Criptografía: un arma muy poderosa

por D.ª Irene Márquez Corbella, licenciada en Matemáticas
D. Jorge Ortigas Galindo, licenciado en Matemáticas
y D.ª María Pilar Velasco Cebrián, doctora en Matemáticas,

En este artículo recogemos un amplio resumen de la historia de la Criptografía, desde la antigüedad hasta los últimos criptosistemas post-cuánticos. En particular, resaltamos el importante uso y desarrollo de la criptografía como arma intelectual durante la Primera y Segunda Guerra Mundial, y durante la Guerra Civil Española, así como los actuales avances relacionados con la seguridad de los criptosistemas y los basados en la teoría de códigos correctores, candidata a mantener la integridad de las comunicaciones cuando los ordenadores cuánticos hagan su aparición.

"Un hombre capaz de descriptar escritos cifrados vale más que cinco generales"

(Napoleón I)

INTRODUCCIÓN

En un conflicto de guerra, es importante saber el máximo sobre el enemigo, pero igual de importante es asegurarnos de que el enemigo no sepa nada de nosotros. De ahí el gran desarrollo del arte de escribir mensajes en clave secreta para proteger la confidencialidad, integridad y autenticidad de la información, que es lo que se conoce como *criptografía* (de las voces griegas *Kriptos,* oculto, y *graphos*, escribir) que, junto al *criptoanálisis* o ciencia dedicada a romper cifrados y acceder a la información protegida, y la *esteganografía* o ciencia sobre la ocultación de mensajes para evitar que se perciba su existencia, constituyen la rama matemática de la *criptología*, fundamento de las secciones técnicas de los Servicios de Información.

CRIPTOGRAFÍA DE CLAVE SECRETA

Los métodos clásicos

Desde la antigüedad, el hombre ha hecho gala de su ingenio para garantizar la confidencialidad de sus comunicaciones. La historia de la criptografía está llena de anécdotas y personajes pintorescos, como esclavos con textos grabados en su cuero cabelludo, alfabetos de extraños símbolos, escritos de tinta "invisible", secuencias interminables de números…

Escítala
Fuente: http://www.blog.singenio.com/2010/10/ambigrama-investigaciones.html

Los primeros usos de la criptografía los encontramos en el Antiguo Egipto (500-525 a. C.), en jeroglíficos no estándares tallados en monumentos, aunque no se piensa que sean intentos de comunicación secreta sino que sólo buscaban añadir misterio, intriga o diversión al espectador letrado.

Los criptosistemas clásicos son criptosistemas de clave secreta, de clave privada o cifrado simétrico, donde la clave de cifrado es un secreto entre el emisor y el receptor, de forma que si un atacante descubre la clave utilizada ha roto el criptosistema

Los criptosistemas clásicos son *criptosistemas de clave secreta, de clave privada o cifrado simétrico,* donde la clave de cifrado es un secreto entre el emisor y el receptor, de forma que si un atacante descubre la clave utilizada ha roto el criptosistema. Una primera división de estos cifrados se puede hacer según el tipo de operación que se utiliza: la sustitución (cambiar las unidades del texto original por otras), la transposición (reordenación de las mismas) o una combinación de estos dos tipos.

Un ejemplo claro de cifrado de transposición es la escítala de Grecia, considerada el primer uso de escritura secreta, utilizada por los espartanos en el 400 a. C. durante la guerra de Atenas y Esparta. El método es extremadamente sencillo, los militares escribían sus mensajes sobre una tira de cuero o de papiro que se enrolla alrededor de la escítala de manera que al desenrollar la tira el texto aparece cifrado mediante la transposición de las letras. El mensaje original se recuperaba cuando se enrollaba sobre un bastón o escítala del mismo grosor.

Más tarde, eruditos hebreos (500-600 a. C.) hicieron uso de sencillos cifrados por sustitución, como el cifrado Atbash que consiste en utilizar el simétrico del alfabeto, lo que se conoce como efecto espejo. A este sistema se hace referencia en *El código Da Vinci* y en el *libro de Jeremías*. Otro ejemplo sencillo de cifrado de sustitución monoalfabético es el *cifrado de César* o *cifrado por desplazamiento*, usado por Julio César en el siglo I. d. C. para proteger sus mensajes de estrategia militar, que consistía en sustituir cada letra por la que ocupa tres puestos a la derecha en el alfabeto. Así el cifrado de César siempre sustituye la letra A por la letra D, la B por la E... Generalizando este sistema, se define transformación con desplazamiento b sobre un alfabeto de m letras a la función

$$T_b(M) \equiv M + b \pmod{m}$$

Este criptosistema no sería seguro hoy en día, pues un simple ataque por fuerza bruta tratando los posibles valores de desplazamiento del alfabeto utilizado daría el texto fuente. Sin embargo, en pleno siglo XXI el capo mafioso Bernardo Provenzano, detenido en 2006, utilizaba este rudimentario algoritmo y mantuvo a las fuerzas de seguridad sin conocer su paradero durante años.

Durante la Edad Media, los copistas empleaban diversos métodos

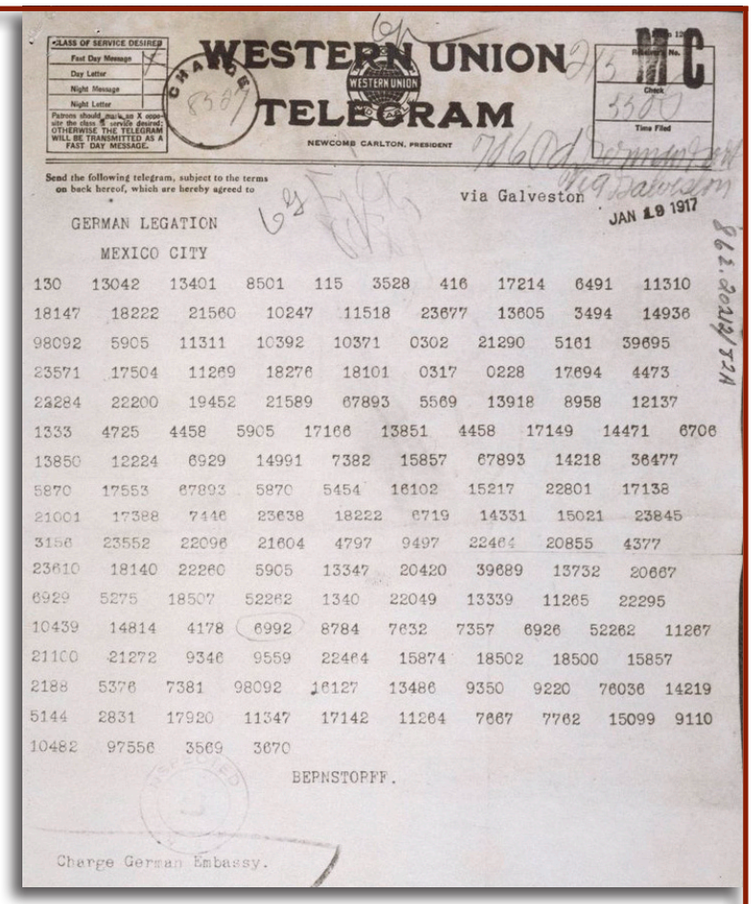
para encubrir su verdadera identidad, como utilizar el alfabeto zodiacal, formar anagramas alterando el nombre de las letras (Xilef, anagrama de Félix) o recurriendo a la fuga de vocales y su sustitución por puntos o consonantes arbitrarias (Thfpfklbctxx por Theoflactus). La obra más antigua sobre criptografía, *Liber Xifrorum,* data del siglo XIV y estudia diversos sistemas basados en simples sustituciones de letras.

La sencillez de estos sistemas hizo que fueran vulnerables hasta prácticamente el Renacimiento. El uso de varios abecedarios y el empleo de una clave que se transcribe sobre el texto original dieron origen al cifrado por sustitución polialfabética, que permitió que durante el siglo XVI se generalizara el uso de la criptografía en los ambientes diplomáticos.

El *cifrado de Vernam (*1917) es un ejemplo de cifrado por sustitución polialfabética, en el que el texto en claro se combina con un flujo aleatorio o pseudoaleatorio del mismo tamaño para generar un texto cifrado. Se trata de un cifrado teóricamente irrompible, pero no resulta muy útil pues para descifrar se necesita conocer la clave que es de igual longitud que el texto a cifrar y si ya se tiene un canal seguro para enviar la clave… ¿por qué no enviar el mensaje en claro directamente? El RC4 o ARC4 es un ejemplo de cifrado de Vernam, usado en algunos de los protocolos más populares que protegen el tráfico de internet, como el protocolo SSL, su sucesor TSL, o protocolos de seguridad en las redes inalámbricas como el WEP.

Criptografía durante la Primera y Segunda Guerra Mundial y la Guerra Civil Española

No está muy lejos de la realidad el dicho de que la criptografía


WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3070

BERNSTORFF.

Charge German Embassy.

Telegrama Zimmermann)
Fuente: http://es.wikipedia.org/wiki/Telegrama_Zimmermann

ha matado más gente que la bomba atómica. De hecho, ha sido en el transcurso de las guerras cuando más desarrollo ha alcanzado la criptografía, estableciendo comunicaciones secretas militares y diplomáticas por medio de nuevas tecnologías. [1,2]

Así, en la Primera Guerra Mundial la ruptura en 1917 por parte de los aliados británicos del telegrama Zimmermann, en el cual Alemania instruía a México para formar alianza junto a Japón contra los Estados Unidos, fue una de las causas de la entrada de los Estados Unidos en la guerra y provocó el cambio de la opinión pública sobre el conflicto. Por otra parte, en la Segunda Guerra Mundial la ruptura del cifrado de la máquina Enigma permitió a los ingleses aprovechar al máximo los aviones de que disponía en la

Máquina Enigma
Fuente: http://inza.wordpress.com/2008/10/12/la-maquina-enigma-en-espana/

Batalla de Inglaterra, cambiar el signo de la contienda en el Norte de África y ganar la Batalla del Atlántico, e hizo que el conflicto acabara al menos un año antes de lo esperado.

... en pleno siglo XXI el capo mafioso Bernardo Provenzano, detenido en 2006, utilizaba este rudimentario algoritmo y mantuvo a las fuerzas de seguridad sin conocer su paradero durante años

La máquina Enigma fue creada por el holandés Alexander Koch en 1919. Tras varias versiones comerciales, surge la versión Enigma-D adquirida por la marina alemana en 1926. Esta máquina estaba formada por varios rotores (discos circulares planos con 26 contactos eléctricos en cada cara, uno para cada letra alfabética, y cableado a un contacto diferente en la cara contraria) conectados entre sí, de forma que el cableado de cada rotor era diferente, haciendo que la clave usada para el cifrado no sirviera para el descifrado y, por tanto, para descifrar el mensaje era necesario tener la misma máquina y conocer el posicionamiento y características de los rotores. En 1929, los polacos interceptaron una máquina Enigma equivocadamente no protegida y un año después determinaron gracias a ayuda francesa el alambrado de los rotores usado por el ejército alemán, pero éste aumentó la complejidad de Enigma en 1939 por lo que los polacos, debido a su escasez de recursos, pasaron su información a franceses y británicos, siendo estos últimos (entre los que se encontraba Alan Turing) en Bletchley Park quienes encontraron medios para quebrar muchas de las variaciones alemanas del Enigma.

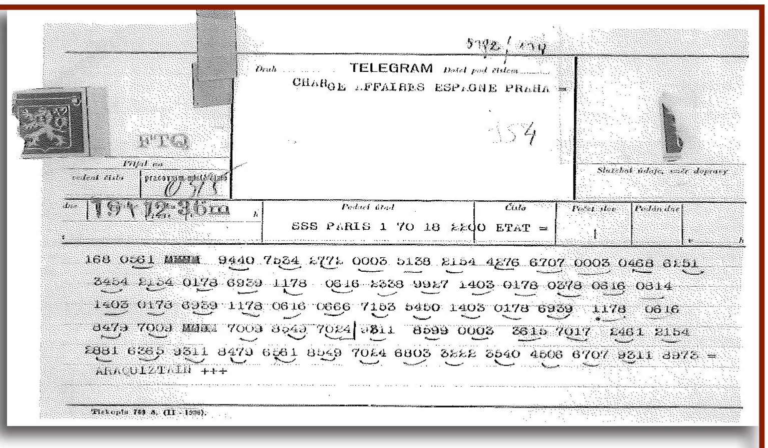
Pero fue la Guerra Civil Española la primera guerra en la que se utilizaron las máquinas Enigma y la primera vez que los británicos intentaron romper el cifrado. En noviembre de 1936 diez máquinas Enigma de tipo comercial fueron adquiridas por el gobierno nacionalista, posiblemente por una propuesta de los alemanes para asegurar las comunicaciones con sus aliados españoles, al contrario de lo que se ha llegado a afirmar de que Hitler regaló a las fuerzas franquistas 15 de estas máquinas. Estas máquinas se concentraron en el Estado Mayor de la Flota, en el Estado Mayor Naval y en el Estado Mayor de Cádiz y fueron usadas por las Fuerzas nacionalistas, como la Legión Cóndor, las marinas italiana, española y alemana, y todos los Cuerpos del Ejército del bando nacional.

Otras máquinas de cifrado usadas en la Guerra Civil fueron: la "Clave Norte", dispositivo de cifrado mecánico anticuado para la época formado por dos ruedas concéntricas dentadas para el alfabeto en claro y cifrado respectivamente; las máquinas Kryha, primera máquina de cifrado de éxito comercial y uso masivo, usada hasta mediados de los cincuenta y utilizada por el Gobierno Vasco y por las fuerzas nacionalistas; y las máquinas Ha-

gelin que, aunque eran inferiores a las Enigma, fueron utilizadas por la Marina italiana porque disponían de un dispositivo de impresión y un contador continuo.

Junto a estas máquinas, fue de gran importancia en la Guerra Civil el uso de códigos, pues la ventaja de la no relación explícita entre el mensaje real y codificado compensaba la desventaja del manejo de libros de códigos. La Sección Segunda del Estado Mayor era la encargada de analizar la información de ambos bandos y enviar resúmenes a los responsables de la operación. El 26 de septiembre de 1936 se crea el Servicio de Información Militar (SIM) y, pocos días después, con el apoyo del General Mola, se forma el Servicio de Información del Nordeste de España (SIFNE).

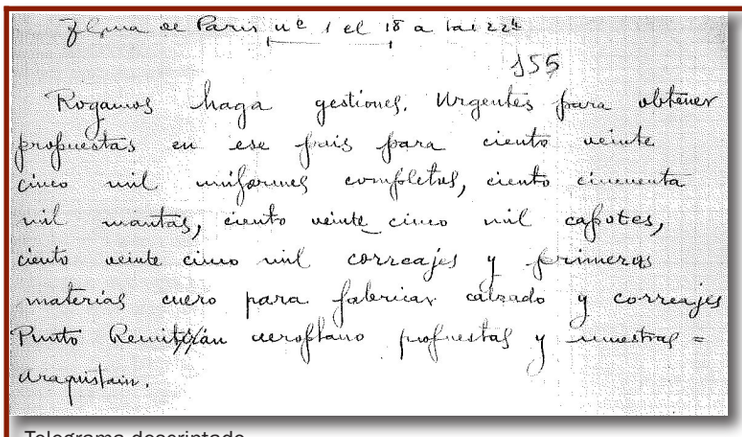
Los cifrados más sencillos consistían en el intercambio del valor de las palabras por otras inocentes, utilizado como medio de comunicación por la Agrupación Guerrillera de Levante en la posguerra y por personalidades republicanas en el exilio. Cabe destacar los *cifrados de trinchera*, que nacieron en la Primera Guerra Mundial y se utilizaron en nuestra Guerra Civil por su facilidad de uso y porque reducían mucho el mensaje, evitando la detección del emisor. Un ejemplo es la clave de Bous utilizada para las comunicaciones cifradas de los Bous de las Fuerzas Navales del Cantábrico de la Marina de Guerra Republicana. Una copia de esta clave, la cual constaba de nueve páginas en las que se cifraba la presencia de enemigos, velocidades, incidencias, distancias y rumbos, fue enviada el 11 de diciembre de 1936 por el Jefe de las Fuerzas Navales republicanas del Cantábrico, Federico Monreal, al Consejero de Defensa del Gobierno Vasco. Otros ejemplos de cifrado del mismo tipo eran los utilizados por el SIFNE



Telegrama cifrado
Fuente: J. R. Soler Fuensanta y F. J. López-Brea Espiau. Soldados sin rostro. Inédita editores, Barcelona, 2008.

para emisión de mensajes mediante radios clandestinas, y los partes de presencia de aviación utilizados por el ejército de la República.

Un método de cifrado por excelencia en la Guerra fue la tabla de homófonos y una variación de ella, el sistema de cinta o sistema español, consistente en una sustitución simple donde cada símbolo se sustituye por otro según una clave. Otro método muy popular fue el sistema manual de cifrado llamado de cinta móvil, consistente en una tabla de homófonos a la que se le añaden dos filas, una con el alfabeto en orden normal y otra con un doble alfabeto aleatoriamente ordenado en una cinta móvil, que fue el método más utilizado por el bando republicano. Otros métodos utilizados en la Guerra Civil fueron: el método de Playfair, usado hasta la segunda guerra mundial y consistente en una tabla de 5x5 elementos donde se introducen las letras del alfabeto bajo una clave; una variante del cifrado de Gronsfeld, en el que la clave eran ocho números donde cada uno indicaba el número de letras del alfabeto que debía desplazarse el mensaje original; y una variante del cifrado de Polibio, utilizado por los comunistas y consistente en una tabla de tres filas y diez columnas para el alfabeto sujeto a una clave.



Telegrama descriptado
Fuente: J. R. Soler Fuensanta y F. J. López-Brea Espiau. Soldados sin rostro. Inédita editores, Barcelona, 2008

La información proporcionada por los criptoanalistas permitió obtener una ventaja estratégica de primer orden al bando nacional al disponer de una información privilegiada sobre la situación de las fuerzas enemigas, su composición, intenciones y carencias. Así, aunque la criptografía por sí sola no gana batallas, puede ayudar mucho, y muestra de ello son estos dos ejemplos:

No está muy lejos de la realidad el dicho de que la criptografía ha matado más gente que la bomba atómica

El 17 de agosto de 1937 el Delegado del Gobierno de Santander informó al ministro de Gobierno en Valencia de la precariedad de su situación y del temor de que los nacionalistas dejaran a la ciudad sin abastecimiento de agua. Los nacionalistas interceptaron el mensaje y lo descifraron, se informó desde Biarritz, donde estaba localizado el Centro de operaciones del SIFNE, a Burgos y finalmente los nacionalistas se hicieron dueños de los manantiales del suministro de agua.

El 20 de octubre de 1937 a las 10 a.m., los mandos de la ciudad de Gijón, en manos republicanas y asediados por el ejército nacionalista, enviaron un telegrama cifrado con una clave nueva al Gobierno Republicano en Valencia indicando que si no enviaban aviación de refuerzo la derrota era segura, pero el mensaje fue descifrado por un Catedrático y criptoanalista en la Oficina Central del bando nacionalista y entregado al Cuartel General a las 13 horas del mismo día. Un par de horas después, la estación de radio de Burgos interceptó un mensaje de Valencia con destino Gijón en el que se les indicaba que no conseguían descifrar el mensaje y solicitando lo reenviasen con la clave antigua. Finalmente, Gijón cayó al día siguiente.

Criptosistemas de clave secreta modernos

A partir de la segunda mitad del siglo XX, con el desarrollo de internet y la expansión de la informática, se hicieron necesarios nuevos sistemas criptográficos para proteger la información durante su transmisión y almacenamiento, pues al crecer la libertad de comunicación se multiplican los riesgos para la privacidad.

Independientemente de la clasificación de cifrados de clave secreta realizada según el tipo de operación, los cifrados simétricos se pueden clasificar en: *cifrados en bloque* y *cifrados en flujo.*

El cifrado en bloque opera con grupos de bits de longitud fija (llamados bloques) aplicándoles una transformación invariante de forma que si un bloque aparece repetido en el mensaje se cifra de igual manera. El ejemplo más conocido es DES (Data Encryption Standard), cuyos orígenes se remontan a principio de los 70. A pesar de la polémica creada por su corta longitud

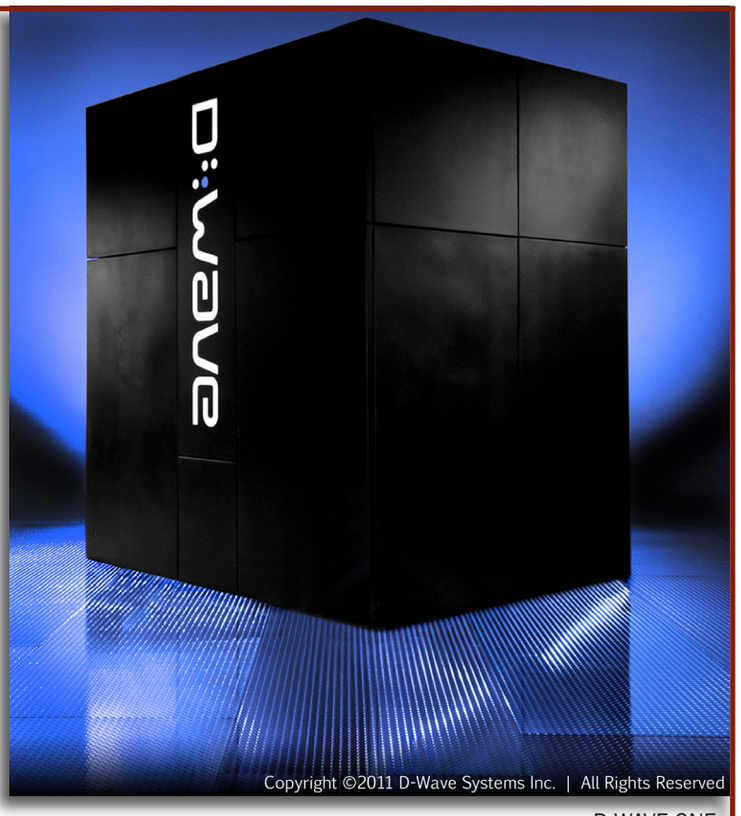
de clave, que permite ataques por fuerza bruta, y las misteriosas cajas S que aparecían en su descripción, este cifrado fue utilizado como algoritmo estándar para cifrar información confidencial por el gobierno estadounidense desde 1976 hasta 2002. En este año fue reemplazado por el AES (Advanced Encryption Standard).

En los algoritmos de cifrado en flujo los mensajes son tratados bit a bit, permitiendo cifrar mensajes arbitrarios, además utilizan un estado que evoluciona a lo largo del algoritmo, siendo muy útiles para algunas aplicaciones como las conversaciones telefónicas, ya que permiten el cifrado en tiempo real. La mayor parte de estos algoritmos se basan en LFSR. Los ejemplos más conocidos son: A5/1, empleado en la telefonía GSM; E0, utilizado en el protocolo del Bluethooth; o SNOW 3G, utilizado en la tercera generación de móviles, también referida como tecnología UMTS o 3GSM. En [3] puede verse con más detalle un ataque sobre este último algoritmo.

Estos sistemas supusieron un salto cualitativo importante ya que permitieron introducir la criptografía en otros campos que hoy en día resultan esenciales, como en la firma digital.

CRIPTOSISTEMAS DE CLAVE PÚBLICA

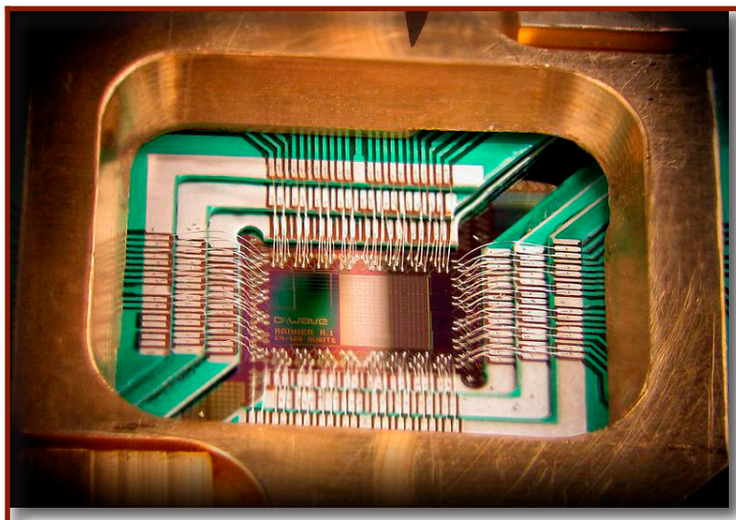
La criptografía de clave pública fue introducida por Diffie y Hellman [4] en 1976, para acabar con el problema del intercambio de claves de los sistemas de cifrado simétrico, es decir, ya no se requiere que el emisor y el destinatario intercambien una clave secreta antes de comenzar la conversación. La idea principal es crear sistemas basados en funciones que tengan la particularidad de no ser reversibles (son asimétricas), como la factorización de números enteros, función en la que se basa el conocido criptosistema RSA, o el cálculo de logaritmos discretos que es utilizado en el criptosistema ElGammal. Tratar de romper por fuerza bruta algunos de estos algoritmos de encriptación está fuera de la capacidad de los ordenadores actuales. Sin embargo…, ¿qué ocurrirá con la aparición de los ordenadores cuánticos?



D-WAVE ONE
Fuente: http://www.dwavesys.com/en/dw_homepage.html

Ordenadores cuánticos

Un ordenador no es sino una máquina electrónica que procesa información digital, que es aquélla que expresamos en binario. Por ejemplo, si queremos introducir una foto en un ordenador debemos escanearla (digitalizarla) y éste la transformará en una sucesión de ceros y unos. Para medir la información digital usamos diferentes unidades, siendo la unidad elemental el bit, que corresponde a cada



Chip D-WAVE ONE)
Fuente: http://michiganstate.247sports.com/Asset/800px-DWave128chipjpg-157444?View=Rendered

uno de los ceros y unos de los que consta la información.

La base teórica de la computación tradicional está basada en saber usar unos y ceros para resolver problemas. Se utilizan los transistores como elemento principal, de forma que las diferencias de energía que existan en él son unos y ceros lógicos.

La computación digital tradicional no tardará en llegar a su límite, puesto que ya se ha llegado a escalas de

En noviembre de 1936 diez máquinas Enigma de tipo comercial fueron adquiridas por el gobierno nacionalista, posiblemente por una propuesta de los alemanes para asegurar las comunicaciones con sus aliados españoles ...

sólo algunas decenas de nanómetros en los transistores que integran los microchips.

De ahí surge la idea de computación cuántica en 1981, cuando Paul Benioff expuso su teoría para aprovechar las leyes cuánticas en el entorno de la computación. En vez de trabajar a nivel de voltajes eléctricos, se trabaja a nivel de cuanto. En la computación digital, un bit sólo puede tomar dos valores: 0 ó 1. En cambio, en la computación cuántica, intervienen las leyes de la mecánica cuántica, y la partícula puede estar en superposición coherente: puede ser 0, 1 y puede ser 0 y 1 a la vez (dos estados ortogonales de una partícula subatómica). Eso permite que se puedan realizar varias operaciones a la vez, según el número de Qbits.

En 1998 nació la primera máquina de 2-Qbit, que fue presentada en la Universidad de Berkeley, California (EE. UU.). Un año más tarde, en 1999, en los laboratorios de IBM-Almaden, se creó la primera máquina de 3-Qbit y además fue capaz de ejecutar por primera vez el algoritmo de búsqueda de Grover. En 2001, IBM y la Universidad de Stanford consiguen ejecutar por primera vez el algoritmo de Shor en el primer computador cuántico de 7-Qbit desarrollado en Los Álamos. En 2007 la empresa canadiense D-Wave Systems [5] presentó supuestamente en Silicon Valley, una primera computadora cuántica comercial de 16-Qbits de propósito general; luego la misma compañía admitió que tal máquina, llamada Orion, no era realmente una computadora cuántica, sino una clase de máquina de propósito general que usa algo de mecánica cuántica para resolver problemas. En 2011 la primera computadora cuántica comercial es vendida por la empresa D-Wave Systems a Lockheed Martin (compañía multinacional de la industria aeroespacial con grandes recursos en tecnología avanzada y guerra global) por 10 millones de dólares. El pasado año 2012 IBM anunció que ha creado un chip lo suficientemente estable para permitir que la informática cuántica llegue a hogares y empresas, se estima que en unos 10-12 años se pueda estar comercializando los primeros sistemas cuánticos. [6,7]

A día de hoy la computación cuántica presenta un gran número de problemas todavía no resueltos, habiendo muchos escépticos sobre la funcionalidad de las máquinas

ya construidas. La presentación del D-wave One generó gran controversia, por ello la empresa canadiense D-Wave Systems publicó un artículo el 12 de mayo de 2011, menos de dos semanas antes de la divulgación de la venta de su primera computadora, en la prestigiosa revista científica Nature [8], donde los científicos de la compañía brindan detalles acerca de la técnica utilizada para generar los 128 Qbits. En agosto de 2012, un equipo de investigadores de la Universidad de Harvard publicó en Nature un trabajo que desarrollaba sus cálculos sobre esta máquina.

En principio los criptosistemas cuya seguridad se basa en problemas de teoría de números, que son los más utilizados actualmente (incluyendo el RSA, DSA y ECDSA), no serían seguros ya que pueden ser atacados en tiempo polinomial con el algoritmo llamado de Shor. En los últimos años se está introduciendo una nueva generación de algoritmos criptográficos, sistemas que resisten ataques utilizando ordenadores cuánticos, lo que ha dado lugar a la llamada *criptografía post-cuántica* que se basa principalmente en funciones Hash, códigos correctores, grafos y retículos.

Criptografía post-cuántica: la criptografía basada en códigos correctores

La Teoría de Códigos Correctores busca enviar un mensaje con la mayor eficiencia y verosimilitud posible a través de canales afectados de ruido que pueden distorsionar la información.

Ejemplos de la vida cotidiana son: el código de barras; el ISBN o ISSN, para identificar libros, revistas o publicaciones periódicas; los códigos ASCII de los ordenadores; los códigos correctores de los dispositivos de almacenamiento y transmisión de información como los CD o los DVD; los chips de tarjetas de crédito o del DNI...

En 1978, Robert McEliece diseñó el primer criptosistema basado en códigos correctores. Además de resistir el ataque de Shor, presenta la ventaja de tener rápidos métodos de cifrado y descrifrado. Sin embargo, el tamaño de sus claves lo hace poco eficiente para multitud de situaciones prácticas.

Tratar de romper por fuerza bruta algunos de estos algoritmos de encriptación está fuera de la capacidad de los ordenadores actuales. Sin embargo…, ¿qué ocurrirá con la aparición de los ordenadores cuánticos?

El ataque más efectivo conocido contra el criptosistema de McEliece es la descodificación utilizando conjuntos de información. Existen muchas variantes de este ataque. En 2008, Bernstein, Lange y Peters consiguieron romper el criptosistema original de McEliece en 1400 días utilizando un ordenador convencional o en 7 días utilizando un cluster de 200 CPU. [9]

Muchas de las técnicas que se han considerado infalibles a lo largo de la historia han sido abatidas por la habilidad de los criptoanalistas

En 1986 Niederreiter, utilizando códigos binarios Reed Solomon generalizados (códigos GRS), presenta la versión dual del criptosistema de McEliece, sin embargo presenta claves más pequeñas y sistemas de cifrado y descrifrado más rápidos.

En 1992, Sidelnikov y Shestakov introducen un algoritmo que nos permite descubrir la estructura del código Reed Solomon utilizado en el criptosistema en tiempo polinomial, con lo que resulta que el esquema original de Niederreiter está completamente roto. Es por ello que en 2005 Berger y Loidreau proponen una nueva versión del esquema de Niederreiter diseñado para resistir precisamente este ataque. La idea principal de esta variante es trabajar con subcódigos del código GRS original.

En 1996, Janwa y Moreno proponen utilizar códigos geométrico-algebraicos para la criptografía [10].

CONCLUSIÓN

Hemos realizado un análisis de la criptografía desde los métodos antiguos hasta algunos ejemplos de la última generación que incluyen sistemas post-cuánticos. Sin embargo, la duda persiste: ¿son capaces los complejos sistemas criptográficos actuales de garantizar el secreto? Muchas de las técnicas que se han considerado infalibles a lo largo de la historia han sido abatidas por la habilidad de los criptoanalistas. Como afirmaba el gran escritor estadounidense Edgar Allan Poe, un gran apasionado de la criptografía, "es dudoso que el género humano logre crear un enigma que el mismo ingenio humano no resuelva".

REFERENCIAS

- [1] J. G. Carmona. Tratado de criptografía con aplicación especial al Ejército. Ministerio de Defensa, 2011.
- [2] J. R. Soler Fuensanta y F. J. López-Brea Espiau. Soldados sin rostro. Inédita editores, Barcelona, 2008.
- [3] D. Blandine and I. Márquez-Corbella. Fault Analysis on the stream Cipher Snow3G. IEEE Computer Society FDTC 2009, 103-110, 2009.
- [4] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transaction on Information Theory, IT-22, 644-654, 1976.
- [5] http://www.dwavesys.com/en/company.html
- [6] http://informaticacuantica.comule.com/index.html
- [7] http://es.wikipedia.org/wiki/Computación_cuántica
- [8] http://www.nature.com/nature/journal/v473/n7346/full/nature10012.html
- [9] D.J. Bernstein. Introduction to post-quantum cryptography. In J. Buchmann, D.J. Bernstein and E. Dahmen, editors, Post-quantum cryptography, 1-14. Springer-Verlag, Berlin, 2009
- [10] I. Márquez-Corbella, E. Martínez-Moro and G.R. Pellikaan. Evaluation of public-key cryptosystems based on algebraic geometry codes. Proceedings of the Third International Castle Meeting on Coding Theory and Applications, Cardona Castel in Cardona. September 11-15, Barcelona, pp. 199-204, 2011.

Doña Irene Márquez Corbella es licenciada en Matemáticas y en la actualidad es Becaria FPU en la Universidad de Valladolid

Don Jorge Ortigas Galindo es licenciado en Matemáticas y en la actualidad es profesor en el Centro Universitario de la Defensa de Zaragoza

Doña María del Pilar Velasco Cebrián es doctora en Matemáticas y en la actualidad es profesora en el Centro Universitario de la Defensa de Zaragoza