas Salomon, en la mañana del 18 de abril de 1943.

El presidente Franklin D. Roosevelt pidió a Frank Knox, Secretario de la Armada, "Get Yamamoto". Knox informó de ello al Almirante Chester W. Nimitz y éste consultó con el Almirante William F. Halsey, Jr., comandante del Pacífico Sur, y luego autorizó una misión para que el 17 de abril se interceptase y derribase el vuelo en el que iba el almirante Yamamoto. Se asignó la misión al 339th Fighter Squadron de la fuerza aérea dado que sus aviones P-38 Lightning poseían la autonomía de vuelo necesaria para la intercepción y captura. A los pilotos se les dijo que iban a interceptar a un "oficial importante" pero realmente desconocían quien era su objetivo.

En la mañana del 18 de abril, a pesar de las advertencias del comandante local de cancelar el viaje por miedo a que se tratase de una emboscada, los aviones de Yamamoto abandonaron Rabaul e iniciaron su viaje de 500 kms. Poco después, dieciocho aviones P-38s específicamente acondicionados despegaron de Guadalcanal. Durante los 740 km que les separaban del punto de encuentro, los aviones mantuvieron silencio absoluto en cuanto a las transmisiones por radio se refiere. A las 09:34 horas de Tokio, ambos contendientes se encontraron y comenzaron una clásica "pelea de perros"

(*dogfight*[64]) entre los P-38s y lo seis Zeros que escoltaban a Yamamoto. El teniente de primera Rex T. Barber se encargó de los primeros bombarderos japoneses, y uno de ellos resultó ser el avión de Yamamoto. El teniente roció el avión con fuego de ametralladora hasta que empezó a salir humo de su motor izquierdo. Barber volvió para atacar a otros bombarderos mientras el de Yamamoto se estrellaba en la jungla.

Una expedición japonesa de rescate encontró el cuerpo de Yamamoto y lo llevó a la base del ejército japonés localizada en Buin[65], donde se le realizó la autopsia el 20 de abril, y luego, inmediatamente después, fue incinerado con su uniforme puesto para intentar así mantener su muerte en secreto.

Sus cenizas fueron transportadas en un bombardero desde Buin a Rabaul, y de allí a Japón sobre el barco de guerra Musashi, el último buque insignia de Yamamoto. Al almirante se le dió un funeral de estado el 3 de junio de 1943, donde recibió, a título póstumo, el título de Almirante de la flota y le otorgaron la condecoración de la Orden del Crisantemo de primera clase. También fue condecorado con la Cruz de Caballero[66] de la Cruz de Hierro de la Alemania Nazi con hojas de roble y espadas. Una parte de sus cenizas fueron enterradas en el cementerio público de Tama, Tokio (多摩霊園), y el resto en la tierra de sus ancestros en el templo de Chuko-ji en la ciudad de Nagaoka.

La expedición japonesa de búsqueda y rescate, dirigida por el ingeniero del ejército teniente Hamasuna, declaró que Yamamoto había salido disparado del avión en el choque, y que su mano enguantada todavía agarraba la empuñadura de su katana; encontraron el cuerpo en posición de sentado y bajo un árbol. Hamasuna explicó que Yamamoto estaba totalmente reconocible, y que tenía la cabeza hacia delante como si estuviese absorto en una profunda meditación. La autopsia del cuerpo desveló que Yamamoto había recibido dos impactos de bala, uno en la

---

[64]En inglés se utiliza la palabra **dogfight** para describir un combate aéreo entre aviones de caza (fighter planes) y ello quizás se deba a las piruetas que, en esos casos, hacen en el aire los aviones y que recuerda a una pelea entre perros.

[65]**Buin** estaba situada en el territorio de Nueva Guinea, en las coordenadas 6° 49' 60S - 155° 43' 60E y era una base ubicada tierra adentro, siendo Kangu beach la posición en la costa mas cercana (12 km hacia el sur).

[66]La **Knight's Cross de la Cruz de Hierro** (en aleman: *Ritterkreuz des Eisernen Kreuzes*, a menudo simplemente Ritterkreuz) fue una Orden de la Alemania Nazi y reconocía la bravura extrema en el campo de batalla o un liderazgo militar exitoso durante el periodo del Tercer Reich.

parte trasera de su hombro izquierdo y otro que entró por la parte izquierda de su mandíbula inferior y salió por encima de su ojo derecho. Este hecho elevó la moral de los Estados Unidos de Norteamérica ya que supuso un mazazo sobre la moral nipona, quienes no tuvieron información oficial del hecho hasta el día 21 de mayo de 1943.

Para disimular el hecho de que los americanos estaban leyendo los códigos japoneses, a las agencias de noticias americanas se les dijo que unos guardacostas civiles en las Islas Salomón vieron a Yamamoto subiéndose a un bombardero en esa área. Tampoco dieron publicidad a los nombres de los pilotos que atacaron el avión de Yamamoto porque uno de ellos tenía un hermano que, en aquellos momentos, era prisionero de los japoneses y el ejército americano temía por su futuro e integridad.

Máquinas para el criptoanálisis

En el mes de abril de 1943 Max Newman, Charles Wynn-Williams y su equipo, que incluía a Alan Turing, trabajando en Bletchley Park completaron el diseño y la fabricación de lo que dieron en llamar *Heath Robinson*[67], que fue el primer intento de utilizar una máquina automática de propósito específico para ayudar en la ruptura del teletipo cifrado alemán conocido como Lorenz y que se encargaba de proteger todo el tráfico alemán de teletipos durante la Segunda Guerra Mundial. La idea de intentar construir la máquina fue de Max Newman y fue diseñada en el Servicio de Investigación en Telecomunicaciones (*Telecommunications Research Establishment TRE*) por C. E. Wynn-Williams, que también había estado involucrado en Bletchley Park en el diseño de una "Bomba" de alta velocidad para romper el tráfico de la máquina Enigma de la Armada alemana. Aunque no han sobrevivido fotografías de ninguna de aquellas máquinas y solo se disponen algunos diagramas y datos fragmentarios, Tony Saler, en el año 2001, comenzó la reconstrucción de esa máquina pionera del criptoanálisis.

En realidad se trata de una máquina experimental con fines específicos que perseguía poder comparar opto-mecánicamente el contenido de dos cintas perforadas de papel; el problema estaba en mantener su sincronización a velocidades de 1000 caracteres por segundo. Una de las cintas contenía el mensaje cifrado, y la otra representaba las secuencias cifrantes producidas por los rotores de la máquina de Lorenz.

[67]Ver http://www.codesandciphers.org.uk/virtualbp/hrob/hrrbld.pdf

A esta primera máquina se la llamó "*Heath Robinson*" por el dibujante (1872-1944) de comics que dibujaba máquinas fantásticas, y cuyo nombre ha quedado en la lengua inglesa como equivalente a cualquier descripción de complejidad innecesaria y de concepción inverosímil. Rube Goldberg (1883-1970) fue el homólogo americano del Robinson británico.

Análogamente, las máquinas Colossus fueron artefactos con cierta capacidad computacional que utilizaron los criptógrafos británicos para leer los mensajes cifrados alemanes durante la Segunda Guerra Mundial. Colossus fue diseñado por el ingeniero Tommy Flowers en la *Post Office Research Station*[68], ubicada en la barriada de Dollis Hill de Londres, con datos e informaciones proporcionadas por el matemático Max Newman y su grupo de Bletchley Park. El prototipo, Colossus Mark I, demostró su correcto funcionamiento en diciembre de 1943 y se puso en producción en Bletchley Park en febrero de 1944. Una versión mejorada, el Colossus Mark II, se instaló por primera vez en junio de 1944, conteniendo modificaciones de Allen Coombs. Al final de la guerra se habían construido diez Colossus.

Los ordenadores Colossus se utilizaron en el criptoanálisis de las comunicaciones alemanas de alto nivel, consistentes en mensajes que habían sido cifrados utilizando la máquina Lorenz SZ 40/42. Un objetivo primordial de las máquinas Colossus era el de poder emular la máquina mecánica Lorenz de forma electrónica. Para cifrar un mensaje, el texto en claro se combina con los bits de una clave, agrupados en grupos de cinco. Ese flujo de secuencia cifrante era generado utilizando doce rotores: a cinco de ellos los británicos los llamaron rotores χ ("chi"), y a otros cinco, rotores ψ ("psi"), y a los dos restantes los llamaron "*motor wheels*". Los rotores χ avanzaban regularmente con cada letra que se cifraba, mientras que los rotores ψ avanzaban irregularmente, bajo el control de los rotores motrices (*motor wheels*).

[68]El laboratorio de investigación del sistema postal británico, (*Post Office Research Station*) estaba ubicado en el barrio de Dollis Hill, al noroeste de Londres. Se estableció allí en 1931 y fue inagurado por el primer ministro Ramsay MacDonald en 1933. En 1943 se construyó el primer ordenador específico del mundo, el Colossus, bajo los diseños del equipo de Tommy Flowers. También en este laboratorio se construyó, en 1957, ERNIE (*Electronic Random Number Indicator Equipment*) para la lotería gubernamental *Premium Bond*, por el equipo dirigido por Sidney Broadhurst. En 1971, Samuel Fedida concivió el teletexto o Minitel conocido como Viewdata y el servico Prestel (*Press Telephone*) que lanzó en 1979. En 1968, se anunció que la estación se reubicaría en un nuevo centro que habría de construirse en Martlesham Heath. Formalmente se inaguró el 21 de noviembre de 1975 por la reina Elizabeth II y hoy el laboratorio se conoce como Adastral Park. En la sede abandonada se construyó Paddock, una especie de museo que consta de dos plantas y donde se exhibe de forma permanente elementos de la Segunda Guerra Mundial.

Bill Tutte, un criptoanalista que trabajaba en Bletchley Park, descubrió que el flujo de secuencia cifrante producido por la máquina mostraba sesgos estadísticos que la distinguían de las secuencias al azar, y que esos sesgos podían ser utilizados para romper la cifra y leer los mensajes. Con el fin de leer los mensajes había que realizar dos tareas: la primera era la de *wheel breaking*, que consistía en descubrir el conexionado (permutaciones) de todos los rotores. Esos patrones se instalaban una vez y luego eran utilizados por un periodo de tiempo fijo y para un número definido de mensajes. La segunda tarea era el *wheel setting*, que se iniciaba cuando ya se conocían el contenido y posición de los rotores. Cada mensaje cifrado con una máquina Lorenz se cifraba empezando desde una posición diferente de los rotores. El proceso de ajuste inicial de los rotores (*wheel setting*) encontraba la posición de partida para cada mensaje. Inicialmente Colossus fue utilizado para ayudar con el ajuste inicial de los rotores, pero más tarde se observó que también podía adaptarse para el proceso de descubrimiento del conexionado de los rotores (*wheel breaking*).

Colossus fue desarrollado después del proyecto *Heath Robinson* ya que éste tenía problemas de sincronización entre sus dos cintas perforadas de entrada, lo cual limitaba seriamente la velocidad del proceso a menos de un millar de caracteres por segundo. Colossus resolvió este problema reproduciendo una de las cintas electrónicamente, eliminando así los problemas de sincronía; la otra cinta podía ser leída por Colossus a mayores velocidades.

Las máquinas Colossus se utilizaron en Bletchley Park durante toda la Segunda Guerra Mundial y, aunque se construyeron diez ejemplares de ella, todas fueron destruidas nada más terminar las necesidades para las que habían sido creadas; en aquellos momentos las Colossus eran consideradas una máquinas tan avanzadas, que era necesario asegurar que sus diseños no terminasen en manos enemigas.

Sin embargo, en 1996 se construyó una réplica perfectamente operativa de un Colossus Mark II por el equipo dirigido por Tony Sale y el resultado de sus esfuerzos se puede ver en el Bletchley Park Museum en Milton Keynes, Buckinghamshire. Una de las razones de reconstruir un Colossus operativo en 1996 era para desmontar el mito americano de que el ENIAC (1946) había sido el primer calculador digital a gran escala de la historia. No fue así, pero el mito se creó porque Colossus (1944) fue mantenido en secreto hasta la década de 1970.

En 1944 se patentó y mantuvo en secreto hasta 2001, la máquina de cifrar ECM Mark II, también conocida como SIGABA o Converter M-134, que era una máquina de rotores utilizada por los Estados Unidos desde

finales de la Segunda Guerra Mundial hasta el final de la década de 1950. Como muchas otras máquinas de entonces, utilizaba un sistema electromecánico de rotores para cifrar los mensajes. Se desconocen los resultados de esta máquina durante su periodo de servicio.

SIGABA era similar a Enigma en sus aspectos más fundamentales y básicos, ya que utilizaba una serie de rotores para cifrar cada carácter del texto en claro y producir un carácter diferente del criptograma. A diferencia de Enigma que utilizaba tres o cuatro rotores, SIGABA incluía quince, y no utilizaba reflector como si hacía Enigma. La máquina tenía tres bancos de rotores con cinco ejemplares cada uno; la señal de avance de dos de los bancos estaba controlada por el resultado del tercero. SIGABA avanzaba uno o más de un paso sus rotores principales en un modo complejo y pseudoaleatorio.

En cuanto a los inconvenientes, podemos comentar que la máquina SIGABA era grande, pesada, cara, difícil de operar, mecánicamente compleja y frágil. No se parecía en nada a un dispositivo práctico como Enigma, que era más pequeño y ligero que las radios con las que se iba a utilizar. SIGABA fue utilizada en las salas de radio de los barcos de la Armada norteamericana pero no podía ser utilizada en el campo de batalla. Por tanto, en circunstancias y escenarios bélicos se utilizaban máquinas menos seguras pero más ligeras como, por ejemplo, la conocida como M-209. La máquina SIGABA se reservó para las comunicaciones tácticas.

La guerra fría y el proyecto Venona

El proyecto Venona[69] es una larga y secretísima colaboración de las agencias de inteligencia de los Estado Unidos e Inglaterra dedicadas al criptoanálisis de los mensajes enviados por diferentes agencias de la Unión Soviética, principalmente durante la Segunda Guerra Mundial.

En los primeros años de la Guerra Fría, Venona sería una fuente importante de información sobre las actividades de inteligencia de la Unión Soviética en el suelo de las potencias occidentales. Aunque desconocido para el público, e incluso para los presidentes Franklin D. Roosevelt y Harry Truman, Venona fue un programa crítico y bien protegido, que está detrás de varios famosos sucesos del principio de la Guerra Fría, tales como en el Caso Rosenberg y las deserciones de Donald Maclean y Guy Burgess. La

[69]Se sabe que hubo al menos trece nombres distintos para este esfuerzo conjunto US-UK. "Venona" fue el último utilizado. Esta elección no tiene significado conocido. En los documentos desclasificados de la NSA, "VENONA" está escrito en mayúsculas.

mayoría de los mensajes que después pudieron ser descifrados fueron interceptados ente los años 1942 y 1945, y descifrados a principios de 1946; sin embargo, el proyecto continuó vivo hasta 1980, cuando fue cancelado bajo la administración de Jimmy Carter.

El proyecto Venona se inició en el año 1943, bajo las órdenes del Jefe de Inteligencia Militar norteamericana (G-2) Carter W. Clarke. Clarke desconfiaba de Joseph Stalin (1922-1953), y temió que la Unión Soviética pudiese firmar otro acuerdo de paz con el Tercer Reich, desactivando el frente ruso y permitiendo a Alemania centrar sus fuerzas militares en la guerra contra Gran Bretaña y los Estados Unidos. Criptoanalistas del *Signal Intelligence Service* (también conocido como Arlington Hall) del ejército americano analizaron mensajes diplomáticos de alto nivel que circulaban cifrados y que interceptaban en grandes cantidades durante e inmediatamente después de terminada la guerra, mediante puestos de radioescucha americanos, británicos y australianos.

Este tráfico, que en parte estaba cifrado con el sistema *One-Time Pa*d, fue almacenado y analizado en relativo secreto por cientos de criptoanalistas a lo largo de un periodo de cuarenta años que empezó a principios de la década de 1940. Debido a un enorme error de cáculo, los soviéticos reutilizaron las mismas páginas de una misma clave en diferentes ediciones de los *One-Time Pad* que, posteriormente, fueron utilizadas para el envío de otros mensajes. Esta reutilización de la misma clave hizo que ese tráfico fuera vulnerable al criptoanálisis de los americanos.

Los sistemas soviéticos, en general, utilizaban un código para convertir palabras y letras en números, a los que se sumaban las claves procedentes de los *One-Time Pads*, y del resultado de la suma obtenían el correspondiente criptograma. Cuando se utiliza correctamente, el cifrado *One-Time Pad* ya hemos mencionado que es teóricamente irrompible, por lo que el éxito del proyecto Venona hubiese sido nulo. Sin embargo, el criptoanálisis de americanos y británicos puso de manifiesto que algunos de los paquetes de clave, los *One-Time Pads* físicos, habían sido incorrectamente usados por los soviéticos para el cifrado de dos mensajes diferentes; concretamente, se trataba de páginas enteras pero no de libros de clave OTP completos. Este hecho permitió muchas veces el descifrado parcial de mensajes, y en algunas ocasiones el descifrado total de los mismos, siendo este el caso sólo para una pequeña fracción del tráfico interceptado.

La generación de *One-Time Pads* era un proceso laborioso, y el estallido de la guerra con los alemanes en junio de 1941 causó un repentino aumento de la demanda de material de claves para la transmisión de mensajes cifrados. Es probable que los generadores soviéticos de código duplicasen ciertas páginas de las cifras para poder atender a la demanda.

Fue en Arlington Hall donde el teniente Richard Hallock, que trabajaba en el tráfico comercial soviético, fue el primero en descubrir que los soviéticos estaban reutilizando páginas de OTP. Hallock y sus colegas lograron romper una cantidad significativa del tráfico comercial, recuperando varias tablas *One-Time Pad* en el proceso. Luego un joven Meredith Gardner, trabajando en lo que terminaría siendo la National Security Agency (NSA), utilizó ese material para romper lo que resulto ser trafico del NKVD[70], y más tarde del GRU[71], por reconstrucción el código que utilizaban para convertir el texto en números.

El 2º de diciembre de 1946, Gardner consiguió su primer éxito al romper el código, revelando la existencia de espionaje soviético dentro del Proyecto Manhattan[72], proyecto que desarrolló la bomba atómica. Otros descifrados indicaron que también había espías soviéticos en Washington, en el Departamento de Estado, en el Tesoro, en la Oficina de Servicios Estratégicos, e incluso dentro de la Casa Blanca. Muy lentamente y utilizando un surtido conjunto de técnicas que van desde el análisis de tráfico hasta la información aportada por desertores, se fueron descifrando más y más mensajes.

Una ayuda importante en las primeras etapas, según mencionó la NSA, puede haber sido el trabajo de cooperación llevado a cabo entre las agencias de inteligencia japonesas y finlandesa contra las cifras rusas durante la guerra del Pacífico; dado que los americanos rompieron los códigos que los japoneses utilizaban en ese tiempo, la intercepción que hicieron de las comunicaciones japonesas también les pudo dar acceso a la información intercambiada entre japoneses y fineses sobre los rusos. También hay informes que hablan de lo útil que fueron en el criptoanálisis las copias de algunos mensajes robados de oficinas soviéticas por el FBI.

---

[70]El **NKVD** (en ruso: **нквд**, Народный комиссариат внутренних дел , *Narodniy komissariat vnutrennikh del*) o **Comisariado Popular de Asuntos Exteriores** fue la policia secreta de la Unión Soviética responsable de las represiones políticas durante el Estalinismo.

[71]**GRU** es la transliteración del acrónimo ruso **ГРУ** que se refiere a "Гла́вное Разве́дывательное Управле́ние" (*Glavnoje Razvedyvatel'noje Upravlenije*), significando **Directorado Principal de Inteligencia** del General Staff of the Armed Forces of the Russian Federation. El nombre completo es GRU GSh: GRU "Generalnovo Shtaba" o "GenShtaba"), es decir, GRU "del Estado General"). El GRU es la agencia de inteligencia más grande de Rusia y tiene desplegados seis veces mas agentes en países extranjeros que la SVR que es la heredera del KGB, y contaba con 25.000 soldados de operaciones especiales (spetsnaz) en el año 1997.

[72]Ver Daniel Patrick Moynihan, Chairman (1997). **Report of the Commission On Protecting And Reducing Government Secrecy; Appendix A: The Experience of The Bomb**. United States Government Printing Office. (http://www.fas.org/sgp/library/moynihan/appa6.html)

La NSA informó que, de acuerdo con los números de serie de los cables Venona, se enviaron millares, pero que sólo una fracción de ellos estaba disponible para su criptoanálisis. Aproximadamente, 2.200 de los mensajes interceptados fueron descifrados y traducidos; un 50 % de los mensajes del año 1943 enviados entre el GRU-Naval en Washington y Moscú fueron rotos, pero desgraciadamente ningún otro cable de ningún otro año pudo romperse aunque se enviaron varios millares entre 1941 y 1945. Todas las claves OTP duplicadas se produjeron en el año 1942, y casi todas ellas habían sido ya utilizadas al final de 1945, quedando sólo algunas sueltas para ser utilizadas más tarde, llegando incluso hasta el año 1948. Después de este punto, el tráfico de mensajería soviética se volvió completamente impenetrable[73].

La existencia del proyecto Venona y de sus descifrados fue conocida por los soviéticos en los primeros años de las intercepciones. No está claro cuándo se enteraron del mismo, ni cuánto tráfico había sido interceptado hasta entonces, ni si había sido realmente descifrado pero, al menos un agente soviético infiltrado en el Secret Intelligence Service británico como representante de los EEUU, Kim Philby, supo de la existencia del proyecto Venona en 1949; Philby era el enlace entre las inteligencias británica y norteamericana. Dado que cuando se enteraron los soviéticos todas las páginas de claves duplicadas habían sido utilizadas, estos entonces optaron aparentemente por no hacer ningún cambio en sus procedimientos criptográficos a pesar de la existencia de Venona. Sin embargo, ya era tarde para alertar a aquellos de sus agentes que podrían estar en riesgo de quedar al descubierto debido a los descifrados en curso.

Los mensajes descifrados por Venona dejaron a la vista detalles sobre el comportamiento soviético durante el tiempo de las páginas de clave duplicadas. Con el primer éxito, Venona reveló la existencia de una red de espionaje soviético[74] en los laboratorios nucleares de Los Álamos[75]. Pronto surgieron las identidades de los espías americanos, canadienses, australianos y británicos al servicio del gobierno soviético, incluyendo las de Klaus Fuchs, Alan Nunn May y Donald Maclean, miembro del círculo de

[73]Ver Haynes, John Earl y Klehr, Harvey (2000). ***Venona: Decoding Soviet Espionage in America***. Yale University Press, pg. 55. ISBN 0-300-08462-5.

[74]Moynihan, Daniel Patrick (1998). Secrecy: The American Experience. Yale University Press, pg. 54 ISBN 0-300-08079-4. "*these intercepts provided...descriptions of the activities of precisely the same Soviet spies who were named by defecting Soviet agents Alexander Orlov, Walter Krivitsky, Whittaker Chambers and Elizabeth Bentley*".

[75]Commission on Protecting and Reducing Government Secrecy. *A Brief Account of the American Experience. Report of the Commission on Protecting and Reducing Government Secrecy. VI; Appendix* A pg. A-27. U.S. Government Printing Office. "*Thanks to successful*

espías conocido como los Cinco de Cambridge[76]. Otros espías trabajaban en Washington en el Departamento de Estado, en el Tesoro, en la Oficina de servicios Estratégicos[77], e incluso en la propia Casa Blanca.

Los descifrados mostraron que los EEUU y otras naciones occidentales fueron objetivo de grandes campañas de espionaje por parte de la Unión Soviética desde el año 1942. Entre los identificados como agentes estaban Julius and Ethel Rosenberg, Alger Hiss, Harry Dexter White, segundo oficial de más alto rango en el Departamento del Tesoro, Lauchlin Currie[78], ayudante personal del presidente Franklin Roosevelt; y Maurice Halperin, jefe de sección en la Oficina de Servicios Estratégicos (OSS).

La identificación de los individuos mencionados en las transcripciones Venona algunas veces es problemática ya que gente con una "relación encubierta" con la inteligencia soviética siempre aparece mencionada por su nombre en código. Para mayor complejidad, a veces la misma persona tiene varios nombres en código que se usan en momentos diferentes, o hay también casos en los que el mismo nombre en código es reutilizado para referirse a individuos diferentes. En algunos casos, especialmente el de Alger Hiss, establecer la relación de una persona concreta con un nombre en código Venona es muy discutido. En otros casos, hay muchos nombres

---

espionage, the Russians tested their first atom bomb in August 1949, just four years after the first American test. As will be discussed, we had learned of the Los Alamos spies in December 1946-December 20, to be precise. The U.S. Army Security Agency, in the person of Meredith Knox Gardner, a genius in his own right, had broken one of what it termed the Venona messages-the transmissions that Soviet agents in the United States sent to and received from Moscow."

[76]Los **Cinco de Cambridge** (también conocidos a veces como los **Cuatro de Cambridge**) era un anillo de espías soviéticos que operaba en el Reino Unido y que se dedicaba a pasar información a la Unión Soviética durante la Segunda Guerra Mundial y durante la década de 1950. Se ha sugerido que también podrían haber pasado desinformación soviética a los Nazis. El anillo estaba compuesto por Kim Philby (críptónimo: Stanley), Donald Duart Maclean (criptónimo: Homer), Guy Burgess (criptónimo: Hicks) y Anthony Blunt (criptónimo: Johnson).

[Un nombre en código o un **criptónimo** es una palabra o nombre utilizado clandestinamente para referirse a otro nombre o palabra. Los nombres en código son de uso frecuente en entornos militares y de espionaje. Tambien pueden ser utilizados en la industria para proteger proyectos secretos y cosas así de la competencia.]

[77]*Report of the Commission on Protecting and Reducing Government Secrecy. VI; Appendix* A pg. A-7. U.S. Government Printing Office. "*KGB cables indicated that the Office of Strategic Services (OSS) in World War II had been thoroughly infiltrated with Soviet agents*."

[78]Ver http://www.nsa.gov/publications/publi00044.cfm

en código que parecen en los ficheros Venona y que no han sido asignados a ninguna persona en concreto. De acuerdo con algunos autores[79], las transcripciones Venona identifican aproximadamente a 349 americanos que, según los mismos autores, tenían relación con la inteligencia soviética, aunque sólo menos de la mitad han sido relacionados con identidades reales.

La Oficina de Servicios Estratégicos, la predecesora de la actual CIA, tuvo en su seno y en distintos periodos entre quince y veinte espías soviéticos [80]. Duncan Lee, Donald Wheeler, Jane Foster Zlatowski, y Maurice Halperin pasaron información a Moscú. Los organismos War Production Board, el Board of Economic Warfare, la oficina del Coordinator of Inter-American Affairs y la Office of War Information incluyeron, al menos, media docena de espías soviéticos entre sus empleados. En opinión de algunos, casi cualquier agencia Americana militar o diplomática de alguna importancia tenía, en mayor o menor número, varios espías soviéticos en plantilla[81].

El proyecto Venona añadió información, en algunos casos clara y en otros de forma bastante ambigua, a varios casos de espionaje. Algunos espías conocidos, incluyendo a Theodore Hall[82], no fueron perseguidos, ni públicamente implicados, porque las evidencias Venona contra ellos no fueron hechas públicas.

Sin embargo, Venona sí aportó información, y además muy significativa, en el caso contra Julius y Ethel Rosenberg, dejando claro que Julius era realmente culpable de espionaje, a la vez que mostraba que Ethel probablemente no llegó a ser más que su cómplice, si es que llegó a tanto. Además, tanto Venona como otras informaciones recientes han demostrado que el contenido del espionaje atómico realizado Julios no fue tan vital como se dijo en su momento, pero en otros temas sí que fue muy intenso.

---

[79]Ver Haynes, John Earl and Klehr, Harvey (2000). *Venona: Decoding Soviet Espionage* Algunos académicos y periodistas discuten las afirmaciones de Haynes, Klehr y de otros respecto a la precisión en la asignación de nombres en código con personas física concretas.

[80]Ver Warner, Michael (2000). *The Office of Strategic Services: America's First Intelligence Agency*; Capitulo X-2. Central Intelligence Agency Publications.

[81]Peake, Hayden B.. *The Venona Progeny. Naval War College Review, Summer 2000, Vol. LIII, No. 3. "Venona makes absolutely clear that they had active agents in the U.S. State Department, Treasury Department, Justice Department, Senate committee staffs, the military services, the Office of Strategic Services (OSS), the Manhattan Project, and the White House, as well as wartime agencies. No modern government was more thoroughly penetrated*."

[82]**Theodore Alvin Hall** (1925-1999) fue un físico americano y un espia atómico que trabajaba para la Unión soviética y que, durante su trabajo dentro del esfuerzo aliado para hacerse con un explosivo nuclear durante la Segunda Guerra Mundial (Proyecto Manhattan), dio una descripción detallada de la bomba de plutonio conocida como "Fat Man", asi como datos sobre los procesos de purificación del plutonio, a la inteligencia soviética.

La información que Rosenberg realmente pasó a los soviéticos estaba relacionada con espoletas de proximidad[83], con información sobre el diseño y producción del avión Lockheed P-80, y con cientos de informes clasificados de la Emerson Radio Corporation. Las evidencias Venona indican que fueron las fuentes con nombre en código "Quantum" y "Pers" las que realmente facilitaron la transferencia de la tecnología de armamento nuclear a la Unión Soviética desde posiciones internas del Proyecto Manhattan.

Cuando Kim Philby supo de la existencia de Venona en 1949, temió que quedase expuesta la cobertura de sus espías Donald Maclean y Guy Burgess. Agentes del FBI le comentaron a Philby que había un agente con nombre en código Homer, cuyo mensaje enviado a Moscú en 1945 había sido decodificado. Como había sido enviado desde Nueva York y su origen era la embajada británica en Washington, Philby dedujo que se trataba de Donald Maclean (Philby no conocía el nombre en código de Maclean). A principios de 1951, Philby supo que la inteligencia norteamericana pronto concluiría que Maclean era el remitente, y aconsejó que Maclean fuese llamado a Moscú. Esto condujo al famoso viaje[84] de Maclean y a Guy Burgess a Rusia en mayo de 1951.

El 1 de febrero de 1956, Alan H. Belmont preparó un informe para el FBI sobre el significado del proyecto Venona y las posibilidades de utilizar sus descifrados en la persecución de delitos y causas penales. Belmont consideró que, aunque los descifrados vendrían a corroborar el testimonio de Elizabeth Bentley[85] y permitían el procesamiento de sospechosos como Judith Coplon y los miembros de los círculos de espías de Perlo (dirigido

---

[83]Una **expoleta o detonador de proximidad**, también llamada expoleta VT fuze, por "tiempo variable", es una espoleta o detonador diseñado para detonar un explosivo automáticamente cuando la distancia al objetivo es mas pequeña que un valor predetermiando o cuando el objetivo pasa a través de un plano dado. Hay varios principios sensibles: detección por radio frecuencia *sensing*, detección óptica, acustica, magnética, de presión,etc.

[84]Ver Yuri Modin, *My Five Cambridge Friends*, 1994, Ballantine, pp. 190-199.

[85]**Elizabeth Terrill Bentley** (1908-1963) fue una americana que espió para la Unión Soviética desde 1938 hasta 1945. En 1945 desertó del Partido Comunista y de la inteligencia soviética y se convirtió en informadora de los EE. UU. Ella puso al descubierto dos redes de espías, haciendo que cerca de 80 ciudadanos americanos fuesen acusados de espionaje a favor de los soviéticos. Cuando su testimonio se hizo público en 1948, fue la sensación del momento y un buen argumento para el anti-comunismo de la población en la era McCarthy.

por Víctor Perlo) y Silvermaster, un estudio cuidadoso de todos los factores implicados llevaron a la conclusión de que no sería conveniente para los intereses de los Estados Unidos utilizar las informaciones del proyecto Venona en procesos judiciales[86].

A lo largo de su historia, el proyecto Venona ha tenido carácter restringido incluso para las más altas instancias del gobierno de los EEUU. Algunos oficiales de alta graduación del ejército norteamericano, después de haber consultado con el FBI y la CIA, tomaron la decisión de restringir el uso de Venona dentro del gobierno; ni siquiera la CIA fue miembro de pleno derecho del restringido círculo de iniciados hasta 1952. El Jefe del Estado Mayor del Ejército, Omar Bradley, preocupado por la larga tradición de filtraciones de información sensible cuya fuente era la Casa Blanca, decidió negar al presidente Truman la existencia misma del proyecto. El presidente recibía lo que era significativo para el proyecto Venona a través de informes de inteligencia y contrainteligencia del FBI, del Departamento de Justicia y de la CIA, pero no se le decía que dicho material venía directamente del descifrado de mensajes soviéticos interceptados. Ese secretismo era, hasta cierto punto, contraproducente ya que Truman terminó desconfiando del director del FBI, J. Edgar Hoover, y sospechaba que los informes habían sido exagerados con fines políticos.

Algunos de los primeros testimonios detallados sobre mensajes codificados de los soviéticos desde la Segunda Guerra Mundial que habían sido descifrados aparecieron en el libro de Robert Lamphere titulado "*The FBI-KGB War*" y publicado en 1986. Lamphere había sido el enlace del FBI con los criptoanalistas y tenía un considerable conocimiento de Venona y de todo el trabajo de contrainteligencia que de él se derivó. Aunque se han ido conociendo algunos detalles, no fue hasta el año 1995 cuando la Comisión sobre el Secreto en el Gobierno, dirigida por el senador Daniel Patrick Moynihan, desclasificó los materiales del proyecto Venona para mayor interés de los historiadores y del pueblo norteamericano.

Una de las consideraciones que se tuvieron en cuenta a la hora de desclasificar las transcripciones Venona, fue la de salvaguardar la intimidad[87] de los individuos que eran mencionados en las mismas, o que pudieran ser

[86]Ver FBI Office *Memorandum; A. H. Belmont to L. V. Boardman* (February 1956). En http://cryptome.org/fbi-nsa.htm

[87]Ver Benson, Robert Louis. *Venona Historical Monograph 4: The KGB in San Francisco and Mexico City and the GRU in New York and Washington*. National Security Agency Archives, Cryptological Museum, dispnible en http://www.fas.org/sgp/library/moynihan/appa6.html.

identificados. Algunos nombres no han sido desclasificados porque, de hacerlo, supondría una invasión de su intimidad . Sin embargo, al menos en un caso, investigadores independientes han identificado una persona cuyo nombre ha sido tachado por la NSA en los documentos liberados.

A pesar de que la mayoría de los estudiosos consideran los documentos Venona como relevantes, precisos y auténticos, eso no es óbice para que haya voces que los cuestionen. Algunos críticos con los papeles Venona que han sido liberados señalan el hecho de que su autenticidad es imposible de verificar, e incluso alguno, como William Kunstler[88], llega a decir que realmente la NSA ha falsificado todo el material Venona en aras a desacreditar al Partido Comunista de los Estados Unidos de América (CPUSA) y a sus miembros. Investigaciones llevadas a cabo en archivos soviéticos sobre materiales de la misma época y circunstancias corroboran algunos de los materiales publicados del proyecto Venona, incluidas las identidades de muchos nombres en código[89].

Algunos permanecen excépticos tanto de la sustancia como de las interpretaciones dominantes realizadas desde que los papeles salieron a la luz pública. Víctor Navasky, editor del periódico *The Nation*[90], ha escrito varias editoriales muy críticas sobre las interpretaciones que John Earl Haynes y Harvey Klehr hacen en ciertos trabajos recientes sobre el espionaje soviético. Navasky afirma que el material Venona está siendo utilizado para "*distorsionar… nuestro entendimiento de la Guerra Fría*" y que esos ficheros son potenciales "*bombas de tiempo de desinformación*"[91]. Respecto a la lista de 349 ciudadanos americanos identificados por Venona que Haynes y Klehr han publicado como un anexo del libro Venona: *Decoding Soviet Espionage in America*, Navasky escribió: "*The reader is left with the implication --unfair and unproven-- that every name on the list was involved in espionage, and as a result, otherwise careful historians and mainstream journalists now routinely refer to Venona as proof that many hundreds of Americans were part of the red spy network*". Navasky va mas allá en la defensa de la gente que aparece en esa lista y declara que una gran parte de lo que ocurrió y se ha dado en llamar espionaje no era más que meros

---

[88]**William Moses Kunstler** (1919-1995) fue un jurista americano que se autodescribía como un "radical lawyer" y activista de los derechos civiles.

[89]Haynes, John Earl y Klehr, Harvey (2003). *In Denial: Historians, Communism, and Espionage*. Encounter Books, pg. 101. ISBN 1-893554-72-4.

[90]Ver http://www.thenation.com/

[91]Navasky, Victir (July 16, 2001). Cold War Ghosts. The Nation.
En http://www.thenation.com/docprint.mhtml?i=20010716&s=navasky

"*intercambios de información entre gentes de buenas intenciones*" y que "*la mayoría de esos intercambios fueron inocentes y estaban dentro de la ley*", y que fueron realizados por "patriotas".

Por otro lado, Ellen Schrecker añade que: "*Porque ellos* [los documentos Venona] *ofrecen algo de luz en un mundo de policías secretas a ambos lados del Telón de Acero, podemos estar tentados a tratar los materiales del FBI y de Venona menos críticamente que otros documentos provenientes de fuentes más accesibles. Sin embargo, hay demasiadas ausencias en los registros para utilizar esos materiales con plena confianza*".[92]

Nigel West[93] por otra parte, expresa su confianza en los descifrados: "*Venona sigue siendo una fuente irrefutable, mucho más fiable que los volubles recuerdos de los desertores del KGB y de las dudosas conclusiones obtenidas por análisis paranoicos mesmerizados [hipnotizados] por conspiraciones maquiavélicas*".[94]

La teoría de la información y de los sistemas secretos

Claude Elwood Shannon (1916-2001), fue un ingeniero y matemático norteamericano al que se le ha llegado a llamar "el padre de la Teoría de la Información"[95]. Shannon es famoso por haber dado fundamentos sólidos a la teoría de la información, a la del diseño de ordenadores y a la de circuitos digitales en su tesis de máster que fue publicada en 1937, cuando tan solo tenía veintiún años. En dicha tesis articulaba la aplicación del Álgebra Booleana a los circuitos eléctricos para construir y resolver cualquier relación lógica o numérica. Se ha llegado a decir que esta tesis de máster ha sido la más importante de todos los tiempos[96].

---

[92]Schrecker, Ellen (1998). *Many are the Crimes: McCarthyism in America*. Little, Brown, pp. xvii-xviii. ISBN 0-316-77470-7.

[93]**Rupert William Simon Allason** (1951-) es un historiador militar y político del Partido Conservador inglés, y tambien fue miembro del parlamento (MP) por el distrito de Torbay en la región de Devon, desde 1987 hasta 1997. Escribe libros sobre espionaje bajo el pseudónimo de **Nigel West**.

[94]West, Nigel (1999). V*enona -The Greatest Secret of the Cold War*. Harper Collins, pg. 330. ISBN 0-00-653071-0.

[95]Ver http://www.bell-labs.com/news/2006/october/shannon.html

[96]Poundstone, William: *Fortune's Formula: The Untold Story of the Scientific Betting System That Beat the Casinos and Wall Street*, Hill and Wang Publishers, August 25, 2005. ISBN-10: 0809046377 ISBN-13: 978-0809046379

En el año 1948 Shannon publicó su artículo titulado "*A Mathematical Theory of Communication*"[97] en dos entregas, en los números de julio y octubre de la revista *Bell System Technical Journal*. Este trabajo se centraba en el problema de cómo codificar mejor la información que un remitente quiere transmitir. En este trabajo fundamental el autor utilizó herramientas de la teoría de probabilidades desarrollada por Norbert Wiener[98], que estaban en sus primeros estadíos, para aplicarlas a la teoría de la comunicación. Shannon desarrolló el concepto de entropía de la información como una medida de la incertidumbre contenida en un mensaje y con ello, esencialmente, inventó la Teoría de la Información. El libro del que es co-autor Warren Weaver, "*The Mathematical Theory of Communication*" reedita el artículo de Shannon de 1948 y la divulgación que de él hizo Weaver. Los conceptos de la teoría de Shannon también fueron difundidos por John Robinson Pierce en su libro "*Symbols, Signals, and Noise*".

La contribución fundamental que la Teoría de la Información había hecho al procesado del lenguaje natural y a la lingüística computacional quedó establecida en 1951, en un artículo de Shannon titulado "*Prediction and Entropy of Printed English*"[99], en el que probaba que si tratamos al espacio en blanco como una letra mas del alfabeto, lo que conseguimos es reducir la incertidumbre del cualquier lenguaje escrito, proporcionando una relación clara y cuantificable entre la práctica cultural y el conocimiento probabilístico.

Otro artículo muy importante fue el publicado también por Shannon en el año 1949 y que tituló "*Communication Theory of Secrecy Systems*"[100], y es, sin duda, el artículo que más ha contribuido al desarrollo de una teoría

---

[97]Claude E. Shannon: *A mathematical theory of communication*. Bell System Technical Journal, 27:379-423 and 623-656, July and October 1948. Disponible en http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

[98]**Norbert Wiener** (1894-1964), matemático norteamericano que fue pionero en el estudio de los procesos estocásticos y del ruido, contribuyendo con aportaciones muy relevantes a la ingeniería eléctrica, a las telecomunicaciones, y al control de sistemas. Wiener es también el fundador y padre de la cibernética, un campo que formaliza la noción de realimentación y que tiene aplicación en ingeniería, control de sistemas, ciencia de los ordenadores, biología, filosofía, y en la organización de las sociedades.

[99]Shannon, C. E.: *Prediction and entropy of printed English*. Bell Systems Technical Journal, 30, pp. 50-64, 1951. Disponible en http://www.cs.brown.edu/courses/cs195-5/extras/shannon-1951.pdf

[100]Disponible en http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf

matemática de la criptografía. En este artículo, se prueba que todas las cifras teóricamente irrompibles deben satisfacer los mismos requisitos que la cifra *One-Time Pad*. A Shannon también se le reconoce haber sido el introductor de la Teoría del muestreo[101], que se encarga de cómo representar una señal continua en el tiempo mediante un conjunto (uniforme) discreto de muestras (valores). Esta teoría es esencial para permitir que las telecomunicaciones pasasen de los sistemas de transmisión analógica a digital en la década de 1960 y posteriores.

La guerra de Corea

Entre los veranos de 1950 y 1953 se desarrolló un conflicto bélico alrededor del paralelo 38 que separaba las dos Coreas con regímenes políticos antagónicos. Ambas intentaron la reunificación coreana bajo sus respectivas ideologías pero esos intentos terminaron en una guerra civil que es la que se conoce como Guerra de Corea. Este es un buen ejemplo de "guerra delegada" en la que dos superpotencias externas dirimen sus diferencias con los recursos, el territorio y la sangre de otros. Otros ejemplos de ese tipo de conflictos son la guerra civil española (1936-1939), la guerra civil griega (1946-1949), la guerra de Vietnam (1959-1975), la guerra civil del Líbano (1975-1990), la guerra de la independencia angoleña (1961-1974), la segunda guerra del Congo (1998-2003), etc.

Fue en este escenario, en el año 1951 cuando la máquina TSEC/KL-7, con nombre en código ADONIS, reemplazó a la máquina SIGABA. KL-7 era una máquina de cifrar que utilizaba rotores, y que se puso en producción en la década de 1950 por parte de la National Security Agency norteamericana. La máquina utiliza ocho rotores, de los cuales siete se mueven de una forma compleja. El rotor que no se mueve está colocado en el centro de la pila de rotores. El sistema KL-7 fue diseñado para operar en modo *off-line*. Tenía el tamaño de un teletipo de la época y, como aquellos, presentaba las tres filas de teclas y el control de mayúsculas, con las letras y los números. La KL-7 daba su salida impresa en una estrecha cinta de papel que luego se pegaba en renglones para componer los textos finales de los mensajes.

[101]El *teorema de muestreo de Nyquist-Shannon* es un resultado fundamental en el campo de la teoría de la información, en particular para las telecomunicaciones y el procesado de señales. Este teorema es conocido normalmente como el *teorema de muestreo de Shannon*, o como el teorema de muestreo de *Nyquist-Shannon-Kotelnikov, Whittaker-Shannon-Kotelnikov, Whittaker-Nyquist-Kotelnikov-Shannon, WKS,* etc., asi como el de *Teorema Cardinal de la Teoría de la Interpolación*. Normalmente uno se refiere a él como el *teorema de muestreo.*

Cuando se cifraba, automáticamente colocaba un espacio después de haber escrito un grupo de cinco letras. Había un adaptador, el HL-1/X22, que permitía el uso de cintas de papel con el código Baudot de cinco bits que eran típicas de los teletipos y que eran muy útiles a la hora de proceder a descifrar un mensaje que había llegado a través de los teletipos. La máquina KL-7 básica no tenía la capacidad de perforar cintas de papel, pero una de sus variantes, la KL-47, si que podía hacerlo ya que la permitían conectarse directamente a la red de teletipos.

Cada rotor tenía 36 contactos para configurar un nuevo estado, una nueva configuración de cifrado/descifrado; los operadores de la máquina debían seleccionar un rotor y colocarle un anillo de plástico externo que contenía unas levas, en la orientación adecuada. Además, los anillos de levas a utilizar y la orientación relativa estaban especificados dentro de la clave. Este proceso se repetía ocho veces hasta que todos los rotores habían sido instalados. Por otro lado, la configuración se solía cambiar todos los días a medianoche hora GMT. La cesta que contenía los rotores era removible, y era frecuente tener preparado un segundo juego de rotores y su correspondiente cesta, permitiendo preparar los rotores antes de que se produjese el cambio de clave, de modo que éste resultase prácticamente inmediato. La cesta sustituida podía dejarse intacta para descifrar aquellos mensajes cifrados el día anterior pero que se recibían después de media noche.

La cesta de rotores tenía dos juegos de conectores en cada extremo que coincidían con los del conjunto principal de rotores. Un par de conectores, con 26 contactos cada uno, los conectaban con el teclado y con la impresora. Otro par de conectores, con diez contactos cada uno, conectaban con el mecanismo utilizado para controlar los motores de paso a paso. Había también un conjunto de micro interruptores colocados debajo de las levas de cada rotor móvil y con las cuales actuaban; a diferentes anillos externos correspondían diferentes conjuntos de levas. El modo exacto en el que todas estas características trabajaban juntas no es públicamente conocido, pero es fácil imaginar que causaban el avance de los rotores de un modo pseudoaleatorio, un principio de diseño que ya se había aplicado con éxito en el caso de la máquina SIGABA. Según algunas fuentes, el avance de los rotores era independiente del texto en claro o del criptograma de entrada[102]. Había un tablero de permutación debajo del teclado que podría haberse utilizado para fijar la conexión de la entrada con la salida de la cesta de rotores, de modo que la misma configuración de rotores podría haber sido utilizada, indistintamente, para el cifrado y el descifrado de mensajes.

[102]Ver http://www.jproc.ca/crypto/kl7.html

La máquina KL-7 fue sustituida por sistemas electrónicos tales como el KW-26 ROMULUS y el KW-37 JASON en la década de 1970, pero los KL-7s se mantuvieron en servicio como sistemas de respaldo o para casos especiales.

En diciembre del año 1967, y debido a problemas financieros en la gestión de un restaurante de Carolina del Sur, un marinero de la armada norteamericana, John Andrew Walker[103], entró en la embajada soviética en Washington buscando un empleo como espía y, como primera entrega, ofreció una copia de una lista de claves de la KL-47 por la que cobró algunos millares de dólares. Las máquinas KL-7s estuvieron comprometidas también en otras ocasiones. Una de ellas, cuando una unidad fue capturada por el ejército de Vietnam del Norte, durante el incidente del barco espía USS Pueblo, y que hoy se puede ver en el Museo Criptológico Nacional de la NSA. El sistema KL-7 fue retirado definitivamente de servicio en junio de 1983, y el último mensaje canadiense cifrado con una KL-7 se envió el 30 de junio de 1987, después de haber estado veintisiete años en servicio.

La máquina sucesora de la KL-7 fue la KL-51, un sistema *off-line* de cifrado que utilizaba cintas perforadas de papel compatibles con los teletipos y que, en su interior, utilizaba ya circuitos eléctricos en lugar de rotores para generar las secuencias cifrantes.

Diecisiete años de espionaje para el Kremlin

John Andrew Walker, Jr. (1937-) empezó a espiar para los soviéticos en diciembre de 1967, cuando tenía serios problemas financieros relacionados con un bar restaurante en Carolina del Sur que él regentaba en paralelo con sus actividades militares. Dicho bar le generaba enormes deudas y le llevó a la ruina. Por esta razón, Walker se fue a la embajada soviética en Washington y se alistó como espía.

[103]**John Andrew Walker, Jr**. (1937-) fue un especialista en comunicaciones de la Armada norteamericana, y actuó como espía para la Unión Soviética entre los años 1968 y 1985; en el climax de la Guerra Fría. En este tiempo, ayudó a los soviéticos a descifrar cerca de doscientos mil mensajes cifrados clasificados de la Armada, y la mayor parte de los estudiosos están de acuerdo en que fue uno de los mas efectivos y destructivos espías soviéticos actuando en los EEUU, de la historia moderna.

Mas tarde Walker justificaría su traición diciendo que los datos de comunicaciones clasificadas de la Armada que él había vendido a los soviéticos estaban completamente comprometidas después de incidente con el USS Pueblo; este incidente tuvo lugar cuando un barco de vigilancia de comunicaciones radioeléctricas de la Armada de los EEUU fue capturado en alta mar por el ejército de Corea del Norte, y su dotación hecha prisionera durante casi un año. Sin embargo, una tesis[104] presentada en el año 2001 en el *U.S. Army Command and General Staff College*, cuya investigación se llevó a cabo con información proveniente de los archivos soviéticos y de un antiguo espía soviético, Oleg Kalugin[105] , sostiene que el incidente con el USS Pueblo ocurrió precisamente porque los soviéticos querían estudiar el equipo que aparecía descrito en los documentos que Walker les había proporcionado.

Cuando Walker era enviado a otro destino o cuando necesitaba información, reclutaba a amigos y miembros de su propia familia (su mujer, su hermano mayor Arthur y su hijo Michael) para que se unieran a su círculo de espías. Su amigo y discípulo en temas de espionaje era un radio telegrafista jefe de la Armada llamado Jerry Whitworth, que tenía acceso a datos altamente clasificados de comunicaciones vía satélite. El circulo de espías creado por Walker continuó proveyendo de información importante a los soviéticos incluso después de que John Walker fuese jubilado en 1976.

Las actividades de Walker nunca levantaron la menor sospecha entre las autoridades norteamericanas, a pesar de su vida extravagante y de vivir muy por encima de la que, oficialmente, era su única fuente de ingresos: la pensión de la Armada. Después de su jubilación, cuando vivía en Norfolk, Virginia, consiguió la licencia de investigador privado y de piloto de aviones privados, hechos que él utilizó para dar cobertura a su lujoso estilo de vida y a sus frecuentes viajes por Norteamérica y Europa occidental, esencialmente para verse con su controlador soviético y recibir instrucciones además de sus pagos. Como tapadera adicional, también se afilió a organizaciones de la derecha radical como la John Birch Society. Se estima que Walker ganó más de un millón de dólares americanos durante las casi dos décadas de actividad como espía.

---

[104]Laura J. Heath: *Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967-1974, as Exploited by CWO John Walker*, Master's thesis disponible en http://www.fas.org/irp/eprint/heath.pdf

[105]**Oleg Danilovich Kalugin** (Олег Данилович Калугин), (1934 -) es un general retirado del KGB, que fue durante mucho tiempo jefe de las operaciones del KGB en los Estados Unidos y que mas tarde se convirtió en un crítico de la agencia.

En mayo de 1985, Walker y sus cómplices fueron arrestados por el FBI bajo la sospecha de espionaje. Las autoridades fueron advertidas de dichas actividades por la hija de Walker, Laura, y por su ex-esposa, personas a las que él había desatendido durante años y a las que, finalmente, negó su pensión alimentaria. Los investigadores analizaron con detalle las cuentas de Walker y encontraron que sus ingresos provenientes de la agencia de detectives eran insuficientes para proporcionar el lujoso estilo de vida que llevaba. A pesar de la resistencia inicial a investigar el caso por parte del FBI, los cuatro hombres fueron detenidos y acusados de espionaje. Tres de ellos recibieron condenas a cadena perpetua.

Inicialmente Walker mantuvo una actitud desafiante, y a él se le atribuye la respuesta a sus interrogadores "*If I had access, consider it gone!*" Sin embargo, después se ofreció colaborar con las autoridades a cambio de un acuerdo para reducir la pena impuesta a su hijo Michael hasta no más de veinticinco años de prisión. Michael, que había tenido un papel menor en el círculo de espías montado por su padre, salió de prisión en libertad condicional en febrero del año 2000. Walker también estuvo de acuerdo en declarar en la causa contra su pupilo en cuestiones de espionaje, Jerry Whitworth, y su testimonio fue esencial para condenarlo. Varios años después de haber sido sentenciado, Walker concedió una entrevista a la BBC, y lo hizo con la condición de que solo se le preguntase sobre sus actividades de espionaje y no sobre su familia o sus propios sentimientos. En la entrevista, Walker ridiculizó el sistema de seguridad de la Armada de los EEUU. Argumentó que éste era prácticamente inexistente, que los almacenes K-Mart tienen mejores medidas de seguridad; sus palabras exactas fueron "*K-Mart protects their toilet paper better than the Navy protects its top secrets*".

Algunos investigadores creen que las casi dos décadas de espionaje de Walker contribuyeron significativamente a la ascensión, sin precedentes, del por aquel entonces director del KGB Yuri Andropov, a la presidencia de la Unión Soviética en noviembre de 1982 tras la muerte de Leónidas Brezhnev.

La guerra de Vietnam

La máquina TSEC/KW-26, con nombre en código ROMULUS, fue un sistema de cifrado utilizado por el gobierno de los Estados Unidos y, más tarde, por otros países de la OTAN. Fue desarrollada en la década de 1950 por la Agencia de Seguridad Nacional (NSA) para asegurar los circuitos de teletipos que estaban en funcionamiento las veinticuatro horas del día. Esta máquina, a diferencia de sus predecesoras como SIGABA y la británica 5-UCO[106], que utilizaban rotores y relés electromecánicos, utilizaba tubos de vacío y memorias de núcleos de ferrita.

El sistema KW-26 (transmisor o receptor) contenía cerca de 800 núcleos de ferrita y aproximadamente 50 circuitos de tubos de vacío, ocupando un volumen equivalente a la mitad de lo que es un rack estándar de 19 pulgadas. La mayor parte de ese volumen y casi todo el kilowatio de potencia eléctrica que consumían sus circuitos de lámparas de vacío, eran precisos para permitir diferentes configuraciones de entrada y salida. Los requisitos de los servicios militares incluían numerosos nodos y velocidades de funcionamiento, lo que incrementó su coste y los retrasos en las entregas. La NSA declaró que era poco probable que alguna vez se utilizasen más de cuatro de las posibilidades que en su diseño permitía.

Este sistema, utilizado y desarrollado por la NSA, basaba su algoritmo de cifrado en el uso de registros de desplazamiento. El algoritmo producía un flujo continuo de bits que se combinaban mediante la función binaria Or exclusivo[107] con los cinco bits del código Baudot de los teletipos y producir así el criptograma en el transmisor, y el texto en claro si se trataba del extremo receptor. En la terminología de la NSA, a este flujo de bits se les

---

[106]La **5-UCO (5-Unit COntrolled)** fue una máquina de cifrado on-line tipo Vernam desarrollada por los británicos durante la Segunda Guerra Mundial para ser utilizada en circuitos de teletipos. Durante los años cincuenta, fue utilizada por el Reino Unido y los Estados Unidos como enlace para temas de criptoanálisis. Ver Ralph Erskine, *The 1933 Naval BRUSA Agreement and its Aftermath, Cryptologia* 30(1), January 2006 pp14-15. La máquina 5-UCO era completamente sincrónica, y por tanto podía ser eléctricamente regenerada en tandem con enlaces de radio de alta frecuencia (HF) es decir, un enlace conectado con el siguiente. Podía operar directamente con circuitos comerciales. El sistema también proporcionaba seguridad frente al control del tráfico (TFS). Otra de las características de la 5-UCO era que el operador que recibía el mensaje podía mantener la sincronización si de repente cambiaba el retardo en el camino mediante "*walking up and down*" la cinta (un carácter cada vez o un bit cada vez). Este procedimiento evitaba la tediosa tarea de tener que volver a empezar. Ver Melville Klein, *Securing Record Communications*: The TSEC/KW-26, 2003, NSA brochure, p. 4, disponible en http://www.nsa.gov/publications/publi00017.pdf

[107]OR-exclusivo = 0 a la salida si las dos entradas son iguales, y 1 si son diferentes.

llama la clave, mientras que la información necesaria para inicializar el algoritmo que la mayoría de los criptógrafos actuales llama clave, la NSA la llama *criptovariable*. Típicamente, a cada KW-26 se le daba una nueva criptovariable cada día.

En el mes de agosto de 1964 se produjo lo que más tarde se conocería como el incidente del Golfo de Tonkin, y que consistió en dos supuestos ataques por parte de las fuerzas navales de la República Democrática de Vietnam a dos destructores americanos, el USS Maddox y el USS Turner Joy. Se dice que tales ataques se produjeron el 2 y el 4 de agosto de 1964 en el Golfo de Tonkin, pero investigaciones posteriores, incluyendo un informe hecho público en 2005 por la NSA, indicaban que probablemente el segundo ataque nunca llegó a producirse. Ese informe también intentó disipar la suposición asumida desde hacía mucho tiempo de que miembros de la administración del presidente Lyndon B. Johnson habían mentido deliberadamente sobre la naturaleza del incidente[108].

Como resultado de tal incidente, se llevó y aprobó en el Congreso de los EE.UU. la denominada Resolución del Sudeste Asiático, más conocida como la Resolución del Golfo de Tonkin, que otorgaba a Johnson la autoridad para ayudar a cualquier país del sudeste asiático cuyo gobierno pudiera considerarse en peligro de una "*agresión comunista*". Esta resolución le sirvió a Johnson como justificación legal para involucrar a los Estados Unidos en la Guerra de Vietnam.

Daniel Ellsberg[109], que estaba de servicio en el Pentágono recibiendo mensajes del barco la noche del ataque, informó que los barcos estaban en misión secreta (nombre en código *Desoto*) cerca de las aguas territoriales de Vietnam del Norte. El 31 de Julio de 1964, el destructor americano USS Maddox (DD-731) inició una misión de recolección electrónica de datos de inteligencia en el Golfo de Tonkin. El almirante George Stephen Morrison estaba al mando de la flota desde su buque insignia el USS Bon Homme Richard (CVA-31). El Maddox tenía órdenes de no aproximarse a la costa a menos de ocho millas (13 km) ni a menos de cuatro millas de la isla de Hon Nieu. Cuando la operación empezó a producirse el barco estaba a 120 miles (193 km) del área atacada[110].

---

[108]Ver http://www.nsa.gov/vietnam/

[109]**Daniel Ellsberg** (1931-), analista militar americano empleado por la RAND Corporation que precipitó un escándalo nacional en 1971 cuando publicó los denominados *Pentagon Papers*, un estudio top-secret del Pentágono sobre las decisiones tomadas por el gobierno de los USA durante la Guerra de Vietnam, en el *The New York Times* y otros periódicos.

[110]**The Pentagon Papers**. Gravel Edition. Volume 3. Chapter 2, *Military Pressures Against North Vietnam, February 1964-January 1965*, pp. 106-268. (Boston: Beacon Press, 1971), disponible en http://www.mtholyoke.edu/acad/intrel/pentagon3/pent4.htm

El 2 de agosto el Maddox fue, como insiste el Pentágono, atacado por tres lanchas torpederas P-4 de patrulla a 28 miles (45 km) de distancia de la costa norvietnamita en aguas internacionales. El *Maddox* esquivó el ataque con torpedos y abrió fuego con sus cañones de cinco pulgadas (127 mm), forzando a huir a las patrulleras. Un avión norteamericano que despegó del Ticonderoga atacó después a las lanchas P-4s en retirada; el piloto dijo haber hundido una de ellas y dejado otra gravemente dañada. De hecho, ninguna de las tres lanchas fue realmente hundida. El Maddox, con un pequeño desperfecto generado por una única bala de ametralladora de 14,5 milímetros, se retiró a aguas survietnamitas donde se reunió con el destructor USS Turner Joy.

El cuatro de agosto, se realizó otra patrulla sobre la costa de Vietnam desde el Maddox y el Turner Joy, y fue dirigida por el capitán John J. Herrick. En ese momento, sus órdenes indicaban que los barcos se aproximasen hasta las 11 millas (18 km) de la costa. Los destructores recibieron señales de radar y de radio que interpretaron como indicios de un nuevo ataque por parte de la marina norvietnamita, por lo que durante dos horas los barcos norteamericanos dispararon sobre los supuestos radares y maniobraron vigorosamente entre informes visuales y electrónicos de los enemigos. Pero una hora después, a la 1:27 p.m. hora de Washington, Herrick envió un cable en el que admitía que el ataque nunca se había producido y que, de hecho, no había naves norvietnamitas en la zona. Sin embargo, a pesar de que nunca hubo ataques por parte de los norvietnamitas, el cinco de agosto, aviones de los portaviones Ticonderoga y Constellation salieron en 64 misiones a destruir las bases de lanchas torpederas y las instalaciones de combustible norvietnamitas (*Operation Pierce Arrow*[111]).

[111]La operación **Pierce Arrow** fue la primera operación militar de los EEUU en la Guerra de Vietnam. Se produjo en respuesta a los incidentes del Golfo de Tonkin en los que el USS Maddox pareció ser atacado sin provocación previa por lanchas torpederas norvietnamitas el 2 de agosto de 1964. El presidente Lyndon B. Johnson ordenó esta operación de castigo que se realizó el 5 de agosto. La operación consistió en 64 misiones de castigo aéreo que partieron de los portaviones *Ticonderoga y Constellation* contra las bases de lanchas torpederas en Hon Gai, Loc Chao, Quang Khe, y Ben Thuy, y contra el almacén de combustible de Vinh. Los EE.UU. perdieron dos aviones por fuego antiaéreo, resultó muerto un piloto y otro, Everett Alvarez Jr., fue hecho prisionero, convirtiéndose así en el primer preso norteamerticano de la Guerra de Vietnam. Los pilotos estimaron que habían destruido el 90% del almacén de petróleo de Vinh, además de haber destruido o dañado 25 lanchas torpederas P-4, lo que representaba casi dos tercios de las capacidades norvietnamitas.

En las costas del Sinaí

El 8 de junio de 1967 se produjo lo que se conoce como el incidente del USS Liberty, que resultó ser un ataque a un barco de inteligencia de señales de la Armada de los EEUU, el USS Liberty, pero esta vez cuando estaba situado en aguas internacionales, a 12,5 millas náuticas (23 km), frente a la costa de la península del Sinaí, al norte de la ciudad egipcia de El Arish. En esta ocasión los atacantes eran aviones de guerra y lanchas torpederas israelíes. Este incidente ocurrió durante la Guerra de los Seis Días, un conflicto armado entre Israel y los estados árabes de Egipto, Jordania, Siria e Iraq. El ataque israelí al USS Liberty mató a 34 miembros del personal norteamericano e hirió a 173. Aún hoy el incidente resulta controvertido. Israel y varias agencias gubernamentales norteamericanas mantienen que fue un error, pero algunos supervivientes americanos dudan de que fuera un error.

Los gobiernos israelí y norteamericano realizaron varias investigaciones para averiguar porqué ocurrió ese incidente y confeccionaron informes en los que concluían que el ataque fue el resultado de un error, causado por la confusión entre los atacantes israelíes acerca de la identidad del USS Liberty, y el hecho de que el propio embajador de los Estados Unidos ante las Naciones Unidas había anunciado públicamente en la ONU que los EE.UU. no tenia barcos dentro de las 350 millas de la costa de Israel. La posición oficial del gobierno israelí fue que el incidente no era el resultado de un ataque intencionado a un barco americano, sino de un ataque deliberado a lo que Israel pensó que era un barco egipcio. Los oficiales israelíes afirman que los Estados Unidos les habían asegurado que no tenía barcos en el área[112], y que sus fuerzas aéreas y navales confundieron erróneamente el Liberty con el barco egipcio El Quseir.

Este incidente hay que examinarlo teniendo en cuenta la tensa atmósfera que había esos días en la zona, la cual que era el caldo de cultivo óptimo para que se diesen ese tipo de errores; el día anterior, es decir, el 7 de junio, Israel había bombardeado accidentalmente una de sus propias columnas de blindados. El propio gobierno norteamericano, preocupado por esos peligros, ordenó al USS Liberty alejarse aún más de la costa la noche anterior al ataque[113].

---

[112]Ver http://www.freerepublic.com/focus/news/1056949/posts?page=101,3

[113]Ver http://www.nsa.gov/liberty/liber00010.pdf y http://www.nsa.gov/liberty/

Capturando la máquina

Otro incidente análogo al anterior se produjo el 23 de enero de 1968 con el USS Pueblo (ALGER-2)[114], un barco de investigación técnica (Inteligencia de la Armada) de la clave Banner que fue abordado y capturado por lanchas de la República Popular Democrática de Corea (Corea del Norte). A este hecho se le conoce como el incidente del Pueblo o la crisis del Pueblo.

Con el envío del USS Pueblo, convertido en el barco de inteligencia de señales, la Armada de los EEUU ignoró las advertencias de la NSA sobre el hecho de que las defensas norcoreanas estaban en guardia y envió, sin protección, dicha nave a las peligrosas aguas norcoreanas. Esta era su primera misión. Con la captura del barco, también fueron capturadas por Corea del Norte las máquinas de cifrado KY-8[115] y KW-7 y luego enviadas a Rusia, que a su vez podría haber pasado toda la información a Vietnam con quien EEUU estaba en guerra. Los códigos de la NSA también habían quedado comprometidos cuando John Walker[116] empezó a vendérselos en secreto a los rusos.

Más tarde, los investigadores de la NSA supieron que el pesquero soviético Izmeritel, situado frente a las costas de Guam, se dedicaba realmente a monitorizar los despegues de los aviones B-52s que tomaron parte en la operación "Arc Light", una incursión de bombardeo sobre Vietnam del Norte; los B-52s no llevaban equipo de cifrado por lo que transmitían en claro las informaciones a través de canales de voz. La NSA también descubrió que Vietnam del Norte era capaz de monitorizar las transmisiones (no cifradas) de los aviones cisterna KC-135[117]. Los Estados Unidos perdieron la guerra del cifrado en Vietnam del mismo modo que los alemanes la perdieron durante la Segunda Guerra Mundial.

Hoy en día, El USS Pueblo está en manos de Corea del Norte, y según los registros[118] de la Armada norteamericana sigue en servicio.

---

[114]**AGER** = *Auxiliary General Environmental Research* representa a un programa conjunto de la Armada con la *National Security Agency* (NSA).

[115]La máquina **KY-8** pertenecía a la gama NESTOR de artefactos criptográficos que se montaban en vehículos. Eran máquinas grandes, bastante pesadas y poco fiables, pero en su apogeo, eran los únicos equipos portables de SECVOX (voz segura) que tenía el ejército norteamericano para su uso en el campo de batalla. Ver http://www.jproc.ca/crypto/ky08.html

[116]Heath, Laura: *An Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967-1974, as Exploited by CWO John Walker*. Tesis de Master en Artes Militares y Ciencias. Georgia Institute of Technology. pp. 54-58. Junio 2005. Disponible en http://www.fas.org/irp/eprint/heath.pdf

[117]Stratotanker KC-135, http://www.boeing.com/defense-space/military/kc135-strat/index.html

[118]Ver http://www.nvr.navy.mil/nvrships/details/AGER2.htm

ARPANET y la semilla del nuevo escenario

Al final de la década de los años sesenta, se pone en marcha la red conocida como ARPANET, que fue desarrollada por la Agencia de Investigación de Proyectos Avanzados de Defensa, (DARPA son sus siglas en inglés) del Departamento de Defensa de los Estados Unidos. Esta red de comunicaciones fue la primera que entró en operación y se basaba en el encaminamiento de paquetes[119]; podemos decir que es la predecesora de la actual Internet global.

A finales de 1966, Larry Roberts llegó al ARPA[120] desde el Lincoln Laboratory del MIT para dirigir un proyecto con objeto de crear una red de comunicaciones especial. Roberts tenía alguna experiencia previa en ese área ya que dos años antes, en 1965, mientras estaba en el MIT, había conectado el ordenador Lincoln TX-2 al ordenador Q-32 de la *System Development Corporation* a través de una línea telefónica, realizando así uno de los primeros experimentos en que dos ordenadores se comunican por teléfono. El concepto inicial de Roberts para la red del ARPA consistía en enganchar las diferentes máquinas de tiempo compartido directamente unas a otras a través del teléfono.

En la reunión que tuvo lugar a comienzos de 1967 en la Universidad de Michigan en Ann Arbor, Michigan, muchos de los asistentes no estaban muy contentos con la idea de tener que asumir la carga de gestionar esa línea directamente conectada a sus ordenadores. Uno de los participantes, Wesley Clark, sugirió la idea de utilizar un ordenador separado, más pequeño, sólo para gestionar la línea de comunicación, de modo que sería ese pequeño ordenador el que se conectaría al *mainframe* de tiempo compartido. Los *mainframes* eran, por aquel entonces, el único tipo de

[119]El **Encaminamiento de Paquetes o Packet switching** es un paradigma de comunicaciones en el que los paquetes (bloques discretos de datos) son redirigidos entre nodos a través de enlaces compartidos con otros tráficos. En cada nodo de la red, los paquetes son puestos en cola o metidos en un *buffer*, dando como resultado de este proceso un retardo variable. Este modo de transmitir contrasta con el otro paradigma, el de conmutación de circuitos, que ofrece un número limitado de conexiones con velocidades y retrasos de transmisión constantes entre los nodos para el uso exclusivo de estos durante el tiempo que se produce la comunicación.

[120]Su nombre original era **Advanced Research Projects Agency (ARPA)**, pero fue renombrada DARPA (para incluir el prefijo de **Defense**) el 23 de marzo de 1972, después volvió a ser ARPA el 22 de febrero de 1993, y de nuevo DARPA el 11 de marzo de 1996.

máquinas que se iban a conectar mediante ARPANET. Este concepto permitió que la mayor parte del trabajo de red fuese desterrado de los grandes *mainframes*; también significó que la operación global la red no estaría sujeta a las peculiaridades de cada host individual y, quizás más interesante, que el DARPA tendría el control completo sobre el tráfico y sobre la misma red. La planificación inicial para ARPANET empezó basándose en esta estructura física y contó con un cierto número de grupos de trabajo sobre temas científicos específicos reunidos desde el final de la primavera y el verano de 1967.

El DES y la criptografía civil

Horst Feistel (1915-1990) fue un criptógrafo que trabajó en el diseño de cifras para IBM, e inició una investigación cuyo resultado fue el desarrollo del Data Encryption Standard (DES) en la década de 1970. Feistel nació en Berlín el año 1915, y emigró a los EE. UU. en 1934. Debido a su condición de alemán, pasó la Segunda Guerra Mundial bajo arresto domiciliario, aunque consiguió la ciudadanía norteamericana el 31 de enero de 1944.

Al día siguiente de obtener la ciudadanía superó unas pruebas de seguridad que le permitió trabajar en el Centro de Investigación de Cambridge de la Fuerza Aérea de los EEUU (AFCRC) sobre los sistemas de Identificación de amigos y enemigos (*Friend or Foe*) (IFF) hasta la década de 1950. Más tarde fue contratado por el *Lincoln Laboratory* del MIT, y posteriormente trabajó para la MITRE *corporation*. Finalmente fue contratado por IBM, donde recibió el reconocimiento por su trabajo en criptografía. Su investigación en IBM condujo al desarrollo de los algoritmos de cifrado Lucifer y el Data Encryption Standard (DES). Feistel fue uno de los primeros investigadores no gubernamentales dedicado al estudio del diseño y de la teoría de los cifradores de bloques. Feistel dio nombre a lo que se conoce como Redes de Feistel, que es un método muy común para construir cifradores de bloques robustos a fuerza de repetir etapas más sencillas. Feistel obtuvo el grado de licenciado en el MIT, y su máster en Harvard, ambos en física.

El Data Encryption Standard (DES) es un método para cifrar y descifrar información. Este método fue seleccionado en 1976 como un estándar oficial por parte de los *Federal Information Processing Standard* (FIPS) de los Estados Unidos, y ha sido ampliamente utilizado internacionalmente. El algoritmo fue originalmente muy controvertido debido a que sus pautas de diseño estaban "clasificadas" (aún hoy lo están), a su relativamente corta longitud de clave, 56 bits, y a las sospechas que originó el saber que en su desarrollo había participado la National Security Agency (NSA) y que

ésta hubiese incluido una "puerta trasera" que debilitase su seguridad real frente a un ataque por parte de la misma agencia. El DES ha sido intensamente analizado en el mundo académico y ha sido el catalizador de la comprensión que ahora se tiene de los cifradores de bloques y de su criptoanálisis.

En la actualidad se considera que el DES es inseguro para ciertas aplicaciones debido principalmente a los 56 bits de longitud de su clave, la cual da lugar a un espacio de claves demasiado pequeño. Ya hay ejemplos en los que se logra descubrir claves DES en menos de 24 horas. Además, existen algunos resultados analíticos que ponen de manifiesto algunas de las debilidades de este algoritmo, aunque ninguna de ellas tiene aplicabilidad en ataques reales. Sin embargo, se cree que el algoritmo es seguro cuando se combina consigo mismo para formar el triple-DES, aunque éste también es víctima de algunos ataques de carácter marcadamente teórico. El año 2000 terminó oficialmente el reinado del DES y comenzó el del conocido como Advanced Encryption Standard (AES).

Los orígenes del DES se remontan a principios de la década de los setenta. En 1972, después de llevar a cabo un estudio sobre las necesidades que tenía el gobierno de los EEUU en temas de seguridad informática, el organismo gubernamental de estandarización, entonces llamado NBS (*National Bureau of Standards*) y ahora conocido como NIST (*National Institute of Standards and Technology*), observó que había necesidad de un estándar para el cifrado de informaciones no clasificadas pero sensibles y que fuese utilizable internamente entre las distintas agencias gubernamentales. Por esta razón, el 15 de mayo de 1973, después de haber consultado a la NSA, el NBS lanzó la propuesta para una cifra que cumpliese ciertos rigurosos criterios de diseño. Sin embargo, ninguna de las cifras presentadas resultó adecuada, por lo que se hizo una segunda convocatoria el 27 de agosto de 1974. En esas fechas, IBM envió un algoritmo que resultó ser aceptable según las especificaciones de la NSA. Lo que IBM envió era una cifra desarrollada entre los años 1973 y 1974 y que se basaba en un diseño anterior conocido como Lucifer, del ingeniero Horst Feistel[121].

El 17 de marzo de 1975, el algoritmo DES propuesto por IBM fue publicado en el registro federal. A partir de ese momento se solicitaron comentarios públicos sobre el mismo, y en el siguiente año se celebraron dos reuniones públicas de trabajo para discutir sobre el estándar propuesto. Hubo ciertas

[121]El equipo que en IBM se encargó del diseño criptográfico de la nueva cifra incluía al propio Feistel, además de a Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith y Bryant Tuckerman.

críticas provenientes de diferentes partes, incluyendo las de los pioneros de la criptografía de clave pública Martin Hellman y Whitfield Diffie, que mencionaban la longitud acortada de clave y la presencia de esas misteriosas cajas de sustitución o "S-boxes" como evidencia de la interferencia de la NSA. Existía la sospecha de que el algoritmo había sido secretamente debilitado por la agencia de inteligencia para que sólo ellos, y nadie más, pudiesen leer los mensajes cifrados con el DES. Alan Konheim, uno de los diseñadores del DES, comentó, "*We sent the S-boxes off to Washington. They came back and were all different*."[122] El Comité de Inteligencia del Senado de los EEUU revisó las acciones de la NSA para determinar si se había producido alguna acción inadecuada y en la parte no clasificada de sus conclusiones, en 1978 se publicó[123] que:

> *"En el desarrollo del DES, la NSA convenció a IBM de que era suficiente un tamaño de clave mas pequeño; indirectamente ayudó en el desarrollo de las estructuras de las S-box; y certificó que el algoritmo final DES estaba, en la medida de sus conocimientos, libre de cualquier debilidad estadística o matemática".*

Sin embargo, también se dice en ese informe que:

> *"La NSA no alteró en ningún modo el diseño del algoritmo. IBM inventó y diseñó el algoritmo, tomó todas las decisiones pertinentes acerca de él, y coincidió en que el tamaño de clave acordado era más que adecuado para todas las aplicaciones comerciales para las que el DES había sido pensado".*[124]

Otro miembro del equipo de diseño del DES, Walter Tuchman, dijo literalmente que "*We developed the DES algorithm entirely within IBM using IBMers. The NSA did not dictate a single wire!*"[125]

Las sospechas de algunos que creían en la existencia de debilidades en las cajas de sustitución del DES (S-boxes) quedaron despejadas en 1990, con el descubrimiento y posterior publicación de lo que se conoce como Criptoanálisis Diferencial por parte de Eli Biham y Adi Shamir. Este criptoanálisis es un método general de romper cifradores de bloques. La cajas

---

[122]Ver Schneier. B.; Applied Cryptography. 2nd Ed., p. 280.

[123]Davies, DW; Price WL: *Security for computer networks*, 2nd ed. John Wiley & Sons. 1989.

[124]Robert Sugarman (Editor) "*On foiling computer crime*". IEEE Spectrum, Julio 1979.

[125]P. Kinnucan: *Data Encryption Gurus: Tuchman and Meyer.* Cryptologia **2** (4) Octubre 1978.

de sustitución del DES eran mucho más resistentes a ese ataque que si hubiesen sido elegidas al azar, lo que sugiere que IBM ya sabía de esa técnica en la década de 1970. De hecho, ese fue el caso en 1994 cuando Don Coppersmith publicó los criterios originales de diseño de las cajas S. De acuerdo con Steven Levy[126], los investigadores de IBM descubrieron el criptoanálisis diferencial en 1974 y la NSA les pidió que mantuviesen esa técnica en secreto[127]. Coppersmith explica la decisión de IBM diciendo que "*eso fue porque [el criptoanálisis diferencial] puede ser una herramienta muy potente, utilizada contra varios esquemas, y había la preocupación de que si tal información fuera de dominio público pudiese afectar de forma adversa a la seguridad nacional*." Steven Levy cita a Walter Tuchman diciendo: "*Ellos nos pidieron que marcásemos todos los documentos como confidencial... De hecho, pusimos un número en cada uno de ellos y los guardamos en una caja fuerte, porque estaban considerados como material clasificado del gobierno de los EE. UU. Me pidieron que lo hiciera, de modo que yo lo hice*". El mismo Shamir comentó, "*Yo diría que, al contrario a lo que alguna gente cree, no hay evidencia de alteraciones en el DES que pudiesen debilitar su diseño básico*."

La otra crítica, la de que la longitud de la clave sea corta, se apoyaba en el hecho de que la razón dada por la NSA para reducir la longitud de la clave de 64 bits a 56 era que los otros ocho bits podrían servir como bits de paridad, lo que resulta un tanto sospechoso. Todo el mundo creyó que la decisión de la NSA venía motivada porque posiblemente la agencia había tenido que realizar un ataque por fuerza bruta a claves de 56 bits varios años antes de que lo pudiese hacer el resto del mundo.

A pesar de las críticas, el DES fue aprobado como estándar federal en noviembre del año 1976, y publicado como tal el 15 de febrero de 1977 pasando a ser el FIPS PUB 46, autorizando su uso para todo tipo de datos no clasificados. Más tarde, y de forma reiterada, fue reafirmado como estándar en los años 1983, 1988 (revisado y publicado como FIPS-46-1), 1993 (FIPS-46-2), y de nuevo en 1999 (FIPS-46-3), donde se describe también el uso del "Triple DES". El 26 de mayo del año 2002, el algoritmo DES fue finalmente sustituido por el algoritmo AES (*Advanced Encryption*

[126]**Steven Levy** (1951-) es un periodista norteamericano que ha escrito varios libros sobre ordenadores, tecnología, criptografía, Internet, ciberseguridad, y sobre intimidad. Levy es el redactor jefe en temas de tecnología y editor senior de la revista Newsweek, en cuya sección de "Science & Technology" escribe.

[127]Steven Levy, *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*, 2001, ISBN 0-14-024432-8.

Standard) que fue elegido por el NIST (*National Institute of Standards and Technology*) después de un concurso público que duró dos años[128]. Sin embargo, hoy en día, el DES todavía se utiliza ampliamente dentro del sector financiero. El 19 de mayo de 2005, el estándar FIPS 46-3 fue oficialmente retirado, pero con esto no terminó la existencia del DES ya que el mismo NIST lo había aprobado anteriormente como estándar en el algoritmo Triple DES[129], que lo contiene, y lo consagró hasta el año 2030 para utilizarlo en la protección de información gubernamental sensible. En el año 1994 dio a conocer otro ataque teórico al DES, al cual se le conoce como criptoanálisis lineal, pero realmente fue un ataque por fuerza bruta publicado en 1998 lo que demostró que el DES podía ser atacado en circunstancias prácticas y, por ello, debía ser sustituido por otro algoritmo más resistente.

La aparición del DES fue el inicio y el catalizador del estudio académico, abierto y sostenido, de la criptografía tanto en los métodos para romper cifradores de bloques en general, como en el diseño de alternativas que no hubiesen sido "afectadas" por la NSA u otras agencias gubernamentales[130, 131]. Una gran cantidad de la literatura técnica en criptografía de las décadas de los años 1970 y 1980 tratan del DES; el DES es el estándar con el que cualquier algoritmo de clave simétrica se ha comparado.

---

[128]Ver http://en.wikipedia.org/wiki/AES_process

[129]NIST, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher* Special Publication 800-67 disponible en http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf

[130]William E. Burr: *Data Encryption Standard*, en NIST's anthology "A Century of Excellence in Measurements, Standards, and Technology: A Chronicle of Selected NBS/NIST Publications, 1901-2000", NIST Special Publication 958, David R. Lide Editor. pp. 250-253, disponible en http://nvl.nist.gov/pub/nistpubs/sp958-lide/cntsp958.htm

[131]Bruce Schneier: *Applied Cryptography, Protocols, Algorithms, and Source Code in C*, Second edition, p. 267. John Wiley and Sons, New York 1996.

El nuevo siglo y el *Advanced Encryption Standard*

El AES o *Advanced Encryption Standard*, también conocido como Rijndael, es un cifrador de bloques adoptado como estándar de cifrado por el gobierno de los EEUU. Este algoritmo ha sido y es intensamente analizado, a la vez que es profusamente utilizado en todo el mundo, al igual que le ocurrió a su predecesor el DES. El AES fue elevado por el *National Institute of Standards and Technology* (NIST) al grado de estándar federal en su publicación, como US FIPS PUB 197 (FIPS 197) el 26 de noviembre de 2001, después de un proceso de estandarización que duró cinco años[132]. El AES comenzó a ser estándar el 26 de mayo de 2002 y, hasta el momento, es uno de los algoritmos más populares utilizados en la criptografía de clave simétrica. Este algoritmo ya está presente en muchos productos comerciales de cifrado y/o de comunicaciones.

La cifra fue desarrollada por dos criptógrafos belgas, Joan Daemen y Vincent Rijmen, y enviado al proceso de selección del AES bajo el nombre "Rijndael", resultado de la fusión de los apellidos de sus inventores. El Rijndael proviene del refinamiento de otro algoritmo anterior conocido como Square[133] que, a su vez, era un desarrollo ulterior de otro algoritmo llamado Shark[134]. A diferencia de su antecesor el DES, Rijndael es una cadena de sustitución-permutación, y no una cadena de Feistel. El AES es rápido tanto en software como en hardware, es relativamente simple de implementar y requiere muy poca memoria.

Una cadena de sustitución-permutación, o SP-network (SPN), es una serie de operaciones que consisten en cajas de sustitución (S-boxes) y cajas de permutación (P-boxes) que transforman los bits de los bloques de entrada en los bits de los bloques de salida. Ambas operaciones tienen en común que son bastante eficientes si se ejecutan en hardware. Las S-boxes sustituyen o transforman los bits de la entrada para dar los bits de la salida. Una buena S-box tendrá la propiedad de que, al cambiar un bit de la entrada, cambie de promedio la mitad de los bits de salida (efecto de avalancha). También deberá tener la propiedad de que cada bit de la

[132]Para más detalles ver http://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process

[133]Joan Daemen, Lars Knudsen, Vincent Rijmen: *The Block Cipher Square*. Fast Software Encryption (FSE) 1997, Haifa, Israel. Lecture Notes in Computer Science, Vol. 1267. pp. 149-165 Springer-Verlag. 1997, disponible en *http://homes.esat.kuleuven.be/~cosicart/pdf/VR-9700.PDF*

[134]Vincent Rijmen, Joan Daemen, Bart Preneel, Anton Bosselaers, Erik De Win: The Cipher SHARK . 3rd International Workshop on Fast Software Encryption (FSE '96). Cambridge UK. Springer-Verlag, pp.99-111, Febrero 1996, disponible en http://citeseer.ist.psu.edu/rijmen96cipher.html

salida deberá depender de todos los bits de la entrada. Las cajas de permutación o P-boxes, son las encargadas de permutar o transponer los bits sobre las entradas de las cajas S. Además, en cada vuelta o ciclo del algoritmo, la clave secreta, se combina con el flujo de cómputo con alguna operación que defina un grupo, típicamente el Or exclusivo (entradas distintas implican la salida a uno, entradas iguales, salida nula).

Hasta el momento, los únicos ataques con éxito contra el AES han sido los denominados *side channel attacks*[135]. La National Security Agency (NSA) revisó los quince candidatos[136] del concurso AES, incluido el Rijndael, y declararon que todos ellos son suficientemente seguros para proteger información no clasificada del gobierno de los EEUU. En junio de 2003, el gobierno de los EEUU anunció[137] que el AES puede ser utilizado también para proteger información clasificada:

> *"El diseño y la resistencia de todas las longitudes de clave del algoritmo AES (es decir, 128, 192 y 256 bits) son suficientes para proteger información clasificada hasta el nivel de SECRET. La información clasificada como TOP SECRET requerirá el uso de las claves de 192 o 256 bits. La implementación del AES en productos para proteger los sistemas de seguridad nacional y/o su información deben ser revisados y certificados por la NSA antes de su adquisición y uso."*

[135]Un **ataque por análisis colateral o side channel attack**, es un ataque que se basa en la información que se obtiene de la implementación física de un criptosistema, y no en debilidades teóricas de los algoritmos. Por ejemplo, en la información sobre tiempos de ejecución, consumo de potencia, emisiones electromagnéticas o, incluso, basándose en el sonido que pueda emitir el artefacto cifrador; todo ello puede ser una fuente extra de información utilizable para romper sistemas prácticos y concretos. Muchos de estos ataques requieren considerables conocimientos técnicos sobre la forma de operar por dentro del sistema que implementa la criptografía. Ver http://www.sidechannelattacks.com/

[136]Por orden alfabético fueron: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, Rijndael, SAFER+, Serpent, y Twofish.

[137]Ver http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf

La era digital y primeros límites para la criptografía civil

Con la llegada de la era digital, casi todo cambió completamente. El inicio de esta revolución lo podemos fijar en la llegada de los microprocesadores, que son un componente electrónico programable que incorpora en un único circuito integrado todas las funciones propias de una Unidad Central de Proceso (CPU) clásica. El microprocesador nació al reducir el tamaño de los registros de cálculo de la CPU de 32 bits a sólo 4 bits, de modo que los transistores y las puertas lógicas necesarias para construirla pudiesen caber en un sólo circuito integrado. Los microprocesadores hicieron posibles las microcomputadoras a mediados de los años setenta y con ello se popularizó la capacidad de cómputo y la informática. Antes de esa fecha, las CPUs de los *mainframes* estaban hechas de voluminosos sistemas de conmutación independientes, que más tarde se convirtieron en pequeños circuitos integrados que contenían algunos pocos transistores que adecuadamente conectados daban diferentes puertas lógicas. Con la integración en un solo circuito de millares o millones de transistores, el coste de la capacidad de computación se redujo enormemente. Con la llegada de los circuitos integrados microprocesadores éstos pasaron a ser la forma más frecuente de construir las CPUs, haciendo que prácticamente desapareciera cualquier otra posibilidad.

Con la popularización de la informática, el ciudadano está más capacitado para desarrollar y analizar aplicaciones y sistemas cada vez más complejos que cada día resultan más necesarios en el desarrollo de todo tipo de funciones en la sociedad de la información. Por ello, en 1984 el Congreso norteamericano sacó la ley *Computer Fraud and Abuse Act*, cuyo objetivo era reducir las actividades de "*hacking*"[138] sobre los sistemas de ordenadores que cada vez eran más frecuentes en todo tipo de actividades. Esta ley convierte en crimen acceder de forma no autorizada a un ordenador o sistema de ordenadores. La ley, sin embargo, en su forma original no afectaba a hackers juveniles que no tenían una intención clara de cometer otros delitos. Esta ley fue enmendada para actualizarla y endurecerla en los años 1994 y 1996. Una nueva enmienda data 2001 que se corresponde con la muy controvertida PATRIOT Act del 26 de octubre de 2001.

[138]En el contexto de la seguridad, un Hacker es alguien involucrado en la seguridad/inseguridad de los ordenadores, que se especializa en el descubrimiento de fallos en el sistema tanto para utilizarlos contra dicho sistema, como para enmendarlos, o que se dedica a conseguir o evitar el acceso no autorizado al sistema gracias a sus conocimientos, tácticas y conocimiento detallado del sistema en cuestión.

La Web

A las puertas de la última década del siglo XX, en 1989, Timothy John Berners-Lee (1955-) y Robert Cailliau (1947-) construyeron un prototipo que terminaría siendo lo que hoy conocemos como la *World Wide Web*[139] en la división de Sincrotrón de Protones del CERN[140] en Ginebra, Suiza. La *World Wide Web*, comúnmente conocida como La Web, es un sistema de documentos de hipertexto interconectados entre sí, que son accesibles a través de Internet. Con un navegador Web, cualquier usuario ve páginas Web que pueden contener textos, imágenes, vídeos, y cualquier otro material multimedia, y puede navegar, de página en página, utilizando los *hyperlinks* contenidos en cada una de ellas.

Desde el principio, Berners-Lee ha jugado un papel muy activo en el desarrollo de los estándares Web, tales como el de los lenguajes de *markup* con el que están compuestas la páginas Web, y en años recientes ha defendido su visión de la Web Semántica. Berners-Lee es también director del *World Wide Web Consortium* que supervisa continuamente el desarrollo de la Web, y es investigador principal y titular de la cátedra de 3Com en el MIT *Computer Science and Artificial Intelligence Laboratory* (CSAIL). El pasado día 20 de febrero de 2007, Bernes-Lee recibió el premio Charles Stark Draper, un premio que tiene una dotación de 500.000 dólares y que está considerado "el Premio Nobel de la ingeniería".

La llegada de la Web y de Internet ha permitido la deslocalización de todos los elementos de una red de comunicaciones o de negocio, lo que supone un cambio radical en el enfoque de la seguridad de estos sistemas. Los perímetros físicos han desaparecido, las jurisdicciones se desvanecen, las soberanías pierden cualquier sentido e, incluso, la propiedad intelectual se marchita inexorablemente. La nueva seguridad de sistemas tendrá que construirse con planteamientos muy distintos a los que se había seguido en el imperio de los *mainframes* y de los ordenadores caros.

---

[139]Ver http://www.w3.org/History/1989/proposal.html

[140]**CERN** es el **Centro Europeo para la Investigación Nuclear** (*Centre Européenne pour la Recherche Nucléaire*), es el mayor laboratorio mundial de física de partículas, y está situado al noroeste de Ginebra, en la frontera entre Francia y Suiza.

El PGP

Por si la Web no fuese suficiente para cambiar la fisonomía del panorama computacional a principios de la década de 1990, en 1991 Phil Zimmermann creó la primera versión de un software de cifrado que llamó PGP, como acrónimo de "*Pretty Good Privacy*", que eligió con cierta ironía inspirándose en el nombre un supermercado llamado "*Ralph's Pretty Good Grocery*"[141], que aparecía en una ciudad de ficción llamada Lake Wobegon que, por aquellos tiempos, recreaba en la radio pública de Minnesota. La ironía radica en su pretensión de que la seguridad del PGP no sólo fuese buena, sino *pretty good*, excelente. Esta primera versión incluía un algoritmo de clave simétrica que había diseñado el propio Zimmermann, al que llamó BassOmatic[142]. Zimmermann ha sido durante mucho tiempo un activista anti-nuclear y, según él, creó el PGP para que gentes con sus mismas inclinaciones pudiesen utilizar con seguridad los tablones de las BBS[143] para almacenar e intercambiar mensajes y ficheros. El PGP no requería licencia alguna para su uso no comercial, ni tenía siquiera un precio formal, y se entregaba con él el código fuente completo. PGP empezó haciéndose popular en Usenet y de ahí a toda la Internet, con lo que rápidamente adquirió una gran popularidad en todo el mundo. Entre sus usuarios y gente que lo apoya, hay disidentes políticos, activistas de los derechos civiles en muchas partes del mundo y, muy especialmente, activistas de las "comunicaciones libres" que se denominaban a sí mismos *cypherpunks*.

---

[141]El eslogan de Ralph's Pretty Good Grocery era "*If you can't find it at Ralph's, you can probably get along without it*".

[142]Este nombre se explica en un comentario que aparece en el código fuente: "*BassOmatic gets its name from an old Dan Aykroyd Saturday Night Live sketch involving a blender and a whole fish. The BassOmatic algorithm does to data what the original BassOmatic did to the fish*."

[143]Un **Bulletin Board System**, o **BBS**, es un ordenador o sistema de ordenadores ejecutando un software que permite a sus usuarios conectarse con el sistema a través de una línea telefónica (o Telnet), y utilizando un programa emulador de Terminal, permite descargarse software y datos, subir datos a la BBS, leer noticias, e intercambiar mensajes, como si fuesen notas en un tablón de anuncios, con otros usuarios. **Community Memory** fue el primer tablón público de anuncios o BBS. Se montó en 1973 en Berkeley, California, y utilizaba un ordenador de tiempo compartido SDS 940 en San Francisco conectado a través de un enlace de 110 baudios a un teletipo en un archivo en Berkeley permitiendo a los usuarios dejar y recoger mensajes.

Poco después de su puesta en circulación, el PGP logró salir de los Estados Unidos de una forma muy peculiar, por lo que en febrero de 1993 Zimmermann se convirtió en el objetivo de una investigación criminal del gobierno norteamericano por "*la exportación de municiones sin licencia*"[144]. Por aquel entonces, a los criptosistemas con claves más largas de 40 bits se les consideraba municiones de guerra según la definición de las regulaciones de exportación de los EE. UU., y el PGP nunca ha utilizado claves más cortas de 128 bits. Las penas por la violación de esas normas eran y son muy duras. Después de varios años, la investigación fue cerrada sin haber encontrado cargos que imputar a Zimmermann o a cualquier otro.

Zimmermann esquivó las regulaciones de un modo original; publicó todo el código fuente del PGP impreso en forma de libro, a través de MIT Press, y éste se distribuyó y vendió profusamente fuera de los Estados Unidos. Cualquiera que quisiese crearse su propia copia de PGP podía comprarse el libro por 60 dólares, quitarle las tapas, separar la páginas, escanearlas y, utilizando un programa de OCR, crear un conjunto de ficheros de texto con el código fuente. A partir de ahí, uno podía hacerse la aplicación utilizando el compilador C de GNU, que sigue siendo accesible y de libre uso. De este modo, el PGP consiguió estar disponible en cualquier parte del mundo. El argumento era sencillo: la exportación de municiones, fusiles, bombas, aviones, y software criptográfico, etc., eran y siguen siendo materia restringida; pero en EEUU la exportación de libros está protegida por la Primera Enmienda de la Constitución norteamericana. Este razonamiento nunca llegó a ser utilizado ante los tribunales en el caso del PGP, pero si se hizo ante la Corte Suprema de los EEUU en el caso Bernstein. Desde el año 2000, el PGP no satisface la definición de armamento no exportable, y puede exportarse a todo el mundo excepto a siete países en concreto y a una lista de individuos y grupos determinados.

Durante el periodo de investigación criminal, el equipo de Zimmermann trabajó en una nueva versión del PGP a la que llamaron PGP 3. Esa versión tenía importantes mejoras, incluyendo una nueva estructura de certificado que subsanaba pequeños fallos de seguridad presentes en los certificados de las versiones PGP 2.x. Más aún, con la experiencia en patentes y problemas de exportación en mente, sus autores se abstuvieron de utilizar

---

[144]El software de cifrado tambien puede considerarse munición. Hasta 1996, *International Traffic in Arms Regulations* del gobierno de los EEUU prohibía la exportación de cualquier cosa que fuese criptográficamente más resistente que un cifrado simétrico de 40-bit (ver http://en.wikipedia.org/wiki/40-bit_encryption).

cualquier cosa que estuviese patentada. El PGP 3 introdujo el uso del CAST-128, también conocido como CAST5, como algoritmo simétrico de cifrado, el esquema de firma DSA y el criptosistema asimétrico ElGamal que no estaban afectados por ningún tipo de patentes.

Después de que terminase la investigación federal en 1996, Zimmermann y su equipo iniciaron una compañía para producir nuevas versiones del PGP. Se fusionaron con Viacrypt, a quienes Zimmermann había vendido los derechos comerciales y que además tenían la licencia para usar el algoritmo RSA directamente de RSADSI. La nueva empresa adoptó el nombre de PGP Incorporated. El nuevo equipo empezó a trabajar en las siguientes versiones del PGP, tomando como base el PGP 3. A diferencia del PGP 2 que era un programa de línea de comando exclusivamente, el PGP 3 fue diseñado, inicialmente, como una librería de software, permitiendo así a los usuarios trabajar desde línea de comando o dentro de un entorno gráfico GUI. El acuerdo original entre Viacrypt y el equipo de Zimmermann fue que Viacrypt tendría las versiones pares del PGP y Zimmermann las impares. Así, Viacrypt, creó una nueva versión, basada en PGP 2, que llamó PGP 4. Para evitar la confusión de que el PGP 3 fuese el sucesor del PGP 4, aquel fue renombrado y lanzado como PGP 5 en el mes de mayo de 1997.

El PGP de código abierto

Dentro de PGP Inc., todavía había cierta preocupación por el tema de las patentes. RSADSI adoptó una actitud desafiante en cuanto a la continuación de la licencia RSA de Viacrypt en la nueva firma. La compañía adoptó un estándar interno informal que llamaron "*Unencumbered PGP*": "*Utiliza algoritmos sin problemas de licencias*". Debido a la importancia del PGP en el mundo (se piensa que es el sistema más ampliamente elegido por su calidad criptográfica), muchos querían escribir su propio software que pudiese interoperar con el PGP 5. Zimmermann terminó convenciéndose de que era necesario, para ellos y para la comunidad criptológica en general, definir un estándar abierto para el PGP.

En el mes de julio de 1997, PGP Inc. propuso al IETF (*Internet Engineering Task Force*) un estándar llamado OpenPGP, y les permitieron utilizar el nombre de OpenPGP para describir ese nuevo estándar. El IETF aceptó la propuesta e inició las actividades del grupo de trabajo OpenPGP.

OpenPGP está en el Internet Standards Track. La especificación actual es el RFC 2440 (Julio 1998). OpenPGP está todavía en desarrollo activo y el sucesor del RFC 2440, que es el RFC 4880, se ha convertido en propuesta de estándar.

La *Free Software Foundation* ha desarrollado su propio programa OpenPGP-compliant llamado GNU Privacy Guard (abreviado como GnuPG o GPG). GnuPG está libremente disponible junto con todo su código fuente bajo licencia GNU General Public License (GPL).

Retos y resistencia del algoritmo RSA

Contemporáneo con la aparición del PGP, se puso en marcha lo que se conoce como la RSA Factoring Challenge, que fue un reto lanzado por los Laboratorios RSA el 18 de marzo de 1991, para animar a investigar en los aspectos computacionales de la teoría de los números, en la dificultad práctica de factorizar grandes números enteros del tipo de los utilizados en el algoritmo de clave pública RSA. Como reto se publicó una lista de números semiprimos, que son números con exactamente dos factores primos y también conocidos como números RSA, junto con unos premios en metálico a entregar por la correcta factorización del alguno de ellos. El más pequeño de ellos tiene 100 dígitos decimales, se le llama RSA-100 y fue factorizado en unos pocos días, pero muchos de los grandes números están todavía por factorizar y es probable que sigan así mucho tiempo.

Los primeros retos de RSA, desde el RSA-100 al RSA-500, fueron etiquetados de acuerdo con sus longitudes en dígitos decimales; más tarde, sin embargo, a partir del RSA-576, lo que se cuentan son los bits binarios que los representan. Algunas excepciones son los números RSA 640, 704, 768, 896, etc., que fueron creados antes de que se cambiase el sistema de numeración.

El reto RSA se dió por terminado[145] el año 2007 ya que, según RSA, "*Now that the industry has a considerably more advanced understanding of the cryptanalytic strength of common symmetric-key and public-key algorithms, these challenges are no longer active*"[146]. El último reto superado con éxito, el 5 de noviembre de 2005, es el RSA-640 que tiene 193 dígitos decimales[147].

---

[145]Ver http://www.rsa.com/rsalabs/node.asp?id=2092

[146]Ver http://www.rsa.com/rsalabs/node.asp?id=2094

[147]**RSA-640** =
3107418240490043721350750035888567930037346022842727545720161948823206440518808150455634682967172328678243791627283803341547107310850191954852900733772482278352574238645401469173660247765234660 9 = 16347336458092538484431338838650908598417836700 3 309231218111085238933310010450815121211816751157 9x1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

El texto "*The Magic Words are Squeamish Ossifrage*" fue la solución de un reto propuesto por los inventores de la cifra RSA en 1977. El problema apareció en la columna de Martin Gardner, *Mathematical Games*, de la revista *Scientific American*. Fue resuelto en el periodo de 1993-1994 por un gran conjunto de ordenadores trabajando coordinadamente bajo la dirección de Derek Atkins, Michael Graff, Arjen Lenstra y Paul Leyland. Mas de 600 voluntarios contribuyeron con tiempos de CPU de aproximadamente 1.600 máquinas, dos de las cuales fueron máquinas de fax, durante un periodo de tiempo de seis meses. La coordinación se llevó a cabo a través de Internet y este fue uno de los primeros proyectos de computación cooperativa distribuida de la historia.

La dificultad de romper el cifrado RSA, es decir, de recuperar un texto en claro dado un criptograma y la clave pública con la que se cifró, está relacionado con la dificultad de factorizar números enteros grandes, pero no se sabe si realmente ambos problemas son matemáticamente equivalentes; la factorización es actualmente el único método de romper el RSA. El descifrado del criptograma de 1977 supuso factorizar un número con 129 dígitos decimales, el RSA-129[148], con objeto de recuperar su texto en claro.

Ron Rivest estimó en 1977 que la factorización de un número con 125 dígitos requeriría del orden de 40×10^{15} años, es decir, 40 Peta-años, incluso con la muy conservadora suposición de que una multiplicación modular pudiese hacerse en tan sólo un nanosegundo. Por este motivo, Rivest creía que el reto RSA-129 nunca sería roto en la práctica. Sin embargo, Rivest falló porque no tuvo en cuenta la posibilidad de que los algoritmos de factorización mejoraran sustancialmente, tal y como lo hicieron en las décadas siguientes. Atkins et al., utilizaron el algoritmo conocido como de la criba cuadrática, el más eficiente en aquellos días e inventado por Carl Pomerance en 1981. La técnica que representa el algoritmo conocido como *number field sieve*, que era asintóticamente más rápido, había sido inventado recientemente y no estaba claro cuando podría superar a la criba cuadrática para números de 129 dígitos o mas. Los requisitos de memoria del nuevo algoritmo también eran algo que preocupaba pero, actualmente este último algoritmo es el más rápido que se conoce para factorizar números realmente grandes.

---

[148] **RSA-129** =
1438162575788886766923577997614661201021829672124236256256184293570693524
573389783059712356395870505898907514759929002687954354 1 =
3490529510847650949147849619903898133417764638493387843990820577 *
3276913299326670954996198819083446141317764296799294253979828853 3

El SSL y las comunicaciones Web cifradas

Poco después de que se iniciase la andadura del PGP, apareció en escena el protocolo conocido como *Transport Layer Security* (TLS) y su predecesor, *Secure Sockets Layer* (SSL). Ambos son protocolos criptográficos para el establecimiento de comunicaciones seguras sobre Internet, y se utilizan para montar otros servicios como son la navegación Web, el e-mail, el fax por Internet, la mensajería instantánea y otras transferencias de datos. Hay ligeras diferencias entre SSL y TLS, pero el protocolo es esencialmente el mismo.

El protocolo SSL fue desarrollado originalmente por Netscape. La versión 1.0 nunca se hizo pública; la versión 2.0 se lanzó en el año 1994 pero contenía cierto número de fallos de seguridad que, en última instancia, dieron lugar al protocolo SSL versión 3.0 que se hizo público en 1996. Esta última versión es la que sirvió de base para el protocolo TLS versión 1.0. La IETF definió por primera vez el protocolo en el documento RFC 2246 en enero de 1999. Empresas como Visa, MasterCard, American Express y muchas otras instituciones financieras utilizan el SSL para su mercadeo a través de Internet. Las conexiones *http* seguras, las conocidas como *https*, son las que permiten actualmente el incipiente comercio electrónico que se observa en Internet.

Algunas de las primeras implementaciones del SSL utilizaban claves simétricas de 40 bits porque las restricciones que el gobierno de los EE. UU. imponía a la exportación de tecnología criptográfica así lo exigían. El gobierno norteamericano impuso explícitamente el límite de 40 bits en el tamaño del espacio de claves, porque éste era lo suficientemente pequeño como para poderlo romper mediante búsquedas por fuerza bruta, y éstas son prácticamente realizables sólo en agencias de investigación nacionales que quisiesen leer el tráfico cifrado. A su vez, éste tamaño aún presentaba, en 1996, obstáculos serios a oponentes peor financiados. Las antiguas limitaciones a claves de 40 bits prácticamente han desaparecido, y las implementaciones modernas utilizan claves de 128-bits o más, para las cifras simétricas.

Primeros ciber-delitos

La década de los noventa fue la época en que Internet se hizo realmente popular para el ciudadano común americano y, lo que es quizás más interesante, tambien para las empresas y comercios occidentales que ven en la nueva red una cornucopia de beneficios.

Fue por aquel entonces cuando Vladimir Levin, un ciudadano ruso, se hizo famoso por haber participado en un intento de transferencia fraudulenta de 10,7 millones de dólares a través de los ordenadores del Citibank. Corría el año 1994. En su momento, los medios de comunicación dijeron que Vladimir era una especie de matemático y que tenía una licenciatura en bioquímica del Instituto Estatal de Tecnología de San Petersburgo.

De acuerdo con las noticias de 1994, Levin logró acceder a las cuentas de varios grandes clientes corporativos del Citibank a través del sistema de transferencia de fondos del banco que operaba sobre redes telefónicas (*el Financial Institutions Citibank Cash Manager*) y después transfirió fondos hacia cuentas abiertas por sus cómplices en Finlandia, Estados Unidos, Holanda, Alemania e Israel.

Tres de esos cómplices fueron arrestados cuando intentaban sacar dinero de las cuentas en Tel Aviv, Rotterdam y San Francisco. Tras el interrogatorio de los cómplices, la investigación se centró en Levin que, por aquel entonces, trabajaba como programador en la compañía de ordenadores AO Saturn con sede en San Petersburgo. En 1994 no había tratados de extradición entre los EE.UU. y Rusia para ese tipo de delitos, por lo que hubo que esperar hasta el mes de marzo de 1995 para que Levin fuese detenido por agentes de Scotland Yard en el aeropuerto de Stansted de Londres mientras hacia escala técnica en un viaje desde Moscú. Los abogados de Levin apelaron contra la extradición de su cliente a los EE.UU., pero fue ésta rechazada por la Cámara de los Lores en el mes de junio del año 1997. Levin fue entregado a los norteamericanos en el mes de septiembre de ese mismo año y fue procesado en la Corte del Distrito Sur de Nueva York. Levin aceptó un acuerdo con el tribunal por el que admitió los cargos de conspiración y fraude, y de haber robado 3,7 millones de dólares norteamericanos. En febrero del 1998 fue condenado a tres años de prisión, y a pagar una indemnización de 240.015 dólares. El Citibank declaró que había conseguido recuperar todo lo sustraído (10,7 millones de dólares) excepto 400.000 dólares.

Después de los enormes problemas ocasionados por sus sistemas, el Citibank los actualizó, sin embargo, nunca se hizo público cómo Levin había logrado conocer los detalles necesarios para entrar a las cuentas

relevantes. Tras su arresto en 1995, miembros anónimos de grupos de hackers de San Petersburgo declararon que Levin no tenía las habilidades técnicas necesarias para entrar en los sistemas del Citibank, que habían sido ellos los que habían conseguido los accesos dentro de las redes del banco, y que ellos también habían vendido a Levin esa información por 100 dólares.

En el año 2005, un autodeclarado miembro de un antiguo grupo hacker de San Petersburgo, dijo que él fue uno de los que originalmente lograron entrar en los sistemas del Citibank y publicó en provider.net.ru (un servidor ruso muy popular que se dedica al mercado de las telecomunicaciones) y bajo el seudónimo de ArkanoiD, un memorando en el que relataba sus actividades delictivas. Según ese documento, Levin realmente no era ni matemático, ni bioquímico ni nada por el estilo, sino un simple administrador de sistemas que se las arregló para conseguir los datos necesarios para entrar en los sistemas del Citibank y saber cómo utilizarlos.

ArkanoiD hizo hincapié en que todas las comunicaciones se hacían sobre redes X.25 y que Internet no estaba involucrada en los hechos. El grupo de ArkanoiD descubrió en 1994 que los sistemas del Citibank estaban desprotegidos y dedicaron varias semanas a examinar, desde lejos, la estructura del banco norteamericano. Miembros del grupo estuvieron jugando aquí y allá con herramientas del sistema, llegaron a instalar y ejecutar juegos, y no fueron detectados por el personal del banco. Los atacantes, por su propia seguridad, no tenían planeado cometer un robo y cesaron en sus actividades en cierto momento. Mas tarde, uno de ellos entregó los datos críticos de acceso a Levin a cambio de los mencionados cien dólares.

El nacimiento de las funciones Hash

Además del cifrado, uno de los atributos que empezó a cobrar más importancia para el comercio electrónico y cualesquiera otras relaciones oficiales a través de Internet, fue el de integridad, la autenticidad y el no repudio. Para construir estas primitivas criptográficas es necesario disponer de funciones de sentido único conocidas como funciones Hash. Aunque había otras posibilidades dentro de la comunidad criptográfica internacional, la administración norteamericana, a través de su laboratorio de estandarización, el NIST, diseñó un sistema de firma digital que incluía una función Hash cuya especificación original es de 1993 y cuyo nombre fue *Secure Hash Standard*.

Hoy en día, a esa primera versión se la conoce como SHA-0; fue retirada oficialmente por la propia NSA poco después de su publicación, para ser sustituida por una versión revisada, publicada en 1995 como el FIPS PUB 180 y comúnmente conocida como SHA-1. La función SHA-1 sólo se diferencia de la SHA-0 en una única rotación binaria ubicada en la planificación de los bloques de mensaje procesados en su función de compresión. La corrección del diseño original se hizo así, de acuerdo con la NSA, para corregir un fallo del algoritmo original que reducía la seguridad criptográfica del conjunto. Sin embargo, la NSA no ha dado ninguna otra explicación al respecto, ni tampoco ha identificado el fallo que se había corregido.

Con posterioridad, se han publicado varias debilidades tanto en la función SHA-0 como en la SHA-1. El algoritmo SHA-1 parece tener una mayor resistencia a los ataques estudiados, coincidiendo esto con la afirmación de la NSA de que ésta nueva versión es más robusta y segura.

La función SHA-1 (al igual que la SHA-0) produce resultados de 160 bits para cualquier mensaje de entrada con longitudes hasta $(2^{64} - 1)$ bits, y se basa en principios muy similares a los utilizados por Ronald L. Rivest en el diseño de las funciones Hash MD4 y MD5.

La quimera de la protección de contenidos multimedia

Al final del siglo XX vuelve a saltar a la actualidad el tema de la protección de la propiedad intelectual de los materiales multimedia. En ocasiones anteriores, la batalla había sido eminentemente legal ya que los procedimientos de copia y, sobre todo, de distribución de las mismas eran bastante lentos y poco eficaces. Sin embargo, con la llegada de Internet y la era digital, la capacidad de copia es, a todos los efectos, literal y la distribución es instantánea y universal.

Para afrontar este riesgo, las compañías dedicadas a la explotación del mercado multimedia y del entretenimiento se entregaron a la tarea de proteger "criptográficamente" sus mercancías, intentando así hacer imposible la copia y volver inútil su distribución. Esto es lo que se pretendió al incluir el "cifrado" en el estándar de los DVDs y dividir en tres "regiones" el planeta para cuestiones de distribución. Sin embargo, algo debió ir mal ya que no tardó en aparecer, concretamente en 1999, el DeCSS que es un sencillo programa de ordenador capaz de descifrar el contenido de los DVDs en los que se protege sus datos cifrándolos con el *Content-Scrambling System* (CSS).

El DeCSS fue concebido por tres personas, dos de ellas todavía hoy desconocidas. El programa fue difundido en la lista de correo en Internet,

LiViD, en octubre de 1999, y el único miembro conocido del trío de programadores noruegos que lo gestó es Jon Lech Johansen, cuya casa fue asaltada en el año 2000 por la policía noruega. Siendo todavía un adolescente en aquel tiempo, Johansen fue llevado ante los tribunales noruegos acusado de violar la sección 145 del código penal noruego, lo que podría suponer una pena de dos años de cárcel y cuantiosas multas pero, finalmente, a principios de 2003 fue absuelto de todos los cargos. Sin embargo, el 5 de marzo de 2003, una corte de apelación noruega estableció que Johansen debía volver a ser juzgado. El tribunal dijo que los argumentos presentados por la acusación así como otras evidencias adicionales merecían la celebración de otro juicio sobre el mismo asunto. El 22 de diciembre de 2003, la corte de apelaciones acordó la absolución, y en 5 de enero del año 2004 la Norway's Økokrim (Unidad de Crimen Económico) decidió no llevar el caso mas lejos.

El programa DeCSS fue distribuido por primera vez el 6 de octubre de 1999 cuando Johansen envió un anuncio del DeCSS 1.1b - una aplicación de código cerrado para el sistema operativo Windows que servía para el vaciado de DVDs (DVD ripping) - a la lista de correo livid-dev. El código fuente fue liberado hacia finales de ese mismo mes. La primera entrega del DeCSS estuvo precedida por otro programa llamado DoD DVD Speed Ripper creado por un grupo hacker moscovita autodenominado Drink or Die (1993-2001), que no incluyó el código fuente y que aparentemente no funcionaba con todos los DVDs. Drink or Die informó de que había tenido que recurrir a desensamblar el código del *player* de la compañía Xing para obtener la clave criptográfica que necesitaba. El grupo que escribió el DeCSS y del cual formaba parte Johansen se llamaba *Masters of Reverse Engineering*. Este grupo podría haber obtenido ciertas informaciones del grupo Drink or Die[149].

El programa DeCSS era un proyecto colaborativo en el que Johansen sólo escribió la interfaz gráfica del usuario. Cuando se liberó el código fuente de la aplicación DeCSS, se hizo público también el algoritmo CSS. Los expertos pronto percibieron que el algoritmo podía ser vencido por un ataque por fuerza bruta, algo muy distinto a los que hacía el DeCSS, que utilizaba una clave secreta auténtica. El cifrado empleado en el CSS es sólo de 40 bits, y no utiliza todas las posibles claves; en 1999, cualquier ordenador de alta gama, ejecutando código optimizado era capaz de encontrar una clave válida por fuerza bruta en 24 horas.

[149]Ver http://www.lemuria.org/DeCSS/dvdtruth.txt

Programadores de todo el mundo crearon cientos de programas equivalentes al DeCSS, algunos sólo para demostrar lo fácilmente que uno podía saltarse el sistema de protección CSS, y otros para añadir funcionalidades para DVDs en sus reproductores en software de código abierto. Las restricciones de licencia del CSS hacen imposible crear legalmente una implementación de código abierto, y los *drivers* de código cerrado no están disponibles para algunos sistemas operativos, por lo que algunos usuarios necesitan la aplicación DeCSS para ver películas de DVD en sus equipos. A principios del año 2000, se desarrolló un programa con el mismo nombre pero con un propósito completamente distinto (eliminar las etiquetas de *Cascading Style Sheets* de un código HTML). Se animó a la gente a mantener accesibles copias de ese programa en sus sitios Web con el objeto dificultar la tarea de los agentes anti-DeCSS en su empeño de encontrar y eliminar el programa DeCSS real[150].

La criptografía de clave pública

Durante toda la historia de la criptografía simétrica, la clave debía permanecer absolutamente secreta y ser acordada previamente utilizando algún método seguro, no criptográfico, para establecerla; por ejemplo, mediante el encuentro físico de los futuros comunicantes, o a través de un correo de confianza, etc. Sin embargo, son muchas e importantes las dificultades asociadas a estas soluciones clásicas para la distribución de claves. La criptografía de clave pública se inventó con el objetivo de superar dichas dificultades y deficiencias, y con ella los comunicantes pueden serlo a través de canales seguros, montados sobre sistemas de transporte o comunicación esencialmente inseguros, sin que para ello hayan tenido que acordar previamente las claves simétricas que van a utilizar en sus comunicaciones.

En 1874, en el libro "*The Principles of Science: A Treatise on Logic and Scientific Method*"[151] de William Stanley Jevons, se describe una interesante relación entre las funciones de sentido único y la criptografía. En dicho libro se señalaba específicamente el problema de la factorización de números como un ejemplo concreto de función de sentido único y resulta que ésta, la factorización, es la función con puerta trasera, la *trapdoor function*, en la que se basa el algoritmo RSA. En Julio de 1996, Solomon W Golom se refería a ese libro del Jevons del siguiente modo[152]:

[150]Ver http://www.pigdog.org/decss/

[151]William Stanley Jevons: *The Principles of Science: A Treatise on Logic and Scientific Method*. Macmillan & Co., London. 1874. 2nd ed. 1877. 3rd ed., 1879. Reimpreso con un prólogo de Erns Nagel, por Dover Publications, New York, NY, 1958.

[152]Solomon W. Golomb: *On Factoring Jevons' Number*, Cryptologia No. 243 Julio 1996.

> *"In his book The Principles of Science: A Treatise on Logic and Scientific Method, written and published in the 1890s, William S. Jevons observed that there are many situations where the 'direct' operation is relatively easy, but the 'inverse' operation is significantly more difficult. One example mentioned briefly is that enciphering (encryption) is easy while deciphering (decryption) is not. In the same section of Chapter 7: Introduction titled "Induction an Inverse Operation", much more attention is devoted to the principle that multiplication of integers is easy, but finding the (prime) factors of the product is much harder. Thus, Jevons anticipated a key feature of the RSA Algorithm for public key cryptography, though he certainly did not invent the concept of public key cryptography".*

En el mes de mayo del año 1976, Whitfield Diffie (1944-) y Martin Hellman (1945-) publicaron el artículo titulado N*ew Directions in Cryptography*. En ese escrito se presenta un método radicalmente nuevo que hizo avanzar mucho en la solución de uno de los problemas fundamentales de la criptografía: la distribución de claves criptográficas. A ese método se le conoce hoy como el protocolo de intercambio de claves de Diffie-Hellman. Los argumentos esgrimidos en el artículo también sirvieron de estímulo para el inmediato desarrollo público de una nueva clase de algoritmos de cifrado que se conocen como algoritmos de clave asimétrica.

Antes de esta fecha, todos los algoritmos modernos de cifrado habían sido algoritmos de clave simétrica, en los que la misma clave criptográfica se utiliza tanto en la operación de cifrado como en la de descifrado, por lo que el destinatario y el remitente del mensaje cifrado deben conocer la misma clave, y mantenerla en estricto secreto. Todas las máquinas electromecánicas utilizadas en la Segunda Guerra Mundial y la Guerra Fría entran dentro de esta categoría.

Necesariamente, la clave de cada uno de estos sistemas simétricos tiene que ser intercambiada entre las partes comunicantes de algún modo seguro antes de que el sistema pueda utilizarse. La expresión usualmente utilizada es la de enviarlo "*a través de un canal seguro*", como pueden ser un correo de confianza al que se le encadena un maletín a su cintura, o un encuentro cara a cara, o mediante una paloma mensajera. Este requisito no es trivial y pronto se convierte en un problema inmanejable si el número de pares comunicantes aumenta, o si no hay canales seguros para el intercambio de claves, o si las cosas se hacen bien y la clave criptográfica se cambia muy a menudo. Si el mensaje tiene que ser seguro respecto a otros usuarios del sistema, es necesario establecer una clave distinta para cada par de usuarios, y ese número crece con el cuadrado del

número de usuarios dentro del sistema[153]. El protocolo Diffie-Hellman (D-H) de intercambio de claves y todas sus mejoras y variantes, hace la operación de los sistemas de clave simétrica mucho más sencilla y segura de lo que jamás antes habían sido.

En contraste con los sistemas simétricos, los sistemas de cifrado de clave asimétrica utilizan un par de claves distintas y matemáticamente relacionadas entre si, en la que una de ellas se utiliza como clave del algoritmo de cifrado y la otra en el de descifrado. Los sistemas que tienen interés criptográfico son aquellos que, además, también tienen la propiedad de que una de las dos claves no puede ser deducida de la otra por ningún método conocido que mejore el de prueba y error; es decir, por fuerza bruta.

Con este tipo de algoritmos sólo se necesita una clave por miembro del sistema ya que haremos que la clave no deducible actúe como clave privada, siempre en secreto y sólo conocida por su usuario titular, y que la otra sea la clave pública, siempre disponible para quien pueda estar interesado. En este caso la clave es pública, por lo que no es necesario el uso de canales seguros de comunicación para ningún tipo de intercambio. En tanto que la clave privada permanezca bien custodiada y en secreto, y que la clave pública esté ampliamente difundida y disponible, no hay riesgo alguno en utilizar la misma clave durante largos periodos de tiempo.

Para que puedan comunicar de forma segura dos usuarios de un sistema de clave asimétrica sobre un canal de comunicaciones inseguro, cada uno de ellos debe conocer bien su propio par de claves, la pública y la privada, así como la clave pública auténtica del otro comunicante. Esas claves públicas no tienen porque ser específicas para esa comunicación sino que pueden haberse estado utilizando durante años con otros usuarios del sistema.

En un escenario en el que se precisa confidencialidad y autenticidad, al principio los comunicantes intercambian sus claves públicas sin cifrar y sobre un canal de comunicaciones inseguro. Luego cada uno cifra su mensaje utilizando su clave privada, y lo que resulta de ello lo cifra con la clave pública del otro. El resultado, doblemente cifrado, se envía a su destino a través de cualquier canal de comunicación. Al llegar a destino, el receptor lo descifra con su clave privada, y lo que resulta de ello, lo cifra con la clave pública del presunto remitente. Si después de esto se obtiene un mensaje reconocible, el destinatario puede estar seguro de que

[153]El número de pares distintos que se pueden formar en un conjunto con n elementos es $\mathbf{n(n-1)/2 \approx n^2}$.

el mensaje realmente proviene de alguien que conoce la clave privada del remitente, y cualquiera que esté espiando en el canal de comunicaciones necesitaría las claves privadas de ambos comunicantes para poder entender los mensajes intercambiados. Sin embargo, este caso sólo es posible con sistemas asimétricos del tipo RSA, pero no ofrecen ninguna prueba sobre quien es cada uno de los comunicantes, no hay identificación ni no-repudio.

Los algoritmos asimétricos basan su efectividad en la existencia de una clase de problemas matemáticos que se denominan *funciones de sentido único*, las cuales se caracterizan por requerir un esfuerzo computacional relativamente pequeño si se evalúan en un sentido, pero que requieren inmensas potencias de cálculo para poder ser invertidas. Un ejemplo clásico de función de sentido único es, como ya hemos mencionado, la multiplicación de dos números enteros. Es realmente fácil y rápido multiplicar dos grandes números primos, pero es muy difícil factorizar el resultado de ese producto en los dos factores que lo componen. Debido a las propiedades matemáticas de las funciones de sentido único, la mayoría de las posibles claves son malas elecciones desde el punto de vista criptográfico, solo una pequeña fracción de todas ellas, y con una longitud dada, son adecuadas; es por esto que los algoritmos asimétricos requieren el uso de claves muy largas para conseguir el mismo nivel de seguridad que la claves simétricas mucho mas cortas. La necesidad de generar simultáneamente ambos elementos del par de claves, y el mismo hecho de realizar las operaciones de cifrado y descifrado, hace que los algoritmos asimétricos sean computacionalmente muy pesados, sobre todo si se les compara con la mayoría de los sistemas simétricos.

Lo que realmente se hace es utilizar sistemas criptográficos mixtos en los que se utiliza una clave de sesión elegida en secreto y al azar o, al menos, de forma impredecible por el remitente, y utilizarla para cifrar todo el cuerpo del mensaje con un algoritmo simétrico. Luego, se utiliza el criptosistema asimétrico para enviar convenientemente cifrada esa clave de sesión adjunta al cuerpo cifrado del mensaje. Así pues, la práctica habitual es utilizar largas claves asimétricas para intercambiar claves simétricas desechables, mucho mas cortas pero de resistencia semejante.

El RSA y otros algoritmos asimétricos

El RSA es un algoritmo de clave pública y el primero que se conoció con la capacidad de generar firmas digitales a la vez que también podía servir para el cifrado de mensajes. El RSA se utiliza ampliamente en protocolos de comercio electrónico, y se le considera seguro si se utilizan claves suficientemente largas e implementaciones actualizadas y bien revisadas.

El algoritmo RSA[154] fue dado a conocer en 1977 por Ron Rivest, Adi Shamir, y Leonard Adleman del MIT. El acrónimo RSA se refiere a los apellidos de sus autores. El MIT consiguió la patente para un "*Cryptographic communications system and method*" que utilizaba ese algoritmo en 1983 (US patent 4.405.829). La patente expiró el 21 de septiembre del año 2000. Dado que un artículo describiendo el algoritmo había sido publicado en agosto de 1977, antes de la fecha en la que se solicitaba la patente, diciembre de 1977, las regulaciones de todo el mundo, excepto los EEUU, descartan la concesión de patentes y por esa razón el algoritmo RSA sólo llegó a ser patente norteamericana. Si se hubiese conocido el trabajo del británico Cocks, ni siquiera la patente norteamericana hubiese sido posible.

Según descubrimientos posteriores, tanto la criptografía asimétrica, como el protocolo de intercambio de claves de Diffie-Hellman, como el algoritmo de claves pública y privada mas conocido, el RSA, fueron desarrollados de forma no relacionada por la Agencia de Inteligencia del Reino Unido unos años antes de que se hiciese público el articulo de Diffie y Hellman en 1976. Esa agencia británica, la GCHQ, en 1997 desclasificó unos documentos, antes considerados como *Top Secret*, con los que se demostró que fueron ellos los que desarrollaron la criptografía de clave pública antes de que lo hicieran los autores americanos mencionados. Varios de esos documentos fueron escritos en la GCHQ durante las décadas de 1960 y 1970, y conducían a esquemas esencialmente idénticos al RSA y al intercambio de claves de Diffie-Hellman ya en los años 1973 y 1974. Algunos

[154]Rivest,R.; Shamir,A.; Adleman, L.: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, Vol. 21 (2), pp.120-126. 1978. Antes fue publicado como una "Technical Memo" del MIT en abril de 1977. Está disponible en http://people.csail.mit.edu/rivest/Rsapaper.pdf

de esos documentos han sido ahora publicados, y los inventores, James H. Ellis[155], Clifford Cocks[156], y Malcolm Williamson[157], han hecho público parte de sus trabajos.

Aunque la GCHQ conocía esta tecnología desde 1973, los anteriores hallazgos fueron considerados más bien como curiosidades y, según lo públicamente conocido, nunca fueron utilizados. La razón de este desinterés quizás esté en lo caros que eran por aquel entonces los ordenadores necesarios para poder utilizar esos criptosistemas.

El concepto de sistemas con claves asimétricas publicado por Whitfield Diffie y Martin Hellman en 1976, estaba muy ligado al trabajo previo de Ralph Merkle[158] sobre distribuciones públicas de claves, y lo que realmente hicieron Diffie y Hellman fue proponer un método concreto para realizarlo. La idea de Merkle sobre el acuerdo público de claves se conoce como Puzzles de Merkle, y se dió a conocer en el año 1978.

Desde la década de los años setenta se ha desarrollado cierto número de variantes del cifrado asimétrico, de la firma digital, de los protocolos de acuerdo de claves y otras técnicas similares dentro del desarrollo de la criptografía de clave pública. El criptosistema ElGamal, inventado en 1984 por Taher ElGamal cuando trabajaba para la empresa Netscape, se basa en la dificultad del problema del logaritmo discreto, y esta muy próximo

---

[155]**James H. Ellis** (1924-1997) fue un ingeniero y matemático nacido en Australia pero de nacionalidad británica que, en 1970, mientras trabajaba en la agencia GCHQ concibió la posibilidad de un "cifrado no-secreto", mas comunmente conocido hoy en día como criptografía de clave pública.

[156]**Clifford Christopher Cocks** es un matemático y criptógrafo británico de la agencia GCHQ que inventó, después de conocer la idea del "cifrado no-secreto" de J. H. Ellis, el ampliamente difundido algoritmo RSA, cerca de tres años antes de que fuese desarrollado por Rivest, Shamir, y Adleman en el MIT. Su autoria no fue reconocida en su tiempo ya que su trabajo estaba clasificado como secreto.

[157]**Malcolm J. Williamson** descubrió en 1974, mientras trabajaba en la agencia de seguridad británica GCHQ, lo que hoy se conoce como protocolo de intercambio de claves de Diffie-Hellman. Williamson ganó la medalla de oro de la Olimpiada Matemática Internacional celebrada en Moscú el año 1968. Estudió en la Universidad de Cambridge donde se graduó en 1971. Después de trabajar un año en la Universidad de Liverpool, se unió al GCHQ, donde trabaja desde 1982.

[158]**Ralph C. Merkle** (1952-) es un pionero de la criptografía de clave pública o criptografía asimétrica, y mas recientemente un investigador y conferenciante de la nanotecnología molecular y la criónica. Merkle aparece en la novela de ciencia ficción *post-ciberpunk*, escrita por Neal Stephenson y titulada *The Diamond Age* (1995), como uno de los héroes de un mundo en el que la nanotecnología está por todas partes.

al desarrollo del esquema de firma digital DSA adoptado por la NSA y el NIST en 1991. En un principio, el sistema DSA no permitía el cifrado/descifrado de mensajes, pero esto pronto quedó refutado por los trabajos sobre canales subliminales de Gustavus J. Simmons[159] (1930-).

La introducción a mediados de la década de los ochenta de la criptografía con curvas elípticas por parte de Neal Koblitz ha dado lugar a una nueva familia de algoritmos de clave pública. Aunque son matemáticamente más complejos que la alternativa RSA o ElGamal, las curvas elípticas proporcionan métodos más eficientes a la hora de abordar el problema del logaritmo discreto, en particular en lo que se refiere al tamaño o longitud en bits de las claves.

La incertidumbre sobre las patentes que acompañan a la criptografía de curvas elípticas es uno de los principales escollos para su amplia aceptación. Por ejemplo, el equipo que desarrolla y mantiene en proyecto OpenSSL aceptó incluir código para criptografía de curvas elípticas en el año 2005 (OpenSSL versión 0.9.8), a pesar de que lo tenía listo ya en el año 2002. Según RSA Laboratories, "*in all of these cases, it is the implementation technique that is patented, not the prime or representation, and there are alternative, compatible implementation techniques that are not covered by the patents*." Sin embargo, con objeto de evitar cualquier problema relacionado con las patentes, la NSA ha comprado licencias para 26 de las patentes que posee el portfolio de patentes Certicom, por un total de 25 millones de dólares, para los algoritmos que aparecen en el Grupo B de Algoritmos de la NSA[160]. Está claro que esta incertidumbre, es muy beneficiosa para los propietarios de las patentes.

La criptografía de Curvas Elípticas proporciona mayor seguridad y de forma más eficiente que la primera generación de técnicas de clave pública (RSA y Diffie-Hellman) actualmente en uso. Por ello, los futuros desarrollos[161] irán migrando progresivamente hacia las curvas elípticas si la política de patentes de Certicom no lo impide.

---

[159]G. J. Simmons: *The Subliminal Channel and Digital Signatures*, Proceedings of Eurocrypt '84, T. Beth, N. Cot, I. Ingemarsson (Eds.), pp. 364-378, Springer-Verlag, 1985.

[160]La conocida como **Suite B** de la NSA es un conjunto de algoritmos criptográficos promulgados por ésta como parte de su Programa de Modernización Criptográfica. Dicho conjunto sirve como base criptográfica interoperable tanto para información no clasificada como para la mayor parte de la clasificada. La Suite B fue anunciada el 16 de febrero de 2005. La correspondiente Suite A es un conjunto de algoritmos secretos dedicados a la protección de comunicaciones altamente sensibles y sistemas de autenticación crítica.

[161]Ver http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm

El *Digital Signature Algorithm* o DSA es un estándar federal norteamericano o FIPS para firmas digitales, y fue propuesto por el NIST en agosto de 1991 para ser utilizado dentro del *Digital Signature Standard* o DSS especificado en la publicación FIPS 186[162], y fue adoptado como estándar en 1993. Tres años después, sufrió una pequeña revisión que se publicó en el FIPS 186-1[163], y el estándar se extendió más allá del año 2000 en la publicación FIPS 186-2[164].

El esquema de firma DSA está cubierto por la patente norteamericana 5.231.668, concedida el 27 de julio de 1993, y adjudicada a David W. Kravitz, un antiguo empleado de la NSA. Dicha patente le fue concedida a "*The United States of America as represented by the Secretary of Commerce, Washington, D.C.*" y el NIST ha hecho que esté disponible en todo el mundo sin plusvalías ni royalties. El profesor Claus P. Schnorr[165] exige que se reconozca que su patente norteamericana 4.995.082 de fecha 19 de febrero de 1991, engloba al algoritmo DSA, pero esta reclamacion está siendo muy contestada.

Limitaciones a la criptografía civil

Ya dentro del nuevo siglo y en territorio europeo hay que resaltar el hecho de que en el año 2000, el gobierno británico de Tony Blair decidió sacar adelante la ley conocida como *Regulation of Investigatory Powers Act 2000* (RIP o RIPA) y que trata de la intercepción de las comunicaciones. La ley tenía como finalidad actualizar la legislación sobre investigaciones policiales respecto a cambios tecnológicos como son, entre otros, Internet y la disponibilidad de cifrado fuerte. Esta ley también sirvió para dar apoyo legal a otras técnicas de vigilancia de los ciudadanos. El titular completo de la ley es:

---

[162]Ver http://www.itl.nist.gov/fipspubs/fip186.htm

[163]Ver http://www.mozilla.org/projects/security/pki/nss/fips1861.pdf

[164]Ver http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

[165]**Claus Peter Schnorr** (1943-) es un distinguido matemático y criptógrafo alemán. Recibió el título de doctor en la Universidad de Saarbrücken en el año 1966, y su habilitación como profesor en 1970. Las contribuciones de Schnorr a la criptografía incluyen sus estudios de los que se conocen como grupos de Schnorr, que se utilizan en el algoritmo de firma digital que lleva su nombre. Schnorr es actualmente profesor de matemáticas e informática en la Universidad de Johann Wolfgang Goethe en Frankfurt. También es un asociado distinguido en los RSA Laboratories, y fue galardonado con el premio Gottfried Wilhelm Leibniz en el año 1993.

> *"An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for the establishment of a tribunal with jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes".*

Los críticos de esta ley y del procedimiento seguido para aprobarla, alegan que el espectro del delito en Internet y la pedofilia fueron utilizados para hacer pasar la ley prácticamente sin debate en la Cámara de los Comunes. La mayoría de las críticas hacen referencia a las regulaciones peligrosamente excesivas que la ley permite y la amenaza que dicha ley supone para las libertades civiles.

Especialmente polémica es la parte tercera de la ley en la que, bajo determinadas circunstancias, se puede solicitar a las personas las claves criptográficas para que las entreguen a una persona debidamente autorizada. La negación o incapacidad para abrir el tráfico cifrado, o para entregar la correspondiente clave, se considerará un delito, con una pena máxima de dos años de cárcel. El debate sobre esta parte tercera hasta el momento ha sido bastante hipotético ya que hasta el 1 de octubre de 2007 todavía no había estado vigente[166]. El primer caso en el que se ha utilizado estos poderes ha sido contra los activistas a favor de los derechos de los animales[167] en noviembre de 2007.

[166]Ver http://www.washingtonpost.com/wp dyn/content/article/2007/10/01/AR2007100100511.html

[167]Ver http://news.bbc.co.uk/1/hi/technology/7102180.stm

El algoritmo RC4 y las conexiones Wi-Fi

En 1996, aparece en escena el algoritmo RC4 que había sido diseñado por Ron Rivest de la compañía RSA Security en el año 1987. Oficialmente el término RC4 se refiere a "*Rivest Cipher 4*", y el acrónico RC también aparece en otros algoritmos del mismo autor como son los cifradores RC2, RC5 y RC6. Inicialmente, el cifrador RC4 era un secreto industrial, pero en el mes de septiembre de 1994 se envió una descripción anónima de dicho algoritmo a la lista de distribución de correo de los Cypherpunks[168], y pronto fue reenviada al grupo de noticias sci.crypt, y de ahí a muchos otros sitios en Internet.

El código filtrado se confirmó como genuino ya que su salida coincidía con el del software propietario RC4 utilizado bajo licencia. Debido a que el algoritmo es conocido, ya no es un secreto industrial, sin embargo el nombre "RC4" sigue siendo una marca comercial. El RC4 terminó por convertirse en parte importante de algunos protocolos de cifrado y algunos estándares, como es el caso del *Wire Equivalenty Protection* (WEP) y *Wi-Fi Protected Access* (WPA) para enlaces WiFi y como en el caso del protocolo *Transport Layer Security* (TLS). La razón principal de su integración en tan amplio número de aplicaciones es su gran velocidad e impresionante simplicidad.

En el año 2001, Scott Fluhrer, Itsik Mantin y Adi Shamir publicaron[169] un artículo sobre un ataque al componente principal del algoritmo WEP de la redes WiFi, que es el algoritmo RC4. En dicho artículo, sus autores exponían varias debilidades de ese cifrador en flujo y describían su utilidad criptoanalítica, a la vez que identificaban un gran número de claves débiles y presentaban varios ataques de claves relacionadas con complejidades asumibles a nivel práctico. Los autores mostraban cómo el RC4 es completamente inseguro en el modo de operación que se utiliza dentro del protocolo WEP, que es parte del estándar IEEE 802.11. Mediante un ataque pasivo y sólo utilizando el criptograma, se puede recuperar una secuencia cifrante arbitrariamente larga y en un tiempo despreciable que crece linealmente con la longitud de la clave; y esto es así tanto para valores iniciales de 24 como de 128 bits.

---

[168]Ver *Thank you Bob Anderson* Cypherpunks mailing list 09/09/1994. Disponible en http://cypherpunks.venona.com/date/1994/09/msg00304.html

[169]Scott R. Fluhrer, Itsik Mantin, Adi Shamir, *Weaknesses in the Key Scheduling Algorithm of RC4*. Selected Areas in Cryptography 2001. Pp. 1-24.

El conocido como *Wired Equivalent Privacy* o *Wireless Encryption Protocol* (WEP) es un esquema criptográfico cuyo objetivo era hacer confidenciales las redes inalámbricas que sigan el estándar IEEE 802.11 y, como tal, es parte del mismo. Las redes inalámbricas radian los mensajes utilizando la modulación de las señales electromagnéticas emitidas, por lo que son "*observables*" por cualquier agente, en principio, ajeno a la transmisión. El sistema WEP pretendía aportar confidencialidad[170] a las comunicaciones, con un grado de calidad que fuese comparable a la que se tenía en las redes de cable tradicionales.

Mediante el criptoanálisis del protocolo, rápidamente se pusieron de manifiesto varios fallos y debilidades serias[171]. Actualmente, una conexión WEP puede ser rota con software disponible en Internet, en menos de un par de minutos. El WEP fue suplantado por el Wi-Fi *Protected Access* (WPA) en el año 2003, y continuado en el estándar completo IEEE 802.11i (también conocido como WPA2) el 2004. A pesar de sus debilidades, el protocolo WEP proporciona un nivel de seguridad suficiente para evitar la intercepción casual de las comunicaciones, pero nada más.

Un ataque con claves relacionadas es una forma de criptoanálisis en la que el atacante puede observar la operación de una cifra bajo el control de varias claves cuyos valores inicialmente no conoce, pero de las que sabe que hay algún tipo de relación matemática entre ellas. Por ejemplo, el atacante podría saber que los últimos 80 bits de las claves son siempre los mismos, incluso aunque no sepa, al principio, cuales son concretamente los valores de esos bits. A primera vista, este tipo de ataques parecen poco realistas ya que puede resultar poco verosímil que un atacante pueda persuadir a un criptógrafo humano de cifrar sus mensajes bajo el control de diferentes claves secretas que estén relacionadas entre si de algún modo. Sin embargo, la criptografía actual no está desarrollada por humanos, sino que se encuentra sumergida dentro de protocolos muy complejos, normalmente no suficientemente trillados por los criptógrafos, y en algunos casos si son posibles los peculiares ataques por claves relacionadas.

---

[170]La **Confidencialidad** ha sido definida por la ISO como "*asegurar que la información es accesible sólo para aquellos autorizados a tener acceso a ella*" y es uno de los servicios fundamentales de la Seguridad de la Información.

[171]Nikita Borisov, Ian Goldberg, and David Wagner: I*ntercepting Mobile Communications: The Insecurity of 802.11* Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, July 16-21, 2001.

Nancy Cam-Winget, Russell Housley, David Wagner, Jesse Walker: *Security flaws in 802.11 data link protocols*. Communications of the ACM 46(5) pp. 35-39 (2003)

Andrea Bittau, Mark Handley, Joshua Lackey: *The Final Nail in WEP's Coffin*, IEEE Symposium on Security and Privacy (Oakland) 2006, disponible en http://www.cs.ucl.ac.uk/staff/M.Handley/papers/fragmentation.pdf

Un importante ejemplo de protocolo criptográfico que falla por un ataque de claves relacionadas es el esquema WEP utilizado en los enlaces WiFi. Cada tarjeta cliente de una red WiFi y punto de acceso en una red protegida por WEP, comparte la misma clave. El cifrado se realiza con el algoritmo RC4, que es un cifrador de flujo y, por tanto, es esencial que la misma clave cifrante nunca vuelva a ser utilizada. Para evitar esto, WEP incluye un vector de inicialización de 24 bits en cada paquete de mensaje. La clave RC4 para ese paquete es el valor inicial IV concatenado con la clave WEP. Las claves WEP tienen que ser cambiadas manualmente y eso ocurre con poca frecuencia. Por tanto, un atacante puede suponer que todas las claves utilizadas para cifrar los paquetes están relacionadas con un IV conocido. Este hecho enfrenta al WEP con una serie de ataques que han demostrado ser devastadores. Lo más sencillo de entender es que un valor inicial de 24 bits sólo deja sitio para 17 millones de posibilidades. Debido a la paradoja del cumpleaños, es probable que por cada 4.096 paquetes, dos de ellos compartan el mismo valor inicial y por tanto, la misma clave RC4, permitiendo que esos paquetes sean atacados.

Ataques todavía más letales sacan ventaja de ciertas claves débiles que presenta el RC4 y que eventualmente permiten recuperar la misma clave WEP. En el año 2005, agentes del FBI demostraron públicamente la posibilidad de hacer todo esto con claves WEP de 128 bits en menos de tres minutos[172], gracias a una amplia oferta de herramientas de software.

Para prevenir ataques con claves relacionadas, el sustituto del WEP conocido como *Wi-Fi Protected Access* (WPA), utiliza tres niveles de claves: una clave maestra, una clave de trabajo y una clave RC4. La clave maestra WPA es compartida con cada cliente y el punto de acceso y, además, se utiliza en un protocolo llamado TKIP para crear frecuentemente nuevas claves de trabajo. La velocidad a la que esto ocurre viene fijada por el mínimo necesario para desbaratar los métodos de ataque conocidos. Después de esto, las claves de trabajo se combinan con un vector inicial (IV) mas largo, de 48 bits, para formar la clave RC4 de cada paquete. Este diseño imita el protocolo WEP de cerca y permite así que el protocolo WPA pueda ser desarrollado con la primera generación de tarjetas de red Wi-Fi, algunas de las cuales implementan partes del WEP en hardware. Sin embargo, no todos los puntos de acceso de primera generación son capaces de ejecutar el protocolo WPA.

---

[172]Ver http://www.smallnetbuilder.com/index.php?option=com_content&task=view&id=24251&Itemid=100

Otro planteamiento más conservador es emplear un cifrador que sea insensible a ataques de claves relacionadas, y que utilice un procedimiento resistente de planificación de claves[173]. Una versión más moderna del protocolo *Wi-Fi Protected Access*, la denominada WPA2, utiliza el cifrador de bloques AES en lugar del RC4, en parte por esta razón. Muchas de las tarjetas de red actuales son incapaces de ejecutar el WPA2.

Evaluaciones criptográficas internacionales

Dado que en el ámbito de la criptografía civil han proliferado numerosos algoritmos, protocolos, normas, etc., pronto se ha visto claro que es necesario evaluar colectivamente la seguridad de cada una de esas posibilidades. Para ello, el procedimiento por el que se optó a principios de la década actual, es la de convocar proyectos de evaluación, o concursos de validación ante los que sus autores presentan los algoritmos.

Ejemplo de ello es el proyecto NESSIE[174] que fue un proyecto de investigación financiado por la Unión Europea entre los años 2000 y 2003. La finalidad principal de esta iniciativa era identificar qué primitivas criptográficas eran seguras. Este proyecto es comparable al proceso para la identificación del AES que organizó el NIST norteamericano, y al proyecto CRYPTREC liderado por el gobierno japonés.

El objetivo de NESSIE era identificar y evaluar la calidad de diseños criptográficos en diferentes categorías, y solicitó publicamente el envio de propuestas en el mes de marzo del año 2000. Se recibieron cuarenta y dos propuestas, y en el mes de febrero del año 2003 se seleccionaron doce. Además de los presentados, en el informe final se incluyeron otros cinco algoritmos ya conocidos pero no enviados como propuestas del proyecto. El informe final declaraba que "*no se había encontrado debilidad alguna en los diseños seleccionados*".

[173]En criptografía, cuando se habla cifrados producto se refieren a un tipo de cifradores, en los que el cifrado y el descifrado se hace en iteraciones (rounds). Lo que se ejecuta en cada ronda es prácticamente lo mismo, a excepción quizás de algunos parámetros estructurales y siempre de una parte de la clave de cifrado. Un planificador de claves o algoritmo de generación de subclaves, es un algoritmo que, dada la clave principal del cifrador, calcula todas la subclaves necesarias para poder ejecutar todas las iteraciones (rounds) del algoritmo.

[174]**NESSIE** = **N**ew **E**uropean **S**chemes for **S**ignatures, **I**ntegrity and **E**ncryption.

Con el año 2003 también llegaron los resultados y las recomendaciones del comité CRYPTREC[175] que es el *Cryptography Research and Evaluation Committee* organizado por el gobierno japonés y que en mayo del año 2000 empezó a evaluar y a preparar recomendaciones sobre distintas técnicas criptográficas para ser utilizadas tanto por parte del gobierno como por parte de las empresas niponas.

Hay un importante solapamiento de los objetivos de las dos anteriores iniciativas y con ello cierto conflicto entre las recomendaciones hechas en los proyectos NESSIE y CRYPTREC. Ambos esfuerzos incluyen a algunos de los mejores criptógrafos del mundo, y los conflictos reales o aparentes de sus recomendaciones tienen que ser examinados con mucho cuidado. Por ejemplo, CRYPTREC recomienda varios cifradores de bloques de 64 bits mientras que NESSIE sólo seleccionó uno, pero CRYPTREC estaba obligado por su constitución a tomar en consideración todos los estándares y prácticas existentes, mientras que NESSIE no. Diferencias similares las encontramos en que CRYPTREC recomienda al menos un cifrador de flujo, el RC4, mientras que el informe NESSIE específicamente dice que no selecciona ninguno de los que han considerado. El cifrador RC4 está ampliamente distribuido como parte de los protocolos SSL/TLS por lo que CRYPTREC lo considera y recomienda utilizarlo sólo con claves de 128 bits. Por ese mismo motivo, por estar en uso, CRYPTREC incluyó en sus recomendaciones un algoritmo de *has*h de 160 bits, a pesar de que sugerían expresamente que se esperase a la llegada de nuevos diseños.

Las recomendaciones del informe CRYPTREC sirvieron de base para el desarrollo de algunas regulaciones y leyes japonesas, como ejemplos de ello tenemos en las leyes de Firma Digital y de Servicios de Certificación (Ley 102 de FY2000, en efecto desde abril de 2001), la Ley Básica sobre la Formulación de una Red Avanzada de Información y Telecomunicaciones del año 2000 (Ley 144 de FY2000), y la Ley de Certificación Individual Pública de diciembre de 2002.

[175]Ver http://www.cryptrec.jp/english/

Ascenso y caída de las funciones *hash*

El algoritmo MD5 (Message-Digest algorithm 5) es una función *has*h muy utilizada en prácticamente todos los productos de seguridad, y aparece en numerosos estándares como valor por defecto. Esta función proporciona resultados de 128 bits al procesar cualquier mensaje con el que se alimente su entrada. Como estándar de Internet (RFC 1321), el MD5 ha sido empleado en una amplia variedad de servicios y aplicaciones de seguridad, y comunmente se ha venido utilizando para comprobar la integridad de ficheros de actualización, de configuración o de otros tipos. Un valor *hash* MD5 típicamente viene expresado como una ristra de 32 caracteres hexadecimales.

La función MD5 fue diseñada por Ronald Rivest en el año 1991 y venía a reemplazar a otra función, también diseñada por él mismo autor poco tiempo antes, y que llamó MD4. La razón de esta sustitución fue que, por aquel entonces, Bert den Boer y Antoon Bosselaers habían encontrado una debilidad en la función MD4 y la habían descrito en uno de sus artículos[176] . En 1993, esos mismos autores publicaron unos resultados preliminares, aunque de interés limitado, sobre como encontrar lo que llamaron una "pseudo-colisión" de la función de compresión que está en el centro de la función *hash* MD4; en este caso se encontraban dos vectores de inicialización distintos que producían el mismo resultado *has*h de salida.

En 1996, Hans Dobbertin publicó su articulo "Cryptanalysis of MD4" en los anales de la conferencia *Fast Software Encryption*[177], y con ello eliminó al MD4 de la lista de funciones *hash* con posible aplicación criptográfica real. En la conferencia plenaria adicional o *rump session* de EuroCRYPT'96, ese mismo autor anunció haber encontrado un modo de obtener colisiones en la función de compresión de la función *hash* MD5. Aunque este no era un ataque sobre la versión completa de la función *hash*, se acercaba bastante, tanto como para que los criptólogos recomendasen su sustitución por otras

[176]B. den Boer; A. Bosselaers: *An attack on the last two rounds of MD4*, Advances in Cryptology, Proceedings CRYPTO'91, LNCS 576, J. Feigenbaum, Ed., Springer-Verlag, 1992, pp. 194-203, disponible en http://homes.esat.kuleuven.be/~cosicart/pdf/AB-9100.pdf

[177]H. Dobbertin: "*Cryptanalysis of MD4*" Fast Software Encryption 1996, LNCS 1039, pp. 53-69 Springer-Verlag. 1996. Ver también H. Dobbertin: "*Cryptanalysis of MD4*". J. Cryptology 11(4). Pp. 253-271. 1998.

funciones *hash* no comprometidas como WHIRLPOOL, SHA-1 o RipeMD-160. En el año 2004 se descubrieron fallos más serios[178] en la estructura de la función *hash* MD5 y éstos sirvieron de puntilla definitiva para el descabello de esta función en su uso criptográfico.

En agosto de ese mismo año, se publicaron, entre otros, modos de cómo generar colisiones[179] en la función MD4 "*a mano*"[180], así como para otras funciones *hash* al uso en esa época. El tiempo medio para encontrar esas colisiones es de cinco segundos empleando un ordenador actual[181]. Como curiosidad, quizás convenga recordar que todavía hoy una variante de MD4[182] sigue prestando servicios (no criptográficos) como parte del esquema de identidad que utilizan los enlaces ed2k y que proporciona descriptores únicos a los ficheros tratados dentro del popular sistema de compartición de ficheros en redes P2P, eDonkey2000[183] y eMule[184].

---

[178]Ver Xiaoyun Wang and Hongbo Yu: *How to Break MD5 and Other Hash Functions* disponible en http://www.infosec.sdu.edu.cn/paper/md5-attack.pdf.
Consultar http://stachliu.com/files/md5coll.c MD5 para obtener el código de un generador de colisiones MD5.

[179]Para disponer de un código en C que permita calcular fácilmente colisiones para la función MD4, consultar el enlace http://stachliu.com/files/md4coll.c MD4 que es un generador de colisiones que implementa las técnicas descritas en el artículo *Cryptanalysis for Hash Functions MD4 and RIPEMD* de Xiaoyun Wang, et al.

[180]Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu1: *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD*, disponible en http://eprint.iacr.org/2004/199.pdf

[181]Ver http://stachliu.com/research_collisions.html

[182]Los enlaces ed2k utilizan una función *hash* que se denomina "*hash raiz*" de una lista de *hashes* MD4, y tienen un valor ditinto al que se obtiene con la función MD4 original.

[183]Ver http://en.wikipedia.org/wiki/EDonkey2000 y http://en.wikipedia.org/wiki/EDonkey_network

[184]Ver http://en.wikipedia.org/wiki/Emule

Criptografías cuánticas

El primero en proponer la idea de lo que hoy se suele llamar "computadores quánticos" fue el físico Richard Feynman, quien la presentó en el año 1981. La principal aplicación que él tenía en mente para esos computadores era la simulación de otros sistemas cuánticos, pero también mencionó la posibilidad de que pudiesen ser utilizados para resolver otro tipo de problemas.

En 1984 Charles Bennett y Gilles Brassard diseñaron el primer protocolo de la criptografía cuántica conocido como protocolo BB84, basándose en las ideas de Stephen Wiesner desarrolladas al final de la década de 1960. El BB84 es un esquema cuántico de distribución de claves que es probablemente seguro, y que se fundamenta en propiedades cuánticas que afirman que la obtención de información sólo es posible a costa de alterar la señal que se mide si los dos estados que se intentan distinguir no son ortogonales entre sí. Normalmente, se habla de este protocolo como el método para generar de forma segura una clave privada entre dos partes distantes para luego poder utilizarla dentro de un sencillo esquema de cifrado One-Time Pad (OTP), aunque este planteamiento es criptográficamente un poco *naïve*.

Las raíces de la criptografía cuántica se remontan hasta finales de la década de 1960, cuando el estudiante universitario de la Columbia University llamado Stephen Wiesner, inventó la codificación conjugada[185,186], y la intentó publicar aplicada a lo que él mismo denominó dinero cuántico imposible de falsificar[187]. El concepto de Wiesner era tan revolucionario, que difícilmente se podía percibir el gran potencial que podría terminar teniendo y no consiguió los apoyos necesarios para continuar con su investigación, ni siquiera para publicar sus ideas en una revista científica.

---

[185]Stephen Wiesner: *Conjugate coding*, Sigact News, vol. 15, no. 1, 1983, pp. 78 - 88 (manuscrito original escrito cerca de 1970), disponible en http:// portal.acm.org/ citation.cfm?id = 1008920

[186]Herramienta criptográfica, propuesta por Stephen Wiesner, que más tarde fue utilizada en el mundo de la criptografía de clave pública como la *Oblivious Transfer*, primero por Rabin, de un modo ligeramente diferente, y luego por Even. Stephen Wiesner introdujo una primitiva llamada *multiplexing* en su artículo "*Conjugate Coding*", que fue el punto de partida de la *quantum cryptograph*y. Desafortunadamente, se tardó más de diez años en su publicación. Even pensó que esta primitiva era equivalente a la más tarde denominada *1-2 oblivious transfer*, Wiesner no vió su aplicación a la criptografía.

[187]Charles H. Bennett, Gilles Brassard, Seth Breidbard, Stephen Wiesner: *Quantum Cryptography, or Unforgeable Subway Tokens*. David Chaum, Ronald L. Rivest, Alan T. Sherman Eds.: Advances in Cryptology: Proceedings of CRYPTO '82. pp. 267-275. Plemum, New York, 1983.

En la mente de Stephen Wiesner, cada billete contendría veinte trampas de luz que serían pequeños artefactos que podrían capturar un fotón con cada uno de ellos. Cada billete también podría ser identificado por un número de serie único. Las veinte trampas de luz se llenarían con veinte fotones polarizados al azar que sólo podrían ser leídos y restaurados por el banco emisor que es el que conoce cúal es la secuencia exacta de filtros polarizadores necesarios para leer ese número de serie. El concepto de Wiesner es brillante pero todavía hoy no se han encontrado los modos que permitan construir tales "*trampas de fotones*", por lo que sus ideas todavía siguen poblando el mundo de la ficción.

En el año 1994 Peter Shor (1959-), un investigador teórico de la informática, se hizo famoso por uno de sus trabajos en computación cuántica, en el que desarrollaba un algoritmo cuántico para la factorización de números compuestos grandes, cuya eficiencia crece exponencialmente más rápido[188] que el mejor algoritmo conocido para esa misma tarea cuando se ejecuta en ordenadores clásicos; a ese prometedor avance se le conoce como el algoritmo de Shor. Este desarrollo se hizo mientras su autor trabajaba en los Laboratorios Bell de la AT&T. Actualmente Shor trabaja como profesor en matemáticas aplicadas del Centro para la Física Teórica (CTP) del MIT.

Dado que el más conocido de los algoritmos de clave pública, el RSA, se basa en la suposición de que es computacionalmente imposible factorizar números grandes con sólo dos factores de tamaños similares, los computadores cuánticos con suficientes quantum bits supondrían una amenaza real a su seguridad ya que podrían romperlo.

Al igual que muchos algoritmos para computadores cuánticos el algoritmo de Shor es probabilístico; dicho de otro modo, que da la respuesta correcta con una probabilidad acotada. Cualquier respuesta que nos proponga ese o cualquier otro algoritmo puede ser fácilmente verificada mediante la división de N por el presunto factor y ver si ésta es exacta. Ejecutando el algoritmo de Shor varias veces, la respuesta correcta llegará a obtenerse con un error exponencialmente pequeño. El algoritmo de Shor fue propuesto en 1994, pero la parte clásica se conocía antes de esa fecha y se debe a

[188]El algoritmo cuántico de Shor para la factorización de un entero N tiene una complejidad del orden de $O((\log N)^3)$ en tiempo y $O(\log N)$ en espacio.

G. L. Miller. Siete años después, en 2001, un grupo de investigación de IBM demostró experimentalmente[189] el algoritmo de Shor factorizando el número 15 en sus dos factores, 3 y 5, utilizando un computador cuántico de 7 qubits[190].

En 2004 se produjo un cambio significativo en lo que se ha dado en llamar Criptografía Cuántica, cuando salió al mercado el primer equipo de explotación que la utiliza, y lo hizo de la mano de la compañía suiza ID Quantique.

En realidad la denominada *Quantum cryptography*, en términos prácticos se refiere a la *Quantum Key Distribution* (QKD), que utiliza principios de la mecánica cuántica para garantizar, en principio, comunicaciones seguras. Los protocolos de criptografía cuántica permiten a dos partes distantes producir simultánea y cooperativamente un vector de bits perfectamente aleatorios que sólo es conocido por ellos dos, y ese vector secreto es el que pueden utilizar los comunicantes como clave en el cifrado convencional de sus comunicaciones.

Una característica importante de la criptografía cuántica es su habilidad para permitir a los dos comunicantes la presencia o no de un tercero que esté "pinchando" su canal (cuántico) para hacerse con información sobre la clave secreta que están generando. Este hecho nace del resultado esencial de la mecánica quántica que dice que "*cualquier proceso de medida de un sistema cuántico perturba al sistema medido*"; dicho de otro modo, un proceso de medida es parte de la historia de ese sistema quántico y no puede quedar indetectado. Cualquier tercera parte que estuviese intentando escuchar el proceso de generación de la clave deberá medir lo que circula a través del canal cuántico, y así, introducir inevitablemente distorsiones

---

[189]Lieven M. K. Vandersypen; Matthias Steffen; Gregory Breyta; Costantino S. Yannoni; Mark H. Sherwood; Isaac L. Chiang: *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*. Nature Vol. 414, pp 883 - 887, 20/27 December 2001.

[190]Un **quantum bit**, o **qubit** es una unidad de información cuántica. Dicha información es descrita como un vector de estado en un sistema cuántico con dos niveles que es formalmente equivalente a un espacio vectorial de dos dimensiones con coordenadas complejas. Fue Benjamin Schumacher quien descubrió el modo de interpretar los estados cuánticos como información, y descubrió cómo comprimir la información dentro de un estado y cómo almacenarla en un número menor posible de estados. A ésto se conoce como la *compresión de Schumacher*. En los agradecimientos de su artículo (Phys. Rev. A 51, 2738), Schumacher dice que el término qubit fue propuesto como una broma durante una de sus conversaciones con Bill Wootters.

detectables por los comunicantes en los extremos. Utilizando superposiciones cuánticas o de entrelazado cuántico, se puede implementar un sistema de comunicaciones que detecta cualquier posible escucha. Si el nivel de intercepciones es suficientemente bajo, entonces se puede llegar a "destilar" una clave que sea secreta y segura para el establecimiento de comunicaciones cifradas convencionales.

Desde el punto de vista de los planteamientos académicos, la seguridad de los protocolos de la criptografía cuántica se basa en principios bastante fundamentales de la mecánica cuántica, mientras que otros sistemas convencionales como, por ejemplo, los de criptografía de clave pública su seguridad se basa en dificultades computacionales no probadas y asociadas con ciertas funciones matemáticas de sentido único.

Hay que recordar que la denominada criptografía cuántica sólo se utiliza para generar sincrónicamente y en secreto una clave en dos puntos geográficamente distantes, y no para transmitir los datos de la comunicación. Estos últimos se protegen con un esquema de cifrado de los muchos que hay en la criptografía convencional, y luego el criptograma resultante puede ser transportado sobre cualquier canal de comunicación. El algoritmo criptográfico mas comúnmente relacionado con la QKD es el de One-Time Pad, que como ya vimos puede considerarse irrompible si se satisfacen sus pocas premisas esenciales. De todos modos, hemos de tener en cuenta que siempre las teorías actúan en unos ámbitos y las realidades en otros, y que, en el día a día, lo que utilizamos son implementaciones reales de principios teóricos que incluso pueden estar muy consolidados, pero lo que se pone en juego en los escenarios reales son las seguridades de las implementaciones, no la corrección de los principios teóricos que las inspiraron. Que falle una implementación real no desmiente un principio teórico, pero la seguridad tan ansiada se pierde.

El declive de la función SHA-1

El 15 de febrero del 2005 saltaron a los medios de información noticias[191] sobre la "ruptura", en toda su extensión, de la función *hash* SHA-1, y no sobre versiones reducidas como solía ser en otros casos. Los mismos autores de ese ataque ya habían publicado resultados similares para otras funciones *hash*[192].

Los autores de tan sonado hito fue un equipo de investigación dirigido por Xiaoyun Wang[193], Yiqun Lisa Yin, y Hongbo Yu, de la Universidad Shandong en República Popular de China, que comunicaron este hecho haciendo circular discretamente un par de folios con sus resultados: [1] colisión del SHA-1 en 2^{69} operaciones *hash* (por fuerza bruta son necesarias 2^{80}), [2] colisiones en la versión inicial de esa misma función, conocida como SHA-0, en 2^{39} operaciones y, por último, [3] colisiones en una versión del SHA-1, reducida a 58 etapas, en 2^{33} operaciones (la versión original y completa tiene 80 etapas).

En la *rump session*[194] de la conferencia CRYPTO 2004, Wang mostró algunos ataques por colisión contra la función *hash* MD5, la SHA-0 y otras funciones del mismo tipo.

---

[191]Ver http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

[192]Xiaoyun Wang; Dengguo Feng; Xuejia Lai; Hongbo Yu: *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD*. Cryptology ePrint Archive. Report 2004/199 received 16 Aug 2004, last revised 17 Aug 2004, disponible en http://eprint.iacr.org/2004/199

[193]**Wang Xiaoyun** (chino simplificado: 王小云; chino tradicional: 王小雲; pinyin: Wáng Xiaoyún) (1966-) es una investigadora y profesora del departamento de matemáticas y ciencia de sistemas de la Universidad de Shandong, en la provincia costera de Shandong, en la China Popular. Wang nacio en Zhucheng, de la provincia de Shandong, obtuvo su grado de *bachelor* en 1987, el de master en 1990 y el de Doctora en 1993 en la Universidad de Shandong, y luego pasó a dar clases en el Departamento de Matemáticas de esa universidad en 1993. Wang se convirtió en profesor titular en 1995, y en catedrática en el año 2001. Trabaja, desde 2005 en el instituto dirigido por el físico y premio Nobel americano Chen Ning Yang en el Centro de Estudios Avanzados de la Universidad de Tsinghua, en Pekín.

[194]Sesión añadida al final del programa del día para acomodar un grupo extra de comunicaciones o una conferencia plenaria adicional. Se trata de una reunión, más o menos informal, donde los participantes tienen la oportunidad de hacer breves presentaciones sobre un tema, trabajos en progreso, ideas para futuros proyectos, quejas, etc. Este tipo de eventos es muy usual entre la comunidad de informática. Para indagar sobre posibles orígenes, ver "*Rump Parlament*" en http://en.wikipedia.org/wiki/Rump_Parliament

Una colisión en una función *hash* es cuando dos valores distintos de la entrada dan el mismo resultado a la salida.

En febrero del 2005 se informó de que los mismos autores, Wang et alt., habían hallado un mejor modo de encontrar colisiones en la función *hash* SHA-1, que se utiliza en prácticamente todos los productos de seguridad. Se estimó que su ataque solo requería menos de 2^{69} operaciones, muchas menos que las 2^{80} operaciones que requiere un ataque por fuerza bruta. Sus trabajos aparecieron publicados en las actas de la conferencia CRYPTO 2005. En agosto de 2005, en la *rump session* de esa misma conferencia, Xiaoyun Wang, Andrew Yao y Frances Yao, anunciaron una versión mejorada del ataque al SHA-1. La complejidad de esta nueva versión es de 2^{63} operaciones.

Un año mas tarde, en la *rump session* de CRYPTO 2006[195], Christophe de Cannière y Christian Rechberger[196] mejoraron mas aún el ataque al SHA-1[197] y publicaron sus resultados en el artículo posterior titulado "*Finding SHA-1 Characteristics: General Results and Applications*", por el que recibieron el premio al mejor artículo en la conferencia ASIACRYPT 2006 celebrada en diciembre de 2006[198], en la ciudad china de Shangai. En ese artículo se presenta una colisión de dos bloques de entrada en una versión de 64 etapas del SHA-1 obtenida, utilizando métodos no optimizados, con 2^{35} evaluaciones de la función de compresión.

En la criptografía cualquier ataque que tenga menor complejidad que el de fuerza bruta se considera una rotura. Sin embargo, esto no significa necesariamente que ese ataque pueda ser útil en la práctica. Este y otros ataques previos a versiones más antiguas como el SHA-0, o reducidas del SHA-1, sentencia al abandono a la función SHA-1 como componente necesario de la firmas digitales, aunque no afecta a otras aplicaciones como, por ejemplo, los HMACs[199] en los que las colisiones de la función *hash* no son importantes.

---

[195]Ver http://www.iacr.org/conferences/crypto2006/rumpsched.html

[196]Christophe De Cannière, Christian Rechberger: *SHA-1 collisions: Partial meaningful at no extra cost?* Rump session CRYPTO'06.

[197]Ver http://www.heise-security.co.uk/news/77244

[198]Ver *Advances in Cryptology - ASIACRYPT 2006. 12th International Conference on the Theory and Application of Cryptology and Information Security*, Shanghai, China, December 3-7, 2006. Xuejia Lai, Kefei Chen, Eds. Lecture Notes in Computer Science, Springer Berlin/Heidelberg, Volume 4284, 2006. ISBN 978-3-540-49475-1.

[199]Un **kyed-Hash Message Authentication Code**, o **HMAC**, es un tipo de código autenticador de mensajes (MAC) calculado utilizando una función *hash* criptográfica en combinación con una clave secreta. Al igual que con cualquier MAC, puede ser utilizada para simultáneamente verificar la integridad de los datos y la autenticidad del mensaje.

En términos de seguridad práctica, la mayor consecuencia que tienen estos nuevos resultados es la de preparar el sendero para descubrir e ingeniar otros ataques más potentes. Si van a llegar o no estos ataques definitivos es algo que está por ver, pero lo cauto es migrar hacia el uso de funciones *hash* más resistentes. Un ataque por colisión no supone los mismos riesgos que un ataque de *preimagen*[200] que daría al traste con el carácter "*de sentido único*", de no-invertivilidad que se le exige a cualquier función *hash* de interés criptográfico.

Muchas de las aplicaciones que utilizan *hashes*, tales como el almacenamiento de *passwords* o palabras clave, o la firma digital de documentos, sólo están mínimamente afectados por un ataque por colisiones. En el caso de la firma digital de documentos, por ejemplo, si el atacante quiere falsificar la firma ya existente del documento, tendría que o bien [1] tener acceso a la clave privada que se utilizó para firmar ese documento, o [2] ser capaz de invertir la función, es decir, encontrar un valor de entrada que dé exactamente el mismo valor de salida que da el documento original firmado. Sin embargo, la posibilidad de encontrar o generar dos documentos correctos y (semánticamente) distintos que den el mismo valor *hash* sí permitiría engañar a un firmante ya que, al firmar uno de los documentos, el que es capaz de leer y evaluar, también estaría firmando otro que desconoce completamente.

---

[200]Un **ataque por *preimagen*** sobre una función *hash* criptográfica es un intento de encontrar un mensaje de entrada que dé un valor concreto a la salida de la función. Hay dos tipos de ataques por *preimagen*: [1] *First preimage attack*, dado un valor *hash h*, encontrar un mensaje *m* tal que *hash(m) = h*. y [2] *Second preimage attack*, dado un mensaje fijo *m1*, encontrar otro mensaje diferente *m2* tal que *hash(m2) = hash(m1)*. Un ataque por *preimagen* se diferencia de un ataque por colisión en que hay un valor *hash* o un mensaje de entrada fijo con el que hay que coincidir. Un ataque por *preimagen* sobre una función *hash* de n bits requiere, de media, 2^{n-1} operaciones para tener éxito. Por otra parte, como consecuencia de la paradoja del cumpleaños, uno puede esperar encontrar una colisión entre dos entradas cualesquiera en $2^{n/2}$ operaciones de la función *hash*.

El criptoanálisis moderno y la inseguridad GSM

Mientras que los cifrados modernos como el AES o todos los que aparecen en los informes de iniciativas como NESSIE, CRYTEC o las del NIST se consideran irrompibles; todavía hoy se incluyen en diferentes productos sistemas criptográficos bastante pobres. Este proceder es la única causa de importantes fracturas criptoanalíticas en años recientes. Ejemplos notables de ellos incluyen al DES porque hoy en día 2^{59} claves no es un número inabordable, al esquema de cifrado Wi-Fi, al WEP, al Sistema de Barajado de Contenidos (CSS) utilizado en los DVDs, a los cifrados A5/1 y A5/2 que están en el núcleo de la protección de las comunicaciones a través de teléfonos móviles GSM, etc. Más aún, ninguna de las ideas matemáticas sobre las que se construye la criptografía de clave pública ha sido demostrada formalmente como "irrompible" por lo que futuros desarrollos bien podrían convertir esos sistemas en inseguros. La longitud de la clave para mantener la seguridad crece a la par que la potencia de cálculo necesaria para romperlas se hace más barata y disponible.

Hasta la fecha se han publicado unos cuantos ataques contra el sistema criptográfico, conocido como A5/1, que se utiliza en los sistemas de telefonía móvil GSM. Algunos de ellos requieren un procesado previo caro y tedioso después del cual el cifrado puede realmente ser atacado en cuestión de minutos o segundos. Sólo desde hace poco tiempo, se conocen debilidades de los algoritmos empleados en el sistema GSM que permiten los ataques pasivos; es decir, aquellos que sólo requieren escuchar la transmisión a interceptar, y luego utilizar la suposición de un texto en claro conocido. En el año 2003, se descubrieron debilidades aún más serias que las anteriores y sobre las cuales se podía montar un ataque que necesita conocer sólo el criptograma[201], o mediante un atacante activo.

---

[201]Un **ataque de sólo criptograma o *ciphertext-only attack* (COA)** es un modelo de ataque criptoanalítico en el que el atacante sólo tiene acceso a un conjunto de criptogramas. El ataque es completamente exitoso si se deducen los correspondientes textos en claro, o aún mejor, si se deduce la clave utilizada. La habilidad de obtener cualquier información acerca del texto en claro que está oculto en el criptograma también se considera un éxito del atacante. Por ejemplo, si un adversario está mandando continuamente criptogramas para conseguir seguridad frente al análisis de tráfico, sería muy útil poder distinguir lo que son envios de mensajes reales y lo que son señuelos sin sentido. Incluso la posibilidad de descubrir la existencia de mensajes reales facilita enormemente la obtención de información mediante el análisis de tráfico.

Ekdahl y Johannson, en 2003, publicaron un ataque al proceso de inicialización del algoritmo A5/1 que lo rompe en pocos minutos utilizando de 2 a 5 de conversación en claro. Este ataque no requiere etapa de pre procesado. En 2004, Maximov et al., mejoraron su resultado dando lugar a un ataque que requiere menos de un minuto de cálculo, y unos pocos segundos de conversación conocidos. Este ataque fue posteriormente mejorado por Elad Barkan y Eli Biham en el año 2005.

En el año 2006[202], Elad Barkan, Eli Biham, Nathan Keller publicaron[203] la versión completa de su trabajo de 2003[204], en el que atacan a cualquier cifrado de la familia A5/x (incluido el A5/3, también conocido como KASUMI), o incluso al propio protocolo GPRS. Los autores declararon que sus ataques son de índole muy práctica y que atacan también a los protocolos, por lo que son efectivos aunque se utilicen cifrados robustos. A diferencia de otros ataques previos que requieren informaciones poco realistas, estos ataques no necesitan de ningún conocimiento de la conversación. Como resultado final, estos ataques permiten a los atacantes pinchar conversaciones tanto en tiempo real como en diferido.

El análisis de tráfico

El análisis de tráfico es cualquier proceso de intercepción y examen de mensajes hecho con el fin de deducir información de los patrones que aparezcan en la comunicación. Este tipo de análisis se puede hacer incluso cuando los mensajes están cifrados y no pueden ser descifrados. En general, cuanto mayor es el número de mensajes observados, o incluso interceptados y almacenados, más se puede inferir de su tráfico. El análisis de tráfico puede hacerse en el contexto de la inteligencia militar o de contrainteligencia, y es un problema grave en la seguridad de los ordenadores y de las comunicaciones entre móviles, por ejemplo.

---

[202]Elad Barkan, Eli Biham: *On the Security of the GSM Cellular Network Security and Embedded Systems*, NATO Security through Science Series, Vol.2.D, IOS Press, pp. 188-195, 2006.

[203]Elad Barkan, Eli Biham, Nathan Keller: *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication* Technical Report CS-2006-07, disponible en http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf

[204]Elad Barkan, Eli Biham, Nathan Keller: *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*. Proceedings of CRYPTO2003, LNCS 2729, pp. 600-616, 2003.

Las tareas del análisis de tráfico pueden realizarse de modo automático, mediante programas de ordenador especializados, de los cuales hay algunos ejemplos comerciales disponibles[205]. Las técnicas más avanzadas de análisis de tráfico incluyen varias formas de análisis de lo que se ha dado en llamar "redes sociales".

Por ejemplo, los analistas británicos en la Primera Guerra Mundial se dieron cuenta de que la señal de llamada por radio para el vicealmirante alemán Reinhard Scheer, comandante de la flota enemiga, había sido transferido a una estación en tierra. El almirante Beattie, desconocedor de la costumbre de Scheer de cambiar las señales de llamada cuando dejaba el puerto, restó importancia a este hecho y no hizo caso a los intentos de los analistas de la Room 40 de que lo tuviese en cuenta. La flota alemana partió, y la flota británica llegó tarde al escenario en el que se produjo la Batalla de Jutlandia. Si se hubiesen tomado más en serio el análisis de tráfico, los británicos podrían haber hecho un mejor papel en ese capítulo de la guerra.

Otro ejemplo del inicial desinterés por el análisis de tráfico lo tenemos al principio de esa misma guerra, cuando el porta-aeronaves HMS *Glorious* estaba evacuando pilotos y aviones de Noruega. El análisis de tráfico daba indicaciones de que los buques alemanes *Scharnhorst* y *Gneisenau* se estaban dirigiendo hacia el Mar del Norte, pero el Almirantazgo británico no dió importancia a ese informe por considerarlo no confirmado. El capitán del *Glorious* no tomó precauciones suplementarias ni dobló la vigilancia y, cuando llegó la hora, fue sorprendido y hundido. Harry Hinsley, el joven que hacía de enlace entre Bletchley Park y el Almirantazgo, declaró más tarde que a partir de aquel momento sus informes sobre análisis de tráfico fueron tomados más en serio.

Un ejemplo en el que sí se tuvo en cuenta la potencia de los análisis de tráfico lo encontramos en el Almirante Nagumo, que en el ataque a Pearl Harbor navegó bajo silencio radioeléctrico absoluto, con sus equipos de radio físicamente cerrados con llave, y dejando a sus operadores de radio en tierra[206], en Japón, para simular desde allí el tráfico ordinario y no levantar sospechas ante los "radioyentes". No está históricamente claro si esta estratagema engañó a los servicios de inteligencia norteamericanos de la flota del Pacífico, pero cierto es que eran incapaces de localizar los transportes japoneses en los días precedentes al ataque.

---

[205]Como los ofrecidos por i2, Visual Analytics, Memex, Orion Scientific, Pacific Northwest National Labs, Genesis EW's GenCOM Suite entre otros.

[206]La razón de dejar en tierra a los radio operadores habituales de la flota y simular su actividad es que, en aquellos días, los operadores de radio era conocidos individualmente por uno y otro bando.

Un ejemplo más reciente de lo que puede hacer el análisis de tráfico hecho por aficionados y conocido como *planespotting*, es que con este tipo de observadores se llegaron a conocer públicamente la existencia de los vuelos secretos de la CIA[207], de las prisiones[208] y de las transferencias de prisioneros hacia y desde las susodichas prisiones mediante los denominados *taxis de la tortura*.

Algunos sistemas nacen muertos

El primero de mayo de 2007 algunos usuarios empantanaron el sitio Web Digg.com[209] con copias de una clave de 128 bits utilizada en el sistema AACS de protección de los discos digitales de alta definición (HD-DVD y Blu-ray). La denominada AACS *encryption key controversy*, o AACS *cryptographic key controversy*, surgió en el mes de abril de 2007 cuando la *Motion Picture Association of America* y el administardor de licencias *Advanced Access Content System* (AACS LA) empezaron a enviar cartas de demanda a sitios web en los que se publicaba un número de 128-bits que, representado en hexadecimal, es el 09 F9 11 02 9D 74 E3 5B D8 41 56 C5 63 56 88 C0[210], familiarmente conocido como el 09 F9[211], que es una de las claves criptográficas utilizadas en la protección de los nuevos soportes digitales de alta definición. Esas cartas exigían una inmediata eliminación de esa clave y de cualquier enlace a ella, amparándose en el *Digital Millennium Copyright Act* (DMCA) aprobado en 1998 por los EEUU. El 22 de mayo de 2001, la Unión Europea aprobó la Directiva Europea del *Copyright* o EUCD, que es muy similar, en muchos aspectos, a la DMCA norteamericana.

---

[207]Ver http://www.mail-archive.com/osint@yahoogroups.com/msg29431.html

[208]Ver http://www.guardian.co.uk/usa/rendition/

[209]**Digg** es un sitio web (www.digg.com) basado en comunidades de usuarios y con un énfasis especial en los artículos de ciencia y tecnología, aunque recientemente se ha expandido y ahora incluye articulos políticos y de entretenimiento. Este sitio Web combina el "*social bookmarking*", el *blogging*, y la *sindicación* con una organización no jerárquica y un control editorial democrático.

[210]Nick Farrell: 0*9 f9 [...] is the number they tried to ban*. The Inquirer. 2 de mayo 2007, disponible en http://www.theinquirer.net/en/inquirer/news/2007/05/02/09-f9-11-02-9d-74-e3-5b-d8-41-56-c5-63-56-88-c0-is-the-number-they-tried-to-ban

[211]Ver http://www.sci-tech-today.com/news/09-F9-An-Unlikely-Star-Is-Born/ story.xhtml?story_id=011001CEELPZ

El 16 de abril de ese mismo año, el consorcio AACS anunció[212] que habían expirado ciertas claves de cifrado utilizadas en las aplicaciones basadas en PCs, y se proporcionaron parches para aplicaciones como WinDVD y PowerDVD que utilizarían nuevas claves de cifrado no comprometidas. Las viejas claves públicamente conocidas todavía permiten abrir títulos antiguos editados en los mencionados formatos, pero no los últimos lanzamientos ya que éstos han sido protegidos con las nuevas claves. Todos los usuarios de los *players* afectados, incluso los considerados "legítimos" por la AACS, tienen que actualizar o sustituir sus *players* si es que quieren poder ver los nuevos títulos en el mercado.

La controversia tomó tintes más oscuros a principios de mayo, cuando el sitio de reunión de noticias Digg recibió una carta de la DMCA y procedieron a eliminar numerosos artículos y a proscribir a todos aquellos usuarios que publicaban y volvían a publicar esa información. Estos hechos han sido calificados por algunos como "*revueltas digitales*"[213] o "*cyber-disturbios*", en los que los usuarios distribuyeron en masa la clave prohibida. La AACS describió estos hechos como un "*interesting new twist*"[214].

La longitud de las claves y su evolución con los niveles de seguridad

En el año 2002 se consideraba que la longitud mínima de una clave RSA debía ser de 1024 bits. En el año 2003 la compañía RSA Security hizo pública sus estimaciones sobre la relación entre seguridad real y longitud de las claves, y dijo que una clave RSA de 1024-bit tiene una resistencia criptográfica equivalente a 80 bits se una clave simétrica, y que 2048 bit de clave RSA equivalen a 112 bits de una buena clave simétrica, y que, por último, una clave RSA de 3.072 bits sería la contraparte asimétrica de una clave simétrica de 128 bits.

RSA recomienda que las claves RSA de 1.024 bits se utilicen hasta el año 2010 y que las de 2.048 bits puedan aguantar hasta el año 2030 y, por último, que se utilicen las claves RSA de 3.072 si lo que se persigue es tener seguridad más allá del umbral del año 2030. Un borrador de una guía sobre la gestión de claves que está desarrollando el NIST va más allá, y sugiere que las claves RSA de 15.360 bits tienen una resistencia equivalente a 256 bits de clave simétrica.

---

[212]Ver http://www.aacsla.com/press/

[213]Ver http://www.australianit.news.com.au/story/0,24897,21659892-27317,00.html

[214]Ver http://news.bbc.co.uk/2/hi/technology/6623331.stm

El NIST, en su documento de agosto de 2007 titulado "SP800-78: *Cryptographic Algorithms and Key Sises for Personal Identity Verificaction*", considera que, para el primer día del año 2011, los cifrados con seguridades equivalentes a 80 bits de cifrado simétrico ya estarán fuera de juego, al menos para la identificación personal, y que los sistemas deberán haber migrado a una seguridad equivalente a 112 bits o a cotas más elevadas. Para los sistemas asimétricos basados en criptografía de curvas elípticas se especifica un mínimo de 112 bits de resistencia, lo que supone utilizar claves de 224 bits de longitud.

¿Qué problemas quedan por resolver en la criptografía actual?

La criptografía moderna ha cambiado mucho en las últimas décadas, pero todavía le quedan varios problemas por resolver, además de descubrir nuevos campos de aplicación que vayan más allá de los que hasta el momento han sido sus nichos naturales.

Aunque el AES sólo tiene siete años de vida pública todavía es necesario avanzar más en los principios y técnicas de diseño para nuevos cifradores de bloques y, sobre todo, de funciones *hash*. Los cifradores actuales se adoptan en la fe de que la probabilidad de que tengan un fallo o alguien lo encuentre y lo pueda utilizar, sea muy pequeña, despreciable a todos los efectos, pero ninguno de los cifradores conocidos se construye sobre alguna prueba teórica que establezca un mínimo a su complejidad algorítmica que es la que fija la resistencia del sistema. Quizás nunca sea posible "demostrar" que un cifrador es seguro, por lo que la criptografía siempre mantendrá cierto grado de "Arte".

Otro tema pendiente es el diseño de cifradores de flujo. Con el advenimiento de las líneas de alta velocidad de transmisión de datos como son las fibras ópticas, y con la llegada de los servicios multimedia como el vídeo en tiempo real, cada día es más necesario disponer de criterios válidos de diseño para cifradores de flujo, ya que los que se han seguido hasta el momento han perdido sus batallas frente al criptoanálisis.

Todo secreto se construye sobre un hecho irrepetible, imposible de adivinar, la clave, a la que sólo puede descubrir la fortuna. Sobre ese secreto es sobre el que se construye la seguridad gracias a los instrumentos criptográficos; por tanto, si la fuente de secretos no es buena, vano es el esfuerzo posterior, y peligrosísima la sensación de (falsa) seguridad.

Toda la criptografía se basa en que alguien, en algún recóndito y secreto lugar del sistema, sea capaz de fabricar una secuencia perfectamente

secreta, uniformemente distribuida, irrepetible y al azar para, con ella, construir claves, valores iniciales, retos, identidades, etc. Las fuentes de azar existen, pero son lentas, son difíciles de contactar y, además, hay que hacerlo sin degradar sus cualidades. Por si fuera poco, esta secreta entrevista con el azar debe poder hacerse desde cualquier sistema hardware (grandes ordenadores, PCs, laptops, PDAs, smartphones, smartcards, etc.) y desde múltiples sistemas software.

Dado que el buen azar es caro y escaso, es necesario poder amplificar el numero de bits que proporciona utilizando generadores de secuencias pseudoaleatorias en las que el azar sólo participa a la hora de inicializar el sistema. Si el generador tiene fallos explotables, de nada sirve la pureza del estado inicial. Son muchos los ejemplos en los que un fallo en la generación de las secuencias aleatorias afecta negativamente a toda la criptografía que las utiliza y, por ende, a toda la seguridad del sistema que termina fallando estrepitosamente.

Aunque el desarrollo social de la firma digital ha sido sorprendentemente raquítico en sus tres décadas de existencia como concepto y como algoritmos, éste sigue siendo un tema pendiente, un hito que hay que alcanzar antes de que podamos hablar realmente de una actividad social o comercial en la red. Los sistemas de firma digital son pocos y, además de adolecer de una oferta excesivamente escasa, tienen el problema de su supervivencia a lo largo del tiempo. Lo más importante de una firma es que su irrepetibilidad se mantenga durante periodos de tiempo muy largos y esa cualidad, que su resistencia durante décadas y décadas de futuro criptoanálisis, es algo que todavía nadie sabe medir o siquiera estimar.

Otro tema relacionado y también pendiente es el de la identificación y la autenticación. Por todos es conocido que el sistema basado en identificadores de usuario y de palabras secretas no da niveles de seguridad adecuados para aplicaciones tan importantes como el *home banking*, o para el comercio electrónico en general. Las tendencias actuales apuntan, quizás equivocadamente, al uso de técnicas biométricas de identificación y al uso de "representantes" a la hora de gestionar los secretos autenticadores frente a la red (tarjetas inteligentes, teléfonos móviles, generadores pseudoOTPs, etc.). Lo que si empieza a estar claro es que no conviene jugar todo a una sola carta y que conviene estudiar la posibilidad de autenticaciones multifactoriales y multimodales.

Como toda tecnología de doble uso, el uso de la criptografía puede afectar a los derechos civiles. La criptografía apoya la libertad individual y colectiva en un mundo invadido por las tecnologías digitales, a través del uso del cifrado, del desarrollo de mecanismos para garantizar el anonimato, y de

los inevitables sistemas *peer-to-peer* de almacenamiento, distribución y construcción cooperativa. Sin embargo, la criptología puede y no debe convertirse en una realidad que permita el control masivo y detallado de los ciudadanos al estilo de un digital *Big Brother*. El antídoto para esto no lo podemos encontrar dentro de la tecnología, sino dentro de la misma sociedad.

Algunos vaticinan que en menos de diez años los *gadgets* criptográficos serán tan pequeños, tan baratos y tan potentes como para permitir el "*marcaje*" de prácticamente cualquier cosa[215]. Sus promotores hablan de la protección de la identidad comercial y de la lucha contra las falsificaciones de fármacos, por ejemplo, pero pueden estar sentando las bases para un control intensivo e implacable de los usuarios más que de los productos. De todos modos, todavía queda mucho camino por recorrer para conseguir realmente esos sistemas pequeños, potentes y baratos que, además, sean criptográficamente seguros e infalsificables, por lo que también en este campo hay cosas que hacer.

Otro de los aspectos pendientes es la interacción con el usuario. Hasta el momento, la experiencia indica que al aumentar la seguridad de los sistemas, los procedimientos a seguir se alejan más y más de lo que un usuario común es capaz o está dispuesto a asumir en aras a mantener la seguridad. Para algunos, el entrenamiento de los usuarios es lo que limita los niveles de seguridad en sistemas tan convenientes e importantes como el comercio electrónico y los sistemas financieros a través de la red; sin embargo, quizás esto pueda ser más consecuencia de un tipo de diseño o planteamiento concreto que de un límite de la naturaleza humana común.

Algo que quizás veamos proliferar los próximos años sea lo que se ha dado en llamar *Symmetric Key Infrastructures* (SKI) y que podrían llegar a ser más importantes para la seguridad de las tecnologías de la información que las ya populares Infraestructuras de Clave Pública (PKI).

Tanto las PKIs como las SKIs tratan el ciclo de vida completo en la gestión de las claves criptográficas: creación y distribución, almacenamiento y recuperación, revocación y eliminación. En las SKIs, las claves deben permanecer secretas y debe estar disponible bien cuando lo requiere un agente individual o cuando lo hace un grupo autorizado que comparte esa clave.

---

[215]Tim Hornyak; *RFID Powder*. Scientific American Magazine, 4 páginas, February 2008.

La mayoría de las aplicaciones desarrolladas en los últimos años han consistido en aplicar la criptografía a la protección de datos "en vuelo", transitando por redes públicas e incontroladas o por correo electrónico. En estos casos, el cifrado y descifrado se hace a la hora del envío o en el momento de la recepción. Las claves son identificadas y a disposición de los actores involucrados en el proceso. Los datos típicamente van cifrados con una clave simétrica que está protegida utilizando técnicas de clave pública. Sin embargo, la clave simétrica por sí misma no parece requerir gestión específica alguna. El único requisito de secreto a largo plazo que se pide en una PKI es el de la clave privada de cada uno de los actores, y ésta suele estar disponible sólo para una agente.

El renacimiento de las SKIs es debido al énfasis que se está poniendo en aplicar los métodos criptográficos a los datos "en reposo", como ocurre en una base de datos, en un fichero en un disco magnético, o en cualquier información dentro de una cinta de salvaguardia. En este caso, el descifrado puede darse mucho después de que se produjese el cifrado y quizás lo haga un actor que no estuvo originalmente involucrado en el cifrado. La clave simétrica en este caso tiene que ser gestionada explícitamente. Más aún, la clave debe estar disponible para más de un actor. La gestión de esas claves requiere infraestructuras más ricas y complejas que las propias de las claves privadas en una PKI.

Por recordar algunos temas que siguen pendientes de atención y de resolución, valdría mencionar el almacenamiento y la verificación histórica de firmas digitales, la notarización en la federación de identidades dentro de la empresa o cualesquiera comunidades, el desarrollo de identificadores no trazables para proteger la intimidad de los agentes humanos, las medidas de protección para impedir la fuga de información, encontrar el modo de impedir lo que se conocen como ataques colaterales, la mediación y armonización entre la seguridad del ciberespacio y la del espacio humano, la defensa frente a los riesgos que suponen los equipos móviles y removibles de almacenamiento y comunicaciones, la seguridad en los sistemas de voz sobre redes IP (VoIP), cómo hacer seguras las iniciativas en boga de virtualización, la seguridad en protocolos como el Ajax y Web 2.0, el desarrollo de herramientas cooperativas para agentes esencialmente competidores, etc.

Para terminar, mencionar que hay más vanguardias en desarrollo y más problemas pendientes de resolver, además de los que están todavía sin identificar. Habrá que aprender a equilibrar, a dimensionar correctamente los sistemas para que sean seguros, flexibles y de uso sencillo; habrá que no perder la vista de la futura proliferación de artefactos electrónicos cuyo comportamiento estará basado en información externa (domótica, redes

de sensores, geolocalización, etc.) o que hace externa haciendo acopio de la misma (telemetrías, posicionamiento, etc.); habrá que ir con cuidado a la hora de utilizar sistemas digitales para el desarrollo de elecciones, para el diagnóstico, para la toma de decisiones, etc., ya que todas esas situaciones requieren, como característica previa, la seguridad de los sistemas, y en muchas ocasiones ésta no ha sido ni siquiera parte de su diseño, por lo que no se puede contar realmente con ella.

Epílogo

La Criptología no es una ciencia de reciente aparición ni parece seguir el frenético desarrollo que otras actividades tecnológicas emergentes tienen. La criptografía más que una ciencia, se ha comportado como un arte durante los últimos casi cinco mil años. En las últimas décadas han surgido nuevos e impensables escenarios de uso como pueden ser la Sociedad de la Información e Internet, y en ellos la Criptología sin duda está teniendo y tendrá un nuevo renacer. En esta ocasión, son muchos más elementos con los que contará para construirse (ordenadores, redes, autómatas, necesidades, escenarios, equilibrios de fuerza, etc.) pero los objetivos de antaño como la protección de la confidencialidad o la integridad, seguirán presentes y seguirán siendo los mismos. Además del secreto, la identidad y el ejercicio de ésta a través de la firma, cobrará incluso más importancia que aquel para las relaciones comerciales y civiles, pero todavía habrán de llegar otros objetivos más sutiles como el anonimato.

La íntima relación de servidumbre de la Criptología con los imperios, los ejércitos y las iglesias se rompió en el último tercio del siglo XX, y ya nadie será capaz de volver a meter el genio en la botella, por lo que no es de extrañar que el estudio y difusión de los avances criptográficos vayan a difundirse lenta pero constantemente, en los ámbitos académicos a través de sus cursos de formación, y en la misma sociedad en general ya que serán la llave de acceso a potestades, informaciones y contenidos de todo tipo.

La tecnología criptográfica, como cualquier otra tecnología, no es ni buena ni mala sino que es ambas cosas a la vez; puede servir para atacar, para defender y para despistar, lo cual es cada día es más importante ya que vamos inexorable e irremisiblemente hacia una sociedad occidental basada únicamente en la información.

Anexo

La criptografía y la seguridad en el 7º Programa Marco europeo y en el Plan Nacional español

Ni en el séptimo Programa Marco de la Unión Europea actualmente vigente, ni en los programas o líneas de trabajo del nuevo Plan Nacional de Investigación, Desarrollo e Innovación hay apartados específicos relativos a la criptografía o a los sistemas y protocolos criptográficos. Sin embargo, dado que ésta es una herramienta necesaria para construir sistemas de seguridad en general, y sistemas avanzados de la sociedad de la información en particular, la criptografía yace latente dentro de algunos de los apartados y proyectos financiados dentro de las iniciativas mencionadas.

La criptografía está incluida en los proyectos de identificación de personas, animales y mercancías, en el control de acceso de las fronteras, está también en las comunicaciones digitales de cualquier tipo, en los sistemas de tele-operación a la hora de autenticar órdenes e identificar las potestades de los operadores, está en los nuevos sistemas de pago que son necesarios para el comercio electrónico, en el control y protección de instalaciones críticas, en el futuro desarrollo de las relaciones de los ciudadanos con las administraciones e instituciones, etc.

El panorama en nuestro país lo podemos analizar a la luz de dos iniciativas: por una parte una red temática directamente relacionada con la seguridad y la criptografía y, por otra, la presencia de estos temas en el Plan Nacional de Investigación.

A finales del año 1998 se funda la Red Temática Iberoamericana de Criptografía y Seguridad de la Información, CriptoRed[216], como consecuencia del estudio que el coordinador de esta red, Jorge Ramió Aguirre, profesor de la Universidad Politécnica de Madrid, realiza con la profesora de la Universidad de La Laguna en Tenerife, Pino Caballero Gil sobre cuál era la extensión de la enseñanza de la criptografía en las universidades españolas. Los resultados de ese estudio se plasmaron en el artículo "E*nseñanza de la Criptografía y Seguridad de la Información en España: primer Informe sobre perfiles de asignaturas*"[217] publicado en el número 34, del mes de abril de 1999, de la Revista *SIC Seguridad Informática en Comunicaciones*.

[216]Ver http://www.criptored.upm.es/

[217]Ver http://www.criptored.upm.es/investigacion/informe.htm

Actualmente, la Red Iberoamericana de Criptografía y Seguridad de la Información cuenta con 681 miembros, de los cuales 361 son españoles, lo que supone un 51,4 % del total. De esos miembros españoles registrados, 106 miembros trabajan en 51 centros universitarios u organismos públicos de investigación, lo que supone una media de 3,6 personas por centro. Como complemento, en el sector privado se encuentran los 155 miembros restantes, que se reparten entre 118 empresas; lo que supone una media de 1,3 personas por empresa. La participación privada es claramente testimonial aunque, globalmente representa más de la mitad de los miembros de CriptoRed.

El 60,8 % de todos los miembros españoles de CriptoRed provienen de tan solo 13 centros diferentes, y a la cabeza de ellos están las Universidades Politécnica de Madrid (10,2 %) y Politécnica de Cataluña (7,0 %), seguida de la Universidad de Alicante (6,5 %).

Centro	Miembros	
Universidad Politécnica de Madrid	19	10,2%
Universidad Politécnica de Cataluña	13	7,0%
Universidad de Alicante	12	6,5%
Universidad de Málaga	10	5,4%
Universidad de Salamanca	10	5,4%
Consejo Superior de Investigaciones Científicas	8	4,3%
Universidad Carlos III de Madrid	8	4,3%
Universidad Autónoma de Barcelona	6	3,2%
Universidad de Castilla-La Mancha	6	3,2%
Universidad de Lleida	6	3,2%
Universidad Complutense de Madrid	5	2,7%
Universidad de Granada	5	2,7%
Universidad de Sevilla	5	2,7%

Aunque la pertenencia a CriptoRed puede servir para poner de manifiesto cuál es el interés real del mundo hispanoparlante en general, y del nacional en particular, por los temas de la seguridad informática y la Criptología, para conocer el interés de la administración española en estos temas es conveniente conocer algo sobre los proyectos de investigación que se financian en estos temas.

Buscando entre los casi 18.200 proyectos financiados por el Ministerio de Educación y Ciencia durante el quinquenio 2003-2007 dentro del Plan Nacional de Investigación, y utilizando palabras clave como *cripto, seguridad, pki*, etc. en la búsqueda, lo que se obtiene es una selección de 722 proyectos, de los cuales sólo 72 tienen una relación directa con el amplio campo de la seguridad informática y la criptografía.

Esos 72 proyectos se han realizado en 34 centros mayoritariamente universitarios, a excepción de algunos como, por ejemplo, el Instituto de Estudios Fotónicos, el Grupo Mondragón o la Fundación Robotiker. Los 8 primeros centros dan cuenta de un 51,4 % de los proyectos financiados, y hay que extender la lista hasta los 11 primeros para justificar el 61% de los proyectos.

Proyectos	Centro
9	Universidad Politécnica de Madrid
6	Universidad Carlos III de Madrid
4	Universidad Politécnica de Cataluña
4	Consejo Superior de Investigaciones Científicas
4	Universidad del País Vasco
4	Grupo MONDRAGON
3	Universidad de Alicante
3	Universidad de Valladolid
3	Universidad Rey Juan Carlos
2	Universidad de DEUSTO
2	Instituto de Ciencias Fotónicas
2	Universidad Abierta de Cataluña
2	Universidad de Lleida
2	Universidad de Sevilla
2	Universidad de Vigo
2	Universidad Rovira i Virgili

En cuanto a las personas, esos 72 proyectos fueron dirigidos por 51 investigadores principales diferentes, lo que marca una tasa de propuesta de proyectos de 1,41 proyectos por investigador principal en cinco años.

En cuanto a los temas, esos cinco años de investigación financiada por el Plan Nacional gestionado desde el Ministerio de Educación y Ciencia se han centrado en 13 temas diferentes y un cajón de sastre, de los cuales, los cinco más frecuentes, acaparan el 55,6 % de los proyectos. La distribución media sería de 5,1 proyectos por tema, pero esta cifra no es muy indicativa ya que la distribución temática es bastante poco uniforme.

Proyectos	Tema
11	Criptografía y comunicaciones cuánticas
9	Sistemas de detección de intrusiones
8	Redes de sensores y redes ad-hoc
7	Comercio electrónico
5	Comunicaciones digitales
5	Identificación biométrica
4	Curva elípticas y criptografía asociada
4	Algoritmos
3	Protección de los derechos de autor
3	Hardware de seguridad y criptográfico
2	Inteligencia y obtención de información
1	Confianza en los sistemas y en la sociedad digital
1	Seguridad y derechos civiles

Los temas en los que más se ha apostado en el pasado quinquenio son los de la criptografía y las comunicaciones cuánticas, la seguridad de los sistemas de información y el desarrollo de nuevos sistemas de seguridad que ayuden a proteger a aquellos, la identificación biométrica simple y multimodal atendiendo a múltiples identificadores intrínsecos (iris, huella dactilar, voz, etc.), las redes de sensores y demás redes ad-hoc de comunicación y transporte de todo tipo de información, y la protección de las comunicaciones digitales.

A continuación, en la siguiente tabla, se hace una relación de los investigadores principales que dirigieron los proyectos de investigación relacionados con los temas de seguridad y que fueron financiados por el Ministerio de Educación y Ciencia, y que han sido identificados en este sucinto análisis.

Nombre	Apellidos	Institución	Centro
ANTONIO	ACIN DAL MASCHIO	Instituto de Ciencias Fotónicas	
JOSÉ MANUEL	ARCO RODRÍGUEZ	Universidad de Alcalá	
ALEJANDRO	ARENAS MORENO	Universidad de Zaragoza	INSTITUTO DE BIOCOMPUTACIÓN Y FÍSICA DE SISTEMAS COMPLEJOS
ARMANDO	ASTARLOA CUÉLLAR	Universidad del País Vasco	DPTO. ELECTRÓNICA Y TELECOMUNICACIONES
EDUARDO	BOEMO SCALVINONI	Universidad Autónoma de Madrid	
PINO TERESA	CABALLERO GIL	Universidad de la Laguna	DPTO. ESTADÍSTICA, INVESTIGACIÓN OPERATIVA Y COMPUTACIÓN
ADÁN	CABELLO QUINTERO	Universidad de Sevilla	ESCUELA UNIVERSITARIA ARQUITECTURA TÉCNICA
ENRIQUE F.	CANTO NAVARRO	Universidad Rey Juan Carlos	ESCUELA SUPERIOR DE CIENCIAS EXPERIMENTALES Y TECNOLOGÍA
VALENTÍN	CARDEÑOSO PAYO	Universidad de Valladolid	ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE INFORMÁTICA
JOAN JOSEP	CLIMENT COLOMA	Universidad de Alicante	
JOSÉ LUIS	DE LA CUESTA ARZAMENDI	Universidad del País Vasco	INSTITUTO VASCO DE CRIMINOLOGÍA
FRANCISCO	DEL POZO GUERRERO	Universidad Politécnica de Madrid	DPTO. TECNOLOGÍA FOTÓNICA
JOSÉ LUIS	DEL VAL ROMAN	Universidad de Deusto	FACULTAD DE INGENIERÍA
JEAN-PIERRE	DESCHAMPS	Universidad Rey Juan Carlos	ESCUELA SUPERIOR DE CIENCIAS EXPERIMENTALES Y TECNOLOGÍA
JOSEP	DOMINGO FERRER	Universidad Rovira i Virgili	DPTO. INGENIERÍA INFORMÁTICA Y MATEMÁTICA
MIGUEL ÁNGEL	ESTEBAN NAVARRO	Universidad de Zaragoza	DEPARTAMENTO DE CIENCIAS DE LA DOCUMENTACIÓN
MIGUEL ÁNGEL	FERRER BALLESTER	Universidad de las Palmas de Gran Canaria	ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN
JOSÉ LUIS	FERRER GOMILA	Universidad de las Islas Baleares	DPTO. CIENCIAS MATEMÁTICAS E INFORMÁTICA

Nombre	Apellidos	Institución	Centro
JORGE	FORNÉ MUÑOZ	Universidad Politécnica de Cataluña	OFICINA TRANSFERENCIA DE RESULTADOS DE INVESTIGACIÓN (OTRI)
JUAN FRANCISCO	GÁLVEZ GÁLVEZ	Universidad de Vigo	ESCUELA SUPERIOR DE INGENIERÍA INFORMÁTICA
PRISCILA	GARCÍA FERNÁNDEZ	Consejo Superior de Investigaciones Científicas	INSTITUTO DE ÓPTICA
JESÚS	GARCÍA LÓPEZ DE LACALLE	Universidad Politécnica de Madrid	ESCUELA UNIVERSITARIA INFORMÁTICA
JORGE	GARCÍA VIDAL	Universidad Politécnica de Cataluña	DPTO. DE ARQUITECTURA DE COMPUTADORES
LUIS JAVIER	GARCÍA VILLALBA	Universidad Complutense de Madrid	
ÁNGEL	GREDIAGA OLIVO	Universidad de Alicante	ESCUELA POLITÉCNICA SUPERIOR
LUIS	HERNÁNDEZ ENCINAS	Consejo Superior de Investigaciones Científicas	INSTITUTO DE FÍSICA APLICADA (IFA)
JORDI	HERRERA JOANCOMARTI	Universidad Abierta de Cataluña	
EDUARDO JUAN	JACOB TAQUET	Universidad del País vasco	ESCUELA TÉCNICA SUPERIOR ING.INDUSTRIALES Y TELECOMUNICACIÓN
JOSÉ IGNACIO	LATORRE SENTÍS	Universidad de Barcelona	DPTO. ESTRUCTURA Y CONSTITUYENTES DE LA MATERIA
LOURDES	LÓPEZ SANTIDRIÁN	Universidad Politécnica de Madrid	DPTO. INGENIERÍA Y ARQUITECTURA TELEMÁTICAS
PIETRO	MANZONI	Universidad Politécnica de Valencia	
ANDRÉS	MARÍN LÓPEZ	Universidad Carlos III de Madrid	DPTO. INGENIERÍA TELEMÁTICA
JOSÉ FERNAN	MARTÍNEZ ORTEGA	Universidad Politécnica de Madrid	DPTO. INGENIERÍA Y ARQUITECTURA TELEMÁTICAS
JOSÉ IGNACIO	MARTÍNEZ TORRE	Universidad Rey Juan Carlos	ESCUELA SUPERIOR DE CIENCIAS EXPERIMENTALES Y TECNOLOGÍA
JOSEP M.	MIRET BIOSCA	Universidad de Lleida	ESCUELA POLITÉCNICA SUPERIOR
FAUSTO	MONTOYA VITINI	Consejo Superior de Investigaciones Científicas	INSTITUTO DE FÍSICA APLICADA (IFA) - CEDEF
JAVIER	ORTEGA GARCÍA	Universidad Politécnica de Madrid	ESCUELA UNIVERSITARIA ING. TÉCNICA TELECOMUNICACIÓN
JUAN	PÉREZ TORRES	Instituto de Ciencias Fotónicas	

Nombre	Apellidos	Institución	Centro
RAFAEL	POUS ANDRÉS	Universidad Politécnica de Cataluña	ESCUELA POLITÉCNICA SUPERIOR. CASTELLDEFELS
CARLOS	RUIZ MIGUEL	Universidad de Santiago de Compostela	DPTO. DERECHO PÚBLICO Y TEORÍA DEL ESTADO
PEDRO JESÚS	SALAS PERALTA	Universidad Politécnica de Madrid	DPTO. TECNOLOGÍAS ESPECIALES APLICADAS A LA TELECOMUNICACIÓN
ÁNGEL	SÁNCHEZ CALLE	Universidad Rey Juan Carlos	ESCUELA SUPERIOR DE CIENCIAS EXPERIMENTALES Y TECNOLOGÍA
LUIS	SÁNCHEZ FERNÁNDEZ	Universidad Carlos III de Madrid	DPTO. INGENIERÍA TELEMÁTICA
RAÚL	SÁNCHEZ REILLO	Universidad Carlos III de Madrid	DPTO. TECNOLOGÍA ELECTRÓNICA
DAVID JOSÉ	SANTOS MEJÍA	Universidad de Vigo	ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN
Mª FELISA	SEDANO RUIZ	Universidad Politécnica de Madrid	DPTO. INGENIERÍA DE SISTEMAS TELEMÁTICOS
JOSÉ MARÍA	SIERRA CÁMARA	Universidad Carlos III de Madrid	DPTO. INFORMÁTICA
JUAN GABRIEL	TENA AYUSO	Universidad de Valladolid	DPTO. ÁLGEBRA, GEOMETRÍA Y TOPOLOGÍA
VICENC	TORRA REVENTÓS	Consejo Superior de Investigaciones Científicas	INSTITUTO DE INVESTIGACIÓN EN INTELIGENCIA ARTIFICIAL (IIIA)
ROBERTO	URIBEETXEBERRIA EZPELETA	Universidad de Mondragón	INFORMÁTICA

En cuanto a la Unión Europea, decir que el programa de trabajo[218] del comité sobre *Information & Comunications Technbologies* (ICT) del 7º Programa Marco de la Unión Europea define las prioridades aplicables en las convocatorias de propuestas de financiación. Las prioridades marcadas son fieles al diseño global del 7º Programa Marco y del Programa Específico, y se mantienen en la línea de las prioridades definidas en la iniciativa i2010 (*A European Information Society for growth and employmen*t). Así mismo, la convocatoria recoge los consejos hechos por los miembros del Comité de Programa ICT y por el *IST Advisory Group*[219], de las *Plataformas Tecnológicas Europeas*[220], y de una serie de consultas particulares hechas a los principales actores europeos en este ámbito.

[218]Ver http://cordis.europa.eu/fp7/ict/programme/workprogramme_en.html
[219]Ver http://cordis.europa.eu/ist/istag.htm
[220]Ver http://cordis.europa.eu/technology-platforms/home_en.html

El programa de trabajo ICT está dividido en siete retos de interés estratégico para la sociedad europea, y en un programa para la investigación en "*Tecnologías Futuras y Emergentes*". De todos esos enfoques, solo dos podrían albergar algún esfuerzo de tipo criptológico.

En el primer reto[221], "*Pervasive and trusted network and service infrastructures*", se afronta el futuro de las redes digitales que desde hace más de quince años se han instalado en el seno de la sociedad europea: Internet, redes móviles, redes fijas y por radio. En él se tratan tanto los aspectos técnicos como los de servicios a la sociedad, por lo que la seguridad de esos sistemas es algo que los gestores europeos no deberán olvidar a la hora de repartir los millones de euros que tiene asignado el programa ICT entre 2007 y 2013. En este caso, la criptografía no es un objetivo en sí pero, en principio, resultará muy necesaria. Quizás no se favorezca el desarrollo de nuevos algoritmos o protocolos criptográficos propiamente dichos, pero si se tendrá que atender a la implementación e instalación de los ya conocidos, lo cual suele ser una importante fuente de debilidades en los escenarios reales.

En el tercer reto[222], el titulado de "*Components, systems and engineering*", la Unión Europea trata de los sistemas denominados "*embedded*" que aportan valor a multitud de productos autónomos que van desde juguetes infantiles hasta automóviles de alta gama, y que constituyen una "*electrónica inteligente*" que es parte de industrias tan importantes como la automovilista, la aeronáutica, las de telecomunicaciones, las comunicaciones móviles, la salud y, en general, de la automatización industrial. Estos sistemas cada día se aproximan mas al modelo de un software ejecutándose en una máquina con capacidades computacionales de propósito cuasi-general y, por este motivo, a estos sistemas les afectan muchos de los riesgos que ya conocemos gracias al software convencional que opera en ordenadores fijos o en equipos móviles. La seguridad de estos sistemas terminará siendo un aspecto muy importante a la hora de diseñarlos y desarrollarlos, por lo que, en el futuro, éste desarrollo quizás también favorezca el desarrollo de la criptología y sus usos.

[221]Ver http://cordis.europa.eu/fp7/ict/programme/challenge1_en.html

[222]Ver http://cordis.europa.eu/fp7/ict/programme/challenge3_en.html

Organismos y departamentos de la Administración Pública con competencia en temas criptográficos

En España, las instituciones que más tienen que ver con la criptología y tecnologías anejas son el Ministerio del Interior y el Centro Nacional de Inteligencia.

El Centro Nacional de Inteligencia, a través de su Centro Criptológico Nacional (CCN)[223], es la autoridad responsable de coordinar las acciones de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, y garantizar la seguridad real de las tecnologías de la información utilizadas en ese ámbito, así como informar sobre la adquisición coordinada del material criptológico. Además de esto, el CCN también sería el encargado de formar al personal de la Administración que deba convertirse en especialista en este campo.

En este sentido, el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información[224], y autoridad de certificación criptológica. Asimismo, el CCN vela por el cumplimiento de la normativa sobre protección de la información clasificada en los sistemas de información y telecomunicaciones de la Administración[225]. Para el desarrollo de estas funciones, el CCN puede coordinarse con las comisiones nacionales a las que las leyes les otorguen responsabilidades en el ámbito de los sistemas de las tecnologías de la información y de las comunicaciones.

Recientemente, el CCN ha montado su equipo de respuestas ante incidentes de seguridad informática y lo ha llamado CCN-CERT[226]. El objetivo principal de este equipo es contribuir a mejorar el nivel de seguridad de los sistemas de información en las administraciones públicas españolas. Su misión es ayudar a dichas administraciones a responder de forma rápida y eficiente ante las amenazas de seguridad que afecten a sus sistemas de información, y para ello opera en tres grandes líneas de actuación: servicios de alertas sobre nuevas amenazas y vulnerabilidades, labores de investigación, formación y divulgación de seguridad de la información, y prestación de servicios de apoyo y coordinación para la resolución de incidentes concretos.

---

[223]Ver www.ccn.cni.es

[224]Ver www.oc.ccn.cni.es

[225]Y esto lo hace de acuerdo con lo señalado en el artículo 4, punto e y f, de la Ley 11/2002 de 6 de mayo.

[226]Ver https://www.ccn-cert.cni.es/

La relación del Ministerio del Interior en temas criptológicos llega a través de lo que se ha dado en conocer como e-DNI, o DNI electrónico[227]. Este proyecto, es una actualización tecnológica del documento de identidad español que desde hace cincuenta años da identidad legal a sus ciudadanos. Este DNI electrónico sirve para acreditar electrónicamente a cada ciudadano en los procesos de autenticación que éstos participen y sirve también para firmar digitalmente documentos electrónicos, otorgándoles la misma validez jurídica que la firma manuscrita. Para ello, en el interior del eDNI se custodian dos identidades RSA certificadas y diferentes, una para autenticación y otra para firma. Las longitudes de las claves RSA que constituyen esas identidades son de 1.024 bits. Ambas identidades se generaron dentro de la tarjeta cuando se inicializó ésta, y fueron certificadas digitalmente por la infraestructura de clave pública del DNI, al expedir dicho documento. La longitud de las claves que firman los certificados digitales es de 2048 bits. Además de estos datos, en el chip digital[228] también se guarda una plantilla biométrica de la impresión dactilar, la fotografía del titular, la imagen digitalizada de su firma manuscrita y los mismos datos de filiación que son visibles en el exterior de la tarjeta.

[227]Ver http://www.dnielectronico.es

[228]Se trata del chip ST19WL34, ver http://www.st.com/stonline/products/literature/bd/10777.pdf

Este cuaderno invita a pasearse por decenas de siglos de la historia de la humanidad en las que la protección de los secretos ha ido siempre de la mano de los grandes. Esta sucinta revisión histórica y cronológica de lo que hoy se conoce como Criptología, permite ver cómo la información y la protección de ésta son dos ingredientes que ayudan a levantar imperios y a hacer rodar coronas. Desde utilizar tecnologías tan sencillas como un bastón de mando, pasando por el imperio de las máquinas en el cifrado y el criptoanálisis, hemos llegado a niveles de computación colectiva y planetaria nunca antes imaginados. Esta historia no se acaba aquí, no se termina con la globalización y el reinado del capital y la economía, sino que continua más allá de nuestros días. Quizás conocer lo ya sucedido pueda arrojar algo de luz sobre lo que habrá de suceder.

Jorge Dávila Muro
Profesor Titular de Universidad
Facultad de Informática de la UPM