Manuel J. Prieto

Historia de la criptografía

Cifras, códigos y secretos, de la antigua Grecia a la Guerra Fría

la esfera de los libros

Índice

Introducción

La necesidad de secretos y de formas de comunicarse seguras ha estado presente en la historia desde el comienzo de las relaciones entre humanos. Mantener información en secreto, para que tan solo uno mismo pueda conocerla y consultarla, es el primer paso. Pero tan pronto como aparecen los conflictos, y no es necesario que sean conflictos armados, la comunicación segura entre dos personas frente a un tercero cobra una importancia esencial. En el ámbito de la guerra o de los enfrentamientos más o menos abiertos y violentos, el intercambio de mensajes ha sido un elemento de preocupación para los gobernantes desde siempre. La amenaza de que un enemigo, un espía o cualquiera que no sea su destinatario legítimo pueda consultar y conocer la información que transporta un mensaje ha dado pie a que el ingenio haya florecido, creando soluciones para compartir y guardar información con garantías de confidencialidad. Dicho esto, también es cierto que durante muchos siglos la simple escritura daba cierta seguridad, ya que la mayoría de las personas no sabían leer ni escribir.

La carrera de los secretos, como otras muchas, perdura después de siglos y siglos, ya que frente a un nuevo método de ocultación de información o a una nueva forma de comunicación segura, han ido naciendo nuevas formas de romper esos avances y por lo tanto de inutilizarlos. Si

el uso de la criptografía a lo largo de la historia hubiese generado una solución definitiva y plenamente confiable, la historia sería otra. Es mucho más relevante para el devenir de los acontecimientos la influencia que ha tenido la criptografía cuando el uso de esta ha fallado y los mensajes que se creían secretos en realidad no lo fueron, que cuando ha funcionado como se esperaba. Esas situaciones han provocado que la balanza se incline hacia un lado u otro en un conflicto y han influido, a veces de manera crucial, en la historia.

Esta carrera entre criptógrafos y criptoanalistas, entre los que buscan guardar el secreto y quienes tratan de romperlo, ha dado pie a historias impresionantes y sorprendentes en algunos casos. En muchos de ellos la pugna ha sido un elemento esencial en el curso de los acontecimientos. El paso del tiempo ha ido obligando a que esos métodos de ocultación de la información sean más sofisticados y sólidos frente a los ataques para destruirlos. Por ello no es de extrañar que las matemáticas y la tecnología se convirtiesen en el pilar fundamental sobre el que se apoya esta rama del conocimiento que es la criptografía. Los países y los gobernantes se han visto obligados, y cada vez con más fuerza a medida que avanzaba la historia, a crear dentro de sus ejércitos, de sus gobiernos y de sus fuerzas diplomáticas unidades dedicadas exclusivamente a este mundo de la criptografía y a su uso para beneficio propio. Matemáticos, ingenieros, lingüistas y, en general, un buen número de mentes privilegiadas han dedicado gran parte de su vida a estudiar cómo romper métodos criptográficos ya conocidos y discernir cómo desarrollar otros nuevos. Estos nacían siendo seguros, *a priori*, pero otras mentes ya luchaban contra ellos en una partida de ajedrez continua.

Aunque en el texto veamos el término *criptoanalista* aplicado a todos aquellos que han trabajado para romper una cifra o un código, sea cual sea el momento histórico, lo cierto es que este término fue acuñado en el año 1923 por William Friedman, uno de los mejores criptógrafos precisamente en ese campo del criptoanálisis. Hasta entonces, para describir esta tarea se usaban grupos de palabras, u otras palabras, como

perlustrador, propia del castellano del siglo XVI. El criptoanálisis ha sido muy importante en la historia. Si no se hubieran roto los códigos y las cifras en determinados momentos, el secreto no se habría perdido y por lo tanto unos u otros no habrían sacado ventaja de ello. Una ventaja a menudo significativa. Si los códigos y cifras funcionaran siempre, las comunicaciones habrían sido secretas y seguras, que es lo que se espera de ellas, y por lo tanto un libro como este no tendría mucho sentido por carecer, en gran medida, de contenido relevante. Sin criptoanálisis y con métodos de cifrado totalmente seguros, la historia y la criptografía no tendrían tanta relación.

Según Friedman el criptoanálisis es la ciencia que abarca todos los principios, métodos y medios empleados en el análisis de los criptogramas, esto es, de los textos cifrados o codificados. Este análisis se hace para solucionar el criptograma, para conocer el texto en claro del que procede el propio criptograma, sin conocer el sistema utilizado en su construcción, su clave, el libro de códigos empleado... Se hace utilizando únicamente el estudio concienzudo de los propios criptogramas. Uno de los aspectos más atractivos de la criptografía y de los criptoanalistas, es que, en realidad, esa partida de ajedrez entre los que luchan por el secreto y los que tratan de romperlo es una batalla de ingenio, de inteligencia.

Por otra parte, como ocurre con todas las historias de ingenio, conocimiento, engaño y astucia, los hechos históricos relacionados con la criptografía suelen ser sorprendentes y apasionantes.

La criptografía podría ser, como veremos, algo tan sencillo como usar un método para ocultar el mensaje en claro, un mensaje que cualquiera pudiera leer en otro caso, o podría ser un método diseñado y acordado entre dos, entre emisor y receptor, para comunicarse con esas mismas garantías. Estos códigos y cifras particulares, acordados *sottovoce* por dos, habrán existido, con toda probabilidad, en cantidades enormes a lo largo de la historia. Es muy probable que muchos lectores los hayan creado de uno u otro modo, incluso sin darse cuenta. Algo tan sencillo como

convenir que se golpeará la puerta dos veces rápidamente, se dejarán pasar unos segundos, y luego se golpeará de nuevo, con el objetivo de identificar al que está al otro lado de dicha puerta, es ya algo parecido a la criptografía. Es un código acordado para enviar un mensaje, en ese caso, para identificar al emisor que está al otro lado de la puerta. Hasta nosotros han llegado miles de casos, de códigos, de formas de buscar la seguridad y el secreto en las comunicaciones.

Este no es un libro únicamente sobre la historia de la criptografía, aunque estará presente en él como no puede ser de otro modo, sino que es un libro sobre la presencia e influencia de la criptografía en la historia, y sobre cómo la primera ha influido en la segunda.

Según *El arte de la guerra* de Sun Tzu, quizás el texto militar más citado en todos los ámbitos, «lo que permite al soberano saber y al buen general intuir, esperar y anticiparse; aquello que sobrepasa los límites del común de los mortales, es el conocimiento previo». En muchos casos, para conseguir sobrepasar ese límite, la criptografía ha sido la barrera a salvar.

El 15 de febrero de 1676 Isaac Newton envió una carta a Robert Hooke, hombre de ciencia con el que el remitente había tenido una relación tensa por discrepancias científicas y por una riña sobre la necesidad de citar unos trabajos en las investigaciones del primero. Quizás también había una cierta lucha de egos, como es lógico. El caso es que la comunidad científica abogó por el entendimiento, aunque solo fuera por el beneficio de la ciencia, y acabó lográndolo. En esa carta de 1676 Newton parafraseó al filósofo del siglo XII Bernardo de Chartres, y dio lugar a la popularización de la sentencia «caminar a hombros de gigantes». Con esa frase se suele reconocer que uno ha llegado hasta su conocimiento o hasta sus logros, no solo por méritos propios, sino apoyándose en lo que otros han estudiado, escrito y avanzado antes. Bien es cierto que hay quien dice que la frase en la carta de Newton debe ser vista con un doble sentido, ya que Hooke, su corresponsal, era más bien bajo y con cierta chepa. Así, Newton reconocía a los científicos que habían sido anteriores

a él y de manera indirecta estaba eliminando a Hooke, que con su altura no podía ser considerado un gigante. No obstante, el sentido que ha pasado a la historia es el primero, y en gran medida describe la base del conocimiento y del avance de la humanidad.

En el mundo de la criptografía es esencial la evolución progresiva, ya que cada método criptográfico, una vez roto, ha mostrado el camino para no cometer los mismos errores y para dar pasos en una dirección que invalide los métodos de ruptura existentes. De igual modo, la propia evolución del conocimiento humano ha determinado la seguridad, o falta de ella, de los métodos de comunicación. Por ejemplo, cuando tan solo unos pocos hombres sabían leer, quizás era suficiente con cambiar algunas pocas palabras en un texto para conseguir que fuera segura esa forma de ocultar el mensaje a los ojos de otros. Así comenzaron los primeros códigos, con procedimientos que en aquel tiempo eran seguros y que hoy descifraría un niño en unos pocos minutos.

El método más básico, y con el que comenzó la historia de los códigos secretos o la ocultación de textos, la historia de la criptografía en su sentido más amplio, se basa en la sencilla ocultación del texto a los ojos indiscretos. Tan simple como eso, no se cambiaba nada del propio texto, sino que este se ocultaba de alguna forma, se hacía invisible. Veremos cómo en la Antigüedad estas estratagemas fueron utilizadas en varias ocasiones. El ingenio ya estaba presente y este tipo de técnicas se mantuvo en activo durante siglos, en ocasiones combinado con algún método básico de modificación del texto.

Esta forma de comunicarse de manera segura a través de la ocultación de los mensajes se conoce como *esteganografía*. Esta palabra proviene de la fusión de las palabras griegas *steganos* (oculto o cubierto) y *graphos* (escritura). La esteganografía es una disciplina cercana a la criptografía, pero en puridad no pertenece a esta. No hay cifra ni codificación del texto del mensaje, del texto en claro, como se denomina en el argot criptográfico, sino que sencillamente hay ocultación. Tampoco es lo mismo cifrar que codificar, como veremos más adelante.

La criptografía o el cifrado de la información estudia los métodos para ocultar el significado de un mensaje, siendo esta versión cifrada del mensaje perfectamente visible a los ojos de cualquiera. Es decir, la seguridad recae en el método que modifica el texto en claro y no en la ocultación a la vista del propio texto. Esta es la gran diferencia entre la criptografía y la esteganografía, si bien esta segunda se suele incluir dentro del campo de la criptografía, ya que el objetivo que persiguen ambas es el mismo.

Las tintas invisibles, serían un ejemplo de esteganografía. De forma general podríamos decir que lo es cualquier técnica o método que permita ocultar un texto, ya sea dentro de otro mensaje o de cualquier otra forma. Hay dos tipos de esteganografía, la técnica y la lingüística. En la primera, algún dispositivo o herramienta nos permite ocultar el mensaje secreto. Podríamos extender la definición de esteganografía técnica para incluir cualquier método donde no sea un texto aquello en lo que está oculto el mensaje real. Nos queda así la segunda categoría, la lingüística, que es aquella donde es un texto lo que oculta el mensaje principal, el mensaje que se quiere transmitir. En este caso, palabras, letras o frases sirven para formar el mensaje oculto. Aún hoy se siguen viendo casos donde las primeras letras de cada una de las palabras o de cada párrafo en un texto, por citar algún ejemplo, componen el mensaje real a transmitir, que queda oculto al diluirse entre el texto completo que lee el destinatario.

Hay infinidad de técnicas, métodos y sistemas para cifrar la información, para tomar un texto en claro y dar lugar a uno totalmente nuevo. Para que se comprenda mejor lo que se va a relatar, trataremos en esta brevísima introducción de asentar algunas bases sobre la terminología y las técnicas criptográficas.

Ya hemos comentado que el texto antes de ser cifrado es denominado «texto en claro» y que a la realización del proceso de encriptación se le llama de manera genérica «cifrar». Estos métodos en ocasiones utilizan una clave, algo similar a una contraseña, y el texto cifrado resultante depende

de esa clave, que también será necesaria para descifrar el texto. Hay un matiz importante a considerar en este momento en que introducimos la terminología. Hay que tener en cuenta que codificar y cifrar son cosas diferentes, si bien en la bibliografía, y en términos generales, la palabra cifrar se suele usar como sinónimo de encriptar, que engloba tanto a los métodos de cifrado como de codificación. Este pequeño matiz puede generar alguna duda si el lector no conoce los detalles, pero tan pronto como expliquemos la diferencia entre codificar y cifrar desaparecerá todo peligro de duda y el contexto marcará claramente el significado real de la palabra cifrar en cada caso.

Cifrar un texto en claro para generar un texto cifrado no tiene sentido alguno si no se dispone del proceso inverso, es decir, del proceso que nos permita conocer el texto en claro a partir del texto cifrado. Este proceso se conoce como «descifrado», y permite al receptor legítimo del mensaje conocer lo que el emisor quería decirle. El proceso completo sería tan sencillo como este:

1. El emisor toma el texto en claro y lo cifra o encripta con un determinado método.
2. El mensaje cifrado se envía al destinatario, e idealmente, si un tercero se hace con el mensaje, no podrá conocer el texto en claro al no conocer el método de cifrado, la clave usada... Es importante la palabra «idealmente» de la frase anterior, ya que como veremos hay una parte del arte de la criptografía que trata justo de leer los mensajes sin ser el destinatario legítimo. Volvemos aquí al papel del criptoanalista.
3. El receptor legítimo recibe el mensaje cifrado y lo descifra, volviendo así al texto en claro y siendo capaz de leer sin problema lo que el emisor quería comunicarle.

Aunque los iremos conociendo a medida que vayan apareciendo en la historia, antes de comenzar es conveniente tener un esquema muy básico de la clasificación de los métodos criptográficos, para crear un

punto de partida y para que el lector siempre pueda volver a esta sencilla referencia en caso de tener alguna duda durante la lectura. A grandes rasgos tendríamos métodos de sustitución, métodos de trasposición y la combinación de ambos.

La sustitución se basa, como su nombre apunta, en el cambio o sustitución de cada letra en el texto en claro por una o varias letras diferentes en el texto cifrado. Aunque hemos hablado de letras por simplicidad, pueden ser cualquier tipo de símbolos o tan solo números los que compongan el cifrado. Al conjunto de esos símbolos se le denomina alfabeto y cuando la sustitución de una letra durante toda la codificación es siempre la misma, esto es, la A siempre se sustituye por la D, por ejemplo, se trata de una sustitución *monoalfabética*. Cuando una letra puede tener varias sustituciones a lo largo del proceso (la A resultaría unas veces en la D, otras en la H) hablaríamos de sustitución *polialfabética*.

En cuanto a los métodos de trasposición, estos no sustituyen las letras o los símbolos del mensaje original, sino que sencillamente las cambian de lugar. Son muchos los sistemas que permiten la trasposición del mensaje, de tal forma que, sin sustituir las letras y solo alterando su posición, el mensaje cifrado sea ilegible. A modo ilustrativo, veamos un ejemplo sencillo. Basta con escribir el texto en varias líneas y luego tomar las letras por columnas. Supongamos que queremos cifrar la frase «por tantos hombres vales cuantas son las lenguas que hables». Lo escribimos en filas de seis caracteres cada una.

PORTAN
TOSHOM
BRESVA
LESCUA
NTASSO
NLASLE
NGUASQ

UEHABL
ESXXXX

El mensaje cifrado que se enviaría se construye tomando las letras en columnas. En este caso, que es solo ilustrativo, lo haremos sin más cambios, pero no es extraño que el orden en la selección de las columnas lo determine alguna clave, y no se tome la primera en primer lugar, en segundo la segunda y así sucesivamente. El mensaje cifrado sería en nuestro caso, por tanto: PTBLNNNUEOORETLGESRSESAAUHXTHSCSSAAXAOVUSLSBXNMAAOEQLX.

De nuevo tenemos que hacer una puntualización sobre la terminología, y es para diferenciar entre cifrar y codificar y a qué nos referimos realmente cuando hablamos de códigos en el mundo de la criptografía. Los códigos podrían ser considerados como un método de cifrado de sustitución, ya que un código no es más que una lista, cuanto más larga mejor, de palabras o frases que serán sustituidas durante el proceso por un símbolo, por una palabra o por una secuencia de números. Los libros de códigos han sido muy utilizados durante gran parte de la historia y, como veremos, no es extraño encontrarse con casos en los que la diplomacia y los gobiernos han utilizado libros de códigos con miles de entradas. Conceptualmente es algo similar a un diccionario. Así, un código haría que, en lugar de escribir España en un mensaje, escribiéramos 12354, si ese fuera el número asignado para España en el código. No es extraño que, una vez escrito el mensaje con las sustituciones marcadas por el código, se cifre con algún otro sistema ese mensaje, para completar su seguridad. Esto sería un *supercifrado*.

A pesar de que habitualmente se utilizan los términos código y cifra como si fuesen sinónimos, lo cierto es que son dos términos con distinto significado. De igual modo, codificar y cifrar también suponen acciones o métodos distintos. Ambos verbos se refieren a formas de ocultar un texto, un mensaje, pero la diferencia reside precisamente en las acciones que se llevan a cabo para ocultar el texto, para cambiarlo. La Real Aca-

demia Española (RAE) indica que encriptar es sinónimo de cifrar, y que esto último es transcribir con una clave. Ahí es donde reside una de las grandes diferencias, en la clave. Siguiendo con las definiciones de la RAE, codificar es transformar mediante las reglas de un código la formulación de un mensaje.

El Diccionario de Autoridades de la Real Academia ya indicaba en 1729 que cifra era «el modo u arte de escribir dificultoso, de comprender sus cláusulas si no es teniendo la clave: el cual puede ser usando de caracteres inventados, o trocando las letras, eligiendo unas en lugar de otras». Dos siglos más tarde el diccionario establecía que la criptografía es el arte de escribir con clave secreta o de un modo enigmático.

En el cifrado, por tanto, el procedimiento se apoya de alguna forma en una clave externa al propio texto en claro, al texto a ocultar. Dicha clave juega un papel fundamental en el proceso de generación del texto final que oculta el mensaje. En estos casos, para revertir el proceso y llegar de nuevo al texto en claro desde el texto cifrado, se necesitará conocer el método o procedimiento de descifrado, y además la clave. En cambio, cuando hablamos de un texto codificado, lo que se hace es sustituir ese texto por otro con base en un código. Esto es, en alguna forma de diccionario que establece una serie de equivalencias para las sustituciones. En los textos codificados, grupo de letras, palabras o incluso frases enteras son sustituidas por su equivalencia en el código.

Las implicaciones de lo anterior son importantes. Si un tercero intercepta un texto codificado, tan solo el desconocimiento del libro de codificación con las equivalencias evitará que sea capaz de hacerse con el mensaje en claro y por lo tanto de acabar con la seguridad del código. Así, en la codificación, es muy importante que no se conozca el diccionario o libro de códigos utilizado para ocultar el texto. Si un tercero, en cambio, intercepta un texto cifrado, tendría que conocer el método de descifrado que debe aplicar y además deberá conocer si esta se utiliza en el método en cuestión. Por lo tanto, las cifras son más seguras que las codificaciones. Tanto es así que, con el tiempo, los métodos de cifrado y

descifrado se han convertido en públicos y conocidos, y toda la seguridad se ha depositado en la clave.

Es conveniente remarcar que cuando hablamos de clave, no solo se trata de una palabra o una frase, que es en lo que habitualmente pensamos al mencionar esa palabra. La clave, como veremos a lo largo del texto, es conceptualmente algo más genérico, y puede ser una secuencia de caracteres casi infinita o una secuencia que se vaya generando sobre la marcha, a medida que se genera el cifrado. Como norma general, digamos que siempre que no exista un código con las equivalencias estaremos ante un cifrado, por complicado que sea encontrar la clave o incluso si esta no existiera.

En ocasiones se combinan ambas cosas, codificación y cifrado. Se habla en estos casos, como hemos visto, de supercifrado. Por ejemplo, se toma el texto en claro, se codifica usando un determinado código y ese texto codificado se cifra entonces para obtener la versión final del mensaje que será enviado al destinatario. Al recibir el mensaje, el proceso debe hacerse en sentido contrario, como si se eliminaran las capas que recubren el texto en claro. Primero se descifra el mensaje recibido y posteriormente este se descodifica.

La preponderancia de la clave sobre el sistema, método o algoritmo de cifrado ya fue descrita en 1883 por el holandés Augusto Kerckhoffs von Nieuwenhof, en su libro sobre la criptografía militar. El principio que lleva su hombre, el principio de Kerckhoffs y que es una máxima básica en criptografía, mantiene que la seguridad de un sistema criptográfico no debe depender de mantener en secreto el algoritmo o método de cifrado, sino que debe depender tan solo de mantener secreta la clave.

Los códigos y las cifras, en términos generales, tienen sus ventajas y sus desventajas. Tener que manejar libros de códigos con todas las equivalencias es un problema logístico que hay que resolver, lo que no siempre es sencillo. Un código es más seguro cuanto más extenso sea, y, por lo tanto, también es más complicado de transportar, distribuir y proteger. Además, si bien es posible memorizar algunas equivalencias,

un libro de códigos extenso obliga a llevarlo siempre encima y a buscar palabra por palabra, por lo que el proceso es largo y tedioso. A cambio, codificar es mucho más sencillo que cifrar, ya que casi cualquiera puede buscar una palabra en un diccionario. Las cifras obligan a menudo a hacer cálculos y sus procedimientos son complicados, por lo que requieren más conocimiento y hacen más complejo su uso de forma generalizada, por ejemplo en un ejército.

La facilidad de uso y la logística han sido decisivas de igual modo a lo largo de la historia y han determinado en muchos casos cómo se ocultaba la información. En términos generales, las comunicaciones diplomáticas o los envíos en las armadas, es decir, en las fuerzas navales, son más proclives al uso de códigos. El motivo principal es que están en un lugar fijo. Aunque el propio barco se pueda mover por los océanos, lógicamente, se puede mantener y consultar un libro de códigos sin mucho problema e incluso mantenerlo a buen resguardo sin muchas amenazas. En cambio, cuando hablamos de un ejército en combate, sus posiciones son móviles y están mucho más expuestos al contacto con el enemigo, por lo que un método de cifrado es más práctico, ya que no hay que cargar con voluminosos libros de códigos, ni consultarlos abiertamente para codificar o descodificar las comunicaciones. En estos casos un método de cifrado sólido basado en una clave que solo esté en la cabeza de aquel que se encarga de las comunicaciones parece una buena opción.

Estas ideas básicas son importantes para comprender los diferentes métodos criptográficos que iremos viendo en el texto y determinar a alto nivel sus potenciales debilidades y fortalezas. Dicho esto, seguiremos encontrándonos en las noticias, en las novelas y en otros muchos sitios, las palabras cifrar y codificar usadas como sinónimos. Es inevitable.

Aunque se trata de un camino progresivo y creciente, podemos estructurar la historia de la criptografía en tres grandes periodos o bloques, si bien las fronteras entre un periodo y el siguiente son difusas. Podríamos denominar criptografía clásica o manual a todos los métodos que se han ideado y utilizado desde la Antigüedad hasta los primeros años

del siglo XX, incluyendo la Primera Guerra Mundial. En estos casos las herramientas son habitualmente el lápiz, el papel y algunos dispositivos sencillos o herramientas simples. Todo se podía hacer y deshacer manualmente, con el tiempo y la paciencia suficientes.

En el periodo de entreguerras comenzaron a aparecer máquinas de cifrado con una complejidad suficientemente elevada y, en muchos casos, con funcionamientos electromecánicos que exceden la capacidad del ser humano, dotado con su cabeza, lápiz y papel, para afrontar su ataque o su réplica. Durante la Segunda Guerra Mundial, como veremos, el papel de estas máquinas fue esencial, y acabada la guerra siguieron cumpliendo con su cometido en la nueva configuración mundial durante mucho tiempo, haciéndose cada vez más complejas y efectivas.

Todo cambió con la llegada del procesamiento informático y los primeros proto-ordenadores, y desde los años setenta hasta nuestros días el mundo de la criptografía se ha transformado aún más. La complejidad de los algoritmos y la capacidad de procesamiento de las máquinas digitales vetaron la criptografía al ser humano, como elemento clave en el cifrado y descifrado propiamente dicho. Nuestro papel ha quedado en el de diseñadores, pero el cifrado y descifrado lo llevan a cabo las computadoras.

Según las últimas tendencias y gran parte de la bibliografía, tanto técnica como más generalista, estamos cerca de otra era en la criptografía gracias a la computación cuántica. Como comentaremos, hoy muchos de los algoritmos de cifrado son resolubles, pero es tan enorme la capacidad de cálculo necesaria para hacerlo, que son seguros en la práctica. La computación cuántica permitiría alcanzar esa capacidad de cálculo y romper sin más los métodos de cifrado que hoy se utilizan.