CRIPTOGRAFÍA Y LA MÁQUINA ENIGMA

La criptografía es la ciencia, y el arte, de transformar un mensaje en un “batiburrillo” ininteligible, de forma que solo los que conozcan una clave puedan reconstruirlo. Es una ciencia porque se rige por reglas matemáticas, pero también es un arte porque no hay forma de saber cuando un sistema de cifrado es bueno. Un criptógrafo que produzca un buen sistema de cifra tendrá siempre como adversario al criptoanalista, que intentará recuperar el mensaje sin conocer la clave. Es una lucha tan antigua como la de la espada y el escudo. Desde los tiempos más remotos se han utilizado códigos secretos para lograr que un mensaje resultara incomprensible para las personas no autorizadas a leerlos. En las tumbas del antiguo Egipto, existen múltiples ejemplos de escritura cifrada: se le atribuía un valor mágico, además del práctico. Vamos a recordar los códigos secretos que a través de la historia nos ayuden a penetrar en el más famoso de ellos: **la máquina Enigma.**

El cifrario de César

El historiador Suetonio (siglo I-II d. C.), describe un sistema de cifrado utilizado por Julio César por el que resultaba imposible captar el sentido de cuanto escribía. Sustituía la primera letra del alfabeto, A, por la cuarta, D, y así sucesivamente con todas las demás. Según este historiador, también el emperador Augusto utilizaba un sistema muy similar, aunque se conformaba con avanzar tan solo una posición.

La scitala espartana

El mensaje cifrado se escribía en una cinta de pergamino o de papiro que se envolvía sobre un bastón. Se retiraba la cinta y se enviaba al destinatario que tenía en su poder una copia idéntica del bastón. Al colocar de nuevo la cinta, aparecía el mensaje.

El atbash hebreo

Se utiliza el alfabeto hebreo. Se van sustituyendo las letras del mensaje de acuerdo con la disposición de una tabla que consta de dos líneas de letras del alfabeto hebreo. El atbash se emplea en la Biblia (libro de Jeremías)

Otros sistemas

Con el paso de los siglos se idearon los cifrarios de rotación, que consisten en dos discos concéntricos que pueden girar de forma independiente; en sus bordes, a intervalos regulares y en el orden habitual, figuran las 26 letras del alfabeto. Este sistema fue utilizado por León Battista Alberti (1402-1472) y Della Porta (1535-1615)

Otro sistema utilizado en el siglo XVI era el de *cifrario polialfabético* de Vigenére (1523-1596) consistía en que la misma letra de origen, en el transcurso de la operación de cifrado, se transforma en distintas letras cifradas. Durante mucho tiempo y erróneamente, se consideró que el cifrario de Vigenère era inexpugnable con métodos criptoanalíticos. Sin embargo ya en el siglo XIX, Kasiski creó el primer método de ataque contra los cifrarios polialfabéticos.

Hasta ahora nos hemos referido a los sistemas de cifrado que proceden del cifrario de César y del atbash. Vamos a tratar ahora sobre los que tiene su origen en la citala espartana, es decir, pasaremos de los cifrarios de sustitución a los de *transposición* .Gran parte de los códigos secretos

de este tipo se basan en el empleo de *rejillas.* Al parecer, éstas fueron incorporadas a la criptografía por Girolamo Cardano en el siglo XVI.

Julio Verne (1828-1905) que sentía una pasión evidente por la criptografía; la utilizó en tres de sus novelas: *Viaje al centro de la Tierra, Mathias Sandorf y La Jangada.*

Criptografía táctica y criptografía estratégica

La finalidad de la *criptografía estratégica* consiste en garantizar el secreto de los mensajes cifrados para siempre, mientras que la *criptografía táctica*, que es menos ambiciosa pero también menos costosa, se conforma con una duración que puede ser incluso de algunas horas o de algunos días.

Auguste Kerckhoffs (1835-1903) es el autor de un tratado muy importante, *La criptografía Militar*, que se publicó en1883. Kerckhoffs ilustra claramente la diferencia existente entre los sistemas de tipo táctico y los de tipo estratégico, cuando afirma que hay que distinguir cuidadosamente entre un sistema de cifrado pensado para la protección temporal del intercambio de cartas entre personas individuales y un sistema criptográfico destinado, por el contrario, a proteger la correspondencia de los jefes del ejército durante un tiempo ilimitado. En opinión de Kerckhoffs, compartida hoy día por todos los criptólogos, un sistema de tipo estratégico debe poseer, como característica fundamental la siguiente: *La seguridad de un sistema estratégico se basa totalmente, o de forma esencial, en el secreto de la clave; si el enemigo descubre el tipo de cifrario utilizado pero ignora la clave empleada para el descifrado, el secreto del mensaje queda aún garantizado.*

Códigos

Hasta ahora hemos visto distintos sistemas de cifrado que poseen una clave fija (= una clave única) y, por consiguiente, resultan totalmente inutilizables en la criptografía estratégica: cifrario de César, la scitala espartana, el atbash bíblico o la rejilla del conde Sandorf. En Criptografía, los sistemas de clave fija se llaman *cifrarios degenerativos*; más respetuoso es el término *cifrarios de código* o, para ser más breves, *códigos*. En realidad, los códigos en los que falta en absoluto el aspecto de secreto son de uso común: uno de los ejemplos más ilustres es el código telegráfico que recibe el nombre de “alfabeto Morse”. Los mensajes se escriben utilizando tres símbolos: el punto, la raya y el espacio. Volvemos a insistir que el alfabeto Morse *no* es un código criptográfico: es tan solo un sistema de trascripción, conocido por todos los especialistas.

Por otra parte existe una zona muy amplia en la que se superponen el estudio de las lenguas y el de la criptografía: es toda esa franja que se refiere al descifrado de las lenguas muertas. Destacamos en este apartado a Champollion que en 1822 descifró los jeroglíficos del egipcio arcaico, utilizando la piedra Rosetta. En dicha piedra, el mismo mensaje figuraba escrito en griego clásico (= texto de origen), en jeroglíficos hieráticos (=primer texto cifrado) y en demótico (= segundo texto cifrado, conseguido “cifrando” el mismo mensaje de origen con un “código” distinto). El demótico es un hierático simplificado que, poco a poco, se fue convirtiendo en escritura de uso común a partir del 700 a. C.

Criptografía mecánica

En la segunda mitad del siglo XVIII, estalló la *revolución industrial*. La pasión por las máquinas, además de estar alentada por exigencias de tipo práctico, se convierte en una especie de actitud filosófica e invade los campos más disparatados, desde las industrias textiles hasta los talleres de fabricación de instrumentos musicales.

Hacia 1820, el matemático inglés Charles Babbage empezó a proyectar su “máquina analítica”, un potente ordenador mecánico con tarjetas perforadas, que constituye el antecedente de nuestros ordenadores electrónicos.

Aunque la máquina de Babbage quedó como un sueño de un visionario, otras máquinas alcanzaron un éxito inmediato. Fue fundamental la invención del telégrafo electrónico, que siguió al

óptico de Claude Chappe, y tuvo una influencia decisiva en el desarrollo de la criptografía en 1835, Samuel Morse expuso su modelo en la Universidad de Columbia; ocho años más tarde se inauguró la primera línea telegráfica, de unos treinta kilómetros de longitud, entre Londres y el castillo de Winsord. El desarrollo de las técnicas de comunicación tuvo también una influencia decisiva sobre las "técnicas de guerra": la situación de las operaciones militares ya se podía controlar a distancia.

La historia de la criptografía corre ya paralela a la historia de los avances técnicos en el terreno de las telecomunicaciones, cuyas etapas nos son bien conocidas. El teléfono, la telegrafía sin hilos, la radio y los ordenadores electrónicos, que Babbage se limitó a soñar, pero que se construyeron realmente durante la Segunda Guerra Mundial, son hitos esenciales en la historia de nuestra sociedad.

La revolución industrial intervino también de forma más directa en la historia de la criptografía: las operaciones de cifrado y descifrado, poco a poco, se fueron mecanizando y automatizando. El elemento típico de las máquinas que se fabricaron, al menos hasta el final de la Segunda Guerra Mundial, es el *rotor*.

Rotores y máquinas de cifrado

En época de guerra se hace indispensable que en el caso de que el enemigo intercepte nuestros mensajes, no tenga manera de saber que significan. La forma de lograrlo consiste en alterar su contenido de una manera que solo el receptor del mensaje pueda devolverlo a su forma original. Si el método empleado para alterar (o "encriptar", por "hacer críptico" su contenido) el texto es demasiado complicado, puede utilizarse una máquina que lleve acabo la tarea. Hoy día, se utilizan ordenadores o microcontroladores para ello. Pero no siempre fué así.

Durante la Segunda Guerra Mundial, la mayor parte de los mensajes transmitidos entre diferentes secciones de cada ejército se hacía mediante el uso de la radio. La radio tiene la desventaja de que cualquier persona que disponga de un receptor funcionando en la frecuencia adecuada puede escuchar los mensajes, por lo que se hace imperioso encriptarlos para mantener el secreto. Los alemanes utilizaron la que luego sería la máquina de encriptar más famosa de la historia: **La máquina Enigma**.

El alto mando alemán utilizó como base para la construcción de su máquina los trabajos de Arthur Scherbius, creador de una máquina encriptadora comercial, basada en una serie de *rotores* que cambiaban una letra por otra. Como Scherbius carecía de dinero suficiente para llevar adelante su empresa, por lo que se asoció a Willie Korn, dueño de la compañía Enigma Chiffiermaschinen AG, de Berlín. Estos dos empresarios mejoraron el diseño de la máquina de Scherbius, adicionándole rotores intercambiables. En 1923 disponían de una nueva máquina prácticamente inviolable que vendían para la protección de secretos comerciales.

Poco apoco, **Enigma** fue penetrando en las fuerzas militares alemanas. Primero fue la marina, luego el ejército y por último la fuerza aérea. Todas adoptaron la Enigma como la "encriptadora" oficial. Cuando el Servicio de Inteligencia, las SS, la GESTAPO y el Servicio de Seguridad e Inteligencia Política del Partido Nacionalsocialista comenzaron a utilizar **la máquina Enigma,** en 1926, la empresa quedó directamente bajo el control del Estado Alemán y la máquina fue retirada del mercado comercial. Enigma que originalmente tenía tres rotores fue modificada por la marina para incorporar un cuarto rotor y hacerla más segura.

Esta máquina se conocía dentro de la Fuerza como "Eins" (modelo uno) o "Wermarcht Enigma" (modelo W) y entró en servicio el 1 de Junio de 1930. Era capaz de "mezclar" el texto de los mensajes de 200 quintillones de formas diferentes. Y con la clave correcta, volverlo a la normalidad. Se transformó rápidamente en el código secreto indescifrable de las Fuerzas Armadas. O al menos eso creían los alemanes.

El talón de Aquiles del **sistema Enigma** fueron las máquinas comerciales. A pesar de ser retiradas del mercado, y de no funcionar exactamente igual que los modelos de las fuerzas armadas, el GCCS (Government Code Ciphering School) de Inglaterra pudo descifrar algunos mensajes provenientes del modelo comercial. Pero rápidamente se dieron cuenta que no podían descifrar los códigos de las **Enigmas 1 y W.** Pero un grupo de matemáticos polacos pudo lograrlo en 1939.

El gobierno inglés ocultó hasta 1986 este hecho, dando la impresión de que habían sido ellos los que lograron romper el código. Cuando la verdad fue revelada, se supo que los polacos, utilizando

cuatro estaciones de escucha en Varsovia, Strogard, Poznan y Krzeslawice, analizaban el **código Enigma** desde 1928. Con la ayuda de varios matemáticos de la Universidad de Poznan, y empleando una máquina Enigma comercial, sentaron las bases para quebrar el código.

Trabajando junto con los franceses, lograron obtener una descripción de los modelos Enigma militares y algunas viejas tablas de códigos. En 1933 los polacos ya podían descifrar mensajes alemanes. Para 1939 habían leído unos cien mil mensajes secretos. Este hecho fue mantenido en gran secreto, para evitar que el ejército alemán modificara su sistema.

Pero de forma sorpresiva, en septiembre de 1938, los alemanes cambiaron completamente el método utilizado para generar códigos. Como respuesta, los polacos fabricaron el primer "computador mecánico" de la historia, la llamada "bomba criptológica", que junto a otro aparato denominado "ciclómetro" los ayudaba a establecer patrones en los mensajes interceptados.

Aunque demasiado complejo como para ser explicado aquí, mencionaremos que el método de trabajo consistía en el uso de varios juegos de 26 hojas de papel perforado con 2601 agujeros, agrupados en 51 líneas de agujeros de 51 columnas. Esto les permitía hallar la forma en que se ajustaban los rotores para formar las claves.

No era una tarea fácil. En un momento, la complejidad de la Enigma obligó a los polacos a utilizar 60 "bombas criptológicas" y juegos de 60 hojas perforadas en lugar de 26. A principios de julio de 1939, el Jefe de Estado Mayor polaco comenzó a compartir los secretos arrancados a Enigma con los servicios de inteligencia aliados.

Gracias a la colaboración de Polonia, los británicos pudieron leer mensajes alemanes a partir de agosto de 1939.

La clave del Enigma queda determinada por la estructura interna de los rotores y por su posición inicial. Los rotores podían ser de nueve tipos distintos, en los modelos empleados por el ejército alemán, y de cuatro tipos en los modelos utilizados por la marina, tenían que sustituirse con frecuencia para evitar que los criptoanalistas enemigos consiguieran alguna pista. De hecho, podemos afirmar que el Enigma está muy por encima de los sistemas criptoanáliticos de lápiz y papel. Para forzarlo (aunque algunos detalles de la solución se siguen manteniendo en secreto), los ingleses recurrieron a máquinas de cálculo gigantescas, llamadas justamente *Colosos*, a las que se puede considerar como precursoras de los ordenadores electrónicos modernos.

Hay quienes afirman que 1943, el año en que entraron en funcionamiento los Colosos, es el año de nacimiento de la informática, pero quizá esta fecha se debería anticipar algunos años, a favor de las ingeniosas máquinas electrónicas proyectadas por el alemán Konrad Zuse en 1936. Al grupo de contraespionaje británico pertenecía Alan Turing, uno de los más famosos matemáticos del siglo XX, que fue uno de los fundadores de la informática teórica.

Desde la aparición de la **máquina Enigma** hasta nuestros días las cosas han cambiado bastante, sólo tenemos que recordar que el **Enigma** tenía un inconveniente grave: carecía de impresora. Los resultados aparecían iluminados en un teclado especial, letra a letra, y una persona tenía que encargarse de transcribirlos a mano en una hoja de papel. Una impresora electromecánica hubiera añadido demasiado peso al dispositivo y éste hubiera sido escasamente manejable: un problema que la técnica moderna permite solucionar sin dificultades.

Vamos a finalizar con unas palabras de un apasionado de la criptografía, Edgar Allan Poe:"es dudoso que el género humano logre crear un enigma que el mismo ingenio humano no resuelva".