Historia de la criptografía

La **historia de la criptografía** se remonta a miles de años. Hasta décadas recientes, ha sido la historia de la criptografía clásica — los métodos de cifrado que usan papel y lápiz, o quizás ayuda mecánica sencilla. A principios del siglo XX, la invención de máquinas mecánicas y electromecánicas complejas, como la máquina de rotores Enigma, proporcionaron métodos de cifrado más sofisticados y eficientes; y la posterior introducción de la electrónica y la computación ha permitido sistemas elaborados que siguen teniendo gran complejidad.

La evolución de la criptografía ha ido de la mano de la evolución del criptoanálisis — el arte de "romper" los códigos y los cifrados. Al principio, el descubrimiento y aplicación del análisis de frecuencias a la lectura de las comunicaciones cifradas ha cambiado en ocasiones el curso de la historia. De esta manera, el telegrama Zimmermann provocó que Estados Unidos entrara en la Primera Guerra Mundial; y la lectura, por parte de los Aliados, de los mensajes cifrados de la Alemania nazi, puede haber acortado la Segunda Guerra Mundial hasta dos años.

Hasta los años 70, la criptografía segura era dominio casi exclusivo de los gobiernos. Desde entonces, dos sucesos la han colocado de lleno en el dominio público: la creación de un estándar de cifrado público (DES); y la invención de la criptografía asimétrica.

1 Criptografía clásica

Véase también: Cifrado clásico

El uso más antiguo conocido de la criptografía se halla en jeroglíficos no estándares tallados en monumentos del Antiguo Egipto (hace más de 4500 años). Sin embargo, no se piensa que sean intentos serios de comunicación secreta, sino intentos de conseguir misterio, intriga o incluso diversión para el espectador letrado. Son ejemplos de otros usos de la criptografía, o de algo que se le parece. Más tarde, eruditos hebreos hicieron uso de sencillos cifrados por sustitución monoalfabéticos (como el cifrado Atbash), quizás desde el 600 al 500 a. C. La criptografía tiene una larga tradición en las escrituras religiosas que podrían ofender a la cultura dominante o a las autoridades políticas. Quizás el caso más famoso es el 'Número de la bestia', del libro del Apocalipsis en el Nuevo Testamento cristiano. El '666' puede ser una forma criptográfica (es decir, cifrada) de ocultar una referencia peligrosa; muchos expertos creen que es una referencia oculta al Imperio romano, o más probablemente al propio emperador Nerón (y así a las políticas persecutorias romanas), que sería entendida por los iniciados (los que 'tenían la clave del entendimiento'), y sin embargo sería segura o al menos negable (y por tanto 'menos' peligrosa) si atraía la atención de las autoridades. Al menos para las escrituras ortodoxas cristianas, casi toda esta necesidad de ocultación desapareció con la conversión y adopción del cristianismo como religión oficial del Imperio por parte del emperador Constantino.

Una escitala, uno de los primeros dispositivos de cifrado.

Se dice que los griegos de la época clásica conocían el cifrado (por ejemplo, se dice que los militares espartanos utilizaban el cifrado por transposición de la escítala). Heródoto nos habla de mensajes secretos ocultos físicamente detrás de la cera en tablas de madera, o como tatuajes en la cabeza de un esclavo, bajo el cabello, aunque esto no son ejemplos verdaderos de criptografía, ya que el mensaje, una vez conocido, es legible directamente; esto se conoce como esteganografía. Los romanos sí sabían algo de criptografía con toda seguridad (por ejemplo, el cifrado César y sus variaciones). Hay una mención antigua a un libro sobre criptografía militar romana (especialmente la de Julio César); desafortunadamente, se ha perdido.

En India también se conocía la criptografía. El Kama Sutra la recomienda como técnica para que los amantes se comuniquen sin ser descubiertos.[*cita requerida*]

2 Criptografía medieval

Fue probablemente el análisis textual del Corán, de motivación religiosa, lo que llevó a la invención de la téc-

nica del análisis de frecuencias para romper los cifrados por sustitución monoalfabéticos, en algún momento alrededor del año 1000. Fue el avance criptoanalítico más importante hasta la Segunda Guerra Mundial. Esencialmente, todos los cifrados quedaron vulnerables a esta técnica criptoanalítica hasta la invención del cifrado polialfabético por Leon Battista Alberti (1465), y muchos lo siguieron siendo desde entonces.[*cita requerida*]

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

La criptografía, el criptoanálisis y la traición cometida por agentes y mensajeros en la conspiración de Babington, durante el reinado de la reina Isabel I de Inglaterra, provocaron la ejecución de María, reina de los escoceses.[*cita requerida*] Un mensaje cifrado de la época de el hombre de la máscara de hierro (descifrado poco antes del año 1900 por Étienne Bazeries) ha arrojado algo de luz (no definitiva, lamentablemente) sobre la identidad real de ese prisionero legendario y desafortunado. La criptografía y su mala utilización estuvieron implicadas en la conspiración que condujo a la ejecución de Mata Hari y en la confabulación que provocó la ridícula condena y encarcelamiento de Dreyfus, ambos hechos acaecidos a principios del siglo XX.[*cita requerida*] Afortunadamente, los criptógrafos también jugaron su papel para exponer las maquinaciones que provocaron los problemas de Dreyfus; Mata Hari, en cambio, fue fusilada.

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

3 Criptografía desde 1800 hasta la Segunda Guerra Mundial

Aunque la criptografía tiene una historia larga y compleja, hasta el siglo XIX no desarrolló nada más que soluciones *ad hoc* para el cifrado y el criptoanálisis (la ciencia que busca debilidades en los criptosistemas). Ejemplos de lo último son el trabajo de Charles Babbage, en la época de la Guerra de Crimea, sobre el criptoanálisis matemático de los cifrados polialfabéticos, redescubierto y publicado algo después por el prusiano Fiedrich Kasiski. En esa época, el conocimiento de la criptografía consistía normalmente en reglas generales averiguadas con dificultad; véase, por ejemplo, los escritos de Auguste Kerckhoffs sobre criptografía a finales del siglo XIX. Edgar Allan Poe desarrolló métodos sistemáticos para resolver cifrados en los años 1840. Concretamente, colocó un anuncio de sus capacidades en el periódico de Filadelfia *Alexander's Weekly (Express) Messenger*, invitando al envío de cifrados, que él procedía a resolver. Su éxito creó excitación entre el público durante unos meses. Más tarde escribió un ensayo sobre los métodos criptográficos que resultaron útiles para descifrar los códigos alemanes empleados durante la Primera Guerra Mundial.

Proliferaron métodos matemáticos en la época justo anterior a la Segunda Guerra Mundial (principalmente con la aplicación, por parte de William F. Friedman, de las técnicas estadísticas al desarrollo del criptoanálisis y del cifrado, y la rotura inicial de Marian Rejewski de la versión del Ejército Alemán del sistema Enigma). Tanto la criptografía como el criptoanálisis se han hecho mucho más matemáticas desde la Segunda Guerra Mundial. Aun así, ha hecho falta la popularización de los ordenadores y de Internet como medio de comunicación para llevar la criptografía efectiva al uso común por alguien que no sea un gobierno nacional u organizaciones de tamaño similar.

4 Criptografía de la Segunda Guerra Mundial

En la Segunda Guerra Mundial, las máquinas de cifrado mecánicas y electromecánicas se utilizaban extensamente, aunque —allá donde estas máquinas eran poco prácticas— los sistemas manuales continuaron en uso. Se hicieron grandes avances en la rotura de cifrados, todos en secreto. La información acerca de esta época ha empezado a desclasificarse al llegar a su fin el periodo de secreto británico de 50 años, al abrirse lentamente los archivos estadounidenses y al irse publicando diversas memorias y artículos.

Los alemanes hicieron gran uso de diversas variantes de una máquina de rotores electromecánica llamada Enigma. El matemático Marian Rejewski, de la Oficina de Cifrado polaca, reconstruyó en diciembre de 1932 la máquina Enigma del ejército alemán, utilizando la matemática y la limitada documentación proporcionada por el capitán Gustave Bertrand, de la inteligencia militar francesa. Este fue el mayor avance del criptoanálisis en más de mil años. Rejewsky y sus colegas de la Oficina de Cifrado, Jerzy Różycki y Henryk Zygalski, continuaron desentrañando la Enigma y siguiendo el ritmo de la evolución de los componentes de la máquina y los procedimientos de cifrado. Al irse deteriorando los recursos financieros de Polonia por los cambios introducidos por

La máquina Enigma fue utilizada extensamente por la Alemania nazi; el criptoanálisis aplicado por los aliados proporcionó una vital inteligencia Ultra.

los alemanes, y al irse avecinando la guerra, la Oficina de Cifrado, bajo órdenes del estado mayor polaco, presentaron a representantes de la inteligencia francesa y británica los secretos del descifrado de la máquina Enigma, el 25 de julio de 1939, en Varsovia.

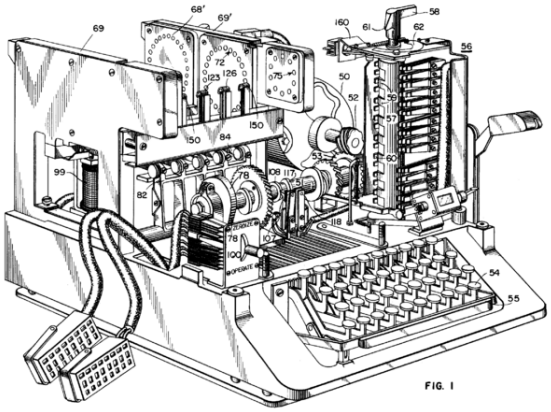
Poco después de que estallara la Segunda Guerra Mundial el 1 de septiembre de 1939, el personal clave de la Oficina de Cifrado fue evacuado hacia el sureste; el 17 de septiembre, tras la entrada de la Unión Soviética en el este de Polonia, cruzaron Rumanía. Desde allí alcanzaron París, en Francia; en la estación de inteligencia polaco-francesa PC Bruno, cerca de París, continuaron rompiendo la Enigma, colaborando con los criptólogos británicos de Bletchley Park, que se habían puesto al día con el tema. Con el tiempo, los criptólogos británicos —en los que se incluían lumbreras como Gordon Welchman y Alan Turing, el fundador conceptual de la computación moderna— hicieron progresar sustancialmente la escala y tecnología del descifrado Enigma.

El 19 de abril de 1945 se ordenó a los oficiales superiores británicos que nunca debían revelar que se había roto el código de la máquina Enigma alemana, porque esto le daría la oportunidad al enemigo de decir que "no fueron vencidos justa y satisfactoriamente".

Los criptógrafos de la Armada estadounidense (en cooperación con criptógrafos británicos y holandeses a partir de 1940) rompieron varios sistemas criptográficos de la Armada japonesa. La rotura de uno de ellos, el JN-25, condujo a la célebre victoria estadounidense de la Batalla de Midway. Un grupo del ejército estadounidense, el SIS, consiguió romper el sistema criptográfico diplomático japonés de alta seguridad (una máquina electromecánica llamada Púrpura por los estadounidenses) antes incluso del comienzo de la Segunda Guerra Mundial. Los estadounidenses llamaron a la inteligencia derivada del criptoanálisis, quizás en especial la derivada de la máquina Púrpura, como «Magic» (Magia). Finalmente los británicos se decidieron por «Ultra» para la inteligencia derivada del criptoanálisis, en especial la derivada del tráfico de mensajes cifrados con las diversas Enigmas. Un término británico anterior fue para Ultra fue «Boniface».

Los militares alemanes también desarrollaron varios intentos de implementar mecánicamente la libreta de un solo uso. Bletchley Park los llamó cifrados Fish, y Max Newman y sus colegas diseñaron e implementaron el primer ordenador electrónico digital programable del mundo, Colossus, para ayudarles con el criptoanálisis. La Oficina de Asuntos Exteriores alemana empezó a usar la libreta de un solo uso en 1919; parte de este tráfico fue leído en la Segunda Guerra Mundial como resultado de la recuperación de material importante en Sudamérica que fue desechado con poco cuidado por un mensajero alemán.

La Oficina de Asuntos Exteriores japonesa utilizó un sistema eléctrico lógico basado en uniselectores (llamado Púrpura por EEUU), y también utilizó varias máquinas similares para los agregados de algunas embajadas japonesas. Una de estas recibió el nombre de «Máquina M» por EEUU, y otra fue apodada «Red». Todas fueron rotas en mayor o menor grado por los aliados.



SIGABA se describe en la Patente USPTO nº 6175625, registrada en 1944 pero no publicada hasta 2001.

Las máquinas de cifrado aliadas utilizadas en la Segunda Guerra Mundial incluían la Typex británica y la SIGABA estadounidense; ambos eran diseños de rotores electromecánicos similares en espíritu a la Enigma, aunque con mejoras importantes. No se tiene constancia de que ninguna de ellas fuera rota durante la guerra. Los polacos utilizaron la máquina Lacida, pero se demostró que era poco segura y se canceló su uso. Las tropas de campo

utilizaron las familias M-209 y M-94. Los agentes SOE utilizaron inicialmente «cifrados de poema» (las claves eran poemas memorizados), pero más avanzada la guerra empezaron a utilizar libretas de un solo uso.

5 Criptografía moderna

5.1 Shannon

La era de la criptografía moderna comienza realmente con Claude Shannon, que podría decirse que es el padre de la criptografía matemática. En 1949 publicó el artículo *Communication Theory of Secrecy Systems* en la Bell System Technical Journal, y poco después el libro *Mathematical Theory of Communication*, con Warren Weaver. Estos trabajos, junto con los otros que publicó sobre la teoría de la información y la comunicación, establecieron una sólida base teórica para la criptografía y el criptoanálisis.

5.2 Criptosecretismo

Poco a poco la criptografía desapareció de la escena para quedarse dentro de las organizaciones gubernamentales dedicadas al espionaje y el contraespionaje. De ellas la más importante fue la NSA de Estados Unidos.

La NSA acaparó y bloqueó casi totalmente la publicación de cualquier avance en el campo de la criptografía desde principios de los 50 hasta mediados de los 70. Por esta razón casi toda la información disponible sobre el tema era la básica y totalmente anticuada. Sus estrategias para conseguir esto fueron las siguientes:

- La NSA disponía de un importante presupuesto lo que le permitía pagar bien a sus empleados, disponer de una plantilla de colaboradores amplia y de conseguir equipamiento de difícil acceso por su precio. Esto conseguía atraer a los mejores investigadores en criptografía.
- Para trabajar, colaborar o recibir cursos y/o recursos de la NSA a los investigadores se les obligaba a mantener secreta la información y someter sus futuros trabajos al control de la NSA. Esto provocaba que para acceder a cierto tipo de información era necesario pertenecer al grupo de 'colaboradores de la NSA'.
- Se presionaba para que no se publicaran artículos o libros sobre criptografía y sobre la propia NSA. Por ejemplo se presionó a David Kahn para evitar la publicación de su libro **Codebreakers**. Finalmente la NSA consiguió quitar tres fragmentos específicos del libro.
- Por ley revelar información sobre criptografía de la II guerra mundial era un acto de traición.
- La NSA supervisaba todas las solicitudes de patentes relacionadas con la criptografía y estaba autorizada por ley para clasificar como secreto cualquier idea que considerara peligrosa que fuera de dominio público.
- La NSA presionaba para cerrar o incluso que no se llegaran a abrir proyectos de investigación que considerar amenazantes. Por ejemplo, consiguió cerrar el proyecto de investigación criptográfica del Centro de Investigación de la fuerza aérea de Cambridge en el que trabajaba Horst Feistel. Posteriormente el mismo Horst Feistel achacó a la NSA el no conseguir organizar un proyecto de investigación sobre criptografía en el Mitre.

Todos estos puntos provocaban que muchos investigadores aceptaran colaborar con la NSA ya que llegaban a la idea de que renunciado a colaborar con ella jamás descubrirían nada que valiese la pena ni tendrían una carrera profesional satisfactoria.

5.3 Un estándar de cifrado

A mediados de los 70 se vivieron dos importantes avances públicos (es decir, no secretos). El primero fue la publicación del borrador del Data Encryption Standard en el *Registro Federal* estadounidense el 17 de marzo de 1975. La propuesta fue enviada por IBM, por invitación de la Oficina Nacional de Estándares (ahora NIST), en un esfuerzo por desarrollar sistemas de comunicación electrónica segura para las empresas como los bancos y otras organizaciones financieras grandes. Tras «asesoramiento» y ciertas modificaciones por parte de la NSA, fue adoptado y publicado como un Federal Information Processing Standard en 1977 (actualmente el FIPS 46-3). El DES fue el primer cifrado accesible públicamente que fue «bendecido» por una agencia nacional como la NSA. La publicación de sus especificaciones por la NBS estimuló una explosión del interés público y académico por la criptografía.

DES fue suplantado oficialmente por el Advanced Encryption Standard (AES) en 2001, cuando el NIST anunció el FIPS 197. Tras una competición abierta, el NIST seleccionó el algoritmo Rijndael, enviado por dos criptógrafos belgas, para convertirse en el AES. El DES, y otras variantes más seguras (como el Triple DES; ver FIPS 46-3), todavía se utilizan hoy en día, y se han incorporado en muchos estándares nacionales y de organizaciones. Sin embargo, se ha demostrado que el tamaño de su clave, 56 bits, es insuficiente ante ataques de fuerza bruta (un ataque así, llevado a cabo por el grupo pro libertades civiles digitales Electronic Frontier Foundation en 1997, tuvo éxito en 56 horas —la historia se cuenta en *Cracking DES*, publicado por O'Reilly Associates). Como resultado, hoy en día el uso sin más del cifrado DES es sin duda inseguro para los nuevos diseños de criptosistemas,

y los mensajes protegidos por viejos criptosistemas que utilizan el DES, y de hecho todos los mensajes enviados desde 1976 que usan el DES, también están en riesgo. A pesar de su calidad inherente, el tamaño de la clave DES (56 bits) fue considerado por algunos como demasiado pequeño incluso en 1976; quizás la voz más sonora fue la de Whitfield Diffie. Había sospechas de que las organizaciones gubernamentales tenían suficiente potencia de cálculo para romper los mensajes DES; ahora es evidente que otros han logrado esa capacidad.

5.4 Clave pública

El segundo desarrollo, en 1976, fue quizás más importante todavía, ya que cambió de manera fundamental la forma en la que los criptosistemas pueden funcionar. Fue la publicación del artículo *New Directions in Cryptography*, de Whitfield Diffie y Martin Hellman. Introdujo un método radicalmente nuevo para distribuir las claves criptográficas, dando un gran paso adelante para resolver uno de los problemas fundamentales de la criptografía, la distribución de claves, y ha terminado llamándose intercambio de claves Diffie-Hellman. El artículo también estimuló el desarrollo público casi inmediato de un nuevo tipo de algoritmo de cifrado, los algoritmos de cifrado asimétrico.

Antes de eso, todos los algoritmos de cifrado útiles eran algoritmos de cifrado simétrico, en los que tanto el remitente como el destinatario utilizan la misma clave criptográfica, que ambos deben mantener en secreto. Todas las máquinas electromecánicas utilizadas en la Segunda Guerra Mundial eran de esta clase lógica, al igual que los cifrados César y Atbash y en esencia todos los cifrados y sistemas de códigos de la historia. La «clave» de un código es, por supuesto, el libro de códigos, que debe asimismo distribuirse y mantenerse en secreto.

En estos sistemas era necesario que la partes que se iban a comunicar intercambiaran las claves de alguna forma segura antes del uso del sistema (el término que se solía utilizar era «mediante un canal seguro»), como un mensajero de confianza con un maletín esposado a su muñeca, o un contacto cara a cara, o una paloma mensajera fiel. Este requisito nunca es trivial y se hace inmantenible rápidamente al crecer el número de participantes, o cuando no hay canales seguros disponibles para el intercambio de claves, o cuando las claves cambian con frecuencia (una práctica criptográfica sensata). En particular, si se pretende que los mensajes sean seguros frente a otros usuarios, hace falta una clave distinta para cada par de usuarios. Un sistema de este tipo se conoce como criptosistema de clave secreta o de clave simétrica. El intercambio de claves D-H (y las posteriores mejoras y variantes) hizo que el manejo de estos sistemas fuera mucho más sencillo y seguro que nunca.

En contraste, el cifrado de clave asimétrica utiliza un par de claves relacionadas matemáticamente, en el que una de ellas descifra el cifrado que se realiza con la otra. Algunos (pero no todos) de estos algoritmos poseen la propiedad adicional de que una de las claves del par no se puede deducir de la otra por ningún método conocido que no sea el ensayo y error. Con un algoritmo de este tipo, cada usuario sólo necesita un par de claves. Designando una de las claves del par como privada (siempre secreta) y la otra como pública (a menudo visible), no se necesita ningún canal seguro para el intercambio de claves. Mientras la clave privada permanezca en secreto, la clave pública puede ser conocida públicamente durante mucho tiempo sin comprometer la seguridad, haciendo que sea seguro reutilizar el mismo par de claves de forma indefinida.

Para que dos usuarios de un algoritmo de clave asimétrica puedan comunicarse de forma segura a través de un canal inseguro, cada usuario necesita conocer su clave pública y privada y la clave pública del otro usuario. Véase este escenario básico: Alicia y Roberto tienen cada uno un par de claves que han utilizado durante años con muchos otros usuarios. Al comienzo de su mensaje, intercambian las claves públicas sin cifrar por una línea insegura. Luego Alicia cifra un mensaje utilizando su clave privada, y luego re-cifra el resultado utilizando la clave pública de Roberto. Luego el mensaje cifrado doblemente se envía en forma de datos digitales mediante un cable desde Alicia hasta Roberto. Roberto recibe el flujo de bits y lo descifra usando su clave privada, y luego descifra el resultado utilizando la clave pública de Alicia. Si el resultado final es un mensaje reconocible, Roberto puede estar seguro de que el mensaje procede realmente de alguien que conoce la clave privada de Alicia, y que cualquiera que haya pinchado el canal necesitará las claves privadas de Alicia y Roberto para entender el mensaje.

La efectividad de los algoritmos asimétricos depende de una clase de problemas matemáticos conocidos como funciones de un solo sentido, que requieren relativamente poca potencia de cálculo para ejecutarse, pero muchísima potencia para calcular la inversa. Un ejemplo clásico de función de un sentido es la multiplicación de números primos grandes. Es bastante rápido multiplicar dos primos grandes, pero muy difícil factorizar el producto de dos primos grandes. Debido a las propiedades matemáticas de las funciones de un sentido, la mayor parte de las claves posibles tienen poca calidad para su uso criptográfico; solo una pequeña parte de las claves posibles de una cierta longitud son candidatas ideales, y por tanto los algoritmos asimétricos requieren claves muy largas para alcanzar el mismo nivel de seguridad proporcionado por las claves simétricas, relativamente más cortas. Las exigencias de generar el par de claves y realizar el cifrado/descifrado hacen que los algoritmos asimétricos sean costosos computacionalmente. Como, a menudo, los algoritmos simétricos pueden usar como clave cualquier serie seudoaleatoria de bits, se puede generar rápidamente una clave de sesión desechable para uso a corto plazo. Por consiguiente, es una práctica común utilizar una clave asimétrica larga para intercambiar una clave simétrica

desechable mucho más corta (pero igual de fuerte). El algoritmo asimétrico, más lento, envía de forma segura una clave simétrica de sesión, y entonces el algoritmo simétrico, más rápido, toma el control para el resto del mensaje.

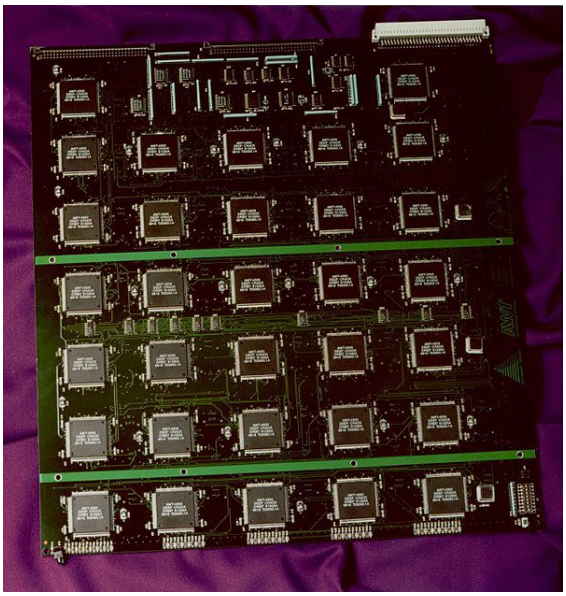
La criptografía de clave asimétrica, el intercambio de claves Diffie-Hellman y los famosos algoritmos de clave pública/clave privada (es decir, lo que se suele llamara algoritmo RSA), parecen haber sido desarrollados de manera independiente en una agencia de inteligencia británica antes del anuncio público de Diffie y Hellman en el 76. El GCHQ ha publicado documentos que afirman que ellos habían desarrollado la criptografía de clave pública antes de la publicación del artículo de Diffie y Hellman. Varios artículos clasificados fueron escritos en el GCHQ durante los años 60 y 70, que finalmente llevaron a unos sistemas esencialmente idénticos al cifrado RSA y al intercambio de claves Diffie-Hellman en 1973 y 1974. Algunos de ellos se acaban de publicar, y los inventores (James H. Ellis, Clifford Cocks y Malcolm Williamson han hecho público parte de su trabajo.

5.5 Política y criptografía

Esto acabó con el monopolio sobre la criptografía que mantenían las organizaciones gubernamentales en todo el mundo (Ver *Cripto* de Steven Levy, un relato periodístico sobre la controversia política en EEUU). Por primera vez en la historia, la gente externa a las organizaciones gubernamentales tenía acceso a criptografía que el gobierno no podía romper fácilmente. Esto desató una considerable controversia tanto pública como privada que todavía no ha amainado. Hay una confrontación entre las organizaciones gubernamentales (inteligencia y seguridad nacional) que quieren mantener el control de la criptografía y por otro lado los defensores de la privacidad, sectores académicos y empresas privadas vinculadas a las nuevas tecnologías, donde se desarrollan avances públicos sobre criptografía, que quieren poner a disposición del gran público y/o explotar comercialmente estos nuevos conocimientos. Esto provoca cambios legislativos para establecer un marco legal sobre el uso, exportación o control de las tecnologías criptográficas. Por ejemplo en Estados Unidos entre 1982 y 1992 hay muchos cambios legislativos que dan mayor o menor poder sobre la criptografía a la NSA, según el bando preponderante en cada momento.[1]

El actor más notable en la defensa del cifrado fuerte para uso público fue Phil Zimmermann con la publicación de PGP (Pretty Good Privacy) en 1991. Distribuyó una versión freeware de PGP cuando previó la amenaza de una legislación, por aquel entonces en consideración por el gobierno estadounidense, que requeriría la creación de puertas traseras en todas las soluciones criptográficas desarrolladas dentro de EEUU. Sus esfuerzos para publicar PGP en todo el mundo le granjearon una larga batalla con el Departamento de Justicia por la supuesta violación de las restricciones de exportación. Finalmente, el Departamento de Justicia abandonó el caso contra Zimmermann,[2] y la distribución *freeware* de PGP se hizo mundial y terminó convirtiéndose en un estándar abierto (RFC2440 u OpenPGP).

5.6 Criptoanálisis moderno



A veces, el criptoanálisis moderno implica un gran número de circuitos integrados. Esta placa es parte del crackeador DES de la EFF, que contenía más de 1800 chips y podía romper una clave DES por fuerza bruta en cuestión de días.

Aunque los cifrados modernos como el AES están considerados irrompibles, todavía siguen adoptándose malos diseños, y en las décadas recientes ha habido varias roturas criptoanalíticas notables. Ejemplos famosos de diseños criptográficos que se han roto incluyen al DES, el primer esquema de cifrado Wi-Fi, WEP, el sistema Content Scramble System utilizado para cifrar y controlar el uso de los DVD, y los cifrados A5/1 y A5/2 utilizados en los teléfonos móviles GSM. Además, no se ha demostrado que alguna de las ideas matemáticas que subyacen a la criptografía de clave pública sean «irrompibles», y por tanto es posible que algún descubrimiento futuro haga inseguros todos los sistemas que dependen de ella. Aunque poca gente prevé un descubrimiento así, el tamaño de clave recomendado sigue aumentando, al aumentar y hacerse más barata la potencia de cálculo para romper códigos.

6 Véase también

- Manuscrito Voynich

7 Referencias

[1] “Cyber-Security and Threat Politics: US Efforts to Secure the Information Age”,Myriam Dunn Cavelty, Routledge 2008

[2] Cnet News staff (11 de enero de 1996). «Feds drop charges in encryption case». *CNet News* (en inglés). Consultado el 7 de noviembre de 2014.

- Steven Levy, *Cripto. Cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad en la era digital*, Madrid, Alianza, 2002.
- David Kahn, *The Codebreakers*, New York, Macmillan, 1967.

8 Enlaces externos

- Línea de tiempo de máquinas de cifrado (en inglés)

9 Text and image sources, contributors, and licenses

9.1 Text

- **Historia de la criptografía** *Fuente:* http://es.wikipedia.org/wiki/Historia%20de%20la%20criptograf%C3%ADa?oldid=79134097 *Colaboradores:* Chewie, Benjavalero, RobotQuistnix, Tamorlan, Fercufer, CEM-bot, Thijs!bot, LogC, CommonsDelinker, Nioger, VolkovBot, Technopat, Erfil, Matdrodes, Barri, AlleborgoBot, Muro Bot, Loveless, Bigsus-bot, Northwoods, Findoridnof, VanBot, AVBOT, Luckas-bot, LyingB, Marmaraba, DSisyphBot, ArthurBot, Xqbot, Jkbw, AstaBOTh15, TiriBOT, RedBot, HRoestBot, Grillitus, David822, WikitanvirBot, MerlIwBot, KLBot2, MetroBot, Johnbot, Elvisor y Anónimos: 18

9.2 Images

- **Archivo:DES_Board300.jpg** *Fuente:* http://upload.wikimedia.org/wikipedia/commons/9/99/DES_Board300.jpg *Licencia:* CC-BY-SA-3.0 *Colaboradores:* ? *Artista original:* ?
- **Archivo:Enigma.jpg** *Fuente:* http://upload.wikimedia.org/wikipedia/commons/a/ae/Enigma.jpg *Licencia:* Public domain *Colaboradores:* ? *Artista original:* ?
- **Archivo:SIGABA-patent.png** *Fuente:* http://upload.wikimedia.org/wikipedia/commons/f/fb/SIGABA-patent.png *Licencia:* Public domain *Colaboradores:* ? *Artista original:* ?
- **Archivo:Skytala&EmptyStrip-Shaded.png** *Fuente:* http://upload.wikimedia.org/wikipedia/commons/b/b2/Skytala%26EmptyStrip-Shaded.png *Licencia:* CC-BY-SA-3.0 *Colaboradores:* ? *Artista original:* ?

9.3 Content license

- Creative Commons Attribution-Share Alike 3.0