



UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

Criptografía

Qué es y por qué es importante

Autor:

Lars Fredrik KARLSTRÖM

7 de diciembre de 2011

Resumen

The art of keeping secrets and messages safe stem back several thousands of years. By its very nature, cryptography is a topic shrouded in mystery, with a fascinating history and numerous legends to be told. But it is also a science in hefty debate, its essential applications both feared and treasured. If you would ask just how important cryptography has been to us, you need only acknowledge the fact that it is due to the secret battle of code breakers during World War II that we may enjoy computers today.

In this essay, we shall explore the dawn of cryptography, its impact throughout the centuries, and shed light on some encoded mysteries that continue to baffle scientists to date. We will also learn the fundamental aspects of encryption and decryption, study various ciphers, and analyze the profound impact that modern cryptographic algorithms have on our lives.

Albeit a few sections might be geared towards readers with a background in computation, the major part of this essay should be accessible - and hopefully captivating - to all audiences alike.

The most current version of this document can be retrieved from the URL <http://cbsmth.se/misc/essay-cryptography/>.

Palabras clave: Criptología; Criptografía; Criptoanálisis; Escritura secreta; Códigos; Cifras

Índice general

1. La historia de la criptografía	2
1.1. Los primeros días	3
1.2. La Primera Guerra Mundial	6
1.3. El origen de las computadoras	7
2. Cifras legendarias	8
2.1. Kryptos, la escultura cifrada	8
2.2. El manuscrito Voynich	9
3. Base teórica	11
3.1. Cifrados de transposición	11
3.1.1. El cifrado rail fence	11
3.2. Cifrados de sustitución	12
3.2.1. El cifrado César	12
3.2.2. Códigos de nomenclatura	13
3.3. Descifrando códigos	13
4. Criptografía moderna	15
4.1. Implementación y impacto	15
4.2. Controversia	16
4.3. Criptografía Public Key	18

Capítulo 1

La historia de la criptografía

La palabra *criptografía* se deriva de las palabras griegas *kruptos*, que significa “oculto” o “secreto”, y *graphein*, que como sufijo denota algo escrito. En tiempos modernos es casi siempre asociada con las computadoras y con fórmulas matemáticas muy complejas. Pero el arte de escribir mensajes con contenido oculto tiene una profunda historia que se remonta hasta cuatro mil años, cuando un escriba en el antiguo Egipto sustituía jeroglíficos populares por unos desconocidos en la tumba de su amo.

Desde la salvaguardia de comandos militares durante las épocas de Grecia y Roma, la criptografía se convirtió en un ingrediente crucial para el éxito de los imperios de negociaciones en Europa, antes de servir como el peso que cambió la balanza en las dos guerras mundiales. Hoy en día es esencial para nuestra sociedad, con transacciones electrónicas así como comunicados en función de algoritmos criptográficos para su custodia.

1.1. Los primeros días

Aunque la cuna de la criptografía se remonta hasta cuatro mil años, el concepto en sí se desvaneció, siendo un bebé, sin salir de Egipto. De hecho, la criptografía — así como su hermano *esteganografía*, la ocultación de mensajes escritos — se ha inventado y abandonado en numerosas civilizaciones antiguas.

En culturas del este como la India, Mesopotamia, y China, los mensajes ocultos son conocidos por haber tenido un sin número de propósitos, el más obvio es el de naturaleza militar. La expansión de estos sistemas se dio desde métodos rudimentarios, sustituyendo palabras como “flechas” o “tropas” con nombres de animales o flores, hasta criptosistemas más desarrollados. Aunque estas cifras podrían haber jugado roles más o menos importantes en su tiempo, no parecen haber alcanzado algún impacto duradero. Una de las razones principales de esto podría ser que la gran mayoría de la gente era analfabeta; simplemente no existían ojos de los cuales defenderse.

Como en muchos otros campos científicos, la antigua civilización griega impulsó el desarrollo de la criptografía, elaborando varios métodos de comunicación discreta. El *scytale* de Sparta, por ejemplo, fue el primer dispositivo usado para crear cifras de transposición.

Envolviendo una pieza de pergamino alrededor de un bastón con un largo y ancho específicos, el mensaje era escrito en el pergamino a lo largo del bastón. El receptor tenía un *scytale* de las mismas dimensiones, lo que le permitía leer el mensaje.

Intentando resolver los problemas de transmisión de mensajes a larga distancia, el escritor Polybius creó una cuadrícula con filas y columnas numeradas, en las cuales se colocaba el alfabeto. Usando estas coordenadas, cada número correspondía a una letra: una conversión fundamental, usada

frecuentemente en la criptografía. Aunque se desconoce si el sistema fue usado alguna vez de la forma que su autor lo deseaba, el *cuadro de Polybius* ha sido usado como base para otros sistemas criptográficos.

Durante las grandes conquistas de Roma, el emperador Julio César utilizó una cifra de sustitución de su propia creación, conocida como la *cifra del César*. El mensaje simplemente era escrito por la transformación de cada letra del alfabeto en correspondencia con una clave de cifrado dado, siendo la decisión de César “tres a la derecha”. Por lo tanto, la letra A se transforma en D, B en E, y así sucesivamente.

Con el declive del Imperio Romano, Europa se vió estancada en los tiempos de oscuridad. La criptografía, sin embargo, fue llevada a nuevos niveles en Arabia, donde numerosos esquemas de cifrado mejorados se construyeron, y aún más importante, el *criptoanálisis* — el estudio de la ruptura de códigos y cifras — fue explorado por primera vez.

Con esta contraparte de la criptografía, el escenario se había establecido para la batalla perpetua entre aquellos que escriben los códigos y aquellos que los descifran. A medida que el mundo árabe disminuía, el conocimiento científico fue amasado y asimilado en occidente - matemáticas y medicina así como cryptología.

Fue en los primeros días del renacimiento cuando la importancia de la criptografía comienza a escalar de manera espectacular, primero en una batalla por el papado entre el Papa Urbano VI y el Papa Clemente VII, y posteriormente en el rápido desarrollo político de una Europa transformandose de un estado medieval a países capitalistas internacionales.

Con embajadas establecidas en cada país, la comunicación diplomática se volvió el blanco principal del espionaje - y así como hoy en día, aquéllos que pueden descifrar los códigos son los que obtienen los beneficios. En aquél

tiempo, el nombre del ganador era Venecia; la pequeña ciudad-estado consiguió crear un vasto imperio de mercado aprovechando su red de inteligencia bien establecida. Eran tan capaces de romper códigos que podrían rentar sus servicios a estados aliados, garantizando un precio muy alto y dándoles la ventaja de leer primero la comunicación interceptada.

En el mismo periodo de tiempo, el espía maestro de la reina Elizabeth, Sir Francis Walsingham, tejió lo que pudo haber sido la mayor red de espías en la historia. Interceptando y descifrando comunicaciones en todo el continente, entre otras cosas, su red boicoteó una rebelión instigada por María, Reina de Escocia - la prima de la reina Elizabeth.

Con estos avances, la criptografía se ha extendido más que nunca, pero en complejidad, todavía sólo igualada a sus predecesores en oriente. Lo que cambió este estado fue la invención de la *cifra polialfabética*, lo que aumenta considerablemente la seguridad de un cifrado mediante la utilización de varios alfabetos de sustitución diferentes.

A partir de entonces, nuevos progresos se han logrado con el paso de los años, con la inteligencia jugando un papel determinante en los conflictos posteriores. Con el paso del tiempo el tablero cambió, con las nuevas tecnologías como el telégrafo y las comunicaciones de radio. Muy pronto, Europa estaba al borde de lo que sería la Primera Guerra Mundial.

1.2. La Primera Guerra Mundial

En el primer día de la guerra, los Ingleses cortaron el cable de comunicación transatlántico de Alemania, lo que obligó a transmitir todos los comandos y ordenes a través de la radio o por medio de cables no controlados por el país. Esto significaba que todo lo que los alemanes transmitieran podía ser interceptado, y con la ayuda de individuos que vinieron a formar parte de la legendaria *Sala 40*, mucho podría ser descifrado.

Las luchas y los logros de los criptoanalistas en la Sala 40 es como tomada de un guión de película. Comenzando como un pequeño equipo de profesores universitarios fluidos en alemán, inicialmente la tarea de descifrar los códigos alemanes parecía imposible. Pero después de un golpe de suerte en la obtención de un libro de códigos, la unidad de pronto se convirtió en una unidad de inteligencia dedicada y extremadamente eficiente, que llegó a tener un gran impacto en el resultado de la guerra. Las comunicaciones descifradas proporcionadas por Sala 40 ayudaron a perseguir a los submarinos alemanes, y la correspondencia diplomática informaba sobre los planes del adversario.

El descodificación más importante realizado durante la guerra fue la de un telegrama diplomático transferido a través del Atlántico. Su texto plano era una invitación a México para participar en la guerra junto a Alemania contra los Estados Unidos, por lo cual México a cambio recibiría los territorios previamente perdidos. La solución y entrega de este mensaje, aunque una prueba terrible debido a la necesidad de mantener Sala 40 un secreto absoluto, finalmente convenció a los Estados Unidos para unirse a las fuerzas aliadas, que significó el principio del fin de la guerra.

Como cualquier héroe de verdad, la inteligencia británica ha cubierto la verdad acerca de su propio éxito en silencio, recibiendo duras críticas de sus compatriotas por su “ineficiencia”.

1.3. El origen de las computadoras

Situado a distancia conveniente de la estación de tren entre Oxford y Cambridge, dos ciudades llenas con talento intelectual, se encuentra uno de los edificios históricos más importantes de la Segunda Guerra Mundial: *Bletchley Park*. Era aquí donde la inteligencia británica y la de los Estados Unidos cooperaron en la ruptura de comunicación alemana cifrada con *Enigma*, una herramienta mecánica utilizada para crear cifras polialfabéticas extremadamente fuertes.

Los avances en la ingeniería electrónica hecha en el lapso entre la Primera y la Segunda Guerra Mundial trajeron consigo dispositivos criptográficos mucho más avanzados que los anteriores, como Enigma y la *máquina de Lorentz*. Esto a su vez requirió la invención de máquinas para romper cifras, la cual fue elaborada por el ahora mundialmente famoso matemático y científico de la computación inglés Alan Turing en Bletchley Park. Refinando un dispositivo de Polonia, Turing creó la *Bombe*, una máquina que utiliza las contradicciones lógicas con el fin de encontrar llaves a las cifras de Enigma.

Aunque sí un dispositivo de cómputo, la Bombe no era programable, y por lo tanto no fue una computadora por definición. La primera computadora programable, *Colossus*, también fue creada por los descifradores en Bletchley Park, con el fin de encontrar claves para el cifrado de Lorentz, el cual era aún más complejo que el famoso Enigma. Como ocurre con muchas invenciones hechas en tiempos de guerra, el Colossus se mantuvo en secreto hasta la década de 1970, lo que significa que algunos investigadores no fueron acreditados por sus innovaciones hasta después de su muerte. En 2007, una imitación funcional de Colossus fue construída, y ahora está en exhibición en el Museo Nacional de la Computación - en Bletchley Park.

Capítulo 2

Cifras legendarias

The urge to discover secrets is deeply ingrained in human nature; even the least curious mind is roused by the promise of sharing knowledge withheld from others.

— Chadwick

2.1. Kryptos, la escultura cifrada

En los terrenos de la Central Intelligence Agency en Langley, Virginia, en una gran escultura de cobre con la forma de una ola, se encuentra una cifra grabada que constantemente se burla de los empleados que pasan por ahí. Eregida al final del año 1990 por el escultor Jim Sanborn, hasta estos días sólo tres partes de la cifra, cual se extiende por los terrenos, han sido resueltos. La cuarta y última parte, que se rumorea para liberar una nueva enigma, sigue sin resolver hasta la fecha.

Las soluciones a los primeros tres partes fueron anunciados nueve años después de que la escultura fuera presentada por primera vez, por un computólogo de California llamado Jim Gillogy. Después de haber anunciado públicamente sus descubrimientos, sin embargo, la CIA alegó que uno de

sus propios criptoanalistas había resuelto las mismas partes el año pasado, usando nada más pluma y papel.

Los primeros dos mensajes fueron cifrados con un cifrado polialfabético estilo *Vigenère*. La tercera utilizó un *cifrado de transposición*, y la cuarta todavía no es conocido.

Al hacer la escultura, que tomó dos años y costó \$250,000 USD, el artista colaboró con un criptoanalista experimentado de la CIA, Ed Scheidt, y — aunque Sanborn luego lo denunció — supuestamente también un “escritor de ficción prominente” anónimo. Cuando *El Código Da Vinci* de Dan Brown fue lanzado en 2003, Kryptos inmediatamente se volvió conocido internacionalmente, como la portada del libro mostró coordenadas misteriosas así como el frase “sólo WW sabe” — ambos elementos del segundo mensaje de Kryptos. Se ha especulado que el autor famoso de hecho era el ayudante anónimo, pero esto no ha sido probado ni denunciado.

El mensaje “Sólo WW sabe” se refiere al director de la CIA anterior, William Webster, quien supuestamente recibió un sobre con las soluciones a los cifras. Este secreto bien guardado, dijo Sanborn, se ha creado para que no se perdieran en caso de que el poseedor actual fallezca antes que el enigma haya sido completamente resuelto.

2.2. El manuscrito Voynich

Escrito hace unos 600 años por un autor desconocido en una manera que nadie nunca ha sido capaz de leer, el manuscrito Voynich — conocido hoy por el anticuario polaca Wilfrid Voynich quien lo compró a los jesuitas en Italia en 1912 — ha sido descrito como el manuscrito más misterioso del mundo.

Se remonta a principios del siglo XV por la datación por carbono, pero

se aparece por primera vez en los registros históricos como una pertenencia de Rodolfo II, emperador del Sacro Imperio y rey de Bohemia, quien lo compró de un individuo desconocido por 600 ducados de oro — un monto asombroso, aproximadamente \$80,000 en moneda actual. Un amante de lo oculto e intrigante, el Emperador sin duda sintió que el documento misterioso justificaba el precio.

El manuscrito pasó a manos de varios hombres durante cien años hasta que se almacenó, acompañado de una carta escrita en 1666, en la biblioteca del Colegio Romano — de donde Voynich finalmente lo recuperó. La carta menciona que uno de los propietarios anteriores del manuscrito cree que el autor era nada menos que Roger Bacon, un filósofo y fraile franciscano quien fue pionero en varias áreas científicas y se acredita como el primer europeo en describir la fórmula de la pólvora.

Aunque la evidencia moderna contradice esta creencia — como Roger Bacon murió en 1294 — mucha gente sigue creyendo que él podría haber sido el autor; comprensible, como el manuscrito parece contener cerca de 250 páginas sobre temas que él investigó, como la botánica, astronomía, biología, y la farmacia, a juzgar por las ilustraciones casi igualmente numerosas.

La colección ha desconcertado a muchos grandes pensadores, incluyendo numerosos criptoanalistas experimentados de las Guerras Mundiales, y sin duda continuarán haciéndolo durante mucho tiempo. Es tan difícil de demostrar la compilación todo un engaño como es descifrarlo, y la imaginación sobre los secretos que podría ser desvelados es suficiente para mentener los cautivados intentando.

But his toil was in vain, for such Sphinxes as these obey no one but their master.

— Johannes Marcus Marci, 1666

Capítulo 3

Base teórica

En los capítulos anteriores hemos explorado el origen de la criptología, y se rascó también la punta del iceberg de su impacto en nuestro pasado. Esto no se podría haber hecho sin mencionar un variedad de esquemas de cifrado, unos de los cuales ahora vamos a investigar más a fondo con el fin de aprender cómo funciona un sistema de cifrado.

3.1. Cifrados de transposición

Una sistema de cifrado de transposición crea una *permutación*, una reordenación distinta del texto original. El scytale de Sparta mencionada en capítulo 1 fue una herramienta usada para crear este tipo de cifrado.

3.1.1. El cifrado rail fence

En un cifrado rail fence, el texto plano se escribe en una cuadrícula en zig-zag. Cuando las letras son colocadas en la cuadrícula, las letras son leídas en filas para crear el texto codificado. Para volver a montar el mensaje, el receptor tiene que conocer cuantas “raíles” fueron usadas. En el siguiente

ejemplo, la clave es usar tres raíles. El texto plano del mensaje es: *EL GATO ES FLOJO*.

E				T				F				O
	L		A		O		S		L		J	
		G				E				O		

Ahora, el mensaje codificado es: *ETFO LAOS LJGEO* (con espacios extra).

3.2. Cifrados de sustitución

En una cifra de sustitución, los caracteres del mensaje original se intercambian a otros de acuerdo con un sistema predefinido, el cual sirve como la clave de la cifra. Este tipo de sistema se encuentra en el rango de los más simples, tales como el cifrado César, a cifrados polialfabéticos que utilizan un número de alfabetos de cifrado diferentes, como la cuadrícula de Vigenère.

3.2.1. El cifrado César

Aplicando el cifrado de César, el alfabeto se desplaza un número dado de posiciones. En acuerdo con la elección del emperador, nuestro ejemplo mueve el alfabeto tres posiciones a la derecha. Otra vez, el mensaje original es *EL GATO ES FLOJO*.

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

Ahora, el mensaje codificado es: *HOJD WRHV IORMR*.

3.2.2. Códigos de nomenclatura

Códigos de nomenclatura difieren de otros cifrados en lo que permite la sustitución de palabras o a veces frases completas con números o palabras claves. El *Gran Chiffre*, utilizado por el rey francés Luis XIV fue un código de nomenclatura muy exitoso que mantuvo a los mensajes archivados ininterrumpidos durante cientos de años. También fueron utilizados con frecuencia en la Primera Guerra Mundial.

A fin de contraarrestar el análisis de frecuencia, un código de nomenclatura puede tener un gran número de sinónimos; códigos que se traducen en el mismo texto plano.

3.3. Descifrando códigos

El campo de criptoanálisis fue descubierto en el siglo IX en Arabia, por el erudito Al-Kindi, también conocido como el padre de la filosofía islámica. Incorporando el conocimiento griego, Al-Kindi hizo grandes avances en campos tan variados como las matemáticas, la medicina, la óptica y la filosofía, así como la criptografía.

Hasta la edad de la criptografía mecanizada, la herramienta principal para descifrar códigos fue el *análisis de frecuencia*, un método de ingeniería inversa para volver el mensaje codificado a texto plano, contando los caracteres que aparece más frecuentemente y comparándolas a las letras más comunes del lenguaje. En Inglés y Español, por ejemplo, las letras más comunes son E, T, y A. Del mismo modo, las letras que ocurren menos son Z, Q, y X.

Si un criptoanalista está estudiando un mensaje codificado que él cree que es escrito en inglés, y da cuenta que las letras E, T y A aparece frecuentemente, podría estar bastante seguro en que la tarea es la resolución de un

cifrado de transposición. Con esa pieza de información vial, puede empezar a repositionar las letras para construir anagramas, hasta que encuentre un patrón que eficientemente resuelve el mensaje completo. Respectivamente, si otros números arbitrarios aparecen con frecuencia, es probable que es un cifrado de sustitución.

Era sólo después de este tipo de estudio formal sobre la criptografía se aparece que las esquemas de encriptación volvió a sistemas más complejas. Pero a pesar de la invención de cifrados polialfabéticos, cifrados de auto-clave y los dispositivos de codificación, los criptanalistas siempre mantuvo su liderazgo, descifrando la mayoría de la correspondencia de importancia. Las tablas sólo acaba de cumplir, como las computadoras cada vez más potentes permitió complejos sistemas matemáticos de encriptación para hacer métodos de prueba y error obsoletos.

Capítulo 4

Criptografía moderna

The common person needs encryption to function effectively in the information age. So it's time for cryptography to step out of the shadows of spies and military stuff, and step out into the sunshine and be embraced by the rest of us.

— Zimmermann

4.1. Implementación y impacto

Hoy en día vivimos en la era de la información, en cual la criptografía se ha convertido en un componente esencial de nuestra vida cotidiana. Su cuenta de banco es puramente electrónica, protegida por varias capas de encriptación y verificación para asegurar la integridad de sus activos. Utiliza tarjetas de crédito y números de identificación personal para realizar las operaciones autorizadas, en las tiendas físicas así como en línea — y la gran mayoría de los servicios que utiliza en el Internet, como Facebook, correo, y chat, hacen un amplio uso de la criptografía.

Algoritmos criptográficos modernos basan su seguridad en fórmulas matemáticas profundamente difíciles de calcular, lo que significa que sin la clave adecuada,

hay cerca de un número infinito de combinaciones a probar.

Los avances también se han hecho en conceptos como la criptografía de clave asimétrica, en la que cada parte involucrada tiene dos claves diferentes pero matemáticamente relacionadas — la solución del viejo problema de la distribución de la clave de cifrado — así como en el hash, una forma de cifrado unidireccional a menudo utilizada para el almacenamiento y la verificación de contraseñas y otra información sensible.

4.2. Controversia

Como usted podría haber señalado, el mundo oscuro de la criptología ha sido durante mucho tiempo inclinado a favor de los criptoanalistas quienes rompen los códigos, que permite a los gobiernos a aprovechar los flujos de datos continuamente. En los últimos años, sin embargo, esto ha cambiado. Hoy en día, cualquier equipo es más que capaz de utilizar esquemas de encriptación prácticamente impenetrables.

Para cualquier gobierno con temor de la actividad del enemigo, esto obviamente es una situación muy alarmante; pero prohibir los algoritmos criptográficos para el uso público en gran medida impone a nuestro derecho humano fundamental a la privacidad. Como Phil Zimmermann, el autor de la sistema de encriptación PGP, afirma en una entrevista:

En una democracia, a veces gente mala puede ser elegido, y si la democracia se le permite funcionar normalmente, estas personas pueden ser sacado del poder por parte de las próximas elecciones. Pero si un futuro gobierno hereda una infraestructura tecnológica optimizada para la vigilancia, donde se pueden observar los movimientos de la oposición política, ver todos sus posibles via-

jes, todas las transacciones financieras, todas las comunicaciones [...] si la incumbencia tiene esta ventaja política sobre su oposición, entonces, si un mal gobierno llega al poder, puede ser el último gobierno que nos elegimos.

Teniendo en cuenta los acontecimientos recientes, los gobiernos están tomando medidas cada vez más drásticas para aprovechar la inteligencia tanto como escudo como arma contra la amenaza terrorista, pero esto se produce con un alto costo; la privacidad personal se convierte en un recuerdo del pasado. El experto en seguridad reconocido Bruce Schneier argumenta que siempre hay que evaluar el *comercio* cuando se trata de la seguridad: ¿si los beneficios valen su costo? Cuando se trata de este tipo de vigilancia, la respuesta simple es *no*. La única manera de acceder a la información debidamente encriptada hoy en día es de alguna manera obtener la clave — una situación que ha llevado a debate y pruebas sobre el derecho de las autoridades para obligar a un sospechoso de entregar esta información.

En varias dictaduras, como China por ejemplo, el uso de la criptografía sin un licencia del gobierno es un delito penal que puede llevar al culpable a la cárcel. La mal disimulada ambición de control que se muestra por los gobiernos de todo el mundo esta acercando la legislación moderna cada vez más a este tipo de estado; es imperativo no permitir la situación fuera de control. ¹

The more corrupt the state, the more numerous the laws.

— Tacitus

¹A principios de este mes, el “Stop Online Piracy Act” causó una gran conmoción internacional, porque el ley permitirá a instituciones gubernamentales así como privadas llevar a cabo la censura — obligando a los búsquedas para excluir sitios web de los resultados, y prohibiendo servicios de mercadeo y pagos de tratar con ellos.

4.3. Criptografía Public Key

En 1976, Whitfield Diffie y Martin Hellman publicó *New Directions in Cryptography*, un documento en el que se introdujo un nuevo concepto revolucionario conocido como la *criptografía de clave pública*. De acuerdo a esta estructura, cada parte tiene dos claves diferentes, aunque matemáticamente relacionadas — una privada y una pública. La clave pública es compartida con cualquier persona sin tener que preocuparse; la clave privada no se puede derivar de él.

El sistema es bastante sencillo: si Alice quiere enviar un mensaje cifrado a Bob, que utiliza la clave pública de él para realizar el cifrado. Entonces, el mensaje sólo puede ser decodificado por Bob, quien tiene acceso a la clave privada correspondiente.

Un requisito para este intercambio es que Alice realmente tenga la clave pública auténtica de Bob, un problema que se ha resuelto parcialmente mediante la *firma* de claves. Si una persona sabe con seguridad que una clave pública es real, él o ella puede firmarlo, añadiendo una capa de confianza a la clave. Otra solución es la existencia de *autoridades de certificación*, organizaciones que certifican la propiedad de los pares de claves.

Además de cifrar mensajes de todo, el sistema de clave pública puede ser usado para generar *firmas digitales*, que pueden ser incluidos en la correspondencia electrónica. Al marcar una firma en contra de la clave pública del autor, el destinatario puede verificar que el remitente de hecho posee la clave privada.

La infraestructura de clave pública es un componente fundamental de *Pretty Good Privacy* y *GNU Privacy Guard*, los cuales constituyen el software de encriptación principal utilizado por entidades privadas y corporativas para cifrar el correo electrónico, documentos, y sistemas de archivos enteros.

Bibliografía

R. Belfield. *The Six Unsolved Ciphers: Inside the Mysterious Codes That Have Confounded the World's Greatest Cryptographers*. Ulysses Press, 2007.

R.S. Brumbaugh. *The most mysterious manuscript: the Voynich Roger Bacon cipher manuscript*. Southern Illinois University Press, 1978.

J. Chadwick. *The decipherment of linear B*. A Canto Book Series. Cambridge University Press, 1990.

D. Kahn. *The codebreakers: the story of secret writing*. Scribner, 1996.

S. Singh. *The Code Book: The Secret History of Codes and Code-breaking*. HarperCollins Publishers, 2010.