Desde que el ser humano escribió la primera palabra, se han querido ocultar y codificar mensajes .

Secretos de Estado, órdenes militares, asesinatos o la simple privacidad entre personas han servido para desarrollar complejos sistemas de encriptación que han desempeñado un rol fundamental en la guerra y la política.

Manuel J. Prieto nos ofrece una perspectiva completa y convincente de la criptografía a lo largo de la historia, desde el cifrado de griegos y romanos hasta la lucha contra Enigma, pasando por el espionaje en época imperial, los gabinetes oscuros, la Guerra de Independencia española, el telegrama Zimmermann o los avances en computación de la Guerra Fría.

Una historia de una batalla de ingenios llena de grandes ideas, debilidades inesperadas, mentes maravillosas y héroes en la sombra.

Manuel J. Prieto

Historia de la criptografía

Cifras, códigos y secretos desde la antigua Grecia a la guerra fría

ePub r1.0

XcUiDi 29-09-2020

Título original: Historia de la criptografía

Manuel J. Prieto, 2020

Editor digital: XcUiDi

ePub base r2.1

AADGD GDXDD FXXXA GAXAD AXGDA ADGAD FFXFG F.

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: PTBLNNNUEOORETLGESRSESAA UHXTHSCSSAAXAOVUSLSBXNMAAOEQLX.

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 Academia 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.

PARTE 1LOS PRIMEROS 3.500 AÑOS

1. Las primeras fuentes

El secreto es inherente al propio ser humano y por lo tanto es muy posible que los métodos de ocultación de información hayan existido desde el mismo momento en el que apareció alguna forma de mantener el registro de dicha información, bien fuera por escrito o por cualquier otro método.

El primer uso de la criptografía del que se tiene constancia data de hace casi 4.000 años, de aproximadamente el año 1900 antes de Cristo. Se trata de un objeto del antiguo Egipto, de un grabado en piedra realizado en la tumba de un noble de la ciudad de Menet Khufu, junto al Nilo, y en el que se cuentan los actos más importantes de su vida. Los símbolos habituales usados en la escritura jeroglífica de la época aparecen aquí modificados en cierta medida, y lo más importante es que hay algunas sustituciones entre ellos. Probablemente el objetivo al hacerlo no fuera ocultar ningún mensaje, motivo por el que habitualmente se usa la criptografía, ya que no tendría mucho sentido para la época describir la vida de un hombre en su tumba con una serie de símbolos a la vista de todos, y a su vez hacer incomprensible este escrito. Ya veremos más adelante cómo sí se ha hecho esto mismo para dejar en algunas tumbas ciertos mensajes cifrados destinados a iniciados. Volviendo a la tumba de Egipto, probablemente los cambios introducidos con respecto a la escritura habitual se debieran tan solo a la intención de dotar de cierta importancia al propio texto y de mejorar estéticamente el resultado final. En este caso, por tanto, faltan muchos de los motivos y de las características inherentes a la criptografía, pero a pesar de ello es considerado por toda la bibliografía como el caso más antiguo de esta disciplina.

Cuatro siglos más tarde, en torno a 1500 a. C., en Mesopotamia, aparecen de nuevo alteraciones en la escritura habitual. Los signos cuneiformes eran modificados en algunas ocasiones, y en este caso sí que el objetivo coincidía ya con el de la criptografía tal y como la conocemos: esto es, ocultar información a determinados ojos. Es curioso que ya se detectara en los escritos cuneiformes de Mesopotamia, que están considerados como una de las primeras formas de escritura de la humanidad, la intención de ocultar el texto en claro. Como decíamos, esta necesidad, este apego al secreto y la confidencialidad en las comunicaciones es tan antiguo casi como el propio ser humano. En el caso mesopotámico, lo que se trataba de dejar por escrito para que no se perdiera u olvidara, a la vez que se deseaba mantener en secreto, no era otra cosa que una fórmula para fabricar un barniz empleado en alfarería.

En textos hebreos, ya unos mil años después del caso mesopotámico, aparecen algunas palabras importantes, habitualmente nombres propios de personas y de lugares, que han sido sometidas a una transformación

en la que de nuevo aparecen sustituciones donde unas letras se cambian por otras del mismo alfabeto. Este es un método básico dentro de la criptografía, la sustitución, y como hemos visto es la primera opción que aparece cuando se quiere alterar un texto para hacerlo ininteligible. No es de extrañar que sea así, por su sencillez, y no es de extrañar que esta sencillez conlleve una enorme fragilidad frente al criptoanálisis. A pesar de esto, veremos que son muchas las ocasiones en las que se ha utilizado.

El método de cifrado de César, uno de los más conocidos de la Antigüedad, es un método de sustitución tan sencillo que roza la ingenuidad. Y más sabiendo que entre esas primeras aproximaciones y la época de César, hubo tratados y muchos otros métodos criptográficos.

En al menos una decena de fuentes clásicas, grecorromanas, nos encontramos con descripciones de métodos de criptografía o esteganografía, habitualmente en textos relacionados con la guerra, como era de esperar. Estas fuentes van desde Heródoto, del siglo V a. C., que como veremos ya nos describe con cierto detalle el uso de algunos métodos de ocultación de información, hasta el poeta Décimo Magno Ausonio, que vivió entre el año 310 y el 395. Entre estos dos extremos hay unos ocho siglos del mundo occidental, en los que la criptografía aparece consignada como algo elemental en las acciones de guerra y en las relaciones diplomáticas. Eneas el Táctico describe varios métodos de ocultación de información en uno de los tratados que dejó escritos, concretamente en uno sobre asedios. Veremos en el resto del libro cómo no son pocas las veces en las que precisamente es un asedio el lugar donde aparece la criptografía como puntal de la acción. Filón de Bizancio, por otra parte, que vivió entre 280 y 220 a. C., dedicó gran parte de su tiempo a escribir sobre mecánica y dispositivos, y ahí nos legó sus pensamientos y recomendaciones sobre cómo escribir y enviar cartas secretas. Vemos, por tanto, que no se trata ni mucho menos de una disciplina extraña o minoritaria, y no solo en el uso, sino también en los textos, ya desde muy atrás en el tiempo.

2. Grecia y roma

Es Heródoto, el historiador clásico que vivió en el siglo V a. C., el que dejó por escrito para la posteridad los primeros casos de uso de las técnicas de comunicación seguras; en este caso, de la esteganografía. No es cualquier autor, ya que se le considera el padre de la historiografía por su obra *Historias* , escrita en torno al año 430 a. C. y en la que recoge los hechos y las luchas entre griegos y persas.

En el primer libro, Heródoto relata cómo Harpago, general medo, se vio como arma del rey Astiages contra su nieto, Ciro. Después de un sueño y dentro de una de esas historias de reyes y venganzas que pueblan las magníficas narraciones clásicas, a caballo entre la realidad y la leyenda, Astiages determinó que Ciro debía morir, a pesar de ser su nieto. Todo había comenzado cuando el rey soñó que su hija Mandane despedía tanta orina que no solo llenaba la ciudad, sino toda Asia. Los magos que asesoraban al rey le llevaron a buscar un marido para su hija, llegado el momento y haciendo caso al sueño, lejos de Media, su reino. El elegido fue Cambises, un persa. Tras el matrimonio, de nuevo una visión azotó al rey Astiages. En ella, del vientre de su hija nacía una parra que daba sombra a toda Asia. Su hija estaba embarazada y los magos que interpretaban los sueños determinaron que el mensaje era claro: el fruto de aquel vientre reinaría sobre Asia, tomando el lugar del propio Astiages. De nuevo con un sueño como base de sus decisiones, Astiages ordenó que, tras el parto, fuera condenado a muerte su nieto, Ciro.

Encargó el infanticidio a Harpago, uno de sus fieles servidores, pero este encontró algo cruel e inmoral el asesinato de un niño, por mucho que los magos determinaran que en el futuro iría contra el rey del propio Harpago. Las palabras de Astiages eran determinantes, según la crónica que Heródoto escribió más de un siglo después, ya que Astiages reinó en la primera mitad del siglo VI a. C.: «Toma el niño que Mandane ha dado a luz, llévalo a tu casa y mátalo, sepultándole después como mejor te parezca».

Cuando Harpago tuvo al niño en sus manos, ricamente vestido, se vino abajo y comenzó a llorar, incapaz de cumplir con el mandato de Astiages. Harpago sabía que su rey se hacía viejo, no tenía descendencia masculina y, por lo tanto, el pequeño que tenía en sus brazos podía ser un futuro rey, ya que la línea sucesoria llegaría a él a través de Mandane. También era consciente de que no cumplir la orden suponía un severo castigo, probablemente la muerte. En ese dilema, Harpago llamó a un pastor llamado Mitradates y le encargó que se llevara al niño y lo abandonara en las montañas para que muriera. Por suerte para Ciro, y para la narración de Heródoto, este pastor también acababa de ser padre, pero su hijo había fallecido nada más nacer. Los pastores cambiaron un niño por otro y Ciro fue criado por ellos. El

cadáver del pobre bebé que había fallecido, el hijo del pastor, fue encontrado en el monte y así quedaron contentos Harpago y Astiages.

La vida del joven Ciro se desarrolló dejando muestras claras de que era un rey lo que habitaba dentro de él. Cuando se hizo mayor de edad y se conocía ya toda la historia sobre sus padres, comenzó Harpago a buscar la forma de poner a Ciro de su lado y en contra de Astiages, ya que sabía que por sí mismo nunca podría enfrentarse al rey. Ciro vivía en Persia y Harpago no tenía forma sencilla de enviarle un mensaje de manera personal, ya que los caminos estaban guardados por hombres de Astiages y no era posible que la comunicación se hiciera sin que llegara a oídos de su rey, al que iba a traicionar. Tomó entonces una liebre y, tras abrirla, le metió en la barriga una carta para Ciro. Le dio entonces el animal a uno de sus hombres, que se debía hacer pasar por cazador y así llegar hasta el persa, pidiéndole además que cuando llegara a su destino dijera a Ciro que debía abrirla con sus propias manos. La carta le descubría a su destinatario el mal momento por el que atravesaba el reinado de su abuelo, Astiages, que había perdido la fidelidad de sus generales, por lo que un ataque aprovechando esa debilidad tendría una victoria como resultado. Ciro, como era de esperar, lanzó el ataque y venció.

Más allá de lo cierto o ficticio que haya en esta historia, lo que sí parece claro es que la esteganografía, aunque en una forma primitiva, ya estaba en la mente y en las intenciones de los hombres del siglo VI a. C. La ocultación de un mensaje para establecer una comunicación segura entre dos extremos, en este caso entre Harpago y Ciro, es por lo tanto tan antigua casi como la civilización. Con el tiempo veremos cómo las matemáticas y todo tipo de métodos ocurrentes han ido poblando la historia, pero el cometido siempre es el mismo, sea una liebre la forma de ocultación o un complicado algoritmo matemático.

Siguiendo con Heródoto, en el libro V de la misma obra tenemos la narración de cómo Histieo, un ateniense que fue tirano de Mileto, envió un mensaje a Aristágoras para que este se rebelase contra los persas. La historia es parecida a la de Harpago y la liebre, pero este caso es un poco más literario e interesante. Histieo rasuró la cabeza de un esclavo que le era fiel y marcó sobre el cuero cabelludo el mensaje. Esperó a que le creciera el pelo lo suficiente como para hacer invisible la piel y entonces envió al esclavo hasta Aristágoras, que recibió la petición del propio esclavo de que le raparan la cabeza. Sin duda este método puede ser efectivo, pero no es muy práctico si el mensaje se ha de enviar con cierta celeridad.

Se repiten en los textos de Heródoto los ejemplos de esteganografía. Demarato fue rey de Esparta durante casi veinticinco años, a partir de 515 a. C. Debido a las intrigas, traiciones, apoyos y desencuentros que llenan la historia de entonces a esta parte, y también antes, Demarato acabó siendo expulsado de Esparta y se vio en la corte del rey persa Darío I. En el mundo persa consiguió tener cierto peso e incluso es muy probable que su opinión fuera muy tenida en cuenta en la selección de

Jerjes como sucesor de Darío. Por todo esto no es extraño que, aun siendo espartano, estuviera al tanto de los planes de Jerjes contra Atenas y Esparta, gracias a lo cual pudo hacer un gran servicio a su patria de nacimiento, a pesar de todo.

Antes de la campaña de Jerjes contra Atenas y Esparta, mientras el persa se preparaba para acometerla, Demarato tomó unas tablillas, según Heródoto, y escribió sobre ellas un mensaje de aviso sobre el inminente ataque. Una vez hecho esto, lo cubrió con cera. Así, el mensaje no podía leerse y a los ojos de cualquier guardián curioso, no eran más que unas simples tablillas. El destinatario del mensaje no tenía más que calentar la cera, que se derretiría y escurriría, para leer el mensaje. Esto, que parece tan obvio, no lo fue tanto y lógicamente, cuando los espartanos tenían ante sí las tablillas, no pensaron en que la cera ocultara nada. Con toda probabilidad no entendían nada de aquel envío. Fue entonces cuando Gorgo, la esposa de Leónidas, tuvo la ocurrencia de retirar la cera para ver si había algo debajo de ella. El mensaje de Demarato quedó así al descubierto y los espartanos sobre aviso del peligro que les esperaba. El resultado de esta acción fue que los griegos comenzaron un proceso de preparación para la guerra, construyendo naves y destinando recursos al ámbito militar, con la vista puesta en el momento en que Persia asomara en el horizonte para atacarles.

Cuando en septiembre del año 480 a. C. la flota persa de Jerjes I se acercó a la bahía de Salamina, en lugar de tener el factor sorpresa de su lado y poder aprovecharlo para vencer con cierta facilidad, se encontró con unos griegos listos para plantarle cara. Estos jugaron bien sus cartas, atrajeron a la bahía a la flota enemiga y allí los persas fueron derrotados.

Con buen criterio, uno podría pensar que quizás estos métodos son simples y que no hay mucha diferencia entre decir un sencillo mensaje a un hombre y enviarlo al destino, y esconderle un mensaje en la cabeza y enviarlo al destino. La traición bastaría, en un caso y en el otro, para que el mensaje cayera en manos del enemigo, bien porque el mensajero contara el mensaje, bien porque dijera que le raparan la cabeza. Quizás la literalidad del texto es importante, y no es lo mismo algo escrito que algo contado por otro. Tampoco el conocimiento o desconocimiento de la validez del emisor. Esto es, la certeza de que el mensaje proviene de quien creemos que proviene. Estos elementos, aunque puedan parecer sencillos, están presentes en la criptografía desde hace siglos y siguen siendo parte clave de cualquier método o solución: la seguridad sobre la identidad del emisor del mensaje y la seguridad sobre la no alteración del mensaje durante el proceso de emisión. Muchas veces se ha descartado un mensaje o se ha dudado de él, sencillamente porque uno de esos dos elementos no estaba garantizado.

Siguiendo con los espartanos, tenemos el que se considera el primer aparato criptográfico de uso militar de la historia. Se remonta al siglo V a. C. y lo utilizaron los lacedemonios durante las guerras del

Peloponeso, entre Esparta y Atenas, para enviar mensajes de manera segura. El instrumento en cuestión es la escítala, o escítalo según otros autores, y no era más que un palo, que debidamente utilizado cumplía con ese cometido de hacer complicada la lectura de un mensaje escrito, si este era interceptado. Es Plutarco, el historiador y filósofo griego nacido en el siglo I, el que nos dejó explicado en su obra *Vidas paralelas* , ya del siglo II, cómo usaban los espartanos la escítala. El compendio de biografías que es la obra de Plutarco, empareja las vidas de algunos hombres, griegos y romanos, y entre los primeros incluye a Lisandro, un general espartano que dominaba la guerra naval y que venció a Atenas.

Habla Plutarco de un mensaje enviado en una correa por los éforos, importantes hombres dentro de Esparta, a Lisandro, con la orden de que se presentase ante ellos. Cuando los éforos mandaban un mensaje a alguno de los comandantes de la armada, explica el biógrafo clásico, cortaban dos trozos de madera redondos y enteramente iguales en el diámetro, en el grueso de la madera. Es decir, tomaban dos palos uniformes del mismo grosor, o partían un palo en dos. A cada uno de estos dos trozos es a lo que se llamaba correas y el emisor se quedaba con un palo mientras que el destinatario se llevaba el otro. Así, los éforos tenían un palo igual al palo que tenía un general o un comandante en el campo de batalla o en campaña, alejado miles de kilómetros.

Cuando querían comunicar algo, tomaban una tira de papiro larga y estrecha, y la acomodaban o enrollaban cuidadosamente a lo largo de la correa, del palo. Podemos imaginar que hacían algo así como forrar la correa con la cinta de papiro, sin que hubiera huecos por los que se viera la correa. Hecho esto, escribían el mensaje a enviar en el papiro enrollado sobre la correa, haciéndolo de manera longitudinal. Es decir, si suponemos que un lápiz con forma hexagonal, forma común en los lápices, es nuestra correa, que ciertamente puede servirnos como tal, sería escribir sobre el papiro enrollado en el lápiz a lo largo de cada una de esas caras del hexágono que van desde la goma a la punta del lapicero. Agotada una línea, se giraba un poco la correa con el papiro enrollado y se continuaba escribiendo. Una vez redactado el mensaje por completo, se desenrollaba el papiro, que sería una tira llena de letras descolocadas e imposibles de entender con normalidad y se enviaba al destinatario. En el caso que cuenta Plutarco, lo envían los éforos a Lisandro. Se remitía solo el papiro, sin la correa, que no era necesaria porque el general tenía la suya, con el mismo grosor y, por lo tanto, una vez recibido el mensaje, no tendría más que enrollar el papiro con el mensaje en su correa, que colocaría cada letra en su sitio y dejaría a las claras el mensaje escrito en origen.

Aunque no lo he mencionado hasta ahora para que la explicación fuera más clara, también se denominaba correa a la tira de papiro sobre la que se escribía. Plutarco narra cómo a través de este método, en el año 404 a. C., Lisandro fue avisado por los éforos de que Farnabazo II de Persia planeaba atacarlo. El mensajero llegó a duras penas hasta

Lisandro, pero gracias a él se preparó para enfrentarse a Farnabazo II y consiguió defenderse con éxito.

Este método es tan sencillo y claro, que no es extraño encontrarlo como ejercicio práctico y como juego en los libros de criptografía destinados a niños. No obstante, contiene ya algunos de los elementos clave en gran parte de los métodos criptográficos que han existido, que han supuesto el quebradero de cabeza de criptógrafos y criptoanalistas, y también han servido de brecha por la que se han roto y venido abajo muchos de ellos. La parte más relevante está en el hecho de que la correa, el palo, que tienen emisor y receptor debe ser exactamente igual y debe ser compartida por ambos, antes de usarse para establecer la comunicación. Si esto no fuera así y junto con el mensaje escrito el mensajero tuviera que llevar también la correa, la seguridad sería muy pobre. Es obvio que si el enemigo capturara al mensajero tendría todo lo necesario para leer el mensaje, esto es, dispondría del propio mensaje cifrado y de la correa con el grosor adecuado para verlo colocado. Por otra parte, es importante que esas dos correas sean únicas, ya que si el enemigo tuviera una tercera correa igual a las dos originales y fuera capaz de interceptar el mensaje, solo tendría que usar su propia correa para enrollar la cinta escrita y leer el texto. Veremos la importancia de estos elementos a lo largo de toda la historia, por eso es interesante que incluso en métodos tan primitivos ya estén presentes de manera clara.

La escítala, aunque muy sencilla, ya es un cifrado del texto, lo que supone un cambio enorme y radical con respecto a los métodos esteganográficos que se habían utilizado hasta entonces. Es decir, aquí no estamos ante un texto en claro que se esconde de alguna forma, en una liebre, bajo el pelo u oculto por la cera. En este caso, el texto que se transmite y que por lo tanto es susceptible de ser interceptado por el enemigo, no está en claro, sino que está cifrado. Si el que lo intercepta no tiene el conocimiento o los medios para descifrar el texto, de nada le servirá haberlo hecho. Esto es tan importante que con el paso de los siglos se ha llegado al extremo de que se envía de manera abierta el texto cifrado y no hay problema en que sea interceptado, confiando en que el método criptográfico utilizado es tan robusto que, aun con el texto cifrado en la mano, nada se puede hacer. Llegará el momento del telégrafo y las comunicaciones que podríamos denominar abiertas, donde veremos esto con todo detalle. Hasta entonces, sigamos en los siglos anteriores a Cristo.

En China se usaba en la Antigüedad un método de ocultación que, de un modo u otro, ha llegado hasta nuestros días. Tras escribir el mensaje en un retal de seda, este se envolvía en cera formando una bolita lo suficientemente pequeña como para que fuera tragada por el portador. El resto del proceso es obvio y, como decía, en la actualidad lo siguen usando los traficantes de drogas; eso sí, para ocultar sus sustancias en lugar de para ocultar información.

En la *Historia del Perú* , escrita por Diego Fernández en 1571, el autor vuelve a las ideas que leemos en Heródoto sobre cómo Histieo envió el

mensaje a Aristágoras usando como lienzo la piel de la cabeza del esclavo. En este caso americano, Diego Fernández indica que la piel del brazo de un indio puede ser un sitio perfecto para escribir un mensaje que pase desapercibido a todos. Para hacerlo visible, basta frotar la piel con carbón, tierra u otro polvo cualquiera. Este método está a caballo entre las tintas invisibles y las ideas esteganográficas más antiguas, pero es una buena muestra de la persistencia de algunas formas de hacer sencillas y que datan de hace veinticinco siglos.

Como otras tantas cosas de nuestra cultura occidental, el primer texto con instrucciones claras sobre cómo se pueden llevar a cabo comunicaciones seguras se lo debemos a los griegos. Fue Eneas el Táctico el que consagró todo un capítulo de su principal obra a este tema. La obra en cuestión es una de las primeras sobre el arte de la guerra y estaba dedicada a la poliorcética, esto es, el arte del asedio. Entre sus ideas y explicaciones sobre cómo se deben proteger las plazas fuertes durante los asedios, tenemos algunas narraciones anteriores, ya descritas por Heródoto, y otras formas básicas de ocultación de textos en las comunicaciones. Eneas explica en su texto sobre los asedios no solo cómo pueden comunicarse con seguridad en dicha situación los asediados y los posibles auxiliadores externos, sino que también habla de la defensa de la plaza, de cómo organizar las tropas, de cómo introducir armas salvando la vigilancia de las tropas sitiadoras… Sin ser un libro dedicado expresamente a la criptografía, sí que nos deja algunas ideas que han ido evolucionando y mejorando con el paso del tiempo.

Uno de esos sencillos trucos era, por ejemplo, sustituir todas las vocales de un texto por puntos, indicando con el número de puntos la vocal que se había eliminado: un punto para alfa, dos para épsilon… Es obvio que la seguridad de este método no era muy elevada, al menos a nuestros ojos, pero era un primer paso y al menos aseguraba que para un analfabeto aquello fuera un texto casi jeroglífico, y que, para alguien capaz de leer, no sirviera un vistazo rápido al texto, en un descuido, para comprender el mensaje. Hay que tener en cuenta que para reconocer un texto con estos pequeños cambios y poder leer algo así de un vistazo, al descuido, habría que ser un buen conocedor del método, ya que dos puntos pueden significar una letra repetida dos veces o tan solo una letra. Como casi todos los métodos que propone Eneas, son inseguros a los ojos de nuestro siglo XXI y también fueron inseguros hace ya muchos siglos, pero hemos de tener en cuenta que estamos hablando de las primeras fuentes, de un pionero en este campo de la escritura secreta.

Proponía, por otro lado, el uso de *astragali* , que sería el plural de astrágalo, que es la denominación de un pequeño hueso del pie. En definitiva, hablamos de una taba, ese huesecillo con el que se ha jugado precisamente desde la época de la Antigua Grecia. Además de para los juegos infantiles, las tabas también podían usarse como forma de comunicación secreta. La idea era que en una taba o astrágalo se perforaran 24 agujeros, uno por cada letra del alfabeto griego,

repartiéndolos por cuatro caras de la taba, cada una con seis hoyos. Todos ellos debían estar conectados, lo que se podría conseguir vaciando la taba por dentro. Sabiendo a qué letra corresponde cada agujero, algo que se puede conseguir marcando la primera letra de alguna forma y conociendo un orden, propone Eneas que el mensaje se construya con un hilo que vaya entrando y saliendo de los agujeros y marcando así las letras. Al deshacer el enredo, que seguro que se produciría sobre la taba a poco largo que fuera el mensaje, el receptor podría recrearlo de fin a principio y más tarde reordenarlo para tenerlo en claro. No es un método sencillo ni práctico y, por supuesto, no es útil para mensajes que vayan más allá de un nombre, una palabra o un texto muy corto. Pero no deja de ser curioso y una propuesta más que sirve de base para idear nuevas formas de cifrado. Por otra parte, un astrágalo rodeado de hilo llamaría la atención de cualquiera, pero quizás pudiera pasar inadvertido dentro de una bolsa llena de ellos.

Además de estos primitivos métodos criptográficos, Eneas explica algunos otros métodos esteganográficos. Uno de ellos ha sobrevivido durante siglos y fue utilizado por espías durante la Primera Guerra Mundial y, con algunos cambios, es la base de varios sistemas utilizados en el espionaje hasta, al menos, la mitad del siglo XX. No está mal si tenemos en cuenta que Eneas vivió en el siglo IV a. C.

Eneas proponía tomar un documento escrito con cualquier mensaje inocuo, hoy podríamos utilizar cualquier novela, y componer el mensaje secreto marcando letras del texto con un pequeño agujero o con una marca apenas perceptible. Lo ideal es que esas marcas solo sean visibles para aquel que sabe que están y, por tanto, las busca. Para conocer el mensaje, basta ir recorriendo el texto para localizar las letras e irlas apuntando en el orden en el que aparecen en el texto. El mensaje, lógicamente, se compondría uniendo todas esas letras seleccionadas. Añadía el autor como recomendación que las marcas fueran muy pequeñas, minúsculas, y que era conveniente separarlas tanto como fuera posible a lo largo del texto, para que no llamaran la atención en un primer momento a cualquier lector.

No es este el único método que propone Eneas en su libro sobre cómo sobrevivir a los asedios. Pone de ejemplo el caso de un hombre que escribió un mensaje en unas hojas, y se las ató a una herida que tenía en la pierna, como si estuvieran sanándola, para hacerlas pasar desapercibidas. Otra idea interesante es aquella en la que propone hacer con plomo pendientes con forma de aro y ocultar dentro de ellos el mensaje. Las mujeres podrían moverse libremente y es probable que el escondite del mensaje, los aros en las orejas, pasara inadvertido. En realidad, estas propuestas de Eneas no dejan de ser eso, propuestas, ya que no se tiene constancia de su puesta en práctica. Otros sistemas recomendados para ocultar mensajes escritos eran el uso de las telas, coser los textos en algunas de las piezas de una coraza o armadura de un soldado o incluso en la suela de una sandalia. Eneas también habla de tablillas, como ya había hecho Heródoto, usando yeso o algo similar para tapar el mensaje grabado en la madera.

Otra fuente y referencia clásica se la debemos a Polibio, un historiador griego nacido dos siglos antes de nuestra era. Según sus indicaciones, para codificar un texto hay que colocar todas las letras en una matriz, en una tabla, con las columnas y las filas numeradas. Una tabla de cinco filas y cinco columnas, es decir, con veinticinco posiciones, sería una base suficiente, ya que el texto sería fácilmente comprensible en cualquier caso. Es decir, si usáramos la primera celda de la tabla, fila 1 y columna 1, para la letra a y la b, al descodificar la palabra casa tendríamos dos opciones: casa y cbsb; lo que nos lleva a discernir claramente qué letra es la correcta de las dos opciones que nos encontramos en la celda.

A partir de la tabla de Polibio, cada letra podrá ser localizada en la tabla a partir de su fila y columna, como se hace habitualmente en el juego de los barcos. El texto cifrado se compondrá sustituyendo las letras del texto en claro por el par de números, fila y columna, que describe la posición de la letra en concreto dentro de la matriz. Tan sencillo como efectivo, y quizás por eso ha perdurado en el tiempo y ha sido la base conceptual de muchos otros métodos.

Hay una ventaja adicional en el método de Polibio y es su facilidad para transmitir la información a distancia, tal y como él mismo ya apuntaba en sus escritos. Al pasar todas las letras a números, se pueden enviar señales luminosas basadas en esos números, remitiendo así el texto codificado a grandes distancias sin necesidad de mensajero. Sugería Polibio usar antorchas para transmitir el mensaje, con las dos manos. El número de antorchas en una mano indicaba la fila de la letra dentro de la tabla y el número en la otra mano la columna. Esta idea de pasar letras a números para su cifrado y codificación es perenne en la criptografía y ha servido para realizar operaciones matemáticas con los textos. En un primer momento solo sumas y restas, pero con el tiempo operaciones mucho más complejas, origen de sistemas más seguros. Por tanto, esta intuición de Polibio es uno de los pilares sobre los que otros se apoyaron. Muchos han caminado sobre sus hombros.

Polibio también se apoyó en otros anteriores a él. Con sus ideas perfeccionaba el sistema que habían creado Kleoxenos y Demokleitos en Alejandría en torno al año 500 a. C., que proponía usar antorchas para enviar mensajes. El propio Polibio indica que el cifrado al que se refiere añade seguridad a la comunicación, pero también admite que a cambio requiere una aplicación y una atención rigurosa. Los alejandrinos habían ideado tiempo antes ese método de comunicación a distancia a través de antorchas, que recibe el nombre de Fryctoria, pero Polibio añadió el cifrado a la comunicación mediante antorchas.

Es cierto que este método tiene algunas debilidades que iremos viendo y que tienen que ver, principalmente, con que es vulnerable ante un simple análisis de frecuencia, pero también contiene ciertas características que han inspirado y han servido de base a criptógrafos posteriores. Como ya

hemos dicho, la criptografía es una disciplina en la que avanzar sobre los problemas y errores de otros es casi una obligación.

Aunque los textos griegos describen estas bases, no sería extraño que un conocedor de los mismos hubiera ido un paso más allá, creando un método de comunicación realmente seguro, y que ese método no nos haya llegado. El texto de Polibio indica que la tabla está ordenada siguiendo el alfabeto. Por lo tanto, si usáramos nuestro alfabeto, la letra a correspondería con la fila 1 y la columna 1, y la letra b con la fila 1 y la columna 2, y así sucesivamente. Si en lugar de usar el orden alfabético colocamos las letras aleatoriamente y esa matriz la conocen tanto emisor como receptor, la comunicación adquiere un nivel de seguridad adicional relevante y no importaría demasiado que un enemigo capturara el mensaje. Igual que ocurre con la escítala espartana, si al partir al frente un comandante se lleva consigo esa matriz de letras colocadas aleatoriamente, podría recibir mensajes desde su ciudad sin demasiado riesgo. De igual modo, en una ciudad asediada se podrían comunicar usando las antorchas que decía Polibio desde la ciudad hacia fuera, aunque el responsable del asedio viera las antorchas y capturara el mensaje. No es un método totalmente seguro, pero dados los conocimientos y prácticas del mundo clásico, se podría confiar en él.

La tinta invisible, que estará presente en repetidas ocasiones a lo largo de la historia, también aparece en las fuentes clásicas como una vía útil para ocultar un mensaje. Dicho esto, lo cierto es que sí hay registros sobre la tinta invisible, pero no hay ninguna fuente directa en la que se mencione su uso en acontecimientos históricos. La descripción más antigua de esta técnica la tenemos en la obra de Filón de Bizancio, aunque la mayoría de sus escritos se han perdido y sabemos de él de forma indirecta. Habla de tinta invisible en el contexto militar, y explica una receta en la que, mezclando nueces molidas y agua, se consigue un líquido que al secarse es invisible. Para que el texto sea visible basta con frotarlo con una esponja humedecida en vitriolo, esto es, en un ácido.

Ovidio y Décimo Magno Ausonio también mencionaron de un modo u otro las tintas invisibles, y, junto con Plinio el Viejo, recomendaban el uso de la leche como elemento natural que sirve para estos fines. Si bien este último autor habla de ello, no indica con qué fines puede usarse. En cambio, Ovidio y Ausonio sí comentan posibles usos, pero curiosamente no hablan de tintas invisibles como elemento útil para la guerra, sino que recomiendan su uso para escribir mensajes de amor que puedan ser secretos y pasar desapercibidos. En su obra *Arte de amar* , Ovidio recomienda escribir con leche fresca un mensaje sobre la espalda de una mujer leal y enviarla a visitar a la amante. El marido de esta, o cualquier otro, no verá mensaje alguno sobre la piel, que en cambio será perfectamente visible al espolvorear carboncillo encima de ella.

Hacemos un salto en el tiempo de varios siglos para ver algún ejemplo de cómo estos métodos han llegado hasta nuestros días. En la Primera Guerra Carlista, la guerra civil española librada entre los años 1833 y

1840 entre los partidarios de Carlos María Isidro de Borbón, absolutistas, y los de Isabel II y María Cristina de Borbón, liberales; algunos mensajes al más alto nivel se enviaron utilizando tintas invisibles como forma de ocultación. En concreto, la correspondencia entre los generales Cabrera y Zumalacárregui, dos de las cabezas del bando carlista, y don Carlos, como se conocía al Borbón que defendían, ocultaba mensajes importantes escritos con tintas invisibles entre las líneas del texto que estaban a la vista y que no tenían tanta relevancia. La tinta invisible que utilizaban, por cierto, era tan sencilla como zumo de limón.

En otra guerra civil española, la que se conoce de hecho como Guerra Civil española, el Servicio de Información de la Generalitat de Cataluña tenía un laboratorio donde, además de falsificar documentos, se creaban y preparaban tintas simpáticas, esto es, tintas invisibles. Esta oficina catalana fue finalmente integrada en el Servicio de Investigación Militar republicano, conocido por sus siglas, SIM. Lejos de ser, como veremos, una anécdota, hablamos de una entidad esencial e importante. Dentro de la sección química de la oficina, trabajaba Francisco Pich Ferrer, que era químico y que creó una tinta simpática especialmente buena, al parecer. Tanto es así que según el jefe del SIM del momento, los colaboradores rusos, con los que tenían una relación estrecha, les solicitaron cantidades enormes de aquella tinta invisible para su propio uso.

Siguiendo con ejemplos cercanos en el tiempo, en 1908 se utilizó este tipo de sustancias para comprobar la autenticidad de determinados documentos. Dentro de las comunicaciones seguras, es vital saber que el documento que tenemos entre las manos procede del emisor del que pensamos que procede. De otra forma, sin esta certeza, podemos ser engañados fácilmente. Bien, pues a comienzos del siglo XX, como decíamos, se utilizaron las tintas invisibles para certificar documentos, incluyendo contraseñas o marcas en documentos importantes, como contratos, cheques, títulos… A un falsificador o copista ilegal podría pasársele por alto ese detalle a la hora de hacer su trabajo y así el receptor podría diferenciar si lo que tenía entre las manos era auténtico o no.

Incluso en la Segunda Guerra Mundial, donde las técnicas de cifrado habían llegado a niveles de seguridad y rigor muy elevados, seguían siendo útiles en algunos casos los viejos y sencillos trucos de las tintas invisibles. Walter Giese, un espía alemán que operó en España durante la guerra, fue interrogado en 1945 en Berlín y declaró que utilizaba una mezcla de ácido cítrico y alcohol para escribir sus mensajes y así ocultarlos a la vista de cualquiera. Giese también habló de un método usado en España durante aquel tiempo, en el que solo se utilizaba agua. Se tomaban dos hojas de papel idénticas, relató el espía alemán, y una de ellas se sumergía completamente en agua. A continuación, sobre una superficie lisa, como un cristal, se colocaba la hoja empapada y encima de esta la hoja seca. Se escribía el mensaje sobre la hoja seca, tomando la precaución de hacerlo con grandes letras mayúsculas, ya que de otro

modo el mensaje no sería fácil de leer. Hecho esto, la hoja mojada se ponía entre papel absorbente y se prensaba, para lo que era suficiente una pila de libros. Se iba cambiando el papel absorbente hasta que la hoja que había estado totalmente empapada en agua quedaba seca. Entonces se hacía llegar al destinatario y este tan solo tenía que meter esa hoja en agua de nuevo para que el mensaje apareciera lo suficiente como para ser leído.

Este salto temporal es sencillamente una muestra de cómo la esteganografía, en su versión más sencilla e intuitiva, ha sobrevivido durante siglos. Más adelante veremos nuevos usos y apariciones de estas técnicas en la historia, de igual forma que veremos cómo la idea básica de la matriz de Polibio aparece una y otra vez.

Si bien en los textos griegos hay descripciones de métodos de codificación y de ocultación de información, no hay casos reales relevantes en los que se consigne su uso, en batallas o comunicaciones entre gobernantes, por citar situaciones en las que se esperaría su presencia. En Roma, en cambio, sí tenemos ejemplos y, en algunos casos, la criptografía estuvo presente en eventos muy relevantes para el devenir de su historia.

En cualquier texto de criptografía, incluso en las introducciones más simples dedicadas a los niños, aparece el popular cifrado de Julio César. Esto se debe a varios motivos. Por una parte, por la propia relevancia de Julio César y, por otra, por la sencillez del método, lo que hace que sea fácilmente comprensible y puesto en práctica por cualquiera, incluso un niño.

Cayo Julio César nació en el año 100 a. C. y su vida se movió entre la guerra y la política. Los éxitos en la primera eran un buen camino para avanzar en la segunda, en la vida política. La expansión de la República de Roma a través de las conquistas era un pasaporte al reconocimiento y al poder. A medida que el territorio se ampliaba, cada vez era más complicado mantener el control y el poder desde las propias instituciones romanas y eran los generales sobre el terreno los que tenían casi pleno poder. Sila, Pompeyo o Julio César son ejemplos de militares que utilizaron su reputación como tales para hacerse con grandes parcelas de poder. Apoyados en la lealtad de sus ejércitos, ansiaban el poder y no dudaron en usar la violencia, incluso la guerra civil, para alcanzarlo.

Las guerras eran grandes oportunidades y Julio César tuvo una de las suyas en la Galia, un territorio que actualmente ocupan Francia, Bélgica y Suiza. En el año 60 a. C. tan solo una parte del sur de la Galia estaba bajo dominio romano. Ese territorio se incluía en una provincia romana, y de ahí viene su nombre popular: Provenza. En ese año 60 a. C. Cayo Julio César había creado una alianza con Pompeyo y Marco Licinio Craso, conocida como el Primer Triunvirato, y un año más tarde fue nombrado cónsul y utilizó su poder e influencia para ser nombrado

gobernador y general de la Galia, donde su objetivo fue claro, conseguir nuevos territorios para Roma.

Durante nueve años, entre el 58 y el 49 a. C., conquistó la Galia hasta el Rin, sofocó las revueltas locales y rechazó las invasiones externas. Incluso realizó expediciones a Britania. La derrota de Vercingetórix y el asedio de Alesia en el año 52 a. C. acabaron por elevar su reputación al máximo, por colocarlo ante sus ejércitos como un mito. Reunió la suficiente confianza como para dar un siguiente paso en su búsqueda del poder.

Aquel gran proyecto militar fue escrito y descrito por el propio Julio César en una obra cuyo título era *Comentarios sobre la guerra de las Galias* (*De bello Gallico*). Esta fuente nos deja información sobre los hechos, añade detalles sobre la vida cotidiana en el ejército y describe cómo combatir, organizar y dirigir la guerra. También aborda la forma de enviar mensajes de manera segura.

Algunas de esas formas de comunicación son básicas, como la que describe en el libro V, donde habla del intercambio de cartas entre Cicerón, asediado, y César. Las cartas del primero eran capturadas por el enemigo, ya que todos los mensajeros eran descubiertos y hechos prisioneros al estar tomados y controlados todos los caminos que rodeaban a Cicerón. En algunos casos, los mensajeros romanos eran cogidos tan cerca del asedio que los mataban a fuerza de tormentos y a la vista de los asediados. En esta desesperada situación, Cicerón pudo hacer llegar un mensaje a César usando una técnica similar a las que hemos visto y que se habían llevado a cabo siglos atrás.

El romano tomó a un desertor de los galos llamado Verticón, que se había pasado a su bando y se había ganado su confianza, y escondió el mensaje que quería sacar del asedio dentro de la lanza de este. El galo fue capaz de salir del asedio y atravesar las zonas controladas por el enemigo sin levantar sospechas, como galo que era. Al final, el mensaje llegó a César, que, recibida la petición de ayuda, se dispuso a responder. Reunió las fuerzas que tenía dispersas por la región y se acercó a territorio nervio, una de las tribus del norte de la Galia. Cuando sus espías le informaron detalladamente de la crítica situación en la que se encontraba Cicerón, César persuadió a un jinete para que llevase un mensaje al asediado. Como precaución para mantener seguro el mensaje en caso de que cayera en manos enemigas, el líder romano lo escribió en griego. No sabemos si César escribió el mensaje usando el griego, o si escribió el texto en latín y tan solo sustituyó cada letra del mensaje en latín por su equivalente en griego. No tiene mayor relevancia histórica, pero sí la tiene desde el punto de vista criptográfico. En un caso hablaríamos de un cambio de idioma, y en otro caso de un cambio en el alfabeto; esto último, algo mucho más común en la criptografía.

Si el mensajero tenía éxito, Cicerón entendería el mensaje en griego sin problemas; y, en caso contrario, si era capturado y el mensaje caía en

manos enemigas, no pondría en peligro a las tropas de César ni revelaría su situación, fuerzas e intenciones. Como vemos, los viejos métodos seguían siendo útiles y cualquier idea o método era bueno siempre que asegurase que el mensaje en claro no era revelado en caso de ser capturado.

Podemos pensar que algo tan sencillo tenía sentido tan solo en tiempos antiguos, contra bárbaros y hombres poco formados. Pero los británicos intentaron siglos después algo similar, utilizando el latín como lengua de comunicación. Sin mucho éxito, como veremos. Y en el siglo XX, en la Segunda Guerra Mundial, los estadounidenses utilizaron esta misma idea base con muy buenos resultados al integrar a indios navajos en las unidades de combate y encargarles la comunicación en su propio idioma navajo. Que los enemigos, los japoneses principalmente, estuvieran escuchando los mensajes de radio no era problema, ya que no entendían nada del idioma navajo, igual que los guerreros galos no conocían el griego en tiempos de César y Cicerón.

Volviendo al asedio de Cicerón, si no le era posible al jinete llegar hasta él, como era de prever, le había pedido César que atara el mensaje a una flecha y la lanzara dentro del campamento asediado. La precaución se descubrió como cierta y los últimos metros de distancia entre las manos de César y las de Cicerón las recorrió la carta atada al palo de una flecha, que se clavó en un cubo al caer en el campamento. No dice César en su escrito si cayó dentro o fuera del cubo, pero, dado que se tardó tres días en descubrir la flecha, bien podemos suponer que cayó dentro. Al final, con retraso, llegó a las manos de Cicerón el mensaje en griego que le decía que resistiera un poco más, que las legiones estaban en camino para romper el asedio y rescatarle. Tanto era así, que desde el campamento se veían a lo lejos las humaredas de lo que ahora sabían que eran legiones romanas que venían en su ayuda.

No han sido estos métodos esteganográficos y de cifrado básico los que han inscrito el nombre de César en la historia de la criptografía. Viendo que el gran militar romano ya tenía interiorizada la importancia de las comunicaciones seguras en campaña, y seguro que también en las intrigas de la vida política, no es de extrañar que trabajara en el desarrollo de un sistema al respecto. Utilizar el griego en sus batallas entre romanos, por ejemplo, no sería garantía de nada y por ello diseñó y pensó cómo comunicarse de manera segura. Tanto es así, que Marco Valerio Probo escribió un tratado dedicado a los códigos de César, aunque lamentablemente se perdió y no ha llegado hasta nosotros.

Le debemos a Suetonio, el historiador que vivió a caballo entre el siglo I y II y autor de *Vida de los doce césares* , el conocimiento del cifrado de Julio César, ya que fue él quien nos dejó escrito cómo este enviaba cartas al ya mencionado Cicerón y a otros romanos, utilizando un método sencillo pero efectivo. Lo que hacía César era sustituir, por eso este es un método de sustitución, cada letra por la que estaba en el abecedario tres posiciones hacia adelante. Aplicado este método sobre nuestro alfabeto, la letra A pasaría a ser la D, la B se sustituiría por la

E, y así sucesivamente hasta llegar a la Z que sería la C en el texto codificado.

En la actualidad se ha denominado cifrado o código César a cualquier método o sistema que funcione de esta forma, sea cual sea el desplazamiento a lo largo del alfabeto, tres posiciones, como en el inicio, o cualquier otra cifra. Cuenta Suetonio cómo Octavio Augusto, hijo adoptivo de Julio César, utilizaba este mismo método, si bien reducía el desplazamiento a una sola posición.

Este rudimentario y sencillo procedimiento de César, la cifra de sustitución básica, está en la base de muchos de los métodos criptográficos de la historia, y la complejidad y seguridad, como veremos, reside en no hacer las mismas sustituciones siempre, es decir, que la A sea unas veces en el texto cifrado una D y otras una E. Hacer impredecibles esas sustituciones es mejorar los métodos criptográficos.

3. Los criptoanalistas árabes

Las revelaciones que tuvo Mahoma durante su vida adulta, desde aproximadamente los cuarenta años hasta su muerte en 632, son claves en el islam. Según la tradición de esa religión, en el año 610, mientras Mahoma meditaba en la cueva de Hira, a poco más de tres kilómetros de La Meca, el arcángel Gabriel le reveló que era el mensajero de Dios. Desde aquel día, Mahoma trataba de memorizar y transmitir los versos y los mandatos que Dios le hacía ver. Los adeptos a ese islam incipiente escuchaban e intentaban retener en sus cabezas todas esas enseñanzas. Varios de ellos las anotaron, pero solo consiguieron componer una colección de pequeños extractos, ya que cada uno recordaba y anotaba lo que le parecía o podía dejar para la posteridad.

Abú Bakr, el primer califa del islam, que fue contemporáneo de Mahoma y que solo vivió dos años más que él, se propuso recopilar todas las sentencias que había dispersas y que suponían las revelaciones del profeta. El Corán es el libro que saldría de aquel proyecto de recopilación de las enseñanzas de Mahoma, y la labor fue compleja, ya que el conocimiento estaba repartido por ese grupo de seguidores iniciales. El trabajo de Abú Bakr fue continuado por Umar y por Utmán, segundo y tercer califa, respectivamente. Así se compuso el Corán, que en sus 114 capítulos presenta las revelaciones que se hicieron a través de Mahoma.

El islam se extendió rápidamente y ya en el siglo VIII vivía una edad dorada en la que había muchos sabios y hombres de ciencia estudiando todo lo relacionado con esta religión, además de gobernantes que dominaban una gran extensión de terreno. Cuando murió Mahoma en el año 632, la Península Arábiga ya era islámica, pero a mediados del siglo siguiente la parte meridional de Asia Central, el norte de África y la Península Ibérica tenían líderes islámicos al frente. La prosperidad y el conocimiento dieron lugar a muchos avances de todo tipo. Entre otros, se hizo común el uso de las codificaciones y los cifrados para comunicarse de manera segura. Tan general era el uso de la criptografía que incluso los funcionarios la utilizaban para proteger determinados archivos y notas que consideraban importantes y, en cierto modo, confidenciales. En el mundo islámico existen manuales del siglo X sobre cómo debían ejercerse los trabajos administrativos públicos, que incluyen secciones dedicadas a la codificación de datos para mantenerlos ocultos a ojos de terceros y para guardarlos de forma segura. Apartados enteros dedicados a la criptografía.

Los árabes de aquel tiempo usaban la cifra de sustitución monoalfabética, donde a cada letra del alfabeto en el que está escrito el texto en claro se le asigna una letra o símbolo diferente. Para calcular ese texto cifrado, se toma cada letra del texto en claro y se sustituye por el símbolo que tiene asignado, que no siempre es una letra, sino que

puede ser cualquier tipo de símbolo. A estas alturas de la historia, en el siglo VIII, lo cierto es que esto no supone una gran contribución a la evolución de la criptografía, ya que son métodos conocidos y utilizados en el pasado. En cambio, donde sí fueron revolucionarios los criptógrafos islámicos fue en el mundo del criptoanálisis, en el trabajo de desentrañar y romper los métodos de cifrados de otros para conocer el texto en claro a partir del texto cifrado.

Era de esperar que desde el momento en que se empezó a utilizar algún método criptográfico para ocultar información, aparecieran los intentos de romper esos métodos, esos códigos, y conocer así los textos que se pretendían ocultar. Dicho esto, es en este momento donde nacen los trabajos sistemáticos y profundos para romper los textos codificados por métodos basados en el conocimiento y la lógica. Por supuesto, cuando hablamos de criptoanálisis no estamos pensando en capturar a un mensajero o persona que sabe la clave y torturarle o sobornarle para que revele la clave o el método de cifrado y se pueda entonces conocer el texto en claro. Los criptoanalistas tienen como cometido encontrar métodos analíticos que, a partir del texto cifrado, permitan deducir y conocer el texto en claro.

Nace aquí, por tanto, la carrera que se ha mantenido hasta nuestros días, en la que los criptógrafos se enfrentan a los criptoanalistas. Los primeros inventan y desarrollan formas de ocultar textos y de comunicarse de forma segura, y los segundos buscan debilidades y fisuras en esos códigos, cifras y sistemas criptográficos para hacer que incumplan su cometido y por lo tanto se puedan conocer los textos en claro y romper la seguridad de las comunicaciones. Nace entonces un mundo apasionante donde el conocimiento es el centro y los secretos son el elemento más preciado. Uno de los secretos más valiosos, como veremos en innumerables casos a lo largo de la historia, aparece cuando se rompe un sistema criptográfico, para mantener esa capacidad de leer las comunicaciones del otro.

Romper el sistema criptográfico del enemigo, que este sea consciente de algún modo de ello y que por lo tanto se vea obligado a cambiarlo y no pueda utilizarlo más, es una ventaja. Pero romper el sistema criptográfico del enemigo sin que este lo sepa coloca al que lo ha roto en una posición todavía más ventajosa, ya que se enfrentará a alguien que actúa como si sus comunicaciones fueran seguras y, por lo tanto, no tendrá reparos en intercambiar y enviar información. Esa información irá directa a las manos de su enemigo. Estas situaciones han sido muy comunes en la carrera entre criptógrafos y criptoanalistas, en la que los éxitos en la ruptura de los códigos y las cifras se han de mantener en secreto para no matar a la gallina de los huevos de oro, esa fuente de información. Cuando un país, un gobernante, un ejército… sabe o sospecha que sus comunicaciones a través de una determinada vía no son seguras, abandona esa vía, y aunque el que ha provocado la situación mejora, no puede sacar la ventaja total de leer el correo del enemigo.

Volviendo al origen del criptoanálisis, los árabes fueron capaces de desentrañar cómo descifrar el propio método que ellos usaban, la sustitución monoalfabética, que hasta aquel momento era un método sólido, seguro y se consideraba fiable. Como decíamos, la sociedad árabe tenía un conocimiento elevado, para su época, de un buen número de disciplinas, entre las que estaban la lingüística y las matemáticas. Y dentro de esta última, la estadística. Las escuelas teológicas eran fundamentales en una sociedad donde la religión era un pilar. En estas escuelas se estudiaba el Corán en profundidad y desde todos los puntos de vista. Siendo el resumen de las revelaciones de Dios a través de Mahoma, cualquier detalle o aspecto que pudiera aportarse sería recibido como un avance. Además, el origen del texto, como hemos visto, tiene un componente de recopilación que contribuía a darle un espíritu de libro en construcción, en estudio.

Para reunir las revelaciones se habían tomado varias fuentes y el resultado final no respondía a un orden concreto o una cronología marcada. Mahoma había estado transmitiendo las revelaciones durante años, y aunque estaban todas en el Corán, no se conocía en qué momento las había ido revelando. Ante este problema, algunos teólogos tuvieron la idea de estudiar las palabras que aparecían en los diferentes capítulos del texto para buscar alguna evolución en las utilizadas en cada caso y así ser capaces de determinar el orden en que Mahoma enunció las distintas partes. Este razonamiento tiene mucha lógica, ya que la forma de hablar de cualquiera de nosotros y las expresiones que utilizamos cambian con el tiempo. Así, estudiando en detalle las palabras y su uso, se podría determinar la época de cada relevación y por lo tanto ordenar el Corán, al menos en cierta medida. Los teólogos también tenían acceso a otros textos de Mahoma, que eran una fuente muy valiosa para llevar a cabo ese análisis de la forma de expresarse del profeta y de sus palabras más comunes en cada momento de su vida.

A este trabajo se entregaron en profundidad, analizando las palabras y las expresiones en detalle. Pero fueron un paso más allá y estudiaron también las letras de cada frase y de cada capítulo. Al hacer esto último, el análisis de las letras, comprobaron que no todas son igual de corrientes en un lenguaje. Esto es algo que, por otra parte, todos sabemos por puro sentido común. Es obvio que la letra a o la letra e son mucho más comunes que la letra z, en el idioma castellano, por ejemplo. Lo que hicieron los teólogos árabes fue poner números a cada letra, cuantificar esta diferencia de frecuencia de las letras en los textos, y caer en la cuenta de que esos números son tan distintos que son relevantes.

Lamentablemente no se tiene constancia del primer hombre que aplicó el criptoanálisis para romper una codificación, pero ese estudio del Corán llevó a un descubrimiento clave en el mundo de la criptografía: el análisis de la frecuencia de las letras. La fuente más antigua donde se describe esta técnica data del siglo IX y se la debemos a Al Kindi. Este filósofo se interesó por muchas disciplinas, desde las matemáticas hasta la astrología, y trabajó en la traducción al árabe de textos de científicos

y sabios clásicos como Aristóteles. Nacido en torno al año 800, fue director de un lugar denominado la Casa de la Sabiduría, en Bagdad, donde se estudiaban y se traducían todo tipo de textos, además de servir de biblioteca, como es lógico. En su origen fue tan solo eso, una biblioteca fundada por el califa, y con el tiempo fue creciendo hasta convertirse en algo mucho más ambicioso, una institución pública de estudio y formación. La Casa de la Sabiduría tuvo entre sus miembros a Ibn al-Haytham, también conocido como Alhacén, pionero del método científico y uno de los hombres de ciencia más importantes de la Edad Media. Incluso se dice de él que es el más importante de ellos entre Arquímedes y Newton. Otro miembro destacado fue el matemático Al-Jwārizmī, o Al-Juarismi, que dejó escrito el importante tratado *Compendio de cálculo por compleción y comparación* , en árabe: *Al-Kitāb al-mukhtas.ar fī h.isāb al-ŷabr wa-l-muqābala* . Esta obra vio la luz a comienzos del siglo IX en lengua árabe, y en ella se exponen algunos elementos clave del álgebra, como son la resolución de ecuaciones. Cuando fue traducido al latín e introducido en el mundo cristiano, dio lugar a varias palabras que desde entonces forman parte de nuestro lenguaje y que nacieron por la derivación directa de las palabras árabes del título y el nombre del autor. La primera de ellas es álgebra, que proviene directamente del al-ŷabr del título del libro. También la palabra algoritmo, omnipresente en el mundo de la computación durante décadas y que hoy ha saltado ya al lenguaje común, proviene del nombre de Al-Juarismi. En resumen, la Casa de la Sabiduría era un centro de máxima importancia científica.

Al-Kindi escribió centenares de obras, como se puede saber por algún catálogo del siglo X, pero lamentablemente la mayoría de ellas se han perdido. La filosofía era uno de sus temas predilectos y de ella no se podía separar en aquel tiempo la teología, por lo que el estudio de los textos sagrados desde todos los puntos de vista era una labor obligatoria a sus ojos. Ese estudio del lenguaje se adentró en el campo de la criptografía y Al-Kindi publicó a mediados de ese siglo IX un tratado sobre el desciframiento de mensajes criptográficos. Este documento histórico estuvo perdido durante siglos, hasta que en 1987 un investigador libanés, Muhammad Mrayati, lo encontró en el archivo Sulaimaniyyah de Estambul. Probablemente, el interés del filósofo árabe por la ruptura de códigos y cifras se debiera a que algunos de los textos que quería leer y estudiar estaban cifrados. El análisis de la frecuencia de las letras en cada lenguaje, que ya conocían los árabes, era una puerta de entrada a esos textos codificados.

A la luz de estos documentos árabes, parece claro que cinco siglos antes de que en el occidente europeo se conociera el análisis de frecuencia como método de ataque contra las cifras y los códigos, los árabes, al menos en algunos lugares, ya conocían y aplicaban estas técnicas.

La descripción que se hace en esos textos del criptoanálisis es sencilla, como sencilla es esta técnica de ataque de mensajes cifrados. Según el texto de Al-Kindi, había que examinar todas y cada una de las letras de una lengua y ver las que se repiten con mayor frecuencia en su uso

corriente, para clasificarlas en grupos. A continuación, se hace lo mismo con las letras o símbolos del texto cifrado, sustituyendo unas por otras con base en las equivalencias en la frecuencia de aparición. Como es obvio, cuanto mayor sea la longitud del texto codificado o cuanto mayor sea el número de textos codificados que tengamos a nuestra disposición, más exacto y fiable será el cálculo de las frecuencias y por lo tanto más efectivo el proceso. Esta técnica tan sencilla y accesible fue el camino que siguió un gran número de criptoanalistas a lo largo de la historia para analizar y romper códigos y, por lo tanto, para cambiar la propia historia.

Con textos suficientemente largos, las equivalencias son más clarificadoras. Es decir, si la letra A en castellano supone el 12,5 por ciento de un texto y siempre se sustituye en el texto cifrado por el símbolo #, por ejemplo, la frecuencia de ese símbolo en el texto cifrado será igualmente del 12,5 por ciento, o cercana a él. Tan sencillo como eso. Incluso cuando el texto no es largo, aparecen unas letras más frecuentemente que otras y eso permitirá al criptoanalista hacer hipótesis e ir probando. Por ejemplo, la E tiene una frecuencia de 13,7 por ciento, aproximadamente, en el idioma castellano. Si nos encontramos en un texto cifrado con la palabra C#S#, donde las letras C y S ya han sido descubiertas y el símbolo # tiene una frecuencia en el cifrado el 13,1 por ciento, podríamos tener dos opciones: # podría ser la A o la E, que tienen frecuencias similares. Ninguna otra letra en castellano, por cierto, sobrepasa el 10 por ciento de frecuencia. Así, podríamos tener la palabra CESE o la palabra CASA, y ambas son válidas en el lenguaje. En la mayoría de los casos, solo por el contexto, podríamos saber la palabra que encaja en el texto cifrado, pero si no fuera así, tan solo habría que buscar otra palabra en el texto cifrado con el símbolo # y ver el resultado con A y con E. Este es el tipo de hipótesis y pruebas que van haciendo los criptoanalistas en su paciente trabajo. Si el texto es largo o son muchos textos los que se han capturado, la equivalencia matemática es casi suficiente para encontrar el texto en claro.

Durante gran parte de la Edad Media occidental no hubo importantes innovaciones, y el uso que se hacía de la criptografía era sencillo y no muy alejado de lo que ya se había hecho en los siglos anteriores. Escribir en vertical, hacia atrás e intentos similares de hacer imposible la lectura eran las técnicas utilizadas. Además de utilizar los métodos clásicos, por ejemplo tomar las letras de otros alfabetos como el griego, sustituir vocales por secuencias de puntos o utilizar el cifrado de César. Lo más avanzado está en el uso de signos como sustitutos de letras. Lo cierto es que entre el año 500 y el 1400, por colocarnos en fechas destacadas, no hubo grandes avances en la criptografía.

Como era de esperar, ya que en esta época el grueso de la cultura estaba en manos eclesiásticas, fueron las figuras religiosas las que hicieron un uso más común de la criptografía. El papa Silvestre II, que lo fue entre 999 y 1003, por ejemplo, ya era reconocido como un gran erudito, teólogo y filósofo antes de llegar a lo más alto de la Iglesia,

cuando todavía era Gerberto de Aurillac. Esto se debería esperar de casi cualquier hombre merecedor de la fumata blanca, pero lo que no es tan común es la afición de Gerberto de Aurillac por las matemáticas. No en vano, se le conoce como el papa matemático. Sus ideas ayudaron a crear el reloj de péndulo, estudió las órbitas planetarias y escribió sobre geometría. Desarrolló el ábaco de manera importante y daba relevancia a la ciencia, llegando a afirmar que el hombre justo vive por la fe, pero es bueno que tenga que conjugar la ciencia con su fe. Un pensamiento revolucionario para los años finales del primer milenio, que, por supuesto, le colocó frente a algunas críticas y problemas. Pero más allá de todo esto, Silvestre II sustituyó los números romanos por los árabes (1, 2, 3… hasta 9), algo que desde su posición de Papa generaba casi una obligación de cambio en los clérigos europeos y, por lo tanto, acabaría llegando a toda la sociedad. Esto supuso un hito en la historia de las matemáticas occidentales y además facilitó que ciertas operaciones y cálculos, para los que hasta entonces hacía falta un conocimiento profundo, salieran del minúsculo círculo donde tan solo algunos expertos eran capaces de llevarlas a cabo.

En el ámbito que nos ocupa, la criptografía, Silvestre II utilizaba para sus notas un primitivo sistema taquigráfico inspirado en los romanos, concretamente en Marco Tulio Tirón, secretario de Marco Tulio Cicerón, y por eso las denominaba notas tironianas. Este sencillo sistema sustituía algunas sílabas por símbolos y signos, lo que tenía dos ventajas. Por una parte, el texto quedaba cifrado al momento, y por otra, el Papa así era capaz de escribir más rápido. Llegó al extremo de dejar su nombre escrito en dos de sus bulas con esta técnica.

Otro importante personaje de la Edad Media que dejó su pequeña muesca en la historia de la criptografía fue Hildegarda de Bingen, una abadesa nacida en 1098 y que, en 2012, más de 800 años después de su muerte en 1179, fue reconocida como doctora de la Iglesia. Otra mente inquieta y polifacética que, entre sus muchos intereses, contó con los números y la criptografía. Hildegarda de Bingen utilizaba un alfabeto para cifrar, que le había sido revelado en un momento de inspiración, según ella misma afirmaba. Como vemos, las técnicas de los criptógrafos de esta época no eran muy distintas de las clásicas, y su uso más habitual correspondía a la Iglesia.

De igual modo que, como hemos visto, el estudio de sus textos religiosos llevó a los árabes a adentrarse en la criptografía, los monjes cristianos de la Edad Media se enfrentaron a algunos textos del Antiguo Testamento donde estaba presente. El caso más destacado es el del Atbash, una forma de codificación de la tradición hebrea. El Atbash es un método de sustitución muy sencillo, donde cada letra se reemplaza por aquella que está a tantas posiciones del final del alfabeto como está del principio la letra original. En castellano, por ejemplo, la A es la primera letra y por lo tanto está a cero posiciones del inicio del alfabeto. En consecuencia, se sustituiría por la letra que está a cero posiciones del final del alfabeto, esto es, la Z. La B se sustituiría por la Y, y así sucesivamente. El propio nombre de esta técnica, Atbash, se inspira en

el método. La primera letra del alfabeto hebrero, aleph (A), es seguida por la última, tav (T), esta por la segunda, beth (B), que, tras una A, es seguida por sh, que provendría de shin, la penúltima letra del alfabeto. De este modo tenemos Atbash.

No es extraño, por tanto, que el Atbash se conozca también como el método del espejo. Uno de los casos en los que se utiliza en el Antiguo Testamento es en el Libro de Jeremías, donde para no nombrar directamente a Babilonia, o lo que es lo mismo, Babel, se escribe su nombre hebreo codificado mediante Atbash.

Estamos ante un método sencillo y no muy seguro, pero, aun así, casos como este hicieron que algunos de los religiosos que se dedicaban al estudio de las antiguas escrituras descubrieran la criptografía y se interesaran por ella. Roger Bacon fue el autor del primer libro europeo de la Edad Media en el que se habla de la criptografía directamente. Fue en el siglo XIII y su título era *Epístola sobre las obras de arte secretas y la nulidad de la magia* . Además de describir siete métodos para ocultar los mensajes, Bacon abogaba de manera directa y clara por el secreto, afirmando que tan solo un loco escribe un secreto de forma que no lo oculte al vulgo. Entre los métodos propuestos por Bacon, que no difieren mucho entre sí unos de otros, todo sea dicho, hay uno que se ha utilizado puntualmente en los últimos tiempos, aunque sencillamente por motivos de estilo. Es la eliminación de todas las vocales, la composición de las palabras únicamente con las consonantes.

Greoffrey Chaucer, famoso por ser el autor de *Los cuentos de Canterbury* , que falleció en 1400, dedicó tiempo a la astronomía y a la alquimia, entre otras temáticas. Entre sus obras está una descubierta más de cinco siglos después de su muerte, en 1952, y que se titula *Equation of the Planets* . En ella aparece parte de su *Tratado del astrolabio* , dedicado a este instrumento de medición de las posiciones y de los movimientos de los cuerpos celestes, y escrito en torno al año 1392. Además de estos temas, Chaucer dejó seis pasajes breves escritos en cifra, usando un alfabeto de símbolos, para sustituir algunas letras del texto por estos símbolos. Estos ejemplos y casos, Chaucer, Bacon, Hildegarda de Bingen o Silvestre II, nos muestran la limitada capacidad de la criptografía en la Edad Media, y de ahí podemos deducir los usos que se le daba.

4. Los nomenclátores

En los primeros años del Renacimiento, las ciudades del norte y el centro de Italia se configuraban como verdaderos centros de poder que luchaban de manera abierta en combates y enfrentamientos discontinuos, y luchaban también de manera oculta, a través de alianzas, intrigas, diplomacia y política. Milán, Florencia, Venecia… eran piezas importantes en la Península Itálica, pero además tenían un peso relevante en el escenario europeo, donde competían con el Estado Pontificio, la corona francesa, Nápoles y la corona de Aragón, entre otros.

La red diplomática de embajadores que conectaba todas las naciones, necesitaba, como es obvio, comunicarse de forma segura, principalmente con su propio estado. Se conocían bien ya por este tiempo todos los sistemas criptográficos que habían existido en el pasado, especialmente los métodos de sustitución, en gran medida porque estos eran muy sencillos de comprender y utilizar y, por lo tanto, muy prácticos para el uso en el día a día. Esa sencillez tenía una contrapartida crítica, como ya hemos comentado, eran fácilmente atacables a través del análisis de frecuencias. Los italianos conocían estas técnicas de criptoanálisis y no es de extrañar que también estuviera en su afán fortalecer sus propios métodos criptográficos, a lo que dedicaban algunos esfuerzos.

El análisis de frecuencia se basa, como se ha visto, en el hecho de que cada letra tiene una determinada frecuencia de aparición en un idioma. Dado que esa información de un idioma es una debilidad, los criptógrafos tenían que buscar cómo solventarla. La solución estaba en un planteamiento sencillo. Las letras más frecuentes en un idioma debían sustituirse de manera alternativa por varias letras o símbolos. El análisis de frecuencia deja de ser efectivo contra un texto cifrado de ese modo. Si la A unas veces se sustituye por la B y otras por la Z, la frecuencia de la A en el idioma, pongamos un 12,5 por ciento, se repartirá entre la B y la Z, que tendrán en torno a un 6 y un 7 por ciento de frecuencia, por lo que ya no se puede hacer la equivalencia entre la B del texto cifrado y la A del texto en claro, ya que las frecuencias no son coincidentes. La forma de aplicar esto era el siguiente paso. Había que buscar un método sencillo y efectivo de cifrado que presentase esta característica. Para ello hubo varias soluciones.

Por ejemplo, supongamos que utilizamos el método de Polibio que ya conocemos y que coloca las letras en una matriz y las identifica por su fila y columna. Si la matriz es de 10 × 10, por ejemplo, podríamos colocar la a en varias celdas de la matriz para así representarla de varias formas. De este modo, no sería posible deshacer la codificación basándose en las frecuencias, ya que la frecuencia de la letra a, las veces que aparece, está repartida entre varios pares de números y por

lo tanto no hay forma de identificar la correspondencia. Lo ideal sería que todos los símbolos o letras del texto cifrado tengan frecuencias parecidas, diluyendo así las diferencias del idioma real. Esta forma de sustitución se conoce como sustitución homofónica, donde a una letra del texto en claro le corresponden varias en el cifrado.

Se tiene constancia por primera vez de esta sustitución homofónica en el arranque del siglo XV, en 1401, en la correspondencia entre el duque de Mantua y Simeone de Crema. Habían acordado ambos las equivalencias de letras para generar el texto codificado, y en esas equivalencias había algunos números y símbolos, que no eran propiamente letras del alfabeto, y que aumentaban el número de elementos en el alfabeto de codificación. Ese extra de símbolos les permitía asignar a las letras más comunes varias posibilidades, repartiendo así las frecuencias altas en varias más bajas y similares al resto.

Este método de cifrado, no obstante, tampoco es resistente a los criptoanalistas, si bien como primer paso fue un avance considerable. Los criptoanalistas elaboraban hipótesis e iban descubriendo el texto, probando opciones. Sabiendo, por ejemplo, que lo que tenemos ante nosotros es la correspondencia que el duque de Mantua envió a Simeone de Crema, podemos suponer que la palabra Mantua aparecerá en varias ocasiones. De las letras que componen Mantua, la a se habrá sustituido por dos símbolos distintos, pero no así el resto. Por lo tanto, buscando esos patrones donde en el texto cifrado cambian tan solo las posiciones segunda y sexta de una palabra, las correspondientes a la a de la palabra Mantua, y el resto coinciden, podremos suponer que estamos ante la codificación de la palabra que buscamos y así determinar un buen número de equivalencias, incluso para las letras que tienen varias opciones de sustitución.

Para evitar este tipo de problemas, se pusieron en marcha en el siglo XVI los conocidos como nomenclátor o nomencladores, que, además del alfabeto cifrado, contenían una serie de palabras comunes codificadas. Se abría así un camino que he llegado hasta el siglo XX, donde se mezclan los cifrados de cierta parte del texto con los códigos en los que se sustituyen palabras o expresiones enteras por un símbolo o por otra palabra. Conceptualmente, un nomenclátor es similar a un diccionario, donde al lado de cada palabra, en lugar de su definición o equivalencia en otro idioma, encontramos qué palabra, símbolo o números la deben sustituir.

En ocasiones, ni siquiera se usaba método de cifrado alguno y lo único que se utilizaba era un nomenclátor en el que se sustituían las palabras o expresiones más importantes, dejando el resto del texto en claro. Ni que decir tiene que la seguridad de esta medida no es demasiada. Estas palabras presentes en el nomenclátor, cuando aparecían en el texto en claro, no eran codificadas sustituyendo cada letra por su equivalencia en el cifrado, sino que toda la palabra se sustituía con arreglo a ese código. Así, siguiendo con el ejemplo del duque de Mantua, su nomenclátor habría definido una palabra en clave para Mantua, de

igual modo que lo hubiera hecho para otras localidades como Florencia, Roma y Venecia y para palabras clave como ataque, repliegue o defensa. Esto complicaría la tarea de los criptoanalistas, pero lo cierto es que los buenos criptoanalistas fueron capaces de romper este tipo de codificaciones, incluso cuando se incluían, quizás a propósito, errores gramaticales y caracteres nulos, que no significaban nada en realidad.

El secretario del papa Clemente VII, Gabriel de Lavinde, a finales del siglo XIV, fue el primero en plantear esta idea de los nomenclátores. Para asegurar la correspondencia del Papa, el secretario creó una lista de palabras que debían ser sustituidas por un determinado símbolo. También incluyó en su planteamiento criptográfico símbolos nulos, es decir, símbolos que no tenían significado alguno y que debían ser descartados al descifrar el texto. Podríamos considerarlos como basura o ruido dentro del mensaje, una idea ocurrente destinada a complicar el proceso de análisis del texto codificado. El objetivo de ambas tretas era impedir el criptoanálisis por frecuencia, como bien sabemos. Desde este primer uso y hasta el siglo XIX, el nomenclátor fue el elemento central de los sistemas de codificación utilizados por los gobiernos y diplomáticos. Como veremos, estas listas de palabras a sustituir por uno o varios símbolos, estos diccionarios, crecieron con el paso del tiempo y llegaron a ser catálogos de miles de palabras, donde cada una de ellas se sustituía por un símbolo, por otra palabra o por una secuencia de números, siendo esto último finalmente lo más común.

La seguridad de los nomenclátores depende del número de palabras, bigramas, grupos de dos letras, o trigramas, grupos de tres letras, que tengan sustitución dentro del mismo. Si las palabras clave que se cambian son unas pocas, será sencillo para el criptoanalista descubrirlas, pues lo hará casi por puro sentido común. Si el número de equivalencias es elevado y, además, como propuso Gabriel de Lavinde, se incluyen símbolos nulos en el texto, la seguridad puede ser más que razonable. Por supuesto, el peligro del nomenclátor está en que el enemigo, o el tercero, tenga acceso a ese catálogo de sustituciones, al propio nomenclátor. Incluso el acceso al texto cifrado y al texto en claro permite conocer las equivalencias establecidas y por lo tanto el sistema pierde toda su seguridad. En cualquiera de los casos, ante la mínima sospecha de que conoce el nomenclátor quien no debe, todos los códigos han de ser desechados y se habrán de generar nuevos símbolos o números para cada palabra.

Es decir, como las equivalencias entre las palabras y los símbolos o secuencias de números son fijas y no dependen de clave alguna, una vez que esa equivalencia es conocida, de nada sirve la pretendida ocultación de información del nomenclátor. Lo que un criptoanalista descubre un día, en este caso, le sirve para futuros mensajes capturados, por lo que el tiempo y el uso actúan en contra de la seguridad de los nomenclátores. Por otra parte, distribuir el nomenclátor entre las partes es un proceso que también entraña riesgos. En ocasiones, incluso la simple observación de los acontecimientos ha ayudado a detectar alguna sustitución, alguna palabra en el nomenclátor.

Los nomenclátores no tardaron mucho en incorporar homófonos, es decir, varias sustituciones para una misma letra o palabra. Así, con el paso del tiempo esos libros de códigos se fueron haciendo más extensos y más complejos. Los primeros usos se hicieron en Italia en el siglo XV, y siguiendo las ideas de Lavinde, secretario del Papa, ya en el siglo XVI era habitual que todos los nomenclátores tuvieran homófonos y elementos nulos y que fueran usados de manera ubicua.

La captura de los textos cifrados del enemigo o del que se quiera espiar es una labor necesaria, porque son la fuente con la que trabajan los criptoanalistas, su alimento. Y lo cierto es que, en contra de lo que pudiera parecer, es relativamente sencillo hacerse con el correo de las personas gracias a los sobornos, a los descuidos, al ingenio o incluso a las acciones de fuerza. Esto ha ocurrido durante toda la historia, pero a medida que se creaban redes de comunicación con cierta regularidad, la facilidad para romper ese secreto del correo era cada vez mayor. En España, tan pronto como en 1513 ya se daban las primeras instrucciones para que no se interceptara la correspondencia privada de nadie, fuera de manera directa o indirecta. En 1521 esta orden se hacía extensible a las Indias, y las penas por violar ese secreto del correo, un concepto que aún hoy genera controversia, eran importantes. Uno podía perder su trabajo, si era posible aplicar tal castigo porque su empleador fuera el gobierno o algo similar, podía ser desterrado e incluso mandado a galeras, además de sufrir penas físicas como los azotes. Ni que decir tiene que, a pesar de estas leyes y castigos, el correo se capturaba y eran los propios gobernantes los primeros en hacerlo.

Los despachos que enviaban desde las Indias personas con poder, con destino al Consejo de Indias, se clasificaban según el nivel de seguridad o confidencialidad asociado. Así, había mensajes clasificados como confidenciales, que solían ser enviados por los altos funcionarios, conteniendo información de cierta relevancia o importancia. Los siguientes eran los envíos marcados como reservados, que llevaban información militar, diplomática o, en cualquier caso, información delicada. En muchos casos bastaba tan solo esa marca de información reservada para que el envío llegara sin abrirse hasta las mismas manos del rey, a pesar de pasar por muchas otras. Por último, había mensajes secretos, que, lógicamente, no eran muy habituales. En estos casos, de una manera u otra, el rey estaba involucrado en el propio envío, en lo que se decía en el mismo. Aunque esta clasificación se utilizaba para intercambiar correo entre las Indias y el Consejo de Indias, es lógico pensar que esta forma de actuar se aplicaba también con otros lugares y en otros ámbitos de la corona española.

En las comunicaciones con las Indias, es obvio que no se confiaba demasiado en las leyes y las amenazas de castigo, porque como precaución se cifraban los mensajes. Y no solo se buscaba la seguridad con el cifrado de las cartas y con las leyes que prohibían la inviolabilidad del correo, sino que también se aplicaba lo que podríamos denominar la seguridad física, al menos a la antigua usanza. Los despachos importantes se envolvían doblemente, se introducían las

cartas en cajones precintados y sobre estos se indicaba el destinatario. Para aumentar la seguridad y tener un registro de las comunicaciones que había en marcha entre un lado y el otro del Atlántico, y conocer las que se habían perdido, en caso de que ocurriera, se llevaba un registro detallado y duplicado de todo lo enviado. El registro de la correspondencia que llegaba desde las Indias se enviaba por duplicado al Consejo de Indias y a la Casa de Contratación de Sevilla. Esta es una muestra más de cómo se buscaba la seguridad en las comunicaciones, una seguridad que en la base debería estar sustentada por la criptografía, por el cifrado. De nuevo, esta forma de actuar, que está documentada para el caso del correo con las Indias, nos apunta cómo debía actuarse en el caso de otros destinos. Y todo esto se hacía, lógicamente, porque se sabía que los enemigos del Imperio español estaban ávidos de esas cartas cifradas, como el Imperio lo estaba de las cartas de otros, para que sus criptoanalistas las analizaran y pusieran en claro la información que transportaban.

Es interesante comprobar cómo en la segunda mitad del siglo XVI, con Felipe II ya en el trono y con cifras y medidas mucho más serias y robustas ya implantadas en el Imperio español, en los territorios más cercanos, las comunicaciones con América seguían utilizando cifrados débiles. Esta dejadez con la seguridad tenía varios motivos. Uno era la propia distancia, que hacía complejo coordinar los intercambios de claves y conseguir que todos los implicados estuvieran al tanto de los cambios, pero también podría ser que se confiara en una solución de último momento, cuando se viera en peligro un envío de correspondencia en alta mar. Bastaría con arrojar al mar esos cajones de cartas de los que hablábamos para evitar que el correo cayera en manos enemigas. Esta orden estaba en las mentes de los capitanes de las flotas y los barcos: frente al riesgo de ser capturada, la correspondencia debía lanzarse al océano, debidamente lastrada para que se fuera al fondo rápido y sin riesgos. Esta forma de actuar, tan radical, se ha utilizado durante siglos, como veremos cuando hablemos de la Segunda Guerra Mundial, en la que naves y submarinos tenían orden de deshacerse por este método tan directo de todo el material criptográfico para evitar que cayera en manos enemigas.

En el problema español con las Indias tenemos otro de los aspectos clave que han determinado el uso de la criptografía, sus problemas y debilidades. El intercambio de claves, la puesta en común entre las partes del cifrado o el intercambio y distribución de libros de códigos, como veremos, es un problema logístico que se ha tratado de solucionar de un modo u otro a lo largo de los siglos y que, a menudo, ha sido un importante quebradero de cabeza.

Como bien sabemos, no se puede negar que la misma corona que generó estas normas y esas leyes que consideraban la correspondencia algo personal y secreto, no tuvo problemas en violarlas cuando había sospechas de que se estaba conspirando contra ella, en otros casos similares o incluso por propio interés, sin más. Se llegó al punto no solo de intervenir las comunicaciones, sino de aplicar directamente la

censura prohibiendo hablar de determinados temas y haciendo, por lo tanto, que el correo vigilado que tratara algunos de ellos no llegara nunca a su destino, ya que era interceptado y destruido.

Algo parecido ocurre en la Iglesia, en la que, a pesar de ser uno de los centros clave de la criptografía en el siglo XVI, tanto en su uso como en su desarrollo, no se veía con buenos ojos que otros la utilizaran. Una carta cifrada, y por lo tanto *a priori* secreta, podría tratar de cualquier cosa, política o religiosa, y como era de esperar, una Iglesia con poder e intereses tanto en la vida pública como en la privada, tenía ahí una importante barrera. Por ello, amenazó con la excomunión a aquellos que cifraran sus comunicaciones. De nuevo, diciendo una cosa y haciendo la contraria, los criptógrafos y criptoanalistas de Roma destacaron en esta época. Los primeros para cifrar las comunicaciones vaticanas, y los segundos, los criptoanalistas, para romper las cifras de otros.

En octubre de 1546 el rey de Francia, Francisco I, prohibía oficialmente que se escribieran cartas o tan solo notas usando algún tipo de cifra. Incluso prohibía el uso de nombres supuestos y formas de ocultación similares. Esto último, con toda seguridad, era difícil de controlar, pero como en otros muchos casos, no es la norma la forma de evitar que algo ocurra, sino que la norma está pensada y descrita para poder aplicar un castigo cuando se demuestre que alguien la ha incumplido. El rey francés dejaba fuera de esta obligación a los embajadores del papado, a los reyes y a los grandes príncipes y hombres poderosos de su época. A pesar de ello, Carlos V y Francisco I también compitieron en este ámbito, y se acusaban mutuamente de usar cifrados para enviar cartas que el otro había interceptado.

Como vemos, durante el siglo XVI todos los gobiernos europeos sabían que debían proteger sus mensajes, y así lo hacían, y trataban por todos los medios de impedir que otros lo hicieran. Una cosa y otra son contrarias y lo que ponen de manifiesto es que todos sabían que sus cartas eran capturadas y copiadas, y por eso las cifraban. Ellos buscaban de igual modo capturar y descifrar, salvo en el caso de los ingenuos que hacían caso a la ley y no cifraban las cartas, en cuyo caso el correo se capturaba también, pero le ahorraban a su enemigo, o medio amigo, el tener que descifrar el texto.

En los reinos de la Península Ibérica en la Alta Edad Media hay casos de uso de criptografía bien documentados, aunque los métodos utilizados son muy simples y casi podríamos decir que poco útiles en cuanto a su seguridad. Cambiar vocales por secuencias de puntos o sustituir algunas letras por otros símbolos, eran formas habituales de intentar ocultar el texto. Varios siglos después, a finales del XIV y comienzos del XV, aparecen algunos intentos de protonomenclátor, como el de la condesa de Urgel, que en su correspondencia se refería al señor de las abejas en lugar del Papa, a la flor mayor de los egipcios en lugar del rey de Francia y al león de la gran aventura en vez de príncipe de Inglaterra. A comienzos de ese mismo siglo XV ya aparece el primer nomenclátor real

en la corte del rey Carlos III de Navarra. Tenía caracteres nulos y términos relacionados con el mundo militar, y sustitutos para identificar a personajes importantes sobre los que hablaba en su correspondencia. La corona de Aragón también utilizaba este tipo de soluciones de codificación, aunque sencillas. A mediados del siglo XV la correspondencia entre Alfonso V de Aragón, el Magnánimo, y el rey de Francia, Carlos VII, de nuevo muestra el uso de un breve nomenclátor.

A finales del siglo XV, debido a la extensión e importancia que alcanzó la diplomacia y por lo tanto enfrentados los gobernantes a una cada vez mayor necesidad de comunicaciones secretas, la criptografía se estableció como una necesidad y un elemento más dentro del día a día de los reyes y de los nobles europeos, entre ellos los españoles.

Una de las formas en las que se ha ido avanzando en el estudio de la historia de la criptografía ha sido aplicando las técnicas y conocimientos modernos, más evolucionados que a las cifras y métodos de encriptación utilizados en los siglos pasados. De esta forma se averiguan cifras, claves y formas de codificar que fueron utilizadas siglos atrás. Esto es lo que hizo el historiador prusiano Gustav Adolf Bergenroth en el siglo XIX con muchas de las cartas de los archivos españoles. Unas veinte cifras usadas en el siglo XV y sucesivos en España fueron puestas en claro por Bergenroth, lo que nos permite hoy comprobar cómo los Reyes Católicos, por ejemplo, trataban de mantener sus secretos. Los archivos siguen guardando cartas cifradas y documentos codificados, que en algunos casos podemos analizar y descifrar sin mucho esfuerzo.

Una lección importante que nos dejó Bergenroth es que el ser humano, la persona que hay detrás de la codificación, es un elemento más a tener en cuenta, habitualmente como debilidad del método de encriptación. Bergenroth reconoció que en sus ataques contra los métodos usados por la corona española de los siglos XV, XVI y XVII, la forma de escribir de las propias personas encargadas de cifrar era una ayuda para su trabajo de criptoanálisis. Por ejemplo, el nomenclátor usado por el duque de Estrada fue desentrañado gracias a que el escribiente ponía siempre un punto detrás de dos determinados signos del texto cifrado. Estudiando la manera de escribir del duque de Estrada y siguiendo un razonamiento lógico, en el que descartó otras posibilidades, Bergenroth fue capaz de comprobar que esos puntos indicaban las sustituciones a textos como V. A., que venía a significar Vuestra Alteza. El duque sustituía la V y la A por otras letras, pero su costumbre mental, o sencillamente porque iba copiando metódicamente del texto en claro y sustituyendo las letras que correspondían, pero dejando otros caracteres, le llevaban a dejar los puntos en el texto cifrado y dar así pistas a los criptoanalistas.

No es trivial este detalle, ya que el factor humano es una fuente más de información en la criptografía. Además de los muchos errores y debilidades que la pereza o la costumbre de los usuarios de los métodos criptográficos han generado a lo largo de la historia, en ocasiones el

rastro de la persona que generaba el mensaje era información útil. Su costumbre de usar determinadas palabras o construcciones era una punta del hilo en manos de los criptoanalistas para deshacer la madeja del texto cifrado. Y es que como apuntaba el propio Bergenroth, el criptoanalista no solo bucea en las palabras, las letras, los símbolos y los números del texto cifrado, sino también en el conocimiento del contexto, los hombres envueltos en la comunicación o la sospecha de determinadas intenciones en el mensaje, que le hacen generar hipótesis que sirven de punto de partida en su labor.

Hay que tener en cuenta que a partir del siglo XIV algunas de las coronas y gobiernos europeos comenzaron a disponer de personal experto y dedicado a la criptografía. No eran tan solo diplomáticos o nobles que además tenían ciertos conocimientos sobre el tema, como había ocurrido antes, sino que se trataba de verdaderos expertos dedicados a ello en exclusiva. En nuestros días una persona que se dedica profesionalmente a traducir sabe en qué idioma fue escrito originalmente el texto que tiene entre manos, aunque esté ante una versión ya traducida, y es capaz de intuir cuál es el idioma nativo de un escritor tan solo por el tipo de estructuras gramaticales que utiliza, aunque esté escribiendo en otro idioma diferente al nativo. De igual modo, un criptoanalista experto era capaz de ver en cierta media el texto en claro que ocultaba lo que tenía entre manos y generar hipótesis de trabajo que le llevaran a descubrir poco a poco el mensaje real. De nuevo hablamos de generar hipótesis, y es que el método científico podría servir para describir el trabajo meticuloso, paciente y constante de los que se enfrentaban a un texto cifrado. Generando ideas, probándolas para ver hasta dónde les llevaban, repitiendo ese proceso una y otra vez, en ocasiones sin éxito, aunque descartando opciones, y otras con éxito y colocando así una pieza en el puzle que deshace el texto cifrado.

En conclusión, conocer a la persona que está detrás del mensaje cifrado es una fuente más de información. En ocasiones, tan solo para saber si el mensaje capturado proviene de un lugar o de otro, lo que ya es un punto de comienzo. Por otra parte, si bien en las últimas décadas los textos están impresos por máquinas y es más complicado saber quién está escribiendo realmente el mensaje, durante siglos la forma de escribir, la caligrafía, delataba al escribiente, también al emisor en la mayoría de los casos, y esa era una fuente valiosa. No eran tantos los que escribían en una corte o en el círculo de un noble, por lo que después de un tiempo, no es extraño que se fueran conociendo las caligrafías y manías de cada uno.

Aunque suponga un salto temporal en el hilo del texto, porque ya llegará el momento en el que hablemos de telegrafía y del código morse, es interesante aquí detenernos en una anécdota sucedida en pleno siglo XX que reafirma esta idea sobre el rastro que deja el emisor, la persona real que hay detrás del propio texto y la importancia de ese detalle.

En el siglo XX, como decíamos, cuando un nuevo espía era aceptado en una red, por lo general, había un periodo en el que este era entrenado o bien puesto a prueba en sus comunicaciones y revelaciones. Durante este tiempo los receptores de los mensajes enviados por radio por los espías se acostumbraban y detectaban su ritmo de tecleo o su toque al enviar las comunicaciones por morse. Así, la velocidad a la que emitía cada espía era ligeramente distinta y durante meses y meses esta característica se tomaba como un detalle más en la comunicación. El receptor y el espía, ambos del mismo bando, se conocían por la forma de emitir. Tanto es así que en muchos casos se empleaban horas de práctica entre emisor y receptor con el único objeto de conocer ese toque del espía, esa forma de teclear en morse. Más tarde, cuando el espía estaba al otro lado de las líneas enemigas, el receptor era capaz de identificarlo por cómo tecleaba e incluso saber si estaba tranquilo, acelerado o si no era él realmente. Esto en ocasiones podía ser tan importante como el uso de armas, explosivos, microcámaras o las técnicas de evasión y encubrimiento.

Hay muchos casos en los que este detalle ha sido una razón de sospecha o confirmación. A veces el cambio en el ritmo por parte del espía causó el descarte erróneo de un mensaje, pero otras sirvió como aviso de que el mensaje no debía ser tenido en cuenta. Por esta razón, entre otras, cuando un espía era capturado y los captores querían enviar un mensaje de engaño, se le hacía transmitirlo al propio espía, aun a riesgo de que cambiara el ritmo para alertar de su captura, y no se ponía a otro emisor a usar los aparatos de envío, ya que esto lo delataría al instante. Así ocurrió con el espía del Mossad Elie Cohen. Espió durante años en los países árabes para el servicio secreto israelí, hasta que en 1965 fue descubierto y detenido. Los agentes sirios que lo capturaron le obligaron a enviar un mensaje cifrado a Tel Aviv para engañar a los israelíes. Cohen varió su toque, su forma de emitir, y así el Mossad supo inmediatamente que su agente en Damasco había caído. Por supuesto, los sirios también dedujeron que Cohen había utilizado esta treta y descartaron el intento de engaño. Finalmente, unos cuatro meses después de este hecho, Cohen fue ahorcado por los sirios, a pesar de los intentos de canje por parte de Israel. Por cierto, un exceso de confianza de Cohen, probablemente, fue la causa de su detención. La regularidad con la que hacía sus emisiones levantó sospechas en el ejército sirio y la inteligencia soviética se ocupó de localizar y detener a Cohen.

Esto es una muestra clara que de la persona que escribe, cifra o envía un mensaje incorpora sin querer información al propio mensaje. Información que puede ser tenida en cuenta por el criptoanalista para atacar el método de cifrado. Cuando, en los siglos XV o XVI solo un puñado de hombres cifraba, sus manías y formas eran una debilidad, como aquel V. A. del duque de Estrada.

Volviendo a la criptografía de la corona española del siglo XV, Miguel Pérez de Almazán fue un aragonés que ostentó varios cargos en la corte de los Reyes Católicos, donde tuvo mucho peso, siendo uno de los secretarios más importantes de los reyes. En muchos aspectos su labor

podría equipararse a lo que hoy correspondería a un ministro de Exteriores. Sin ir más lejos, fue el firmante el 31 de marzo de 1492 de la Real Provisión que ordenaba la expulsión de los judíos de los reinos de Castilla y que fue enviada a todas y cada una de las ciudades principales, a las ciudades menores y a muchas villas y señoríos, con orden estricta de no abrirse y leerse dicha comunicación hasta el primer día de mayo de aquel año.

Se presume que fue él quien impulsó la criptografía en la corte católica en la década de 1480, aunque ya hay constancia en los archivos de usos de cifras en la década anterior. El nombre de Pérez de Almazán aparece de manera habitual y casi constante en toda la correspondencia entre la corte y los más importantes personajes, desde el Gran Capitán a los gobernantes de otros países. No había tema en el que no estuviera enredado, desde la gestión de los matrimonios de conveniencia de la familia real, hasta la solución de problemas como la sublevación de las Alpujarras. Incluso estuvo mezclado en asuntos inquisitoriales.

A finales de 1487, Rodrigo González de la Puebla, jurista que provenía de familia de conversos, como también era el caso de Pérez de Almazán, fue enviado como embajador de los Reyes Católicos en la corte inglesa. El principal encargo que llevaba sobre sus hombros era negociar el matrimonio de la infanta Catalina con el heredero inglés, Arturo Tudor, que era príncipe de Gales e hijo primogénito de Enrique VII de Inglaterra. Durante el año siguiente se cruzaron varias cartas entre las costas inglesa y española para unir las dos cortes e ir así acordando los términos del enlace matrimonial. El método utilizado para hacer más seguro el contenido de la correspondencia no era muy avanzado, pero se estimaba suficiente para librar a los mensajes de los curiosos y de los posibles traidores. Al fin y al cabo, el viaje desde la isla inglesa hasta la Península Ibérica no era ni corto ni sencillo y había riesgo de que las cartas se perdieran o cayeran en manos poco amigas. Los españoles utilizaban un sencillo nomenclátor en el que palabras y expresiones como Fernando, Isabel, rey de Inglaterra, rey de Francia, rey de Portugal, alianza, matrimonio, guerra, hijo, se sustituían por una cifra, escrita en números romanos. Los libros de codificación, con el listado de equivalencias entre números y texto, crecieron con el paso del tiempo y cada vez se iban incorporando más y más palabras, algunas tan comunes como bueno, sí, no, meses, pérdidas, ahora, mar, pero… Con la incorporación de tantos cambios de palabras por códigos, el texto codificado al final se convertía ciertamente en incomprensible para cualquiera que no supiera las equivalencias. Para hacerse una idea basta saber que el texto «Las tropas del rey llegarán por mar en socorro de Granada» quedaría en algo como: «DCCCCXXXIX IIIC de XVI llegarán MDCCXCIIII MCCCCLXXXVIII en CXIV de CII».

No siempre se cifraba todo el texto, y era habitual que algunas palabras aparecieran codificadas entre un texto en claro. Esto, lógicamente, era una gran desventaja desde el punto de vista de la seguridad, ya que dejaba una importante información en manos de cualquier criptoanalista, ofreciéndole el contexto de las palabras ocultas. Por

ejemplo, en 1491 la reina Isabel la Católica enviaba a Rodrigo de la Puebla, que se encontraba en Londres, el siguiente texto: «Considerando si la ciudad de 102 debe ser 90 o 39 90, estamos construyendo una 188 allí —en Santa Fe—, en las que esperamos reunir buenas 97 y todo lo necesario para 94 102 o, al menos, para tenerla tan estrechamente cercada que 39 sea necesario 94 de nuevo».

En este texto 102 era Granada, 90 significaba conquistada, 39 no… Con unas pocas cartas interceptadas y analizando los acontecimientos anteriores y posteriores a la carta, este tipo de cifrados acaban por ser rotos con cierta facilidad. Según Bergenroth, al que antes aludíamos, a partir de 1495 comenzaría a solventarse este error.

A pesar de todo, no es extraño encontrarse en la correspondencia de los embajadores y hombres de la corte católica números de codificación por encima del 2.000, lo que nos lleva a deducir que el número de palabras y expresiones que no eran consignadas claramente en las cartas, sino escritas de forma codificada, excede ese umbral. Este método, hecho con las herramientas y conocimientos del siglo XV, complicaba sobremanera la escritura de las cartas, o su codificación, así como su descodificación. Piensen en buscar cada palabra en un largo diccionario de equivalencias, una a una, cuando ese diccionario tiene más de 2.000 entradas. Más adelante veremos cómo los franceses, siglos después, solucionaron este problema, en parte, con un doble índice. Esa complejidad de uso conllevó algunos problemas y errores, por lo que en ocasiones se pedía a los embajadores que prescindieran del cifrado, sacrificando así la seguridad del mensaje en beneficio de una mejor comprensión del mismo. En los archivos hay documentos cifrados donde se dejaron escritas por el receptor cosas como «sin sentido», «pedir otro despacho» o «no se entiende», que son consecuencia de la complejidad del descifrado.

Entre América y la corte en Europa también las cifras eran importantes, como hemos comentado. De hecho, Cristóbal Colón ya utilizaba los nomenclátores para comunicarse. En agosto del año 1500, el recién llegado gobernador de Santo Domingo, Francisco de Bobadilla, se enfrentó a una complicada situación. Había sido designado por los Reyes Católicos en mayo de 1499 como juez pesquisidor y gobernador de las Indias en sustitución del propio Cristóbal Colón. Sobre este último pesaban quejas por su forma de administrar, que no contentaba ni a los colonos ni a los nativos. Se encontró el nuevo gobernador con que gran parte de los españoles, dirigidos por Francisco Roldán, se habían rebelado contra los hermanos Colón. Bobadilla detuvo a estos últimos y los envió de vuelta a Castilla, presos. Junto con ellos el gobernador remitía varias cartas de Cristóbal Colón dirigidas a su hermano y que habían sido cifradas. En ellas el descubridor prevenía y aconsejaba a su hermano armarse contra el nuevo gobernador. Como vemos, la criptografía había extendido su presencia más allá de gobiernos y embajadas, y aunque no fueran métodos muy seguros, la idea de su utilidad se había extendido.

5. La conjura de Babington

En 1509 Enrique VIII fue nombrado rey de Inglaterra y señor de Irlanda, al morir su padre, Enrique VII, que había sido el primero de la dinastía Tudor. Se cumplía sin problemas aquello de «el rey ha muerto, viva el rey», que en la versión inglesa es en realidad «el rey ha muerto, larga vida al rey», lo que es distinto, aunque el sentido de la sentencia sea el mismo. Enrique VIII se casó seis veces a lo largo de su vida y en ese lío amoroso arranca la historia que muestra las posibilidades de engaño y el poder que concede a un bando conocer las codificaciones o los métodos criptográficos que usa aquel a quien se enfrenta.

En un primer momento Enrique VIII no estaba destinado a ser el rey, ya que su hermano mayor, llamado Arturo, era el primogénito y por lo tanto el sucesor. Tanto es así que se había preparado su matrimonio con Catalina de Aragón, hija de los Reyes Católicos, para consolidar las alianzas entre ambos reinados. Recuerden las cartas cifradas de Rodrigo de la Puebla, embajador de los Reyes Católicos ante los ingleses, negociando este enlace. El matrimonio tuvo lugar en noviembre de 1501, y en abril del año siguiente el heredero del trono inglés fallecía, dejando viuda a la que entonces era la princesa de Gales. El lugar de Arturo en la sucesión fue ocupado por su hermano Enrique, y no solo se quedó con el puesto para heredar el trono, sino que también acabó desposando a la que había sido la mujer de su hermano Arturo. Esto tuvo lugar en 1509, cuando ella tenía veintitrés años y él estaba a punto de llegar a los dieciocho. La alianza entre Aragón y los Tudor volvía a crearse así, a través del matrimonio, después de que la Santa Sede, con Julio II al frente, declarara nulo el enlace de la aragonesa con el fallecido Arturo Tudor, por no haber llegado a consumarse, según la propia viuda.

Catalina de Aragón no había abandonado las islas británicas en el tiempo transcurrido entre un matrimonio y el otro. De la unión con Enrique VIII dio a luz en seis ocasiones, aunque el destino de las seis criaturas fue poco favorable. Tres de ellas fueron mortinatas o vivieron apenas unas horas, una alcanzó tan solo la semana de vida y otra no llegó a los dos meses. La excepción a tan triste regla fue una niña, la única que de toda esta prole alcanzó la edad adulta. Era María Tudor, que acabaría siendo reina de Inglaterra en 1553. Este cúmulo de desgracias en torno a la descendencia, llevó a Enrique VIII a plantearse romper su matrimonio y buscar otra esposa que le diera algún hijo varón al que llamar príncipe de Gales. En este contexto hizo aparición Ana Bolena, una noble inglesa de la que Enrique VIII se enamoró.

En 1527 el rey de Inglaterra pedía al papa Clemente VII la anulación de su matrimonio con Catalina de Aragón. El argumento se basaba en el parentesco que les había unido antes de casarse, pero el Papa fue contrario a la anulación, como también lo fue Carlos V, que tenía cierta

influencia sobre la Santa Sede. Aquel conflicto llevó a la ruptura de los ingleses con la Iglesia de Roma, a que Enrique VIII fuera declarado jefe de la Iglesia de Inglaterra en 1531, a la anulación del matrimonio en 1533 y, por supuesto, llevó a Ana Bolena al trono de Inglaterra. A partir de aquí la religión fue el motivo de la guerra y la justificación de todo tipo de enfrentamientos.

En noviembre de 1542 las tropas de Enrique VIII vencieron a los escoceses en la batalla de Solway Moss, cerca de la frontera angloescocesa. El rey escocés Jacobo V se había negado a romper con la Iglesia católica, como le había pedido su tío el rey inglés, y acabó pagando con una derrota el enfrentamiento. Con una derrota y casi con su vida, ya que, aunque no estuvo presente en la batalla debido a su debilidad y a su enfermedad, las noticias que le llegaron del desenlace de la misma le afectaron profundamente. Tanto es así que dos semanas después, falleció, con treinta y tres años de edad y con una hija recién nacida a la que llamarían María y que era la heredera al trono de Escocia. Cuando la niña tenía nueve meses de edad fue coronada, continuando así con la presencia de la casa Estuardo en el trono escocés.

Enrique VIII dejó entonces Escocia fuera de sus movimientos bélicos, y comenzó a planear el acercamiento de María a sus intereses. Según sus planes, casar a la niña escocesa con un hijo suyo, haría que Inglaterra y Escocia se unieran bajo el reinado de la casa Tudor. Enrique liberó a algunos nobles escoceses y trató de utilizarlos en su favor, convenciéndoles de las ventajas del matrimonio que planeaba. María de Guisa, la madre de la niña reina, ejercía como regente y había dos motivos que la ponían en contra de Enrique VIII y sus planes: era católica y era francesa. Los nobles escoceses se pusieron del lado de la regente y no del rey inglés, lo que desembocó en la preparación de la boda entre la reina escocesa María y el delfín de Francia, Francisco, afianzando así la unión entre Escocia y Francia, algo que ya se había hecho con la boda de María de Guisa y el fallecido Jacobo V.

Enrique VIII no se daba por vencido y aumentó sus presiones diplomáticas y su intimidación sobre Escocia con actos de sabotaje y razias. Ni la muerte del rey inglés en 1547 acabó con el enfrentamiento, ya que su hijo, el nuevo rey Eduardo VI, continuó con él. Este Eduardo era el joven que, de haberse cumplido los planes de su padre, se habría desposado con la joven reina escocesa. El punto final llegó en la batalla de Pinkie Cleugh, en septiembre de ese mismo 1547, donde los escoceses fueron vencidos de nuevo. María se vio obligada a poner rumbo a Francia para salvarse.

Diez años después de aquel viaje se casó por fin con Francisco, el delfín francés, y cuando este se convirtió en el rey Francisco II de Francia, María podía decir que era la reina de Escocia y la reina de Francia. Esto ocurrió en 1559 y un año después el joven rey fallecía, lo que causó que la reina escocesa volviera a su tierra. Allí se casó con su primo, Enrique Estuardo, y comenzó un declive político que acabó con el

asesinato del rey consorte, que dejaba tras de sí un hijo, llamado Jacobo como su abuelo. María seguía siendo católica, pero sus nobles cada vez estaban más distanciados de ella. Su siguiente matrimonio no mejoró las cosas y acabó prisionera de sus propios súbditos. Encontró la salida a la situación en la renuncia al trono en favor de su hijo, que sería Jacobo VI de Escocia, y que tenía entonces menos de un año de edad.

María no se daba por vencida y escapó de su prisión, reunió un ejército y trató de ganarse el retorno a la corona por la fuerza, pero perdió en el campo de batalla. Desesperada y rodeada, huyó hacia el sur, esperando que la reina Isabel I de Inglaterra le ofreciera protección. En realidad, había escapado de una prisión para ser derrotada en batalla y acabar en otra prisión. El problema no era sencillo. María era católica y podría tener ciertos derechos al trono de Inglaterra gracias a su abuela y a la hermana mayor de Enrique VIII, Margarita Tudor. La línea de sucesión de María Estuardo al trono inglés no era muy clara, pero eso no importaba a los católicos ingleses, que estaban en contra de su reina, Isabel I, principalmente porque esta era fruto de un matrimonio ilegítimo a sus católicos ojos, como era el de Enrique VIII y Ana Bolena, hecho a espaldas del Papa.

Era 1568 y a María Estuardo le esperaban años de confortables prisiones para reinas, pero prisiones al fin y al cabo, aunque fueran castillos y casas nobles. No era una mala vida la que llevaba, pero no tenía libertad y seguía cautiva de sus enemigos ingleses. El hijo, Jacobo VI de Escocia, no sentía mucho afecto por su madre y nunca hizo demasiado por ella, temeroso quizás de que liberarla y llevarla a Escocia la colocaría cerca del trono y le restaría a él libertad de acción.

Como vemos, fueron décadas de luchas de poder, nada más y nada menos que por el trono inglés y por el trono escocés. Una guerra que arrastraba, como hemos contado, muchas afrentas y hechos del pasado, muchos intereses y que se personalizaba en María Estuardo. El punto final a esta historia tiene a la criptografía como protagonista, como elemento esencial.

Pocas esperanzas le quedaban a la reina escocesa, después de dieciocho años, de cambiar su situación de prisionera. Además, estaba aislada, ya que todas las cartas que enviaba eran confiscadas y nunca le entregaban la correspondencia que llevaba su nombre en el lugar del destinatario. Esto cambió el 6 de enero de 1586, cuando por fin pusieron en sus manos todo un paquete de cartas. Eran misivas que le habían escrito a lo largo del tiempo desde diferentes lugares de Europa, mostrándole su comprensión y apoyo. Partidarios no le faltaban fuera de su cárcel de oro. Aquella colección de cartas se había acumulado en la embajada francesa en Londres y Gilbert Gifford, un inglés que acababa de volver a su país después de pasar años en Roma, se ofreció a los partidarios franceses de María para hacérselas llegar. La embajada francesa había retenido todo el correo porque sabía que era confiscado y leído por los captores y que nunca llegaba a María, y ahora tenía la posibilidad de cambiar esa falta de comunicación.

Gifford aseguró a los franceses que él sería capaz de introducir el correo en Chartley Hall, donde la dama escocesa estaba prisionera, y de entregarlo a su destinataria original. Aquel paquete de correspondencia de enero de 1586 fue tan solo el primero de otros muchos. La vía de comunicación que se abrió fue bidireccional, ya que Gifford también era capaz de sacar de Chartley Hall el correo de María. El curioso caballo de Troya que se usaba para hacer entrar y salir la correspondencia era un barril de cerveza. El tapón del barril era hueco, y ahí se escondían las cartas, tanto para introducirlas como para extraerlas. El cervecero local las escondía en el tapón y llevaba el barril a Chartley Hall. Uno de los sirvientes de María en su encarcelamiento sacaba las cartas del tapón, una vez que el barril estaba en el edificio, y se las entregaba. No es muy diferente este método de otros casos de esteganografía que vimos en la Antigüedad. María Estuardo tenía muchos más partidarios de los que esperaba antes de comenzar a leer sus cartas, en gran medida gracias a ser la dama católica frente a la Iglesia de Inglaterra. Tanto es así que, en Londres, sus partidarios más audaces estaban conspirando para rescatarla.

A la cabeza de dicha conspiración estaba Anthony Babington, un noble inglés que, aunque públicamente se mostraba como protestante, era católico. La religión real que profesaba toda su familia, el catolicismo, había traído muchas desgracias, incluso la muerte de alguno de sus miembros combatiendo a Enrique VIII. Eso había hecho que Babington tuviera un odio enorme a Isabel I y todo lo que representaba. El plan de venganza que diseñó incluía no solo liberar a María Estuardo, sino también asesinar a Isabel I y además lanzar una rebelión en Inglaterra apoyada desde los países enemigos del trono isabelino. Aquella conspiración contra el trono inglés ha pasado a la historia con el nombre de su impulsor: Babington.

Gifford, que se había convertido en el cartero de María Estuardo, se presentó un día ante Babington y le entregó una carta de la reina escocesa. Esta le decía que le habían llegado rumores a través de sus partidarios sobre los movimientos de Babington contra Isabel I y a favor de la propia María, por lo que estaba deseando tener noticias suyas. La respuesta del conspirador no tardó en ser redactada y enviada a María Estuardo por el método habitual del tapón del barril. Babington detallaba sus planes para liberar a María y explícitamente hablaba del asesinato de Isabel I, justificándolo en su excomunión por el papa Pío V. Pero el conspirador tomó una precaución adicional, codificó la carta.

Babington utilizó un nomenclátor para la codificación, con símbolos que sustituían a cada una de las letras del alfabeto añadiendo además otros 35 símbolos adicionales para palabras o frases completas. Para hacer más seguro el método, había cuatro símbolos que eran nulos, es decir, que no significaban nada ni se correspondían con ninguna letra del texto en claro original. Además, si una letra aparecía dos veces consecutivas en el mensaje en claro, en la codificación se ponía un símbolo concreto que indicaba que era una letra doble, precediendo al símbolo de la letra

en cuestión. Con este nomenclátor, el emisor confiaba en que su mensaje estuviera seguro si alguien lo interceptaba y trataba de leerlo.

Gifford se movía por Londres y por Chartley Hall, la prisión de María, sin problema y con discreción. En sus movimientos, solía dar rodeos y tomar ciertas precauciones. Se había ganado la confianza de la reina escocesa, de Babington y de otros católicos contrarios a la reina inglesa. Estaba en el centro de la conspiración, con acceso a todas las personas y a las comunicaciones, lo que no es mala posición para un agente doble. Gilbert Gifford trabajaba en realidad para Francis Walsingham, secretario principal de Isabel I y cabeza y organizador de un completo sistema de espionaje al servicio de la corona inglesa. El agente se había ofrecido a Walsingham para ese trabajo contra María Estuardo, para infiltrarse entre los católicos que estaban en contra de su reina. Su pasado en Roma era una coartada perfecta para hacerse pasar por uno de los conspiradores y partidarios de la escocesa. En 1585 Gifford le había dicho al jefe de los espías ingleses que conocía el trabajo que estaban haciendo los hombres de Walsingham y que él estaba dispuesto a entrar a su servicio. Le aseguró también que no tenía escrúpulos ni miedo al peligro y que cualquier cometido que le encargaran, lo cumpliría.

Francis Walsingham, que acabaría siendo *sir* Francis Walsingham, nació en torno a 1532 dentro de una familia cercana a la realeza británica. Viajó por Europa siendo muy joven y cuando volvió a su país natal, sus estudios en leyes y su preminente situación social le hicieron llegar al Parlamento. Los idiomas que conocía, su inteligencia y su formación aristocrática, le hacían el candidato perfecto para tratar de conocer las ideas de los extranjeros que se movían entre las altas clases inglesas, y conocer así los posibles partidarios o contrarios a la corona, en un tiempo plagado, como casi todos en la historia, de intereses y de movimientos encubiertos. Aquel cometido le gustaba tanto a Walsingham que con sus recursos fue construyendo una red de espías a su propio servicio y por lo tanto al servicio de aquel al que él sirviera. Una red que acabó no solo trazada a través de todo el reino inglés, sino que se extendió a las más importantes ciudades de Europa.

Entre 1570 y 1573 fue embajador en la corte francesa, en un tiempo en que se planeó el matrimonio entre la reina Isabel I de Inglaterra y el duque de Anjou, el hermano del rey francés. La matanza de San Bartolomé, en agosto de 1572, dentro de las guerras de religión en Francia entre católicos y protestantes, puso a estos últimos en desventaja y acabó con las posibilidades de aquel matrimonio real. También hizo perder capacidad de influencia y contactos al embajador inglés. En cualquier caso, las intrigas y los movimientos de influencia eran ya parte de la vida de Walsingham, que al volver a Inglaterra fue nombrado secretario de la reina.

Walsingham no dejó pasar la oportunidad y puso a Gifford a su servicio. Fue del propio jefe del espionaje la idea de que el agente doble se pusiera en contacto con la embajada francesa para adentrarse en la

red. Su plan funcionó a la perfección. Lógicamente, todos los mensajes que entraban y salían de Chartley Hall a través de Gifford hacían una parada durante su camino en las manos de Walsingham. Entre las personas que dirigía el jefe de los espías ingleses había especialistas en abrir los sellos de lacre sin romperlos y en volver a dejar los mensajes como habían salido de las manos del emisor, sin señas de haber sido leídos y copiados. Como decíamos, tener acceso a todas las comunicaciones de tus enemigos sin que estos lo sepan es una de las mayores ventajas que uno puede tener a su favor en cualquier conflicto. Pero hay un valor aún más determinante: la capacidad de modificar un mensaje o crear un mensaje que el enemigo tome como suyo. Esta ventaja estaba entre las armas que Walsingham tenía en su mano para luchar contra los que querían acabar con su reina.

Cuando las cartas de Babington, codificadas con el nomenclátor, llegaron al jefe de los espías, este las puso en manos de su equipo de criptoanalistas. Walsingham conocía perfectamente la importancia de la criptografía por su servicio a la corona y por eso tenía entre sus colaboradores a un criptoanalista muy capaz, Thomas Phelippes. Experto lingüista, Phelippes hablaba inglés, francés, italiano, español, latín y alemán. Conocía además las técnicas de criptoanálisis de la época y dominaba, por tanto, el análisis de frecuencias, lo que, unido a su capacidad de trabajo, hacía que los encargos de Walsingham fueran resueltos más pronto que tarde.

Una vez puesto sobre su mesa el mensaje que Babington había codificado con el nomenclátor y cuya destinataria era María Estuardo, Phelippes calculó las frecuencias de los símbolos e hizo equivalencias tentativas entre los símbolos y las letras del alfabeto, basadas en los datos que había calculado. Cuando alguna de esas equivalencias se mostraba incoherente, por generar un mensaje sin sentido, la descartaba y probaba con otra. Poco a poco fueron apareciendo palabras con sentido que aseguraban que un símbolo correspondía con una determinada letra, y gracias a sus conocimientos, también fue detectando los símbolos nulos que había incluido Babington y los que sustituían a palabras o frases completas. Cuando tuvo los mensajes totalmente descubiertos, los entregó a Walsingham, que tenía ante sí un complot para matar a la reina de Inglaterra y para rescatar a María Estuardo, nada menos.

Colocado por su buen hacer como jefe de espías en una posición magnífica y de enorme ventaja, Walsingham no se precipitó y se dispuso a sacar el máximo rendimiento posible de esa posición. Podría haber hecho apresar a Babington al momento y usar la carta en su poder como prueba para acabar con él y con su conspiración, pero había una opción mejor. Si esperaba a que María respondiera y se involucrara más directamente en las propuestas de su partidario inglés, especialmente con respecto al magnicidio de Isabel I, esta también podría ser puesta en una situación mucho más comprometida, acusada de participar activamente en el plan para asesinar a la reina.

Walsingham no se equivocó y pocos días después tenía en su mano una carta de María a Babington donde esta hablaba del complot y añadía sus propias aportaciones. Animaba a que el asesinato no se llevara a cabo antes de su liberación, que al menos fuera a la vez, ya que en caso de no ser así sus carceleros podían tomar represalias contra ella e incluso matarla a su vez. En resumidas cuentas, María Estuardo estaba de acuerdo con el magnicidio de su prima Isabel I y, por supuesto, con su propia liberación.

Ni tan siquiera esto, tener una prueba tan clara e implicatoria de la reina escocesa, fue suficiente para el jefe de los espías, que quiso conocer a todos los implicados y capturar así a un buen número de importantes católicos que estaban en contra de su bando. Habiendo descubierto el nomenclátor que utilizaban Babington y María en sus comunicaciones y siendo capaz de romper el lacre de las cartas y volverlas a cerrar sin que sospechara el receptor, podía dar un paso más y modificar las propias comunicaciones añadiendo lo que deseara. Así lo hizo. Pidió a Phelippes, que según parece era un hombre de variados talentos, que imitara la caligrafía de María y añadiera una posdata al final. Se conservan estas cartas y lo cierto es que no es fácil diferenciar la parte escrita por la escocesa de la parte escrita por el criptoanalista inglés. Que la carta estuviera escrita con símbolos hace este ocultamiento más sencillo, ya que una de las claves para el reconocimiento grafológico es cómo se unen unas letras con otras para formar las palabras e incluso el enlace concreto entre dos letras, por ejemplo, una l y una a. En este caso, al ser símbolos, no hay conexión entre ellos y el único cuidado que hubo de tener Phelippes fue imitar la forma en la que la emisora escribía o dibujaba cada símbolo.

En la posdata se solicitaba a Babington los nombres y más información sobre el resto de participantes, así como sobre los hombres que llevarían a cabo el plan de manera directa. Conocer quiénes eran y su posición podía ayudar, según el texto añadido a la carta, a que María pudiera pensar alguna recomendación o mejora en el plan. Por último, solicitaba conocer cuántos y quiénes eran conocedores del complot.

Hecho el añadido, la carta continuó su camino y llego a Babington, que confiaba plenamente en la seguridad de la codificación que estaba utilizando para dirigir la conspiración. Quizás si no hubiera usado ningún método criptográfico hubiera sido más precavido e incluso hubiera tenido un nivel razonable de sospecha sobre las comunicaciones. De hecho, este caso y en general toda la historia de las comunicaciones secretas es una lección directa y explícita sobre lo necesario que es siempre sospechar y pensar en que el enemigo, o cualquier tercero, puede estar accediendo a los textos o incluso, como en este caso, modificándolos. La confianza a menudo se muestra como el peor de los males y acaba pagándose cara.

En poco tiempo Walsingham tenía en su poder información clave sobre los conspiradores y con ello no solo evitaba el complot, sino que clavaba un puñal mortal en el bando católico. El final llegó poco después. Para

recabar ayuda para su plan desde otros países, Babington se disponía a hacer un viaje y para ello tenía que solicitar el correspondiente documento que le permitiera viajar al extranjero. Cuando se presentó a hacerlo, el hombre que lo atendió sabía que debía detenerlo, pero se encontraba solo, por lo que entretuvo al conspirador todo lo que pudo, llevándolo a una taberna cercana, mientras se organizaba un pequeño grupo de soldados que fuera a capturarlo. Babington advirtió los movimientos de los trabajadores al servicio de la corona y se levantó de la mesa en la que estaba, simulando que iba a pagar lo que había tomado y dejando su capa y su espada en la propia mesa en la que estaba sentado, para no levantar sospechas. Se escabulló por la puerta de atrás y escapó de la taberna primero, y luego de la ciudad. Se cortó el pelo y se tiñó la piel para hacerse pasar por un hombre sencillo y ocultar su aspecto aristocrático. Durante diez días consiguió ocultarse de sus perseguidores, aunque a mediados de agosto fue capturado. Con él cayeron seis de los conspiradores. Fueron torturados, mutilados y ejecutados sin miramientos y con ensañamiento, buscando que sus últimas horas de vida fueran lo más dolorosas y terribles posible.

Unos días antes, el 11 de agosto, mientras María Estuardo daba un paseo a caballo, acompañada, por los alrededores de Chartley Hall, varios jinetes se acercaron a ella y su grupo. Quizás en un primer momento la escocesa pensara que había llegado el momento de su rescate y que aquellos hombres eran sus partidarios, de los que Babington era el cabecilla. En realidad, era casi lo contrario. No podían hacerla prisionera porque ya lo era, pero los jinetes venían a comunicarle que era detenida por su participación en el complot contra la reina y que por lo tanto se aplicaba en su caso una ley de 1584, la Ley de Asociación, que el Parlamento había aprobado para procesar a cualquiera que formara parte de un plan contra la reina. La situación de María Estuardo empeoraba, y de una prisionera política, podríamos decir, pasó a ser una procesada por un delito grave.

Dos meses más tarde, en octubre de 1586, en Anglia Oriental, en el extremo este del país, comenzó el juicio, en el que participaban varios jueces y un buen número de hombres principales, entre los que estaba el propio Walsingham. También estaba en la sala Phelippes, el criptoanalista, sentado entre el público. La defensa de la reina escocesa se basaba en asegurar que desconocía el plan y que, si bien no negaba su existencia, no se le podía culpar a ella de que unos pocos hombres, partidarios de su causa, hubieran trazado un complot por su cuenta para asesinar a Isabel I y para rescatarla a ella. Afirmaba que no había participado de forma alguna en el plan y que ni siquiera estaba al tanto del mismo. No sabía María que su correspondencia había sido espiada y confiaba en que, incluso en ese caso, el texto codificado hubiera cumplido con su cometido de ocultar el mensaje original. Pero la capacidad del criptoanálisis a finales del siglo XVI era más que suficiente para romper ese tipo de métodos basados en los nomenclátores, haciéndolos poco seguros.

Las pruebas eran determinantes y María Estuardo, que había sido reina de Escocia, que había sido reina de Francia y que había sido candidata al trono inglés, fue condenada a muerte por participar en una conspiración contra la reina Isabel I. El 8 de febrero de 1587, en el castillo de Fotheringhay, fue decapitada. Sus ropas y el resto de efectos personales que habían viajado con ella hasta allí, fueron incinerados, para evitar que cualquier reliquia fuera convertida en un símbolo de ella misma y de la resistencia católica contra el trono inglés. María, según parece, se mostró digna en su instante postrero.

Los movimientos de María Estuardo contra el trono inglés eran conocidos por Felipe II, aunque este, haciendo honor a su sobrenombre, se mantuvo al margen de manera prudente, probablemente porque no confiaba demasiado en el éxito de la empresa. Había sido informado por su embajador en Inglaterra, Bernardino de Mendoza, en una carta de mayo de 1586. La carta de Mendoza estaba cifrada e iba dirigida al jefe del espionaje de Felipe II, Juan de Idiáquez. El mensaje había sido cifrado por el propio Bernardino de Mendoza, como deja claro en el comienzo de la carta: «Lo que aquí dice suplico a Vuestra Merced se descifre con cuidado y lo ponga en manos propias de Su Majestad, va cifrado de la mía». Cuando el rey Felipe II conoció lo que le contaba su embajador, anotó al margen del texto ya descifrado que, si aquella conspiración la conocían seis gentilhombres, además del embajador, era obvio que la conocían algunos más. Supuso el rey que la falta de secreto hacía inviable el intento.

Thomas Phelippes también generó algún problema a la corona española sirviendo a Walsingham, y también después de la muerte de este en 1590. Phelippes siguió trabajando para el trono británico cuando Jacobo I lo ocupaba, a pesar de que la edad del criptoanalista andaba ya cerca de los setenta años. No había perdido mano en su trabajo, y así, en torno a 1620 rompió la cifra que usaban los españoles, obligándoles a cambiarla. La correspondencia entre el conde de Oñate, en Venecia, y el archiduque Alberto, en Flandes, fue capturada y acabó en Londres. Del éxito de Phelippes contra la cifra española y de todo el asunto de capturas y correspondencia perdida, tuvo conocimiento un agente español en las islas británicas y avisó del hecho a la corona, lo que acabó provocando el cambio de cifra. No había sido aquella una situación rara e inusual, pues en Londres se conocían bien las cuestiones que se comunicaban el conde-duque de Olivares y el papado, por ejemplo. Las cifras y los nomenclátores eran comunes, como también lo eran el robo de correspondencia, su copia y los criptoanalistas.

Entre los muchos actos que se organizaron en 1559 con motivo de la boda de la hija de Enrique II de Francia, Isabel, con Felipe II, rey de España, se puso en marcha un torneo medieval. Lógicamente, con un objetivo muy lejano al combate real y tan solo como un acto más dentro de las celebraciones por el casamiento. En un enfrentamiento del rey Enrique contra el conde de Montgomery, una astilla de la lanza se coló por la fina ranura que permitía la visión a través de la celada del rey

francés y le atravesó un ojo, dejando al rey herido de gravedad. Se puso al monarca en manos de los mejores médicos y cirujanos y ante lo complicado de la situación, se probaron incluso los métodos más drásticos, incluyendo la trepanación del cerebro del rey. Antes de llevar a cabo la operación, los médicos tuvieron a su disposición a algunos condenados a muerte a los que provocaron los mismos daños que tenía Enrique II, para luego intentar salvarlos. Ninguno de estos condenados sobrevivió, como tampoco lo hizo el propio rey.

Como era de esperar, su hijo fue nombrado rey al momento. Francisco II tenía diecinueve años. Pero el nuevo monarca no tenía gran interés por gobernar, o al menos no contaba con hacerlo tan pronto. Así, dejó de lado los asuntos de Estado y los delegó en sus tíos, el cardenal de Lorena y Francisco de Guisa. Este Francisco II es el mismo del que hemos hablado ya y cuya esposa no era otra que María Estuardo. Tanto esta como la madre del joven rey, Catalina de Medici, apoyaban a los tíos del rey en su labor de gobierno. No pasó mucho tiempo antes de que la debilidad del rey y la tensión entre protestantes y católicos lanzaran las luchas abiertas por el poder.

En un primer momento los protestantes franceses esperaban que el joven rey, Francisco II, les beneficiara, pero el paso de los meses demostró lo equivocados que estaban en sus esperanzas. Los Guisa y el resto de hombres que manejaban el poder en realidad, eran partidarios de los católicos y contrarios a los protestantes. Para cambiar la situación, en marzo de 1560 un grupo de protestantes puso en marcha un plan, conocido como la conjura de Amboise. Ese plan era audaz, consistía en raptar al rey para alejarlo así de la influencia de su familia. El príncipe de Condé, Luis de Borbón, líder hugonote, con el apoyo de un buen número de aristócratas y hombres poderosos, estaba supuestamente al frente de la conjura. Las cabezas visibles eran Jean du Barry y el conde de Castelnau, pero el grupo de conspiradores se extendía mucho más allá y por varias ciudades. Como es lógico, mantener una conjura de esta importancia en secreto con tantos participantes no fue sencillo. Los Guisa acabaron por enterarse del plan y de los participantes en él y reaccionaron. Además de poner al rey a buen recaudo en el castillo de Amboise, se prepararon para el enfrentamiento y comenzaron a realizar detenciones. Muchos de los conjurados fueron ahorcados en esos mismos días, a mediados de marzo, e incluso alguno fue descuartizado y su cuerpo mostrado como lección ejemplar. La supuesta cabeza de todo aquello, el príncipe de Condé, fue arrestado y encarcelado. A pesar de todas las acusaciones, el preso aseguraba que no había tenido nada que ver con la conjura de Amboise.

Era de suponer que pasara el tiempo de cárcel ciertamente atemorizado por las consecuencias que la participación en la conspiración estaba teniendo entre sus compañeros protestantes. Pero entonces el príncipe de Condé recibió una carta de *Madame* de Saint-André. La carta era muy dura si se leía de manera completa, pero tenía un mensaje oculto muy diferente. Es un caso de esteganografía extremo, ya que el texto

oculto no lo estaba en realidad y estaba a la vista de todos. La carta decía lo siguiente:

Creedme, príncipe, preparaos a

la muerte. O sentaría mal

defenderos. Quien quiere perderos es

amigo del Estado. No se puede encontrar a nadie

más culpable que vos. Los que,

por un verdadero celo por el rey

os han convertido en tan criminal, eran

personas honestas e incapaces de ser

sobornadas. Tomo mucho interés en

todos los males que habéis hecho en

vuestra vida para querer ocultaros

que el fallo de vuestra muerte ya no es

un secreto tan grande. Los infames,

ya que así calificáis a aquellos

que se han atrevido a acusaros, merecen

también tan justa recompensa como vos

la muerte que os preparan; vuestro único

empecinamiento os persuade de que vuestro único

mérito os ha creado enemigos,

y que no son vuestros crímenes

los que causan vuestra desgracia. Negad

con vuestro descaro acostumbrado,

que hayáis tenido nada que ver en

todos los proyectos criminales de

la conjura de Amboise. No es

como vos habéis imaginado

imposible convenceros. En

todo caso, encomendaos a

Dios.

Como decíamos, leída de manera habitual la carta contiene un mensaje, pero si hacemos algo tan simple como leer solo las líneas impares (primera, tercera, quinta…) el mensaje es muy diferente. Después de mostrarse partidaria del preso, en las últimas líneas de la carta la autora le aconseja sobre lo que debe hacer: «Negad que hayáis tenido nada que ver en la conjura de Amboise».

No había ninguna prueba ni testimonio que involucrara al príncipe de Condé en la conjura y por lo tanto debía resistir y negar relación alguna con los conjurados. El plan le salió bien y poco tiempo después fue puesto en libertad.

Este caso de la conjura de Amboise es especialmente relevante porque involucra a la corona francesa y está relacionado con las luchas de religión entre hugonotes y católicos, pero lo cierto es que hay otros casos en la historia, hasta en nuestros días, en los que se ha ocultado algún tipo de mensaje en las líneas de un texto, en las primeras letras de las palabras, o en las primeras letras de las líneas de un texto. Algo que parece tan arriesgado que es casi una locura, pero que, como vemos, funciona en no pocas ocasiones.

Aunque el caso es un poco más tardío, del siguiente siglo, algo parecido le pasó a John Trevanion, un político inglés del siglo XVII que en la guerra civil inglesa estaba en el bando realista. En este conflicto, realistas y parlamentarios se enfrentaron durante varios periodos, y en 1648 fue hecho prisionero por los hombres de Cromwell y acabó encarcelado en el castillo de Colchester. Con toda seguridad acabaría ajusticiado, y en ese momento recibió la carta de un amigo que le alentaba a afrontar el trance postrero con ánimo y resignación. La carta ocultaba un mensaje mucho más interesante, como era de esperar para que la historia de Trevanion tuviera algo que ver con la criptografía. Tomando la tercera letra después de cada signo de puntuación, el preso era advertido de que al final de la capilla del lugar donde estaba preso había una pared deslizante que le permitiría escapar. Trevanion dio con el mensaje y convenció a sus captores de que le llevaran a la capilla y le dejaran solo, preparando su alma para el más que probable encuentro con la muerte. Ni que decir tiene que consiguió escapar del castillo.

Otro buen ejemplo lo tenemos en *La Celestina* , que es el nombre con el que se conoce popularmente a la *Tragicomedia de Calisto y Melibea* . Se publicó por primera vez en Toledo en el año 1500 y probablemente los problemas de su autor con la Inquisición hicieron que decidiera quedarse en el anonimato y no firmar la obra. No firmarla de manera directa, ya que en posteriores ediciones se incluyeron unos versos que formaban el siguiente acróstico tomando las primeras letras de cada línea: «El bachiller Fernando de Rojas acabó la comedia de Calysto y Melibea y fue nascido en la Puebla de Montalván».

Los templarios nacieron como orden en el siglo XII y además de monjes y soldados, con el paso del tiempo se convirtieron en poderosos hombres de negocios que hicieron un uso considerable de algunos mecanismos financieros, que también se utilizaban ya en Venecia y otros lugares, para prestar dinero y para enviarlo de un lugar a otro o de una persona a otra, sin tener que viajar con el propio dinero. No hay muchas certezas sobre los métodos criptográficos que utilizaron los templarios, pero sí parece claro que lo hicieron para proteger y asegurar esos movimientos económicos, para validar sus letras de cambio.

Uno de los métodos que se les atribuye es la sustitución de cada letra por un dibujo, muy similar al método que utilizaron unos siglos después los francmasones, aunque no es exclusivo de estos dos colectivos. La importancia del uso que hicieron los templarios de la criptografía no es tanto por su método o por la seguridad del mismo, que distan mucho de ser sólidos, sino por el fin con el que la utilizaron. Durante siglos la criptografía vivía dentro de los límites del mundo diplomático y militar, salvo en contadas excepciones. Fueron los templarios los primeros que la utilizaron para un fin comercial, para asegurar y validar sus letras de cambio, como decíamos. Existen al menos tres documentos manuscritos, dos en Francia y uno en Italia, que datan del siglo XIII y en los que aparece el alfabeto templario, que es similar en la idea al que veremos a continuación.

Damos un salto de siglos para hablar del método utilizado por los francmasones, ya desde el comienzo del siglo XVIII, para sus comunicaciones secretas e incluso para dejar mensajes escritos en algunos lugares. Es tan sencillo que es otro de esos casos en los que se puede convertir fácilmente en un juego de niños. Se trata de una forma de cifrado por sustitución simple, es decir, a cada letra le corresponde un símbolo o dibujo, y ese dibujo proviene de la posición en la que se colocan las letras dentro de una tabla y dentro de una cruz, añadiendo puntos para poder alcanzar todas las letras del alfabeto.

Este tipo de escritura perduró durante siglos, con algunos cambios. También se conoce como cifrado Pigpen y en él cada letra se describe en el cifrado por las líneas y puntos del lugar en el que está dentro del dibujo. Así, el texto Plus Ultra correspondería a:

La primera forma marca la celda de la P, que tiene en el dibujo una línea arriba y otra a la derecha, junto con un punto que la diferencia de la G.

La L, segunda letra del texto que hemos usado como ejemplo, tiene en el dibujo líneas en la izquierda y en la parte inferior, de nuevo con un punto para diferenciarla de la C. Como vemos, un método sencillo y muy fácil de memorizar y reproducir, por lo que no es extraño que siga presente aún en nuestros días, si no en el mundo de la criptografía, sí en el mundo de la educación, en los videojuegos, en el arte e incluso en forma de tipografía. Hay diferentes versiones con ligeros cambios. Por ejemplo, en ocasiones se prescinde de las dos cruces, para codificar de la S en adelante, y en su lugar se usa una tercera rejilla, donde se utilizan dos puntos en las celdas en las que se sitúan las letras del alfabeto posteriores a la R.

Como decíamos, este método era utilizado por los francmasones para dejar algunos mensajes ocultos en determinados lugares. Por ejemplo, la tumba de Thomas Brierley, en Inglaterra, además de los símbolos masones habituales, el compás y la escuadra, tiene un texto escrito según este alfabeto. Los textos grabados sobre la tumba en la codificación Pigpen hablan de la fecha del ingreso de Brierley, suponemos que en la propia francmasonería, y contienen también la frase «Santidad del Señor».

Este método no fue ideado en el siglo XVIII, sino que data de mucho antes. De igual forma también se había utilizado antes, por los Tudor, por ejemplo, y se usaría después. El método fue descrito por Vigènere, uno de los hombres más importantes de la historia de la criptografía, y este atribuía su creación a Heinrich Cornelius Agrippa, el sabio ocultista y teólogo nacido en 1486.

Los templarios, realmente no utilizaban la rejilla que acabamos de ver, sino que colocaban sus letras con base en su cruz, la cruz del Temple.

PARTE 2LOS PIONEROS Y LA SISTEMATIZACIÓN DEL SECRETO

6. La búsqueda de la cifra indescifrable

Un cambio importante en el siglo XVI en la gestión de lo que podríamos llamar inteligencia, usando terminología actual, fue la generalización y sistematización entre los estados y los poderes de la captura de información del enemigo o de aquel del que se quería saber. Usando de nuevo la terminología actual, la inteligencia de señales (SIGINT), que es la obtención de información a través de la interceptación de las señales o mensajes, sean transmitidos por el medio que sea, electrónico o no, tomó relevancia en aquel siglo y, como veremos en detalle, se crearon entidades dentro de los estados dedicadas a la captura de mensajes, no únicamente de enemigos, sino de cualquier otro gobierno, estado o personaje poderoso. Lógicamente, muchas de estas comunicaciones viajaban cifradas, por lo que la criptografía se desarrolló tras la estela de este auge de la inteligencia. Los estados italianos fueron teniendo poco a poco personal dedicado al criptoanálisis, cada vez con mejor preparación y resultados; y no fueron los únicos. La diplomacia fue ganando terreno y con ella, de nuevo, la criptografía. Además, como algo esencial. Los más expertos se dedicaban a tiempo completo a la tarea de crear nuevas formas de cifrado, a la vez que trataban de romper los sistemas de otros. Aparecieron entonces los primeros grandes nombres de la criptografía, que en muchos casos idearon soluciones que se mantuvieron útiles durante siglos. También se escribieron tratados que ayudaron a que el conocimiento fluyera por toda Europa.

Los Sforza, señores de Milán, también tenían sus asistentes en este ámbito, y uno de ellos, Cicco Simonetta, escribió el primer tratado de la historia dedicado exclusivamente al criptoanálisis y descifrado, del que tenemos constancia. En 1444 Simonetta ya era secretario y canciller de Francesco Sforza, y este tenía en tanta estima su contribución que llegó a decir que, si Cicco no hubiera existido, se habría visto obligado a crearse uno de cera. Simonetta era el jefe de la cancillería de los Sforza en Milán, y bajo su tutela se movían todas las acciones y trabajos, entre ellos la diplomacia y cualquier asunto relacionado con la criptografía. Volviendo a su legado en forma de texto, el *Tratado de descifrado* , escrito en Pavía en 1474, contiene la forma de actuar que guio a sus contemporáneos y que obligó a la criptografía a evolucionar. Sus doce puntos son una lección tan importante y una mirada tan directa a ese momento incipiente de la criptografía, que merece la pena conocerlos. Nos permiten ver, en cierta medida, cómo trabajaban los primeros criptoanalistas occidentales, cuáles eran sus procesos y su forma de pensar:

Si las palabras en un texto cifrado tienen cinco o menos finales diferentes, el texto en claro es probablemente un texto en italiano, y si no es italiano, será latín. Como alternativa, busque todas las palabras

de una sola letra. El latín normalmente solo las tiene de un tipo, a, mientras que el italiano las tiene de varios.

Si el texto cifrado tiene muchas palabras de dos o tres letras, el texto estará probablemente en italiano.

Si el texto en claro está en italiano, entonces ya sabe qué letras son vocales, porque son las que aparecerán al final de las palabras. Si una de estas letras finales aparece frecuentemente también como una palabra de una sola letra, será probablemente una e.

Las palabras de dos letras suelen comenzar en italiano por l.

La palabra de tres letras más común en italiano es che.

En cualquier caso, si el texto está escrito en latín, las letras que aparecen al final de las palabras son vocales, la s, la m o la t. Excepto para ab, ad, y quod, que son muy comunes.

En los textos en latín las palabras de una sola letra son habitualmente una a, pero también son posibles la e, la i y la o.

En latín las palabras más comunes de dos letras son et, ut, ad, si, me, te y se. Una lista un poco más larga de opciones es: ab, ac, ad, an, y at; da, de y do; ea, ei, eo, et, ex y es; he, hi, id, ii, in, ir, is y it; me, mi, na, ne y ni; ob, os, re, se y si; tu, te, ue, ui y ut.

Las palabras de tres letras en latín cuya primera y última letra coinciden son: ala, ama, ara, ede, eme, ere, ehe, ixi y iui.

Cualquier letra que en latín aparezca tres veces seguidas es una u.

Las letras en latín que aparezcan repetidas consecutivamente en palabras de cuatro letras son, probablemente, ll o ss, como en esse o ille.

Una regla final que es cierta tanto para el italiano como para el latín: si se encuentra con una letra que está siempre seguida por una única posible letra, entonces es una q seguida por una u, y, además, la letra detrás de la u será una vocal.

De esta breve guía podemos deducir que lo primero de todo era determinar el idioma en el que está escrito el texto. En este caso las posibilidades son el italiano y el latín. El siguiente paso es tratar de descubrir a qué corresponden las vocales y, finalmente, tratar de identificar algunas consonantes. En este proceso, el texto irá apareciendo; como cuando uno juega al ahorcado o hace crucigramas, cada letra es una pista que lleva a hacer hipótesis y descubrir otras letras, avanzando en la conclusión del puzle.

Es interesante también ver cómo en este momento de la historia se habla de la longitud de las palabras en el texto cifrado, ya que esta longitud es igual que en el texto en claro. No se eliminan los espacios en blanco en el texto cifrado o se construye este utilizando bloques de un número constante de letras, algo que, como veremos, se comenzará a hacer precisamente para anular esta forma de atacar un cifrado. Es curioso ver, asimismo, que en el texto de Simonetta se ataca el cifrado desde la estructura de las palabras y del propio texto, no tanto desde el análisis de frecuencias. Esto, por cierto, ha llamado la atención de algunos investigadores, que en los últimos años han puesto en duda el uso generalizado de las matemáticas y la estadística para atacar los métodos de cifrado, en el siglo XV y la primera parte del XVI, en Europa.

En la historia de la criptografía han sido varias las cifras que en su momento se han tomado por inviolables y perfectas. En realidad, todas las cifras siempre se han tomado por seguras y por lo tanto irresolubles por el enemigo, o al menos inviolables en un margen de tiempo suficiente, tras el cual, la información ya no es valiosa para el enemigo o peligrosa para el emisor, por haber caducado su utilidad. Pero solo algunos pocos métodos criptográficos han llegado a ese nivel especial donde la cifra se ha mantenido inviolable durante un buen periodo de tiempo. A menudo, porque incorporaba alguna técnica o característica nueva que los criptoanalistas del momento no sabían cómo sortear para llegar al mensaje en claro. En esa reducida lista está la cifra de Vigenère, que supuso un salto hacia delante considerable, dejando atrás la criptografía de sustitución monoalfabética, a la que un sencillo análisis de frecuencia dejaba al descubierto. Este conocimiento generado por Vigenère, una vez extendido y dominado por todos los involucrados en el mundo de las cifras y el espionaje, hacía poco útiles los métodos habituales de criptoanálisis y por lo tanto daba seguridad a quien lo utilizaba.

El camino desde la sustitución monoalfabética hasta Vigenère no fue corto ni directo, como es lógico. Recuerden de nuevo que en el arte de la criptografía se camina a hombros de gigantes. Así, todo comenzó en torno a 1460, cuando Leon Battista Alberti dio el primer paso de ese camino. Nacido en Génova en 1404, hacía honor a la imagen típica del hombre renacentista, ya que sus intereses y conocimientos eran heterogéneos. Arquitecto, poeta, músico, matemático, filósofo… entre sus intereses también estaba la criptografía. Trabajó para tres papas y para algunas de las más importantes familias de la época, siendo especialmente importante su relación con la ciudad de Florencia. Un día, cuando paseaba por los jardines del Vaticano con el secretario papal Leonardo Dato, la conversación derivó hacia la criptografía. Dato le confesó que en el Vaticano se había puesto sobre la mesa la necesidad de cifrar los mensajes de manera general y con seguridad, y que ni él ni otros a los que había consultado tenían los conocimientos suficientes y la capacidad necesaria para idear un método de codificación que

ofreciera garantías. Alberti se hizo cargo de la petición y prometió ayudar a Dato, del que era buen amigo.

Cuando Alberti comenzó a profundizar en la criptografía, cayó en la cuenta de que los métodos utilizados hasta ese momento tenían como punto débil que el alfabeto de destino del cifrado en cada codificación siempre era el mismo. Para cada letra del texto en claro había un único sustituto, fijo y constante, facilitando así la labor del criptoanalista mediante el ya conocido análisis de frecuencias. No hay que olvidar que los criptoanalistas árabes habían desarrollado las bases de esta forma de atacar códigos y que por lo tanto es posible que Alberti conociera esas técnicas de estudio del lenguaje y de análisis de textos, tanto codificados como sin codificar. Reflexionando sobre el tema, concluyó que si se alternaban varios alfabetos de cifrado durante el proceso, ese punto débil desaparecía y el análisis de frecuencias se volvía inútil. Se entiende por alfabeto de cifrado el alfabeto de equivalencias de las letras ordenadas de acuerdo al alfabeto habitual. Esto es, si el alfabeto estándar es A, B, C… un alfabeto de cifrado puede ser F, G, T… donde la A del texto en claro se sustituiría por la F, la B por la G, la C por la T, y así sucesivamente. Tener varios alfabetos de cifrado e ir cambiándolos a medida que se cifra cada letra, hace que a cada letra en el texto el claro le corresponda una diferente cada vez que aparece. Esto diluye la frecuencia de las letras del texto en claro entre esas varias letras codificadas. Esta idea, que habíamos comentado y ejemplificado, es tan sencilla como efectiva, pero fue Alberti el primero en caer en ello.

Leon Battista Alberti desarrolló el método de codificación que lleva su nombre a mediados del siglo XV, entre 1466 y 1470, y lo plasmó en su tratado *De Componendis Cyphris* , donde aparecen por primera vez esos conceptos sobre varios posibles alfabetos de cifrado como destino para una misma letra. Era la primera piedra en la construcción de una barrera frente al análisis de frecuencias, la primera piedra de la conocida como sustitución polialfabética, por esa idea de utilizar varios alfabetos, y fue escrita para un grupo relativamente cerrado de personas dentro del Vaticano, no para su divulgación general. Tanto es así que no fue publicado hasta 1568, un siglo después de su escritura. Hay que tener en cuenta que la difusión de estos textos podría ser algo incongruente con la necesidad de secreto asociada a este mundo. Sus escritos estaban dirigidos tan solo a sus pupilos y colaboradores, a sus más allegados y a aquellos que prestaban servicio en el mismo bando. Alberti dirigió su tratado a una audiencia privada y selecta, y expresamente pidió en él que no se permitiera que el texto cayera en las manos del público en general. Alberti estaba convencido de que este tipo de conocimiento, quizás por el poder que daba a quien lo dominaba y usaba, debía estar al servicio de los estados. Esta idea del siglo XV, por cierto, sigue vigente en nuestros días y el debate sobre el control de la criptografía, si debe corresponder a los estados o si es conveniente que todos y cada uno de nosotros podamos usarla para comunicarnos con total confidencialidad con quien deseemos, sigue sin resolverse con claridad.

Alberti reflexiona en sus estudios sobre la relación entre vocales y consonantes dentro de un texto, lo que indica cierta preocupación por estos aspectos estadísticos de la composición de las palabras. Expone que, mientras que en la poesía las vocales no son superadas por las consonantes por más de una ratio de uno contra ocho, en la prosa escrita las consonantes generalmente no superan a las vocales más allá de una ratio de uno a tres. Esa diferencia entre poesía y prosa nos lleva a pensar que el trabajo de investigación había sido profundo, ocupándose de analizar textos de varios tipos. De igual forma, Alberti aborda cuestiones como que mientras entre las vocales la letra o es la menos frecuente, en los textos en latín la e y la i aparecen con mucha frecuencia. Con base en esto, Alberti idea el método para cifrar que diluye esa debilidad de la repetición de las letras en el idioma, y propone así el uso de homófonos, es decir, de la equivalencia de varias letras en el texto cifrado para una letra habitual en el idioma del texto en claro.

Es interesante considerar cómo acometían los criptoanalistas de esta época su trabajo, si tenemos en cuenta la recomendación de usar homófonos y el proceso de ataque a una cifra descrito por Cicco Simonetta. Este último decía que, en italiano, las palabras solían acabar la mayoría de las veces con una vocal. Por lo tanto, aunque el uso de homófonos diluya la frecuencia de esas vocales entre varias letras del texto cifrado, lo cierto es que seguiría siendo relativamente fácil saber qué letras corresponden a vocales sencillamente por su posición en el texto, siendo esto un paso de gigante en cualquier proceso de criptoanálisis. Este problema se soluciona con facilidad rompiendo la estructura del texto en claro y transcribiendo el texto cifrado de tal forma que no se pueda conocer a simple vista el final de las palabras. Si se eliminan los espacios en blanco o se escriben las letras en bloques fijos, de cinco letras, por ejemplo, desaparecen esas pistas tan útiles para el criptoanalista. En cualquier caso, sirva esto como idea de la importancia del conocimiento del idioma a la hora de analizar una cifra, y también para comprobar cómo los más mínimos detalles pueden ser una carta mal colocada que arruine todo el castillo de naipes de una cifra. Esto último veremos que es una de las claves de la criptografía en la historia, cuando muchos buenos métodos han sido mal usados o usados sin todo el rigor necesario, dando pistas al enemigo para tirar del hilo y hacerse con el código o con el método de cifrado utilizado.

La propuesta de este gran criptógrafo que más peso ha tenido a lo largo de la historia y que ha resistido durante siglos, se basaba en un disco, el conocido como disco de Alberti, que era un dispositivo compuesto por dos anillos concéntricos, uno fijo en el centro y otro rodeando a ese primero y además móvil, es decir, que puede girar. En la versión del italiano renacentista, el anillo externo tenía 24 posiciones en las que están grabadas 20 letras latinas, en mayúscula y ordenadas alfabéticamente, y los números del 1 al 4. Las letras que eliminó Alberti de su disco externo no las consideraba esenciales para hacerse comprender. El disco interno, el que podía girar, tiene 24 posiciones

donde están las letras latinas, en minúscula, y el símbolo &, e incluye algunas de las que no están en el disco exterior: la H, la K y la Y.

La posibilidad de girar uno de los discos y enfrentar así cada una de las 24 posiciones del disco externo con cualquiera de las posiciones del disco interno, hace que el número de destinos para cualquier letra del texto en claro sea de 24. Para comunicar un mensaje, emisor y receptor debían tener cada uno un disco de Alberti. Además, las letras del anillo interno, que están descolocadas, debían seguir el mismo orden en ambos. Al principio del mensaje, el emisor indica dos letras, cada una de un anillo, que deben estar enfrentadas. Por ejemplo, la letra k del anillo móvil se coloca enfrentada a la letra B del anillo externo. La codificación se hace tomando cada letra del texto en claro, buscándola en el anillo externo y sustituyéndola por aquella que está en el anillo interno en esa misma posición, enfrentada a ella. Si el proceso fuera este y solo se modificaran las posiciones de los anillos al comenzar la codificación, tendríamos un método que cambia de alfabeto entre dos comunicaciones distintas, pero que no lo hace en un mismo mensaje, por lo que, si este es suficientemente largo, el análisis de frecuencias sería un ataque válido para conocer el mensaje original. Con el objetivo de solucionar este problema Alberti incluyó en su método la posibilidad de cambiar las posiciones de los anillos cada vez que se deseara. Como hemos indicado, el anillo externo contiene letras mayúsculas y el interno letras minúsculas, por lo que, si en el texto cifrado uno se encuentra una letra mayúscula, debe saber que lo que está indicándole el emisor es que debe recolocar los anillos, usando como posición de referencia esa letra mayúscula. De este modo, sí tenemos un método de codificación polialfabético. La idea era poderosa, y si bien existía la necesidad de que el emisor y el receptor tuvieran dos discos exactamente iguales, la seguridad era mayor que en métodos de cifrados que existían hasta ese momento.

Johannes Trithemius, un abad alemán nacido en 1462, tomó el testigo de las ideas sobre sustitución polialfabética. Nacido en Trittenheim, su nombre proviene precisamente de ese lugar, ya que el real era Johann von Heidenberg. Sus intereses, como parece común y también lógico entre los pioneros de la criptografía, iban de las lenguas a las matemáticas y a la astrología. En la intersección de estas disciplinas, Tritemio, como también se le conoce, creó el cifrado que lleva su nombre y que se basa en una codificación polialfabética, donde tenemos un alfabeto en claro que va de la A a la Z y tantos alfabetos de cifrado como letras. Tritemio concibió una tabla donde cada fila contiene las letras del alfabeto ordenadas de distinto modo. La primera fila, eso sí, tendría el alfabeto ordenado como se hace habitualmente. De nuevo tenemos una herramienta básica para hacer cifrado polialfabético y así cifrar con mayor seguridad. El propio Tritemio denominó a esta matriz como *tabula recta* .

No se emplean por tanto dos alfabetos de cifrado, como proponía la primera idea de Alberti, sino que se propone la utilización de tantos alfabetos distintos como letras hay en el propio alfabeto. Todo ellos son

posibles destinos de la codificación de cada letra del texto en claro. El cuadro resultante es la tabla en la que se representan todos esos alfabetos. La siguiente imagen muestra cómo sería la matriz o *tabula* de Tritemio, si bien la original tenía algunos cambios en las letras, como es lógico. Por claridad, nosotros usamos una versión castellanizada, en la que incluimos también la Ñ.

En la primera fila de la tabla tenemos el alfabeto en claro o alfabeto llano, donde están escritas las letras en el orden que todos conocemos. En la segunda fila está el primero de los alfabetos de codificación, que en realidad es un alfabeto al que se le ha aplicado una cifra César de una posición. Dicho de otro modo, todas las letras están desplazadas una posición, y por lo tanto comienza por B, C, D… y finaliza con Z, A. En la tercera línea, con el segundo alfabeto de cifrado, tenemos un desplazamiento de dos posiciones, comenzando por C y finalizando en la letra B. Esto se repite en las filas restantes, aumentando el desplazamiento en cada caso (tres posiciones, cuatro posiciones…) hasta completar todos los alfabetos de codificación. El último comienza por Z, A, B… y finaliza con la Y. Como vemos, cada uno de los alfabetos de cifrado está ordenado, aunque haya sufrido un desplazamiento sobre el alfabeto en claro, por lo que el uso de uno solo de esos alfabetos resultaría en un cifrado de tipo César, que a estas alturas de la historia era fácilmente rompible.

A partir de esta matriz, el método de cifrado de Tritemio es sencillo. Se toma la primera letra del mensaje a cifrar y esta se deja tal cual, es decir, se lleva al texto codificado la misma letra que está en el texto en claro. A continuación, se localiza la fila que tiene como primera letra la segunda del mensaje en claro y se toma la segunda letra de ese alfabeto de cifrado, es decir, la segunda de esa fila. Se busca entonces la fila o el alfabeto que comienza con la tercera letra del texto en claro y se reemplaza esa letra por la tercera del alfabeto.

El siguiente ejemplo ilustra el proceso. Para cifrar la frase HABLOENESPAÑOLCONDIOS, se deja la primera letra sin hacer variaciones, la H. A continuación, se tiene la letra A en el texto en claro, por lo que tomamos la fila o alfabeto que comienza por A y tomamos su segunda posición para componer el texto codificado. La A se sustituye por la B. Esto nos lleva a la fila que comienza por B para la tercera sustitución, y de ahí tomamos la tercera posición, lo que resulta en D. Completando el proceso, el resultado sería el siguiente texto codificado: HBDNSJTLAYKYAXPDDTZHM.

Este método de codificación dista mucho de ser seguro, pero supuso un avance interesante en la línea de lo que expuso Alberti. Tritemio describió este método con detalle en su obra conocida como *Polygraphia* , publicada en seis volúmenes de manera póstuma en 1518, cuando el abad alemán ya llevaba dos años reunido con su Señor en el Cielo. Se publicó en lengua latina, el lenguaje culto de la época, pero acabó siendo traducido al alemán y al francés, lo que deja clara la relevancia de su texto y la importancia de la temática. En torno al año

1500 escribió una obra titulada *Esteganografía* , donde se mezclan ideas filosóficas y mágicas con cuestiones criptográficas. Como decíamos, no supuso una revolución práctica ni la seguridad, pero abrió camino a nuevas ideas y métodos de cifrado, que nos legaron otros.

Jacobo de Silvestri, florentino del siglo XVI, fue un criptógrafo que también estuvo cerca del papado y que probablemente fue influido por las técnicas y explicaciones de Alberti. Fue el primero en sugerir la utilización de símbolos más allá de las propias letras del alfabeto habitual e incluso de ilustraciones, para codificar los mensajes. Además, se propuso por primera vez en la historia escribir un relato sobre la evolución de la criptografía desde la Antigüedad hasta aquel momento, hablando de la escítala espartana, por ejemplo, y concluyendo el tratado con los métodos de criptoanálisis que se conocían y se podían aplicar ya en el siglo XVI, para romper los métodos de ocultación de textos. No solo se dedicó a recopilar conocimientos, lo que no es poco, sino que también ideó variaciones sobre los métodos criptográficos conocidos, y todo ello se convirtió en la fuente de la que otros bebieron.

En 1501 nacía en Pavía Girolamo Cardano, un matemático italiano con formación en leyes y en medicina. Como vemos, otro nombre que hace honor al tópico renacentista. Publicó más de cien textos y dejó otros tantos escritos, entre los que había dos enciclopedias de saberes generales. Destacó por sus avances en álgebra, sobre las soluciones de las ecuaciones de tercer y cuarto grado. También el azar le atrajo de manera importante, llegando a dejar plasmadas sus ideas en lo que se considera el primer tratado relevante sobre probabilidades. La estadística y las probabilidades, como ya sabemos, juegan un papel importante en la criptografía, por lo que no es extraño que Cardano también se interesara y escribiera sobre esta. En uno de esos tratados, recopilaba los conocimientos sobre el tema y los extendía a aspectos más mundanos, como la apertura de cartas sin dejar rastro o cómo fabricar tinta invisible. De entre las cuestiones que aportó al tema criptográfico, destaca la que se considera la primera autoclave de cifrado de la historia. Proponía trabajar con una tabla como la Tritemio y utilizar como clave el propio texto en claro, y volviendo a comenzar por la primera letra de la clave con cada nueva palabra del texto a cifrar. Por ejemplo, si el texto en claro fuera HABLO EN ITALIANO CON LAS MUJERES, la clave usada para cada letra sería: HABLO HA HABLOENI HAB HABLOEN. La clave determinaba cuál de los alfabetos había que usar en cada caso. Como vemos, el texto en claro es el que determina la propia clave y esto genera varios problemas de seguridad en el método, facilitando su ruptura. Por lo tanto, esta idea, *a priori* interesante, no condujo a ningún avance práctico, una situación que ya hemos visto con varios de estos pioneros de la criptografía. No llegaron a la solución definitiva, pero prestaron sus hombros para que otros fueran caminando cada vez más lejos.

Cardano sí logró, no obstante, grabar su nombre en la historia de la criptografía, si bien no fue con algo en la línea de Tritemio o Alberti, sino con un método de esteganografía que se ha utilizado durante

mucho tiempo, siendo muy común en los siglos XV y XVI en la correspondencia diplomática. La rejilla de Cardano, como se conoce su propuesta, no es más que un papel o cartón al que se le han hecho diferentes ventanas o agujeros, de manera irregular, es decir, colocados sin ningún patrón sobre el papel. El emisor del mensaje coloca esta rejilla sobre un papel en blanco, y escribe a través de las ventanas el mensaje a enviar, escribiendo en cada hueco lo que este le permita con su espacio, de tal forma que en unos casos el hueco le permitirá escribir una letra, en otros alguna sílaba y en algunos casos una palabra completa. Escrito el mensaje secreto sobre la hoja en blanco, se retira la rejilla y se escribe toda la página, respetando el mensaje secreto ya escrito, con un texto inocuo pero coherente. Para descifrar el texto basta con poner una réplica exacta de la rejilla usada para componer el mensaje sobre la carta, para conseguir que quede a la vista el mensaje oculto a través de los huecos.

Las ideas en torno a la clave y el juego con varios alfabetos, desde varios puntos de vista, eran ladrillos que iban componiendo el pilar de la gran cifra que estaba a punto de llegar. Giovan Battista Bellaso, otro italiano del siglo XVI, que en ocasiones aparece citado como Belaso o Belasso, siguió las ideas de Tritemio y de otros de los pioneros para acabar diseñando un método para generar autoclaves más avanzado que el que había pensado Cardano. No se sabe mucho de su vida, pero sí se tiene constancia de sus propuestas sobre la criptografía polialfabética y las claves. Tomando directamente su explicación sobre cómo encriptar, Bellaso proponía tomar varias palabras en latín o en cualquier otro lenguaje, lo que podríamos llamar clave, y el texto del mensaje a cifrar, escribiendo ambas cosas en papel de tal forma que cada letra de la clave quedara sobre cada letra del texto en claro. Como es habitual, la clave se debía repetir tantas veces como hiciera falta, hasta completar la longitud del texto a cifrar. Esto, junto con varios alfabetos identificados o indexados por sus letras de cabecera, siguiendo las ideas de Tritemio, componía todo lo necesario. A la hora de cifrar una letra del texto en claro, se tomaba el alfabeto que marcaba la letra correspondiente de la clave. Este sistema, cercano a las ideas anteriores, permitía que cada emisor y receptor acordaran una clave y que esta determinara el resto del proceso y el resultado. Si una clave se creía comprometida o había sido descubierta, bastaba con acordar otra para volver a hacer seguras las comunicaciones.

El trabajo de los pioneros, como vemos, llevó su tiempo y sus esfuerzos y son varios los nombres que se suman. Giovanni Battista Della Porta, nacido en 1535, fue uno más de esos pioneros. De nuevo tenemos como escenario a Italia, ya entrado el siglo XVI. Era otro hombre renacentista con interés por múltiples disciplinas, entre las que estaban las matemáticas y la criptografía. Dejó por escrito muchas de sus ideas e investigaciones, y entre esos escritos tenemos un método criptográfico que utiliza una clave para indicar cuál de los alfabetos posibles de codificación se debe utilizar en cada paso. Es decir, giraba en torno a la misma idea que Bellaso. Porta propone una matriz con varios alfabetos en los que cada uno de ellos está escrito en dos filas. Cada alfabeto contiene todas las letras, pero el orden de las letras, al menos en una de

esas dos filas es impredecible o, dicho de otro modo, las letras están desordenadas. Se busca en el alfabeto la letra del texto en claro a cifrar y se sustituye por la que tiene arriba o abajo. Por ejemplo, supongamos que dentro de la matriz de alfabetos tenemos el siguiente, indexado o identificado por la letra D:

Si la clave es DOMINGO y nos disponemos a codificar la primera letra del mensaje en claro, tendremos que usar este alfabeto, ya que hemos dicho que es el que corresponde con la D, primera letra de la clave. Para codificar la letra E, la buscamos y la sustituimos por la letra que tiene debajo, en este caso, la U. Si tuviéramos que codificar la T, que está en la fila inferior, tomaríamos la letra de la fila superior, y sería la C. Para codificar la siguiente letra, repetiríamos el proceso, pero usando el alfabeto indicado por la segunda letra de la clave, la O en el ejemplo que estamos viendo, donde la clave es DOMINGO. Este proceso se repite hasta el final y si llegamos al final de la clave, volvemos a comenzar por su primera letra, de forma cíclica. Porta, por cierto, también dedicó algún esfuerzo a la esteganografía, utilizando un huevo duro como portador del mensaje. Escribió el texto sobre la cáscara, valiéndose de una tinta de alumbre y vinagre, que traspasaba la cáscara y marcaba el mensaje sobre la superficie blanca de la clara.

La fama final se la llevó Blaise de Vigenère, un diplomático francés nacido en 1523, aunque sus pies se asentaban sobre las piedras que habían ido colocando todos los anteriores. Por su trabajo, como es lógico, tenía conocimientos de criptografía, y muy pronto, desde su estancia de dos años en Roma en torno al año 1550, ya conocía los textos de Alberti, de Tritemio y de Porta, aunque no profundizó en ellos más allá de lo meramente necesario para llevar a cabo su trabajo como diplomático. Cuando tenía treinta y nueve años ya había acumulado suficiente riqueza como para dejar su carrera profesional y dedicarse al estudio y a todo aquello que le estimulaba. Fue entonces cuando analizó y desarrolló los trabajos anteriores sobre criptografía y cuando llegó al método que tomaría su nombre y que inscribiría este en los libros de historia.

En la combinación de todos los alfabetos está el poder del método de Vigenère, que propone saltar de una fila a otra con el cifrado de cada letra. Esta idea, como sabemos, no es nueva, sino que estaba ya descrita en la obra de Bellaso que se publicó en 1553 y que, por cierto, tenía el sencillo nombre de *La cifra del Sig. Giovan Battista Belaso* .

En la idea de Vigenère, lo que han de hacer el emisor y el receptor es acordar qué alfabetos se van utilizando y en qué orden. Para ello, se utiliza una clave, otra idea que no es nueva, sino que es recogida de los pioneros de los que hemos hablado. Habitualmente el mensaje en claro es más largo que la clave, por lo que esta se repetirá de forma cíclica, como ya hemos visto.

Por ejemplo, si la clave es la frase HABLOENINGLESCONLOS CABALLOS y la primera letra del texto en claro es la L, se escribirá en

el texto cifrado, la letra que está en la misma posición que la letra L (posición 12) en el alfabeto cifrado que comienza por H, primera letra de la clave. Si la segunda letra es la O, se buscará la letra en la posición de la O en el alfabeto cifrado que empieza con la letra A. Así se va saltando de manera sucesiva entre un alfabeto y otro, generando un texto cifrado que, a aquellas alturas de la historia, mediados del siglo XVI, era completamente inviolable por las técnicas de criptoanálisis conocidas en la época. No tenía sentido ya contar el número de veces que aparecía una determinada letra para intentar averiguar cuál era a partir de su frecuencia, ya que una misma letra del mensaje cifrado correspondía a varias letras del texto en claro de forma desordenada y con multitud de posibilidades. Esta ambigüedad hace que el criptoanalista no pueda rastrear su origen aplicando las técnicas conocidas en la época. Por otra parte, debido a que no hay restricción alguna al texto que se puede utilizar como clave, las posibilidades de la misma son potencialmente infinitas. Esto hace imposible un ataque al sistema mediante la prueba de manera sistemática de todas y cada una de las claves posibles, lo que se conoce como un ataque por fuerza bruta, ya que el número de posibilidades es suficientemente grande como para hacer inútil el intento.

Vigenère publicó en 1586 su visión de la criptografía, incorporando este método en una obra titulada *Traicté des chiffres* . Era un avance enorme, pero sorprendentemente no tuvo el uso que el sentido común parece recomendar. En su lugar, muchos gobiernos y diplomáticos siguieron utilizando métodos anteriores, nomenclátores sencillos e incluso sistemas basados en ideas más o menos ocurrentes, pero débiles ante el ataque serio de un concienzudo criptoanalista.

Solo el paso del tiempo hizo que estos avances en la criptografía se fueran extendiendo por los estados y los gobiernos europeos, consiguiendo que los conocimientos se homogeneizaran y se fueran dejando de lado los métodos de cifrado hechos *ad hoc* por cada criptógrafo. Los métodos conocidos pero basados en una clave, siendo esta lo que hay que mantener en secreto, se demostraron como más seguros que la opción de idear un sistema de cifrado propio e intentar mantenerlo en secreto. Los criptoanalistas buscaban un fallo en el sistema, y habitualmente lo encontraban, lo que hacía que todo se desmoronara, dejando las comunicaciones abiertas y sin protección. Llegados a este punto, cuando un método criptográfico de este tipo se rompía, había que comenzar de cero. Con el método de Vigenère, bastaba con cambiar la clave para volver a unas comunicaciones seguras.

En un ámbito más conceptual, se publicó en 1641 un libro en Gran Bretaña con el título de *Mercurio o el mensajero veloz y secreto* , en el que se muestra cómo un hombre con privacidad y rapidez puede comunicar sus pensamientos a un amigo a cualquier distancia. El autor era John Wilkins, vicario y matemático, que sería rector del Trinity College de Cambridge y uno de los fundadores de la Royal Society. En el libro repasaba muchos códigos y cifras y trataba de ofrecer información

suficiente para conocer y comprender la criptografía. Wilkins proponía determinar un grupo cerrado y reducido de símbolos que sustituyeran a todo el alfabeto. Estos pocos símbolos, combinados de distintas maneras podrían sustituir a todo un alfabeto. Las reflexiones del matemático inglés en torno a la codificación iban al corazón mismo de la información. Para Wilkins la escritura era uno más de los métodos de comunicación de información donde, según dejó escrito, cualquier cosa que sea capaz de presentar una diferencia competente, perceptible para cualquier sentido, puede ser un medio suficiente mediante el cual expresar las cogitaciones. Esta idea está detrás de los métodos de comunicación antiguos basados en humo, en antorchas, en toques de campanas… pero también está la idea básica que hay detrás de las codificaciones que vendrán en el futuro y que siguen hoy plagando nuestro día a día, donde la información se envía y almacena como pulsos eléctricos, como estados binarios en dispositivos y elementos electrónicos.

7. El arte de perlustrar en el siglo XVI

Los cambios sucesivos a lo largo de los siglos XV y XVI fueron colocando a los criptógrafos en primera fila de la lista de miembros necesarios en el servicio de un gobierno o un estado. El aumento de la seguridad, la popularización del conocimiento gracias a los escritos de hombres como los que hemos visto, hacían que lo que parecía una ciencia oscura y sin una solidez matemática se fuera convirtiendo en una disciplina con ciertas certezas. Los nomenclátores seguían usándose, así como los códigos y las soluciones más o menos ocurrentes, pero cada vez había más expertos que incorporaban conocimientos provenientes del estudio. De igual forma, los criptoanalistas ganaban prestigio, y a pesar de luchar con cifras cada vez más complicadas, la falta de rigor y los métodos tradicionales, que seguían en uso, les permitían apuntarse éxitos a menudo.

El arte de perlustrar o la búsqueda de la contracifra, como se conocía en aquel tiempo en castellano al criptoanálisis, deparó éxitos a algunos y verdaderos problemas a otros. Dice la leyenda que el rey Felipe II llegó a ver la mano del diablo en la labor de los rompedores de cifras, ya que sin la ayuda del maligno no había explicación posible para que sus enemigos conocieran lo que estaba cifrado de tan buena forma.

Esa leyenda de Felipe II y su pensamiento en la mano del diablo, se debe en realidad al francés François Viète. Este era un destacado matemático y además de ser consejero de Enrique III y Felipe IV, prestó sus servicios como criptógrafo. Al servicio de Felipe IV dio verdaderos dolores de cabeza al rey español. Cuando su rey le encargó romper el cifrado de algunas cartas que habían sido capturadas a los españoles, le sirvió de manera ejemplar, ya que fue capaz de poner todas ellas en claro. Dejó escritas las técnicas que usaba para sus criptoanálisis, que giraban en torno al análisis de frecuencias, tanto de letras como de símbolos, bigramas y trigramas, así como en torno a algunos trucos para localizar vocales y consonantes. Estos textos, por cierto, se dieron por perdidos durante siglos, hasta que finalmente fueron localizados en los archivos. Como vemos, Viète hacía uso de las técnicas conocidas.

Cuando en España supieron que su cifra no era segura y que los franceses leían sin problemas su correspondencia, tomaron ciertas medidas. Ya saben que unas veces se gana y otras se aprende, y en este caso los españoles aprendieron que debían mejorar sus cifras. Más allá del cambio de cifra y del aumento de las precauciones en su uso y en las comunicaciones, poco se podía hacer contra Viète por violar la correspondencia real filipina, ya que al fin y al cabo era fiel servidor de su señor. Aun así, Felipe II trató de jugar sus cartas y denunció ante el Vaticano al criptoanalista francés, acusándole de brujería y de tratos con el diablo. De aquí viene, con toda seguridad, la leyenda de que el rey prudente creía que el diablo había tenido que ver con la ruptura de sus

cifras. Una leyenda que está en gran parte de la literatura especializada en criptografía, pero, teniendo en cuenta el conocimiento que Felipe II tenía de las cifras, de su uso y de sus debilidades, lo más razonable es pensar que el rey supiera que no hacía falta un diablo para comprometer una cifra. Tan solo una buena cabeza, método y tiempo. El Papa, que también conocía con detalle lo que podía hacer un buen perlustrador, dejó pasar la denuncia y anuló la jugada del rey español para que el francés pagara de algún modo lo que había hecho. Si el Papa hubiera optado por otra postura, una acusación formal de brujería hecha desde el Vaticano habría supuesto algunos problemas para Viète.

No todo eran virtudes, no obstante, en este perlustrador francés. Según parece era poco discreto, una cualidad que nunca sobra en el ámbito del espionaje y las cifras. Habiendo roto una cifra veneciana, no pudo aguantar su orgullo y su lengua e hizo pública la hazaña, delante del propio embajador veneciano en París, Giovanni Mocenigo. Le contó ufano que su país había capturado cartas del rey de España, y de otros personajes importantes, y que en todos los casos él había sido capaz de conocer lo que decían esas cartas, de descifrarlas, en definitiva. Incluso, en un alarde de incontinencia, llegó a insinuar al propio embajador veneciano que conocía la cifra de su república. Viète le mostró cartas descifradas y le dio algún detalle de la cifra veneciana, para que el otro no dudara de su palabra.

Como era de esperar, el embajador puso en conocimiento del gobierno veneciano, el Consejo de los Diez, todos estos detalles en junio de 1595. No tardaron más que unos días en cambiar su cifra en la república y por lo tanto Francia perdió su ventaja, al fin y al cabo, por la falta de discreción de Viète.

No es de extrañar esta reacción de Venecia, entre otras cosas porque fue uno de los lugares donde los hombres de cifras tuvieron más relevancia y conocimiento, aunque cada estado tenía su experto. El Vaticano tenía a su servicio a Mateo Argenti, que escribió un tratado donde recogía veinte formas de cifrar distintas y decenas de alfabetos criptográficos. En el bando español hubo también hombres cuya vida se dedicó a las cifras, siempre al servicio de su rey. Es el caso de Luis Valle de la Cerda, que trabajó para Juan de Idiáquez y Olazábal, que a lo largo de su vida fue embajador del Imperio en Génova y Venecia, secretario y consejero de Felipe II, entre otros cargos. Los venecianos contaron con Pietro Partenio y Agostino Armadi, por ejemplo, y se tomaban la criptografía con seriedad y rigor, convocando concursos entre los descifradores para diseñar nuevos métodos de cifrado.

Venecia disfrutó durante las primeras décadas del siglo XVI de la mejor red de informadores de Europa, gracias a la acción diplomática y también a la red de agentes que le proveían de información, tanto en el oeste como, especialmente, en el este. Los otomanos habían perdido terreno en el arte del cifrado, no solo con respecto a Europa, sino también con respecto a su propio pasado. Una muestra clara de esto la tenemos en 1567, muy avanzado ya el siglo, cuando las autoridades de

la Sublime Puerta dieron orden al bailo veneciano, es decir, al embajador de Venecia, de no enviar más comunicaciones cifradas a su república veneciana, a menos que proporcionara primero los detalles del cifrado que estaba utilizando. Este caso muestra, por una parte, la incapacidad de los otomanos para romper el método usado por los venecianos, y por otra el descaro total con respecto a la seguridad de las comunicaciones, ya que estaban revelando que lo que enviaba el bailo a Venecia era capturado y, al estar cifrado, no podían leerlo. Es cierto que también es un caso de ingenuidad, en mi opinión, por parte de las autoridades de la Sublime Puerta, si esperaban que por emitir una orden al respecto los venecianos iban a dejar de enviar y recibir con su bailo comunicaciones cifradas, secretas y, seguramente, seguras. En 1570, el gran visir Sokollu Mehmet Bajá, que lo fue bajo tres sultanes diferentes, pidió al representante de Venecia en su territorio que le ayudara a formar en el cifrado a algún funcionario de su entorno, petición que no fue atendida, como era de esperar. Cuando esto ocurría entre Venecia y el Imperio otomano, ya era conocido en toda Europa el gran nivel de los criptógrafos venecianos, que desde décadas antes, desde comienzos de siglo, habían destacado.

Venecia tenía entre su personal dedicado a las cifras a uno de los más destacados criptógrafos de la época, Giovanni Soro, y ya hemos visto que compartir conocimiento entre estados no era lo más común, por lo que un experto, que sí formaba a colegas en su mismo estado, era una ventaja importante. Bajo la tutela y control directo del Consejo de los Diez, la labor de los criptógrafos se volvió clave. El Consejo de los Diez era elegido anualmente por el Gran Consejo de Venecia y su finalidad era proteger al propio Estado veneciano, detectando y desbaratando las revueltas internas y controlando la actividad internacional relacionada con el espionaje, los intereses cruzados entre estados, las influencias ocultas… El Consejo de los Diez vendría a ser el equivalente a la policía política o a parte de los servicios secretos que habitualmente han existido en los últimos siglos. Como ya hemos indicado, la existencia de tratados y la popularización de la criptografía permitían que las bases de su conocimiento pudieran ser aprendidas de manera relativamente sencilla, por lo que no es de extrañar que Soro supiera de los logros de gente como Alberti y el resto de pioneros de los que ya hemos hablado.

Soro era el responsable de las cifras y los códigos ya en 1506 y se mantuvo unido a este mundo hasta su muerte en 1544. Por ello, no es de extrañar que cuando el ejército de Maximiliano I de Habsburgo, a la sazón emperador del Sacro Imperio Romano Germánico, y los demás miembros de la Liga de Cambrai, con Francia, Aragón y el papado, se erigió como una amenaza seria para Venecia, los mensajes cifrados fueran a parar a manos de Soro cuando eran capturados a dicho ejército por los informadores de Venecia. Soro tenía una sala del Palacio Ducal, donde trabajaba. Así ocurrió con una carta escrita por el comandante de las fuerzas de Maximiliano I, Marco Antonio Colonna, enviada en abril de 1516 a su emperador. El trabajo de criptoanálisis no debió de ser sencillo, pero cuando Soro logró saber lo que decía el mensaje, la situación cambió sensiblemente a favor de los venecianos. Como ocurre en ocasiones, tan solo conocer el estado del enemigo es

una ventaja definitiva. Colonna, el condotiero de las tropas imperiales, jefe de los mercenarios que estaban al servicio del emperador, pedía 20.000 ducados de manera inmediata, debido a que se había quedado sin dinero con el que pagar y mantener a sus tropas. La urgencia y lo crítico de la situación lo denotaba el propio texto, donde el condotiero pedía ese importe para alimentar y pagar a sus tropas y si no podía hacerlo, le pedía que el propio Maximiliano I se personara en Lodi, la ciudad de Lombardía donde estaban las tropas, para ponerse al frente de ellas.

La fama de Soro se extendió entre los aliados y enemigos de Venecia ya mucho antes de que ocurriera lo de la carta de Colonna. Unos años antes, en 1510, Roma pedía su ayuda en algunas ocasiones para intentar descifrar mensajes que había capturado o conocido y a los que su propio personal no era capaz de sacar partido. Y esas peticiones se repitieron durante mucho tiempo, ya que hay constancia de que en 1526 el papa Clemente VII le hizo al menos dos encargos y en ambos casos Soro fue capaz de descifrar lo que el Papa le entregó. Se trataba de varias cartas de Carlos V a su emisario en Roma, así como de un mensaje del duque de Ferrara a su embajador en España. No parece muy razonable que Venecia hiciera gala entre los otros estados de su capacidad para el cifrado y el descifrado, pero lo cierto es que así fue. Una de las posibles razones para ello puede estar en que se utilizaran los servicios de Soro para ganar aliados o para ayudar a estos en determinados momentos. Un hecho que apunta en este sentido ocurrió en el caso que acabamos de comentar, en el que el Papa pidió ayuda para conocer los textos de Carlos V, ya que la petición se llevó hasta el Consejo Mayor de Venecia, donde estaba el propio *dux* junto con veintidós consejeros del mayor nivel, para que decidieran al respecto. Como hemos visto, la respuesta fue afirmativa, y sin duda buscaría alguna contrapartida política y diplomática.

Tanta era la confianza del papado en el criptógrafo de los venecianos, que en una ocasión el mismo papa Clemente VII conoció que una de sus cartas cifradas había sido capturada y puesta en manos de los florentinos. Para ser capaz de evaluar la seguridad de su cifra y actuar así en consecuencia, envió su propio mensaje cifrado a Soro, para que lo rompiera. Si Soro lo rompía, era posible que los florentinos pudieran hacerlo. Por contra, si ni siquiera Soro era capaz de hacerlo, su mensaje no serviría de nada a Florencia, porque nunca podrían desentrañarlo. El veneciano respondió al Papa que no había sido capaz de romper su cifra, para tranquilidad del pontífice. Dicho esto, siempre cabe la posibilidad de que el veneciano diera falsa seguridad al Papa sobre su cifra para que este la mantuviera en uso, y una vez rota por él, a pesar de haberle dicho al papado que no había sido capaz de hacerlo, tener las comunicaciones secretas papales a su alcance. No sería extraña esta forma de actuar.

En 1530, cuando el príncipe de Salerno visitó Venecia y fue recibido por el propio dux, pidió ver a tres personas: el bibliotecario de la basílica de San Marcos, Pietro Bembo, que era autor de una de las primeras

gramáticas italianas; el historiador y cronista Marin Sanudo y el «maestro de cifrado», según sus palabras textuales, Giovanni Soro.

A pesar de todo esto, los venecianos sabían que no eran inmunes a que sus propias comunicaciones fuesen capturadas y descifradas y a que algunos fueran poco discretos o imprudentes, actuando de la peor forma que se puede actuar con respecto a la criptografía, esto es, no utilizándola. Así lo pone de manifiesto una nota del Consejo de los Diez de 1539, que indica que, a pesar de todos los esfuerzos hechos, tienen constancia de que algunos de los temas tratados en el Consejo eran conocidos por quien no debía y que aquello suponía un problema grave.

En mayo de 1542, dos años antes de que falleciera Soro y quizás temiendo ese momento, Venecia nombró dos asistentes para que trabajaran junto a él. Los tres compartían una sala en el Palacio Ducal y cuando había alguna cifra que romper, estaban recluidos y casi incomunicados, como esclavos, hasta que eran capaces de hacerlo. Compartían conocimientos entre ellos y Soro documentó sus técnicas, las cifras que había roto y cómo lo había hecho. Cifras italianas, españolas, francesas… pero el libro que escribió se ha perdido, al menos hasta este momento. Tan solo algunas notas y referencias que quedaron escritas en los textos de sus pupilos, que se harían cargo del puesto tras su muerte, nos acercan a Soro. La estela y conocimientos de Soro marcaron a sus sucesores Giovanni Battista de Ludovicis, Girolamo Franceschi o Agostino Amadi. Este último también fue un criptógrafo brillante y un buen divulgador.

En Florencia, a mediados de siglo, destacó un italiano por sus dotes para descifrar mensajes, un hombre llamado Pirrho Musefili. Tanto es así, que entre 1546 y 1557 fueron requeridos sus servicios por algunos de los personajes más importantes de la época, y sus víctimas, por supuesto, también fueron personajes igualmente importantes. Musefili fue capaz de averiguar el significado de los nomenclátores del rey Enrique II de Francia con algunos de sus emisarios, o de algunos de los hombres clave de España en Nápoles. Entre sus clientes estuvieron Fernando Álvarez de Toledo y Pimentel, el gran duque de Alba, o el rey de Inglaterra. Este último le envió un criptograma que habían encontrado en Francia oculto en la suela de unos zapatos dorados. El sucesor de Musefili fue Camillo Giusti, que mantuvo la reputación y éxito de los florentinos en el campo de las cifras, trabajando para los Medici. No es de extrañar, por cierto, que Maquiavelo, en su tratado *El arte de la guerra* , dejara patente la importancia de la criptografía.

En el ámbito del Imperio español, Carlos V continuaría con los usos y formas de sus predecesores, haciendo seguras las comunicaciones con sus embajadas y también con muchos de sus colaboradores. Es el caso del arzobispo de Zaragoza, que intercambiaba correspondencia con el rey usando un pequeño nomenclátor para codificar los mensajes. Otros nomenclátores le servían para comunicarse de manera segura con embajadores, capitanes, consejeros… En 1556 Carlos V renuncia a sus títulos y coronas y deja paso al reinado de su hijo, que gobernará con el

nombre de Felipe II y con el sobrenombre de rey prudente. Esa prudencia y su forma de afrontar la responsabilidad de la corona, con organización y trabajo, nos hacen pensar que la criptografía ocupó el lugar que merecía.

El 24 de mayo de 1556, cuando llevaba tan solo cuatro meses como emperador, Felipe II escribió una carta a Fernando I de Habsburgo, hermano de Carlos V y por lo tanto su tío, para cambiar la cifra que estaban utilizando. Fernando era entonces archiduque de Austria y rey de Hungría y Bohemia, y acabaría siendo emperador del Sacro Imperio Romano Germánico. Sospechaba el rey de España que las cifras que venía usando su padre podían haber sido comprometidas. Exactamente el rey prudente pedía el cambio de la cifra, «no solo por ser antigua y por haber muerto muchos y otros mudados de destino de los que estaban en el secreto, sino por estar también harto divulgada y no convenir por esta razón al buen éxito de los negocios».

La cifra general de Felipe II, como se conoce a la que se implantó con su llegada al trono, era la utilizada para mantener seguras las comunicaciones con las embajadas de los principales lugares fuera de las fronteras del Imperio español. La seguridad de las comunicaciones con Portugal, Flandes, Nápoles, Sicilia, Milán, Roma, Venecia… dependía de ella. Se componía de tres elementos básicos y era un buen sistema para su tiempo. El primero de ellos era un vocabulario de sustitución monoalfabética que incorporaba varias posibles elecciones para algunas de las letras, haciendo así menos vulnerable el sistema al análisis de frecuencias. El segundo elemento era un silabario, que permitía cifrar grupos de dos o tres letras comunes. Y por último había un nomenclátor, un diccionario de sustitución para palabras de uso habitual, como lugares, personas o determinadas acciones.

Cinco meses después de aquella carta de Felipe II a su tío Fernando I, la nueva cifra entró en vigor. Como es lógico, se consideraba indescifrable y resistente a las técnicas criptográficas de la época, pero según un texto del historiador Aloys Meister, de 1906, tan solo tres meses después de implantar la nueva cifra, en febrero de 1557, Tiphon Bencio, un secretario del Papa, se hizo con una carta que había sido enviada al cardenal Francisco Pacecco, que estaba en Siena, y la cifra filipina fue rota. A pesar de esto, no parece que los españoles fueran especialmente torpes como criptógrafos, y se tomaban muy en serio el tema, como demuestra el hecho de que durante el reinado de Felipe II se cambiaran dieciocho veces las cifras. La entrega de cada una de ellas, por cierto, se debía hacer en mano a su destinatario, y se enviaba por canales seguros, como eran navíos de guerra propios o vías bien conocidas. Antes de comenzar a usarla, se esperaba al acuse de recibo por parte del destinatario.

Uno de los peligros más serios para las cifras, desde entonces y hasta ahora, eran los traidores, los funcionarios corruptos o las personas que estaban en el lugar apropiado para aprovecharlo y obtener algún beneficio. Un ejemplo de esto lo tenemos en 1564, cuando Felipe II

ordenó un cambio de cifra en la correspondencia con Francia después de que el embajador en aquel país, Francés de Álava, descubriera que uno de sus sirvientes se había hecho con la cifra y, con toda probabilidad, la había vendido. Esto se repitió en otras ocasiones, como en el caso de Juan del Castillo, que vendió información y cifras a Guillermo de Orange, nada más y nada menos, o el de Gabriel de Zayas, que hizo lo propio con el embajador italiano. A este juego de espías, traidores, robos e intrigas, como era de esperar, también jugaron los españoles.

Felipe II y su administración usaban distintos métodos para hablar con distintos destinatarios. Desde sencillas cifras de sustitución donde cada letra se sustituía por otra, un método muy vulnerable, a cifras más complejas, donde se usaban números y, por supuesto, los nomenclátores, donde se combinaban sustituciones y palabras codificadas directamente. Por esto, no es de extrañar que los conocimientos sobre cifras fueran un requerimiento esencial para los personajes importantes, comenzando por el propio rey.

Es curioso también ver algunos de los métodos esteganográficos que utilizaron los espías del Imperio de Felipe II. Como ya hemos comentado, la esteganografía fue el primer método de ocultación de mensajes puesto en marcha, pero ha sobrevivido con buena salud al paso de los siglos. Por ejemplo, en 1586, Sancho Martínez de Leiva, un caballero importante que combatió en Flandes con Juan de Austria y con el duque de Parma, Alejandro Farnesio, y que llegó a altas posiciones en el Estado, escribió a Juan de Idiáquez hablándole de la conveniencia de contar con los servicios de un italiano que era capaz de escribir con letra minúscula, en papeles igualmente minúsculos. Como argumentos a favor de este italiano, se decía que podía dejar un mensaje escrito en el canto de un papel y escribir en un documento tan pequeño que podría ser escondido en una sortija. No es poco útil esta capacidad, si tenemos en cuenta que Bernardino de Mendoza, militar, diplomático y jefe de espías, dejó escrito en su tratado militar *Teórica y práctica de guerra* , que, para burlar un asedio, se podía escribir en un papel minúsculo un mensaje y meterlo en un cilindro de metal. El hombre que iba a escapar del lugar portando el mensaje tendría que tragarlo y llevarlo dentro de sí, para burlar al enemigo en caso de ser capturado y registrado. También cuenta Mendoza que en alguna ocasión el mensaje se había escrito sobre la espada, por lo que algunos vigilantes llegaban al extremo de revisar y lavar las espadas para evitar que el mensaje se les pasara por alto. Al lavarlas, es de suponer que cualquier tipo de tinta simpática fuera eliminada.

La tinta invisible es otro de los métodos de ocultación utilizados en esta época, por lo que no es de extrañar que cuando se cogiera a un sospechoso, se le levantara la camisa para ver si tenía algún texto escrito, y como precaución frente al uso de alguna tinta invisible, se le lavara bien el pecho y la espalda, para borrar el mensaje si existiera. Los servicios secretos de Felipe II utilizaban la tinta invisible hecha con vitriolo romano, es decir, sulfato, que pulverizaban y mezclaban con

agua. Con el resultado escribían el mensaje sobre el papel, y sobre este escribían un texto normal, inocente y que podía leer cualquiera. Este texto se escribía con carbón de sauce diluido en agua. Para leer el mensaje cifrado, la carta se pulverizaba con galla de Istria, y el texto oculto aparecía como por arte de magia.

También el zumo de limón, así como el de rábano, la cebolla o la tinta de alumbre, que está basada en el sulfato de aluminio, eran sustancias utilizadas en esta época para escribir textos ocultos. Es curiosa la forma en la que el remitente del mensaje indicaba que había algo escrito en la carta con estas tintas invisibles. De otro modo, en muchos casos el receptor no llevaría a cabo el proceso de hacer visible lo escrito. Esto se hacía con determinadas fórmulas pactadas por emisor y receptor. Por ejemplo, si el texto de una carta, escrita por una cara, acababa con un «los amigos os besan las manos», el receptor sabía que a la vuelta de la hoja había un texto escrito con una tinta simpática.

Cuando al comienzo del libro hablábamos de las tintas invisibles, ya comentamos la obra de Diego Fernández, del siglo XVI, sobre la historia del Perú. En esta misma obra se mencionan los cifrados de rejilla ideados por Cardano y publicados en 1550, por lo que es seguro que los españoles los conocían. De hecho, se ha localizado un ejemplar de rejilla utilizado por los servicios de Felipe II. Este método de la rejilla ha sido usado en España, y en la América relacionada con España, durante siglos. En el XIX se seguía utilizando en Perú, y en el siglo XX, cuando José Antonio Primo de Rivera, el fundador de Falange, estaba preso en Alicante, se comunicaba con el exterior utilizando este sencillo método.

Entre los criptógrafos del Imperio español destacó Luis Valle de la Cerda, que además fue una figura clave también en la gestión de la Hacienda imperial. Formado en la Universidad de Salamanca, comenzó muy joven como perlustrador, con tan solo dieciocho años, y cuando Alejandro Farnesio le otorgó el cargo de secretario de cifras, descifró varias cartas del rey francés Enrique III que habían sido capturadas. Su capacidad como criptoanalista llegó hasta los oídos del propio Felipe II, dejando Flandes por una corta temporada, donde estaba el duque de Parma, e instalándose en Madrid a las órdenes directas de Juan de Idiáquez. De vuelta a los Países Bajos, tuvo éxito con la ruptura de la clave de la correspondencia inglesa y su fama se hizo demasiado peligrosa, ya que colocó al español entre los objetivos de los enemigos de su rey. Delataron su nombre y posición como descifrador, por lo que se esforzó en mantenerse discreto y simular otras ocupaciones. La suerte le acompañó cuando, estando preso de los ingleses, fue capaz de mantener la mentira sobre su identidad durante todo el cautiverio, que acabó a costa de dinero propio. Al parecer, la reina inglesa ofrecía una interesante cantidad por el criptógrafo español, por lo que fue todo un éxito escapar de las manos de sus captores sin que se descubriera su verdadera identidad. Siguió trabajando con éxito un tiempo en el ámbito criptográfico, hasta que en 1606 el rey le otorgó un cargo dentro del Consejo de la Santa Cruzada como contador, donde también destacó.

Su labor como descifrador siguió vigente a pesar del cambio de puesto en el Estado español. Incluso con el duque de Lerma, muerto ya Felipe II, se le encargaban trabajos y se le entregaba correspondencia y todo tipo de documentos cifrados.

En 1581 se resolvió que uno de los empleados en los servicios de criptográfica que tenía el Imperio español en Flandes, nacido allí, estaba entregando información sobre las cifras españolas a Philips van Marnix, uno de los líderes flamencos de las revueltas contra Felipe II. Tan importante era este flamenco para sus paisanos que un poema suyo, *Wilhelmus van Nassauwe* , fue empleado como himno de guerra por los holandeses y ha llegado hasta hoy convertido en el himno nacional de Holanda, siendo además el himno nacional más antiguo del mundo. Con la información sobre las cifras españolas que había conseguido en los años anteriores a ese 1581, gracias a la ayuda del traidor a los españoles, fue capaz de descifrar algunas comunicaciones de sus enemigos al más alto nivel. En 1577 hizo público un mensaje que había enviado don Juan de Austria, a la sazón gobernador de los Países Bajos, a su hermano Felipe II, y que había sido capturado en Francia. El mensaje instaba al rey español a aplastar la revuelta holandesa con mano dura y por la fuerza. Frente a esto, don Juan de Austria lanzó una queja por la falta de confidencialidad de su correo, que podría ser tomada en serio, de no ser porque casi todos los países y gobiernos y durante casi todas las épocas, como hemos visto y veremos, han hecho lo mismo de lo que se quejaba. Es más, lo mismo que denunciaba don Juan de Austria lo hacían los servicios de espionaje de su hermano y rey. Decía el gobernador español que tal acción era un insulto notable y un crimen de traición. Que el hecho de interceptar y abrir las cartas de su soberano es un crimen de lesa majestad y que los responsables no pueden excusarse de modo alguno. Manchan su propia reputación, afirmaba don Juan de Austria en su queja, apelando a esa idea que aparece y desaparece a lo largo de la historia, de que los caballeros de honor no leen la correspondencia privada de otros caballeros.

8. Los Rossignol, los Wallis y los gabinetes oscuros

Dentro de la guerra de asedio, la estrategia pasa no pocas veces por asfixiar al ejército que aguanta dentro de la fortificación, evitando que les llegue cualquier provisión o ayuda. Si el bando que está fuera está bien dotado y es paciente, los recursos de los fortificados acabarán por escasear. Este tipo de situaciones suele darse cuando ambas partes son militarmente incapaces de vencer al otro. Es decir, cuando no se puede romper el cerco y penetrar en el lugar fortificado, pero tampoco se puede lanzar un ataque desde dentro que acabe con el problema. En un bloqueo de este tipo y con el tiempo corriendo en su contra, una de las pocas opciones que restan a los asediados para vencer es recibir ayuda desde el exterior. Mientras esto ocurre, en cualquier caso, las tropas de cada lado de las murallas desconocen cuántos recursos, armas y comida le quedan a cada bando para seguir manteniendo el pulso. Saber quién está más cerca del límite es clave.

En abril de 1628 el ejército del rey francés comandado por Enrique II de Borbón sitiaba la ciudad de Réalmont, donde resistía un grupo de hugonotes. Desde las torres de la fortificación los protestantes disparaban al ejército que les atacaba desde fuera y se resistían a rendirse. A su vez, las tropas encerradas recibían las constantes descargas de la artillería del rey. Del asedio se escapó un hombre con un mensaje cifrado, con el objetivo de contactar con refuerzos hugonotes en el exterior y pedir ayuda. No tuvo suerte en su empeño y fue capturado por los hombres del rey de Francia mientras intentaba pasar las líneas del asedio. El mensaje cifrado, por supuesto, también fue interceptado. Aquello evitaba que la ayuda fuera solicitada, lo que era ya una ventaja, pero mientras no fueran capaces de descifrar el texto, los asediadores no sabrían cuál era la situación real de las tropas dentro de la fortificación. Ninguna de las personas cercanas a Enrique II fue capaz de romper la cifra y entonces le recomendaron hacérselo llegar a un hombre que tenía fama de aficionado a la criptografía y de ser bueno en ese tipo de trabajos. Efectivamente, no mucho después de que pusieran el mensaje interceptado a disposición de ese hombre, el texto estaba puesto en claro. La carta era una petición de ayuda, como se suponía, pero además exponía la desesperada situación de los protestantes dentro de Réalmont. Estaban agotando sus municiones y, salvo que fueran ayudados de manera urgente, tendrían que rendirse.

Enrique II de Borbón devolvió el mensaje cifrado que habían capturado a los asediados y les hizo saber que estaba al corriente de su crítica situación, aunque hasta aquel momento no daban señales de estar en una posición precaria y seguían resistiendo. Esto fue suficiente para que los hugonotes comprendieran que habían perdido toda posibilidad de vencer en aquella batalla y que por lo tanto era absurdo seguir

resistiendo. Capitularon y dieron así la victoria a los católicos, que habían vencido gracias a Antoine Rossignol, el criptógrafo aficionado.

Cuando esta historia llegó a oídos del poderoso cardenal Richelieu, hizo llamar a Rossignol a su servicio. Estaba entonces en marcha otro asedio, el de La Rochelle, una plaza en la costa de la Francia atlántica, que hasta aquel momento había sido un lugar seguro para los hugonotes pero que las tropas del rey Luis XIII de Francia, con Richelieu al frente, estaban atacando. Como había ocurrido en Réalmont, los asediadores habían capturado algunas de las comunicaciones que se habían enviado desde La Rochelle. De nuevo Antoine Rossignol demostró sus dotes para la criptografía rompiendo sin problemas las cifras y puso en conocimiento de los católicos que los asediados estaban pasando hambre y que esperaban la ayuda de los ingleses por mar. Richelieu ordenó la construcción de un dique que cortara el acceso a la ciudad desde el mar, y por lo tanto bloqueara la posible ayuda de los ingleses. Navíos hundidos y un trabajo de ingeniera ímprobo, dieron lugar al bloqueo del acceso por mar. Preparándose para combatir con la flota inglesa, los católicos franceses desplegaron cañones apuntando hacia el Atlántico. La ayuda del otro lado del mar llegó para los hugonotes, pero cuando los ingleses repararon en lo que tenían enfrente, un bloqueo, y a los franceses bien preparados para combatirles, no hicieron muchos esfuerzos por romper la barrera y socorrer a los asediados. Un mes después de aquel socorro fallido, los hugonotes rendían la ciudad de La Rochelle al cardenal Richelieu. De nuevo un criptoanalista, de nuevo Rossignol, había sido una pieza importante en la victoria del rey de Francia.

Dos años después de estos hechos, en 1630, Antoine Rossignol trabajaba a tiempo completo para el rey de Francia y este le pagaba generosamente. Tanto, que el criptoanalista tuvo su propio castillo cerca de París, rodeado por unos jardines diseñados por Jean Le Nôtre, el jardinero del rey. Los servicios que ofrecía bien merecían esos pagos, según parece.

En el asedio de Hesdin, por ejemplo, los católicos fueron capaces, una vez más, de conocer la precaria situación del enemigo gracias a la captura de un mensaje cifrado que fue puesto en claro por Rossignol. No contentos con esto, los reales escribieron un mensaje para su enemigo, haciéndole saber que conocían su situación y lo inútil que era resistir, ya que la ayuda que habían intentado solicitar nunca llegaría. Ese mensaje al enemigo fue codificado usando la misma cifra con la que habían escrito el mensaje de auxilio que había sido capturado.

En 1643 la corona francesa pasó a Luis XIV, el Rey Sol, después de la muerte de su padre. Tenía entonces el rey tan solo cuatro años de vida y entre las muchas cosas que heredó estaban los servicios de Rossignol. En esos años de servicio a la corona francesa y a sus hombres y mujeres principales, el criptógrafo deshizo traiciones, hizo claros mensajes cifrados entre embajadas y ayudó a que mucha de la información que los enemigos de la corona creían secreta para los reales, no lo fuera.

Richelieu disfrutó de sus servicios, como ya hemos visto, y su sucesor como primer ministro, el cardenal Mazarino, no lo hizo menos. Este nombró a Rossignol miembro de la Cámara de Cuentas y del Consejo de Estado, lo que revela la confianza que tenía en él y lo consciente que era de que tenerlo al tanto de los asuntos más importantes sería un medio para prevenir problemas y ataques. Además, estos cargos también dejan claro que Antoine Rossignol era un hombre de política y de saberes más amplios que los meramente criptográficos. Durante el reinado de Luis XIV, Rossignol trabajaba en una sala contigua a la del rey, en Versalles, lo que le permitía servirle en tres ámbitos clave: descifrando los mensajes de terceros, cifrando los mensajes propios y aconsejando al rey cuando su opinión o ayuda era requerida.

En su ámbito principal, en la criptografía, no solo actuó como criptoanalista, rompiendo las cifras de los enemigos de la corona, sino que también mejoró la propia seguridad de las comunicaciones reales. Mejoró los nomenclátores que se utilizaban para cifrar los mensajes del rey y sus allegados, llevando a Francia a donde no había llegado en siglos, en todo lo relacionado con las cifras. Como es lógico, descifrar sistemas de cifrado y codificación conlleva conocer los puntos débiles de estos y por lo tanto coloca a un buen criptoanalista, como era el francés, en disposición de mejorar sus propios métodos de cifrado, evitando precisamente esos errores que conoce y explota en los otros. Tanto es así que se conoce el cifrado de los Rossignol como Le Grand Chiffre, es decir, la Gran Cifra.

Rossignol se había percatado de que los nomenclátores solían listar los elementos, tanto los textos en claro como los cifrados, en orden alfabético o numérico, si se sustituían letras por números, y colocando de manera paralela unos y otros. Esta era la práctica habitual desde dos siglos antes, desde que se habían hecho populares en el Renacimiento. En contadas excepciones, tan solo cuando los nomenclátores eran muy cortos y por lo tanto podían ser caóticos, no ocurría este fallo de escribirlos de modo ordenado. Fue Rossignol quien se dio cuenta de que ese orden le ayudaba a desentramar los nomenclátores y a tener un hilo por el que empezar a tirar en su análisis. Por ejemplo, si averiguaba o sospechaba que una determinada palabra, pongamos «defender», equivalía al número 50, y otra como «Italia» era representada en el texto cifrado por el número 85, sabía que un «atacar» era un número por debajo de 50 y que «Francia» sería un número entre 50 y 85, ya que Francia está en el orden alfabético entre «defender» e «Italia». Estas rendijas, que pueden parecer sin importancia, son los lugares por los que se cuela un criptoanalista para comenzar a hacer conjeturas e hipótesis e ir probando cuáles de ellas le hacen avanzar por el buen camino. El proceso, como supondrán, se acelera a medida que va penetrando en la cifra, y si bien puede ser complicado conocer las primeras palabras, una vez que se tienen algunas pistas toda la cifra se desmorona como un castillo de naipes, dejando ver claramente el mensaje original, aquello que precisamente se quería ocultar.

Con esto en la cabeza, Rossignol rompió en sus propios nomenclátores esa regla no escrita, desordenando las relaciones. Así, aunque la lista de palabras clave en el nomenclátor estaba ordenada, los números por los que se sustituía cada una de esas palabras no llevaban ningún orden. Para facilitar la labor de codificación y decodificación, Rossignol usaba dos listas. La primera, la que se utilizaba para codificar, tenía las palabras en claro ordenadas alfabéticamente y, como ya hemos dicho, los códigos asignados a cada palabra no guardaban orden alguno. Esto hacía más compleja la decodificación, ya que habría que buscar el número del texto codificado en la lista para buscar su equivalencia, sin que esta lista ayudara con su orden al proceso. Para hacer más ágil este trabajo de decodificación, Rossignol creó una segunda lista, la de decodificar, donde los códigos estaban ordenados y lo que aparecía desordenado eran las palabras en claro. Esto muestra que el francés conocía bien su trabajo y sabía qué implicaba cada aspecto del mismo, por lo que intentaba optimizarlo. Los nomenclátores de Rossignol eran algo así como un diccionario bilingüe de los actuales, donde podemos ir de un idioma a otro y del otro al uno, usando diferentes partes del diccionario y siempre utilizando la búsqueda alfabética.

Los nomenclátores se iban haciendo cada vez más largos y completos, ya que cuanto mayor fuera el número de palabras codificadas a través del nomenclátor y no a través de un método criptográfico de sustitución, mayor sería la seguridad de las comunicaciones. A finales del siglo XVII, algunos nomenclátores tenían hasta 3.000 entradas. Esto hizo que fuera muy complicado mantener ese doble libro ordenado que había diseñado Antoine Rossignol y se optó por una solución intermedia, a pesar de que se perdía algo de seguridad. El listado de palabras en claro se dividía por bloques y se mantenía el orden dentro de los mismos, aunque no entre los bloques. Por ejemplo, en la cifra general de la corona española de 1677, las palabras del nomenclátor entre las sílabas bal y ble se correspondían con números entre el 131 y el 149, pero las inmediatamente siguientes correspondían a otro bloque numérico diferente que comenzaba por el 322.

Por todo esto Rossignol se convirtió en un personaje habitual en los textos de la época relativos al Rey Sol. Por ejemplo, en las populares *Memorias* de Louis de Rouvroy, duque de Saint-Simon, donde se trata acerca de la corte de Luis XIV, aparece Antoine Rossignol descrito como el más capacitado descifrador de Europa. No se le escapaba cifra alguna, asegura el conde, e incluso algunas era capaz de leerlas inmediatamente, lo que le daba importancia como hombre y mucha cercanía al rey. Todos los países y muchos hombres importantes tenían criptógrafos a los que pedían ayuda, como ya hemos visto con los venecianos. No era extraño que embajadores, espías, jefes militares… tuvieran conocimientos de criptografía y fueran capaces de codificar e incluso de hacer algunos criptoanálisis. Pero por encima de todos ellos la corte francesa tenía a su servicio a un hombre de sumo valor dedicado en exclusiva a la criptografía y al que habían otorgado plena confianza. Rossignol falleció en diciembre de 1682, a pocos días de cumplir los ochenta y tres años y aun entonces, y a pesar de estar

retirado, el rey seguía visitándolo y reconociendo su valor y su servicio a Francia.

Muerto el primer Rossignol criptógrafo, uno de sus hijos continuó con lo que podríamos denominar el oficio familiar. Su padre había invertido tiempo y esfuerzo en su formación y Bonaventure Rossignol fue el segundo criptógrafo francés de la saga. Si hacemos caso a las fuentes de la época, parece que las enseñanzas del padre calaron en el hijo, porque se le consideraba excelente en aquello que hacía. Como su padre, formaba parte de la Cámara de Cuentas y prestó grandes servicios.

Bonaventure Rossignol tuvo dos hijos, y cuando el primogénito falleció prematuramente, el segundo cambió la carrera eclesiástica a la que estaba orientado por el negocio familiar. El nombre de este tercer criptógrafo de la saga era casi una señal, ya que se llamaba Antoine-Bonaventure, es decir, llevaba los nombres de su abuelo y de su padre. Cuando este tercer Rossignol falleció, se llevó consigo al otro mundo las claves para descifrar los papeles de Estado que tenía en su poder y que estaban cifrados.

A finales del siglo XIX, en 1890, Victor Gendron, un historiador militar que estaba investigando las campañas de Luis XIV, descubrió varias cartas de este rey codificadas con la cifra de los Rossignol. Un oficial del ejército francés de la Tercera República llamado Étienne Bazeries, que trabajaba con códigos y cifras dentro de su servicio como militar, dedicó tres años a desentrañar las cifras de los Rossignol que había descubierto Gendron. Durante dos siglos, ni siquiera los franceses pudieron leer los textos propios que habían quedado cifrados por el último Rossignol, pero eso no desalentó a Bazeries, que tras estudiar los números que aparecían en las cartas, se dio cuenta de que había casi seiscientos diferentes. Pensó que estaba ante una cifra homofónica, es decir, una cifra en la que cada letra se podía escribir utilizando varios números, haciendo así que el análisis de frecuencias no fuera válido. Dedicó mucho esfuerzo a investigar esa idea, pero lamentablemente acabó siendo una vía muerta. Lo siguiente que probó fue si se habían usado números para sustituir pares de letras, en lugar de letras aisladas. Hizo un análisis de frecuencia de los pares más recurrentes en francés y contrastó esos pares con los números más habituales en las cifras. De nuevo, una vía muerta. El siguiente ataque fue similar a este último, pero utilizando sílabas en lugar de pares de letras. Emparejó los números más frecuentes en las cartas cifradas con las sílabas más comunes en el idioma francés. No llegaba a ninguna conclusión clara, hasta que probó una idea que le vino a la cabeza y que tenía que ver con todas esas pruebas sobre sílabas y pares de letras. Se dio cuenta de que la secuencia 124-22-125-46-345 aparecía muy a menudo en algunas cartas y pensó que debía de ser una expresión habitual. Probó con *les ennemis* , es decir, los enemigos. Según su hipótesis, esos cinco números correspondían con les-en-ne-mi-s. Partiendo de ahí, sustituyó todas las apariciones de cada uno de esos números por las letras correspondientes, apoyándose en esa semilla que le otorgaba la

expresión «los enemigos». A medida que hacía sustituciones, aparecían nuevas hipótesis para otros números, que encajaban en los trozos del texto en claro que se iba vislumbrando. Cada nueva palabra descubierta aportaba nuevas equivalencias para números que eran la semilla para descifrar nuevas palabras y por lo tanto nuevos números. No todo era tan sencillo, sino que los Rossignol, verdaderos maestros en su arte, habían complicado la cifra incluyendo trampas, números nulos, que no significaban nada, y hasta números que no solo no significaban nada, sino que indicaban que el número anterior no debía ser tenido en cuenta. Desmadejar todo aquello le llevó un tiempo a Bazeries, pero seguro que tanto esfuerzo mereció la pena cuando cayó en la cuenta de que estaba siendo el primer hombre en doscientos años en leer la correspondencia más secreta de algunos reyes franceses.

En este punto, volviendo a los tiempos anteriores, los franceses conocían perfectamente la importancia de las cifras y el valor que aportaban al poder, tanto para atacar como para defenderse, en el más amplio sentido. Por tanto, no es de extrañar que llegaran a la conclusión de que no era suficiente con confiar todo este ámbito a los Rossignol. Pusieron en marcha un plan para reclutar criptógrafos y criptoanalistas, llegaron a ofrecer premios en metálico a quien diseñara una cifra fuerte y a quien consiguiera romperla. Con esta fuente de expertos, Francia creó el organismo que se conoce como Cabinet Noir, que traducido literalmente sería cámara o gabinete oscuro, y que se ocupaba de descifrar todas las comunicaciones secretas que la corona era capaz de capturar. Los espías y personajes de todo tipo al servicio del rey, bien por lealtad o bien por un pago, proveían de textos cifrados a ese gabinete oscuro que se encargaba de poner los textos en claro y hacérselos llegar al rey, a sus consejeros, al ejército… las comunicaciones diplomáticas de otros estados con sus representantes en Francia se movían con un flujo constante por las mesas de los criptógrafos franceses al comenzar el siglo XVIII. Esa idea y ese modo de trabajo inauguró una nueva época en Europa, como veremos.

La importancia que Francia otorgaba a la criptografía también afectaba a la seriedad y rigor con la que se tomaban la codificación de sus propias comunicaciones. Todos los diplomáticos y todos aquellos que hacían uso de los nomenclátores reales tenían instrucciones estrictas sobre cómo trabajar y qué precauciones tomar. Si hay algo que nunca sobra en el mundo de los espías, y por extensión en este mundo de los mensajes secretos y los códigos, es la desconfianza y la precaución. Como dijo Mark Twain, el famoso escritor estadounidense del siglo XIX y primeros del XX: «No es lo que no sabes lo que te mete en problemas, es lo que sabes con certeza que, simplemente, no es como tú crees». De forma paralela a esa idea de Twain, el gran problema no está en saber que tus comunicaciones no son seguras, sino en creer que sí lo son cuando no es cierto.

Luis XV aprendió esta lección en 1774, con una desagradable sorpresa. Le entregaron un paquete de cartas que había sido comprado en Viena por 1.000 ducados. Además de la correspondencia entre el rey de Prusia

y los agentes de este en varios lugares, por supuesto, también en Francia, el paquete contenía cartas francesas. Luis XV las creía seguras porque habían sido cifradas con todo el cuidado y rigor, usando las cifras que sus asesores tenían como irrompibles. Esas cartas habían sido descifradas y el texto en claro estaba ahora ante los ojos de Luis XV, y por lo tanto también había estado ante los ojos del rey de Prusia. Esto significaba una cosa: el gabinete oscuro, el Cabinet Noir, no era un servicio que tuvieran solo los reyes franceses. De hecho, España tenía el suyo propio y los ingleses también habían puesto en marcha su Black Chamber. El gabinete oscuro vienés funcionaba con una eficiencia impresionante. El rey de Francia decidió que quizás la ruta vienesa de información era más valiosa que la suya propia. Así, aquel paquete de cartas que habían obtenido los hombres de la embajada francesa en Viena, fue solo el primero de muchos. Dos veces a la semana, los franceses se encontraban con un discreto proveedor de información que, a cambio de dinero, les iba entregando documentos provenientes del gabinete oscuro de Viena, es decir, del servicio de captura y desciframiento de información austriaco. Toda la correspondencia que pasaba por Viena era abierta, copiada, descifrada y entregada a su rey. Por supuesto, la carta original volvía a ser cerrada como si nada hubiera pasado, y seguía su camino. También llegaban hasta los ojos del rey Luis XV de Francia aquellos mensajes, en un envío especial que obtenía puntualmente dos veces por semana. El gran juego del espionaje, como vemos, tenía una densa red de conexión entre los distintos contrincantes y todos pasaban cartas por debajo de la mesa.

Durante el siglo XVIII los gabinetes oscuros eran un elemento habitual al servicio de los estados y del poder de cada país. En el fondo no era algo nuevo que espías a tiempo completo o sencillamente personas que veían una oportunidad de ganar dinero se hicieran con correspondencia ajena y con documentación de otros países, en muchos casos sin que existiera un enfrentamiento de ningún tipo entre los estados. Todo ello se hacía para que los servicios criptográficos los pusieran en claro. Lo que había cambiado era la institucionalización de estos gabinetes oscuros de documentos cifrados, y la sistematización de esta forma de trabajo. En Europa, el gabinete oscuro que mejor fue capaz de llegar a ese nivel de profesionalización y sistematización fue, como se ha consignado, el vienés, el Geheime Kabinettskanzlei, cuya traducción directa sería más bien oficina del gabinete secreto, y no oscuro. Su funcionamiento era tan sobresaliente que no es de extrañar que incluso otros servicios de espionaje, como el francés, trataran de aprovecharse de sus resultados, como hemos visto.

Ese nombre de Oficina del Gabinete Secreto no fue el único que tuvo desde su creación en el año 1711, sino que lo cambió varias veces para ocultar, en la medida de lo posible, su existencia y su función. La red postal estaba infiltrada en sus puntos más importantes, y en Frankfurt, Ratisbona, Augsburgo y Núremberg, entre otros lugares, había delegaciones de esta institución no tan secreta que efectuaban el trabajo de captura y copia del correo. Todo el correo copiado era enviado a Viena. En algunos casos incluso las cartas originales, antes de ser abiertas y copiadas, eran enviadas a Viena, donde estaban los más

capaces en cada una de las labores del gabinete. Esto ocurría cuando alguna de las valijas estaba especialmente bien sellada y se temía que el proceso de apertura para copiar y de cierre posterior no pudiera pasar desapercibido.

Todos los días, a las 07.00 horas, la correspondencia que iba dirigida a cualquiera de las embajadas que otros estados tenían en Viena, era entregada al gabinete secreto, comenzando así un trabajo en el que tan importante era la rapidez con que se efectuaba como la falta de señales o secuelas que dejaba. Todas esas valijas diplomáticas, usando la terminología actual, estaban debidamente selladas, habitualmente con lacre, por lo que el primer paso era soltar ese sello, normalmente con algo tan sencillo como una vela. Una vez abierto el paquete de cartas diplomáticas, se apuntaba cuidadosamente el orden en el que las cartas se encontraban en el paquete, que bien podría ser una carpeta de cuero o algo similar, para volverlas a poner en el mismo orden y en las mismas posiciones al finalizar. Hecho esto, todas las cartas de cada paquete pasaban a los responsables máximos del gabinete, que decidían qué cartas, o incluso qué partes de algunas cartas, merecía la pena copiar e investigar y cuáles no. No toda la correspondencia era cifrada, como es lógico, y esas cartas en claro eran copiadas de manera rápida por los empleados, en algunos casos incluso utilizando alguna forma de taquigrafía o al dictado, para que el proceso fuera lo más rápido posible. La celeridad era importante, ya que un retraso en el correo podría hacer sospechar a la embajada que algo podría haber pasado por el camino, como efectivamente estaba ocurriendo. Sabemos que hay muchos casos o problemas que pueden retrasar el correo, pero en el mundo de la diplomacia y el espionaje, un nivel de sospecha elevado nunca está de más, por lo que no dar pie a que esa sospecha nazca es una buena premisa.

Todos los idiomas habituales en la Europa de la época eran conocidos en el gabinete. Había traductores que conocían varios de ellos y siempre estaban dispuestos. Un hombre dotado para los idiomas, como es lógico, era persona clave al servicio del gabinete. Por ejemplo, cuando se decidió que el armenio también era un idioma relevante en la correspondencia incautada, uno de estos funcionarios políglotas recibió el encargo de aprenderlo, y le dieron 500 florines por ese nuevo conocimiento extra que ponía al servicio de la institución. Pudiera uno pensar que, controlados y espiados los países relevantes, los verdaderos enemigos de un importante imperio como el austriaco, gran parte del problema estaba resuelto y no se habría de prestar atención a los países de segunda fila. Tomar esta decisión sería tanto como perder la oportunidad de conocer las relaciones entre estos países secundarios y los principales, de cuyos acuerdos uno puede aprender. También sería renunciar a la posibilidad de conocer algo que un espía al servicio de cualquiera de ellos descubriera sobre uno mismo. En resumen, la información nunca está de más. Por cierto, durante la Guerra Fría, el espionaje de esos países secundarios se mostró como algo relevante.

Si alguna carta cifrada aparecía en una valija, es decir, una misiva con símbolos extraños o cuyo lenguaje no fuera claramente identificado, tomaba un rumbo diferente dentro del gabinete secreto. Con toda probabilidad, una carta cifrada ocultaba dentro de sí un mensaje interesante, ya que se habían tomado la molestia de cifrarla.

Copiada toda la correspondencia seleccionada de cada una de las valijas, y cuando solo habían pasado un par de horas desde el comienzo del trabajo, las cartas se colocaban cuidadosamente de nuevo en su paquete, en la misma posición y en el mismo orden en el que fueron encontradas, y se resellaba la valija. El gabinete secreto vienés tenía réplicas de los sellos que rompía para abrir las valijas, forjados copiando un original. El lacre, la cera o el material que tuviera el sello original abierto al comienzo del proceso, se había guardado y era usado de nuevo, para que el paquete final que volvía al camino del correo, a pesar de haber sido destripado, no mostrara ninguna señal de haber sido violado. En torno las 09.30, todos los envíos diplomáticos del día estaban de vuelta en la oficina de correos.

Poco después llegaba hasta allí el correo diplomático que pasaba por Viena, con destino a otro lugar, y se repetía el proceso. Finalizada esa parte del trabajo, llegaban las cartas y documentos incautados por la policía en su labor de control político y, al finalizar el día, el proceso comenzaba con todas las cartas que partían de Viena. Esto es, la correspondencia que las embajadas y los diplomáticos de otros países enviaban desde Viena, y también desde otras ciudades importantes, era espiada y parte de ella iba al gabinete secreto para ser esclarecida.

La cantidad de información que se generaba a diario con todos estos procesos de violación del correo no era poca, y cerca de un centenar de cartas eran seleccionadas cada día para ser copiadas y posteriormente investigadas.

No es de extrañar que este metódico y constante trabajo fuera levantando las sospechas de los enemigos y los amigos de Austria. Saber lo que uno mismo hacía en su propio país le debería llevar a sospechar que otros mantenían un organismo similar. Por si las sospechas no fueran suficiente, en algunos casos, contados casos para el volumen de valijas abiertas cada día y la velocidad a la que debía hacerse el trabajo, se cometieron errores. Por ejemplo, en una ocasión, al volver a sellar una carta destinada al duque de Módena, equivocaron el sello en el gabinete, usando el del duque de Parma, que era similar. El destinatario, al ir a abrir su correspondencia, cayó en el error y asumió, como era de esperar, que su correo había sido violado y que se había resellado para hacerlo pasar por confidencial cuando no lo era. El duque de Módena envió el sello del de Parma que había recibo por error cerrando su carta junto con una nota en la que le decía claramente que aquello significaba que no solo él, el duque de Módena, estaba bajo vigilancia y su correo era leído, sino que también el de Parma estaba en esa misma situación. De otro modo, no tenía sentido que ambos sellos estuvieran en manos del tercero que estaba leyendo su correo

pretendidamente secreto. Sabiendo todo esto, no es extraño que la información más delicada y conflictiva se cifrara como recurso para mantener los mensajes fuera del alcance de los ojos del resto de estados. Como veremos claramente en otros momentos de la historia, no es suficiente con descifrar un mensaje, sino que hay que hacerlo en un tiempo reducido, ya que no es extraño que cierta información caduque, o pierda valor si es conocida unos días o incluso unas horas después de ser interceptada. Por esta razón el cifrado también es una garantía, porque incluso cuando se sabe que el método criptográfico puede ser desentrañado, si esa labor lleva tiempo, la cifra también cumple con su cometido, al menos en parte.

Por supuesto, toda esta maquinaria vienesa no hubiera tenido sentido sin un engranaje dedicado a romper las cifras, sin un sistema de criptoanálisis igualmente metódico y confidencial. En estas labores el gabinete secreto vienés era igual de efectivo que en el resto del proceso. De hecho, aplicaban a los criptoanalistas una forma de motivación basada en los retos y los objetivos. El tiempo en el que se debían descifrar las cartas incautadas, como ya hemos visto, era clave, por lo que la presión sobre ellos era elevada. Para hacerles esta dura tarea más llevadera, los periodos de descanso eran habituales y se solían alternar semanas de trabajo con semanas de descanso. Además, cuando era necesario aplicar un sobreesfuerzo a la tarea, porque se sospechaba que una carta contenía un mensaje importante, se ofrecía una elevada suma de dinero como premio e incentivo para aquel que consiguiera llegar al mensaje en claro el primero. Además, el propio emperador reconocía personalmente la labor de aquellos que destacaban en el criptoanálisis. Quizás el hecho donde más claro queda el reconocimiento de Viena a los criptógrafos, es el pago que se les hacía cuando las circunstancias no les daban la oportunidad de hacer su trabajo, porque las claves se habían conocido de algún otro modo, habitualmente, robándolas en la embajada o interceptando su envío. En estos casos, como el trabajo de los criptoanalistas se vuelve innecesario si la clave es conocida, los empleados del gabinete que se dedicaban a esta tarea recibían una paga adicional para compensar la imposibilidad de acceder a los ingresos extra a los que hacíamos referencia.

La selección y entrenamiento de los criptoanalistas se llevaba a cabo con rigor y con la vista puesta en los resultados a medio y largo plazo. Seleccionados buenos conocedores de los idiomas y con capacidades para el análisis de textos, no era raro que incluso fueran enviados al extranjero a perfeccionar sus conocimientos. Aquellos funcionarios del gabinete secreto que dedicaban parte de su tiempo a formar a otros, recibían una compensación económica por ello. Por último, el director del gabinete secreto, su máximo responsable, era elegido siempre entre aquellos que habían servido como criptoanalistas. Todos estos beneficios y el cuidado que se ponía en la labor de descifrado, tuvieron como resultado el buen funcionamiento de la entidad y la eficiencia y efectividad en su labor.

En sus décadas doradas, entre 1730 y 1760, funcionaba como un reloj y era la más eficiente de todas estas instituciones en el mundo. Alcanzó casi el siglo y medio de vida, ya que fue disuelto en 1848. Bajo el gobierno de María Teresa I de Austria, precisamente en los años más espléndidos de la institución, su director fue el barón Ignaz de Koch, que actuaba como secretario de la emperatriz de puertas hacia fuera. Su mandato empezó en 1749 y acabó en 1763, y como muestra de su inteligencia y de su capacidad para moverse en el gran juego de los espías, escribió en una carta al embajador austriaco en París, en septiembre de 1751, que en lo que llevaban de año habían roto dieciocho cifras y que temía que aquella buena capacidad para el arte del criptoanálisis fuera en realidad contraproducente. Temía el barón que más pronto que tarde en las cortes europeas cayeran en la cuenta de lo que estaban haciendo y los dejaran ciegos del todo, cambiando sus claves de manera continua y haciendo cada vez más seguras sus cifras y más complicado el trabajo del gabinete.

Francesco Capaccini, fue un sacerdote romano que formó parte de los servicios vaticanos durante el siglo XIX y que contribuyó a diseñar el sistema de comunicaciones del papado con sus sedes europeas, para intentar evitar que los gabinetes de los distintos países conocieran la correspondencia de las altas instancias romanas como si fueran propias. Durante su juventud, fue un gran aficionado a la astronomía y leyó todo lo que pudo sobre el tema, además de mostrar cierto interés por las claves y las cifras. Los primeros servicios de Capaccini fueron como director de espías en Holanda, donde era internuncio, creando una red de informadores para evitar los movimientos contrarios a Roma.

A comienzos del siglo XIX el papado tenía nuncios, cónsules y enviados de diferente tipo por gran parte del mundo, pero esa importante red no era explotada como fuente de información y además sus comunicaciones eran enviadas a través del correo de cada país, lo que hacía que esas comunicaciones, por secretas que fueran, acabaran siendo leídas por los servicios de espionaje de cada uno de los estados, antes de llegar a su destino. Por ejemplo, en 1801, durante la negociación en París del concordato entre la Santa Sede y Francia, las cartas que intercambiaban el secretario de Estado papal y su nuncio en la capital francesa eran copiadas y leídas. Unos años más tarde, durante la celebración del Congreso de Viena, donde se discutían las fronteras y las relaciones internacionales en Europa tras la derrota de Napoleón, los austriacos conocían perfectamente las comunicaciones de Ercole Consalvi con Roma. El diplomático y cardenal era ministro plenipotenciario, nombrado por el papa Pío VII. Durante el congreso y en las discusiones vienesas estaba en juego conseguir la restitución de los territorios perdidos. Las protestas vaticanas contra el servicio postal que pasaba por Viena fueron comunes durante la primera mitad del siglo.

En algunas ocasiones el Vaticano envió mensajeros personales, que debían portar las cartas y entregarlas en mano. Este método era poco

eficiente, no era una solución general, pero es otra muestra clara de la falta de seguridad de las comunicaciones entre el Papa y sus hombres y sus diplomáticos europeos. El propio Capaccini advirtió que se debía dar por hecho que la correspondencia desde los Países Bajos era leída sin problema por terceros. Capaccini comenzó entonces a desarrollar un sistema propio de cifrado, buscando cifrar los mensajes de tal forma que, aunque las cartas fueran abiertas, no se pudiera conocer su contenido. Su labor inicial fue convencer a los altos responsables del papado de la necesidad de mejora en los cifrados, y habló a dichos responsables de cuestiones tales como el análisis de frecuencia, los homófonos y los valores nulos en los códigos. De igual forma, no solo pensó en los cifrados, sino también en la propia logística de los mensajes y en los procedimientos que debían seguirse para conseguir el objetivo de que la correspondencia diplomática vaticana fuera segura, a pesar de viajar por los servicios postales de otros países.

En 1831 Francesco Capaccini fue nombrado secretario de Cifras y Claves del papado de Gregorio XVI. La biblioteca vaticana, como podemos suponer, estaba bien dotada de tratados sobre criptografía, de mensajes cifrados y de documentos de todo tipo, lo que permitió a Capaccini profundizar en la búsqueda de un cifrado seguro. Las cifras y códigos de la Santa Sede mejoraron sensiblemente con las recomendaciones de Capaccini y este no dejó de ganar prestigio ni de seguir estudiando y mejorando hasta el día de su muerte, el 15 de junio de 1845. Tanto es así que murió de un infarto fulminante, y cuando encontraron su cadáver tenía sobre sí los papeles que estaba leyendo, que trataban sobre criptografía y criptoanálisis.

Como decíamos, la preocupación de Capaccini no solo fue la mejora de las cifras, sino que su visión era más amplia. Comprendiendo las cifras y el criptoanálisis como lo hacía, no es de extrañar que aceptara que sus comunicaciones, al menos en parte, podían ser descifradas y leídas por algunos criptoanalistas. Por ello, Capaccini diseñó un sistema de mensajeros y correos para las cartas más importantes, para que no cayeran en manos que las pudieran distraer durante su viaje. En la literatura especializada, en ocasiones se habla de este grupo de correos como *Los mensajeros de Dios* . No siempre eran hombres de iglesia, sino que la red de comunicaciones diseñada por Capaccini se apoyaba también en comerciantes u hombres de negocios que se movían por Europa y cuya lealtad al papado estaba fuera de toda duda. Incluso llegó a utilizar el sistema bancario de la época para asegurar la correspondencia, enviando a través de él la clave para descifrar cartas que habían sido remitidas por otros canales. En ocasiones, hasta una misma carta era separada en varios envíos y cada uno de ellos seguía un camino distinto a través de la red de mensajeros al servicio del papado. Al final, el secretario de Estado reunía todas las partes, conseguía la clave a través del servicio financiero y, por fin, descifraba el texto en claro.

Esta idea de Capaccini es un concepto que hoy se mantiene dentro de la seguridad lógica de las comunicaciones y que es una de las bases de

muchos sistemas de identificación basados en claves. Se conoce como la ruptura de canal y hace referencia al uso de distintos canales o métodos de envío para compartir todo lo necesario para identificarse en un sistema o, en el caso de Capaccini, para componer y descifrar un mensaje. En este caso del siglo XIX, aquel que quisiera leer la correspondencia papal tendría que capturar las partes del mensaje que viajaban por distintos caminos de esa red de comunicaciones virtual que recorría Europa, y además capturar la clave que se enviaba a través de los servicios financieros. Canales distintos que mejoraban la seguridad y que fueron una gran idea en las primeras décadas del siglo XIX… y lo siguen siendo hoy.

La unión de las matemáticas y la criptografía se fue consumando con el paso del tiempo. Uno de los hombres que comenzaron a enlazar ambos mundos de manera sólida fue el inglés John Wallis. Nacido en 1616, recibió una buena educación y empezó una vida religiosa, siguiendo los pasos de su padre, que era reverendo. Su primer contacto con las cifras llegó en 1643, cuando servía como capellán y le mostraron una carta cifrada que habían capturado los puritanos, para que intentara descifrarla. Wallis comentó que no estaba seguro de poder hacerlo, pero que si lo que tenía ante sí no era más que el uso de un nuevo alfabeto, podría conseguirse. Se puso manos a la obra, según dejó escrito, después de la cena de aquel mismo día, y antes de acostarse ya había puesto en claro el texto de la carta, que estaba oculto por un método de codificación no demasiado complicado. Aquello le dio confianza en su habilidad como criptógrafo y comenzó a tejer su reputación.

Poco después esa reputación estuvo a un paso de desaparecer, ya que un nuevo encargo de su bando en aquellos enfrentamientos religiosos le situó ante un sistema numérico mucho más complejo que el anterior. Estuvo a punto de tirar la toalla. Resolver el problema le llevó unos tres meses, pero finalmente dio con la solución. Tras esto, durante la Guerra Civil inglesa y a petición del Parlamento, descifró algunas comunicaciones de Carlos I, ganándose así varios honores y cargos en su carrera religiosa y un puesto como profesor en Oxford. En 1649 el rey Carlos I fue ejecutado e Inglaterra fue una república desde entonces hasta 1660.

Hasta el 3 de septiembre de 1658, cuando falleció, Oliver Cromwell fue el lord protector de Inglaterra, Escocia e Irlanda. Cuando comenzaron las negociaciones de Carlos II para restaurar el trono inglés y ocuparlo, las cartas cifradas iban y venían constantemente, y Wallis volvió a hacerse valer rompiendo las cifras. Carlos II sabía por algunas confesiones que gran parte de su correo era capturado y que sus cifras no eran seguras, ya que había un hombre en Oxford, Wallis, que se encargaba de poner en claro los textos. Inglaterra volvió a tener rey y cuando Carlos II llegó al trono, hizo llamar a John Wallis. A pesar de que había trabajado en los últimos meses en contra de los intereses del nuevo rey, este le ofreció formar parte del círculo de sus hombres más cercanos, nombrándolo capellán del rey. Lo que realmente quería

Carlos II era tener cerca al criptógrafo que había demostrado estar muy por delante de la mayoría en esas labores.

Wallis está presente en los libros de matemáticas, pero no por su contribución al mundo de la criptografía, sino por sus avances en cálculo. Fue un precursor del cálculo infinitesimal y el matemático que comenzó a utilizar el símbolo de infinito que seguimos viendo en nuestros días. Esto demuestra que su cabeza, además de bien dotada para las matemáticas, era capaz de abrir nuevos mundos y de usar la creatividad para solucionar determinados problemas. Su mente siguió activa y buscando nuevos retos durante toda la vida. En sus últimos años, cuando era incapaz de dormir por las noches, decidió sacarle partido al insomnio y practicar su cálculo mental, llegando a extremos como el cálculo de la raíz cuadrada de un número de 53 cifras. Precisamente en esos últimos años de su vida fue cuando más tiempo dedicó a las labores criptográficas.

A Carlos II le sucedió Jacobo I de Inglaterra y VII de Escocia, que era el tercer hijo varón del rey Carlos I y que reinó hasta febrero de 1689. Entonces el reino cayó en manos de Guillermo III y María II, época que se conoce popularmente como el reinado de Guillermo y María. John Wallis, el criptógrafo que había comenzado sus servicios con los enemigos de Carlos I, seguía en la primera línea de la corona inglesa después de tres reinados. El conde de Nottingham, que ejercía como secretario del rey para la guerra, le hacía encargos constantemente y al poco tiempo de comenzar el nuevo reinado, puso ante Wallis cinco cartas con varias cifras que eran nuevas para el criptógrafo. El conde de Nottingham, Daniel Finch, no era paciente con estos encargos y presionaba a Wallis, que le respondía que estaba dedicando horas sin fin a romper las cifras a pesar de tener ya setenta y tres años. Tan urgente era dar solución a aquellas cartas que provenían de Francia, que el mensajero que las había llevado tenía orden de esperar junto a Wallis a que este cumpliera con su trabajo y volver al momento con el texto en claro. Para asegurarse de que el conde comprendía cómo funcionaba el criptoanálisis y que de nada servían las urgencias, incluyó una nota al respecto en el mensaje de vuelta con el texto en claro.

El verano de aquel año, 1689, la correspondencia entre Luis XIV de Francia y su embajador en Polonia acabó en poder de los ingleses. Las manos inglesas que la recibieron eran las de Wallis y como era de esperar por todos sus servicios anteriores, también esta cifra fue rota. En aquellas cartas cifradas el rey de Francia pedía a su embajador que instara al rey de Polonia, Juan III Sobieski, a declarar la guerra a Prusia de manera conjunta. En otra, se proponía desde Francia un matrimonio entre los jóvenes de ambas coronas. Con este conocimiento en su poder, gracias a Wallis, Inglaterra podía anular los intentos de Francia de buscar alianzas con Polonia, pero el criptógrafo les advirtió que hacer públicos y notorios estos fallos en la seguridad de las comunicaciones del rey francés provocaría que este cambiara las cifras y les dejara ciegos de nuevo. Hay que tener en cuenta que al servicio del rey de Francia estaban los Rossignol, por lo que los temores del inglés eran

justificados. Este tipo de disyuntivas se han presentado innumerables veces en la historia. El conocimiento del enemigo, gracias a un espía o a la intervención de las comunicaciones, ha de ser utilizado con cautela para que no se advierta claramente ese fallo, ya que de otro modo se solucionará y no podrá seguir explotándose. Como veremos, en algunas ocasiones la decisión de usar cierta información y hacer palpable la inseguridad de las comunicaciones del enemigo ha debido tener en cuenta que la discreción y el beneficio futuro se ganaban directamente a costa de la vida de personas.

No debió de ser demasiado discreto el rey inglés con sus conocimientos, ya que el rey de Prusia le regaló a Wallis una cadena de oro por sus servicios, y otros obsequios similares de otros enemigos de Francia llegaron al matemático. En Hannover, buscaron ganar para su lado un talento como el de Wallis, después de ver lo importante que era jugar la partida con una pieza así en sus filas. Como era de esperar, el inglés era ya demasiado importante y demasiado mayor para caer en tentaciones, pero apuntaron alto al buscar un sustituto, ya que seleccionaron a Gottfried von Leibniz, que además era compatriota. Le pidieron que formara en el ámbito de la criptografía a un grupo de jóvenes. Leibniz, que había nacido en Leipzig en 1646, es otro de los grandes nombres de la historia de las matemáticas y también de la filosofía. De nuevo, una mente privilegiada, un genio a los ojos de muchos de sus contemporáneos y de muchos de los sabios de los siglos posteriores, se sintió atraído por la criptografía.

Leibniz pidió a Wallis que le enseñara sus conocimientos, pero este le dio largas argumentando que era complicado explicar la labor del criptoanálisis, ya que no había un método fijo y directo para llevarla a cabo. Leibniz temía que los conocimientos del inglés se fueran con él a la tumba, lo que no era descabellado teniendo en cuenta la edad de Wallis. Este al final reconoció que no tenía problema en servir a otros países puntualmente, pero que no estaba dispuesto a entregar sus conocimientos a estados que no fueran el suyo, a menos que su rey se lo pidiera. Leibniz, que en esto parece más hombre de ciencia que hombre de gobierno, le pidió al criptógrafo inglés que en cualquier caso formara a jóvenes en su disciplina, que entregara su conocimiento a otros, aunque no fuera a él, para que no se perdiera.

Wallis jugó con las palabras de Leibniz en beneficio propio y pidió a su gobierno que le pagara para formar a sus sucesores, en este caso, no solo sucesores en el ámbito del conocimiento sino también en el sentido estricto, ya que la persona a la que Wallis estaba pensando en formar era a su propio nieto. La propuesta fue aceptada y en 1699 comenzó esa labor de tutelaje. Dos años después, Wallis escribió al rey para decirle que el joven estaba preparado y que había demostrado su valía rompiendo varias de las mejores cifras utilizadas por los ingleses e incluso alguna francesa, contada entre las mejores provenientes de los Rossignol. Ambos países eran dos polos clave en Europa y habían tenido a un hombre como precursor de la criptografía en la corte, con resultados excelentes. A un lado del mar había estado John Wallis, al

otro, Antoine Rossignol. Bien es cierto que los separaban los diecisiete años que el francés le llevaba al inglés y que, si el primero trabajó tanto en el criptoanálisis como creando métodos de cifrado, el último casi no dedicó tiempo a crear nuevos métodos y se centró en romper cifras.

John Wallis falleció el 28 de octubre de 1703 y su responsabilidad fue a parar al nieto que había tutelado, William Blencowe, que tan solo tenía veinte años. Aunque heredaba el trabajo y la responsabilidad, lo cierto es que su predecesor, Wallis, había dedicado su vida a otras cuestiones y la criptografía era una labor secundaria para él. Blencowe, en cambio, se dedicaría a ello a tiempo completo y con un salario fijo y elevado. Tuvo éxito en su trabajo, pero falleció muy joven, en 1712, con veintinueve años de edad.

9. La derrota de la gran cifra de París

En 1803 se organizó un complot para asesinar a Napoleón. Como bien sabemos, no tuvo éxito, pero sí generó las condiciones adecuadas para que el Senado le proclamara emperador el 18 de mayo de 1804. El 2 de diciembre de aquel año, Napoleón se coronaba a sí mismo en la catedral de Notre-Dame. Fue así literalmente, ya que, aunque tenía todo el reconocimiento papal, fue él mismo el que se impuso la corona. Para entonces ya disponía de la inteligencia militar más afinada que había tenido Francia. Conocía los movimientos y las intenciones del resto de naciones europeas y el personal dedicado a ello especulaba sobre cómo se reaccionaría, por ejemplo, en Prusia, ante un determinado movimiento del emperador austriaco. Los agentes napoleónicos estaban en los principales centros de poder y decisión y la información fluía hacia el general francés. A pesar de ello, o quizás precisamente por el exceso de información, Napoleón era escéptico con respecto a las informaciones que le llegaban, alegando que eran contradictorias en muchos casos y que a menudo no eran conclusiones sacadas de la propia observación del espía o agente, sino que eran rumores que estos habían oído.

El Cabinet Noir francés seguía funcionando con Napoleón en el poder, aunque es probable que este no le prestara todo el interés que merecía en algunos casos. En los temas internacionales, Napoleón no era tan estricto como en los nacionales, los internos. Según comentó a un confidente durante su destierro en Santa Elena, Napoleón había prohibido acceso a esos mensajes internos a sus propios ministros y generales y, por contra, eran las comunicaciones de estos, que salían del Cabinet Noir, las que más le interesaban. Le divertían sus quejas por mantenerlos alejados de París, de sus comodidades y entretenimientos, pero a la vez los mantenía bajo control.

Además de ser un lector voraz de literatura y de todo tipo de libros, Napoleón prestaba mucha atención a los reporteros extranjeros. Algunos diarios británicos eran traducidos y se le enviaban para que él los leyera con detalle. A partir de esas lecturas, en Francia eran capaces de estimar cómo iban las campañas de sus enemigos, cómo eran los movimientos de sus tropas y en qué lugares y con qué éxito estaban trabajando los generales más importantes de su contrincante al otro lado del Canal. En 1808, por ejemplo, Napoleón escribió a Jean-Baptiste de Champagny, que había sustituido un año antes a Tallyerand como ministro de Exteriores, quejándose de que no le llegaban como debieran los periódicos ingleses, haciéndole saber también la importancia de la información que habitualmente le reportaban. Wellington, en cambio, opinaba que la prensa en ocasiones se extralimitaba en su obligación de informar y contaba demasiados detalles. El inglés envidiaba el control que Napoleón ejercía sobre la prensa francesa. Es lógico que, si Napoleón confiaba en los periódicos

extranjeros para importar conocimiento de inteligencia, protegiera en la medida de lo posible sus intereses controlando la prensa local. En noviembre de 1809 Wellington se quejó ante el secretario de la Guerra y las Colonias, lord Liverpool, de esto mismo, de la cantidad de información que la prensa daba sobres los movimientos y las campañas militares. Se quejaba el general inglés de que no se ejercía control ni censura alguna sobre lo publicado y que se hacían públicos así los movimientos, las posiciones de las tropas, el tamaño de las fuerzas… y que eso hacía que fuera más difícil hacer la guerra en España y Portugal, que era el territorio donde Wellington estaba combatiendo entonces.

No hay que confundir la importancia y veracidad que Napoleón atribuía a sus fuentes con su visión de la criptografía. No era extraño que el propio Napoleón cifrara su correspondencia, como ocurrió, por ejemplo, en la campaña en Rusia. Como veremos, también cambió su cifra cuando supo o sospechó que había caído en manos enemigas.

Como ocurriría en las guerras mundiales, Francia buscaba estrangular en cierta medida a su rival cercenando el comercio y los movimientos marítimos. Llevaba tiempo promoviendo acciones con ese objetivo, pero el decreto de Berlín, con algo más de un año de vida, no había acabado de conseguirlo. Portugal era uno de los puntos de fuga de su plan y por eso se propuso invadirla. En diciembre de 1807 Francia promulgó el decreto de Milán, prohibiendo a los barcos neutrales viajar a Gran Bretaña, en una muestra clara de sus intenciones. En ese mismo año quedó de manifiesto igualmente que Napoleón deseaba tener una base de su ejército directamente en España, para que le otorgara ciertas garantías y capacidad de maniobra. El emperador había impuesto a Portugal unos términos que debía cumplir, y al incumplir una parte de ellos puso sobre la mesa la excusa que Francia necesitaba para lanzar su ataque contra el país ibérico. El 18 de octubre de 1807, el ejército francés atravesó la frontera pirenaica, con el permiso de España, y al poco tiempo estos dos países firmaron el tratado de Fontainebleau, en el que se acuerda la invasión conjunta de Portugal y el reparto del futuro botín.

Menos de un año después de aquello el hermano de Napoleón era nombrado rey de España como José I. Los que eran aliados se tornaron en enemigos y España se rebeló contra Francia. Sobre la Península Ibérica combatieron portugueses y españoles contra franceses, y poco después los británicos se unieron de forma directa y activa a esa guerra. Estos hicieron un uso mayor de la inteligencia que los franceses, aunque también lo tenían más fácil, ya que los propios ciudadanos del país estaban de su lado. Wellington escribió que por todas partes les llegaba información, desde campesinos, sacerdotes… Los británicos le daban más importancia a la criptografía que los franceses, y gracias a los guerrilleros españoles y a esa ayuda de los propios habitantes de la península, los despachos militares y las comunicaciones interceptadas a los napoleónicos eran muy habituales.

El movimiento guerrillero estaba regulado desde diciembre de 1808 por la Junta de Sevilla a través de diferentes reglamentos. Uno de ellos hablaba del corso terrestre, trayendo a tierra la idea de la patente de corso naval, que permitía, sin ser militar, atacar barcos y poblaciones costeras enemigas en nombre del rey o la autoridad que la otorgaba. Antes incluso de esta regulación formal, la Junta de Sevilla ya animaba a los españoles a la lucha de guerrillas, atacando a los enemigos cuando y como se pudiera, en la retaguardia, interceptando su logística y, por supuesto, capturando sus comunicaciones siempre que fuera posible.

Hasta 1811 los generales de Napoleón utilizaban métodos de sustitución para llevar a cabo sus cifrados, sin mucho más avance, por lo que eran fácilmente descifrables incluso tan solo con un simple análisis de frecuencia, algo que, como sabemos, había sido descubierto un milenio antes. A partir de ese año de 1811 los franceses fueron sofisticando sus métodos criptográficos, lo que hizo más complicado el trabajo de los criptoanalistas británicos y españoles. No obstante, estos cifrados sencillos, conocidos como *pettits chiffres* en contraste con la Gran Cifra de París que se implantó después, siguieron utilizándose. Entre los intendentes que prestaban servicio en el ejército británico había un hombre llamado George Scovell que se reveló como un gran criptógrafo.

Los británicos habrían creado una unidad dedicada a las comunicaciones, al frente de la cual estaba un capitán, que no tardaría mucho en ser promocionado. Ese era Scovell, que, si bien acapara para sí un gran mérito, como veremos, formaba parte de una unidad y además se vio ayudado por la seriedad con la que los británicos se tomaron la gestión de las comunicaciones, tanto las propias como las capturadas al enemigo. En las propias, los británicos eran cuidadosos con el envío, con quién lo hacía y con el éxito o el fracaso en la entrega de cada mensaje. Por contra, los franceses no eran tan cuidadosos con los envíos y no se preocupaban tanto por si los mensajes eran capturados, ya que confiaban en la solidez de su cifrado, por lo que el único mal que asumían en la pérdida de un mensaje era la falta de comunicación, ya que el enemigo no podría saber qué contenía el mensaje cifrado. No imaginaban el error que estaban cometiendo.

En la primavera de 1811 los franceses introdujeron un nuevo código, basado en combinaciones de 150 números, que superaba sensiblemente a los 50 números que venían utilizándose, conocido por ellos mismos como el cifrado del ejército en Portugal. El responsable de poner ese código en marcha fue el mariscal Auguste de Marmont, que en julio de 1810 había tomado el mando del ejército francés en el norte de España, con el objetivo de dinamizar las comunicaciones entre sus tropas.

Scovell tardó un par de días en romperlo. A comienzos de 1812 se puso en funcionamiento un nuevo código mucho más complejo, el conocido como la Gran Cifra de París, basada en la Grand Chiffre de Luis XIV, y que tenía 1.400 números que podían aplicarse para sustituir tanto palabras enteras como partes de palabras o elementos nulos. Esto

permitía que una palabra pudiera ser cifrada de varias formas. Por ejemplo, si existía un número para cada letra de la palabra Castilla y un número a su vez para la sílaba Cas, el emisor podría elegir entre usar el número de Cas, o la secuencia de números de C, A y S.

Los franceses, no obstante, cometieron un fallo al crear su Gran Cifra. A las 1.200 entradas que ya tenía la cifra anterior, añadieron otras 200 con términos específicos para España, pensando en la guerra en la península. Estos dos centenares de nuevos elementos se añadieron al final de la lista, por lo que, a partir de cierto número, los británicos ya podían concluir que los franceses se estaban refiriendo a alguna persona o lugar intrínsecamente relacionado con España y su geografía.

En la parte final del año, Francia ya se había ocupado de distribuir desde París copias del nuevo código a todos los comandantes militares. El uso de los códigos tenía el problema de la distribución de los libros con las equivalencias, pero proporcionaba un nivel de seguridad suficiente y eran más sencillos de usar que otros métodos, como los propuestos por Vigenère, donde la modificación constante de la clave conllevaba ciertos problemas logísticos en un ejército grande, diseminado por todo un país y con poco conocimiento y destreza criptológica en muchas de sus unidades y mandos.

A medida que se fue generalizando su uso, los mensajes cifrados con esa Gran Cifra de París comenzaron a ser capturados y Scovell se puso manos a la obra contra el cifrado napoleónico, un trabajo que le llevaría varios meses. La introducción de una cifra tan poderosa, a juzgar por los propios franceses, los llevó a bajar la preocupación sobre cómo se enviaban los mensajes y qué ocurría con los que caían en manos enemigas, una política que, como ya hemos apuntado, es un error de enormes dimensiones en cualquier situación. Lo primero que hizo Scovell con los textos enemigos, como era de esperar, fue aplicar el análisis de frecuencias que tan bien le había funcionado anteriormente. No consiguió resolver el problema, pero sí comprobó que ciertos números, como el 2, el 13, el 210 o el 213, aparecían más veces que el resto. No tardó en aventurar con éxito que el número 210 correspondía a la palabra francesa «et», que era la palabra de dos letras más común en el idioma del cifrado.

Por otra parte, bien sabemos ya a estas alturas que resolver un código es como resolver un crucigrama, a medida que se van descubriendo trozos, letras o palabras, se va avanzando en el conocimiento de la solución. Así, Scovell tuvo la suerte de contar entre todo ese material que se incautaba a los franceses, entre esas comunicaciones capturadas, con algunos despachos que mezclaban en un mismo mensaje partes cifradas y partes sin cifrar. Conviene recordar que este es un error grave en la criptografía y que nunca se debería hacer, ya que un mensaje de este tipo es de enorme valor para el trabajo del criptoanalista. Las partes en claro otorgan un contexto al mensaje que es una ventaja y un conocimiento importante a la hora de atacar el texto. Scovell se encontró con regalos en forma de mensajes

napoleónicos capturados, cifrados tan solo en parte, como, por ejemplo: «He recibido su carta, y es una pena que no fuera capaz de atacar 1214.609.656.803, ocupada 58.850.112.1168.13.1388.1153.820». Este texto, unido al conocimiento o hipótesis sobre emisor y receptor, probablemente por saber dónde y a quién había sido capturado, llevó al inglés a adivinar lo que significaba: «He recibido su carta, y es una pena que no fuera capaz de atacar al ejército inglés mientras estaban ocupados en el asedio de 1168 en Salamanca».

La guerrilla española era una fuente continua y enorme de comunicaciones cifradas. La partida de Julián Sánchez, el guerrillero y militar conocido como El Charro, se movía por la zona de Salamanca donde las tropas napoleónicas comunicaban su vanguardia portuguesa con su retaguardia, e incluso con Francia. Esa partida fue creciendo y creciendo y la cantidad de capturas de información que puso en manos británicas era el alimento sobre el que trabajaban los criptoanalistas de Wellington.

Scovell no se basó en el análisis de frecuencias ni en técnicas matemáticas para su trabajo, sino que aprovechó la gran cantidad de información que tenía y su conocimiento del francés, su gramática y cómo lo utilizaba su enemigo, para buscar patrones y generar hipótesis que podía comprobar gracias a la gran cantidad de texto cifrado. Dicho de otro modo, Scovell nos recuerda la forma de atacar las cifras que recogió Simonetta allá por el siglo XV.

Por ejemplo, el criptógrafo inglés se encontró con el número 918 delante de texto sin cifrar que indicaba, por el tiempo verbal, que se estaba hablando en primera persona, algo como: 918 no descuidaré. No tardó en aventurar que ese número correspondía a la palabra «yo». No fue una tarea sencilla, pero cuando llegó el verano de 1812 la Gran Cifra de París había sido rota por los británicos y por lo tanto estos conocían con facilidad los movimientos y planes de las tropas enemigas, así como la información que intercambiaban los generales y oficiales napoleónicos.

El 9 de julio de 1812 el rey José I envió un mensaje a su hermano Napoleón, que en su viaje hacia el norte acabó en manos de los guerrilleros españoles. El mensaje estaba escrito en un pequeño trozo de papel, probablemente pensado para ir oculto dentro de la fusta del jinete que lo llevaba. Aunque estaba codificado con la Gran Cifra de París, los británicos consiguieron conocer su contenido y así saber que José I estaba moviendo un importante refuerzo militar para unirse al mariscal Auguste Marmont cerca de Salamanca. Según los planes del rey, dichos refuerzos llegarían el día 24 de julio hasta donde estaba Marmont. Conociendo los planes franceses, Wellington se adelantó a sus movimientos y atacó a Marmont el día 22 de julio en Salamanca, consiguiendo una gran victoria. Combatir de este modo, con un conocimiento continuo y profundo del enemigo, sus planes y sus movimientos, permitió a Wellington adelantarse a los napoleónicos en unas ocasiones y prepararse para las acciones de ataque de estos en otras.

Tan entusiasmado estaba el líder británico con los servicios de Scovell y la ventaja que le proporcionaban, que en enero de 1813 no fue del todo prudente en una carta que escribió al político español Andrés de la Vega. En ella Wellington le decía al español: «Adjunto un extracto de una carta del rey José a Napoleón, que estaba cifrada y que hemos logrado descifrar. Bien merece su atención y la de sus amigos en las Cortes». No fue del todo prudente, decíamos, y casi podríamos aventurar que fue jactancioso, porque si era importante que Andrés de la Vega tuviera esa información interceptada, podría habérsela hecho llegar igualmente sin decirle el origen y exponiendo tan solo que provenía de fuentes totalmente fiables. El sentido común dicta que una comunicación sobre la interceptación de comunicaciones puede ser interceptada a su vez, y si los franceses se enteraran de algún modo de que su Gran Cifra, el código que estaban utilizando, no daba seguridad, lo habrían cambiado al momento. Por suerte para Wellington, no ocurrió nada y los franceses siguieron usando el mismo código.

Aunque Scovell era importante en el desarrollo de la Guerra de la Independencia, como se conoce en España, o Guerra Peninsular (Peninsular War) como la conocen los británicos, las tareas criptográficas en su patria natal estaban de capa caída. La familia del obispo Edward Willes había ejercido oficialmente el cargo de descifrador, pero en 1812 la saga se detuvo y también la existencia del puesto.

Antes de la batalla de Salamanca en julio de 1812, a la que hacíamos referencia, Wellington envió a Londres algunos de los mensajes cifrados que habían interceptado a los franceses en la península. La respuesta llegó nueve meses después, y aun así el descifrado distaba mucho de ser completo, ya que tan solo habían sido capaces de averiguar los significados de 164 de los 1.400 códigos de la Gran Cifra de París, unos resultados muy pobres comparados con los que había obtenido Scovell, y además en mucho menos tiempo. Wellington respondió a esta ayuda criptográfica en mayo de 1813 con un poco de sorna, enviando una carta que decía que estaba muy agradecido por la parte del código que habían descubierto, y que respondía con toda la información que contenían las cartas y que había sido descubierta por el teniente-coronel Scovell, sin haber usado las pocas equivalencias de códigos que tan amablemente le habían hecho llegar desde Londres.

La batalla de Vitoria es considerada como el punto final del dominio francés sobre la Península Ibérica. El 13 de marzo de 1813 el rey José I tuvo otro revés en sus comunicaciones y un mensaje suyo destinado al general Honoré Charles Reille, que hacía poco había sido nombrado comandante del ejército de Portugal francés, fue interceptado. El mensaje, una vez descifrado, reveló que los napoleónicos estaban reduciendo las fuerzas que iban a enfrentarse a Wellington, ya que parte de ellas iban a ocuparse de una ofensiva contra la guerrilla española. Al día siguiente, el 14 de marzo, otro despacho cayó en manos de Scovell. En este caso el destinatario era el rey José y el emisor era uno de los oficiales a su servicio, el coronel Lucotte, que regresaba de París con las

directivas que el propio Napoleón le había dado sobre cómo debía conducirse la guerra en España. Lucotte no tenía entidad suficiente como para utilizar la Gran Cifra de París, ya que esta estaba reservada para los mandos superiores del ejército y para la propia corte imperial de Napoleón, por lo que en este caso el mensaje interceptado utilizaba un código menos complejo, aunque nuevo para Scovell.

Según la propia nota que dejó Scovell en el mensaje descifrado, aquel trabajo le había llevado tan solo seis horas y lo había hecho en Freineda, una pequeña localidad portuguesa donde Wellington tenía su puesto de mando, cerca de la frontera salmantina entre España y Portugal. Esta vez, a diferencia de lo que hizo con la carta que entregó al político español Andrés de la Vega, Wellington advirtió a Londres, cuando envió la información que había descifrado Scovell y que venía directamente de París, que no se hiciera público el contenido y que fuera tratado con discreción, precisamente por provenir de un mensaje cifrado capturado.

El triunfo en Vitoria fue decisivo para la Guerra de la Independencia, pero también puso fin al control de los británicos sobre la Gran Cifra de París, ya que acabó con el código. El 21 de junio de 1813 el rey José abandonó su carruaje y huyó del campo de batalla montado a caballo, dejando tras de sí sus pertenencias, entre las que estaban algunas de las obras que trataba de llevarse de España, como cuatro pinturas enrolladas, y un estuche de cuero donde, entre los documentos personales del rey, estaba la copia del código francés, la copia de «Sa Majesté Catholique», como ponía el documento, la copia de la Gran Cifra de París. José Bonaparte avisó del hecho al ministro de la Guerra francés, advirtiéndole de que su copia se había perdido y de que posiblemente estaba en poder de los británicos. Le decía a su vez que lo prudente sería, sin duda alguna, encargar la creación de un nuevo código y dejar de utilizar el anterior. Como era de esperar, el consejo se aceptó y se siguió.

Tan solo un mes después, en julio de 1813, un mensaje interceptado a los franceses cuyo destinatario era el mariscal Louis-Gabriel Suchet, comandante del ejército francés en la zona de Cataluña, utilizaba un código nuevo. Scovell comenzó a atacar este nuevo código, pero la buena situación británica hacía que el ejército francés hubiera abandonado casi por completo el territorio peninsular y, por lo tanto, sus comunicaciones se movían fuera de la amenaza de los guerrilleros españoles, lo que redujo enormemente el número de interceptaciones. Sin este flujo de información cifrada Scovell no tenía alimento para su trabajo.

Otro detalle que indica que Scovell comprendía bien cómo funcionaba la criptografía fue el método que propuso al ejército para sus comunicaciones. Un método que, bien usado, aporta un nivel de seguridad muy elevado. Proponía Scovell entregar dos ediciones iguales de un diccionario de bolsillo, si bien esto funcionaría en realidad con cualquier libro, a dos unidades militares o dos centros de mando. Los

mensajes se debían escribir seleccionando las palabras de ese libro y poniendo en el mensaje el lugar en el que estaba la palabra. Si cada código tenía página, línea y posición de la palabra de la línea, se podría cifrar y descifrar el mensaje sin problemas, y sería muy complicado romperlo. Por supuesto, para una misma palabra se deben seleccionar diferentes posiciones cada vez, entre todas sus apariciones en el libro, y por otra parte el libro debe ser suficientemente extenso. Ya comentamos que este método, originario del siglo XVII, había sido usado a lo largo de toda la historia.

No solo Scovell destacó como criptógrafo en nuestra Guerra de la Independencia, sino que también algún español aportó su granito de arena. El general Joaquín Navarro Sangrán, que había estado en la batalla de Bailén como parte de la artillería, combatió a los franceses en el campo de batalla y en la inteligencia. En agosto de 1811 rompió alguna cifra francesa sencilla y el general Castaños ya pedía en alguna carta que le ayudara con este tipo de cuestiones. El trabajo de criptoanalista lo desempeñó con cierto éxito, recibiendo los elogios tanto del propio Castaños como de Wellington. En una carta remitida por este a Henry Wellesley, el embajador británico, en junio de 1812, escribe el militar británico que envía copias de las cartas interceptadas en cifra, de las que sería interesante descubrir su clave. Continúa Wellington pidiendo que sean remitidas al general Navarro, por si pudiera sacar algo de ellas, ya que, por su parte, los británicos de momento no habían conseguido nada. A pesar del ejemplo del general Navarro, sí parece claro que en esta época los españoles no disfrutaban, como sí lo habían hecho en el pasado, de un servicio de cifra y contracifra solvente. Asombra ver la candidez de algunas de las cifras usadas por los militares y políticos españoles en aquel tiempo.

En 1812 Napoleón, todavía envuelto en la guerra en España y Portugal, abrió un nuevo frente en el extremo opuesto de Europa, lanzando contra Rusia el ejército más numeroso que se había formado hasta entonces. Francia confiaba en que las cosas le fueran bien en el este, a pesar de todo, y ya desde diciembre de 1811 el emperador había encargado a su ministro de Exteriores, Hugues-Bernard Maret, que pensara cómo poner en marcha una fuerza que actuara de forma más o menos secreta, y que se encargara de todo lo relativo a la información en Rusia, que reportara información sobre las fuerzas enemigas, sus relaciones internacionales, que se encargara de interceptar las comunicaciones y de traducirlas, lo que incluía el descifrado de los mensajes capturados si era necesario. Cuando en junio de 1812 la Grande Armée cruzó el río Niemen, dando así comienzo a la invasión, no se habían cumplido los deseos de Napoleón y esa fuerza de inteligencia e información en Rusia no estaba operativa, por lo que la visión que en Francia se tenía sobre su oponente era, según palabras textuales del propio Maret, «desactualizada, incompleta e incierta».

En cambio, los rusos tenían una mejor estructura de inteligencia e información. Mijaíl Barclay de Tolly, que había sido nombrado ministro de la Guerra por el zar Alejandro I, puso en marcha poco después de

llegar al cargo una red de agregados militares en las embajadas, cuya labor era trabajar en la información secreta sobre cada país. Aunque esta posición no estuvo activa en Francia hasta 1820, sí denota que el ministro de la Guerra ruso daba una importancia clave a la captura de información, la inteligencia y, por tanto, a la criptografía. Y no solo el ministro, desde el comienzo del siglo Rusia había trabajado en mejorar sus cifrados, en promover su uso y en crear expertos en el criptoanálisis. El gabinete oscuro ruso cumplía su función y en una Europa donde las intrigas diplomáticas y las guerras estaban a la orden del día, la captura de despachos y mensajes cifrados y su ruptura era una labor esencial, que marcaba la diferencia entre jugar esa partida de ajedrez viendo todas las piezas del tablero o jugarla conociendo solo las posiciones de las piezas propias.

Napoleón desconocía el control que Wellington tenía sobre sus movimientos en la península gracias al descifrado de la Gran Cifra de París, y quizás por ello pensaba que en Rusia podría servir con una cifra más simple, que era la que se utilizaba habitualmente en el este.

PARTE 3LAS COMUNICACIONES Y LA PRIMERA GUERRA MUNDIAL

10. La popularización de la criptografía y las comunicaciones

Llegó un momento en que la seguridad que durante mucho tiempo habían dado las ideas y los avances progresivos que se consolidaron en la cifra Vigenère, volaron por los aires. Ya no se podían dar por seguras las comunicaciones, debido a que un buen criptoanalista tenía conocimientos suficientes como para romper los cifrados y las formas de trabajo habituales. El movimiento pendular que ha ido definiendo la historia de la criptografía, yendo y viniendo de los criptógrafos a los criptoanalistas y estableciendo periodos en los que las cifras eran seguras y periodos en los que no, situó la ventaja del lado de los criptoanalistas. Ningún avance o método seguro de cifrado fue desarrollado durante las siguientes décadas.

Lógicamente, esto no hizo que se dejara de usar la criptografía o que no se intentase desarrollar nuevas formas de cifrado. De hecho, en este periodo la criptografía se hizo muy popular fuera de los ámbitos habituales destinados a la guerra, la diplomacia o el gobierno. Fue un elemento clave en algunas novelas e incluso en los diarios se publicaba algo parecido a los anuncios por palabras donde se utilizaba alguna forma de criptografía para que solo el emisor fuera capaz de conocer el mensaje. Esto era un deleite para los cada vez más comunes aficionados al criptoanálisis, que se divertían rompiendo estos códigos.

Cuando hablábamos al comienzo del libro de alguna de las técnicas esteganográficas de la Antigüedad, mencionábamos a Eneas el Táctico que ya en el siglo IV a. C. proponía esconder un mensaje en una carta o texto inocuo, haciendo pequeñas marcas, agujeros o puntitos debajo de las letras que iban componiendo el mensaje. En el siglo XIX, en Inglaterra, algunas personas ahorraron en su correspondencia gracias este método. El correo postal era entonces relativamente caro para muchos bolsillos, ya que el coste dependía de varios parámetros. Más adelante veremos cómo Charles Babbage cambió esto para siempre, pero lo cierto es que pagar un chelín por cada mil millas, que era el precio aproximado en la época, suponía un coste elevado si la carta tenía que hacer un viaje largo. En cambio, había una norma que permitía enviar periódicos por correo sin coste alguno. Esta norma fue la que aprovecharon muchas personas para enviar cartas sin pagar coste alguno. Cogían un periódico y utilizaban el método descrito por Eneas siglos antes, marcando las letras discretamente en el texto del periódico, para enviar cartas o mensajes personales.

En las novelas los códigos se convirtieron en algo común. En *Viaje al centro de la Tierra* , de Julio Verne, aparecía como elemento esencial un pergamino que ocultaba un mensaje detrás de una serie de caracteres rúnicos. No es este el único caso en el que Verne incluyó de alguna forma la criptografía en sus obras. En su novela *Matías Sandorf* , publicada por entregas entre junio y septiembre de 1885, y más tarde

como libro, Verne incluyó un sistema criptográfico que había descrito un coronel austriaco en un tratado sobre el tema en 1881, y que ya se había utilizado en Holanda el siglo anterior. Se trata de una rejilla giratoria que es una evolución, podríamos decir, de la rejilla de Cardano que ya conocemos. En este caso, la rejilla, al girar 90, 180 y 270 grados, descubre diferentes palabras, ya que los huecos en cada caso, en cada giro de la rejilla, caen en lugares diferentes. Así, si la rejilla de Cardano es capaz de seleccionar o marcar, en realidad mostrar a través de los huecos de la rejilla, 10 o 12 letras del texto inocuo que oculta el mensaje secreto, en esta versión giratoria el número de letras en el texto en clave se multiplica por cuatro, ya que cada giro, sobre un mismo texto, muestra diferentes posiciones.

También el más conocido y brillante detective de todos los tiempos, Sherlock Holmes, se las vio en alguna ocasión con las cifras, como en el relato de *Los bailarines* , también conocido como *La aventura de los monigotes* , donde aparece un mensaje escrito tras unos pequeños hombres danzantes, cada uno de los cuales, con su postura, equivale a una letra y por lo tanto su secuencia esconde un mensaje. Otro gran escritor que dejó en sus historias muestras de su pasión y conocimientos criptográficos fue Edgar Allan Poe, que en *El escarabajo de oro* colocó un mensaje cifrado en el centro de la historia y expuso el criptoanálisis del texto dentro del propio relato. En 1841 escribía en el *Graham's Magazine* que «apenas podemos imaginarnos una época en la que no existía una necesidad, ni siquiera un deseo, de transmitir información de un individuo a otro, de modo que eludiera la comprensión general».

La afición de Poe fue mucho más allá e incluso publicó un anuncio en la revista *Alexander's Weekly Messenger* de Filadelfia solicitando textos cifrados. Retaba a los lectores a que idearan un método de cifrado o utilizaran alguno que conocieran y que le enviaran ese texto cifrado. Él los iría resolviendo y si en algún caso no era capaz de hacerlo, el lector se llevaría una suscripción gratuita a la revista. Era 1839 y aunque el mundo de los códigos y la criptografía atraía muchos intereses, los mensajes de los lectores solían ser vulnerables al análisis de frecuencias, sumado a un poco de trabajo y sentido común. Poe se ganó una gran reputación como criptoanalista gracias a aquel reto público, ya que resolvió la inmensa mayoría de los mensajes. Alguno quedó sin solucionar y, al menos en uno, Poe, tras invertir mucho tiempo y esfuerzo, alegó que el mensaje que le habían enviado no tenía detrás ningún texto en claro o un método de cifrado real, sino que era una broma o un intento de engaño de un lector. Dicho de otro modo, el mensaje no era tal, sino que era una serie de letras sin sentido, puestas al azar.

Un siglo más tarde aquel texto que se le había resistido a Poe fue finalmente descifrado por dos expertos criptográficos, y descubrieron por qué se le había resistido. El texto tenía un buen número de faltas de ortografía, nada más y nada menos que dieciséis, y esto hizo imposible el estudio con éxito del texto cifrado. No era una serie de letras sin sentido, como alegaba Poe, pero tenía tantas erratas que se le parecía

bastante. El estudio estadístico de las letras, el análisis de frecuencias, quedaba seriamente inutilizado por estas erratas.

Que la cultura popular mostrara la criptografía de forma tan clara también tenía su relevancia en el uso militar y político de la misma, como es lógico. Esto daba lugar a funcionarios mejor preparados y con más capacidad para comprender la importancia e implicaciones de la criptografía y sus métodos. Por ejemplo, William Friedman, uno de los más importantes criptógrafos estadounidenses, que trabajó durante la Segunda Guerra Mundial en la ruptura de los códigos japoneses y del que hablaremos posteriormente en detalle, reconoció la influencia del propio Poe en su vocación, ya que el interés por estos temas le nació cuando era un niño a partir de la lectura de *El escarabajo de oro* .

Aunque es muy anterior a este periodo, es curioso que en un libro tan antiguo como el *Kama Sutra* , que data del siglo IV, aparezca la criptografía como uno de los saberes básicos de cualquier mujer. Entre las sesenta y cuatro artes que deben conocer y dominar las mujeres, según el texto, están el canto, el ajedrez, la cocina y también el arte de la escritura secreta. Para que la interesada en el tema no parta de cero, el texto incluye dos métodos criptográficos, sencillos pero que pudieran ser de utilidad. Uno de ellos sustituye unas letras por otras basándose en su similitud fonética y el segundo propone un método de sustitución de letras, sin más. Sabemos que este segundo método no resistiría mucho tiempo un criptoanálisis, pero quizás sí es útil para intercambiar algún mensaje con un amante o con otra dama, escondiendo el texto a los ojos del mensajero.

Otro caso curioso e interesante es un método sencillo de codificación que aparece en el siglo XVIII y que a partir de entonces ha sido muy utilizado, por ejemplo por la resistencia francesa en la Segunda Guerra Mundial y por la flota republicana al comienzo de la Guerra Civil española. Se trata del uso de un mismo libro por ambas partes, donde el mensaje indica las palabras que hay que ir seleccionando. Pedro Resard de Wouves, en 1787, propuso al conde de Floridablanca usar este método como base, aunque no hay pruebas de que llegaran a hacerlo. María Antonieta también fue otra precoz usuaria del método. Parece casi un juego de niños, pero lo cierto es que sin saber a ciencia cierta cuál es exactamente el libro que se está utilizando, incluyendo la edición exacta, el método ofrece cierta seguridad.

Lo primero que se ha de hacer es ponerse de acuerdo entre las partes sobre el libro que se va a utilizar. Por ejemplo, *Alicia en el país de las maravillas* . Las dos copias del libro deben ser exactamente iguales, es decir, de la misma edición. Esto es obligatorio, ya que el mensaje se compone indicando para cada palabra a cifrar, la página, la línea y la posición de dicha palabra en tal línea. Esas tríadas de números son las que el emisor irá apuntando para componer el mensaje. El receptor tendrá que tomarlas e ir buscando, palabra a palabra, en el libro con esas referencias. El método es engorroso y lento, pero tan sencillo y

fácil de poner en funcionamiento que es normal que su uso haya pervivido.

En este contexto no es de extrañar que *sir* Charles Wheatstone, un inventor y científico inglés nacido en 1802, invirtiera también parte de su tiempo en diseñar una técnica de codificación que alcanzó cierto uso y popularidad y que curiosamente no lleva su nombre, sino el de un amigo suyo al que le enviaba mensajes cifrados con esta técnica. El destinatario era Lyon Playfair, que vivía cerca de Wheatstone, y como ambos compartían cierta afición por la criptografía, se juntaban a menudo para hablar de este y otros temas. Una muestra clara de este interés está en la siguiente anécdota. Wheatstone y su amigo Lyon Playfair se reunían en ocasiones delante del periódico para buscar los mensajes cifrados que eran enviados a través de los anuncios de prensa y descubrir el texto en claro que trataban de ocultar. En una ocasión se toparon con un texto de amor que un joven de Oxford le enviaba a su amada a través del periódico *The Times* . Él le proponía a su querida que huyeran juntos, para poder disfrutar de su amor. Wheatstone y Playfair, quizás por seguir el juego y pensando en los jóvenes enamorados, publicaron un mensaje en el mismo periódico y usando el mismo método y clave criptográfica que utilizaban los amantes, disuadiendo a la pareja de llevar a cabo la locura de escaparse juntos. Unos días después apareció un nuevo mensaje en *The Times* . Era de la joven e iba dirigido a su novio: «Querido Charlie, no escribas más. Nuestro cifrado ha sido descubierto».

Wheatstone tuvo mucho que ver en la creación del cifrado Playfair. Este método es muy sencillo y parte de una palabra clave que el emisor y el receptor deben acordar por un canal seguro, como es lógico, previamente a su uso. Sobre una matriz de 5 × 5 se escribe la clave al comienzo y posteriormente el resto de letras del abecedario, sin repetir las que ya están en la clave y combinando la I y la J en una misma celda. Por ejemplo, si la clave fuera NAPOLEÓN, la matriz sería la siguiente:

N A P O L

E B C D F

G H IJ K M

Q R S T U

V W X Y Z

Como vemos en la matriz, se comenzó escribiendo la clave, NAPOLEÓN en este caso, pero sin repetir las letras, por lo que la O y la N finales no aparecen. A partir de ahí, se escribe el resto del abecedario, sin escribir las letras que están en la clave, que ya aparecen al comienzo de la tabla.

El mensaje a enviar se dividía entonces en pares de letras o dígrafos, con la condición de que cada par debe contener dos letras diferentes.

Para hacer esto, si coinciden dos letras iguales seguidas, se introduce una letra que no cambie el sentido del mensaje entre esas dos letras. Si el número de letras es impar, se añade una letra adicional para completar; lógicamente, una letra que no cambie el sentido de la frase. Por ejemplo:

texto a enviar: En mis dominios nunca se oculta el sol.

texto en claro en dígrafos: En-mi-sd-om-in-io-sn-un-ca-se-oc-ul-ta-el-so-lx.

Ahora, para cada dígrafo hay tres opciones. Si ambas letras están en la misma fila, se cogen las letras de la matriz situadas a su derecha, y si una de las letras está al final de la línea, se vuelve al comienzo de la misma línea. Si ambas letras están en la misma columna, se cogen las letras situadas debajo de cada una y de nuevo se actúa de forma circular sobre la columna si una letra está en la última posición. En la tercera opción, es decir, si no están en la misma fila ni en la misma columna, para la primera letra se busca en su misma línea la letra que comparte columna con la segunda letra del dígrafo, y para cifrar la segunda se hace lo mismo, buscando la columna de la primera letra. Así, el texto anterior quedaría como sigue en el ejemplo que hemos utilizado con la clave NAPOLEÓN:

Texto en claro en dígrafos: En-mi-sd-om-in-io-sn-un-ca-se-oc-ul-ta-el-so-lx.

Texto cifrado: GE GK TC LK GP KP QP QL BP QC PD ZF RO FN TP PZ

El receptor, conocida la clave, tan solo tiene que replicar la matriz e invertir el proceso para descifrar el mensaje.

Playfair se entusiasmó con el método, que, si bien era sencillo de comprender y por lo tanto de aplicar, ofrecía una seguridad interesante siempre que la gestión de las claves fuera buena. La idea de utilizar dígrafos en lugar de letras aisladas lo hacía más resistente a las técnicas de criptoanálisis de la época. Con el paso del tiempo, el análisis de frecuencias se extendió también a estos pares de letras y el sistema Playfair se convirtió en vulnerable. En cualquier caso, los criptoanalistas de la época no tenían tanta información sobre los digramas y además su estudio era más complejo, ya que, en lugar de veintiséis letras posibles, como se tiene en un método de sustitución sencillo, los posibles digramas de un idioma son varios cientos. Esto hace que la cantidad de texto cifrado necesaria para realizar un análisis concluyente sea mucho mayor.

En 1854 Lyon Playfair ya era un hombre influyente y bien relacionado. En una cena en la que estaban presentes el príncipe Alberto, marido de la reina Victoria, y Henry John Temple, conocido como lord Palmerston y que sería primer ministro cinco años más tarde, Playfair habló del método criptográfico que había ideado Wheatstone. Más tarde, puso en contacto al propio Wheatstone con el vicesecretario del ministro de Asuntos Exteriores para que le convenciera de la idoneidad de su idea.

El vicesecretario, tras la explicación, adujo que era demasiado complicado para ser utilizado durante una batalla, a lo que el inventor alegó que él podría enseñárselo a los niños de una escuela de primaria en quince minutos. Esto no hizo cambiar de parecer al vicesecretario. Aquella negativa no evitó que dejaran de promover su método de cifrado y al final consiguieron que la Oficina de Guerra británica lo adoptara. La labor de promoción que hizo Lyon Playfair y el uso de sus influencias para dar a conocer el método creado por Wheatstone acabaron causando que fuera conocido por el apellido de Playfair y no por el de Wheatstone.

Se estrenó en la Guerra de los Boers, y aunque como hemos dicho no era invulnerable, lo cierto es que se utilizó también en la Gran Guerra e incluso en la Segunda Guerra Mundial, si bien ya en 1914 el militar estadounidense Joseph Oswald Mauborgne publicó un trabajo en el que exponía una solución al método Playfair. Lógicamente para entonces no era un método seguro, pero sí servía como encriptación de cierta seguridad para mensajes no críticos o para mensajes que, pasado un determinado tiempo, pudieran ser leídos sin que esto tuviera importancia. Es decir, si de forma rápida había que decirle a una unidad de artillería, por ejemplo, que comenzara el bombardeo en 30 minutos, se podía usar este método. Si el enemigo capturaba el mensaje enviado por radio y tardaba más de 30 minutos en descifrarlo, la información ya no les serviría de nada.

En la Guerra de los Boers se dio uso a un idioma común como solución para la codificación de la información, de manera similar a lo que haría más tarde, en la Segunda Guerra Mundial, el ejército de Estados Unidos con los indios navajos. En los años 1900 y 1901 los británicos sabían que sus líneas telegráficas no eran seguras y que habían sido pinchadas. Aquello era una desventaja, pero les daba también la oportunidad de engañar a sus enemigos, enviando información falsa. Esto es algo que se ha hecho de manera recurrente cuando se sabe o se sospecha que el enemigo está escuchando las comunicaciones. La solución por la que optaron los británicos fue la utilización del latín, sin más codificaciones, para intercambiar información. Suponían que cualquier buen oficial inglés tendría educación clásica suficiente como para entender un mensaje en latín y que sus enemigos no serían capaces de comprenderlo. Lo utilizaron en alguna ocasión, pero se comprobó pronto que los británicos acertaban en que sus enemigos no iban a comprenderlo, pero se confundieron en que los oficiales británicos podrían entender el latín sin problemas. La solución vino de la mano de la cifra Playfair, que era suficientemente sencilla y segura.

La cifra Playfair no fue la única contribución de Wheatstone al mundo de la criptografía. En la Exposición Universal de París de 1867 presentó un dispositivo con dos alfabetos distribuidos a lo largo de dos circunferencias, de manera similar al disco de Alberti, y dos agujas, como las de un reloj, cada una de las cuales apuntaba a uno de los alfabetos. Visualmente sería como un reloj con dos circunferencias que en lugar de números tuviera letras a lo largo del perímetro de cada

circunferencia. La manecilla larga la podía mover el usuario a lo largo de la circunferencia externa, que era fija, no giraba. La circunferencia interna, en cambio, se podía mover y era la que determinaba el cifrado, al modo del disco de Alberti. Se debía poner esa parte móvil al comienzo del cifrado y del descifrado en la misma posición, para que las equivalencias entre letras se mantuvieran. Las agujas estaban unidas de tal forma que cuando se movía la manecilla larga y se seleccionaba una letra, la pequeña apuntaba a la letra de cifrado que se debía tomar. Esto sería un cifrado demasiado sencillo, así que Wheatstone incorporó un sistema por el que, con cada giro completado por la manecilla larga, la pequeña variaba y ya no apuntaba a la misma letra. La ventaja de este dispositivo era la sencillez de uso, que eliminaba errores humanos. A cambio, para cuando se propuso este método, los cifrados de esa clase ya tenían un criptoanálisis conocido, ideado por Babbage y Kasiski y que veremos más adelante, que acababa con ellos. Este dispositivo diseñado por Wheatstone, con algunas modificaciones, fue usado unos setenta años más tarde por el ejército de Franco en la Guerra Civil española e incluso después de esta.

El método Playfair es una muestra paradigmática del avance en la criptografía, gracias a que comenzaron a abrirse camino las sustituciones poligráficas, es decir, aquellas que no trabajan letra a letra, sino que agrupan las letras en digramas, trigramas, etc., y son estos los que se codifican.

Otro gran avance conceptual de mediados del siglo XIX fue lo que se conoce como cifrado fraccionario. Pliny Earle Chase publicó un artículo en 1859 en el que proponía la aplicación de operaciones matemáticas al texto a cifrar. Lógicamente, para hacer esto primero había que pasar el texto a números, algo que se podía conseguir fácilmente y por distintos métodos. Sin ir más lejos, con una tabla de Polibio o con cualquier otra tabla en la que se coloquen las letras aleatoriamente. Hecho esto, todo tipo de operaciones matemáticas se podía aplicar sobre la secuencia de números, tomándolos uno a uno, por pares, en grupos de cuatro o cinco…

La comunicación rápida entre puntos alejados ha sido clave desde el comienzo de la historia. Durante siglos, no obstante, en términos generales, los mensajes podían llegar tan lejos y tan rápido como pudiera llegar un hombre trasportándolos, más allá del uso de algún animal como la paloma o de algún método singular. Dicho de otro modo, lo más rápido que podía viajar un aviso, una noticia o cualquier tipo de información dependía de lo rápido que fueran los caballos, los barcos o incluso de lo rápido que fuera un hombre corriendo. Los sistemas de postas, en los que los correos cabalgaban largas distancias cambiando cada cierto tiempo los caballos cansados por otros frescos, fueron una forma de conectar los territorios durante mucho tiempo.

Había pocas formas de evitar estas restricciones. Podríamos decir que el uso de palomas mensajeras era el más avanzado de los métodos de comunicación a distancia. Los griegos ya las utilizaban para hacer

saber, por ejemplo, los ganadores de sus juegos y en el ejército romano eran muy comunes. Podríamos admitir que también las señales de humo se salen un poco de esa limitación. De hecho, las señales de humo tienen siglos de historia. En la antigua China, los soldados apostados a lo largo de la Gran Muralla alertaban de los ataques enemigos a través de señales de humo que viajaban de torre en torre. De este modo, en tan solo unas horas el mensaje de peligro podía recorrer centenares de kilómetros. No obstante, estamos hablando de varias horas para completar la comunicación. Ya hemos visto, por otra parte, cómo Polibio, en torno al año 150 antes de Cristo, proponía el uso de antorchas para enviar información. Las señales de humo que en la cultura popular están asociadas a los nativos norteamericanos, fueron una solución empleada de igual modo en otros casos y épocas. Por supuesto, con el humo tampoco se pueden hacer envíos complejos y la información no va mucho más allá de un estar alerta o algún mensaje así de corto y simple. Cada tribu de los nativos norteamericanos tenía su propia forma de dar significado a las señales, pero en términos generales la información era similar a que una bola de humo significa que había que estar alerta, dos querían decir que todo estaba tranquilo y tres advertían de la existencia de problemas o peligros. Es obvio que no hay lugar para mayores complejidades.

A finales del siglo XVIII el mundo sufrió una revolución en el ámbito de las comunicaciones y, por supuesto, la criptografía se vio envuelta en este salto hacia delante. En 1792 un joven inventor francés, Claude Chappe, presentó lo que podríamos denominar como un telégrafo óptico, que a través de un brazo articulado podía servir para establecer comunicaciones a distancia. Era una forma avanzada y muy mejorada del sistema de comunicaciones mediante antorchas o humo del que hablábamos hace un momento. Chappe comenzó a desplegar por Francia una serie de torretas que tenían sobre ellas dos brazos que se movían mecánicamente y que podían girar para componer hasta noventa posiciones diferentes. El invento tenía un tamaño considerable, lo que permitía que fuera visto desde unos quince kilómetros, o incluso más si el terreno era favorable. Como vemos, las posibilidades que proporcionaban noventa posiciones son muchas más que las que ofrece una bola, dos o tres de humo. En no demasiado tiempo el mensaje podía, además, recorrer algunos cientos de kilómetros, dependiendo, eso sí, de la asistencia humana para que el mensaje recibido en una de las torres de comunicaciones fuera relanzado desde esa misma torre. El operador de una torre colocaba los brazos de un determinado modo, lo que tenía su significado, y el operador de la torre siguiente lo veía en la distancia y repetía en su propia torre la posición de los brazos. Así, el mensaje viajaba a través de Francia.

Napoleón vio que aquel invento permitía unas comunicaciones muy rápidas para la época y ordenó el despliegue masivo, llegando a las quinientas torres instaladas. El invento se iba a llamar taquígrafo en un primer momento, por aquello de la escritura rápida, pero se acabó llamando escritor en la distancia, es decir, telégrafo. Su uso militar fue

inmediato, pero también se extendió a otro tipo de comunicaciones, siempre, eso sí, relacionadas con el gobierno y el Estado.

Los telégrafos ópticos se extendieron por varios países y se crearon diferentes prototipos e ideas a partir de la propuesta de Chappe. En España, Agustín de Betancourt, un ingeniero y militar afrancesado y con múltiples inquietudes, desde la ciencia básica a la arquitectura, diseñó su propia versión en los mismos años en los que Chappe lanzaba su propuesta. Betancourt trabajó en métodos avanzados de comunicación durante su estancia en París, en la segunda mitad de la década de 1780, con la ayuda de un relojero suizo llamado Abraham-Louis Breguet. Más tarde, estando en Inglaterra y sabiendo de las pruebas que había hecho Chappe para comunicar con su telégrafo las ciudades de Lille y París, y conociendo igualmente que los británicos estaban trabajando en ello, Betancourt presentó su prototipo, junto con Breguet.

Arrancó entonces una polémica sobre cuál era la mejor propuesta, si la conocida como Betancourt-Breguet o la del francés Chappe. La Academia de las Ciencias francesa, en la que había entonces hombres tan importantes como Lagrange o Coulomb, analizó el trabajo hispano-suizo y alabaron su precisión y rapidez. La Academia llegó a aceptar como mejor la versión que provenía de fuera de Francia, pero las razones económicas derivadas de que el invento de Chappe ya estaba funcionando en algunos lugares, acabaron por hacer que el uso práctico y el desarrollo sobre el terreno beneficiaran al francés.

Durante algunas décadas, a caballo entre el siglo XVIII y el XIX, los telégrafos ópticos gozaron de cierto uso, a pesar de sus desventajas y problemas. Tenían una dependencia importante de la climatología, ya que la difusión de las señales dependía de la capacidad del operador para ver la señal en la distancia. Por lo tanto, con poca luz, niebla, lluvia… su función era muy complicada, por no mencionar su inutilidad de noche o en las horas de escasa luz. Además, estaban los accidentes geográficos y los errores derivados de la transcripción del operador para reenviar el mensaje.

A pesar de todo esto, y desde el punto de vista de la seguridad de las comunicaciones y por lo tanto desde el de la criptografía, la emisión abierta y libre de los mensajes daba una importancia añadida a dicha seguridad. Un mensaje enviado a caballo, encerrado en un sobre y entregado en mano, está protegido en cierta medida de los ojos ajenos. Incluso las cartas enviadas por correo tradicional, aun sabiendo lo que suponen cosas como los gabinetes oscuros, conllevan en el propio envío cierta privacidad. Pero cuando los mensajes se hacen a la vista de todos, es necesario que esa comunicación esté encriptada, ya que del mismo modo que el operador puede ver en la distancia el mensaje, lo puede ver cualquier otro. Si se trata de asuntos militares, el enemigo, sin ir más lejos.

El camino, no obstante, había sido abierto y la convergencia de la idea básica del telégrafo óptico con nuevos inventos y conocimientos, llevó al

telégrafo eléctrico, que acabó por inutilizar el sistema en que habían trabajado Chappe y Betancourt, entre otros. La electricidad fue el elemento clave en este avance. Hans Christian Oersted, danés, descubrió en 1820 la relación entre la electricidad y el magnetismo en un experimento en el que un hilo conductor era capaz de mover una aguja imantada cuando una corriente se movía por dicho hilo. Esta interacción entre las fuerzas eléctrica y magnética fue algo revolucionario y los resultados del experimento, incluso sin una aclaración formal y científica que los explicara, fueron publicados y alcanzaron gran difusión. Karl Gauss y Weber consiguieron transmitir señales en la Universidad de Gotinga entre dos edificios separados algunos cientos de metros. El envío gracias a la electricidad de señales entre dos puntos relativamente alejados no es lo mismo que el envío de mensajes, pero era un paso relevante.

El telégrafo eléctrico, no obstante, no llegó de la mano de ningún laboratorio científico, sino que fue la industria la que aplicó y aunó los conocimientos de los científicos para llegar a la solución práctica. La necesidad que vino a cubrir el invento fue la de mantener el orden en el tráfico de los ferrocarriles. El envío de mensajes a través de la sucesión de impulsos eléctricos era algo necesario y distintos inventores trabajaron sobre esa idea. Como ocurre en otros muchos casos, aparecieron varias soluciones muy parecidas, aunque ligeramente diferentes. La revolución industrial y la ciencia hacían viable el tendido de grandes líneas de hilo de cobre y que la electricidad viajara por esos hilos llevando consigo, de un modo u otro, información, o lo que es lo mismo, un mensaje. Estas propuestas estaban libres de gran parte de los problemas y restricciones que hemos enumerado para el telégrafo óptico: las distancias eran mayores, no era necesario un operador que retransmitiera el mensaje cada pocos kilómetros y, por supuesto, podía operar de noche y con poca visibilidad.

Los ingleses William F. Cooke y Charles Wheatstone patentaron un diseño en el que la orientación de las agujas receptoras de las señales marcaba la letra adecuada, lo que hacía muy sencillo enviar y recibir mensajes, ya que no era necesario ningún lenguaje o alfabeto adicional. El problema residía en la complejidad de fabricación del aparato, por una parte, y en la necesidad de varios cables para la transmisión, por otra. Aunque el sistema evolucionó y se llegó a utilizar durante algún tiempo en su país natal, acabó por descartarse como solución universal. En 1839 el sistema inglés estaba en funcionamiento entre las estaciones de ferrocarril de West Drayton y Paddington, que distaban entre sí cerca de 30 kilómetros. Los problemas del sistema de Cooke y Wheatstone, principalmente su complejidad, residían precisamente en el uso del lenguaje con el que hablamos y escribimos. La solución al problema llegó con la simplificación del lenguaje de comunicación gracias a la utilización del código morse.

Samuel Morse fue el creador del código telegráfico más utilizado y el secreto de su éxito estaba en la sencillez y, como decíamos, en la convergencia con otras ideas e inventos para componer una solución

práctica. Técnicamente el código morse solo requiere que el circuito eléctrico se cierre durante más o menos tiempo para enviar así pulsos cortos y largos, que se traducen para el operador en los puntos y las rayas con las que se compone el código. Todas las letras tienen su equivalente en una secuencia muy corta de puntos y rayas, pulsos cortos y largos, y por lo tanto no hay limitaciones en cuanto a los mensajes que se pueden enviar. Dicho de otro modo, con este método de codificación tan sencillo, compatible con la tecnología de su tiempo a unos costes relativamente bajos, se puede enviar cualquier texto, algo mucho más práctico que las antiguas señales de humo. Además, está basado en la electricidad, por lo que se puede utilizar de día, de noche y a grandes distancias.

El 24 de mayo de 1844 Morse envió el primer mensaje telegrafiado del mundo desde el Capitolio, en Washington. El destino del mensaje era la estación de tren de Baltimore y ambos puntos estaban unidos por una línea experimental pagada gracias al Congreso de Estados Unidos. El contenido de aquel primer mensaje, que recorrió unos 65 kilómetros, era una cita de la Biblia, concretamente del Libro de los Números (23, 23): «¡Mirad lo que Dios ha hecho!».

El telégrafo diseñado por Morse se extendió por Estados Unidos y comenzó a ser utilizado de manera general, por los militares, por los periodistas, por los comerciantes… las líneas de ferrocarril iban siempre acompañadas por la línea de postes telegráficos que tendían los cables de un lado a otro del enorme país. Tantas barreras libró el nuevo sistema de comunicación, que el 13 de agosto de 1858 la reina Victoria de Gran Bretaña y el presidente de Estados Unidos, James Buchanan se comunicaron de un continente a otro, después del impresionante trabajo que, plagado de imprevistos, llevaron a cabo los barcos para unir con un cable submarino cada orilla del Atlántico.

Es justo que el nombre de Morse vaya unido al del telégrafo, ya que fue el que consiguió completar una idea en la que otros tuvieron también su parte relevante. Hans Christian Oersted, Michel Faraday, por sus trabajos sobre el electromagnetismo, Leonard D. Gale, que ayudó a Morse en la Universidad de Nueva York, o Alfred Vail, colega y estrecho colaborador del propio Morse, entre otros, situaron a este en el punto exacto para cambiar el mundo. Una vez más, un hombre, Morse, caminó a hombros de gigantes.

El telégrafo, entre sus ventajas intrínsecas, no ofrecía seguridad. Cualquiera podía escuchar en las líneas y hacerse con los mensajes. El código morse no es ninguna forma de criptografía y la equivalencia entre cada letra del alfabeto y los puntos y las rayas es perfectamente conocida por todos. Además, los propios operadores de las líneas tenían que conocer el mensaje, para enviarlo usando el morse. Este era un cambio, fuera del ámbito militar, con respecto a las comunicaciones por carta, donde el texto iba oculto dentro de un sobre o con alguna solución similar. Los trabajadores de las empresas de telegrafía firmaban documentos comprometiéndose a guardar el secreto y

mantener la confidencialidad en las comunicaciones; pero esto, en la práctica, no es garantía suficiente.

Este nuevo método de comunicación interesó mucho a los empresarios y comerciantes, además de a los servicios públicos, lo que hizo que tras su estela creciera también el interés por la criptografía. Por entonces, aún se tenía como seguro y fiable cualquier método basado en la cifra Vigenère, aunque los trabajos de Babbage y Kasiski, como veremos, habían echado por tierra esa inviolabilidad. Los mensajes secretos o importantes eran cifrados de alguna forma por el emisor antes de ir a la oficina telegráfica a encargar el envío. Este tipo de mensajes tenía un sobrecoste porque el operador debía emplear más tiempo en procesarlo. Habitualmente, un operador era capaz de transmitir hasta 35 palabras por minuto, en inglés. Esta velocidad se alcanzaba cuando el operador era capaz de memorizar el mensaje o frases enteras, y por lo tanto ocuparse solo en pasar las letras a morse y en enviar. Lo cierto es que lo hacían a una velocidad admirable. En cambio, en el caso de un mensaje cifrado, no hay posibilidad de memorizar el texto, por lo que el operador está obligado a consultar el mensaje y a enviar casi letra por letra, lo que ralentiza notablemente el envío. Y esto tenía un sobrecoste.

11. Babbage contra la cifra indescifrable

Llegó un momento, como es obvio en nuestros días, en el que el ordenador se hizo con el mundo de los códigos y la criptografía y desde entonces no tiene sentido cifrar o intentar descifrar sin su ayuda. Los cálculos necesarios para que una cifra soporte un ataque a través de un *software* , solo son accesibles a su vez al propio *software* , por lo que podemos afirmar que, desde hace unas décadas, criptografía y computación van de la mano. Esta conexión comenzó desde los primeros momentos de existencia de algo parecido al ordenador, aunque sea de forma lejana. Y el pionero que unió ambos mundos fue Charles Babbage.

Nacido en 1791, era hijo de un banquero de Londres, por lo que, a pesar de perder parte de su herencia por casarse sin el permiso paterno, tuvo el dinero suficiente para dedicarse a resolver los problemas que le estimulaban el cerebro, sin tener que preocuparse mucho por cómo ganarse la vida. Su educación había sido privilegiada, pero no paró ahí su interés por determinados ámbitos y se formó de manera autodidacta en diferentes campos, especialmente en las matemáticas y en el funcionamiento de los dispositivos mecánicos. Formó parte de la Real Sociedad de Matemáticas londinense, de la Sociedad Astronómica y de la Sociedad Estadística, e investigó y publicó artículos en estos campos. Sus inventos, por otra parte, son muy heterogéneos. Desde el velocímetro a un avisador de vacas para trenes, pasando por el sistema de señales de los faros o el dinamómetro. Antes de continuar, aclaremos en qué consistía ese avisador de vacas, por lo original del invento. Babbage diseñó un dispositivo que se colocaba en la parte delantera de las locomotoras y que atrapaba o apartaba a los animales de las vías, evitando así accidentes y muertes de animales. Nunca llegó a producirse y a utilizarse, si bien la idea es la misma que acabó implantándose con éxito en todos los trenes, esa estructura delantera en forma de pico tan habitual en las locomotoras a vapor. Sus investigaciones también le llevaron a darse cuenta de que la anchura de cada anillo del tronco de un árbol, anillos que se pueden ver únicamente talándolo, dependía de cómo había sido el clima en el año en concreto en que ese anillo estaba desarrollándose. Hizo avances en la estadística aplicados al mundo de los seguros y está considerado como uno de los padres de la computación.

Si hay dos cualidades útiles en el mundo de la criptografía, además del propio conocimiento, son el trabajo sistemático y la creatividad a la hora de enfocar los problemas. Babbage demostró tener esta segunda cuando alteró el sistema postal para siempre. Pensando sobre él, cayó en la cuenta de que, en el proceso de franqueo, quizás era más caro el collar que el perro y que la gestión del coste de los envíos reportaba menos beneficio que el propio envío. Pensó que, al menos, se podría optimizar. En su época, en el siglo XIX, por el franqueo de una carta se

pagaba una cantidad dependiendo de la distancia que debía recorrer la carta y esto obligaba a calcularla cuando el cliente se presentaba en la oficina postal. El precio se establecía en función de la distancia que la carta iba a recorrer hasta las manos del destinatario. Y había que cobrarlo una vez establecido.

Babbage se planteó que, calculando e implantando unas tarifas comunes para todos los envíos, se eliminaría el trabajo de tener que hacer todos esos cálculos para el cobro de cada uno de ellos de manera independiente, y además se simplificaría el propio cobro. Y ese trabajo que desaparecía, quizás ahorrara más dinero del que se ganaba con un coste variable por carta. La intuición de Babbage apuntaba en la buena dirección y así se pasó a tener un coste fijo por envío, con alguna variación, por ejemplo si el destino era internacional. El sistema se ha mantenido en el tiempo y es el que rige en la actualidad, donde se compran sellos para franquear las cartas, sabiendo de antemano el coste que hemos de pagar y eliminando todo ese proceso de cálculo de la oficina de correos.

El reconocimiento a Babbage como precursor de la computación se debe a su máquina diferencial. Babbage se había dado cuenta de que las tablas de cálculo que se utilizaban en astronomía, navegación o ingeniería estaban llenas de errores. Esto desesperó a Babbage y a su compañero en aquel análisis de las tablas, el astrónomo John Herschel. Llegaron a encontrar casos indignantes a sus ojos, como el de la primera edición del texto «Efemérides náuticas para hallar latitudes y longitudes en el mar», que contenía más de mil errores. Estos eran provocados, con toda lógica, por el tedio y el poco interés que despertaban estos cálculos rutinarios en aquellas personas que tenían que hacerlos a mano y uno a uno, para esos libros y tablas de cálculo. Como en tantos otros inventos a lo largo de la historia, ha sido la búsqueda de una forma de evitar el trabajo tedioso o duro lo que ha conducido al éxito. Babbage tenía que calcular de forma repetitiva, y llegó a pedir al cielo desesperadamente que aquellos cálculos los pudiera hacer la fuerza del vapor. Uniendo estos elementos, cómo evitar los errores en los cálculos de las tablas que luego otros utilizaban y cómo evitar la inversión en horas de aburridos cálculos repetitivos, Babbage pensó en la posibilidad de diseñar una máquina que resolviera esos problemas. Dicho de otro modo, pensó que era más estimulante crear una nueva máquina para hacer cálculos por él, que seguir invirtiendo tiempo en hacerlos.

En 1823 había dado a luz lo que se conoce como su máquina diferencial número 1, una máquina calculadora de unas 25.000 piezas y cuya construcción consiguió cofinanciar gracias al gobierno británico, que aportó casi 17.500 libras, una pequeña fortuna en ese momento. A pesar de haber recibido una importante suma como subvención para llevar la idea a la práctica, no consiguió llegar a buen puerto. En cualquier caso, como ya hemos dicho anteriormente, unas veces se gana y otras se aprende, y aquella versión primera de la máquina diferencial le permitió aprender y afrontar con mayor conocimiento la versión segunda. Por el

camino, eso sí, perdió la posibilidad de volver a recibir financiación del gobierno para su proyecto. No podemos saber muy bien si fue por esa falta de dinero extra o por otros motivos, aunque probablemente fuera una combinación de varias causas, pero lo cierto es que el segundo intento de construir su máquina diferencial no acabó mucho mejor. No llegó a desarrollarse el prototipo, pero el diseño de Babbage ya era de por sí una revolución por ser programable, y definió algunas de las características básicas sobre las que se trabajaría más adelante en el desarrollo de los primeros ordenadores. La idea genérica de tener una memoria donde almacenar datos, un procesador que hiciera los cálculos y la capacidad para dar instrucciones como «repetir acción» o «si Y hacer X», siguen presentes en la computación actual.

Esta relación de Charles Babbage con el mundo de la informática es importante para la criptografía por las bases que sentó, como acabamos de comentar, que permitieron que algo más de un siglo después la criptografía y la computación se unieran para siempre. Pero no menos importante en el ámbito criptográfico fue su pelea contra la cifra Vigenère, uno de esos proyectos en los que se embarcó llevado sencillamente por su interés y por el estímulo de alimentar su vida y su mente con retos.

Desde muy joven los códigos y su relación con las matemáticas habían sido un campo atractivo para el científico inglés. Él mismo contaba cómo en alguna ocasión, cuando era niño, chicos mayores que él usaban códigos para comunicarse entre ellos y cuando él conseguía romperlos, le pegaban en represalia por haberlo hecho y, quizás, por hacerlos sentir algo tontos. Descifrar códigos era, para él, una de las artes más fascinantes. El paso del tiempo hizo que su capacidad como criptoanalista fuera creciendo, y eso a su vez llevó a que algunas personas informadas de su buen hacer con los códigos se acercaran él para pedirle ayuda. Así, auxilió, por ejemplo, a un estudioso de la vida de John Flamsteed, el primer astrónomo real británico, que vivió a caballo entre el siglo XVII y el XVIII, a descifrar las notas taquigrafiadas de este. También resolvió la cifra de Enriqueta María de Francia, esposa del rey Carlos I de Inglaterra (este, por cierto, era nieto de María Estuardo) para ayudar a un historiador. Se requirió también su ayuda en algunos casos legales. Su propio interés, sumado a esa fuente continua de consultas y por lo tanto de textos cifrados, le permitió acumular a lo largo de su vida un gran volumen de códigos de todo tipo y muchas horas de criptoanálisis. Babbage afirmaba que una de las características más singulares del arte del desciframiento es la fuerte convicción que tienen todas las personas, incluso las que están moderadamente familiarizadas con él, de que son capaces de construir un código que nadie más puede descifrar. «También he observado —continuaba— que cuanto más inteligente es la persona, más íntima es esta convicción». Él mismo cayó durante un tiempo en esa vanidad que denunciaba, aunque acabó cambiando de bando y empleando su tiempo en el criptoanálisis.

Entre todas esas peticiones, consultas, lecturas y comentarios que le fueron llegando a lo largo de los años, en 1854 Babbage se encontró con un texto publicado en el *Diario de la Sociedad de las Artes* , en el que un dentista llamado John Hall Brock Thwaites describía y afirmaba haber diseñado una cifra revolucionaria. En realidad, el método creado por el dentista era la cifra de Vigenère. Babbage escribió a la publicación comunicándoles el hecho, y haciéndoles saber que ese método era muy antiguo y que estaba presente en la mayoría de libros sobre el tema. Thwaites se negó a admitir que se había equivocado y que había llegado al método con unos tres siglos de retraso. En lugar de eso, desafió a Babbage a romper su código. Aquello fue suficiente para que el científico se pusiera a investigar cómo podía romper el cifrado Vigenère, que por aquel tiempo se tenía como un método seguro e inaccesible a los métodos criptoanalistas conocidos.

Ya hemos comentado que para atacar un sistema criptográfico lo que hay que buscar es una pequeña debilidad por la que investigar y hacer que el método de cifrado deje poco a poco de mantener el secreto y vaya revelando lo que tiene dentro. La cifra del dentista, que en realidad era la cifra Vigenère, era polialfabética y por lo tanto poco vulnerable al análisis de frecuencias de las letras. El método que se proponía romper Babbage también tenía su problema con las repeticiones, y si la longitud del texto era suficientemente larga, podía comenzar a descubrirse a través de palabras comunes o repetidas. Si bien cada letra se sustituye por una diferente en cada aparición, lo cierto es que a través de esas palabras repetidas se puede ir descubriendo la clave, comenzando por su longitud. Buscando secuencias repetidas en el texto cifrado había un punto por el que comenzar. Esas repeticiones podrían indicar que las mismas letras en el texto llano han sido codificadas con la misma parte de la clave en cada caso, aunque también podría no ser así. La probabilidad de que sean las mismas letras con las mismas partes de la clave aumenta a medida que ese texto repetido es más largo. Es decir, a mayor longitud de la secuencia repetida en el texto cifrado, mayor es la probabilidad de repetición también en el texto en claro y en la clave. La búsqueda de esas coincidencias va generando información sobre la longitud de la clave, que es un primer paso. No hay que olvidar que el texto se cifra repitiendo la clave tantas veces como haga falta para completar lo que podríamos denominar como la cobertura del texto en claro.

Como sabemos, la clave sirve para cifrar el texto en claro y obtener el texto cifrado. Pero también sirve para descifrar el texto cifrado y volver al texto en claro. El método de Babbage permitía conocer la longitud de la clave e ir avanzando en la búsqueda de las letras de la misma, analizando de nuevo las frecuencias de sus apariciones. En resumidas cuentas, Babbage fue capaz de romper la cifra que hasta entonces se tenía por indescifrable y, por lo tanto, por totalmente segura: la cifra de Vigenère. Podría haber revolucionado entonces el mundo de la criptografía y haberle dado una lección al dentista, pero no ocurrió ninguna de esas dos cosas. El descubrimiento del brillante matemático quedó en un cajón de su propio estudio y nunca vio la luz, no fue hecho

público en modo alguno. Tuvieron que pasar varias décadas hasta que, ya en el siglo XX, se reveló el descubrimiento al estudiarse en profundidad todas las notas que había dejado Babbage. Para entonces, no obstante, otro hombre había roto ese tipo de cifrados usando una técnica similar y en ese caso sí se había hecho público el descubrimiento. Este hombre fue un oficial del ejército prusiano llamado Friedrich Wilhelm Kasiski, que consiguió este reto cuando ya estaba retirado. Publicó el método, que era un salto de gigante en el mundo del criptoanálisis, en el año 1863.

Cuando Kasiski hizo público su método para romper cifrados polialfabéticos, los criptoanalistas volvían a tener ventaja. Como hemos visto, el método ideado por Babbage y Kasiski, cada uno por su lado, no era complejo y suponía que los cifrados conocidos hasta entonces eran vulnerables. Solo los libros de códigos se mostraban como una vía sólida para mantener la seguridad de las comunicaciones, pero ya hemos visto que se deben mantener algunas precauciones y buenas prácticas de uso para que esa seguridad sea tal.

Durante el asedio de Jartum, en 1884, dentro de las guerras coloniales inglesas, el jefe de los británicos, el general Charles George Gordon, se vio rodeado por sus enemigos. Como hemos visto en otros casos, las comunicaciones seguras con el exterior son clave en los asedios, y en esta ocasión no era distinto. Los problemas para los británicos comenzaron cuando los africanos capturaron un barco, el *Abbas* , que entre otras cosas tenía los libros de códigos que se usaban en Jartum para comunicarse con el exterior. Gordon los había sacado de la ciudad para evitar que cayeran en manos enemigas, sabiendo que aquello le dejaba en una mala posición.

Tanto es así que se diseñó un plan para ayudar a la ciudad desde el exterior y se consiguió introducir dentro de ella un texto con los detalles. Pero el mensaje estaba codificado y los libros de códigos ya no estaban en manos de los criptógrafos de Gordon, por lo que no eran capaces de leer las instrucciones y el plan quedó en nada. En casos como este, usar métodos de cifrado basados en clave en lugar de libros de códigos hubiera significado una gran diferencia. El simple conocimiento de que la ayuda está en camino, en el caso de un asedio, puede significar la diferencia entre resistir y esperar, exprimiendo las fuerzas y los recursos, o intentar una salida arriesgada y casi suicida como última opción, cuando no optar directamente por la rendición. Esto es lo que ocurrió en Jartum. El mensaje codificado no sirvió de nada, ya que Gordon y sus hombres no fueron capaces de leerlo. Antes de la llegada de los refuerzos, Jartum cayó y Gordon fue decapitado. Su cabeza fue clavada y exhibida en una pica. Tan solo dos días después llegó la ayuda desde el exterior para descubrir que ya era demasiado tarde y que la ciudad había sido tomada.

12. Radiotelegrafía

A finales del siglo XIX la criptografía estaba en un punto complicado, con la gran cifra indescifrable de Vigenère rota y sin una alternativa que ofreciera seguridad a las comunicaciones, tanto civiles como militares. En este contexto apareció un nuevo invento que rompía las ataduras de la telegrafía al cable, a las líneas tendidas. Este nuevo avance llegó de la mano del físico italiano Guglielmo Marconi.

En 1894 Marconi comenzó a experimentar y a comprobar cómo un circuito eléctrico era capaz de generar una señal que influía en la corriente de otro circuito, con el que no tenía conexión directa y que estaba a cierta distancia. Aumentando la potencia, utilizando antenas, mejorando los circuitos… en poco tiempo aquellos pulsos de información saltaban distancias de más de dos kilómetros. La radio, el invento de Marconi, no necesitaba cables y unía a emisor y receptor por el aire. En 1896 Marconi emigró a Gran Bretaña y obtuvo la primera patente por su invento. El alcance de las emisiones fue aumentando y de salvar 15 kilómetros en el Canal de Bristol pasó no mucho después a comunicar ambos lados del Canal de la Mancha. Comunicaciones reales y fiables, sin requerir la construcción de líneas de telégrafo, sin los problemas del trazado, sin la necesidad de la inmovilidad del emisor y del receptor. En el último año del siglo XIX dos barcos que cubrían la Copa América, la carrera de vela más importante del mundo, fueron equipados con radio para que las noticias llegaran del mar a Norteamérica al momento y que cada día la prensa pudiera publicar cómo estaba marchando la competición. Las noticias volaban por el aire por primera vez en la historia.

El invento de Marconi atrajo el interés de los militares, como no podía ser de otra manera. Las posibilidades que se abrían para las comunicaciones en campaña, en combate, sin necesidad de tender cables, con toda libertad de movimientos, eran inmensas. La coordinación de la flota sería mucho más sencilla, con la posibilidad cierta de comunicación entre las naves e incluso de estas con tierra. Esa naturaleza de la radio que hace que las emisiones vayan en todas las direcciones es un valor esencial, pero también hace que la información llegue a todo el que esté dispuesto a escuchar, incluido el enemigo. La criptografía, una vez más y con mayor motivo, era la solución al problema.

La telegrafía sin hilos se vio desde el primer momento como una herramienta esencial para mejorar las comunicaciones de las unidades militares en campaña, a pesar de que también conllevaba peligros. El cambio en la guerra naval sería crucial, ya que las nuevas capacidades de comunicación permitirían que el mando en tierra fuera capaz de dirigir a la flota que estuviera en el mar equipada con radios de larga distancia. Hasta entonces, los almirantes y capitanes recibían

instrucciones antes de partir y una vez iniciada la navegación, las decisiones y la información eran suyas.

A la vez que Marconi desarrollaba su invento, un oficial naval británico, el capitán Henry Jackson, realizaba una serie de experimentos similares pare enviar señales sin hilos. Marconi ofreció su invento a los británicos y la Royal Navy colocó a Jackson al frente del proyecto que tenía como objetivo dotar a sus naves e instalaciones de telegrafía sin hilos y formar al personal que fuera a operar esta nueva forma de comunicación. Se creó una sección dedicada a este nuevo mundo en la escuela de torpedos HMS Vernon, aprovechando los conocimientos de ingeniería eléctrica que ya tenían algunos de sus miembros. El nombre que la escuela comparte con varios barcos de la historia naval británica, proviene precisamente de uno de esos barcos.

Uno de los colaboradores de Marconi, H. A. Madge, se instaló en la Escuela Vernon, como supervisor de los trabajos y formador. Madge se había graduado en Cambridge y estuvo allí desde 1908 hasta el comienzo de la Gran Guerra. A pesar de estos movimientos, parte de los mandos navales pensaba que el sistema era complejo y que la deficiente formación y conocimiento del mismo por parte del personal haría que en caso de guerra la duda y el peligro emergieran peligrosamente, por la falta de control y el uso ineficiente del nuevo sistema. Frente a esto, Winston Churchill, a la sazón primer lord del Almirantazgo, afirmaba que la comunicación inalámbrica, junto con la que se llevaba por cable, ofrecía la capacidad de intercambiar información, a menudo vital, con los barcos que estaban cerca o incluso en contacto con el enemigo. El centro de inteligencia, seguía Churchill, debe recibir toda la información posible, esté donde esté la fuente, y digerirla.

El ejército francés también se tomó con interés la telegrafía sin hilos y en 1903 se instaló en la misma Torre Eiffel una estación de comunicaciones que permitía llegar incluso a comunicarse con las unidades en Marruecos. La Torre Eiffel fue proyectada y levantada con la vista puesta en la Exposición Universal de París de 1889, y desde el principio se dotó a la idea de cierta función científica, ya que ese era un buen argumento para levantarla en un primer momento y, especialmente, para mantenerla en pie una vez pasada la exposición. Contra sus detractores se utilizaban las observaciones astronómicas y meteorológicas como una barrera, así como los posibles experimentos que se podrían llevar a cabo. Era un puesto de observación privilegiado, advertían sus impulsores, y un puesto de comunicación esencial para el telégrafo óptico del que ya hemos hablado. Por todo esto no es de extrañar que fuera allí donde se hicieron las primeras pruebas de telegrafía sin hilos y donde se instalaron los equipos militares.

Los alemanes, como el resto de países, tenían gente adentrándose en el uso de la telegrafía sin hilos. La marina germana, a través de su Admiralstab, su Estado Mayor del Almirantazgo, había ordenado la instalación de una potente estación de comunicaciones en Nauen, un pequeño pueblo a menos de 40 kilómetros de Berlín, que sigue siendo

hoy conocido por aquel hecho, ya que tiene la instalación para emisiones de radio más antigua que sigue en pie. Desde allí los alemanes podían enviar señales de radio de onda larga que, idealmente, les permitían comunicar con cualquiera de sus unidades militares, especialmente las navales.

Todos los países, además del uso de las capacidades existentes, investigaban cómo mejorar los sistemas, aumentar la distancia de las comunicaciones y mejorar su calidad. En cualquier caso, era un mundo incipiente con muchas dudas y problemas para el uso práctico, pero la investigación daba sus frutos de manera recurrente. Los equipos permitían cada vez mejor calidad en la señal, mejores transmisores, una recepción más clara y mayores capacidades de control sobre las señales y su envío. No es de extrañar que esta idea de recibir información por el aire, de comunicarse sin necesidad de hilos, asombrara también a la población civil, por lo que poco a poco fueron apareciendo radioaficionados que tenían equipos más modestos pero que jugaron su papel en la guerra europea que estaba por venir.

La gran contrapartida de todo esto era la que ya conocemos: las comunicaciones inalámbricas, como ya hemos advertido, son capturadas también por el enemigo, por lo que se deben cifrar o codificar para mantener la información oculta a sus ojos. Esos aficionados civiles a los que hacíamos referencia hace un momento, también serían puntos de captura de información, extendiendo así la imaginaria tela de araña de cada país por donde las comunicaciones pasan.

En la guerra ruso-japonesa de 1904, los nipones habían dotado a su flota con aparatos de radio. No eran demasiado avanzados ni potentes, ya que solo operaban en una frecuencia y su alcance era de algo menos de cien kilómetros. Los rusos habían hecho lo mismo, tanto en las naves como en algunas posiciones terrestres. En este contexto tuvo lugar lo que podríamos considerar como el primer caso de análisis de tráfico de señales de la historia. Los rusos cayeron en la cuenta de que a cada ataque japonés le precedía un aumento del número de mensajes intercambiados por sus mandos.

Una de las reflexiones básicas de la criptografía se la debemos a Kerckhoffs y es ciertamente relevante en el mundo que estamos exponiendo, con comunicaciones ubicuas, abiertas y a la vista del enemigo. A finales del siglo XIX Auguste Kerckhoffs, un lingüista holandés que trabajó como profesor, llevó a cabo un trabajo, que publicó en varias partes, en el que estableció la base teórica que permite definir los métodos criptográficos como seguros. Veremos más adelante cómo sobre esta vía establecida por él se siguió avanzando. Kerckhoffs expuso que la seguridad de un sistema criptográfico se basa totalmente en el secreto de la clave. Esto, que es conocido como el principio de Kerckhoffs, sigue siendo hoy una realidad y un patrón conceptual sobre el que se apoyan la mayoría de los métodos criptográficos. Llevada esta aseveración a la actualidad, vemos que no es importante el algoritmo de encriptación, lo

que estamos llamando método de cifrado, sino que es la clave la que otorga la seguridad. Hoy, los algoritmos son públicos y conocidos, pero mientras la clave no sea conocida, en términos generales la seguridad permanece. Dicho de otro modo, debemos dar por sentado que el criptoanalista que trate de romper un mensaje cifrado por nosotros conoce el método para cifrar y descifrar y, por supuesto, tiene acceso al propio mensaje cifrado.

Las reglas que marcaba Kerckhoffs en sus artículos como elementos deseables en cualquier método o sistema criptográfico son las siguientes:

Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.

La efectividad del sistema no debe depender de que su diseño permanezca en secreto.

La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.

Los criptogramas deberán dar resultados alfanuméricos.

El sistema debe ser operable por una única persona.

El sistema debe ser fácil de utilizar.

Claude Shannon, que es uno de los personajes clave en el mundo de las tecnologías de la información, tenía una forma más gráfica y directa de explicar el principio de Kerckhoffs: ten por seguro que el enemigo conoce el sistema.

13. La primera guerra mundial y la sala 40

En la Gran Guerra la criptografía jugaría un papel esencial en varias situaciones. Ya saben que cuando hablamos de que la criptografía fue importante en un acontecimiento, solemos hacerlo precisamente porque falló en su cometido de mantener el texto seguro y oculto frente a los ojos de cualquiera que no sea su legítimo destinatario. Esto, lógicamente, es lo extraño. Lo habitual suele ser que la criptografía pase desapercibida porque su papel es efectivo. Antes incluso de que comenzara la Gran Guerra, la Primera Guerra Mundial, la criptografía ya tuvo cierta relevancia para su desarrollo.

Los servicios de inteligencia y criptografía franceses interceptaron un largo mensaje emitido desde el Ministerio de Asuntos Exteriores alemán, con destino a su embajada en París. El texto iba cifrado, pero los franceses fueron capaces de ponerlo en claro. Era la declaración de guerra a Francia. Para ganar cierto tiempo y poder mejorar así su preparación para la guerra e incluso para tomar algunas decisiones, los franceses alteraron el mensaje para que fuera incomprensible para el embajador alemán.

El 28 de julio de 1914 el Imperio austrohúngaro declaró la guerra a Serbia. El 1 de agosto Alemania declaró la guerra a Rusia, y dos días después hacía lo mismo con Francia e invadía Bélgica, declarándole la guerra oficialmente al día siguiente. El día 5 Montenegro envió la declaración de guerra a Austria-Hungría y el día 6 Serbia comenzó la guerra con Alemania y el Imperio austrohúngaro entró en guerra con Rusia. El día 7 de agosto algunas tropas británicas desembarcaron en Francia y el 12 de agosto, Francia y Gran Bretaña declararon la guerra a Austria-Hungría.

En medio de esos días, a las pocas horas de haber comenzado la Primera Guerra Mundial y antes de que oficialmente los británicos se vieran embarcados en ella, una conversación entre el responsable de la inteligencia del Almirantazgo, el contraalmirante Henry Francis Oliver, y el director de Educación Naval, *sir* James Alfred Ewing, impulsó la creación de una unidad clave en la criptología de la Primera Guerra Mundial, y más allá. Aquella conversación tuvo lugar de manera informal durante un almuerzo en el club Pall Mall. Oliver le comentó a Ewing que durante los últimos días había recibido en su oficina comunicaciones capturadas a los alemanes, pero que de nada le habían servido en su labor de inteligencia y que estaban cifradas o escritas en algún código que no sabían romper. Ewing era aficionado a la criptografía, y de ahí el que Oliver le hiciera el comentario. Con el panorama que estaba presentando Europa en aquellos días, era obvio que las comunicaciones, y por lo tanto la información capturada, iba a crecer de manera importante y que era urgente poner solución al problema. Oliver le ofreció a Ewing que dejara de lado temporalmente

su labor en el ámbito de la formación y se hiciera cargo de una nueva sección en su oficina, una sección que, lógicamente, se dedicaría a la criptografía y en la que Ewing podría poner al servicio de su país los conocimientos que tenía en ese campo.

Ewing era físico e ingeniero y había nacido en Escocia en 1855. Para cuando llegó la Primera Guerra Mundial ya era un hombre de alto prestigio que había pasado por varias instituciones educativas y era un referente en las propiedades magnéticas de los materiales. Había sido nombrado caballero en 1911 y el propio Oliver lo describió como un hombre distinguido, que cuidaba su aspecto y su forma de vestir al máximo para mostrar siempre la dignidad de su posición.

Acorde a su forma de pensar y de conducirse como científico, Ewing sabía que sus conocimientos de criptografía no eran suficientemente profundos y, por lo tanto, tras aceptar el puesto, comenzó un periodo de estudio en el que visitó a otros expertos y se adentró en los libros de criptografía, a la vez que los mensajes alemanes capturados seguían llegando a la oficina de inteligencia que dirigía su amigo Oliver. El flujo cada vez era mayor, y ya superaba el centenar de comunicaciones diarias, lo que puso de manifiesto que aquel trabajo iba a ser demasiado para un solo hombre. Ewing necesitaría ayuda y se puso a buscarla. Siendo la labor tan delicada, ya que hablamos de una tarea relacionada con la inteligencia y en la que el secreto y la discreción son tan importantes como los conocimientos técnicos, Ewing se apoyó en sus contactos en las escuelas navales. Personas que había conocido como responsable de formación naval y que eran dignas de su confianza.

Como ha ocurrido innumerables veces a lo largo de la historia, las tareas relacionadas con el espionaje, y las labores criptográficas deben incluirse en ese ámbito, no eran entonces muy bien vistas por los mandos militares. Creían que era una forma poco honorable y digna de afrontar la guerra. En cualquier caso, y si bien en ocasiones las formas de conseguir los mensajes enemigos no son del todo limpias, la captura del tráfico enemigo y el criptoanálisis de las comunicaciones era necesario para afrontar la guerra. Tanto es así que pocos días después de que Ewing se hiciera cargo de su nuevo puesto, el general *sir* George Macdonogh, el director de la Inteligencia Militar dentro de la Oficina de Guerra británica, se acercó a él para hacerle una propuesta. El ejército, en su visión más amplia, estaba interceptando cada vez más mensajes cifrados del enemigo, y lo cierto es que no sabían qué hacer con ellos. Macdonogh pidió a Ewing colaboración para que el conocimiento que tenían y el que tuvieran en el futuro en la Inteligencia Naval se filtrara a otras unidades del ejército. La idea pareció buena en un primer momento, pero lo cierto es que las reticencias de unos y otros y sus rivalidades consiguieron apagar esa colaboración.

Al comenzar la guerra, la marina británica tan solo tenía una estación de escucha de emisiones de onda larga, situada en la costa noreste. Esto suponía una limitación para cubrir todas las posibles comunicaciones enemigas o interesantes para el devenir de la guerra, pero la ayuda les

llegó desde la población civil. Un abogado llamado Russell Clarke, junto con algún otro radioaficionado, había estado escuchando las señales navales alemanas, ya desde antes de la guerra, por puro entretenimiento. Una vez iniciado el conflicto, no tardaron en ponerse en contacto con el ejército para proporcionarle información y ofrecerle su ayuda. Ewing, que era el primer interesado en que se capturaran mensajes enemigos, ya que eran la base de su trabajo, consiguió dotar a Clarke de una estación de escucha en el este, en Norfolk, por donde eran escuchadas las señales enemigas en el ámbito del Mar del Norte. Ewing se apoyó también en la compañía Marconi para colocar varias estaciones y no tardó en superar la decena de puestos de escucha, por donde el tráfico de comunicaciones navales alemanas iba directo a su mesa de trabajo. Los mensajes se capturaban encriptados, por supuesto, pero sin mensajes no había nada que hacer y con ellos sus criptoanalistas tenían algo sobre lo que trabajar.

Ese grupo de criptoanalistas tenía que romper, para comenzar, los métodos de cifrado y codificación que estaban usando los alemanes, pero la importancia de su trabajo se fue haciendo patente con el paso de los días, lo que hizo que nuevas personas se incorporaran al equipo. El despacho de Ewing, que era donde habían estado trabajando desde el comienzo, no tardó en quedarse pequeño. En la primera planta del ala derecha del edificio se habilitó una sala para que trabajaran y se trasladó allí a todo el equipo. El sitio era perfecto porque en el mismo pasillo estaban los más altos mandos y por lo tanto era una zona de acceso restringido. Junto a la sala que asignaron a los criptógrafos se acondicionó otra como sala de descanso, con camas de campaña, en previsión de largas jornadas de trabajo. El área fue nombrada con el número que el Almirantazgo había asignado burocráticamente a aquella sala del edificio: la sala 40. Desde entonces, el área de criptoanálisis del Almirantazgo se conocería como la Sala 40, Room 40 en su idioma original.

El personal de la Sala 40 era variado, como es habitual en los equipos de criptoanálisis. Había lingüistas, científicos, expertos en crucigramas y juegos similares y, por supuesto, algún militar. Un buen ejemplo de este tipo de perfiles es el caso de Alexander Denniston, un lingüista brillante, que había estudiado en La Sorbona y en la Universidad de Bonn, por lo que conocía el idioma alemán en detalle. Otro de los seleccionados al comienzo de la guerra fue William Montgomery, un reverendo que había traducido varias obras teológicas del alemán al inglés y que había demostrado su interés y dotes para la criptografía al descifrar un mensaje secreto que se había recibido en una postal. En realidad, el mensaje era tan secreto que no había tal mensaje, ya que la postal llegó en blanco y tan solo tenía escrita la dirección: *sir* Henry Jones, calle del Rey, 184; Tighnabruaich, Escocia. El destinatario, *sir* Henry Jones, tenía un hijo prisionero de los turcos y la postal había llegado desde Turquía, por lo que el destinatario pensó al momento que era un mensaje de su hijo. El pueblo, Tighnabruaich, no era muy grande, por lo que no hubo problema en que el servicio postal local entregara la carta a *sir* Henry Jones, el único habitante con ese nombre, a pesar de que la dirección era incorrecta, ya que no existía ninguna calle del Rey

en la localidad. La historia llegó a manos del reverendo Montgomery y no tardó en generar alguna hipótesis y ver dónde le llevaba. Sin duda la dirección era un código, ya que no tenía sentido que el emisor, dando por sentado que era el hijo cautivo de *sir* Henry, supiera el nombre y la localidad y se inventara el resto de la dirección sin motivo aparente. La calle y el número eran la clave de acceso y el reverendo pensó que la Biblia, bien conocida por emisor y receptor y con mensajes suficientes casi para contar cualquier cosa, podía ser una buena referencia. Calle del Rey bien podría ser el Libro de los Reyes y el 184 podrían ser varias cosas, entre otras, capítulo 18 y versículo 4. Ese texto reza: «Porque cuando Jezabel destruía a los profetas de Jehová, Abdías tomó cien profetas, los cuales escondió de cincuenta en cincuenta por cuevas, y sustentolos a pan y agua». El mensaje que enviaba el hijo al padre era que estaba preso, pero que tenía pan y agua, o lo que es lo mismo, que en la medida de lo posible estaba siendo bien cuidado, lo que debería tranquilizar a *sir* Henry. Por supuesto, si había alguna censura o algún control por parte de los turcos, no había problema, ya que la postal no decía nada. En cualquier caso, la mente del reverendo Montgomery había mostrado que disfrutaba con este tipo de juegos y que era capaz de generar hipótesis sobre mensajes y cómo ocultarlos, una diversión que sería de gran valor como trabajo serio dentro de la Sala 40.

A pesar de los éxitos de la Sala 40 contra los códigos alemanes, lo cierto es que estos también disponían de un servicio de criptografía competente que se hizo con los códigos de Francia, Reino Unido y Rusia. Este último país tuvo algunos problemas con la utilización de sus propios códigos. Por otra parte, a pesar de que las comunicaciones vía radio, la telegrafía sin hilos, como se la conocía, ya se habían probado en la guerra ruso-japonesa de los años 1904 y 1905, lo cierto es que aún era una tecnología con limitaciones. Los instrumentos de envío eran aparatosos, lo que no hacía fácil su transporte, y además su uso hacía que las transmisiones fueran lentas, lo que, si se añadía a la encriptación, sumaba un tiempo desesperante. Esto hacía que en ocasiones se dejara de lado la seguridad en beneficio de la practicidad y no se codificaran los mensajes enviados por radio. Los rusos fueron especialmente descuidados en este aspecto, lo que ayudó en muchas ocasiones a sus enemigos, que obtenían información solvente y fiable sin mucho esfuerzo.

El Primer y Segundo Ejército rusos estaban operando en 1914 en territorios que hoy pertenecen a Polonia y sospechaban que sus viejos códigos criptográficos eran conocidos por el enemigo, por lo que trabajaron en nuevas versiones más complicadas, confiando en que aquello hiciera seguras las comunicaciones por radio que ambos ejércitos rusos tenían que compartir para coordinarse en el combate. Durante los primeros meses se dieron situaciones tan extrañas como que el nuevo código solo era conocido por uno de los ejércitos, por lo que el otro no era capaz de entender sus comunicaciones. Cuando el Segundo Ejército, que sí conocía los nuevos códigos, se dio cuenta del problema, volvió a utilizar los códigos anteriores, que se tenían por inseguros, pero el mando del Primer Ejército ya había recibido la orden de descartarlos y de utilizar el nuevo código, lo que acabó causando de

nuevo que las comunicaciones se perdieran. En resumen, hizo aparición el caos en las filas rusas.

En medio de aquellos problemas de comunicaciones entre los rusos, los alemanes, comandados por el general Paul von Hindenburg, acertaron a jugar sus cartas. Hindenburg se había retirado del ejército unos años antes, en 1911, cuando ya tenía sesenta y tres años. Con el arranque de la Gran Guerra retornó al ejército alemán, como comandante del Octavo Ejército, que combatía en el Frente Oriental. El nuevo general al mando del Octavo tenía como jefe de su Estado Mayor a Erich Ludendorff. Este continuó con el plan que había diseñado el coronel Hoffman y que había comenzado antes de la llegada de Hindenburg y Ludendorff. Los dos ejércitos rusos involucrados, el Primero y el Segundo, que operaban respectivamente bajo el mando de los generales Rennenkampf y Samsónov, se comunicaban constantemente y todo indicaba que los alemanes sucumbirían. De hecho, Hindenburg estaba allí a petición de Moltke, después de que el general Prittwitz recomendara que su Octavo Ejército retrocediera hasta el Vístula.

El plan alemán esperaba que las dos columnas rusas continuaran avanzando de manera independiente, y proponía que parte de las tropas se movieran rápidamente en tren hasta el extremo izquierdo de las posiciones del Segundo Ejército ruso, mientras otras unidades alemanas se enfrentaban al flanco derecho. Es decir, la mayoría de las fuerzas alemanas marcharían contra el ejército de Samsónov, mientras que se llevaba a cabo una operación de engaño con unos pocos efectivos que hiciera creer al Primer Ejército ruso que Königsberg estaba mejor defendida y por lo tanto tomara más precauciones en el ataque y los movimientos rusos se retrasaran. Era un plan muy arriesgado y audaz, pero era una baza a jugar por los alemanes, que sabían su desventaja global, a pesar de combatir en terreno propio y de mantener intacta la red ferroviaria en la zona, clave para el movimiento de tropas. Por otra parte, se sustentaba sobre la hipótesis del avance independiente de los ejércitos rusos, una suposición que se apoyaba en información capturada.

El general de caballería ruso Yakov Zhilinsky era el destinatario de un mensaje enviado por Rennenkempf: «Detenido temporalmente. Imposible avanzar ya que los trenes de suministro no han llegado». El mensaje, enviado por radio, fue capturado por los alemanes y leído sin problemas. Los rusos estaban fuera de la zona con líneas telegráficas tendidas, por lo que no tenían otra opción que utilizar la radio y, como ya hemos comentado, sus problemas con los códigos y los equipos los llevaban a dejar de lado la seguridad. Ese fue el caso del mensaje de Rennenkempf, que no había sido codificado. Cuando los mandos alemanes se toparon con aquel mensaje, su primer impulso fue dudar de su veracidad, con buen criterio, ya que bien podría ser una tetra, un engaño. La confirmación no tardó en llegar, pues varios mensajes más, tanto enviados en abierto como protegidos por débiles códigos que los alemanes no tardaron en romper, pusieron a los alemanes ante una visión clara de la situación. Su plan estaba funcionando.

Los alemanes hicieron eficientes movimientos masivos de tropas usando el ferrocarril, colocándose en aquellos lugares donde más daño podían hacer a los rusos. Conocer los planes de estos, sus posiciones y sus fuerzas era una ventaja que no se podía desaprovechar. Y la causa de todo era la incapacidad de los rusos para usar de manera adecuada la criptografía.

El resultado de aquella batalla de agosto de 1914, conocida como la batalla de Tannenberg, que no hay que confundir con la batalla homónima de 1410, donde la Orden Teutónica venció a polacos y lituanos, fue una victoria brillante de los germanos. De hecho, comparten nombre ambas batallas, la medieval y la batalla de la Gran Guerra, en gran medida porque los alemanes querían unir la épica de ambas victorias. Acababa de comenzar la Primera Guerra Mundial y, contra pronóstico, el Segundo Ejército ruso quedó arrasado y se puso la primera piedra para que también el Primer Ejército acabara consumido. Estas pérdidas dejaron a los rusos en una situación precaria de la que tardarían meses en recuperarse.

El día 30 de agosto, cuando vio a su ejército derrotado, el general Samsónov le dijo a su jefe de Estado Mayor que no se sentía capaz de explicarle aquella catástrofe al zar después de que este hubiera confiado en él. Decenas de miles de rusos se movían en retirada. Entre las bajas, los 30.000 muertos, además de 50.000 heridos y más de 90.000 prisioneros rusos, de la batalla de Tannenberg, estaba un hombre que se disparó con su revólver en la cabeza. El hombre que había decidido acabar con su vida antes de tener que explicar aquella debacle a su zar era Alexander Samsónov. En el otro lado, Hindenburg, recién reincorporado al ejército alemán, firmaba una victoria rutilante.

Por otra parte, si bien al principio de la guerra los franceses no eran capaces de descifrar los códigos alemanes con la facilidad suficiente y la rapidez necesaria como para que sirviera para una ruptura en el campo de batalla, sí podían conocer las posiciones de las unidades, su tamaño e intuir sus movimientos, a partir del tráfico de radio y de ciertos indicadores en los mensajes. Parte de las tropas alemanas no tenían personal con formación en criptografía y eso hacía que se enviaran mensajes en claro e incluso comunicaciones sin cifrar con preguntas sobre los códigos. Esto, junto con la captura de información en alguna acción de guerra por los franceses, hizo que estos fueran capaces de obtener algunas claves y por lo tanto descifrar las comunicaciones alemanas.

Esto hizo posible, por ejemplo, que en el otoño de 1914 los franceses organizaran más efectivamente sus posiciones al conocer con cierta antelación los objetivos de las tropas alemanas.

La armada alemana utilizaba libros de códigos para proteger sus comunicaciones, que, gracias a la radio, permitían mantener en contacto, coordinados e informados a los buques incluso cuando estaban lejos de la costa. Era una gran ventaja, pero como ya hemos

comentado, los libros de códigos no se pueden cambiar en un plazo corto de tiempo, cosa que sí ocurriría con un método de cifrado tan solo cambiando la clave. Esto lo acabó pagando caro la armada germana, ya que tan solo un mes después de comenzar la guerra, el crucero alemán *SMS Magdeburg* ayudó de manera involuntaria a los ingleses.

El *SMS Magdeburg* era un crucero ligero de la Kaiserliche, la Marina Imperial alemana, que, en los primeros días de la guerra, en el verano de 1914, fue enviado al Mar Báltico. El día 25 de agosto, en una operación de reconocimiento en torno al Golfo de Finlandia, el buque encalló. Mientras intentaban resolver la situación tratando de remolcarlo con un destructor, aparecieron dos barcos rusos que atacaron al buque alemán varado. Obligados a dejar la nave, los germanos trataron de hundirla, pero no lo consiguieron, y lo más grave fue que entre el caos y las prisas por abandonar el barco, no cayeron en la cuenta de que debían destruir o de llevarse con ellos el libro de códigos. Una vez que los rusos subieron a bordo del *SMS Magdeburg* y comenzaron a registrarlo, encontraron el libro de códigos de la marina de guerra alemana, Signalbuch der Kaiserlichen Marine, además de otra información importante como la clave activa en aquel momento y un mapa del Mar Báltico y del Mar del Norte que mostraba también la rejilla que permitía a los alemanes indicar dónde estaba cada barco. Algo así como el mapa del juego de los barcos, donde cada celda se usaba para indicar en qué zona de aquellos mares estaba un buque o a cuál debía moverse. Todo ello dotaba a los enemigos de Alemania de la capacidad de romper las comunicaciones de su armada y la posibilidad de leer los mensajes que enviara. Mensajes que, no hay que olvidarlo, se enviaban por radio y por lo tanto estaban potencialmente al alcance de todos, tanto los propios marinos del káiser como sus enemigos. Los rusos entregaron poco después el libro a Inglaterra, que sacó un gran partido de ese regalo de sus aliados. Concretamente el 13 de octubre de 1914, el capitán Smirnoff, de la Armada Imperial rusa, se encontró con Winston Churchill y compartió todo lo capturado. Una muestra más de la importancia de la captura, si tenemos en cuenta los personajes que intercambiaron el botín del *SMS Magdeburg* .

El libro de códigos del *SMS Magdeburg* establecía que todos ellos tenían cuatro letras, siendo la primera y la tercera consonantes, y la segunda y la cuarta vocales. Esto tenía una gran ventaja, todas las palabras del código eran pronunciables, lo que seguramente era de gran ayuda en la transmisión, donde alguien le dictaría al emisor real las palabras. De todas formas, los alemanes eran precavidos y sus comunicaciones, además de ir codificadas de acuerdo a un libro como el que llevaba el *SMS Magdeburg* , eran cifradas. En resumen, tener el libro de códigos era una gran ayuda para los británicos y para los rusos, pero no resolvía el puzle en su totalidad.

Dicho esto, en la Sala 40 no tardaron mucho en romper el cifrado. Un detalle interesante es que si alguien se había tomado la molestia de que al codificar cada código este fuera pronunciable con esa estructura de vocales y consonantes que hemos comentado, no tendría mucho sentido

perder tal estructura con el cifrado. Así, el cifrado sustituía las vocales por vocales y las consonantes por consonantes. Esto supuso una ayuda importante para los criptoanalistas que fueron capaces de romper el cifrado. Cada vez que los alemanes cambiaban la clave del cifrado, sus enemigos tenían que repetir el proceso, aunque la ventaja seguía de su lado. En 1914, cuando se capturó el *SMS Magdeburg* , la clave era modificada cada tres meses, aunque con el paso del tiempo fueron mejorando la seguridad y en 1916 era cambiada cada noche.

Los submarinos alemanes usaban para asegurar sus comunicaciones el mismo código que los buques de superficie, si bien la parte del cifrado era diferente. El método que utilizaban los submarinos era una trasposición de columnas, pero de nuevo la clave no era modificada con la regularidad suficiente, por lo que los británicos eran capaces de leer sin problemas todas sus comunicaciones.

La lección aprendida con el *SMS Magdeburg* hizo que los ingleses se tomaran en lo sucesivo ciertas molestias para buscar los libros de códigos del enemigo siempre que tenían ocasión, es decir, cuando capturaban un barco enemigo o incluso cuando lo hundían y el pecio quedaba a una profundidad razonable para intentar llegar hasta él. Esto ocurrió con un submarino alemán que fue hundido cerca de la costa inglesa, que un buzo registró hasta encontrar los libros de códigos. Incluso en una ocasión, los restos de un zepelín abatido dieron a los ingleses la ocasión de conocer los códigos que estaban utilizando sus enemigos.

Los británicos llegaron a tener un especialista en este tipo de operaciones en los pecios alemanes. El submarinista de la Royal Navy, E. C. Miller estaba especializado en acciones a gran profundidad y sus servicios dieron algunos réditos interesantes para la Sala 40. En 1915, por ejemplo, le encargaron sumergirse y buscar en un submarino enemigo que se había hundido frente a la costa de Kent, en el extremo sureste del país. Miller encontró una caja metálica en la cámara de oficiales del submarino que contenía los planos de los campos de minas alemanes, los códigos de la marina y un código de alto secreto destinado a comunicarse en alta mar con los buques.

Por suerte para los ingleses, el del *SMS Magdeburg* no fue un caso aislado. A mediados de agosto de 1914, antes incluso del accidente del *SMS Magdeburg* , el mercante alemán a vapor *Hobart* rondaba la costa de Melbourne, en el sureste de Australia, cuando un oficial de la armada australiana, el capitán Richardson, subió a bordo del barco para hacer una inspección de seguridad. Iba disfrazado de personal civil y se identificó como un agente público encargado del control de posibles cuarentenas a aplicar sobre el cargamento. El capitán del *Hobart* no debió de sospechar nada, ya que probablemente ni siquiera sabía que la guerra había comenzado en Europa tan solo unos días antes. En cualquier caso, no entraba dentro de los planes del capitán alemán dejar que los australianos tuvieran acceso a algunos importantes documentos que llevaba a bordo, entre los que estaba el

Handelsverkehrbuch (HVR), el libro de códigos que la armada alemana le había entregado y que permitía que los buques mercantes y los buques militares de la Flota de Alta Mar alemana intercambiaran comunicaciones. El capitán del *Hobart* trató de ocultar los documentos, pero fueron descubiertos y Richardson se los pidió amablemente, a punta de pistola.

Si bien aquellos libros de códigos capturados al *Hobart* eran considerados interesantes, no se les dio en Australia la importancia real que tenían y durante un mes no se informó al Almirantazgo británico de la captura. Cuando por fin se hizo el informe, se dio inmediatamente la orden de llevar aquel libro de códigos a Londres lo más rápido posible. Incluso el método más rápido para hacer aquel transporte invertía varias semanas en cubrir la distancia, por lo que el libro no llegó hasta octubre a la capital británica. Para entonces, ya había ocurrido el accidente del *SMS Magdeburg* .

Otro golpe de suerte para los británicos en aquellos primeros meses de conflicto en el ámbito criptográfico ocurrió a mediados de octubre, cuando cuatro destructores germanos que estaban minando la costa holandesa fueron sorprendidos por una flotilla de la Royal Navy, que acabó hundiéndolos. Solo uno de los buques alemanes tenía libros de códigos a bordo, y su capitán, siguiendo las instrucciones que tenía entonces para aquel tipo de situaciones, metió los documentos en una caja de plomo y la lanzó por la borda. Aquello parecía una buena idea, pero como decíamos, la suerte estuvo en este caso del lado británico.

Unas semanas después, en los últimos días de noviembre, un barco pesquero de arrastre tuvo la suerte de atrapar en su red la caja que había lanzado el destructor alemán. Esta y su contenido acabaron en el Almirantazgo en Londres, que conseguía de aquella forma un nuevo libro de códigos alemán, el Verkehrsbuch.

La Royal Navy, la armada británica, también utilizaba códigos para asegurar sus comunicaciones. Estos códigos eran amplísimos catálogos de palabras, cuya codificación las convertía en secuencias de cinco números, y como era de esperar tenían un buen número de homófonos, es decir, de palabras con varias opciones diferentes para la codificación. Además de los homófonos, los británicos empleaban en sus códigos polífonos, que es justo lo contrario. Es decir, había códigos, secuencias de cinco números, que podían significar diferentes palabras a la hora de descodificar el texto, de pasar del código al texto en claro. La identificación de las palabras en claro que se correspondían con el código polífono se hacía mediante un sistema de letras que acompañaba al código y que indicaba cómo hacer la sustitución.

El libro de códigos alemán capturado gracias al accidente del *SMS Magdeburg* permitía a la Sala 40 descifrar tan solo una parte de los mensajes de la armada alemana que capturaban, pero eran mensajes sin relevancia, a menudo meros informes meteorológicos. La mayoría de las comunicaciones seguían ocultas para los criptógrafos británicos.

Como hemos visto otras tantas veces a lo largo de la historia, el criptoanálisis no es un camino recto, sino que es más equiparable a un árbol donde tan solo una de las ramas lleva al fruto, al éxito. Se trata, por tanto, de ir probando caminos y descartando opciones. Y una vez que uno toma el camino adecuado, poco a poco, cada paso ilumina aún más ese camino correcto y hace más obvio y sencillo el siguiente paso.

Así, cuando el oficial de la Royal Navy Charles Rotter, que era un buen conocedor del alemán, vio algunos de los mensajes, pensó que quizás se trataba de un cifrado doble, es decir, que después de codificado el mensaje en claro, ese texto codificado se había vuelto a alterar sustituyendo unas letras por otras mediante algún tipo de clave. Rotter ya tenía un camino que tomar dentro del árbol. Comenzó buscando en los mensajes secuencias que pudieran corresponder a palabras comunes en alemán en ese contexto naval. Probando posibilidades, buscando palabras en los mensajes, junto con los libros de códigos, sin los que el trabajo no habría tenido sentido, fue decodificando pequeños fragmentos, algunas letras que le llevaban a probar con palabras, no ya tan comunes pero posibles a juzgar por las letras que ya conocía. En aproximadamente una semana, Rotter había encontrado la clave que estaban utilizando los alemanes para cifrar los mensajes, una vez codificados con el libro que llevaba el *SMS Magdeburg* . Con la clave y el libro, la Sala 40 conocía dónde estaba la fruta del árbol, cómo alcanzarla en cada mensaje capturado y si estaba cifrado con aquel código naval. Así, desde noviembre de 1914, la Sala 40 se centró en los mensajes de la armada alemana y el conocimiento que generaron para su bando fue clave. Conocían las operaciones y los movimientos de la flota de alta mar germana con un nivel de detalle más que suficiente para jugar con una gran ventaja.

Aquel mismo noviembre de 1914, Henry Francis Oliver fue ascendido y su puesto en la dirección de la inteligencia del Almirantazgo fue ocupado por el capitán Reginald William Hall. Este no conocía lo que se estaba haciendo en la Sala 40 antes de llegar al puesto, lo que muestra claramente la cautela y secreto que se mantenía en torno a ese pequeño grupo de hombres y su labor. Para Hall, lo que se estaba haciendo con los códigos navales alemanes era una gran noticia, pero determinó que había que ir más allá y conseguir también conocer otra información: los cables diplomáticos.

La Sala 40 interceptó durante la guerra mensajes alemanes por toda Europa y por otras partes del mundo. Los agentes alemanes enviaban y recibían información por radio que de uno u otro modo acababa en manos de los británicos, y estos sacaban partido de ello. Como es habitual a lo largo de la historia, el espionaje y la criptografía fueron de la mano. Esta sirvió para que el espionaje se pudiera llevar a cabo, en muchos casos, y el espionaje sirvió de fuente de información para la criptografía de manera constante. En ocasiones, capturando mensajes cifrados, pero en otras haciéndose directamente con los libros de códigos o información de similar importancia.

La Sala 40 se aprovechó también de esta relación de beneficio mutuo. Por ejemplo, gracias a una acción de espionaje los británicos consiguieron romper el código diplomático alemán, algo que, como veremos con el telegrama Zimmermann, acabó por tener unas consecuencias enormes. Alexander Szek eran un joven belga que tenía ciertas dotes para la telegrafía, lo que acabó por hacer que los británicos contactaran con él. Hablaba varios idiomas y, tras la toma de Bruselas por los alemanes en agosto de 1914, estos le pidieron ayuda técnica precisamente con sus aparatos de radiotelegrafía. Se vio más o menos forzado a ponerse al servicio de los británicos para espiar a los alemanes, con los que tenía una relación estrecha. Tenía acceso al código diplomático alemán y poco a poco fue copiándolo y entregándoselo a sus contactos del espionaje británico. No podía robarlo o actuar de manera descuidada, ya que el menor apunte de sospecha de los alemanes les haría cambiar el código y mejorar la seguridad. Szek vivió una situación para la que no estaba preparado y que requería unos nervios que el joven no tenía. Poco después, en 1915, Szek murió en circunstancias poco claras. No hay muchas certezas sobre la muerte del joven. Los británicos incluso llegaron a negar que hubiera trabajado para ellos, algo que algunas memorias, publicadas décadas después, desmienten.

14. El telegrama Zimmermann

A mediados de enero de 1917 la Inteligencia Naval británica interceptó en la Sala 40 un telegrama, encriptado. El destinatario era el embajador alemán en Washington y el remitente era Arthur Zimmermann, nombre que gracias a ese telegrama pasaría a la historia, ya que las consecuencias de aquella interceptación de las comunicaciones acabaron por cambiar el rumbo de la Primera Guerra Mundial. A esas alturas de la guerra, el conocimiento que se tenía en Londres de los códigos alemanes era más que notable y la Sala 40 hacía su trabajo sigilosamente, alimentada por una red de puestos de escucha que los británicos habían sembrado por todo el territorio para capturar las comunicaciones inalámbricas alemanas.

La situación de la guerra, tras dos años largos, era de estancamiento y los alemanes buscaban reforzar su posición y asfixiar a su gran enemigo. El frente del oeste era una lucha terrible por unas pocas centenas de metros adelante o atrás de la línea de trincheras, donde ganar ese ínfimo terreno tenía un precio enorme en vidas y recursos. Es la imagen asociada a la Primera Guerra Mundial en la cultura popular, las trincheras del frente del oeste, estancadas, embarradas, oscuras, grises y devoradoras de vidas. Los brutales bombardeos y los asaltos suicidas de los soldados contra las alambradas y las posiciones enemigas. La guerra en el mar tampoco era decisiva, y si bien tras la batalla de Jutlandia los británicos mantenían bajo control a la flota alemana en el Atlántico Norte, los submarinos germanos hundían los mercantes que partían o iban con destino a las islas británicas. Este estrangulamiento, como ocurriría también en la Segunda Guerra Mundial, tenía como vía de escape la ayuda, en forma de mercancías y recursos, que llegaba desde Estados Unidos.

Uno de los riesgos de aquella estrategia era que el hundimiento de naves estadounidenses y la muerte de sus ciudadanos provocara que el país norteamericano abandonara su neutralidad y declarara la guerra a Alemania. El hundimiento del *RMS Lusitania* en mayo de 1915 había generado uno de esos momentos peligrosos. Un submarino alemán, el *U-20* , torpedeó el transatlántico y lo mandó al fondo del océano con un solo torpedo y en unos 18 minutos. Al fondo se fueron también casi 1.200 personas, mucho más de la mitad del pasaje, ya que sobrevivieron tan solo 761 personas. Los ataques de los submarinos alemanes a las naves que iban y venían al Reino Unido no eran nuevos, a pesar de los posibles incidentes diplomáticos que pudieran surgir. Aun estando en las cercanías de la costa británica, donde más probable era el ataque y la Royal Navy ofrecía protección y escolta, y aunque se tenía al *Lusitania* por una nave suficientemente rápida como para no ser cazada por un submarino, el hundimiento ocurrió. No se puede decir que no se conocieran los riesgos de aquellos viajes transatlánticos, y no solo por los antecedentes. El gobierno alemán, a través de su embajada en

Estados Unidos, había publicado en la prensa estadounidense un aviso explícito al respecto, una advertencia del peligro de viajar a bordo de barcos de países enemigos de Alemania, como era el caso de *RMS Lusitania* , que navegaba con bandera de Reino Unido. El aviso publicado decía: «Viajeros destinados a embarcarse en el viaje atlántico, recuerden que debido al estado de guerra existente entre Alemania y sus aliados y Gran Bretaña y sus aliados: la zona de guerra incluye las aguas adyacentes a las islas británicas; que de acuerdo con el aviso formal dado por el Gobierno Imperial Alemán, las naves con bandera de Gran Bretaña, o de alguno de sus aliados, son susceptibles de ser destruidas en esas aguas y que los viajeros que naveguen en zona de guerra en barcos de Gran Bretaña o sus aliados lo hacen bajo su propio riesgo».

Ni siquiera el hundimiento del *Lusitania* , con 128 ciudadanos estadounidenses, que es cierto que supuso un momento crítico, cambió la política contraria a la participación en la guerra del presidente Woodrow Wilson. Este era un convencido defensor de la solución negociada a la guerra y, además de preservar a su país de los sacrificios materiales y en vidas que conllevaría su participación directa en el conflicto, pensaba que la neutralidad de su país ayudaba a un fin negociado de la guerra. Alemania había prometido que en adelante sus submarinos saldrían a la superficie antes de actuar, lo que debía evitar en gran medida ataques a buques civiles, llevados a cabo por error. Esto alejó la sombra del cambio de postura de los norteamericanos.

En los primeros días de enero de 1917 el Alto Mando Supremo se reunió en el castillo de Pless, en la conocida como conferencia de Pless. Entre otras cuestiones, la marina germana trataba de convencer al káiser de que debía permitir la guerra submarina sin restricción alguna. Según sus estimaciones, en un plazo de entre seis meses y un año, el Reino Unido sería llevado al límite si se cortaban sus vías de suministro del Atlántico. El káiser Guillermo II era partidario, al menos hasta aquel momento, de la moderación en la guerra submarina, algo a lo que además se habían comprometido los alemanes. A pesar de ello, finalmente se acordó que el día 31 de enero entraría en vigor la orden por la que los submarinos podrían atacar cualquier tipo de barco y de cualquier modo, sin restricciones, tanto en las costas británicas como en toda la extensión del Atlántico. Si antes se había apaciguado a los Estados Unidos con la prudencia en el uso del submarino, el cambio de criterio conllevaba a su vez el riesgo de provocar la entrada de ese país en la guerra. Para evitar esto, el gobierno germano, a través de Arthur Zimmermann, a la sazón ministro de Asuntos Exteriores, diseñó un plan para mantener alejado al monstruo, al gigante dormido, como se diría unos años más tarde en la siguiente guerra mundial. Zimmermann llevaba en el cargo desde el 22 de noviembre de 1916 y a pesar de ser recibido con optimismo por el gobierno de Wilson, desde su nuevo puesto comenzó a pensar en cómo obligar a Estados Unidos a estar atento y ocupado en otro lugar, que le mantuviera definitivamente alejado de la tentación de participar en la guerra europea. Esto dejaba vía libre para la estrategia de agotamiento de Inglaterra a través del bloqueo naval basado en la guerra submarina. Los mandos del ejército

del káiser sabían que sus submarinos eran casi invulnerables en ese tipo de combate, donde sus torpedos rasgaban el agua mientras ellos seguían sumergidos, y tomaban aquella baza como un elemento clave para el devenir del conflicto. Unos doscientos submarinos estaban listos para estrangular definitivamente al Reino Unido.

Desde la conferencia de Pless hasta la apertura de la guerra submarina sin restricciones, Zimmermann disponía de unas tres semanas de plazo para lanzar su plan. Este tenía que ser comunicado por el ministro de Exteriores germano al embajador en México, Heinrich von Eckardt, para que se pusiera en marcha lo antes posible. Y aquí venía el problema. Es más, el telegrama debía llegar primero al embajador en Washington, el conde Johann Heinrich von Bernstorff, y este debía entregárselo a su colega del sur.

Los cables telegráficos que los germanos tenían a su disposición para hacer las comunicaciones diplomáticas desde Berlín de manera directa habían quedado inutilizados nada más comenzar la guerra. El 5 de agosto de 1914 los cables que reposaban sobre el lecho del Canal de la Mancha y que cruzaban el Atlántico habían sido cortados por el *CS Alert* , un barco británico dedicado a este tipo de trabajos de cableado marítimo. Estas acciones se llevaron a cabo en otros lugares y las comunicaciones alemanas se vieron así obligadas a buscar otros caminos, que no eran los propios, para sus comunicaciones. Otro de los barcos británicos que participaron en este tipo de operaciones fue el *CS Telconia* , que aún puede verse, erróneamente, en algunas fuentes como el responsable del corte del cable principal que unía Alemania y Norteamérica. Aquella medida de 1914 se mostró clave casi tres años más tarde.

Sin una vía directa, Zimmermann tenía varias opciones para informar de los planes a su embajador en Washington. Una opción era la transmisión por radio. Desde 1906 los alemanes tenían un emisor enorme en su territorio, en la localidad de Nauen, como ya sabemos, a 30 kilómetros al oeste de Berlín, que era usado para comunicarse con las colonias o con los barcos en alta mar. En Long Island, en Nueva York, los alemanes tenían también un receptor desde 1912, si bien su uso había sido interrumpido, en 1914 precisamente, para evitar su uso en la contienda y que comprometiera así la neutralidad de Estados Unidos. En 1915 se había vuelvo a autorizar su utilización para comunicaciones diplomáticas, siempre que los oficiales del ejército norteamericano tuvieran copia de los códigos usados.

Llevar el mensaje físicamente era otra opción. Se podía hacer usando un submarino para cruzar el Atlántico y así dárselo casi en mano al embajador Von Bernstorff. De hecho, el *Deutschland* había cruzado no mucho antes, en noviembre de 1916, desde Alemania hasta Estados Unidos para entregar a su personal diplomático destinado allí materiales médicos, entre otras cosas, y el libro para el código 0075. Cuando llegó el submarino a Estados Unidos fue inspeccionado para comprobar que no llevaba armas y las autoridades locales dejaron

descargar las valijas diplomáticas, que contenían los códigos. Todo estaba listo para que repitiera el viaje llevando a bordo el mensaje de Zimmermann, pero el cambio en la política de guerra submarina hizo que finalmente el *Deutschland* cambiara de cometido y acabara combatiendo en lugar de haciendo transportes. Descartando estas dos opciones, solo otros dos caminos eran realmente válidos.

El primero de ellos llevaría el telegrama de Berlín a Suecia, país que ofrecía sus capacidades de comunicación diplomática a los alemanes. De allí, desde Suecia, hasta las Islas Canarias, luego a Cabo Verde e Isla Ascensión, a medio camino entre África y América, y desde ese punto hasta su destino al otro lado del océano, que era Argentina. Lógicamente, una vez cruzada la masa de agua a través de los cables submarinos, el mensaje tenía que salir de la embajada alemana en Buenos Aires y subir hasta México y, finalmente, Estados Unidos. La segunda opción que tenían los alemanes a su alcance era la utilización de los cables diplomáticos estadounidenses, que eran mucho más directos y que iban de Berlín a Copenhague, y de ahí a Washington de manera directa. Los norteamericanos, neutrales, permitían a Alemania usar sus claves como acto de buena voluntad. Con esas dos posibilidades sobre la mesa, Zimmermann sabía que el mensaje era tan importante y tan crítico para la evolución de la guerra que la decisión sobre cómo enviarlo no era trivial. Algunos historiadores aseguran que se usaron las dos vías para que el mensaje llegara a su destino a pesar de cualquier problema, pero lo cierto es que la vía utilizada fue el cable estadounidense y la opción sueca fue dejada de lado. Los registros alemanes sobre sus comunicaciones diplomáticas no dan pie alguno a pensar en la utilización del camino sueco.

Como hemos visto, ninguno de los caminos era directo, y lo peor para los alemanes era que ambos pasaban por dominios ingleses. Así, las dos vías estaban interceptadas por los ingleses y no les hubiera ido mejor a los alemanes usando la opción sueca en lugar de la estadounidense. Lo cierto es que el mensaje de Zimmermann, que había salido el día 16 de enero, estaba ya el día 17, a las pocas horas, en la Sala 40 británica. Las órdenes de Zimmermann acabaron aquella misma noche en la que se lanzaron sobre la mesa de los miembros de la Inteligencia Naval británica, concretamente de Nigel de Grey y Dillwyn Knox. Era un texto largo y escrito en clave con el código 0075, que los alemanes habían comenzado a usar no mucho antes para sus comunicaciones diplomáticas más importantes y secretas con Estados Unidos y que había llegado vía submarina hasta allí, como hemos visto. Desde un tiempo antes se usaba para comunicarse con otros países europeos, pero solo Estados Unidos lo utilizaba en América, siendo desconocido para México, entre otros países. Era un código de doble entrada, con unos 10.000 elementos, donde un determinado grupo de números correspondía a una palabra concreta. Lógicamente, a estas alturas los códigos estaban suficientemente bien diseñados como para que su equivalencia con las palabras fuera totalmente aleatoria y que no hubiera ningún orden en los códigos o en las palabras que pudiera servir de gancho para comenzar a trabajar en la ruptura del código. El

telegrama, cuando llegó a la Sala 40, era algo así en sus primeras líneas:

0158 0075 4280 6321 9206 1783 5841 7390 8214 4569 4099 1439

3366 2479 4367 1783 4111 0652 5310 1139 8436 1284 9088 2895

2785 1139 8636 5731 7100 5224 8888 2785 2834 7009 1783 4852

4099

Los criptoanalistas británicos sospechaban que los primeros grupos de números correspondían a algún patrón regular, a algún texto que se repetía siempre en las comunicaciones de este tipo. Es decir, igual que todos comenzamos los mensajes con un «estimado amigo» o con la fecha del día, los británicos esperaban que eso mismo ocurriera con el mensaje, importante a todas luces, que tenían sobre su mesa. El primer número (0158) era el del telegrama, el segundo (0075) la codificación utilizada, el tercero (4280) era el emisor, en este caso la Oficina de Exteriores de Berlín, los dos siguientes grupos correspondían a la fecha de envío, el 16 de enero.

En un telegrama, por otra parte, no es extraño encontrarse la palabra STOP. Y ese era el siguiente código a identificar. Lógicamente el último número (4099) correspondía con STOP, pero como cualquier código que se precie, el código 0075 de los germanos tenía varios números para identificar una palabra que se repetía tanto, ya que de otro modo sería claramente identificable por los criptoanalistas. Sobre el papel esto tiene sentido, pero como tantas otras veces la debilidad humana es la brecha de seguridad por la que comenzar a escarbar. Los operadores que codificaban los mensajes solían aburrirse de su tarea, lo que no es de extrañar, ya que aunque se trataba de un trabajo importante era bastante monótono y sistemático. Así, acababan por memorizar unos pocos códigos para las palabras más comunes y en lugar de consultar el código, utilizaban aquellas secuencias, que recordaban. La palabra STOP era uno de estos casos, precisamente por su frecuencia en los telegramas. El STOP del final (4099) está también en la primera línea. De igual modo, los números 1783 y 2785 fueron marcados como candidatos a ser códigos para esa misma palabra, STOP. Esto puede parecer poca cosa, pero como hemos visto en otros casos, el descifrado de un mensaje es un proceso iterativo y de hipótesis que va dando sus frutos poco a poco y que, eso sí, se acelera a medida que se va avanzando en el trabajo.

En las primeras horas desde su envío, Nigel de Grey y otros criptoanalistas de la Sala 40 consiguieron resolver parte del mensaje. Había sido enviado desde Berlín a las 19.50 del día 16 de enero, y a las 10.30 del día 17 los criptoanalistas habían sido capaces de extraer algunas partes del código, aunque palabras clave como Texas, Nuevo México o Arizona, seguían ocultas. No obstante, Nigel de Grey había estado trabajando con el código 0075 y fue capaz de extraer suficiente

información como para saber el sentido general del mensaje y por lo tanto apreciar el enorme impacto e implicaciones del texto alemán.

La idea era audaz. Los alemanes proponían a México una alianza para que este país invadiera Estados Unidos alegando sus derechos históricos sobre ciertos territorios, como Texas, Nuevo México o Arizona. Para afrontar esta lucha con más garantías, la alianza prometía la provisión de ayuda militar y económica por parte de Alemania. Además, Zimmermann quería que el presidente de su nuevo aliado en Norteamérica persuadiera a Japón para que también declarara la guerra a Estados Unidos. Si todo el plan salía tal y como estaba planteado por los alemanes, el presidente Wilson tendría un frente en el Atlántico, un frente contra Japón en el Pacífico y un frente terrestre en el sur, contra México. Todo esto debía ser una barrera suficiente como para que Estados Unidos no entrara en la guerra en Europa.

Los británicos se dieron cuenta de que aquella información podría llevar a Estados Unidos a tomar por fin parte en la guerra, lo que supondría una ayuda enorme para los aliados y dejaba a sus enemigos en una situación de desventaja. Había tres problemas que se debían resolver antes de poner el telegrama en conocimiento del presidente de Estados Unidos. Tenían que asegurarse de que el texto descifrado en la Sala 40 era el correcto y que el texto del telegrama era el que los criptoanalistas decían. Además, debían acabar por resolver todas las dudas al respecto y completar una lectura total y correcta del mensaje. Tenían que probar, por otra parte, que el telegrama y la información eran auténticos y que no se trataba de ninguna operación de engaño o de cualquier tipo de plan con otra intención. Dicho de otro modo, tenían que asegurarse de que el emisor era el gobierno alemán en sus más altas instancias, que los destinatarios eran los correctos y que las instrucciones del telegrama eran las que parecían, que no había dobles lecturas. Por último, tenían que salvaguardar la intervención de la Sala 40 sobre las comunicaciones de los cables de Estados Unidos y en la medida de lo posible mantener el secreto del servicio de captura de las comunicaciones y el trabajo de los criptoanalistas con respecto a los códigos que los alemanes consideraban aún seguros. No hubiera sido nada bueno para las relaciones entre los británicos y los estadounidenses que los primeros se presentaran ante el presidente de los segundos diciendo que estaban escuchando las comunicaciones que viajaban por sus cables y que casualmente ahí habían capturado un mensaje alemán. Si habían capturado y descifrado ese mensaje que viajaba por el conducto de Estados Unidos, habían capturado y descifrado también las comunicaciones del propio gobierno norteamericano.

Mientras esto ocurría, el telegrama había llegado a Washington a través del cable estadounidense. En la embajada alemana descifraron el mensaje, codificado con el 0075, y lo cifraron usando otro código, el 13040, para enviarlo a México. De hecho, en las notas originales con las instrucciones para el envío del telegrama desde Berlín, estaba la orden de enviar directamente el mensaje a México desde Berlín, usando el

código 13040. Esta instrucción finalmente no fue ejecutada, y probablemente fue descartada cuando se renunció también al uso del submarino *Deutschland* como transporte del mensaje. Como hemos dicho, el 0075 no era común para las comunicaciones fuera de Europa y nadie lo conocía en México. Aun así, la confianza en el código que se usaba en México era alta, ya que a pesar de que los diplomáticos del káiser sospechaban que las comunicaciones enviadas a México acababan en manos británicas, enviaron el telegrama de Zimmermann. No se equivocaban los germanos: alguien en la oficina de telégrafos de México trabajaba para la embajada británica en el lugar y les proporcionaba una copia de los mensajes que llegaban para las delegaciones de los países enemigos.

Había pasado algo de tiempo desde el envío del mensaje original desde Berlín el 16 de enero. Aunque tan solo tres días después, el 19, el telegrama había sido enviado desde Washington a México protegido con el código 13040, la Sala 40 no tuvo sobre sus mesas de trabajo esa nueva codificación capturada por la embajada británica en México hasta el 19 de febrero, un mes más tarde. Para entonces Alemania ya había declarado la guerra naval y submarina sin restricciones y el presidente Wilson había reaccionado a este anuncio rompiendo las relaciones diplomáticas con Alemania.

El telegrama encriptado con el código 13040 sí podía ser puesto en claro por la Sala 40 en mayor medida, ya que este código había sido roto y era menos seguro que el 0075, si bien no todas las palabras eran conocidas por los británicos. Además, la captura en México permitía informar a Estados Unidos del plan alemán sin poner al descubierto sus intromisiones en el cable estadounidense y sin dañar, por tanto, las relaciones entre los dos países. El 22 de febrero, el telegrama Zimmermann fue entregado a Walter Hines Page, el embajador de Estados Unidos en Londres. Dos días después el presidente Wilson ya había sido informado, y la indignación por la traición de su confianza y generosidad acercó a Estados Unidos un poco más a la intervención en la guerra. El 1 de marzo la historia del telegrama Zimmermann y los planes alemanes para provocar una guerra entre México y Estados Unidos que tuviera a estos ocupados, fue publicada por los periódicos. La indignación ya no estaba únicamente en el gobierno, sino también en la opinión pública estadounidense, que hirvió de ira pidiendo, ahora sí, la participación en la guerra. Aun así, todavía había algunas sospechas sobre la autenticidad del telegrama y había quien pensaba que todo podía ser un plan británico para atraer las fuerzas de Estados Unidos a su bando. Esta duda acabó por disiparse cuando los norteamericanos se hicieron con una copia, a través de la Western Union, del mensaje enviado desde Washington a México y la enviaron a su embajador en Londres. Nigel de Grey descifró el mensaje delante del embajador usando el código 13040, que conocían en la Sala 40, y eso acabó por certificar que todo era cierto. Unos días después, el 3 de marzo de 1917, el propio Zimmermann admitió públicamente ser el autor del telegrama.

Menos de medio año antes de esos primeros días de marzo de 1917, en noviembre del año anterior, Woodrow Wilson había luchado por su reelección como presidente de Estados Unidos. El Partido Demócrata, el suyo, había usado el siguiente eslogan para pedir el voto para Wilson: «Él nos mantuvo fuera de la guerra». En 1916 la lucha, que se había supuesto corta en los primeros días, excedía los dos años y los demócratas consideraban un éxito suyo haber alejado ese fantasma de su país, asegurando que una victoria republicana llevaría a Estados Unidos a la guerra contra Alemania y contra México. Incluso después de hacerse pública la guerra submarina sin restricciones y de cesar las relaciones diplomáticas, había reticencias para entrar en la guerra. Pero la situación se volvió insostenible tras hacerse público el contenido del telegrama Zimmermann. El 6 de abril de 1917 el Congreso de Estados Unidos declaró la guerra a Alemania. Las tropas, los recursos y las armas estadounidenses fueron una ayuda importante y, unos meses más tarde, la situación alemana era insostenible.

El texto exacto del telegrama más famoso de la Primera Guerra Mundial, que acabó por cambiar el curso de la guerra y que es uno de los hechos más significativos de la historia de la criptografía, era el siguiente:

Nos proponemos comenzar el primero de febrero la guerra submarina, sin restricción. No obstante, nos esforzaremos para mantener la neutralidad de los Estados Unidos de América.

En caso de no tener éxito, proponemos a México una alianza sobre las siguientes bases: hacer juntos la guerra, declarar juntos la paz; aportaremos abundante ayuda financiera; y el entendimiento por nuestra parte de que México ha de reconquistar el territorio perdido en Nuevo México, Texas y Arizona. Los detalles del acuerdo quedan a su discreción [de Von Eckardt].

Queda usted encargado de informar al presidente [de México] de todo lo antedicho, de la forma más secreta posible, tan pronto como el estallido de la guerra con los Estados Unidos de América sea un hecho seguro. Debe además sugerirle que tome la iniciativa de invitar a Japón a adherirse de forma inmediata a este plan, ofreciéndose al mismo tiempo como mediador entre Japón y nosotros.

Haga notar al presidente que el uso despiadado de nuestros submarinos ya hace previsible que Inglaterra se vea obligada a pedir la paz en los próximos meses.

Los alemanes habían confiado en la seguridad de un libro de códigos, pero ya hemos visto multitud de casos en los que esta forma de ocultar los mensajes acaba siendo invalidada por los criptoanalistas. Aunque en muchos casos los libros tengan decenas de miles de entradas, los usuarios acaban utilizando solo una parte de ellas y como con el paso del tiempo se han ido usando más y más las comunicaciones, los criptoanalistas disponen de texto suficiente para atacar cada código y

finalmente sus suposiciones y los errores de uso de los emisores hacen que sean capaces de desentrañar los mensajes codificados.

15. Los códigos de trinchera y el adfgvx

Cuando comenzó la Primera Guerra Mundial, las nuevas formas de comunicación que la tecnología permitía convivían con formas antiguas de hacerlo, como las palomas mensajeras. Poco a poco las comunicaciones inalámbricas dominaron el campo de batalla, aumentando la facilidad para capturar y conocer las comunicaciones enemigas y, por lo tanto, haciendo más necesario, si cabe, el uso de la criptografía. También la guerra de trincheras, con el uso indiscriminado de la artillería y las ametralladoras, se convirtió en asunto central en la Gran Guerra.

Las trincheras suponían posiciones cercanas al enemigo y una forma de combatir determinada, basada en los asaltos y en la defensa de la posición. Los cifrados habituales eran seguros, pero demasiado complejos para su uso generalizado por hombres sin mucha formación y la distribución de libros de códigos suponía un riesgo enorme de que estos cayeran en manos enemigas, por las constantes idas y venidas de ataques, avances y retrocesos. Por eso aparecieron los códigos de trinchera. Por contra, la poca movilidad de las tropas atrincheradas hacía que la distribución de los libros de códigos fuera muy sencilla. La forma de operar que se implantó fue el uso de códigos no muy extensos, junto con la orden general de avisar tan pronto como un libro de códigos se viera comprometido, para anular su uso y distribuir uno nuevo. Además de esto, se cambiaban con cierta regularidad.

A comienzos de 1916 los franceses y los británicos ya usaban los conocidos como códigos de trinchera. Los alemanes tardaron un año más, pero también acabaron por incorporar un libro de unas 4.000 entradas. Cuando los estadounidenses entraron en combate en Francia, tenían 1.600 palabras codificadas en sus libros, que se distribuían a nivel de compañía. No era demasiado seguro este libro estadounidense, ya que cuando un teniente aficionado a la criptografía, llamado Rives Childs, trató de romper el código, lo consiguió en menos de cinco horas. Pudo resolver todos los mensajes cifrados que le habían entregado para probar la seguridad del código, 44 en total. Por supuesto, se plantearon al momento su mejora, adaptando algunas de las características que ya tenían los códigos de otros países, algunas de las cuales eran conocidas desde mucho antes. Por ejemplo, incorporaron los códigos de doble entrada, más sencillos de utilizar, como ya hemos visto. Cada dos semanas los códigos se cambiaban, lo que era un avance, aunque les costó cierto tiempo a los estadounidenses ponerse al nivel del resto de países. Cuando lo hizo, era ya el verano de 1918, fecha en la que introdujeron el código Potomac, el primer código de trinchera avanzado.

En 1914 el Bureau du Chiffre, la Oficina de Cifras francesa, llevaba varias décadas de actividad y brindaba a Francia una cierta ventaja frente a sus enemigos. Antes de la guerra ya se había preocupado de

capturar las comunicaciones alemanas y la sección de criptología que operaba dentro del Ministerio de Guerra se expandió tan pronto como la Primera Guerra Mundial arrancó. No mucho después de que los alemanes pasaran la frontera, en agosto de 1914, y por lo tanto dejaran atrás sus líneas telegráficas, las comunicaciones tuvieron que hacerse vía radio, es decir, que los franceses tuvieron acceso directo a ellas. Los franceses fueron depurando su forma de tratar toda la información que eran capaces de capturar, así como los métodos e instalaciones para hacerlo y para analizar dicha información. No solo se centraban en el propio contenido de las emisiones alemanas, sino que anotaban la fuerza con la que llegaba la señal, con lo que trataban de delimitar y conocer las zonas en las que emitían las estaciones enemigas. Anotaban también las señales de las estaciones, el volumen del tráfico en cada lugar y buscaban patrones, con lo que podían estimar dónde estaban los puestos de mando y por dónde se situaban otro tipo de unidades, mucho más móviles. Los franceses, por tanto, tan solo con el análisis del tráfico, fueron trazando sobre los mapas los lugares en los que estaba el enemigo y los puntos hacia donde se movía. Desde entonces, este tipo de análisis son comunes y forman parte del día a día del ejército, ya que el propio tráfico de señales aporta mucha información. Por otra parte, este conocimiento es una fuente más que sirve a los criptoanalistas para atacar los mensajes cifrados que capturan, ya que pueden saber el tipo de métodos de cifrado que usa una u otra unidad, o pueden generar esas hipótesis sobre los mensajes que hemos visto que son tan útiles: tipo de mensaje, si tiene cabeceras identificando al emisor, determinadas firmas, información fija…

Al comienzo del conflicto los alemanes usaban una cifra basada en la trasposición doble de columnas, que se denominaba ÜBCHI, y que, para desgracia suya, era conocida y había sido rota por los franceses ya antes de la guerra. La cifra usaba una clave que era proporcionada por el mando y el uso de la misma estaba en vigor en todo el frente occidental durante entre ocho y diez días, antes de ser modificada. Los criptógrafos del coronel Cartier, el responsable del Bureau du Chiffre, no solo tenían que enfrentarse a las comunicaciones terrestres, sino que prestaban también servicio a la marina francesa, que no tenía servicio propio de criptografía, y analizaban comunicaciones diplomáticas, donde el tráfico entre Madrid y Berlín era una fuente clave.

El 2 de septiembre de 1914, la amenaza alemana sobre París obligó a trasladar a Burdeos el Bureau du Chiffre, lo que supuso un traspié del que se recompuso pronto. Lo que sí supuso un problema para Francia fue la indiscreción. Los comentarios en torno al conocimiento que se tenía de las claves alemanas y en torno a la ruptura de los códigos, se movían sin control de arriba abajo en la jerarquía militar. Tanto es así que el 3 de octubre el mando francés emitió una orden prohibiendo este tipo de comentarios y pidiendo discreción al respecto. El mal ya estaba hecho, y los alemanes mejoraron su seguridad, poniendo más cuidado y cambiando las claves. No fue suficiente, en cualquier caso, ya que el conocimiento que había desarrollado el Bureau du Chiffre le permitió seguir atacando sin problemas las cifras alemanas y leyendo sus comunicaciones. A comienzos de noviembre, por ejemplo, los alemanes

cambiaron su clave, y tres días después esta ya era conocida por los criptoanalistas franceses. El siguiente cambio de clave no fue efectivo para los alemanes ni siquiera veinticuatro horas, ya que el mismo día que entró en vigor fue averiguada.

Los franceses tenían una ventaja clave en el frente occidental gracias al trabajo y al éxito del Bureau du Chiffre, pero de nuevo la indiscreción hizo aparición. Cuando los franceses supieron, gracias a la intercepción y descifrado de las comunicaciones, que el káiser Guillermo II iba a visitar la localidad belga de Tielt, ocupada en aquel momento por los alemanes, planearon un bombardeo sobre el lugar, precisamente cuando el káiser se encontraba allí. La acción fue narrada por *Le Matin* , un diario francés, explicando de dónde y cómo había salido la información sobre la visita del káiser. Como es lógico, los alemanes tomaron medidas y el 18 de noviembre implantaron un nuevo sistema de cifrado, que resultó ser otro paso en falso, ya que su sencillez hizo que en los primeros días de diciembre los franceses ya lo hubieran roto.

A comienzo de 1915, el coronel Cartier recibió un memorándum sobre cómo resolver el método de cifrado que los alemanes habían implantado en el mes de noviembre anterior y que ya había sido roto, como hemos dicho. Este método era conocido por los franceses como ABC, y el memorándum ofrecía una forma de hacerlo más sencilla que la que había implantado el personal del Bureau du Chiffre. El documento estaba firmado por Georges Jean Painvin, un teniente de artillería de veintinueve años que en aquel momento prestaba servicio en el Sexto Ejército francés. Painvin no tenía experiencia en criptografía antes de la guerra, como sería de esperar, ya que en su vida de civil era profesor de paleontología. Painvin había tenido contacto unos meses antes, tras la batalla de Marne, en los primeros días de septiembre de 1914, con el capitán Victor Paulier, que pertenecía a la Oficina de Cifras que dirigía Cartier y que había sido enviado al Sexto Ejército, donde servía el joven paleontólogo. Con él había aprendido cómo romper la ÜBCHI, la cifra alemana, y había hecho algunas aportaciones, llegando él mismo a descubrir algunas claves del enemigo. Tras recibir el memorándum sobre la cifra ABC, Cartier puso su interés en Painvin, y hasta el ministro de Guerra, Alexandre Millerand, hizo gestiones para que dejara el Sexto Ejército y se incorporara al Bureau du Chiffre.

El 5 de marzo de 1918, aproximadamente dos años después de que Painvin comenzara su carrera oficial como miembro del grupo de criptógrafos de Cartier y poco antes de la gran ofensiva alemana que comenzó ese mismo mes, el día 21, los alemanes introdujeron una nueva cifra, conocida como ADFGX. Un comité de expertos criptógrafos la había seleccionado como la opción que ofrecía mayor seguridad y solidez; tanto es así que incluso la consideraban totalmente segura en aquel momento, indescifrable. La cifra ADFGVX era una mezcla de sustitución y trasposición. Alemania tenía el tiempo en su contra y quería aprovechar el momento para dar un vuelco a la guerra. El día 3 de marzo se había firmado el tratado de paz de Brest-Litovsk, por el que Rusia daba un paso atrás y se daba por finalizado su proceso de

alejamiento de la guerra. Esto permitió que muchas tropas alemanas se desplazaran del frente oriental al occidental. Sabiendo que la llegada de los norteamericanos sería clave, los alemanes estaban decididos a lanzar una ofensiva clave esa primavera. Erich von Ludendorff había ideado un plan para llevarla a cabo.

El factor sorpresa, como es habitual, era vital para el éxito de la maniobra alemana. Las comunicaciones, por tanto, debían ser cuidadas al máximo y aseguradas en la medida de lo posible. Para ello se buscó una cifra, dejando de lado los libros de códigos, que proporcionara esa seguridad. Se reunieron expertos en criptografía a los que se les pidió que plantearan alternativas, cifras que ellos consideraban seguras, a la vez que un nutrido grupo de criptoanalistas tratada de romper todos esos métodos propuestos, con la intención de encontrar así la mejor opción. La Abhorchdienst, la oficina alemana que se dedicaba a romper los códigos enemigos, los criptoanalistas al servicio del káiser, se había puesto en marcha en 1916, bien avanzada la guerra, y tenía que contrastar el cifrado seleccionado. De entre todas las cifras analizadas, la Abhorchdienst seleccionó una que había creado el coronel Fritz Nebel, un oficial de inteligencia que tenía entonces veintisiete años. No fueron capaces de romper aquel cifrado y la propuesta de Nebel, por tanto, fue seleccionada para ser llevada al frente como solución. Oficialmente su nombre era GEDEFU 18, que proviene de Geheimschrift der funker 18, lo que viene a ser Cifra de telegrafistas 18. Pero este no es el nombre con el que ha pasado a la historia, ya que habitualmente se la conoce como la cifra ADFGX,

Nebel propuso representar las letras del alfabeto en una tabla de 5 × 5, recuperando de nuevo las antiguas ideas de Polibio y algunas ideas más que ya conocemos, donde las coordenadas se corresponden precisamente con esas letras que le dan nombre a la cifra: ADFGX. Las letras del alfabeto se colocan en la tabla de acuerdo a la clave y la letra I comparte celda con la letra J. Por ejemplo, si la clave es «CARLOSGANTE» la tabla resultante sería:

Así, la letra P sería identificada como GF, por su fila y columna. La razón para usar esas letras ADFGX en lugar de números, como se hace habitualmente para identificar las filas y la columna de cada letra, es la forma en la que se iban a enviar los mensajes cifrados: el código morse. En este código, la representación de los números es relativamente similar entre unos y otros, por lo que, en un añadido de efectividad en las comunicaciones, se sustituyeron los números por una serie de letras del código morse que ofrecen suficientes diferencias entre ellas, dentro del código, para reducir la probabilidad de error en la transmisión. Es decir, en el propio método de cifrado tenemos una seguridad extra que limita los errores en el envío y en la recepción. El código Morse para estas letras es: A(.-), D (-..), F(..-.), G(--.) y X(-..-).

No es nada trivial este hecho de incorporar información o alguna característica en el propio método que haga que la información contenga, por decirlo de algún modo, un control de errores automático.

Un error en la comunicación o en una letra puede dar al traste con todo el mensaje, y ese error puede deberse perfectamente al factor humano que supone el cifrado, la codificación en morse, la operación de los aparatos para enviar el mensaje, la recepción y el paso de morse a texto… cualquier mejora en ese ámbito es un seguro que merece la pena tener en cuenta. En nuestra vida cotidiana podemos ver este hecho en el NIF español, donde la letra cumple exactamente esa función. La letra del NIF se calcula a partir de los números del propio NIF y sirve como método de control simple para validar si un NIF es correcto o no. Si por cualquier problema se escribe mal o se pierde alguno de los números, la letra nos permitirá detectar ese error, ya que cada secuencia de números da lugar, mediante un algoritmo, a una letra concreta. Lo mismo ocurre con los dígitos de control de las cuentas bancarias o incluso, si volvemos a la historia, ese es el motivo por el que se usa la señal SOS para pedir ayuda.

A comienzos del siglo XX se utilizaba CQ como señal de alerta en las transmisiones telegráficas y de radio. Esa señal indicaba que el mensaje era relevante o interesante para todas las estaciones y se adoptó como forma de realizar una llamada general. No obstante, no era algo oficial su envío como método de petición de ayuda. No lo fue hasta que la Compañía Marconi Internacional de Comunicaciones Marítimas le añadió una D, de la palabra Distress, en 1904. Hay muchas frases que se han tratado de encajar en ese CQD, igual que ha pasado con el SOS. Por ejemplo: Come Quick, Danger o Come Quickly, Drowning. Son frases hechas *a posteriori* y por lo tanto no explican la existencia del código, no es este su acrónimo, pero, eso sí, pueden ayudar a recordar la señal. La señal CQD no vivió mucho, ya que fue sustituida en 1906, en una conferencia internacional celebrada en Berlín, por la señal SOS. El motivo del cambio y su adopción fue que las letras SOS, en código morse, que es como se realizaban las comunicaciones de radio y telégrafo, añaden una seguridad extra. La secuencia es muy fácil de enviar y muy fácil de reconocer, evitando así los errores en la transmisión. En morse SOS es (… . - - - … .) que se puede repetir y repetir sin problema. Tres puntos, tres rayas, tres puntos, tres rayas… una señal difícil de malinterpretar. De nuevo, esas explicaciones a través de frases que aseguran que SOS proviene de Save Our Ship o Send Out Succour, por ejemplo, son falsas. El motivo es mucho más práctico, el mismo por el que los alemanes se decidieron por las letras ADFGX para identificar las filas y las columnas en su tabla de letras. Por cierto, en 1912 el buque *Titanic* usó tanto el código CQD como el SOS para pedir ayuda durante su hundimiento.

El propio creador del método, el coronel Fritz Nebel, reconoció que su formación en el campo de la radiotelegrafía le había llevado a seleccionar las letras que más fácilmente podían enviarse y que a su vez menos problemas podían causar en su uso a la hora de transmitir mensaje en morse.

Volviendo al método de cifrado, no acababa con el primer paso asociado a la tabla, sino que la secuencia obtenida tras la sustitución de cada

letra del mensaje por el parte de coordenadas que la sitúan dentro de la tabla no es el mensaje cifrado definitivo, sino que el proceso es un poco más complejo. Ese primer mensaje codificado se transpone por columnas, usando una segunda clave. Por ejemplo, si queremos enviar el mensaje «AL MEDIODÍA», la primera parte del método de cifrado, si usamos la tabla que hemos generado anteriormente con la clave CARLOSGANTE, tendremos la secuencia:

AD AG GD DX FD FX AX FD FX AD

Para la segunda parte del proceso usaremos la clave YUSTE y tendremos el siguiente resultado:

El orden en el que se toman las columnas viene determinado por el orden alfabético de las letras de la clave y el mensaje final a enviar, tras la trasposición de columnas será: GDFD AXAX GFXA DDXF ADFD, que se enviará sin espacios en blanco: GDFDAXAXGFXADDXFADFD. Es decir, Nebel combinaba la sustitución y la trasposición.

Cuando llegaron las primeras muestras de la nueva cifra al Bureau du Chiffre francés, sus expertos quedaron un poco desconcertados, ya que suponía un cambio en lo que se venían encontrando hasta aquel momento. Painvin comenzó a trabajar de manera obsesiva en el criptoanálisis del nuevo método que estaba usando su enemigo. Las ofensivas se sucedían y cada día que pasaba los alemanes avanzaban y su artillería hacía retroceder a las fuerzas aliadas. En la primera de ellas, conocida por los alemanes como la batalla del Káiser, Kaiserschlacht en alemán, y lanzada el 21 de marzo, casi 6.500 piezas de artillería, unos 3.500 morteros y más de 700 aviones fueron puestos sobre el tablero. Los aliados tenían menos recursos y, además, su frente era muy extenso. Los británicos tenían sus unidades estiradas a lo largo de 95 kilómetros, por lo que el conocimiento de los movimientos e intenciones alemanas hubiera sido de un valor enorme, pero lamentablemente para ellos la cifra ADFGX estaba funcionando y cumpliendo con su propósito. En el primer día de la ofensiva los alemanes se habían hecho con aproximadamente la misma cantidad de terreno que los británicos habían conseguido capturar en los ciento cuarenta días de la ofensiva del Somme de 1916. En abril llegó una segunda ofensiva y el 27 de mayo se lanzaba la tercera, la ofensiva Blücher-Yorck, que llegó a ganar 65 kilómetros en cinco días.

Poco después, en junio de 1918, la artillería alemana estaba a unos 100 kilómetros de París y se estaba preparando una gran ofensiva final, por lo que los aliados estaban obligados a anticiparse a ese movimiento para detenerlo o neutralizarlo en la medida de lo posible y conseguir así resistir. Para ello, la opción más clara era descifrar las comunicaciones alemanas y así conocer sus planes para adelantarse a ellos, concentrando sus posiciones en el lugar del frente donde más conveniente fuera. Painvin seguía comprometido en cuerpo y alma a su tarea contra la cifra ADFGX, una tarea que tenía una cuenta atrás en marcha, ya que en casos como este la información caduca en muy poco

tiempo. Una vez lanzada la ofensiva alemana, ya no había posibilidad de adelantarse en modo alguno para anularla. Painvin se empeñó tanto en la tarea que perdió varios kilos durante el proceso. Había llegado a la conclusión de que los alemanes cambiaban la clave cada día, pero de igual modo que el tiempo corría en su contra, el éxito alemán jugaba en cierta medida a su favor. Cuanto más avanzaba el ejército enemigo y más activas eran sus ofensivas, más tráfico de mensajes era capturado por los franceses y puesto a disposición del equipo de Cartier. Painvin invertía horas y horas de trabajo en mensajes cuyo desciframiento ya no serviría de manera directa para nada, por ser información de días pasados y descubrir claves que ya habían caducado, pero cada prueba y conclusión le permitía adentrarse paso a paso en el cifrado alemán.

De algún modo el tiempo corría en contra de ambos bandos en conflicto. Los alemanes necesitaban avanzar lo máximo posible antes de que los recursos y los soldados estadounidenses, que ya estaban en parte sobre el terreno, lo hicieran más complicado. Los aliados, por su parte, tenían que frenar la ofensiva de los alemanes. Las enormes piezas de artillería alemanas, como el Gran Berta, comenzaban a amenazar la capital francesa, donde se preparaban ya para evacuar algunas partes clave del aparato del gobierno, se reforzaban construcciones para resistir el bombardero y en las casas se comenzaba a acumular comida, esperando la escasez que llegaría en breve.

El 26 de abril de 1918 Painvin concluyó con éxito el criptoanálisis del método ADFGX que venían utilizando los enemigos. Había creado un método para poder descubrir, a partir de mensajes cifrados capturados, las claves que utilizaban los alemanes y por lo tanto descifrar dichos mensajes. Su método era laborioso, pero llevado a cabo en paralelo por un grupo de personas, podría resolverse en tiempo suficiente como para que los mensajes descifrados fueran útiles para el ejército, para adelantarse al enemigo y estropear sus planes y, por lo tanto, importantes para el devenir de la guerra. Unas semanas después, el 1 de junio, los alemanes incluyeron una nueva letra en el código, la V, y el código ADFGX pasó a ser el código ADFGVX.

El motivo del cambio era la necesidad de transformar la tabla de 5 × 5 posiciones en otra de 6 × 6, y tener así la posibilidad de incluir de manera sencilla y natural en el método de cifrado los números, es decir, los dígitos del 0 al 9. Esto permitiría que las comunicaciones fueran más rápidas y que los números, muy habituales en los mensajes, pudieran ser descritos con una posición en la tabla y no como secuencias de letras. El cambio provocó que el método de Painvin dejara de funcionar, por lo que se vio obligado a enfrentarse de nuevo al problema. Pero todo su trabajo anterior y su intuición le ayudaron a darse cuenta del cambio y no tardó en conjeturar que habían aumentado la tabla y que lo habían hecho para incluir números. Había dado de lleno con los cambios introducidos por los alemanes. Painvin aseguró que, ante el cambio, había asumido que la letra extra en la tabla, que generaba una nueva fila y una nueva columna, se había introducido para codificar números. Fue su primera hipótesis y lo primero que probó. Afortunadamente para

su bando, acertó a la primera, a lo que contribuyeron una serie de mensajes alemanes en los que se repetía todo el texto y tan solo cambiaba un número. Eran mensajes en los que se pedía un informe sobre la situación en su zona del frente, y ese mensaje se reenvió a varias divisiones, cambiando en el mensaje tan solo el número identificativo de la división. Eso era todo lo que Painvin necesitó para dar por bueno su criptoanálisis.

El 2 de junio, tan solo un día después del comienzo de su uso, la cifra ADFGVX estaba rota y por lo tanto las órdenes alemanas eran conocidas al momento, de nuevo, por sus enemigos. Como ya hemos comentado, la cantidad de tráfico en las comunicaciones jugaba a favor de los aliados. Tan solo en el primer día tras la entrada en vigor de la nueva cifra, más de setenta mensajes alemanes fueron puestos ante Painvin. Capturar mensajes sin importancia a menudo era de gran ayuda. Sin ir más lejos, esa circunstancia que hemos visto donde el mismo mensaje rutinario se enviaba a diferentes unidades sobre el terreno, era muy útil para el equipo de criptógrafos franceses. Estos mensajes sin importancia *a priori* permitían descifrar el ADFGVX y conocer las claves usadas, por lo que a partir de ese momento ya se podían descifrar todos los demás mensajes, más importantes. No obstante, no se tenía éxito en todos los casos y tampoco era extraño que no fueran capaces de encontrar las claves y por lo tanto de descifrar las comunicaciones alemanas. En cualquier caso, por pequeña que fuera la ayuda era de un valor considerable.

Se descifraban mensajes como «envíen municiones rápidamente, incluso durante el día si no son vistos». Con esta forma de pedir municiones, se indicaba de forma indirecta el lugar desde el que se iba a lanzar una ofensiva. Este mensaje, concretamente, iba dirigido al mando del Decimoctavo Ejército Alemán, que estaba entonces en Remaugies, en el centro de la pinza que formaban las líneas germanas.

Esta información era corroborada por otras fuentes, como el reconocimiento aéreo, y se reforzaba así la parte del frente adecuada para intentar bloquear a los germanos. La importancia del trabajo de Painvin en la evolución de la guerra es muy difícil de concretar, pero es cierto que cuando los alemanes estaban a menos de 100 kilómetros de París, la capacidad de conocer de antemano los movimientos del ejército alemán supuso una ventaja enorme. En torno al 9 de junio se capturaron mensajes que indicaban que el siguiente paso hacia París se daría con un ataque a la zona de Montdidier y Compiègne, por lo que reforzó esa parte las líneas francesas. Cuando 15 divisiones alemanas se lanzaron a la ofensiva, se toparon con un enemigo que les estaba esperando y el resultado fue desastroso para los atacantes.

Fue una tremenda suerte para los franceses haber sido capaces de conocer los mensajes alemanes y por lo tanto sus planes en aquel junio de 1918. No fueron muchas las claves ADFGVX que se rompieron en la oficina de Painvin, a pesar de conocer cómo hacerlo, ya que necesitaban

capturar mensajes cifrados en número suficiente para llevarlo a cabo, pero aun así su contribución tuvo un valor cierto.

Painvin, tras la guerra, volvió a sus clases y se alejó del mundo de la criptografía, después de ser una pieza clave en la historia de la Primera Guerra Mundial. Medio siglo después, Nebel, el alemán creador del ADFGX, conoció la historia de cómo su método había sido roto por los franceses, y en concreto por Painvin. Nebel comentó entonces que él había propuesto algún paso más en el proceso, una trasposición adicional, pero que la idea se había descartado por razones prácticas. En esa misma época Nebel y Painvin se conocieron en persona y frente a las explicaciones de Nebel sobre el recorte que había sufrido su método antes de ponerlo en práctica, el francés comentó que probablemente en ese caso no habría podido romper el cifrado, ya que sería mucho más robusto.

16. La verdadera cifra indescifrable

Como ya hemos visto, hay muchas cifras que se han tomado como totalmente seguras a lo largo de la historia, incluso en algunos casos se ha usado el nombre de cifra indescifrable (*le chiffre indéchiffrable*) para el cifrado de Vigenère. Puede ser que fueran seguras durante un tiempo o frente a un posible enemigo, pero también hemos visto cómo en ninguno de los casos eso era totalmente cierto, y más si tenemos en cuenta que la mano del hombre está en el uso de las cifras y en no pocas ocasiones se convierte en el eslabón más débil de la cadena. Pero existe una cifra, un método criptográfico que es totalmente seguro, aunque, por otra parte, en una materia viva como es la criptografía ninguna afirmación puede ser tan atrevida como esa.

Gilbert Vernam, un ingeniero estadounidense nacido en 1890, trabajó en 1917 en el laboratorio de AT&T en Manhattan, en la sección de investigación y desarrollo. Su empeño iba dirigido a mejorar los sistemas de telegrafía de la empresa. Era un hombre inteligente y con una visión muy especial de la tecnología que manejaba. Al parecer era capaz de idear un circuito electrónico y tener su funcionamiento claro antes incluso de plasmarlo en un papel y sin ni siquiera haber hecho prueba alguna al respecto. Tan solo un año después de entrar en la empresa, fue asignado a un proyecto de investigación secreto. El proyecto llevaba unos meses en marcha, desde el verano, en aquel diciembre de 1917, con Estados Unidos ya en la Primera Guerra Mundial, y giraba en torno a la seguridad en las comunicaciones de los teletipos, o lo que es lo mismo, de los telégrafos de impresión. Este tipo de telégrafos, dotados de un teclado similar al de un piano, aunque con menos teclas, podía transmitir e imprimir directamente a un ritmo de unas 60 palabras por minuto, algo mucho más eficiente que el sistema morse habitual, que se movía en algo menos de la mitad. Estos aparatos fueron los primeros en imprimir los despachos telegráficos en los caracteres habituales del alfabeto, es decir, no requerían traducción o decodificación alguna. El sistema había sido patentado en 1855 por David Edwin Hughes, un inglés emigrante en Estados Unidos. Este sistema tenía en cada extremo de la línea una rueda con las letras del alfabeto y se movían ambas de forma sincronizada.

El sistema, eso sí, no era seguro, ya que un oscilógrafo podía medir las fluctuaciones de la corriente a lo largo de la línea y por lo tanto leer sin problemas la información que se estaba transmitiendo. De igual forma que en el código morse los puntos y las rayas sirven para codificar todas las letras a través de sus secuencias y combinaciones, en el telégrafo de impresión se usaba un código similar, ideado por el ingeniero francés Émile Baodot en el año 1874. Cada letra se codificaba usando cinco pulsos, algo similar a lo que hoy todos conocemos como bit. En este caso, el 0 y el 1 que asociamos con los dos posibles valores de un bit de información, correspondían directamente con un pulso

eléctrico o con la ausencia de corriente eléctrica. El teclado del emisor generaba estos pulsos por la línea, que al llegar al destino se convertían de nuevo a una letra, que era impresa. Las posibles combinaciones de esos cinco bits de información son 32 (2 elevado a 5 y dos posibles estados por ese bit y cinco posiciones de bit). Así, había valores para todas las letras del alfabeto y aún quedaba alguna opción adicional para el espacio en blanco, para cambiar de letras a números y viceversa o para el salto de línea.

El mensaje que se recibía por un teletipo quedaba impreso en una cinta, que iba quedando marcada en función de la secuencia de pulsos. Vernam pensó que se podrían combinar en la emisión los pulsos generados por el teclado con una serie de pulsos externos, y con la ausencia de esos pulsos externos. Dicho de otro modo, se podría combinar el mensaje en claro con una clave para generar el mensaje a enviar, que estaría cifrado. Dentro del teletipo la información se movía en una cinta que se iba agujereando o no en función de los pulsos eléctricos y que cerraba un circuito cuando había un agujero y no lo cerraban en caso de no haberlo. De esta forma, los pulsos eléctricos acababan convertidos en algo mucho más palpable. Esto ayudó a Vernam a diseñar su sistema, que vendría a ser algo así como la sincronización de dos cintas, la del mensaje y la de la clave, donde en función de la combinación de agujero o no agujero en cada una, determinaría el valor del bit final. Si el emisor y el receptor tenían exactamente la misma cinta de clave y la sincronizaban con el envío y recepción, se podría transmitir un texto cifrado y descifrarlo en el destino.

Vernam patentó estas ideas, conocidas como el cifrado Vernam, en 1919, y utilizaba lo que se conoce habitualmente en el mundo de la computación como operación XOR o, dicho de otro modo, un OR exclusivo (exclusive OR), aunque él no usó entonces esta terminología. Esto quiere decir que solo el resultado será un 1 cuando ambos pulsos sean diferentes, de ahí la palabra exclusivo. En lógica, una proposición del tipo «Cierto o Cierto» da como resultado Cierto, pero en este caso, con el operador XOR, como son coincidentes ambos elementos el resultado sería falso. La tabla de posibles combinaciones es:

Cierto + Cierto = Falso

Cierto + Falso = Cierto

Falso + Cierto = Cierto

Falso + Falso = Falso

Con esto se tendría el cifrado del mensaje, que combina cada uno de los pulsos o ausencia de pulsos del mensaje y la clave. En destino, la decodificación es sencilla y sin ambigüedades. Tenemos en el descifrado la clave sincronizada con la usada en origen y el mensaje encriptado, así que si la clave tiene un agujero (Cierto) y el texto cifrado es igual

(también Cierto), el valor en la cinta del texto plano solo puede ser una ausencia de pulso (Falso).

El sistema diseñado por Vernam funcionaba sin problemas y este tenía a su alcance la capacidad para construir los dispositivos de envío y recepción que implementaran su idea. Es más, la facilidad de uso del sistema era una de sus ventajas, ya que el emisor no tenía que cifrar el mensaje antes de enviarlo, sino que el propio dispositivo cifraba en origen y descifraba en destino, sin tener que hacer ningún trabajo adicional. Tan solo con colocar una cinta con la clave, el operador escribía el texto en claro, y este se transmitía cifrado de manera automática por la propia máquina. El receptor, que también había colocado la cinta con la clave en el dispositivo, recibía texto en claro después del proceso automático de descifrado realizado por el dispositivo. Este aspecto no solo otorga facilidad y rapidez a las comunicaciones cifradas, lo que hace que se puedan utilizar por más personas y en más situaciones sin depender de la formación de los operadores, sino que también elimina del proceso de cifrado y descifrado cualquier posible error humano.

La idea fue un éxito dentro de AT&T, la empresa para la que Vernam trabajaba, y poco después también el ejército mostró su interés en esta criptografía automática, como la denominaron dentro de AT&T. Por otra parte, eso sí, cualquiera podría interceptar el tráfico, como ya hemos comentado, aunque obtendría un texto cifrado, y si Vernam quería que el sistema fuera útil tenía que conseguir además que fuera seguro.

En los primeros prototipos que crearon, la cinta con la clave giraba de manera circular, por lo que cada cierto tiempo la clave volvía a repetirse, al llegar el bucle de nuevo al inicio de la cinta. Toda la seguridad del sistema residía en la clave, y si esta se repetía cada cierto número de caracteres cifrados, el método creado por Kasiski hacía el sistema vulnerable. Con una clave circular el sistema no dejaba de ser polialfabético y los criptoanalistas ya sabían cómo atacar y romper ese tipo de soluciones. La longitud de la clave era algo crítico en la seguridad de este método, y por ello los técnicos de AT&T crearon cintas de clave cada vez más largas, lo que hacía que en la práctica se ganara en seguridad, aunque seguía siendo un sistema vulnerable. Llegó un momento en que el propio dispositivo perdía practicidad, una de sus ventajas, ya que la cinta era tan larga que la complejidad de su uso y manejo era un problema. Ese punto débil del sistema de Vernam ocupó a varios expertos en criptografía en la empresa, y el sistema se mejoró desde el punto de vista de la ingeniería, aplicando soluciones que mejoraban la seguridad, como la combinación de dos cintas de clave, pero en el fondo el sistema seguía siendo vulnerable.

Profundizando en el problema, fueron varios los que llegaron a una conclusión con dos caras. Por una parte, el método de Vernam se podría convertir en totalmente resistente al criptoanálisis si la clave fuera del todo aleatoria e infinita. Esa, lógicamente, era la cara de la moneda. La cruz era que en la práctica esas condiciones necesarias son imposibles.

Joseph O. Mauborgne, el militar estadounidense que en 1914 había publicado la solución al cifrado Playfair, tuvo un papel esencial en la creación de esa idea de la clave de un solo uso y de su resistencia al criptoanálisis. Vernam y Mauborgne habían dado con el sistema perfecto de cifrado e incluso estaban cerca de tener un dispositivo capaz de acercarse en la práctica a su ideal. Para ser justos, el primero que había expuesto la idea de clave de un solo uso, infinitamente larga, había sido Frank Miller, un criptógrafo estadounidense que ya en 1882 había llegado a esa conclusión que más tarde Vernam acabó de concretar y patentó.

Unas décadas más tarde, en 1940, el matemático, ingeniero y criptógrafo Claude Shannon desarrolló los caminos teóricos, los teoremas y las demostraciones matemáticas que le llevaron a dotar de rigor y solidez matemática a esa idea de la cifra indescifrable. Demostró que eran posibles los cifrados perfectos, esto es, cifrados que seguirían siendo totalmente seguros por muy largo que fuera el mensaje en claro cifrado. En palabras de Shannon, «después de interceptar una cantidad determinada de material, el enemigo no está en una posición más ventajosa que antes». Hemos visto ya muchos casos en los que la cantidad de texto cifrado es clave para el criptoanálisis y que este es viable y más sencillo a medida que aumenta ese texto disponible. Shannon demostró que, matemáticamente, el sistema perfecto existía, pero expuso también que los requerimientos, que ya hemos comentado, eran demasiado elevados para llevar tal sistema a la práctica. Por cierto, fue en aquel mismo documento en el que trataba del sistema de cifrado perfecto donde Shannon utilizó por primera vez una expresión por la que ha pasado a la historia de la ciencia: teoría de la información. Y es que Shannon es un personaje clave en la historia de la ciencia de la computación y se le considera como el pionero y un pilar esencial de la teoría de la información.

Al finalizar la Primera Guerra Mundial el servicio de criptografía del Reino Unido era posiblemente el mejor del mundo. La Sala 40 acabó leyendo y descifrando el tráfico diplomático y naval alemán sin problema. El gobierno británico decidió que su trabajo debía seguir en tiempo de paz, manteniendo el secreto. El problema llegó cuando hubo que asignar un presupuesto a la Sala 40 y a otras oficinas dedicadas a la inteligencia. La falta de fondos llevó a reducir el número de estaciones de escucha y, por lo tanto, el flujo de información que se debía analizar también decayó. La falta de documentos hizo que se tuviera que prescindir también de personal. Por otra parte, se dejaron de lado las comunicaciones militares y el trabajo se centró en las emisiones diplomáticas.

Así fueron los comienzos del Government Code and Cypher School, conocido habitualmente como GC&CS. Se unieron en él, en 1919, las agencias de inteligencia de señales de la Oficina de Guerra, cuyo nombre era MI1b, y la Sala 40. Hugh Sinclair, el director de la Inteligencia Naval, fue el designado para lanzar la nueva entidad y su primer director operativo fue Alastair Denniston. Su misión era

asesorar al resto de áreas gubernamentales sobre los códigos y métodos de cifrado que debían utilizar, ayudarlos con su provisión, así como estudiar los métodos de cifrado de las comunicaciones utilizados por las potencias extranjeras. El 1 de noviembre de 1919 fue oficialmente formado el GC&CS, pero sus comienzos no fueron sencillos. En marzo de 1922, dado que el trabajo se centraba en las comunicaciones diplomáticas y no en las militares, el GC&CS pasó a depender de la Oficina de Relaciones Exteriores, dejando a un lado las relaciones con el Almirantazgo.

El gobierno británico mantuvo vivas leyes que permitían al gobierno capturar comunicaciones. La ley de Secretos Oficiales, aprobada en 1920, permitía al secretario de Estado, incluso en tiempo de paz, obligar a las compañías de comunicaciones a entregarle todos los mensajes que pasaran por sus cables. Bastaba con determinar que era conveniente para el interés público. Esta orden se puso en activo al momento y durante las siguientes dos décadas todos los cables con interés para el gobierno y con origen o destino en Reino Unido, acabaron en la mesa de trabajo del GC&CS. Menos oficial, eso sí, era la forma de obtener las claves que pasaban por Malta. Como siempre, se jugaba por encima y por debajo de la mesa.

Las manos británicas no diferenciaban entre países aliados y enemigos, y los códigos diplomáticos franceses y estadounidenses habían sido rotos y por lo tanto las comunicaciones que pasaban por el GC&CS acababan puestas en claro para conocimiento del gobierno. La marina italiana, que era del escaso tráfico militar que se interceptaba, tenía la costumbre de codificar editoriales políticos y enviarlos, lo que facilitó al GC&CS conocer su libro de códigos en poco tiempo.

Los alemanes, en cambio, habían aprendido la importancia de la seguridad y las consecuencias del telegrama Zimmermann los llevaron a mejorar sus códigos. Al acabar la guerra, utilizaban un libro de 100.000 grupos de códigos numéricos de cinco dígitos, cada uno de los cuales equivalía a una palabra o expresión. Este método tenía debilidades y fue mejorado incluyendo números aleatorios que se agregaban al código propiamente dicho, además de otros cambios. Estos códigos, que permanecieron en uso hasta 1942, con bastante éxito, fueron analizados por el GC&CS y se determinó que eran irrompibles.

La intervención más importante del GC&CS en la política internacional en la década de 1920 ocurrió en las relaciones con Rusia. Los códigos rusos no eran muy seguros y los británicos los leían sin problemas. Además, Ernst Fetterlein, uno de los principales criptógrafos rusos de la época zarista, había huido y había ofrecido sus servicios y conocimientos al país que más le pagara. Los británicos lo pusieron de su lado.

En mayo de 1920 el comisario de Comercio Exterior soviético, Leonid Krasin, se reunió en Londres con el primer ministro británico, para impulsar un acuerdo comercial que mejorara las deterioradas

relaciones entre ambos países. Las instrucciones que recibía Krasin directamente de Lenin eran conocidas por el GC&CS y por lo tanto también por el primer ministro. El líder ruso pedía a Krasin que no se fiara del británico, que era un hombre sin escrúpulos ni vergüenza. Esto era una mera anécdota al lado de la intención real de la misión diplomática, que también fue conocida gracias a los criptógrafos británicos. Los rusos pretendían usar el acuerdo comercial para transferir decenas de miles de libras a las organizaciones políticas británicas favorables a Rusia y para potenciar las publicaciones comunistas.

Rompiendo uno de los principios básicos de los servicios de inteligencia, el gobierno británico, de acuerdo con el propio GC&CS, entregó a varios periódicos los telegramas rusos interceptados y descifrados. Esto mismo se repitió en otras ocasiones a lo largo de la década, siempre para hacer públicos los movimientos de Rusia por influir en la política y en la sociedad británica. No en todos estos casos el GC&CS estuvo de acuerdo con la difusión pública de su trabajo, a diferencia de lo que ocurriría en el primer caso. En mayo de 1927 las relaciones entre ambos países quedaron finalmente rotas. En aquella ocasión se publicaron detalles del espionaje soviético en territorio británico, en contra de la opinión de Denniston, el director del GC&CS, que temía las consecuencias. El temor de este se cumplió y los rusos cambiaron sus códigos diplomáticos, adoptando una libreta de un solo uso. En la nueva situación, los códigos diplomáticos soviéticos, igual que había pasado con los alemanes, se volvieron irresolubles para la inteligencia británica. Hasta bien entrada la Segunda Guerra Mundial, esos códigos continuarían siendo seguros.

17. La Guerra Civil Española

En la Guerra Civil Española, ambos bandos tuvieron su servicio de criptografía, tanto para desarrollar e implantar métodos propios, como para atacar y romper los usados por el bando enemigo. Tras el primer momento de confusión, cuando comenzó a plasmarse claramente en las previsiones de unos y otros que el conflicto no se resolvería de manera rápida, se dieron los pasos para estructurar cada área necesaria, entre ellas la inteligencia y, por supuesto, la criptografía. Los primeros días fueron complejos, con unos y otros usando las cifras que conocían con anterioridad a la guerra, que en muchos casos eran compartidas con el enemigo. No había formación, los métodos era sencillos y a menudo inútiles para mantener la seguridad. Se podría llegar a decir incluso que cualquier comunicación enemiga captada podría ser leída sin demasiado esfuerzo. La falta de formación llevaba a cometer algunos de los errores que ya hemos descrito como básicos: mezclar texto en claro y cifrado en un mismo mensaje, o enviar un mensaje cifrado de varias formas, por no saber qué claves se tienen en el lugar de recepción del mensaje. Poco a poco fue solventándose ese caos inicial y los mandos de cada bando fueron organizando los usos, estableciendo reglas y distribuyendo las claves. En cualquier caso, al partir ambos bandos de bases muy parecidas, seguía habiendo un profundo conocimiento del otro y de su forma de hacer.

Los servicios de información del bando nacional se organizaron para cifrar las comunicaciones propias, capturar las del enemigo y descifrarlas. Gran parte de esta organización recayó en Antonio Sarmiento León-Troyano, que debió trabajar para que grupos heterogéneos, de distintas procedencias e incluso distintos países, con distintas formaciones, asumieran una forma de trabajo común. Sarmiento León-Troyano acompañó a Franco en su vuelo a Sevilla al comienzo de la guerra y sirvió de enlace con los alemanes y con los italianos. Con el paso de la guerra se fueron unificando bajo su mando los diferentes servicios de escucha, cifrado y descifrado. Esa centralización de trabajos, tanto de la escucha como del criptoanálisis, fue un acierto del bando de Franco, que le reportó ciertos éxitos.

En el bando republicano la situación fue mucho más caótica y no se desarrolló un servicio de escucha y descifrado tan sistemático como el del bando contrario, en gran medida por la propia diversidad de los republicanos. Esto hizo que los nacionales fueran capaces de romper muchas de sus cifras y por lo tanto conocer sus mensajes e intenciones. Igual que en el ejército franquista, el paso del tiempo fue generando cierta solidez en los métodos criptográficos republicanos y cierta formación entre sus filas, pero el desarrollo llegó antes en su enemigo y el conocimiento acumulado jugó en su contra. Posiblemente los asesores soviéticos fueran creando esa cultura sobre el cifrado tan necesaria en

el bando republicano, pero aun así los resultados no fueron los mejores si los miramos globalmente.

También hay que tener en cuenta que el bando nacional, con el paso de los meses de guerra, fue ganando territorio, lo que supone capturar puestos enemigos y hacer prisioneros. En muchos de estos casos, es de suponer, se encontrarían con claves, documentos cifrados y todo tipo de información que los llevaría a conocer mejor cómo operaba en el ámbito criptográfico su enemigo y por lo tanto a actuar con más eficacia.

Volviendo a Sarmiento León-Troyano, su trabajo de organización y sincronización de los diferentes servicios fue enorme, más teniendo en cuenta que se trataba de grupos de distintas nacionalidades, preparación y técnicas. Al inicio de la guerra entró a formar parte del Cuartel General de Franco y lo acompañó en su vuelo a Sevilla, como decíamos. Poco tiempo después, empezaría a encargarse de las secciones de Escucha, Radiogoniometría y Desencriptación, actuando también como enlace en asuntos de transmisiones con los especialistas alemanes e italianos. A finales de 1937 asumió además la jefatura de los Servicios de Escuchas, Cifra y Desencriptación, unificando los diferentes centros militares dedicados a estos menesteres. Poco tiempo después añadió a estos cometidos la jefatura de los servicios de radiogoniometría. Acabada la guerra, y hasta 1944, desempeñó el cargo de jefe del Negociado de Escuchas, Cifra y Criptografía. Como vemos, era sin duda un hombre clave en el ámbito que nos interesa, en la parte del bando nacional.

La coordinación que Sarmiento León-Troyano dio al bando nacional no se produjo en el republicano y la distribución de claves y su uso de manera general fue mucho más complicada, con grupos y entidades que no compartían las mismas claves o no las actualizaban de manera sincronizada. El 20 de octubre de 1937 la ciudad de Gijón estaba en manos republicanas, pero rodeada de tropas nacionales. Los mandos de la ciudad enviaron un mensaje al gobierno republicano, que entonces estaba en Valencia, indicando que la derrota era segura si no se enviaba la ayuda de la aviación para aligerar la situación de los asediados. La moral estaba muy baja y recibir ayuda desde fuera era necesario. El mensaje, por supuesto, iba cifrado. También, por supuesto, fue capturado por los nacionales y descifrado poco después del mediodía del mismo día de emisión. La estación de escucha en Burgos interceptó unas horas después un mensaje de respuesta desde Valencia, indicando que no conseguían descifrar el mensaje y solicitaban que lo enviaran de nuevo, usando una clave anterior. Este es tan solo un ejemplo de los problemas del bando republicano con la distribución de claves. Al día siguiente Gijón estaba ya en manos de los nacionales, que aprovecharon la ocasión y la baja moral de los asediados, tal y como ellos mismos habían informado.

La Comandancia de Baleares prestó un gran servicio al bando nacional en lo que a información se refiere. Constituyó un grupo de escucha y

descifrado, desde el comienzo de la guerra, ya en agosto de 1936, a cuya cabeza estaba Baltasar Nicolau Bordoy. Además de él, en el grupo había empleados de telégrafos que se dedicaban a escuchar las comunicaciones y, por supuesto, criptoanalistas provenientes de diferentes ámbitos sociales: matemáticos, aficionados a los crucigramas, jugadores de ajedrez… Entre todos fueron capaces de romper más de noventa claves y códigos enemigos a lo largo de 1937, trabajo que siguió en los años restantes de guerra y que le valió varios reconocimientos directos de Franco. De hecho, el mando del general Franco era el destino natural de sus descubrimientos, en ocasiones por radio, pero también, cuando la información lo requería, esta viajaba en avión directamente desde Mallorca hasta donde estuviera el propio general, ya fuera Salamanca, Burgos o cualquier otro lugar de la península.

Como ejemplo de los primeros meses en los que la criptografía no estuvo a la altura del momento histórico, tenemos una de las claves usadas por un grupo de guardias civiles. Durante el asedio al santuario de Nuestra Señora de la Cabeza, en el que las tropas republicanas se enfrentaron a unos dos centenares de guardias civiles y a un millar de civiles en Andújar, Jaén, los asediados trataron de comunicarse con el exterior cifrando los mensajes. Volvemos a ver cómo la criptografía es un recurso esencial en un asedio. Durante los nueve meses que duró aquel, entre septiembre de 1936 y mayo de 1937, los nacionales esperaron un rescate. Un rescate que, como en otras ocasiones en esta misma guerra, podría servir además como propaganda. En este caso el enfrentamiento no acabó bien para los que estaban dentro, que durante el asedio habían enviado palomas con mensajes cifrados para tratar de comunicarse con las tropas nacionales. Una de estas palomas fue abatida y el mensaje quedó descifrado en unas pocas horas. Más allá de la importancia del mensaje, lo relevante para nuestro objetivo es plasmar la inocencia del cifrado. El texto en claro se había camuflado con una sencilla sustitución numérica, donde a cada letra del alfabeto se le asignaba un número, comenzando en el 25. Un método que, como sabemos, es muy frágil frente a un simple análisis de frecuencia e incluso sin tener que recurrir a uno se podría deducir el texto en claro. Por si esto fuera poco, los números estaban ordenados, por lo que sabiendo que la a es el 25 y la d el 30, los números entre el 25 y el 30 solo podían corresponder a alguna de las letras entre a y d.

La variedad de métodos criptográficos utilizados en el tiempo que duró la guerra es muy extensa. Desde las máquinas Enigma que llegaron a España y que utilizó el bando nacional, hasta códigos muy sencillos, similares a los códigos de trinchera que se habían usado en la Primera Guerra Mundial. Por ejemplo, la Clave de Bous, que en diciembre de 1936 usaba la marina republicana en el Cantábrico para comunicarse, eran tan solo nueve páginas de códigos. Estos códigos indicaban qué número equivalía a una determinada situación en el mar. Lógicamente se trataba de situaciones siempre habituales y mensajes como «enemigo a la vista, me acerco a la costa y abro fuego», quedaban reducidos a una cadena compuesta por tan solo unas nueve letras y números.

Otros ejemplos de este tipo de códigos sencillos lo tenemos referenciado por José Bertrán y Musitu, que en el bando nacional dirigió una importante red de espionaje que operó en el norte de España. Esta red se denominaba Servicio de Información de la Frontera del Norte de España (SIFNE) y más tarde se integró en el Servicio de Información y Policía Militar (SIPM). La red, que operaba tras las líneas enemigas, tenía que comunicar información con rapidez y eficacia, a través de radios clandestinas. Los códigos usados eran tan solo números que, si bien no permitían llegar al detalle, aportaban información valiosa. Cada número indicaba cierta información y los siguientes aportaban detalles y cambiaban de significado, basándose en el número precedente. Por ejemplo, si el primer dígito era un 1, indicaba que se concentraban tropas del ejército de tierra enemigo, un 3 significaba lo mismo, pero para tropas de aviación, un 4 advertía de que el ataque era inminente… Si el segundo dígito era de nuevo un 1, que seguía al primero, ese 1 indicaba un determinado lugar en el que se concentraban tropas. Si el primer número era el 4, que advertía de un ataque inminente, el segundo número de la codificación indicaba el lugar del ataque, y los dos siguientes indicaban el día del mes previsto para el mismo.

Uno de los métodos más populares utilizados durante la guerra en España fue la cinta, que estuvo en uso en ambos bandos. Se basa en una tabla de homófonos en la que una cinta móvil, de ahí el nombre, funciona como clave frente a las letras del alfabeto, ordenadas de la A a la Z. Es decir, sería una tabla donde la fila primera muestra el alfabeto ordenado y la segunda fila, el alfabeto desordenado, siendo esta segunda fila una cinta que se puede mover, dando lugar así a diferentes combinaciones. El resto de la tabla cuenta con números distribuidos en algunas celdas, para generar esos homófonos.

Las tablas de homófonos fueron muy populares y constituyeron métodos más o menos creativos y sofisticados. Playfair también fue utilizado, como se descubrió no hace mucho, e incluso cifrados similares al descrito por Polibio, con algunos cambios. Hasta se hizo uso de la esteganografía en sus versiones más básicas. En el otro extremo estarían los usos de máquinas de rotores, como la propia Enigma, aunque hubo otras máquinas, de nuevo, en los dos bandos.

Entre los casos curiosos, podemos citar el día del propio levantamiento del bando franquista contra el gobierno, el 18 de julio de 1936. Esa mañana, Jorge Dezcallar, que era el enlace del capitán Luis López Varela con el general Mola para coordinar el levantamiento en Barcelona, llamó al capitán y le dijo que «mañana recibiría cinco resmas de papel». El mensaje oculto era que la sublevación se había programado para las cinco de la mañana.

Otro hecho peculiar ocurrió en Madrid, cuando estaba asediado por los nacionales, pero aún se mantenía en el bando republicano. En esa situación a la Quinta Columna madrileña le llegaban instrucciones a través de la radio, es decir, de las emisiones que todos podían escuchar con sus aparatos caseros. Con algún libro de cifrado común,

previamente acordado, el Cuartel General del Generalísimo daba instrucciones a los quintacolumnistas usando la radio como canal de envío del mensaje. Lo primero que hacía el mensaje radiado era identificar al destinatario del mismo, con una fórmula acordada. Es decir, una palabra o frase sin importancia o relevancia dentro del mensaje, hacía que el quintacolumnista en cuestión supiera que el mensaje iba dirigido a él. Las frases que se emitían a continuación tenían las instrucciones que el receptor debía seguir, después de decodificarlas convenientemente según un libro de códigos anteriormente acordado.

Durante la guerra se utilizaron distintas máquinas para cifrar, algunas ya anticuadas para el momento, y otras incipientes, como la Enigma o la Kryha. Esta última fue la primera máquina de cifra con cierto éxito comercial y aguantó en activo hasta los años cincuenta. A través de la marina italiana llegaron algunas máquinas Hagelin. El uso de estas herramientas avanzadas de cifra fue habitual en el banco nacional, pero no así en el republicano. Estos trataron de comprar, desde las entidades del gobierno, algunas máquinas de cifrado en Inglaterra, acudiendo también a los ministerios de aquel país, aunque los acercamientos no llegaron a buen puerto.

Probablemente por recomendación alemana, el bando sublevado adquirió algunas Enigma. No obstante, ya en 1931 el gobierno español del momento, a través del responsable de lo que hoy sería el Ministerio de Asuntos Exteriores, pidió un informe a la embajada en Berlín sobre el tipo de máquinas de cifrado usadas en Alemania. No llegó a más el interés y las primeras Enigma, diez en concreto, fueron adquiridas por el bando franquista en 1936 para asegurar las comunicaciones militares y diplomáticas. Estas máquinas cumplieron con su cometido entre los contendientes peninsulares, pero la inteligencia británica rompió el cifrado de esas máquinas Enigma comerciales, que eran más débiles en cuanto a su seguridad que las utilizadas por el ejército alemán. Dillwyn Knox, miembro de la inteligencia británica del que ya hemos hablado y que estuvo en activo hasta la Segunda Guerra Mundial, dirigía el grupo de personas que lo lograron. En cualquier caso, las marinas española, italiana y alemana, así como las principales unidades nacionales, cifraron sus comunicaciones sin que sus enemigos en la guerra fueran capaces de desvelarlas. Desde noviembre de 1936 hasta el final de la guerra, las máquinas cumplieron su cometido, e incluso después de la Guerra Civil española, y con la Segunda Guerra Mundial en marcha, el ejército español las siguió utilizando, incluso para sus comunicaciones con los agregados militares en París, Roma o Berlín.

Uno de los hechos de la Guerra Civil en el que la criptografía jugó un papel importante fue en el caso de buque *Mar Cantábrico* , un mercante con 132 metros de eslora y con capacidad para 7.500 toneladas de carga. Al comenzar la guerra, estaba en el puerto de Valencia y fue incautado por el bando republicano, dándole como primer uso el de prisión. A finales de 1936, el buque recibió la misión de navegar hasta Nueva York para recoger un importante cargamento de material bélico,

especialmente aviación. Aunque hay ciertas dudas, sí parece probado que llevaba varios aviones, motores, piezas de artillería, miles de armas de menor calibre, munición, bombas, granadas, aparatos de radio, ropa y alimentos.

Tras partir del puerto estadounidense, se dirigió a Veracruz, en México, para completar la carga. En un sobre que debía abrirse tan solo una vez en alta mar y que entregó el embajador en México, Félix Gordón Ordás, se indicaba al buque cómo debía actuar. Desde el otro lado del Atlántico debía dirigirse a Santander directamente, sin escalas, salvo que el gobierno español modificara estas instrucciones, y debía hacerlo a buen ritmo, para asegurar estar en el destino como máximo en las primeras horas de la madrugada del 6 de marzo, y siempre antes de la medianoche de ese día. Le indicaba también cómo y con quién podría comunicarse, y entre esas instrucciones figuraba el uso de la Clave X, que se le había entregado en el mismo momento que el sobre con las instrucciones. Este método era una cifra de sustitución monoalfabética con homófonos. Cada letra se sustituía por un número de dos dígitos. La clave, como bien podemos evaluar a estas alturas del texto, no era muy segura. Para cada letra había tres posibles números a elegir.

A B C D E F G H I J K L M

10 14 15 01 17 29 09 12 03 08 19 12 07

30 49 40 31 48 46 35 45 37 33 42 51 34

69 67 79 70 66 71 72 65 75 63 77 61 74

N O P Q R S T U V W X Y Z

27 18 02 22 16 05 20 11 06 23 26 25 04

50 44 32 53 43 36 56 47 38 58 41 54 39

73 60 76 62 78 89 64 81 68 85 87 86 82

Los nacionales estaban al tanto de la ruta y del cargamento del buque *Mar Cantábrico* . Aunque ha habido varias teorías sobre la fuente de dicha información, que van desde deserciones hasta deslices en las comunicaciones, lo que parece más cierto es la captura de ciertos mensajes y su descifrado. Entre la multitud de códigos y claves republicanas que desentrañó el grupo de criptoanalistas de Baleares que antes mencionábamos, hay algunas que tuvieron que ver con este caso. Concretamente, las claves Bocho, que era de tipo cinta, y Victoria, denominadas así por los criptoanalistas nacionales, eran las utilizadas por el gobierno vasco y el delegado del gobierno en Santander para comunicarse con el ministro Indalecio Prieto, a la sazón ministro de Marina y Aire. Mientras el *Mar Cantábrico* cruzaba el océano con su cargamento rumbo a Santander, ese triángulo formado por el gobierno vasco en Bilbao, la delegación del gobierno en Santander y el ministro,

que estaba en Valencia, intercambiaba información que acababa en manos enemigas.

El ministro comunicó a Bilbao, el 13 de febrero, que se estaba examinando la idea de establecer allí una fábrica de aviones y pedía valoración de las necesidades para llevar esa idea a cabo. El 5 de marzo, una nueva comunicación del ministro al norte, enviada en este caso a Santander y a Bilbao, usando la clave Bocho, mencionaba la llegada del *Mar Cantábrico* y hacía referencia a las instrucciones anteriormente comunicadas. La comunicación interceptada, que resultó fatal para el *Mar Cantábrico* , se transmitió el domingo 7 de marzo a las 21.15 horas, usando la clave Bocho, conocida por la Comandancia de Baleares. En ella el ministro compartía con el gobierno vasco que el buque *Mar Cantábrico* llegaría frente a Santander el lunes por la tarde. El capitán del barco quería saber si era mejor esperar a la noche para acercarse al puerto, y el ministro pedía al destinatario que se decidiera ese aspecto en el norte, lo que tiene sentido por conocerse mejor sobre el terreno la situación que se iba a encontrar el barco, y que comunicara dicha decisión al propio barco. En caso de no recibir instrucciones desde tierra, el barco haría el acercamiento al puerto por la noche. El ministro concluía hablando de la protección aérea de la llegada y pidiendo que se emplearan los barcos de guerra de la zona para dar auxilio al *Mar Cantábrico* , ya que seguramente estaría vigilado por el enemigo.

Unas horas más tarde de esta comunicación, en torno a las 23.00 horas de ese mismo día 7 de marzo, el crucero *Canarias* , que servía en el bando nacional, fue informado por radio de la llegada del buque *Mar Cantábrico* a Santander en la tarde del día siguiente. El *Canarias* , junto con otros barcos, se dispuso a interceptar el navío republicano y dirigirlo a un puerto propio, con la intención firme de no hundirlo y así hacer suya la carga que venía de Estados Unidos y México. El despliegue fue considerable, e incluso se dispusieron barcos en el sur de la península para tratar de evitar la huida hacia algún refugio en el Mediterráneo. El barco asediado había desplegado una acción de engaño cambiando su nombre por *Adda* y cambiando los colores y algún elemento más, simulando ser un buque británico.

Pasó media jornada desde que el *Canarias* interceptara al *Mar Cantábrico* , dándole orden de parar las máquinas, hasta hacerlo navegar hasta El Ferrol. La estratagema de engaño del carguero continuó y comenzó a enviar mensajes de auxilio en inglés, lo que atrajo a algunas naves extranjeras que acudieron en ayuda. Pero la mentira no se sostuvo más allá de eso y no recibió ayuda. Lo que sí recibió fue fuego desde el *Canarias* , ante la negativa a aceptar las órdenes enemigas. El *Mar Cantábrico* acabó con un boquete en el casco y con varios incendios a bordo, algo peligroso y que amenazaba con arruinar la valiosa mercancía que transportaba. Finalmente veintitrés hombres del *Canarias* subieron al mercante republicano y se hicieron con su control, poniendo rumbo a El Ferrol.

Fue el mayor buque civil apresado en la guerra. Su captura fue muy relevante para el desarrollo del conflicto en el norte de la península, y no solo por el material que transportaba y que nunca llegó a manos republicanas, sino también por el golpe moral e incluso también por la pérdida del propio buque.

El día 10, tres días después de la captura, desde Santander se informaba a Valencia de que el *Mar Cantábrico* había sido sorprendido por el *Canarias* , y que se desconocía qué había sido del barco y de su tripulación. Es interesante remarcar que se pensaba que el barco fue sorprendido. No se sospechaba que sus claves habían sido descubiertas. De hecho, comunicaciones posteriores atribuían la captura a algunos desertores que habían informado a los facciosos sobre el rumbo del *Mar Cantábrico* . Según los mandos republicanos, no podía explicarse de otra manera que se hubiese sorprendido al *Mar Cantábrico* en la extraña derrota que seguía. Estas comunicaciones seguían usando las claves Bocho y Victoria, y siguieron activas durante meses, por lo que el bando nacional estuvo en condiciones de adelantarse al enemigo en la guerra en el norte de la península, también tierra adentro.

Quizás por estas informaciones que hablan de deserción, hoy sigue sin haber certeza absoluta sobre el peso de la captura y descifrado de información en el destino del barco *Mar Cantábrico* . La información, en este caso y en otros muchos, era un factor más para las decisiones y acciones de uno y otro bando.

En el bando nacional, junto con la Legión Cóndor llegó un grupo de personas enviadas para desarrollar el servicio de captura de información y de descifrado, además de labores de espionaje. Elaboraban un informe diario que se enviaba al alto mando nacional, con información muy variada, proveniente de varias fuentes o procedimientos, entre los que estaba el descifrado de mensajes interceptados. Por parte del otro gran aliado extranjero del bando franquista, los italianos, también se puso en marcha, ya en octubre de 1936, un servicio similar. Entre otras fuentes, tenían espías en la zona republicana que informaban a Roma y cuyos datos finalmente acababan, de nuevo, en el alto mando nacional.

Los republicanos recibieron ayuda soviética también en este ámbito, aunque no parece que fuera tan importante como la ayuda internacional recibida por los nacionales.

Cuando, en el bando nacional, una información provenía de la ruptura de un mensaje cifrado capturado al enemigo, se solía indicar en la comunicación que la fuente era totalmente segura. Esta es la referencia, por cierto, que aparece en la información sobre el buque *Mar Cantábrico* que podemos ver en el parte de guerra del *Canarias* cuando documenta el aviso que recibe sobre el barco republicano que debe interceptar. Esa fuente segura que apuntó en su informe el *Canarias*

hace pensar aún más que el desciframiento de los mensajes fue crítico para la suerte del *Mar Cantábrico* .

No obstante, siempre existe el riesgo de que las capturas cifradas se hayan emitido así para engañar al enemigo, sabiendo o sospechando que captura y descifra el tráfico propio. Por lo tanto, siempre conviene ser prudente. La información puede ser tan valiosa como leer directamente el corazón del correo enemigo, o tan peligrosa como tomar por cierto algo que el enemigo nos envía como engaño. Es labor de la inteligencia saber interpretar y aprovechar cada situación. Un buen ejemplo de los errores en este campo lo tenemos en agosto de 1937, cuando el delegado del gobierno republicano en Santander informaba al ministro, que estaba en Valencia, de la delicada situación en la que se encontraban y le hacía partícipe de su miedo a que los nacionales se hicieran con el control del agua potable, dejando a la ciudad en una delicada situación. El mensaje fue capturado y descifrado. El miedo, que probablemente era bien fundado, se acabó convirtiendo en realidad y los nacionales pusieron su empeño en controlar el suministro de agua potable a Santander. Cuatro días después la noticia salía publicada en varios periódicos internacionales, y se incluía en ella que los nacionales habían capturado y descifrado las comunicaciones enemigas. Por supuesto, la clave que utilizaban los republicanos fue modificada al momento.

En cualquier caso, esto no era lo habitual. José María Iñiguez Almech fue un destacado catedrático de la Universidad de Zaragoza, doctorado en matemáticas, que prestó sus servicios como criptoanalista en el bando nacional con un éxito relevante. Entre sus contribuciones, averiguó una clave enemiga que estuvo en funcionamiento durante once meses y gracias a ella pudieron conocer el texto en claro de unos 35.000 mensajes. Como vemos, no era tan común cambiar claves con la regularidad necesaria y la autoconfianza era demasiado alta.

Aunque hemos comentado ya los problemas del bando republicano con la gestión de las claves y su uso, también es cierto que según los expertos en la criptografía guerracivilista, es muy complicado documentar y estudiar lo ocurrido en el bando derrotado. En cualquier caso, hubo personajes muy destacados que pusieron su talento al servicio de la República, como es el caso de Faustino Antonio Camazón. Este vallisoletano nacido en 1901, matemático, políglota y con una vida aún por descubrir en ciertos aspectos, destacó no solo en España y su guerra, sino también más allá de ese lugar y momento. Llegó a ser comisario de policía y trabajó para los servicios secretos españoles en el norte de África. Durante la guerra, ofreció formación a los milicianos para que estos conocieran, al menos, lo básico del uso de la criptografía. Como decíamos, no hay mucha información sobre la trayectoria de Camazón y su biografía se va reconstruyendo a trazos, con alguna mención puntual en algunos documentos, algunos comentarios de su familia, y siempre gracias al empeño de investigadores y aficionados a la criptografía españoles.

Al finalizar la Guerra Civil, se exilió en Francia, siendo internado en un campo de concentración, como tantos otros españoles que cruzaron al país vecino tras la derrota. Salió del campo, probablemente, gracias a algunos conocidos franceses de su época en el norte de África, con los que había desarrollado cierta relación y que conocían su faceta como criptógrafo. Es posible que su valedor fuera Gustave Bertrand, que entonces era responsable del criptoanálisis del Estado Mayor francés. Se integró entonces en el equipo de expertos que trabajaban en Francia con el objetivo puesto en los mensajes cifrados de la Alemania nazi. Formó parte del grupo PC Bruno de la inteligencia francesa y a medida que este país iba siendo presa de la *Blitzkrieg* alemana, fue enviado al sur de Francia, junto con sus compañeros. Allí se creó un nuevo puesto de escucha, el PC Cadix, y entre sus compañeros estaban los criptógrafos polacos que, como veremos, fueron los primeros en descifrar la máquina Enigma y cuya contribución en este campo a la guerra y a la historia es más que importante. Una de las fotos de Camazón que se han hecho públicas, tomada en 1942, muestra al español junto con Marian Rejewski, Henryk Zygalski y Jerzy Rozycki, tres nombres propios clave de la historia de la criptografía en el siglo XX. No es, por cierto, el único español en la foto, como tampoco fue el único español en colaborar con Francia en el ámbito de las cifras en aquella época. La relación con los polacos, eso sí, no debió de ser la mejor posible, debido a que unos venían de un país invadido por los soviéticos y los españoles estaban exiliados por combatir en el bando apoyado por los soviéticos en la Guerra Civil.

Cuando el sur de Francia, donde estaba el puesto PC Cadix, fue también ocupado por el enemigo, sus integrantes se movieron al norte de África. La nebulosa de la vida de Camazón se extiende también sobre su papel en la guerra, un papel que con toda probabilidad bien merecería un estudio destacado.

Como veremos también cuando nos adentremos en la Segunda Guerra Mundial, los franceses colaboraron estrechamente en el ámbito criptológico con los británicos y con los estadounidenses, por lo que es más que probable que Camazón y el resto de españoles tuvieran relación con algunas personas de Bletchley Park, como el propio Alan Turing. Tanto es así que, acabada la guerra mundial, Estados Unidos tentó al español, pero este decidió quedarse en Francia, siempre dentro de los servicios secretos. Cuando se jubiló, en 1966, volvió a España, donde residió hasta su muerte en 1982. Tras su muerte, su importante biblioteca fue vendida por la familia y hoy está custodiada en la Universidad de Zaragoza, donde se conoce como la Biblioteca del Espía.

La capacidad de comprensión de las cifras y de cómo debían ser que tenía Camazón, se puede comprobar en un documento de agosto de 1937, cuyo título es «Condiciones que debe requerir una cifra de uso general». En él se indican siete reglas que todo buen sistema de cifrado debe cumplir, por supuesto, para el momento y contexto en el que se movía. Recomendaba varios puntos a tener en cuenta: que no se usaran tablas ni medios auxiliares impresos; que no se indicara en el propio

mensaje un cambio de clave; que se modificara la clave a diario, a poder ser, y que este cambio no precisara comunicado entre las partes; que la operación de cifrado y descifrado fuera sencilla y rápida, y que fuera capaz de evitar en sí misma errores; y por último, hacía referencia a la capacidad de la cifra para resistir el criptoanálisis, dejando apuntado el análisis de frecuencia y la teoría de Kerckhoffs.

Además de esas reglas, Camazón proponía una cifra de su creación, que, como era de esperar, miraba a esas reglas para buscar la solidez y la seguridad, aunque es más un método sencillo y rápido que seguro. Como clave de su cifra el criptógrafo proponía utilizar la fecha del día, con algunos cambios. A cada mes le había asignado una secuencia de cuatro números: enero la 1213, febrero 3214, marzo 2134… seguida por el número de orden del mes. Así, enero quedaría en 12131, febrero en 32142, y marzo en 21343. A estos cinco números se añadía el día del mes en el que se cifraba el mensaje, y se multiplicaría el número resultante por el día de la semana, del 1, lunes, al 7, domingo. El 5 de marzo de 1937, que fue viernes, daría entonces lugar a la clave diaria 1067175, que es el resultado de 213435 multiplicado por el 5 del viernes. De ese número, el 1067175 en nuestro ejemplo, se eliminan las cifras repetidas, comenzando por la izquierda, sustituyéndolas por los números en orden de menor a mayor, que no aparecen en la cifra. Así, el 1067175 quedaría en 2063175, al sustituir el 1 de la izquierda, repetido, por el 2, y el primer 7 por el 3. Esta secuencia sería la clave generada para el día 5 de marzo de 1937. Como vemos el proceso es sencillo, se puede hacer rápidamente y permite generar una clave diaria sin tener que compartir un documento con información para ello. A cambio, las claves no son aleatorias, que sería lo deseable, sino que hay un método detrás. Averiguado el método de generación de clave, quedaría arruinada la seguridad del proceso.

Además de este procedimiento de generación de la clave, Camazón propone el método de cifrado completo, pero basta esta primera parte de generación de la clave para poner en valor su preocupación por usar métodos sólidos y seguros, en un entorno en el que aún en 1939 es posible encontrarse cifrados de sustitución simple donde a cada letra se le asigna un número de dos cifras, como es el caso del Tribunal Especial de Guardia de Barcelona.

PARTE 4LA SEGUNDA GUERRA MUNDIAL

18. Las máquinas de rotores en el camino hacia la guerra

Las matemáticas siempre han tenido una estrecha relación con la criptografía, pero a medida que los siglos han pasado y se han hecho más complejos los sistemas, las matemáticas se han hecho más importantes como pilar de la criptografía. En 1929, Lester S. Hill, un matemático estadounidense, interesado en la relación entre las matemáticas y las comunicaciones, publicó un artículo en la revista *American Mathematical Monthly* exponiendo un criptosistema en el que las ecuaciones algebraicas eran la base sobre la que se describían las acciones y procesos del cifrado. No era un avance relevante en cuanto a la seguridad del método, pero fue Hill el primero en unir el álgebra y la criptografía, comenzando a desbrozar un camino que se ha ido ensanchando con el paso del tiempo y que es por el que transitan los métodos criptográficos actuales.

Los avances en la ciencia criptográfica a lo largo del periodo de entreguerras iban afianzando el conocimiento matemático detrás de los métodos, y creando así una serie de pilares sobre los que se afirmaban las ideas criptográficas. Las cifras polialfabéticas tenían como punto débil los posibles rastros en ellas del texto claro, tanto de sus palabras como del propio idioma en el que estaba redactado. Esos rastros permitían a los criptoanalistas encontrar hilos de los que tirar, hipótesis sobre las que trabajar. En 1935 Solomon Kullback, que formaba parte del equipo de criptógrafos estadounidenses dirigido por William Friedman en el Signals Intelligence Service (SIS) del ejército de su país, desarrolló un análisis matemático sobre los cifrados polialfabéticos. Kullback demostró en ese estudio que un cifrado polialfabético puede ser vulnerable al análisis de frecuencia, siempre que el texto cifrado disponible para el criptoanálisis sea suficientemente abundante.

Ya sabemos que si la clave es infinita el cifrado será seguro. Pero también sospechamos que generar una clave infinita y que a su vez ese sistema de generación de clave tenga utilidad operativa, esto es, se pueda usar en la práctica, es un empeño más que complicado. Por lo tanto, la clave en algún momento tiene un fin y se volverá a comenzar por el principio de la misma. Ya hemos visto también que, en siglos pasados, en los cifrados basados en una clave de unas pocas letras, esa clave se repetía de manera cíclica para cifrar todo el mensaje. Si, por ejemplo, tuviéramos una clave de longitud diez, formada por diez caracteres, la letra primera, la undécima, la vigésimo primera… del texto en claro, serían cifradas con la misma letra de la clave. De igual modo, la segunda, la duodécima… lo serán con la segunda. Por lo tanto, concluyó Kullback, cualquier cifrado polialfabético realizado con una clave de longitud n, puede reducirse en principio a un problema de romper n cifrados de sustitución monoalfabéticos independientes. Para hacer posible este análisis de frecuencia de cada uno de los cifrados monoalfabéticos, se necesita un número de letras cifradas

suficientemente alto, lo que multiplicado por los distintos cifrados monoalfabéticos, que serán tantos como la longitud de la clave, nos lleva a requerir una cantidad de texto cifrado elevada. Cuanto más larga sea la clave, más largo tendrá que ser el texto cifrado. La longitud de la clave, por supuesto, tampoco es conocida por el criptoanalista, por lo que tendrá que llevar a cabo la exploración de las distintas posibilidades para saber cómo extraer los n cifrados monoalfabéticos del texto cifrado polialfabéticamente.

Este tipo de conocimientos y razonamientos, si bien no lleva a la resolución directa de los cifrados, sí supone una base importante. Unido al conocimiento del idioma, al funcionamiento de las máquinas de cifrado y a los procedimientos y costumbres de los ejércitos y operadores que usaban las máquinas, permitieron tanto a los polacos, como a los británicos y a los estadounidenses encontrar formas de atacar los cifrados, diseñar máquinas y procedimientos que aceleraran los procesos de criptoanálisis mediante automatismos que, finalmente, llevaran a romper el cifrado de las máquinas de rotores.

El descifrado de los sistemas criptográficos alemanes es uno de los elementos clave en la historia de la Segunda Guerra Mundial. En este conflicto los avances científicos y técnicos fueron revolucionarios y ambos campos, la guerra y la ciencia, se retroalimentaron de manera acelerada, algo que, por otra parte, ha sido habitual a lo largo de la historia. Muchos conocimientos técnicos estaban, antes de la guerra, en el punto exacto para ser explotados. Vannevar Bush, por ejemplo, que tuvo un papel relevante en el desarrollo de la bomba atómica, quizás uno de los ejemplos paradigmáticos de este encuentro entre guerra y ciencia, y que fue presidente de la Comisión Investigadora para la Defensa Nacional estadounidense, aseguraba que «los descubrimientos científicos revolucionaron por completo el concepto ideal de guerra y, hacia el final de la contienda, todo lo que creíamos saber acerca de la guerra ideal estaba obsoleto. Fue la única vez en la historia que ocurrió y no puede volver a ocurrir, porque antes de la guerra había una gran reserva de conocimiento técnico acumulado, lista para su utilización, pero nunca se había aplicado a asuntos militares; y además hubo un gran florecimiento de nuevas ideas y nuevos aparatos».

Esta relación no es algo nuevo, sino que tiene siglos de historia. Basta ver los tratados matemáticos o las investigaciones químicas relativas a la artillería, para ver que la conexión entre la ciencia y el ámbito militar siempre ha estado ahí. Lo que ocurre es que como casi todo lo relacionado con la Segunda Guerra Mundial, el orden de magnitud es enorme. Se estudiaba y desarrollaba cada detalle, con una dotación de recursos nunca antes vista. Sirva como ejemplo el testimonio del capitán de fragata Peter Gretton, jefe de grupo de escolta naval, que nos muestra la aplicación de técnicas que hoy son perfectamente habituales en el mundo empresarial y que, si bien han sido potenciadas por la cantidad de datos y la capacidad de computación actual, en su núcleo son similares. Decía Gretton que los científicos, en el ámbito de la batalla del Atlántico, analizaban ataques de aviación, ataques a

submarinos con determinados buques, estadísticas sobre movimientos de convoyes y todo tipo de datos similares. Con estos datos estadísticos, elaboraban hipótesis que ponían a prueba para analizar los resultados. Cambiaban la forma de navegar, el uso de los aviones, cómo defender los convoyes… Por ejemplo, un grupo de estos protocientíficos de datos estudió el tamaño de los convoyes que cruzaban el Atlántico y que eran asediados y hundidos por las manadas de lobos de la Ubootwaffe, los submarinos alemanes. Descubrieron que, si se doblaba el tamaño de los convoyes, se optimizaba el esfuerzo en protección de ese tráfico, ya que el número de suministros transportados se duplicaba, pero en cambio la fuerza de protección tan solo había que aumentarla un poco para conseguir el mismo nivel de seguridad y protección. Este uso más eficiente de los buques de escolta suponía poder lanzar más convoyes a la ruta e incluso derivar buques de protección a otras tareas.

El avance de la criptográfica durante la Segunda Guerra Mundial fue enorme, e igual de enorme fue el aprovechamiento para la propia guerra de la criptografía y el criptoanálisis. El método para atacar cifrados polialfabéticos descrito por Babbage y por Kasiski, se sabía efectivo y tan solo había que seguir unos pasos sistemáticamente: buscar repeticiones de grupos de letras en el texto cifrado; calcular la distancia entre esos grupos, ya que esa distancia será un múltiplo de la longitud de la clave; determinar la longitud buscando divisores comunes a las distintas longitudes de las diferentes secuencias de letras repetidas; agrupar las letras cifradas con cada uno de los alfabetos; y, por último, aplicar el análisis de frecuencias a cada grupo de letras. En la teoría, como hemos visto, existe una forma de conseguir que este método sea totalmente inútil y es haciendo que no se repitan nunca las secuencias, es decir, que, en el salto de un alfabeto a otro durante el cifrado de las letras, nunca se vuelva a un alfabeto utilizado anteriormente, o, si se hace, que sea tan larga la distancia en el texto cifrado que se convierta en una tarea imposible encontrar la conexión. Generar ese número enorme de alfabetos y hacerlo, además, de manera automática, está en la base de las máquinas de rotores.

La idea de Vernam de unir en un único dispositivo comunicación y cifrado, en un teletipo en su caso, se había mostrado poderosa. De hecho, a medida que el siglo XX avanzaba las máquinas de escribir iban poblando todas las oficinas del mundo civilizado, ocupando más y más espacio en ellas y, por supuesto, también en las embajadas y en las instalaciones militares y gubernamentales. Los inventores y las empresas no tardaron en hacer suya la obligación de satisfacer la demanda de dispositivos que incluyeran el cifrado de manera interna e implícita, como el teletipo de Vernam.

Para alcanzar este objetivo, los criptógrafos se inspiraron en algunos inventos anteriores. Por ejemplo, Thomas Jefferson, uno de los firmantes de la Declaración de Independencia de Estados Unidos y el tercer presidente que tuvo ese país, diseñó un mecanismo conocido como la rueda de Jefferson y que ya contiene alguna idea que más tarde incorporaron las máquinas de rotores, la solución de la industria

criptográfica a la demanda a la que hacíamos referencia. Este dispositivo era un cilindro que se formaba con 36 discos de madera de igual tamaño, numerados y atravesados por un perno que los unía a la vez que permitía que giraran libremente. A lo largo del perímetro de cada disco, en la parte exterior, estaban grabadas las letras del alfabeto, en un orden distinto en cada uno de ellos. La clave estaba en el orden en el que se montaban los discos dentro del dispositivo, es decir, de su orden a lo largo del cilindro que ellos mismos formaban. Ese orden era exactamente lo que tenían que acordar y conocer emisor y receptor para cifrar y descifrar, y dado que tenemos 36 discos, el número de combinaciones diferentes es de 3.719.933.268 elevado a 41, es decir, un número de 42 dígitos.

Para cifrar se había de dividir el texto en claro en bloques de 36 letras. Se giraban los cilindros hasta que se leyera, a lo largo de una de las líneas de letras que formaba el disco, el primer bloque, las primeras 36 letras del mensaje. Entonces se escogía cualquiera de las otras secuencias de letras que forman los discos y se enviaba como texto cifrado. Se giraban entonces los discos para que, en otra línea diferente, se pueda leer el segundo bloque del texto en claro, y de nuevo se envía cualquiera de las otras 25 filas de letras.

La rueda de Jefferson nunca llegó a utilizarse. Una idea similar fue creada por el francés Étienne Bazeries en 1891, sin conocer los diseños del estadounidense, y gracias a la enemistad de este inventor francés con su compatriota León de Viaris, se profundizó en el criptoanálisis del sistema de criptografía basado en los discos giratorios, antecedente de las máquinas de rotores. El ejército de Estados Unidos perfeccionó el diseño y en 1922, gracias al equipo de criptoanalistas dirigido por William Friedman, comenzó a utilizar el sistema M-94, que era una rueda similar a la de Jefferson y Bazeries, con algunas mejoras para desterrar los problemas detectados en estas últimas. Este sistema, y alguno más avanzado, el M-138, fueron utilizados hasta el final de la Segunda Guerra Mundial, aunque fue roto con éxito por los criptoanalistas alemanes.

Todas estas ideas, como decíamos, sirvieron de inspiración y de base para el diseño de esas máquinas de escribir con cifrado incluido que demandaban los gobiernos y buscaba la industria. Las ideas que se iban probando y los prototipos generados, no disponían todavía de la capacidad para memorizar varias letras y codificarlas en bloque, por lo que seguían operando letra a letra. Así, no eran viables criptosistemas con transposiciones y las líneas de trabajo se movían en el mundo de los cifrados polialfabéticos. Por lo tanto, el criptoanálisis ideado por Kasiski y por Babbage los hacía vulnerables, salvo que la longitud de la clave fuera tan grande que el periodo de repetición fuera un número suficientemente grande como para que esos métodos de ataque fueran inviables por la imposibilidad práctica de realizarlos. Esta idea, por cierto, sigue siendo válida en la actualidad, donde a pesar de la enorme capacidad de los ordenadores, los sistemas se muestran seguros, no por la seguridad total de los mismos, sino por la incapacidad práctica, dada

la capacidad de computación actual, de resolver el cifrado en un tiempo razonable y útil.

Ante este problema, de manera paralela en varios lugares y en varias empresas, se fue llegando a la misma solución: la máquina de rotores. En 1915 dos oficiales navales holandeses, Theo A. Hengel y Rudolf Spengler, fueron los primeros en idear una máquina de rotores para cifrar. Construyeron un prototipo que presentaron a la armada holandesa, aunque esta no apoyó la idea. La patente de los dos oficiales tuvo varios problemas, precisamente por pertenecer ellos al ejército. Cuando finalmente recibieron la aceptación definitiva para poder patentar su idea, era noviembre de 1919. Todo esto provocó que hasta el año 2003 no se considerara a Hengel y Spengler como los verdaderos creadores de la máquina de rotores.

Durante todo ese tiempo, hasta 2003, se consideró el inventor de la primera de esas máquinas a Edward Hugh Hebern, un estadounidense que entre 1912 y 1915 patentó varios diseños de dispositivos de cifrado. En 1917 patentó una máquina con un rotor que podía ser insertado en ambas orientaciones y así cifraba y descifraba. Más tarde la mejoró añadiendo rotores y creó una empresa, Hebern Electric Code Company, para comercializar su invento patentado. Lo cierto es que el negocio no fue todo lo bien que esperaba el creador y después de vender poco más de una decena de máquinas, su empresa entró en bancarrota e incluso le llevó a prisión, debido a que algunos de sus inversores lo acusaban de fraude.

A partir del invento de Hebern, William Friedman, del que hablaremos con detalle más adelante, mejoró el diseño y creó la máquina conocida como SIGABA o ECM Mark II. Esta incorporaba la rotación irregular de rotores, lo que la hacía más segura al aumentar la complejidad del texto cifrado, su variabilidad. Este detalle es quizás el elemento más relevante de esta máquina, haciéndola, al menos en este aspecto, mejor que sus contemporáneas. De hecho, la máquina Enigma alemana tenía un movimiento mucho menos aleatorio de sus rotores, si bien técnicamente ninguno de los dos era puramente aleatorio.

19. La máquina Enigma

La máquina Enigma, que fue un elemento clave en la Segunda Guerra Mundial, llegó ligeramente tarde para la Primera Guerra Mundial. En 1918, Arthur Scherbius y Richard Ritter, dos alemanes, crearon la empresa Scherbius y Ritter, cuya actividad era el diseño y creación de diferentes tipos de inventos. Scherbius, que se había formado en ingeniería eléctrica en la Universidad Técnica de Múnich y en la Universidad de Hannover, alcanzando el título de doctor, era un experto en motores. No obstante, los diseños de la empresa eran diversos, desde motores hasta turbinas o almohadas eléctricas. El 23 de febrero de 1918 solicitaron la patente de una máquina de cifrar basada en discos móviles que variaban de posición durante el cifrado. Era la primera versión de las máquinas de rotores, como se las conoce habitualmente, y era la idea inicial de Enigma. El invento tendría su lugar en la historia, aunque aún le quedaba algún paso que dar, ya que aquella primera versión, el modelo A, era grande y pesada, algo que se iría mejorando con nuevos diseños, con los modelos siguientes, modelo B y modelo C. Este último fue lanzado en 1926 y entre otras mejoras su peso se había reducido significativamente, desde los casi 50 kilos de la primera versión hasta los casi 12 del modelo C. El modelo D fue el más avanzado y llevó a sus creadores al éxito comercial.

En 1919 Hugo Alexander Koch había patentado en Europa, concretamente en Holanda, la máquina de rotores. La falta de ventas hizo que finalmente los diseños y derechos de Koch fueran adquiridos por Scherbius en 1927. Tres días después de que Koch patentara su invento en 1919, el sueco Arvid Gerhard Damm hacía lo propio con su diseño, pero algunos problemas en el funcionamiento de su máquina impedían el éxito comercial. Entre sus inversores estaba Karl Wilhelm Hagelin, padre de Boris Hagelin. Este había estudiado ingeniería y se incorporó a la empresa de Damm, de la que acabaría siendo el máximo responsable. En 1926, con los diseños mejorados y con una máquina más estable y segura, el ejército sueco encargó un pedido importante y la empresa comenzó una senda de éxito. La máquina Hagelin era capaz de imprimir, en lugar de usar lámparas para ir mostrando las letras resultado del cifrado, y era muy ligera. Con el paso de los años la empresa se convirtió en proveedora del ejército estadounidense, que diseñó y realizó mejoras en la C-38, un modelo de Hagelin, que rebautizaría como M-209. De este modelo hubo unas 140.000 unidades operando durante la Segunda Guerra Mundial, llevando definitivamente a Hagelin y a su empresa al mayor éxito comercial de todas las empresas dedicadas a las máquinas de rotores para el cifrado.

La armada alemana en febrero de 1926 y el ejército en junio de 1928, encargaron máquinas Enigma a la empresa de Scherbius y Ritter, añadiendo en los pedidos cambios que solo debían incorporarse a los modelos militares, haciéndolos más avanzados y seguros. Es posible ver

en estas peticiones poca fidelidad al espíritu del Tratado de Versalles, porque lo cierto es que con el paso de los años se mejoraron las propias máquinas, se implantó su uso de manera general en el ejército alemán y se fueron diseñando procedimientos para su utilización, cada vez más avanzados y estrictos. Entre los alemanes que asistieron a las primeras demostraciones de Enigma al ejército estaba Wilhelm Tranow, un personaje que, como veremos, fue clave en las labores criptográficas en la Segunda Guerra Mundial. Los acercamientos no fueron sencillos, ya que las duras restricciones impuestas al ejército alemán por los vencedores de la Primera Guerra Mundial hacían que el precio de las máquinas, unos 5.000 marcos cada una, lo que serían hoy unos 20.000 dólares, supusiera un coste muy significativo. Aunque la Inteligencia Naval alemana, conocida como N en aquel momento, estaba interesada, se habían reducido tanto su personal y su presupuesto, que Scherbius no tuvo éxito en un primer momento en sus ventas. No obstante, después de un tiempo, y con el ejército alemán reconstruyéndose en la sombra, Tranow volvió a contactar con Scherbius, en 1924, y llegaron a un acuerdo.

La Inteligencia Naval, conocida como B-Dienst, aunque su nombre oficial era Beobachtungsdienst, fue creada en 1919, pero hasta 1923 no estuvo realmente operativa, y aun así en aquel momento los recursos tampoco eran importantes. Tenía entonces algunas estaciones de escucha en el Mar del Norte y en el Báltico y una unidad de criptografía. Una de las primeras tareas de esta unidad fue el estudio de la batalla de las cifras y las señales durante la Primera Guerra Mundial: hasta dónde había llegado cada país. Tranow y otros criptógrafos del B-Dienst se dedicaron a leer libros, revistas militares, memorias… e ir sacando conclusiones. Esto les sirvió para aprender de errores anteriores y para prepararse tanto para proteger sus comunicaciones como para penetrar en el conocimiento de los movimientos y mensajes de otros países. Dentro de estas últimas labores, pusieron bajo la lupa a los británicos, cuyos mercantes enviaban todos los días un mensaje de radio con su posición, lo que era un comienzo. También las cifras de la Royal Navy eran materia de estudio de los alemanes. Sus movimientos se enviaban mediante mensajes cifrados, y los germanos implantaron una red de informadores que les decían qué barcos británicos llegaban a un puerto, cuáles lo dejaban, y cualquier otro dato de interés. Al capturar la información cifrada que enviaban los propios barcos a Londres, los criptoanalistas del B-Dienst tenían pistas suficientes para buscar palabras del texto en claro, como nombres de puertos y barcos que conocían gracias a los informadores. Así, poco a poco, se iban desvelando los libros de códigos.

Volviendo a las Enigma, la idea del disco de cifrar no era nueva. Alberti ya había trabajado sobre este concepto en el siglo XV, pero las nuevas capacidades técnicas podían hacer su uso práctico más sencillo e incorporar variaciones que aumentaran la fuerza del método de cifrado. Scherbius era el inventor, el diseñador de la compañía y desarrolló determinados elementos en sus máquinas de cifrar que las hacían más sólidas y resistentes a un posible criptoanálisis.

Dicho de manera esquemática, una máquina Enigma tiene tres componentes. En primer lugar, un teclado en el que el operador escribe el texto en claro, es decir, escribe igual que lo haría en una máquina de escribir tradicional. En segundo lugar, el motor de cifrado propiamente dicho, que toma la letra que ha pulsado el operador y la transforma en una totalmente distinta. Este segundo elemento es el corazón de la máquina, es donde ocurre realmente el cifrado y donde están sus fortalezas y las debilidades. El tercer y último elemento sería el tablero donde una serie de luces le indican al operador cuál es el resultado del cifrado. Es decir, el operador pulsa, por ejemplo, una A en el teclado, el motor de cifrado se pone en marcha y genera la letra de salida, la letra cifrada, que es indicada al operador mediante una luz en el panel de cifrado. El motor funciona mediante impulsos eléctricos y tiene la gran ventaja de que cada vez que se cifra una letra, el propio motor varía, generando así la seudoaleatoriedad continua en el cifrado que hará que un criptoanalista no pueda averiguar el mensaje en claro con facilidad.

Hemos visto que la repetición es uno de los enemigos principales de los métodos criptográficos, y por ello es decisivo que la máquina de cifrado vaya variando de tal forma que no se generen ciclos o estos ocurran tras cifrar un texto suficientemente largo. El motor de cifrado se basaba en lo que se denominaba un rotor, que no es otra cosa que un disco con puntos metálicos, conectores eléctricos, en ambas caras. Estos puntos metálicos, en una máquina con un único rotor, conectarían las entradas desde el teclado con las salidas en el tablero de luces. Dentro del propio rotor se conectan las entradas con las salidas de manera no directa, es decir, irregularmente. Cada conector de una cara se conecta mediante un cable interno del propio rotor a un conector de la cara opuesta. Por lo tanto, un rotor contiene internamente una maraña de cables que unen los conectores de ambas caras.

En el caso más sencillo, al pulsar en el teclado, por ejemplo la A, un impulso eléctrico llega a un conector del rotor y el cableado interno del rotor hace que ese impulso salga por uno de los conectores de salida e ilumine una lámpara en el tablero, por ejemplo la correspondiente a la J. Tras esto, el rotor hace un pequeño giro. Así, si volvemos a pulsar la A en el teclado de la máquina, el impulso eléctrico no llegará al mismo conector de entrada del rotor, ya que este ha girado, y por lo tanto, al cambiar el conector de entrada cambia también el de salida. Esta vez, al pulsar de nuevo la A, la lámpara iluminada en el tablero no será la correspondiente a la J, sino otra cualquiera. La corriente eléctrica, como es lógico, proviene de una batería incorporada en la propia máquina que la hace portátil y útil para ser usada en casi cualquier lugar, también en el campo de batalla.

Un solo disco, un solo rotor, tendría una debilidad. Una vez completada una vuelta del disco, las correspondencias se repiten y la A en la entrada, siguiendo con el ejemplo anterior, volvería a iluminar la J en la salida. Como ya hemos dicho, la repetición es enemiga de la seguridad y, por lo tanto, el diseño de Scherbius incorporó varios rotores. Así, cada vez que el primer rotor completaba una vuelta, el segundo giraba una

posición. Esto hacía que la longitud de los ciclos, para volver al punto inicial, fuera mucho más larga. Conceptualmente es similar a las agujas de un reloj. Cuando la aguja larga completa una vuelta, la corta se mueve una posición y permanece estática en ella hasta que hay un nuevo giro completo de la aguja larga.

En el caso de la máquina Enigma, si bien hubo diferentes versiones con pequeños cambios, el funcionamiento era todavía más complejo y los alemanes habían incorporado algunos aspectos de uso que aumentaban la seguridad exponencialmente, al hacer mucho más elevado el número de combinaciones posibles de los elementos. Para comenzar, la máquina Enigma tenía tres rotores conectados entre sí, en su versión más sencilla. Estos rotores tenían 26 conectores en cada una de sus caras, correspondientes a 26 letras. Los tres rotores no estaban fijos en la máquina, sino que se podían sustituir unos por otros. De igual forma, tampoco estaba establecido el orden de los mismos, por lo que el número de combinaciones se multiplicaba y multiplicaba. Hay que tener en cuenta que cada rotor tiene unas conexiones internas distintas, por lo que el circuito de conexión entre la letra del teclado, que sería el texto en claro, y la luz que indica la letra cifrada, será diferente según el orden de los rotores. Si vemos el funcionamiento interno de la máquina como un circuito eléctrico que conecta una letra del teclado con una letra del tablero de bombillas, podemos imaginar claramente cómo se va construyendo ese circuito a través de los rotores. La corriente eléctrica entra en el primer rotor por un conector y, gracias al cableado interno, sale por un conector de la cara opuesta. Este conector de salida del primer rotor está en contacto con un conector de entrada del segundo rotor, que a su vez está cableado hacia un conector de salida. Ocurre algo similar con el tercer rotor, y la salida de este llevaría a una letra del panel de luces, ya que cada conector de la cara de salida del último rotor activa una luz distinta.

Para mejorar la seguridad, cada máquina iba acompañada de un juego de cinco rotores distintos, de los que se tenían que tomar tres para configurar la máquina. Como el orden es importante, tenemos 60 opciones diferentes de seleccionar tres rotores para la máquina. La posición inicial de los rotores también era un elemento crítico de la configuración de partida de la máquina, ya que el mismo rotor, en distintas posiciones, primera, segunda o tercera, genera un circuito diferente y por lo tanto un cifrado también distinto. Cada rotor tenía 26 números escritos a lo largo del canto, de su perímetro. Al colocar el rotor dentro de la máquina y cerrar la tapa que los protegía, se venía a través de un orificio en dicha tapa el número del canto del rotor que quedaba en la parte superior. La tapa tenía tres ventanas, una para cada rotor, y esos tres números definían la configuración de inicio de la máquina. En resumen, para dotar a la máquina de una determinada configuración en su posición de inicio, el operador tenía que tomar tres discos de los cinco que la acompañaban, colocarlos en el orden adecuado dentro de la máquina, y girar los discos para que los números deseados del canto de cada rotor quedaran en la posición superior. El número de opciones de configuración de la máquina que brindaban las posiciones de los rotores era de 17.576, es decir, $26 \times 26 \times 26$. Ya

hemos visto que según cuáles fueran los rotores que se seleccionaran y el orden de los mismos, generaba 60 opciones de inicio, por lo que el número de posibles combinaciones de origen de la máquina es enorme. Esto hace que sea casi imposible probar todas las posibles opciones, lo que llamaríamos un ataque por fuerza bruta.

Con esta configuración inicial establecida en la máquina, el operador de la misma comenzaba a pulsar el mensaje en claro en el teclado, y como se ha visto por cada tecla pulsada se iluminaba una bombilla en el tablero de luces. El operador debía ir apuntando las letras que indicaran esas luces, ya que así compondría el mensaje cifrado. Enigma es una máquina tan solo de cifrado, no tiene incorporado ningún tipo de envío. Por lo tanto, una vez cifrado el mensaje a emitir, esa secuencia de letras que es el mensaje cifrado, debe ser enviada por radio y en código morse por un operador de comunicaciones. El receptor de la comunicación recibirá el mensaje cifrado y lo escribirá en un papel. El operador de la máquina Enigma que debe descifrar el mensaje en destino, lo primero que tiene que hacer es poner en la máquina la misma configuración que se usó para cifrar y a partir de ese momento comenzar a teclear las letras una a una. La máquina iluminará en el panel las letras correspondientes a cada una de las letras pulsadas y así el receptor tendrá el mensaje en claro. Es decir, dada una configuración de la máquina y para una misma posición de los rotores, que hay que recordar que van girando cada vez que se cifra una letra, dos letras estarán unidas conceptualmente en la máquina. Por tanto, si se pulsa una en el teclado se iluminará la otra en el panel, y viceversa. Este detalle es muy importante, ya que es el que permite que la máquina sirva a la vez para cifrar y para descifrar, lo que supone una gran comodidad.

Lo que acabamos de describir es el funcionamiento básico de una máquina Enigma no militar, la que podía comprar cualquier empresa o entidad que no fuera el ejército alemán. Las Enigma militares tenían añadido un tablero de conexiones en la parte frontal que multiplicaba las opciones de configuración de la máquina y, por tanto, también su seguridad. Este tablero o panel de conexiones tenía 26 clavijas, cada una correspondiente a una letra, y había 10 cables que podían unir dos de estas letras como el operador quisiera. Era algo similar a las clásicas centralitas telefónicas, donde la operadora unía dos puntos del clavijero, dos teléfonos, mediante un cable, introduciendo la clavija de cada extremo del cable en esos dos puntos del clavijero que deseaba unir. Esos 10 cables unían dos letras, y lo que hacían era cambiar en el circuito una letra por otra. Esto es, si en el clavijero se unían la A y la J, por ejemplo, al pulsar en el teclado una A, el circuito eléctrico que ya hemos explicado era extendido y antes de comenzar el proceso en los rotores se hacía el cambio de la A por la J. Estos 10 cables, que podían conectar dos letras cualesquiera de las 26 de la máquina, eran un elemento más de la configuración inicial de la máquina y lo que hacían era aumentar el número posible de esas configuraciones, hasta alcanzar billones de combinaciones.

Falta aún otro detalle de la máquina y es que la parte del circuito que contenía los rotores tenía un añadido a lo que hemos explicado. En realidad, del tercer rotor no iba al panel de bombillas, sino que volvía al segundo y al primero. Esto se hacía mediante un disco similar al resto de rotores, pero con contactos tan solo en uno de sus lados. Este elemento se conocía como reflector y la corriente entraba por un conector y salía por otro conector, ambos de la misma cara, la que estaba en contacto con el último rotor. El circuito se alargaba así y el viaje de la corriente a través de la maraña de claves que tenían los rotores internamente se multiplicaba, ya que no pasaba por los tres rotores, sino que lo hacía dos veces por cada uno. Era un elemento necesario para que la máquina fuera capaz de cifrar y descifrar de manera sencilla, es decir, para que el camino de doble dirección funcionara.

El reflector añadía complejidad y seguridad a la máquina, pero también tenía un efecto que, si bien en principio parecía no tener demasiada importancia, lo cierto es que resultó clave para que la máquina Enigma acabara siendo rota. Una letra en el texto en claro nunca podría cifrarse como ella misma, es decir, la A nunca podría resultar en la A tras el cifrado. Además de esta restricción y algunos otros detalles de la máquina, los procedimientos de uso impuestos a los operadores por los responsables, también crearon condiciones que eliminaban aleatoriedad en la máquina y por lo tanto creaban pequeñas grietas por las que atacar el cifrado. Por ejemplo, en el clavijero no se podía conectar una letra con la letra inmediatamente anterior o posterior, o un rotor no podía estar durante dos días consecutivos en el mismo hueco de la máquina. Como veremos, hubo un momento en el que, por seguridad, se comenzó a enviar cada mensaje con su propia configuración de los rotores y el resultado de esa decisión fue crítico para que los criptoanalistas tuvieran éxito.

Por otra parte, las malas costumbres de los operadores y la falta de conciencia sobre la relevancia de sus mensajes, fueron otro de los elementos que debilitaron la seguridad de Enigma. Una vez más, el factor humano como punto débil.

Como hemos visto, es esencial que la configuración de la máquina fuera exactamente la misma en el emisor y en el receptor antes de comenzar la comunicación. Cualquier cambio o diferencia, por mínimo que fuese, alteraba el resultado de tal manera que era imposible el descifrado del mensaje. Para ello, todas las unidades con una máquina Enigma tenían una hoja impresa que se entregaba por un canal seguro, que marcaba la configuración exacta de la máquina para cada día del mes. Esto es, los rotores que debían colocarse en la máquina, el orden de los mismos, su posición inicial y, por supuesto, las conexiones de los cables del clavijero.

Así, todos los mensajes de un día usaban la misma configuración, que cambiaba cada medianoche. Esto es muy importante, ya que cuando los aliados lograban conocer la configuración de las máquinas y por lo

tanto descifrar los mensajes de los alemanes, ese conocimiento tan solo era válido para veinticuatro horas. Si se descubría unas horas o unos días más tarde, únicamente serviría para descifrar mensajes pasados y en muchos casos ya con información caducada. Dicho de otro modo, el combate contra la máquina Enigma empezaba de cero cada día a las doce de la noche.

Las hojas de especificaciones de configuración de la máquina para cada día del mes, como es lógico, eran uno de los elementos más secretos y más protegidos por parte de los alemanes. Si ese paquete de información con la configuración para todo un mes caía en manos enemigas, la máquina Enigma perdía su seguridad, ya que los aliados tan solo tendrían que tomar un mensaje cualquiera capturado, ver el día, configurar la máquina y leer el mensaje. Una muestra clara de la importancia de estos papeles es que los que usaba la Kriegsmarine, la marina alemana, estaban impresos con tinta soluble, de tal forma que, en caso de peligro, tan solo tenían que arrojar los documentos al agua para que todo lo impreso se borrara al diluirse la tinta.

Como ya hemos dicho, este es el funcionamiento básico de una máquina Enigma estándar, pero durante la Segunda Guerra Mundial hubo diferentes versiones de Enigma, con algunos cambios. Por ejemplo, había Enigma con cuatro rotores. De igual forma, hubo también distintos procedimientos para usar las máquinas. La marina alemana, que fue quizás la unidad que usó las máquinas Enigma con más cuidado y precauciones, en parte por su dependencia de ella para las comunicaciones seguras, enviaba antes de cada mensaje cifrado con Enigma la configuración de los rotores, su posición inicial, usando otro sistema de comunicación distinto.

Rudolph Schmidt fue un general de la Wehrmacht, laureado con la Cruz de Hierro con Hojas de Roble y que mandó el Segundo Ejército Panzer en el frente del este. Había combatido en el ejército imperial alemán durante la Primera Guerra Mundial y, a pesar de la purga tras la derrota en la guerra, pudo mantener su vida como militar, ascendiendo durante los años veinte y treinta. Su hermano Hans-Thilo no tuvo la misma suerte tras la Primera Guerra Mundial, en la que también había participado, y fue expulsado del ejército. Se puso entonces al frente de una fábrica de jabón, tratando de crearse un hueco en el mundo de los negocios, pero no le fue mucho mejor y la crisis económica que estranguló a Alemania en los años veinte enterró su negocio, dejándolo en una situación muy precaria, algo que, por otra parte, le estaba sucediendo a gran parte de la sociedad de aquella República de Weimar.

Hans-Thilo se vio obligado a pedir ayuda a su hermano, que no solo había cumplido el deseo de ser militar, algo que a él le había sido negado, sino que disponía de una posición mucho más solvente que la suya y con la suficiente influencia como para conseguirle un puesto de trabajo que le ayudara a seguir adelante. Rudolph era el jefe de personal del Cuerpo de Señales del ejército alemán, por lo que encontró un hueco sin problema en los organismos que él controlaba. De hecho,

Rudolph tuvo mucho que ver en la adopción de la máquina Enigma por el ejército alemán. El empleo que consiguió para su hermano Hans-Thilo estaba en la Chiffrierstelle, la oficina responsable de las comunicaciones cifradas alemanas. Un lugar donde se manejaban secretos, por donde se movía información sensible y donde la discreción y la confianza eran valores más importantes que la propia capacidad de trabajo. Por ello, quizás parezca lógico que uno crea que su hermano, en quien confía, es un buen candidato. Hans-Thilo, que estaba casado, se instaló solo en Berlín, donde estaba la Chiffrierstelle, dejando al resto de su familia en Baviera, donde el coste de la vida era más asumible.

Rudolph no pensó que la situación de precariedad de su hermano y el hecho de que hubiera sido rechazado por el ejército de su país unos pocos años antes podrían llevar a Hans-Thilo a traicionar a uno y a otro, a su país y a su propio hermano, del que probablemente tenía envidia. Hans-Thilo Schmidt estaba en el lugar y en el momento apropiados para solucionar sus problemas económicos y para cobrarse la venganza contra su patria. Tenía acceso a secretos alemanes y lo sabía, y también sabía que esos secretos valían dinero.

El 8 de noviembre de 1931 Hans-Thilo Schmidt se citó en un hotel de Verviers, en Bélgica, con un agente secreto francés cuyo nombre en clave era Rex. Hans-Thilo había llevado hasta allí dos documentos que había distraído de su oficina. Eran las instrucciones para utilizar la máquina Enigma, que permitiría a los franceses conocer en detalle cómo era usada por los alemanes. A cambio de dejar a Rex fotografiar aquellos documentos, Schmidt consiguió 10.000 marcos de la época, una cantidad más que importante. Se convertía así en Asché para los franceses, ya que este fue el nombre en clave que asignaron a Schmidt como agente. Se iniciaban así años de vida como espía, traicionando a Alemania. Años en los que el nazismo se haría con el poder y cambiaría su país y la propia Europa.

Aunque lo que habían conseguido los franceses era un gran paso para conocer las capacidades criptográficas de las que disponía Alemania y cómo planteaba el uso de sus máquinas, lo cierto es que tan solo con aquella información no se podía descifrar un mensaje cifrado con una Enigma. Para hacerlo era necesario conocer la configuración inicial de la máquina antes de comenzar el cifrado, y eso no podía saberse tan solo con tener una máquina y su forma de uso. De hecho, en documentos alemanes de la época se constata que estos dan por hecho que los enemigos tienen a su disposición máquinas Enigma como las suyas, sobre las que son capaces de trabajar y probar métodos para tratar de romper sus mensajes secretos. El número de posibles configuraciones iniciales de la máquina es tan elevado, que asumían que aquello no suponía un problema de seguridad.

Lo que había conseguido el agente Rex de Schmidt era algo muy relevante, pero el Bureau de Chiffre francés no sacó mucho partido de ello. De igual forma que los alemanes sabían que la variedad de configuraciones mantenía los mensajes cifrados por Enigma a salvo, los

franceses se daban por vencidos antes siquiera de comenzar. El sentido común y el conocimiento que tenían en el momento frenaban cualquier intento de atacar Enigma.

Los franceses tenían una conexión con el corazón de la oficina criptográfica de Alemania a través de Hans-Thilo Schmidt, pero no sabían muy bien cómo sacarle partido a la información que conseguían. Tenían otra conexión internacional, de un tipo totalmente diferente, con otro país europeo, con Polonia. Desde comienzos de los años veinte existía un acuerdo de cooperación militar entre Francia y Polonia, y dado que los polacos ya se habían mostrado interesados en cualquier información o descubrimiento que tuviera que ver con las capacidades criptográficas alemanas y, por lo tanto con la máquina Enigma, se abrió un flujo de información. Los documentos fotografiados gracias a Schmidt acabaron en poder del Biuro Szyfrów, la oficina de cifrado polaca. Sus problemas frente a Enigma, así como la información, eran los mismos que tenían los franceses, pero en Polonia decidieron investigar en profundidad cualquier posibilidad que los llevara a conseguir la clave de un mensaje oculto con Enigma, y por lo tanto a su descifrado.

Entre los manuales de uso que Schmidt había entregado estaba la descripción de los libros de códigos que indicaban la configuración específica de la máquina para cada día, algo así como la clave que permitía que la máquina cifrara de un determinado modo. Esto es importante, ya que la clave que usaba el emisor tenía que ser la que usaba el receptor para descifrar el mensaje, por lo que estos libros eran parte esencial del uso de Enigma. La descripción de configuración de la máquina indicaba las posiciones de los rotores y las conexiones en el clavijero. Cualquier cambio en esa configuración hacía que el resultado fuera totalmente distinto al cifrar, o que el descifrado fuera imposible.

Según parece, la motivación material del traidor alemán era más importante que el interés de venganza o el resentimiento. Probablemente, lo que deseaba Hans-Thilo Schmidt era el dinero, y la falta de patriotismo o amor por su país hizo que no tuviera reparos en aprovecharse de su situación. Según el capitán Gustave Bertrand, uno de los miembros del equipo de criptógrafos franceses de la época y el hombre que aceptó en última instancia la oferta de Schmidt de pasar información, era un *playboy* y el dinero que provenía de su traición le permitía vivir de un modo que nunca hubiera podido disfrutar con el sueldo de funcionario. Gustave Bertrand, por cierto, fue el hombre que sirvió de valedor a Camazón, el criptógrafo español, para que dejara el campo de concentración y se integrara en la criptografía francesa.

Durante los siete años que duró su relación con Francia, al espía alemán también le consiguieron mujeres. De nuevo, mujeres que no habría podido conseguir con su vida de funcionario en Berlín, y que disfrutaba en sus viajes por algunas capitales europeas. A cambio, más de 300 documentos secretos salieron directamente del corazón de la oficina de cifrado alemana, con destino a los que más tarde serían sus

enemigos en la guerra. Llegaron en primera instancia a Francia, pero pronto viajaban hasta Polonia e incluso acabaron en las mesas de trabajo británicas. Entre ese caudal de documentos había, además de fotos de las máquinas, instrucciones de uso, textos en claro y su equivalente cifrado, junto con la configuración que se había utilizado en la máquina para el cifrado.

Hans-Thilo Schmidt no se limitó a pasar información sobre criptografía, sino que, con el paso del tiempo, además de ello, que ya era casi una rutina, comenzó a informar a Francia también de otro tipo de detalles, como los planes de rearme nazis o incluso las intenciones que tenían con respecto a Europa. Schmidt se ganó un puesto en el Forschungsamt (FA), o la Oficina de Investigación de la Luftwaffe, el ejército del aire alemán, poco después de que esta fuera creada en abril de 1933. Este organismo se ocupaba de la captura de señales y la criptografía, además de la formación de todo lo relacionado con ello. Desde allí Schmidt amplió el rango de información y el campo de documentos a los que podía llegar, y el dinero francés se encargó de que todo esto siguiera siendo entregado por el traidor Asché. Desde su posición informó de que los nazis no solo controlaban el correo y las llamadas telefónicas internas del país, sino que habían puesto en funcionamiento un campo en Dachau para llevar allí a sus oponentes. Más valioso fue, sin embargo, el aviso de que las llamadas, tanto entrantes como salientes, de la embajada de Francia en Berlín estaban siendo escuchadas y que el código diplomático francés había sido roto. De hecho, es muy probable que la falta de cuidado de Francia con respecto a sus códigos diplomáticos, a pesar del aviso, hiciera que la FA, Oficina de Investigación de la Luftwaffe, acabara descubriendo a Schmidt. En un mensaje capturado por la FA y enviado a la embajada francesa, se especificaba información que había proporcionado el alemán, y dado que el código usado por los franceses no era seguro, en unas pocas horas Hermann Göring, máximo responsable de la Luftwaffe, tenía un informe al respecto a su disposición. Esto ponía en riesgo a Schmidt, ya que la FA comenzaba a ser consciente de una posible fuga de información entre su personal. La FA era capaz de descifrar los mensajes diplomáticos también de los británicos y los estadounidenses, que, por otra parte, en ocasiones pecaban de falta de seriedad a la hora de mantener seguras sus comunicaciones. Estas advertencias habían sido puestas en conocimiento de Francia por Schmidt.

En marzo 1940, con la guerra ya en marcha, el espía alemán seguía siendo una fuente de información desde el mismo centro del nazismo. Avisó de las intenciones alemanas de lanzar un ataque a través de las Ardenas, un combate en el que su hermano Rudolph comandaría el 39.º Cuerpo Panzer. Con la ocupación de Francia llegó el fin de Schmidt. Cuando su agente francés de contacto, Rex, fue capturado por la Gestapo, desveló el nombre de algunos de sus colaboradores, con el objetivo de salvar su propia vida. Lo consiguió, pero a cambio Hans-Thilo Schmidt fue detenido a finales de marzo de 1943 y acusado de espionaje. En septiembre de ese mismo año murió, aunque no se sabe con certeza si fue ejecutado o si se suicidó. Acababa así la vida de Asché, cuya traición a Alemania fue importante, si no clave, para que

arrancara uno de los caminos que llevaría a la victoria aliada, un camino de los muchos que confluyeron en aquel destino final. Ese camino fue la ruptura de Enigma y por lo tanto el conocimiento aliado del contenido de muchas de las comunicaciones de su enemigo.

Hans-Thilo Schmidt también complicó la vida de su hermano. Este había tomado parte en la invasión de Polonia en 1939 y, como hemos dicho, comandó el 39.º Cuerpo Panzer en la conquista occidental de la primavera de 1940. En junio de ese año se colgó al cuello la Cruz de Caballero de la Cruz de Hierro y fue promocionado. Disfrutó de varios años de éxito militar, llegando a ser el sustituto de Guderian al mando del Segundo Ejército Panzer desde 1941. Cuando su hermano fue capturado en 1943, encontraron varias cartas de Rudolph en las que criticaba al Führer y le culpaba de algunos de los problemas en el campo de batalla. El 10 de abril de 1943 fue relevado de sus cargos en el ejército y comenzó un proceso contra él. Consiguió salir del trance sin pasar por un consejo de guerra, gracias a sus amistades dentro del ejército y al reconocimiento que disfrutaba en su seno. Se alegó que estaba enajenado cuando escribió aquellas cartas y acabó en un centro de internamiento para enfermos mentales. No volvió nunca al ejército, aunque intentó su readmisión, y tras la guerra fue detenido por los rusos y enviado a un campo de prisioneros, donde estuvo hasta septiembre de 1955. Murió dos años después.

Como decíamos, los británicos también tuvieron acceso a lo que iban consiguiendo los franceses, aunque mucho tiempo después que los polacos. Esa información se envió a Reino Unido en unas carpetas rojas, por lo que la fuente de los documentos era conocida como Pimpinela Escarlata. Aunque provenía de Francia, los británicos sospechaban que sus vecinos al otro lado del Canal de la Mancha no estaban trabajando solos. Llegaron a esta conclusión cuando vieron que algunos de los documentos con información de la fuerza aérea alemana no podían haber sido conseguidos en el oeste, sino en el este. La captura del tráfico de comunicaciones había ocurrido necesariamente demasiado lejos para que estuviera bajo el control francés, por lo que todo hacía sospechar que había alguien escuchando las comunicaciones del Reich en el este. Esa sospecha acabó creando el triángulo de colaboración contra Enigma que formaron Francia, Polonia y Reino Unido.

20. Los criptoanalistas polacos contra Enigma

Al acabar la Primera Guerra Mundial, como bien sabemos, la Sala 40 británica no paró sus trabajos de criptoanálisis y a pesar del armisticio y de que los tiempos habían cambiado, el mundo del espionaje siguió activo y los alemanes eran uno de los objetivos prioritarios. Su situación privilegiada cambió en 1926, cuando interceptaron un mensaje cifrado con un método totalmente nuevo y, a todas luces, invulnerable. Acababan de hacerse por primera vez con un mensaje encriptado por una máquina Enigma. Con el paso de los meses, estas máquinas fueron alcanzando a todas las entidades alemanas y al mismo ritmo la Sala 40 se fue quedando poco a poco a oscuras: no podía descifrar aquellos mensajes y por lo tanto la inteligencia británica perdió una de sus bazas más importantes. El enemigo principal de la última guerra y uno de los países a vigilar más de cerca, Alemania, podía comunicarse de manera segura. De nuevo el péndulo de la historia de la criptografía cambiaba de lado y ahora eran los creadores de códigos los que tenían la ventaja de su lado, dejando a los criptoanalistas en un callejón sin salida. No solo los británicos se mostraban incapaces de atacar los cifrados de Enigma, sino que igual de incapaces eran los franceses y los estadounidenses.

La situación alemana tras las condiciones del Tratado de Versalles, firmado en junio de 1919, transmitía cierta tranquilidad a los que habían sido los países del bando aliado de la Primera Guerra Mundial. Sobre el papel, Alemania estaba obligada a pagar importantes cantidades de dinero y tenía prohibido desarrollar muchas iniciativas militares, desde fabricar material de guerra hasta hacer crecer su ejército por encima de los 100.000 hombres, algo más si incluimos los oficiales, pero sin disponer de artillería pesada o del arma submarina. Esta inocente tranquilidad hizo que no se considerase crítica la nueva situación con respecto a las comunicaciones cifradas alemanas y que no se invirtiera tiempo ni recursos de manera excepcional para atacar a Enigma. Es más, a la sombra de la paz y del Tratado de Versalles, los recursos dedicados a la criptografía en los países aliados cayeron.

Polonia, en cambio, no estaba en una situación tan apacible como otros lugares en Europa. En 1918 había recobrado su independencia como país, después de casi un siglo y cuarto de ocupación, pero las tensiones no habían desaparecido en muchos de sus territorios. Con varios conflictos armados en los primeros años de su nueva existencia, y con el monstruo soviético al acecho, todos los esfuerzos militares polacos eran pocos, incluyendo los relacionados con la criptografía. Entre febrero de 1919, tres meses después de finalizar la Primera Guerra Mundial, y marzo de 1921, soviéticos y polacos combatieron en una guerra por mover sus fronteras, cada cual buscando sus intereses. Alemania también era una amenaza en potencia, atada por las correas del Tratado de Versalles, pero sin duda peligrosa. Polonia, consciente de

que se encontraba entre dos países que la miraban con deseo, cerró una alianza con Francia como parte de los ocho Acuerdos de Locarno, firmados en 1925. Estos acuerdos entre varios países, entre los que estaban Francia, Alemania, Reino Unido, Italia y Polonia, recogían garantías entre unos y otros, establecían fronteras y, como decíamos, marcaban una alianza militar entre Francia y Polonia. Además, unos años más tarde, en 1932, los soviéticos y los polacos firmaron un pacto de no agresión. Este tipo de acuerdo se repitió también con Alemania en 1934. Nadando y guardando la ropa, actuando por tanto con inteligencia y precaución, Polonia no abandonó sus labores de inteligencia.

En mayo de 1919, durante la guerra polaco-soviética a la que hacíamos referencia, Polonia creó la Oficina de Cifrado, que ya demostró su importante valor en aquel conflicto. En agosto de 1919, cuando los soviéticos estaban muy cerca de alcanzar Varsovia, la Oficina de Cifrado fue capaz de poner en claro centenares de mensajes enemigos, hasta 410, ayudando a que la situación diera un vuelco inesperado y permitiera a los polacos salir con éxito del trance. Al comenzar la década de los años treinta, varias entidades similares dedicadas a la criptografía estaban funcionando en diferentes partes del ejército y la inteligencia polaca. En diciembre de 1932 se creó una Oficina de Cifrado Central, el Biuro Szyfrów en idioma polaco, para aglutinar todos los esfuerzos y conocimientos. Sus responsabilidades eran tanto la criptografía, es decir, la generación de nuevas cifras y los métodos de encriptación, como la criptología, el estudio de las cifras, principalmente para romper los métodos de cifrado enemigos.

Como responsable de la Oficina de Cifrado fue designado el capitán Maksymilian Ciężki, nacido en 1898 y destinado en principio a continuar con el trabajo como agricultor que tenía su padre, pero la Primera Guerra Mundial se cruzó en su camino. Luchó en el bando alemán en el frente occidental, donde comenzó a entrar en contacto con las unidades dedicadas a las comunicaciones. Después de diferentes servicios, de periodos de formación y de emprender acciones clandestinas a favor de su país, Polonia, en 1923 entró en la inteligencia del Estado Mayor, en la Segunda División, donde su objetivo fundamental era todo lo relacionado con Alemania. Con él al mando, la oficina ocupada de vigilar a Alemania cayó en la cuenta, como había hecho la Sala 40 británica, de que los alemanes habían alcanzado un nuevo nivel en sus comunicaciones que hacía imposible su trabajo de criptología. Era el mes de julio de 1928. La confirmación de que los alemanes estaban usando máquinas Enigma les llegó ese mismo año, cuando desde Alemania se envió un paquete a Polonia y este acabó en la aduana, donde se inspeccionó rápidamente antes de ser devuelto. El contenido era una máquina Enigma.

El grupo de Ciężki también tenía acceso a la versión comercial de la máquina Enigma: tan solo tenían que comprarla, y eso hicieron, usando un comprador y una dirección falsos para que la empresa alemana no supiera que estaba entregando una de sus máquinas a los criptógrafos

del ejército polaco. Dedicaron importantes esfuerzos al estudio de la máquina, sabiendo que esa versión comercial era diferente de la que usaba el ejército alemán. Para llevar a cabo parte de estos esfuerzos, el ejército polaco se dirigió a la Universidad de Poznan, y en enero de 1929 reclutaron a alumnos de los últimos cursos de matemáticas. Conscientes de la importancia del idioma en la criptografía, sabían que, en la Universidad de Poznan, por su localización, muchos de los estudiantes habían asistido a escuelas donde el alemán era habitual. Finalmente, dos alumnos fueron seleccionados para la oficina de cifrado polaca, Jerzy Rozycki y Henryk Zygalski. Un tercer estudiante, Marian Rejewski, había destacado en el curso de criptografía y en las pruebas de selección que se habían llevado a cabo, pero había abandonado Poznan temporalmente. Al año siguiente, en 1930, Rejewski se unió a sus compañeros para trabajar sobre los mensajes cifrados alemanes que se interceptaban. Todavía lo hacían desde Poznan, pero en septiembre de 1932 acabaron sus estudios y se trasladaron a Varsovia. En esos cuatro años, desde que en julio de 1928 se dieran cuenta de que se enfrentaban a Enigma, los polacos no habían hecho avances significativos contra la máquina militar alemana.

Marian Rejewski, trabajando solo, en el transcurso de unas pocas semanas a finales de 1932 consiguió algo que no se sabía hacer en los años anteriores y algo que Alemania no esperaba que fuera posible. Ni Alemania ni el resto de países que sabían a qué tipo de máquina se estaban enfrentando. Rejewski tenía dos cosas a su favor, una máquina real sobre la que trabajar y una buena cantidad de tráfico cifrado capturado. Además, conocía lo que Hans-Thilo Schmidt les había entregado a los franceses. Sabía que el procedimiento de uso de los alemanes indicaba que las primeras seis letras de cada mensaje cumplían una función especial, señalar parte de la configuración de la máquina usada para cifrar dichos mensajes en particular. El libro de configuraciones diario establecía el orden de los rotores, sus posiciones y el resto de elementos necesarios para establecer la configuración básica de la máquina. Con esta configuración en la máquina, el operador cifraba la posición de los rotores que iba a usar para cifrar el mensaje. Escribía estas posiciones dos veces, indicando qué número o letras debían quedar en la parte superior de los rotores, y cifraba esa secuencia. A continuación, movía los rotores hasta esas posiciones y cifraba el resto del mensaje.

Esas primeras letras cifradas con la configuración básica del día fueron el punto de partida para que Rejewski diera con una solución. Rejewski había sido capaz de crear un modelo matemático para representar el funcionamiento de la máquina, y con la ayuda de la información proveniente de Hans-Tilo Schmidt, que describía los procedimientos e incluía configuraciones usadas, estaba en disposición de avanzar con seguridad. Partiendo de esa base, el criptógrafo polaco tardó un poco más de tiempo en dar con el cableado de todos los rotores, pero su empeño finalmente tuvo éxito. El siguiente objetivo, una vez que se había diseñado un procedimiento que permitía conocer la configuración de una máquina a partir de mensajes cifrados, era conseguir una forma de aplicar ese procedimiento con la suficiente eficacia como para obtener

las claves diarias. En palabras del propio Rejewski, con lo que ya sabían sobre Enigma tan solo tenían que construir la máquina para poder romper del todo los mensajes alemanes. Es más, durante un tiempo habían conseguido leer los mensajes alemanes, ya que las configuraciones no se cambiaban a diario y la información de Schmidt era duradera, pero a medida que la guerra se acercó, los nuevos procedimientos de uso de Enigma se hicieron más estrictos y esa capacidad se disolvió.

La búsqueda de patrones en los mensajes, que indicaban la configuración en la que se debía disponer la máquina, era la base del método, pero había que encontrar el patrón válido entre más de 100.000 posibilidades, y hacerlo además en un tiempo razonable. Henryk Zygalski tuvo la ingeniosa idea de emplear hojas perforadas y tabuladas, que servían para buscar los patrones válidos, es decir, contenían una secuencia de letras que podían identificar las configuraciones válidas. Las hojas perforadas contenían las posibles combinaciones de orden de los rotores y los cifrados de Enigma de determinados patrones o secuencias habituales. Al colocar esas hojas sobre una mesa de luz, aquellos casos en los que coincidían los agujeros en las hojas perforadas dejaban pasar la luz y se revelaban los posibles casos de configuración válida de la máquina. La generación de las hojas era un trabajo que requería paciencia, detalle y atención, siendo terriblemente repetitivo para hacerlo manualmente. Durante algún tiempo estuvieron obteniendo las configuraciones de Enigma de manera manual, utilizando la réplica que habían construido. En ocasiones acababan con los dedos sangrando, a base de probar de manera sistemática posibilidades y posibilidades en la máquina.

Los tres matemáticos y criptógrafos polacos, con alguna ayuda, crearon un dispositivo electromecánico que automatizaba la búsqueda de la configuración exacta. El ingenio diseñado era básicamente una máquina Enigma doble, con seis rotores, que podía comprobar de manera automática miles de posibilidades en el tiempo en el que una persona podía apenas comprobar un caso. La idea era similar a la de las hojas perforadas de Zygalski, probar combinaciones de las posiciones de los rotores y secuencias de los mensajes, hasta dar con una combinación que generaba el texto en claro de los mensajes. A este dispositivo los polacos le dieron el original nombre de Bomba, exactamente así, como la palabra del español. El nombre probablemente se debiera al sonido de tictac que hacía la máquina, que recordaba al del temporizador de una bomba. Al encontrar una posible solución, la máquina emitía un sonido, para alertar al operador. Los franceses la llamaban Bombe y, como veremos, los británicos continuaron con ese nombre en sus dispositivos contra Enigma. Los polacos construyeron seis de esas máquinas y con toda su infraestructura puesta al máximo rendimiento, en unas pocas horas eran capaces de encontrar la solución y tener la configuración de cifrado de los mensajes y por lo tanto el contenido de estos.

Durante cinco años el flujo de mensajes cifrados capturados fue leído sin problemas por los polacos. En ese tiempo los alemanes introdujeron algunos cambios en los procedimientos que suponían piedras en el camino para las capacidades y herramientas que Rejewski y sus compañeros habían creado, aunque ninguna de esas piedras fue una barrera definitiva. Los cambios diarios en los rotores supusieron un mayor trabajo y el nuevo reflector introducido en noviembre de 1937 requirió un esfuerzo extra.

En septiembre de 1938 el procedimiento de configuración diario de la máquina fue modificado. Para no repetir la misma configuración durante todo el tráfico de cada día, el operador decidía la posición de los rotores, y la enviaba codificada dentro del propio mensaje. El libro de configuraciones diario que se distribuía a cada operador seguía indicando los rotores que había que colocar en la máquina, su orden y las conexiones del clavijero. Pero la letra que había de mostrar cada rotor en su parte superior se convirtió en algo variable. Tal configuración del rotor se cifraba y se enviaba dentro del mensaje. Este pequeño cambio sí que hizo que los criptógrafos polacos quedaran bloqueados e incapaces de descifrar Enigma.

Por si esto fuera poco, en diciembre de 1938 las Enigma usadas por el ejército alemán fueron dotadas de dos rotores adicionales, con cableados desconocidos por los polacos. Las posibilidades de configuración, como bien sabemos, se multiplicaron y se cambiaban a diario. Con tres rotores, las combinaciones en el orden de los rotores eran seis (123,132, 213, 231, 312, y 321) y por lo tanto las seis bombas eran dotación suficiente para probar cada configuración inicial. Ahora, con cinco rotores, las posibles combinaciones en el orden de los rotores eran 60, y el equipo polaco no tenía recursos ni tiempo para afrontar la construcción de 60 bombas. Por lo tanto, las seis bombas polacas dejaron de cumplir su función. Tan solo quedaban a su alcance los mensajes que seguían enviándose en algunos casos y algunas unidades usando los procedimientos anteriores.

En junio de 1939 se intensificaron los rumores sobre Polonia lanzados por la propaganda alemana. El 30 de junio, previendo una crisis importante, Gwido Langer, el responsable del Biuro Szyfrów, envió una frase acordada anteriormente para contactar con los franceses y los británicos. La frase era «hay algo nuevo» y poco después en Varsovia se reunieron especialistas en cifrado de los tres países. El jefe del Estado Mayor polaco había dado permiso para compartir la información más clasificada en torno a la criptografía con Francia e Inglaterra.

Se habían reunido seis meses antes en París, y Dillwyn Knox, uno de los hombres que llevaba en la Sala 40 desde la Gran Guerra, expuso que, sin conocer el cableado interno de los rotores, era imposible descifrar los textos alemanes de las máquinas Enigma capturados. Los polacos habían hecho avances muy importantes, pero en enero consideraron que todavía no era el momento de poner la información en común. En junio la situación había empeorado y la decisión era otra. Cuando les

enseñaron la máquina Enigma sobre la que habían estado trabajando y las modificaciones que le habían hecho para poder descifrar los mensajes, los británicos y franceses supieron que estaban ante un avance importante. Denniston pidió permiso para hacer venir de la embajada británica a un dibujante, con el objetivo de que documentara cómo era la máquina para poder reproducirla. Langer le respondió que no haría falta, que se habían ocupado de hacer dos réplicas, una para los franceses y otra para los británicos.

Desde 1933 los polacos estaban descifrando los mensajes alemanes de Enigma, aunque ya no era efectivo su método y no fue suficiente su conocimiento una vez que la guerra avanzó. Se produjeron cambios en los procedimientos de uso de las máquinas, además de sustituir las propias máquinas, añadiendo elementos que las hacían más seguras. En cualquier caso, la aportación de su conocimiento y su experiencia era un paso de gigante para los franceses y los británicos, especialmente estos últimos. El país del este estaba en un callejón sin salida por varios motivos, pero había llegado a un punto a partir del cual podían continuar sus aliados del oeste.

Por ejemplo, Knox, que había empleado gran parte de su tiempo en conocer y tratar de desentrañar la máquina alemana, estaba desconcertado por un elemento de esta, un disco que había en la misma antes de los rotores, y que Knox suponía cableado como los propios rotores, uniendo las entradas y las salidas de manera aleatoria. Rejewski le mostró y demostró que ese disco no contribuía al cifrado, y que tan solo era un elemento de utilidad dentro de la máquina. Ese disco efectivamente conectaba entradas y salidas, como hacían los rotores, pero sin incorporar complejidad. Es decir, la A en la entrada conectaba directamente con la A en la salida, la B con la B y así sucesivamente en los 26 conectores.

En 1939 Rejewski y sus compañeros abandonaron Polonia y tras pasar por Rumanía y estar a punto de caer en manos enemigas, llegaron a Francia. Se integraron en el equipo de Gustave Bertrand en el centro de descifrado y captura de comunicaciones PC Bruno, cerca de París. Como ya hemos comentado, entre sus compañeros había varios españoles. En junio del año siguiente tuvieron que alejarse de París, pero siguieron sirviendo a los aliados en el ámbito criptográfico. Uno de los momentos más delicados para el secreto de la ruptura de la Enigma alemana por parte de los aliados durante toda la Segunda Guerra Mundial llegó precisamente durante la huida de los polacos y del propio Bertrand.

En noviembre de 1942, Langer, el que había sido responsable del Biuro Szyfrów polaco y que había seguido el mismo destino que el resto, vio que una camioneta con antenas estaba cerca del lugar donde ellos transmitían sus comunicaciones desde Francia a Londres. Había llegado el momento de huir, ya que los alemanes habían estrechado el círculo peligrosamente. Bertrand, el responsable francés, se quedó en Francia, pasando a la clandestinidad. En enero de 1944 fue arrestado en París y

la Abwehr, el espionaje alemán, le ofreció convertirse en agente doble. El francés aceptó la oferta, pero tan solo para preparar su huida a Inglaterra, donde se reuniría con su familia, a la que había enviado allí mucho tiempo atrás.

Los polacos, por su parte, se dividieron en grupos para salir de Francia y llegar a Inglaterra por distintos caminos. Algunos fueron camuflados en barcos pesqueros y viajaron a Gibraltar y al norte de África. Rozycki embarcó en uno de ellos, pero su nave naufragó durante una tormenta y él perdió la vida. Otros tomaron un camino diferente, y se dirigieron a España. Este fue el caso de Rejewski y Zygalski, que fueron traicionados por su guía y acabaron en Barcelona, en una prisión para refugiados franceses.

Entre los pocos contactos que se permitían a los presos con el exterior, estaba la Cruz Roja. Por suerte para los polacos, había compatriotas en esa Cruz Roja que cuidaban de los refugiados en España que huían de los nazis. Dado que el polaco era un idioma que los responsables españoles de la prisión no conocían, la Cruz Roja utilizaba las listas de nombres de presos para comunicar mensajes secretos con los presos. Mezclando nombres reales con otras palabras del idioma, los mensajes eran comunicados a los presos polacos sin que los guardas se enteraran:

Zygmunt Przybylski.

Komisja Przyjezdza (el significado real era Llegará una comisión).

Jutro Zestolicy (que en realidad es Jutro Ze stolicy, que significa mañana de la capital).

Bedzie Uwas (era Bedzie U Was, esto es, estará contigo).

Como vemos, los códigos y cifrados están donde menos se los espera y tienen formas innumerables. En resumen, los polacos recibieron ayuda, fueron cambiados de campo y debido a las presiones de los aliados, finalmente fueron liberados por el gobierno español. Viajaron a Portugal y finalmente a Inglaterra. Curiosamente, no se integraron en Bletchley Park, donde se estaba llevando a cabo la principal batalla contra la criptografía alemana y donde estaban Turing, Knox y otros personajes a los que habían ayudado en su cometido, sino que fueron destinados a atacar las cifras de las SS y las SD en una unidad de criptoanálisis secundaria.

Langer y Ciężki, los máximos responsables de la antigua unidad de criptografía polaca, no tuvieron tanta suerte. También fueron traicionados por sus guías, pero ellos acabaron capturados por la Gestapo en la frontera entre España y Francia. Fueron enviados a un campo de concentración en Checoslovaquia, y después de un tiempo los mandos del campo supieron de la importancia de aquellos dos prisioneros. En marzo de 1944, pocos meses antes del Día D, Langer fue

interrogado. La primera pregunta fue muy sencilla: «¿Ha sido usted un agente doble?». La segunda apuntaba de forma mucho más certera: «Usted fue responsable de Biuro Szyfrów polaco y continuó operando en Francia desde 1940, ¿hasta dónde llegaron en su capacidad de descifrar Enigma?».

Langer respondió que efectivamente habían sido capaces de leer los mensajes de Enigma en Polonia, antes de la guerra, pero que los cambios en los procedimientos alemanes puestos en funcionamiento en 1938 les dejaron ciegos. Langer, en una arriesgada apuesta, pidió que contrastaran aquello con Ciężki, quien era realmente el experto en criptoanálisis, les dijo. Por suerte para ambos, las historias coincidieron, quizás porque lo habían hablado en algún momento. Este fue uno de los trances que más comprometieron el secreto relativo a información descifrada alemana por parte de los aliados, a la ruptura de Enigma y a la capacidad de los aliados para conocer las comunicaciones secretas nazis. Como decíamos, quedaban pocas semanas para el Día D, y cualquier problema podría ser fatal y tener consecuencias inesperadas.

Los polacos dieron los primeros pasos en la ruptura de la máquina Enigma. Ellos fueron los primeros en leer de manera continua los cifrados del ejército y de la Luftwaffe, la fuerza aérea alemana, aunque no llegaron a romper usos más sofisticados de la máquina como el que hacía la marina. Compartieron su conocimiento con los británicos, siete años antes de que comenzara la guerra y durante el tiempo que pudieron, incluso con el conflicto ya en marcha. Cuando los nazis avanzaron en sus procedimientos y los métodos de la Bomba polaca dejaron de ser efectivos, los británicos habían avanzado lo suficiente como para seguir desentrañando los mensajes de Enigma, también los de la marina. En resumen, los británicos llegaron más lejos y desde luego las ideas que desarrollaron y cómo las implementaron cambiaron la guerra, pero el mérito de los polacos no puede ser ensombrecido en modo alguno. En este caso, más que en ningún otro, podríamos hablar de la idea de los que caminan a hombros de gigantes.

21. Bletchley Park

A medida que se avanzaba en los años treinta, C, el nombre con el que conoce al responsable máximo de la inteligencia británica, fue instando a Denniston a reforzar su personal con el tipo de personas adecuadas para su cometido. Esa costumbre de llamar C al Servicio Secreto de Inteligencia británico proviene de su primer director, *sir* Mansfield George Smith-Cumming, que solía firmar su correspondencia con esa letra C mayúscula escrita en tinta verde, proveniente de su apellido Cumming. Denniston buscó en las universidades los perfiles adecuados, entre los que había historiadores, expertos en cultura clásica, filólogos, matemáticos… Se unieron varios profesores universitarios, como, por ejemplo, Gordon Welchman, que se unió en septiembre y que era profesor de matemáticas en Cambridge. Había recibido una carta del propio Denniston, unos meses antes del comienzo de la guerra, preguntándole si llegado el momento estaría dispuesto a servir a su país.

El 1 de septiembre de 1939 las tropas alemanas atacaban la estación de radio de Gleiwitz, y así comenzaba la invasión de Polonia y, oficialmente, la Segunda Guerra Mundial. Dos días más tarde, Inglaterra y Francia declaraban la guerra a Alemania y el 4 de septiembre, tan solo un día después, Alan Turing se reunía con el equipo de criptógrafos británicos que dirigía Knox, ese equipo a donde llegaron también Welchman y John Jeffreys, otro profesor de Cambridge. Igual que Welchman, Turing había asistido el año anterior a un curso de formación del GC&CS, y estaba también entre los seleccionados para servir a su país, si así lo deseaba.

Alan Turing era hijo de un funcionario británico en India y su infancia no fue sencilla, en cierta medida por su propio carácter y por su capacidad e intereses, que le alejaban de lo que era un alumno típico. Desorganizado y algo caótico, se interesaba por cuestiones matemáticas más allá de los temas que formaban parte del temario que proponían sus profesores. Ese interés por aprender y profundizar en aquellas ideas que le atraían continuó durante el resto de sus estudios. En Cambridge, por ejemplo, los alumnos podían utilizar la biblioteca fuera del horario reglado, y el bibliotecario recordaba que era muy habitual encontrar a Turing allí, a deshoras, con aspecto descuidado y con un montón de libros abiertos. Como veremos, su contribución a la criptografía aliada en la Segunda Guerra Mundial fue clave, pero aun así esa no fue su mayor contribución a la historia, ya que sus ideas sobre computación fueron determinantes y en muchos sentidos abrieron el camino para lo que vendría después. Algunos de los conceptos que plasmó en sus escritos son esenciales en el mundo de la computación, del *software* y de la estructura de las computadoras, y también fue un pionero en la inteligencia artificial. Aún en la actualidad la máquina de Turing se sigue estudiando en las universidades para comprender la universalidad del *software* y de los algoritmos, y el test de Turing sigue estando en la

base conceptual de la inteligencia artificial. En 1952 fue condenado por su homosexualidad y se le obligó a un tratamiento hormonal. El resultado del mismo le afectó gravemente, tanto física como mentalmente y en junio de 1954 se suicidó. Entonces el secreto sobre todo lo que se había hecho en Bletchley Park estaba en vigor y el reconocimiento a su servicio a los aliados no llegaría hasta mucho más tarde. Afortunadamente hoy su figura es todo un símbolo y goza de ese gran reconocimiento. Sin duda, Alan Turing fue una de las personas más importantes del siglo XX.

El GC&CS crecía y cobraba importancia, y a finales de mayo de 1938 un semanario local de Buckinghamshire publicaba la noticia de que la mansión de Bletchley Park y sus más de 220.000 metros cuadrados de terreno habían sido adquiridos por alguien, con cierto secreto. Con toda probabilidad era un empleado del gobierno. Tan pronto como la compra fue efectuada, comenzaron a tenderse líneas telefónicas. El comprador era el almirante Hugh Sinclair, conocido como Quex Sinclair, que había sido director de la Inteligencia Naval británica y que desde 1923 era el director del SIS, del Servicio Secreto.

Una vez que se creó la infraestructura necesaria, en el propio Bletchley Park y alrededores, se pusieron en marcha distintas secciones de trabajo. La dedicada a la Enigma alemana estaba compuesta por Knox, Jeffreys, Welchman y Turing. Knox había mandado construir más réplicas de la máquina, a partir de la que le habían entregado los polacos y usando como base máquinas Tipex británicas, además de generar hojas perforadas sobre las que trabajar. Para hacer esto último, crearon un dispositivo que les ahorraba trabajo, lo aceleraba y además eliminaba errores.

El equipo de Knox partía de los conocimientos que habían llegado a través de Polonia y de su propio trabajo. Así, tomaron secuencias de letras comunes en los mensajes, como nombres de unidades, fechas, órdenes militares… y buscaron esas secuencias en los mensajes cifrados, es decir, textos de la misma longitud, y donde además ninguna de las letras de la palabra en el texto en claro coincidiera consigo misma en la posición dentro del texto cifrado. Ya sabemos que, debido al diseño de la Enigma, ninguna letra resultaba tras el cifrado en ella misma. Una A en el texto en claro nunca era una A en el cifrado. Esto no era gran cosa, pero les permitía trabajar en desentrañar la caja negra, en cierto sentido, que tenían entre sus manos. Gracias a que el tráfico de mensajes cifrados era considerable y que era capturado, el material que tenían para probar y estudiar era enorme. Turing descubrió otra característica interesante que permitía reducir el número de posibles configuraciones de la máquina a probar para dar con la configuración usada en un determinado mensaje. Se dio cuenta de que ciertos bucles en la equivalencia entre letras en claro y cifradas eran un camino más fácil para que las bombas británicas hicieran su trabajo.

No hay que olvidar que los últimos cambios antes de la guerra habían dejado en un callejón sin salida a los polacos, por lo que había que

repensar cómo atacar la Enigma, que en ese momento operaba con tres rotores de varios disponibles y con el clavijero de 10 conexiones. En resumen, la complejidad había aumentado significativamente. Turing ideó un dispositivo, al que llamaron Bombe, siguiendo de nuevo con la idea de Rejewski y sus compañeros, que tenía noventa rotores y que podía encontrar la configuración usada por las Enigma, buscando patrones en los mensajes, a través de un procedimiento de prueba y error que se aprovechaba de todos los detalles que Turing, Welchman y el resto de británicos habían ido averiguando. Algunas de estas averiguaciones permitían a la máquina ahorrar mucho tiempo al descartar caminos muertos una vez localizada una opción imposible. La Bombe, en cualquier caso, era un dispositivo en desarrollo y presentaba fallos y problemas. Welchman, que tenía una buena mente como ingeniero además de como matemático, fue capaz de encontrar la solución a algunos de esos problemas y de saber cómo implementar en la realidad algunas de las ideas que iban teniendo.

Los *bamburismos* de Turing, como acabaron llamando a esas pequeñas grietas por las que comenzaban a desentrañar las configuraciones, demostraron ser una idea que, aunque requería esfuerzo, llegaba a generar grandes resultados. Los llamaban así, bamburismos, por una fábrica de Banbury, una localidad al norte de Oxford, donde se producían las grandes láminas en las que se perforaban los agujeros para buscar los patrones válidos en los mensajes cifrados capturados, y así encontrar la configuración usada en la máquina.

Esto no ocurrió de la noche al día y los descifradores de Enigma se tuvieron que ganar la credibilidad suficiente como para que el ejército y el gobierno británico les dotaran de recursos para poder llevar a cabo sus ideas. Ese problema, unido a los de gestión del complejo, eran dos de los inconvenientes principales para su buen funcionamiento. La situación había empeorado de tal forma que Edward Travis, ayudante de Denniston, que era el responsable de GC&CS, se unió a Nigel de Gray, un veterano de la Sala 40 y un hombre con peso, para intentar cambiarla, comenzando por el propio Denniston. En 1941 Winston Churchill había visitado Bletchley Park y si bien ya conocía por algunas reuniones a Turing y Welchman, entre otros, el encuentro les dio confianza para redactar una carta dirigida al primer ministro. Este les había agradecido su trabajo y se había interesado por la labor y el bienestar del personal. Welchman aprovechó todo esto para poner las cosas en claro en la carta enviada a Churchill. Le contó que el trabajo se estaba retrasando, que habían intentado resolver la situación por los canales habituales, sin éxito, que la falta de personal hacía que los descifrados se retrasaran y, aunque no directamente, dejaba claro que Denniston quizás no era la persona adecuada para dirigir aquel monstruo, que debía funcionar como una máquina perfecta. El 21 de octubre de 1941 la carta le fue entregada en mano al primer ministro. Ese mismo día Churchill respondió de forma lacónica, escribiendo un mensaje en tinta roja sobre una hoja amarilla, pidiendo que se les diera con extrema prioridad todo lo que pidieran desde Bletchley Park y que le informaran de que se había hecho así. A esa hoja le pegó una

pegatina con el texto *Action this day* , que indicaba que debía procesarse su respuesta ese mismo día, sin demora.

Los resultados llegaron de inmediato, con más personal militar y civil destinado a Bletchley Park y con presupuesto asignado para que se encargaran más Bombes a la empresa British Tabulating Machine Company. En febrero de 1942, poco después de todo esto, Denniston fue relevado del mando del GC&CS, aunque se mantuvo como director adjunto, y el propio Edward Travis fue nombrado en su lugar.

Bletchley Park fue creciendo hasta convertirse en un complejo enorme, donde los procedimientos y las responsabilidades se fueron clarificando. Había distintos cobertizos o cabañas, *hut* en el idioma inglés, que, numerados, se centraban cada uno en una labor concreta. Así, el cobertizo 6, donde estaba Welchman, se centraba en los mensajes del Heer, el ejército de tierra alemán de la Wehrmacht, y la Luftwaffe, el ejército del aire. Los mensajes de este último se habían conseguido romper desde agosto de 1940, mucho antes de que las Bombe estuvieran en funcionamiento. Esto era de gran ayuda, pero no era más que una parte de la guerra. La Luftwaffe tenía una serie de procedimientos menos sofisticados y seguros que otras partes del ejército y fue fácil para Bletchley Park romper su cifrado y leer sus mensajes durante toda la guerra. En el cobertizo 8, donde estaba Alan Turing, el objetivo era el cifrado utilizado por la Kriegsmarine, la marina alemana. Estos eran lo más conscientes de la importancia de la seguridad y de la capacidad de la inteligencia de señales, comenzando por su máximo responsable, Karl Dönitz. Como veremos, la guerra en el mar uno fue de los puntos críticos de la contienda, donde además las comunicaciones, como es lógico, eran muy importantes. El éxito en este ámbito se mostró como un elemento esencial para el desarrollo de la guerra, especialmente para la conocida como batalla del Atlántico.

Toda la información que salía de Bletchley Park era agrupada bajo el nombre en clave de ULTRA, y todo lo revelado como ULTRA era del más alto secreto, por supuesto, para proteger las propias actividades de Bletchley Park, además de para poder aprovechar lo descubierto. ULTRA proviene de la etiqueta que se creó para marcar el nivel de confidencialidad de la información que salía de allí, que era aún más secreta que TOP-SECRET, era ULTRA-SECRET. Un ejemplo de las precauciones que se tomaron para proteger la información de ULTRA, es que en ocasiones se enviaban aviones de reconocimiento a determinadas zonas y se dejaban ver de forma clara ante el enemigo, a pesar del riesgo que esto suponía. De esta forma, aun cuando los aliados llevaran a cabo la acción gracias a la información proveniente de Bletchley Park, esperaban que los alemanes creyeran que aquel avión de reconocimiento que habían visto era la fuente de la información.

Esta labor de protección del secreto fue cada vez más complicada, entre otras cuestiones, porque cada vez tenía más éxito y porque el número de personas involucradas en las labores asociadas al descifrado de Enigma creció hasta cerca de los 10.000 individuos. Entre ellos, gran parte eran

mujeres, que después de la orden de Winston Churchill de atender todas las peticiones que provinieran del lugar, fueron enviadas allí desde las secciones femeninas de la marina y la fuerza aérea. Todos ellos firmaron documentos de confidencialidad y ni siquiera tenían permiso para contar a sus familias lo que hacían. Esta prohibición se prolongó hasta mucho después de la guerra, ya que los británicos trataron de mantener en secreto lo que habían hecho durante la Segunda Guerra Mundial, para poder seguir haciendo cosas similares en el nuevo contexto mundial que arrancó con la derrota de la Alemania nazi y de Japón. Algunos personajes importantes, pero sobre todo muchas personas anónimas, mantuvieron sus actividades criptográficas en secreto. Cuando este se levantó, sin duda muchos maridos, muchos hijos y toda una sociedad en general vieron con ojos distintos a esos hombres y mujeres anónimos que habían desarrollado una labor clave en la guerra. En 1943 el personal de Bletchley Park lo componían 3.800 empleados, que llegaron a 5.600 el año siguiente y hasta los 9.000 al acabar la guerra. El secreto sobre todas sus actividades no se levantó hasta mediados de los años setenta.

Con todo este personal, no es extraño que hubiera algunas fugas de información a pesar de los controles, el secreto y la estricta vigilancia. Entre los casos más llamativos, especialmente una vez finalizada la guerra, está el de John Cairncross, al que se llegó a relacionar más tarde con los cinco de Cambridge, el grupo de espías soviéticos en el que estaba Kim Philby. Cairncross era comunista, pero nunca había llegado a tener una afiliación directa a ningún partido ni a significarse públicamente. Desde 1937 trabajaba como informador de los rusos, y en 1942 entró a formar parte del cobertizo 3. En este lugar se traducían y analizaban los textos, una vez descifrados, capturados al ejército alemán. El agente ruso sacaba información del recinto oculta en sus pantalones y se la hacía llegar a los soviéticos. Lo cierto es que los rusos estaban recibiendo información ULTRA por canales oficiales, pero no deja de ser curioso saber que los responsables de Bletchley Park tuvieron reticencias en compartir información con los rusos en un primer momento, precisamente para que no descubrieran lo que estaban haciendo con la máquina Enigma, y que los rusos a su vez tuvieran información sobre el lugar, sus actividades y los resultados de estas, gracias a un agente que trabajaba en el mismo corazón de uno de los lugares más importantes de la inteligencia británica durante la Segunda Guerra Mundial.

No todos los hombres fueron anónimos después del paso del tiempo, y Turing es quizás el caso más destacado, pero también hubo mujeres entre la élite de criptoanalistas. Joan Clarke se unió en junio de 1940 al equipo del cobertizo 8. Estudiaba matemáticas en Cambridge, y allí fue donde Gordon Welchman descubrió su talento y la reclutó para Bletchley Park, a pesar de lo cual su trabajo inicial era más administrativo que criptográfico. Con un sueldo inferior al de sus compañeros masculinos e incluso inferior al de las mujeres que habían llegado de las secciones femeninas militares, acabó siendo un miembro más del equipo del cobertizo, que, probablemente, tuvo la labor más complicada de todas. Su contribución comenzó como lingüista en lugar

de como matemática, a pesar de no tener formación en lo primero y sí en lo segundo. Aunque en mucha de la bibliografía se hace referencia a ella por su breve relación sentimental con Turing, que en realidad como hemos dicho era homosexual, llegó a comprender las ideas de Turing sobre los bamburismos con detalle y a sacarle el máximo partido. No en vano, en 1944 fue nombrada directora adjunta del cobertizo 8.

En la primavera de 1942, en el cobertizo 6 comenzaron a descifrar algunos mensajes que hablaban de las poblaciones de los campos de concentración. En estos mensajes también se dejaban caer algunas ideas y palabras que claramente se estaban refiriendo a muertes. Tanto es así que, en octubre de 1942, el Ministerio de Asuntos Exteriores sugirió al GC&CS que se hiciera un archivo cuidadoso de todos los informes relacionados con aquellas actividades, para su uso en un futuro tribunal de crímenes de guerra. Sin embargo, llegado el momento de los juicios de Núremberg, la cantidad de pruebas ya acumuladas, que además eran mucho más directas y explícitas, llevaron a la inteligencia británica a mantener en secreto los mensajes que habían capturado y descifrado, para así proteger el secreto de Bletchley Park.

De igual forma que la información de Hans-Tilo Schmidt ayudó a los polacos, los británicos buscaron fuentes similares de información, y en ocasiones se encontraron con esta casi sin buscarla. Analizando lo que sabían y lo que podrían hacer, los hombres del cobertizo 8 aseguraron que, si pudieran conocer la configuración diaria de un mes completo, que era la información que se distribuía entre los operadores de Enigma, podrían dar un salto enorme en su trabajo y comenzar a recuperar por sí mismos esas configuraciones diarias. Todo tipo de ideas fueron puestas sobre la mesa para intentar cumplir con la petición de Turing y sus compañeros. Knox, por ejemplo, sugirió enviar a los alemanes un mensaje falso, haciéndose pasar por uno de ellos, y pedir que le transmitieran directamente la información. Esta idea se descartó, porque podría alertar a los alemanes sobre el tipo de trabajo que se estaba realizando en Bletchley Park.

Ian Fleming, el que más tarde sería el creador de James Bond, que entonces formaba parte de la Inteligencia Naval británica, planteó en septiembre de 1940 una acción digna de una película. Su propuesta comenzaba con un bombardero alemán que se debía conseguir o simular de forma convincente. Un grupo de cinco personas, digno de una misión así de arriesgada y con un buen dominio del alemán, al menos en algunos de sus miembros, deberían vestirse como alemanes y simular que habían tenido problemas, con vendas y sangre. El avión se lanzaría al Canal, como si fuera un accidente y haría una petición de SOS. Una vez rescatados por un barco alemán real, debían hacerse con el control del mismo, por supuesto por la fuerza, acabar con los que se encontraran a bordo, para que no quedaran testigos del hecho, y volver en un bote a puerto inglés, llevando consigo lo que pedía el cobertizo 8.

A pesar de lo arriesgado del plan, no se descartó y dado lo que había que ganar, se pidió a Ian Fleming que detallara el plan lo máximo que

fuese posible. Así lo hizo, indicando cuándo debía despegar el avión para aprovechar la cola de las incursiones alemanas sobre Inglaterra, específicamente cómo hacer que el avión pareciera con problemas para tener que amerizar… e incluso preparó una historia para hacerla pública si el plan fracasaba, que permitía no levantar sospechas en los alemanes en ese caso. Finalmente, en octubre, la operación Ruthless, como se había denominado el plan de Fleming, fue definitivamente cancelada.

Como ya hemos comentado, las Enigma que iban a bordo de barcos y submarinos debían ser hundidas ante cualquier riesgo de caer en manos enemigas y toda la documentación relacionada con ellas estaba impresa en tinta soluble para que los papeles quedaran en blanco si eran arrojados al agua, que era exactamente lo que tenían que hacer si veían que estaba todo perdido. Esto, por fortuna para los aliados, no siempre se cumplió.

Aun sin conocer el contenido de los mensajes que se intercambiaban los submarinos y los barcos alemanes, los británicos eran capaces de conocer la posición aproximada de los submarinos y sus concentraciones gracias a la captura de las señales. El 12 de febrero de 1940 el submarino *U-33* fue atacado por el *HMS Gleaner* británico, con la suerte de que, aunque los submarinos en labores de minado, como estaba el *U-33* en aquel momento, no debían llevar máquinas Enigma a bordo, en este caso sí la llevaba. El comandante alemán, Hans von Dresky, temía que, debido a la poca profundidad de las aguas de la costa británica en las que su nave se iba a hundir, los británicos pudieran bucear y llegar hasta ella. Por ello colocó explosivos antes de abandonar la nave y sacó los rotores de la máquina, distribuyéndolos entre sus oficiales. El objetivo era lanzarlos al agua en cuanto pudieran, pero no llegaron a hacerlo y los rotores cayeron en poder británico. Con este pequeño botín, y poniendo en marcha un inteligente juego en el que hacían a los alemanes emitir mensajes cuyo contenido los británicos intuían o hasta conocían, comenzaron el proceso de ruptura del sistema criptográfico alemán.

Sabiendo que los submarinos alemanes llevaban a bordo una de aquellas máquinas Enigma para enviar sus comunicaciones de forma segura, durante meses la Home Fleet, la parte de la Royal Navy que navega en aguas territoriales británicas, intentó hacerse con una de las máquinas aprovechando la captura de un submarino en el océano. Una vez hundidos no había nada que hacer, pero cabía la posibilidad de hacerse con una máquina y con los libros de códigos que portara el submarino si este era abordado antes de hundirse. Frente a este objetivo los alemanes intentaban hundir sus naves a toda prisa, tras abandonarlas, para evitar que su tecnología y conocimientos cayeran en manos enemigas y para proteger precisamente las máquinas Enigma y los libros de códigos. Hubo varios casos en los que los hombres arrojaron al mar los rotores de la máquina y los libros de códigos antes de ser capturados. Otras veces la balanza se inclinó al otro lado. En abril de 1940, una pequeña embarcación alemana que transportaba

munición al puerto de Narvik para la invasión de Noruega fue abordada por el destructor británico *HMS Griffin* . No cumplieron con las órdenes de destruir o hundir la máquina Enigma y su documentación, y todo fue a parar a manos británicas en Bletchley Park. Aquí hicieron buen uso de todo ello y en el cobertizo 8 consiguieron descifrar los mensajes de la marina alemana durante un tiempo.

El 7 de mayo de 1941 el *U-94* avistó y comenzó un ataque contra el convoy OB-318, y como ya era habitual, avisó de su posición y trayectoria para que acudieran otros submarinos. Dos días más tarde llegaba a la zona tras navegar cientos de kilómetros en superficie, ocultándose alguna vez de emergencia ante la presencia de aviones, el *U-110* de Fritz-Julius Lemp. Este, de familia militar, había nacido en 1913 en una colonia alemana en China y a aquellas alturas de la guerra ya llevaba en su cuello la Cruz de Caballero y había hundido casi 100.000 toneladas enemigas. Lo cierto es que sus grandes logros habían sido conseguidos con su anterior nave, el *U-30* , y las patrullas con el *U-110* no estaban marchando todo lo bien que debieran, teniendo en cuenta también que la guerra había evolucionado y cambiado y que la situación de los submarinos y las capacidades enemigas no eran las mismas. Tampoco la tripulación que acompañó a Lemp en el *U-30* estaba ahora con él, salvo algunos de los oficiales. A pesar de ello el nuevo submarino mantenía el mismo emblema en su torreta que ya había lucido el *U-30* , un cachorro de terrier, en homenaje al perro de Lemp.

Tras conversar con el *U-201* de Adalbert Schnee, el *U-110* y este acordaron cómo hacer el ataque. En torno al mediodía del 9 de mayo, el *U-110* atacó y hundió dos mercantes del convoy, lo que provocó que la escolta del mismo comenzara su labor de rastreo y combate contra el submarino y que este tuviera que hacer una inmersión de emergencia para ocultarse e intentar escapar. El hidrófono de la fragata *HMS Aubretia* había detectado los torpedos y tras variar su posición avistó el periscopio del *U-110* , comenzando el ataque con cargas de profundidad. Configuradas para que explotaran entre los 30 y los 80 metros de profundidad, las explosiones resultaron efectivas y los daños en el interior del *U-110* fueron severos. Dos buques más, el *HMS Bulldog* y el *HMS Broadway* se unieron al *HMS Aubretia* , que tras localizar de nuevo su objetivo repitió el ataque, esta vez con las cargas preparadas para explotar a mayor profundidad. Este segundo golpe fue aún más certero que el primero y el *U-110* quedó ingobernable, con problemas en el timón, en los hidrófonos, en los motores… Por si esto fuera poco, debido a las fugas de agua que habían entrado en contacto con las baterías, se había comenzado a producir gas venenoso y la alarma por gas a bordo de un submarino solo tenía una vía de escape, la superficie, pues de otra forma no podía limpiarse el aire y la muerte era segura. La nave empezaba a ascender cuando el pánico comenzó a reinar entre la tripulación, a pesar de los esfuerzos de los experimentados oficiales para contrarrestarlo, conscientes como todos de que acabarían envenenados de seguir encerrados y respirando aquel aire. Los sistemas que debían actuar sobre los tanques de lastre, que tenían que ser vaciados de agua para que la nave subiera, no

funcionaban y los nervios y los gritos recorrían el submarino de proa a popa. Entonces la salvación, por una vez, llegó en forma de carga de profundidad. La explosión de una de ellas sacudió el submarino una vez más y desbloqueo el sistema de soplado de los tanques, que comenzaron a vaciarse. El *U-110* cambió de trayectoria y comenzó a subir rápidamente. En la superficie, sabiendo que el aire del exterior era la necesidad prioritaria en aquel momento, los hombres abrieron la escotilla de la torreta inmediatamente y entonces Lemp dio por fin la orden de abandono del submarino.

El *HMS Broadway* , al ver emerger al enemigo, se prepararó para usar su artillería contra él, acercándose además a toda máquina. Comprobaron que la tripulación alemana no estaba en disposición de defenderse, sino que por contra estaba lanzándose al agua, abandonando la nave de manera apresurada. No hay que olvidar que escapaban del gas venenoso por una parte y del posible hundimiento del submarino, por otra, que podría llevarlos en su barriga hasta el fondo, a una muerte segura. Lemp, en la torreta, apremiaba a sus hombres para que se lanzaran al agua. Acabó por abandonar la cubierta del *U-110* también él, y según parece, una vez en el agua preguntó por uno de sus hombres, un teniente en prácticas, que estaba convaleciente de una enfermedad y que posiblemente necesitara ayuda para mantenerse a flote. Este detalle explica por qué Lemp era respetado y apreciado por su tripulación.

La zona se había llenado de combustible complicándolo todo. Lemp, ya en el agua, se dio cuenta de que el submarino no se hundía y trató de volver a bordo para solucionar ese problema, cumpliendo así con el mandato de no dejar nada al alcance del enemigo, que ya había enviado un comando de abordaje para entrar en el *U-110* y capturar los preciados libros de códigos y la máquina Enigma. Aunque los testimonios están condicionados por la rapidez y la tensión del momento, es posible que Lemp llegara a subir de nuevo a bordo, donde hubo varios disparos de los integrantes del comando británico para controlar a los alemanes, alcanzado a varios de ellos, quizás al propio Lemp, que fue uno de los hombres que no sobrevivió a la captura del *U-110* .

Los ingleses tuvieron éxito en su búsqueda, y el riesgo que corrieron sus soldados entrando en el *U-110* , por el estado de la nave, a la búsqueda de la máquina Enigma, tuvo su premio. La nave hacía agua, aunque no había rastro de contaminación en el aire. El registro del submarino duró varias horas y el comando de abordaje volvió a su buque, el *HMS Broadway* , con una máquina Enigma, libros de códigos, mapas, libros de instrucciones alemanes… incluso, casi como trofeo, se llevaron el sextante y la Cruz de Caballero de Lemp. Hay quien considera lo que se encontró en el submarino de Lemp como la captura más valiosa de toda la guerra. El objetivo, una vez conseguido aquel botín, era llevar el submarino a la costa para estudiarlo y repararlo, pero los británicos no dominaban, como es lógico, el gobierno del submarino alemán y seguramente no se fiaban de sus prisioneros lo suficiente como para

pedirles ayuda, lo que acabó provocando que debido a su precario estado y a la falta de pericia en su gobierno, tras diecisiete horas de navegación, el *U-110* levantara la proa y comenzara a hundirse irremediablemente, a 560 kilómetros de Islandia. La pérdida del submarino, una vez ocurrida, tenía una gran ventaja para sus captores: el desconocimiento del hecho por parte de los alemanes. Tanto es así, que lo ocurrido en alta mar con el *U-110* fue mantenido en secreto desde aquel momento y hasta 1959, a pesar de que 400 marinos británicos habían tomado parte en ello.

Se hizo creer a los prisioneros alemanes del *U-110* que no se había podido obtener nada de valor del submarino, del mismo modo que a Dönitz y al resto del ejército y al gobierno alemán. Si los germanos sospecharan, aunque fuera mínimamente, que los británicos se habían hecho con una de sus máquinas Enigma y especialmente con sus libros de códigos, habrían cambiado la configuración y los códigos, restando utilidad a la captura. Ese juego de sospechas, en el que los alemanes observaban comportamientos extraños o casualidades poco probables que jugaban en su contra, se dio durante toda la guerra. En sentido contrario también, ya que los alemanes tenían a su vez sus sistemas de inteligencia y escuchas.

El informe sobre el abordaje del *U-110* fue clasificado como secreto y desde el momento de su redacción se indicó que debería mantenerse como tal secreto hasta 1972, durante treinta años. Gracias al *U-110* los ingleses tenían en su poder las claves diarias de Enigma de abril y junio, aunque habían perdido las de mayo. Además, los alemanes dividían el Atlántico en cuadrados y cada uno de ellos tenía un identificador único, lo que les permitía situarse en aquel enorme territorio acuático. Ahora, uno de aquellos mapas de cuadrados estaba en poder del enemigo, que podía entender y conocer el sistema de referencias de posiciones que usaban los alemanes, con información, por ejemplo, de los pasos libres de minas en el Golfo de Vizcaya.

Estas acciones, y otras muchas, tanto de captura o hundimiento de submarinos, como otras acciones de guerra, llevaron a algunos mandos nazis a plantearse la posibilidad de que Enigma hubiera sido rota por el enemigo y no fuera segura. En octubre de 1941 se llevó a cabo una investigación oficial, a cargo del vicealmirante Erhard Maertens, que concluyó que no parecía que los aliados hubieran roto los cifrados alemanes. En cualquier caso, este tipo de sospechas y dudas hacía que se aumentara la seguridad cambiando protocolos de uso e incluso algún detalle en las propias máquinas. Sin ir más lejos, unos meses después, en febrero de 1942, los submarinos comenzaron a utilizar Enigma con cuatro rotores en lugar de tres, algo que, como ya hemos visto, suponía un revés para las Bombe aliadas, que no estaban diseñadas para buscar configuraciones de cuatro rotores y por lo tanto se volvían inservibles. Las ventajas iban de un lado a otro. En pocos sitios se vivió más que en el Atlántico aquel constante vaivén de la ventaja a la desventaja.

Si a finales de 1940 y principios de 1941 habían tenido lugar los primeros tiempos felices para la Ubootwaffe nazi, entre enero de 1942 y agosto de ese año se repitieron los éxitos. Esos ocho meses se conocen como los segundos tiempos felices y en esta ocasión se alcanzaban las costas americanas. Los alemanes aprovecharon la falta de preparación y de coordinación de las defensas antisubmarinas en la zona, además de la incapacidad aliada para detectarlos y atacar, para hundir un buen número de barcos, más de 600, con una pérdida total que superó los tres millones de toneladas. En esta situación no es de extrañar que la presión sobre el cobertizo 8 creciera cada semana y casi cada día, ya que descifrar la Enigma naval se había tornado en un elemento crítico y necesario para que la guerra corriera a favor de los aliados. Dicho esto, una cosa había cambiado en el contexto. Si, como decíamos, ahora los submarinos también alcanzaban las costas norteamericanas, los recursos y conocimientos de los criptógrafos de Estados Unidos también estaban ahora junto a los de Bletchley Park.

En otros ámbitos, en otros cobertizos de trabajo, el éxito sí estaba del lado aliado, donde seguían descifrando las comunicaciones del ejército de tierra y del ejército de aire alemanes, lo que suponía una ventaja enorme en otros teatros de operaciones, distintos del Atlántico. En el norte de África, por ejemplo, los mensajes de Enigma descifrados eran un activo valioso para enfrentarse a las tropas de Rommel.

22. Los criptógrafos alemanes

Aunque habitualmente se habla de la criptografía en la Segunda Guerra Mundial haciendo referencia al gran éxito de los aliados contra las máquinas de cifrar alemanas y japonesas, lo cierto es que también los alemanes sacaron partido a la ruptura de los códigos de los enemigos. Ya hemos hablado de la B-Dienst, la Inteligencia Naval alemana, pero no era ni mucho menos la única unidad dedicada a la captura de señales y al descifrado de los mensajes aliados. Ya desde los primeros años veinte, los alemanes, a pesar de la escasez de todo tipo de recursos, tenían personas trabajando contra los códigos rusos, italianos, británicos y franceses, entre otros. De hecho, uno de los problemas de los criptógrafos nazis durante la guerra fue que estaban repartidos por varias entidades y la colaboración entre ellas no fue la mejor. En el bando aliado, en cambio, Bletchley Park concentraba gran parte del esfuerzo y era un centro de convergencia de información, recursos y talento.

Cuando Hitler llegó al poder en 1933, Wilhelm Fenner, que venía siendo responsable de los cifrados durante varios años, se puso a la cabeza del OKW-Chi, Oberkommando der Wehrmarcht Chiffrierabteilung, la unidad dedicada a la inteligencia de señales. La Luftwaffe también puso en marcha su unidad de captura y descifrado de señales, con el nombre de Forschungsamt, donde trabajó Hans-Thilo Schmidt. La agencia Pers-Z, nombre que provenía de Personalabteilung-Z, estaba integrada dentro de los Asuntos Exteriores del gobierno alemán, y su objetivo era el mismo. Estas son solo algunas de las oficinas, unidades y agencias que fueron creadas en torno a la criptografía en la Alemania nazi. En muchos casos, se llegaron a robar personal entre ellas, lo que a la larga no beneficiaría a los germanos y sí a sus enemigos. En 1938 eran diez las entidades que trabajaban en la captura de señales y la ruptura de los cifrados y códigos. Incluso cuando el OKW-Chi dirigido por Fenner controlaba varias agencias, estas no colaboraban de manera clara.

La Guerra Civil española sirvió a los alemanes de campo de pruebas real en muchos ámbitos, también en el de la criptografía. En 1938, la marina británica era ya un objetivo prioritario y se emplearon recursos para intentar conocer lo máximo posible de sus códigos. Los británicos utilizaban libros de códigos y tablas de sustraendos, esto es, números que restaban de los códigos. Estos métodos eran habituales y habían sido muy comunes durante todo el siglo. Una vez tomado el código de una determinada palabra del libro de códigos, a ese número se le restaba un número de la tabla de sustraendos. Así, el libro de códigos podía mantenerse en el tiempo, pero al ir cambiando los sustraendos, la variabilidad del resultado aumentaba y el criptoanálisis era mucho más complejo. El mensaje final era enviado con un indicador que permitía al

receptor conocer qué números de su tabla de sustraendos debía usar y así podía invertir el proceso y obtener el mensaje en claro.

Los alemanes fueron capaces de ir conociendo los libros de códigos de la marina británica y las tablas de sustraendos, en parte por errores en el uso de los métodos, enviando el mismo texto cifrado y sin cifrar, y también por la búsqueda de palabras conocidas en textos cifrados, como nombres de barcos, puertos… aprovechando la red de agentes de información que tenían por el mundo, tal y como hemos comentado. De nuevo, como en los siglos anteriores, los criptoanalistas buscaban pequeñas pistas para averiguar los códigos paso a paso. Además, Wilhelm Tranow se dio cuenta de que, si bien los británicos tenían distintos libros de códigos para los buques de superficie, los submarinos y otras naves, todos usaban las mismas tablas de sustraendos. Esto les facilitó el trabajo. Este y otros errores llevaron a que, en agosto de 1939, con la guerra a punto de comenzar, varios códigos británicos, entre ellos el Código Naval 1, fueran leídos por los alemanes con cierta regularidad. En torno al 40 por ciento de los mensajes capturados eran descifrados. Estos éxitos avalaron a Tranow y al resto de responsables de los departamentos de criptografía a la hora de solicitar recursos y personal.

En esa misma época, el Pers-Z leía los códigos diplomáticos de algunos países como Irlanda, Portugal o Noruega y estaban luchando contra la máquina Enigma que había implantado la diplomacia suiza. En 1939, el Código Naval 2 de los británicos ya se había roto en cierta medida, lo que permitía a los alemanes conocer los informes de inteligencia que enviaban al Almirantazgo los agregados en las embajadas de otros países. De igual forma que los aliados, tanto en la Primera como en la Segunda Guerra Mundial se hicieron con información y documentos que les ayudaron a conocer los métodos criptográficos enemigos, los alemanes consiguieron algo similar en la invasión de Noruega en mayo de 1940. Distintos documentos y libros de códigos fueron capturados a los británicos y acabaron en el B-Dienst, siendo de gran ayuda para Tranow y sus hombres. El avance hacia el oeste durante la *Blitzkrieg* se benefició del conocimiento que tenían de los códigos franceses. Información importante tanto sobre los británicos como sobre los propios franceses fue capturada y descifrada. Así, los alemanes sabían que la Royal Air Force (RAF) tenía escasez de combustible y también supieron que la Fuerza Expedicionaria Británica no lucharía hasta el final sobre suelo francés, sino que buscaría una escapatoria llegado el momento. Fenner aseguró después de la guerra que en el OKW-Chi varios de los sistemas de cifrado utilizados por los franceses ya eran leídos sin problemas en los primeros meses del conflicto.

Los italianos también tenían sus servicios de escucha y descifrado, como el Servizio Informazioni Militari (SIM) o el Servizio Informazioni Speciali della Regia Marina (SIS), cuyos descubrimientos en muchos casos eran compartidos con los alemanes. La posición mediterránea de estos servicios les ayudó en la guerra marítima en la zona y en el combate en África. En septiembre de 1941, tres meses antes de que

Estados Unidos entrara en la guerra, el general Cesare Ame, responsable del SIM, puso en marcha el robo de los códigos, militares y diplomáticos de los norteamericanos, directamente de su embajada en Roma. Una noche, cuatro hombres, dos de ellos trabajadores de la propia embajada, entraron en la misma, y se llevaron los documentos que necesitaban, entre otros un libro encuadernado en cuero negro con los códigos diplomáticos. En las oficinas del SIM en Roma fotografiaron los libros y volvieron a la embajada para dejarlos de nuevo donde estaban. Estos libros, con toda probabilidad, fueron compartidos con los alemanes, así como la información que fueron obteniendo los italianos gracias a ellos.

La ayuda de Italia fue importante en el norte de África, donde también se encontraron los alemanes con una suerte inesperada. El Departamento de Estado de Estados Unidos designó un nuevo agregado militar en El Cairo en octubre de 1940. El coronel Bonner Francis Fellers tenía como una de sus tareas más importantes en su nuevo puesto informar sobre las operaciones británicas en el Mediterráneo y en Oriente Medio. Los británicos, que ayudaron fielmente a Fellers en su trabajo compartían con él información y planes propios, además de información de inteligencia sobre los italianos y los alemanes. No era extraño que incluso visitara a las tropas en el frente y conversara con los mandos. Con todo esto, Fellers enviaba diariamente un informe cifrado a Estados Unidos, suficientemente importante como para que el propio Roosevelt le prestara atención. Esa valiosísima información era capturada por los alemanes y los italianos y, gracias al robo que había promovido Cesare Ame en la embajada estadounidense en Roma, la podían descifrar sin muchos problemas.

Esta fuente, entre otras, permitía a los alemanes conocer la situación de sus enemigos tanto en el norte de África como en el Mediterráneo. Rommel disfrutaba así de una importante ventaja que le permitía planear mejor sus movimientos y ataques. Por otro lado, los convoyes de suministros británicos en el Mediterráneo también se ponían en peligro en mayor medida gracias a toda la información de inteligencia capturada a Fellers. En defensa del estadounidense hay que decir que él cumplía con su trabajo de forma excepcional y que al menos en dos ocasiones solicitó a Washington revisar la seguridad de los códigos que usaba en las comunicaciones, consciente de que un problema en ese ámbito era una catástrofe. Sus peticiones no fueron escuchadas y así sus informes, que incluían hasta el nombre de los barcos que se movían por Suez, seguían llegando a manos alemanas en cuestión de horas. Después de codificar los mensajes, Fellers los enviaba a través de la Compañía de Telégrafos de Egipto en El Cairo, para que cruzaran el Atlántico hasta su país. La señal era capturada por las tropas alemanas en la zona, y también por la unidad de escucha de la Luftwaffe en Atenas. En menos de una hora estaba ante los criptógrafos alemanes y una vez puestos los mensajes en claro y traducidos al alemán, estos se enviaban al centro de mando de Rommel, a la Oficina Central de Seguridad del Reich (RSHA), a Göring, a Himmler, al mariscal de campo Keitel y al propio Hitler. Esta lista de distribución de la información da

una idea de la calidad de la información y de lo vital que era la misma para la evolución de la guerra en África.

En enero de 1942, por ejemplo, Rommel, aprovechando la información de inteligencia que había recibido, lanzó una ofensiva. Avanzó casi 500 kilómetros en poco más de dos semanas. Los problemas que generó este avance de Rommel fueron enumerados por Fellers en sus informes, y por lo tanto iban directos también al propio Rommel. La cantidad de tanques en cada unidad, sus posiciones, la cantidad de suministros y combustible que les quedaba… Incluso la contraofensiva aliada fue advertida por el norteamericano y por lo tanto conocida por Rommel, que reaccionó.

A mediados de aquel año la situación en el Mediterráneo y en el norte de África pendía de un hilo. Malta estaba siendo asfixiada, y sin esa isla la situación aliada en la zona quedaría seriamente tocada, lo que dejaría vía libre a los convoyes de suministros alemanes para llegar hasta las tropas en el norte del continente africano. Todo esto había sido expuesto por el propio Fellers, añadiendo la situación detallada. En junio, con las tropas de Rommel a menos de 150 kilómetros de Alejandría, la fuente fiable del agregado militar estadounidense en El Cairo, a la que Rommel llamaba «nuestro pequeño amigo», cesó. Como bien sabemos, los aliados también capturaban el tráfico y descifraban una parte significativa de las comunicaciones germanas. En Bletchley Park detectaron la existencia de esa fuente de información en el norte de África, llegando incluso a leer en algún mensaje alemán la frase «una fuente militar aliada en Egipto». Las sospechas sobre dónde podría estar la fuga de información incluían a Fellers. El 12 de junio los británicos pusieron en conocimiento de Estados Unidos sus sospechas, aunque también indicaban que probablemente no era un traidor, sino que todo había sido contra su voluntad. Fellers fue trasladado, aunque no fue procesado e incluso fue ascendido de rango por su buen trabajo. El sustituto cambió totalmente la forma de cifrar la información que enviaba, usando una máquina Hagelin M-209.

Un caso similar al de Fellers ocurrió en el bando contrario con el embajador de Japón en Berlín, el coronel Hiroshi Oshima. Este hombre contaba con la total confianza de los alemanes, y tenía incluso conversaciones con Hitler. La información que manejaba, por tanto, era del máximo nivel, con detalles, por ejemplo, del muro Atlántico o de las armas V1 y V2. Oshima enviaba puntualmente información a su país de todo ello, utilizando el código diplomático japonés, la máquina Púrpura en terminología estadounidense. Ese método había sido roto y no era extraño que los estadounidenses llegaran a conocer el contenido de los mensajes de Oshima antes incluso de que lo conocieran en Japón.

La criptografía y la captura de señales estuvieron presentes durante toda la guerra y casi de manera total, tanto en un bando como en el otro. Pero en algunas de las batallas más importantes su influencia o peso fue más destacado. Como ya hemos comentado, diferentes unidades alemanas relacionadas con la inteligencia de señales tuvieron

bajo un cierto control los cifrados y comunicaciones aliadas. La Luftwaffe, por ejemplo, era capaz de capturar y descifrar las comunicaciones de la RAF. Esto podría haber sido una gran ventaja durante la batalla de Inglaterra, pero en lo cierto es que la lucha se desarrolló de una forma que evitó esa ventaja. El Chi-Stelle, la unidad de cifras del Servicio de Inteligencia de Señales de la Luftwaffe, había hecho un gran trabajo y tenía 24 estaciones de escucha repartidas por Europa, incluso algunas de ellas móviles. Tenía una en el Paso de Calais y con la información de que disponía conocía las fuerzas de la RAF y dónde tenían la base. Esto era una gran ventaja *a priori* para afrontar la batalla de Inglaterra, que tuvo lugar entre julio y octubre de 1940, pero su mejor servicio estaba en las acciones de defensa, no de ataque. Es decir, si lo prioritario en ese momento de 1940 hubiera sido proteger a Alemania de las incursiones británicas, el tiempo que les llevaba a los criptógrafos de la Chi-Stelle descifrar el mensaje no hubiera impedido que la información estuviera lista a tiempo para reaccionar. En la batalla de Inglaterra la situación era otra. Cuando la Luftwaffe capturaba la señal de la RAF antes de una misión de defensa británica, el tiempo que requería el descifrado era mayor que el margen que tenían los alemanes para reaccionar, por lo que no servía de nada. Por lo tanto, la Luftwaffe tenía un arma más en sus manos a la hora de parar las incursiones sobre el continente, pero esa misma arma no podía ayudarle en los ataques sobre la isla británica.

Por supuesto, también los británicos tenían la capacidad de leer gran parte de los cifrados de la Luftwaffe. De esa forma se habían enterado, por ejemplo, y ya en el verano de 1940, de la orden de no bombardear los muelles británicos, ya que debían ser utilizados para la futura invasión que tenían prevista los nazis. Este fue tan solo uno de los detalles que se conocieron en Bletchley Park sobre la operación León Marino, el plan de los alemanes para invadir Inglaterra. Este plan, como sabemos, nunca llegó a ejecutarse.

En agosto de 1942 el teniente general británico Bernard Montgomery, conocido popularmente como Monty, se puso al frente del Octavo Ejército para contener y combatir a las tropas acorazadas de Rommel, cuyo sobrenombre era el Zorro del Desierto, precisamente por su capacidad para aprovechar sus fuerzas acorazadas en ese entorno. Este también tenía información clasificada sobre su enemigo, proveniente de los servicios de escucha de señales y descifrado alemanes, pero lo cierto es que el partido que le sacó el bando aliado a este tipo de fuentes fue mayor. Montgomery conocía los planes de Rommel y sus movimientos gracias a Bletchley Park. Y también conocía los problemas de suministro que azotaron a los alemanes en un determinado momento y que fueron explotados con gran éxito por sus enemigos.

23. EL BLACK CHAMBER ESTADOUNIDENSE

Volvemos atrás en el tiempo para centrarnos ahora en la guerra en el Pacífico, en la criptografía estadounidense y su combate con las máquinas y los cifrados japoneses. El viaje de Estados Unidos en este ámbito, que culminó en la Segunda Guerra Mundial, había comenzado mucho antes, en el final de la Primera Guerra Mundial.

Herbert Osborn Yardley es un nombre asociado a la criptografía estadounidense, que en el tiempo de entre guerras fue clave. Según algunas fuentes, no era tan buen criptoanalista como hombre de negocios, como *conseguidor* , podríamos decir. Aunque ingresó en la Universidad de Chicago, la abandono en el primer año y comenzó a trabajar como telegrafista para el ferrocarril. Seguía así los pasos de su padre, que se había dedicado a eso mismo, había sido jefe de estación y telegrafista. En 1912 aprobó el examen y pasó a trabajar para el gobierno, siguiendo como telegrafista. Esto le abrió la puerta del Departamento de Estado, donde comenzó a tener relación con los códigos. Como ya hemos comentado, el telégrafo y los códigos han tenido una estrecha relación a lo largo de la historia. Rompió varios códigos propios de su país y así demostró, por un lado, su capacidad como criptoanalista, y por otro la debilidad de la seguridad norteamericana.

Cuando comenzó la Primera Guerra Mundial, se puso en contacto con el Departamento de Guerra del gobierno, le advirtió de los problemas y carencias del país y le propuso crear una entidad dedicada a la criptología. Propuso, como es lógico, que él estuviera al mando. La propuesta fue aceptada y Yardley se puso a la cabeza de un nuevo grupo de criptólogos, con un importante presupuesto a su disposición, lo que le permitió contratar a lingüistas, psicólogos, matemáticos… El nuevo grupo fue denominado MI-8 y estaba integrado dentro de la División de Inteligencia Militar del ejército.

Yardley ayudó en labores de contraespionaje, descifrando mensajes y notas incautadas a espías y a agentes enemigos, además de ayudar al propio ejército. Tras la guerra, el MI-8 siguió operando, ingresando dinero tanto del ejército como del Departamento de Estado. Para sortear algunas restricciones administrativas y poder recibir fondos sin problema, Yardley creó una empresa en Nueva York, que se dedicaba básicamente a lo mismo, a los códigos comerciales.

En ese tiempo de paz el objetivo principal fueron los códigos diplomáticos japoneses, y fue en este ámbito donde se centraría la organización de Yardley, a la que acabaría llamando Cámara Negra, Black Chamber, un nombre que nos recuerda a las oficinas de criptografía europeas de siglos atrás.

En noviembre de 1921 se celebró la Conferencia Naval en Washington, donde se debían establecer los límites de tonelaje de los buques principales de las marinas de Gran Bretaña, Japón, Francia, Italia y el propio Estados Unidos, entre otras, todas ellas con intereses en el Pacífico y en el este asiático. Era, por lo tanto, una conferencia para limitar la capacidad militar de las armadas de estos países. Una decisión clave para el futuro. Para poder comparar unos barcos con otros, cuya tecnología podía ser distinta y donde cada uno podía ser mejor en una determinada característica, se optó por tomar el tonelaje como medida final. Este tonelaje se determinaba en ratios entre unas marinas y otras. Así, un 5/3 entre Estados Unidos y Japón determinaba que el primero podía tener barcos hasta sumar 525.000 toneladas en su marina, mientras el segundo se quedaba en 315.000.

La primera oferta que Japón puso sobre la mesa fue de 10/7, siendo ellos el número menor. Durante las negociaciones, a finales de noviembre, la Oficina de Asuntos Exteriores de Japón envió un mensaje cifrado a su embajada en Washington, con instrucciones para su delegación en la conferencia. Debían mantener ese 10/7 cuanto fuera posible, pero en caso de necesidad, podía bajar medio punto en la ratio, hasta 10/6,5 y como último recurso autorizaban a aceptar un 10/6.

La oficina de Yardley estaba entonces descifrando los códigos japoneses y las comunicaciones eran interceptadas regularmente. Así, el secretario de Estado norteamericano, Charles Evan Hughes, no tardó en ser informado de los límites con los que se planteaban la negociación los japoneses. Entrar en una negociación sabiendo de antemano dónde está el límite del contrario, es algo impagable. Las reuniones y discusiones siguieron con una posición inamovible de Estados Unidos, hasta que se cerraron en 10/6 el 10 de diciembre de 1921. Al final Japón quedaba con capacidad para tener 18 acorazados, mientras Estados Unidos y Gran Bretaña tenían permiso, gracias al acuerdo, para llegar hasta los 30.

Aquella conferencia fue el punto culminante del Black Chamber de Yardley, el mejor servicio que prestó a su país. A partir de ahí, comenzaron los problemas. En 1924 la financiación se había reducido a la mitad y en 1929 Yardley se enfrentó a un nuevo secretario de Estado, Henry L. Stimson, que consideraba muy poco ético capturar y descifrar las comunicaciones diplomáticas de otros países, esto es, la labor principal del Black Chamber. Stimson dejaría escrito en sus memorias que los caballeros no leen el correo de otros caballeros, justificando su visión, quizás ingenua, de la diplomacia internacional. Todo acabó en enero de 1931, cuando las relaciones contractuales entre Yardley y el gobierno quedaron rotas, y por lo tanto su oficina se cerró.

En abril de aquel año, Yardley comenzó a publicar artículos sobre criptografía en el *Saturday Evening Post* , y en el verano lanzó un libro al mercado. Bajo el título de *The American Black Chamber* , el libro ponía al descubierto toda la actividad de Yardley y su oficina durante la última década dando servicio al gobierno. Destapó todas sus acciones,

incluida la que hemos visto sobre la Conferencia Naval de 1921, donde Japón salió claramente perjudicado. El libro fue un éxito de ventas, y la polémica y el enfado, como es lógico, también fueron enormes. Los diarios japoneses enviaron a corresponsales a entrevistar a Yardley y los hechos que narraba indignaron a Japón, que, con razón, consideraba que se había traicionado su confianza y la del resto de países durante una conferencia de desarme, casi una conferencia de paz. Decenas de miles de copias de la traducción al japonés del libro fueron vendidas. Otras naciones se enteraron también de cómo sus códigos habían sido rotos y de cómo sus comunicaciones diplomáticas eran capturadas copiando los telegramas que se enviaban a través de empresas como Western Union.

En junio de 1931 Japón exponía ya de manera clara la necesidad de mejorar sus códigos militares. Esta era otra de las consecuencias de la decisión de Yardley de hacer público su trabajo durante más de una década para el gobierno de Estados Unidos. Los japoneses comenzaron a probar nuevas máquinas criptográficas, más complejas, más seguras y más caras. Es decir, la decisión de Yardley también hizo mucho más complicado el trabajo de los que serían sus sucesores.

La Black Chamber fue finalmente cerrada y Estados Unidos se quedó con tan solo un criptoanalista en el Departamento de Guerra, William F. Friedman. Era hijo de inmigrantes judíos rusos y él mismo había nacido en Rusia, si bien llegó a Estados Unidos cuando tenía tan solo un año de vida, en 1891. Friedman estudió agricultura, principalmente porque la matrícula de esa asignatura era gratuita, y eso lo llevó a interesarse por la genética. Gracias a sus estudios encontró trabajo en la empresa de George Fabyan, un hombre que se había hecho multimillonario gracias a la industria textil y que había montado su propio laboratorio de investigación. Dentro de las materias que se trataban en el centro Riverbank, como se llamaba el centro de investigación de Fabyan, estaba la genética. Otra de las ramas del centro era la criptografía, donde se pretendía demostrar que las obras de Shakespeare eran en realidad de Francis Bacon. Friedman se sintió atraído por la criptografía y aprendió sobre el tema. Riverbank tenía cierto nivel en cuanto a la criptografía se refiere, como prueba que durante la Primera Guerra Mundial varios de sus miembros colaboraron con su país dando formación a los soldados y criptógrafos del ejército. Entre ese personal de Riverbank que colaboró con el gobierno estaba Friedman. En 1921 dejó su trabajo para pasar a formar parte del Cuerpo de Señales del ejército estadounidense.

Dentro de la División de Inteligencia Militar, la Black Chamber se había dedicado a romper códigos, mientras que el Cuerpo de Señales trabajó en desarrollar los códigos que debía usar el ejército. A esta actividad fue a la que se consagró Friedman en la década de 1920, como director de Signals Intelligence Service (SIS). Con el paso del tiempo y a medida que la oficina de Friedman perdía fuerza, el Cuerpo de Señales fue ampliando sus trabajos y comenzó a dedicarse también al criptoanálisis. El aumento de responsabilidades hizo que se autorizara a Friedman a

buscar algún colaborador. Lógicamente un solo hombre dedicado a estas tareas en el Departamento de Guerra era una dotación claramente insuficiente, y pronto fueron tres personas. Estos nuevos fichajes no tenían experiencia en el criptoanálisis, y fue Friedman el que redactó un manual para que aprendieran. Todo esto no impidió que además se pidiera a Friedman que su oficina estudiara tintas invisibles, pensara cómo imprimir y distribuir los códigos a las unidades militares dispersas por un territorio, formaran en el uso de la criptografía a oficiales…

Yardley había mantenido durante años una relación con las compañías privadas de comunicaciones, que le había permitido tener acceso al tráfico que estas procesaban. Las compañías de cable, especialmente, entregaban copias del tráfico que viajaba por ellas. Esto había comenzado en tiempo de guerra y era visto como algo razonable. En tiempo de paz, las empresas eran cada vez más reticentes a llevar a cabo estas prácticas, claramente ilegales. La desaparición de Yardley en las relaciones detuvo al momento esta colaboración y dejaron de llegar cablegramas a los criptógrafos militares. De igual forma que el cierre del Black Chamber dejó a Friedman como único responsable de la criptografía militar, a comienzos de los años treinta del siglo XX no había comunicaciones internacionales que acabaran en su poder y no había forma de capturarlas.

Dicho esto, las comunicaciones por radio estaban al alcance de todos y tan solo había que colocar las antenas en los lugares adecuados y captar el tráfico. En general las embajadas no tenían enlaces directos con sus países, por lo que las comunicaciones diplomáticas que entraban y salían de Estados Unidos podían ser capturadas tan solo con escuchar en las frecuencias adecuadas. En 1931 Friedman fue autorizado a montar una estación de escucha experimental en el estado de Virginia. Gracias a ella sus hombres podían comenzar a trabajar con tráfico real y con cifrados reales de otros países. Esta apertura, aunque prudente, chocaba con las leyes que marcaban la escucha de las comunicaciones de terceros por radio como un delito. El estado de Virginia está en la costa este, por lo que no era el mejor sitio para capturar comunicaciones de los tres principales países sobre los que Estados Unidos tenía puesto el foco de atención: Japón, Rusia y México. La situación fue cambiando con el paso de los años y para cuando comenzó la Segunda Guerra Mundial, en 1939, el Cuerpo de Señales tenía ya unidades de escucha en Hawái, en las Islas Filipinas, en el Canal de Panamá, en Texas… En octubre de ese mismo año, con la guerra en Europa ya en marcha, Estados Unidos decidió que también sería conveniente comenzar a mirar con especial interés el tráfico alemán.

La armada de Estados Unidos estaba algo mejor en temas criptográficos, llevando ventaja a la oficina de Friedman y por lo tanto al resto de su ejército. Las armadas estaban obligadas a contemplar y pensar en frentes de combate enormes, a usar las líneas de comunicaciones de manera continua e incluso a lidiar con todos los elementos técnicos y tecnológicos que incorporaban los buques. Quizás

todo esto las predispuso a poner una mayor atención en el ámbito de las comunicaciones enemigas y su desciframiento.

Se habían percatado ya de la importancia de la escucha de las comunicaciones, del criptoanálisis y también de la complejidad añadida que suponía el japonés, el idioma de uno de los países sobre los que tenían puesta una atención especial. Por ello, cada año, enviaban un oficial naval a Tokio para aprender japonés, y a partir de 1927 se enviaron dos o tres oficiales por año. El idioma japonés suponía un reto importante, ya que cada letra enviada en morse podía ser el equivalente a un ideograma, por lo que la transcripción de los mensajes y su estudio obligaba a conocer el idioma con cierta profundidad. La armada estadounidense encargó a la conocida empresa de máquinas de escribir Underwood Typewritter, una serie de máquinas especiales que imprimiera los elementos de la escritura japonesa. Al pulsar una letra de nuestro alfabeto, lo que entenderían al leer el morse, la máquina escribiría el símbolo japonés correspondiente.

Lo que ocurrió con los mensajes capturados japoneses fue similar a lo que les había ocurrido a los polacos cuando Alemania comenzó a usar la Enigma. Las intercepciones del tráfico diplomático de Japón, entre Tokio y las principales capitales del mundo, se convirtieron en algo incomprensible. La oficina de Friedman había aprovechado el conocimiento de sus predecesores sobre los códigos japoneses, pero ahora todo era distinto. Su desconcierto era el mismo que había experimentado el Biuro Szyfrów polaco unos años atrás, y el motivo también era el mismo. Los japoneses habían comenzado a usar máquinas de rotores para cifrar sus comunicaciones. No obstante, las máquinas que usaban los japoneses eran más sencillas que Enigma. Por otra parte, mientras los polacos tenían a su alcance máquinas Enigma comerciales, los hombres de Friedman no tenían idea sobre el tipo de dispositivo al que se enfrentaban. El ataque por tanto se hacía algo más complejo, pero al analizar los cifrados de la máquina Roja, como se conocía a la versión diplomática de la máquina utilizada por Japón, los estadounidenses comenzaron a ver patrones que, como ya hemos comentado, son las grietas por las que ha de colarse un criptoanalista. El SIS se dio cuenta de la alta frecuencia de las vocales, y comenzó a sospechar que las vocales se cifraban como vocales y las consonantes como consonantes, para que así las secuencias resultantes del cifrado fueran pronunciables. Esto facilitaba la labor de envío y transcripción de los mensajes. Un error que ya se había dado en el pasado en Europa, como hemos visto.

Frank Rowlett y Solomon Kullback, que junto con Abraham Sinkov y el propio William Friedman componían el grupo de criptoanalistas del SIS, se centraron en varios mensajes especialmente largos que habían capturado. No tardaron en detectar diferentes cifrados dentro de esos mensajes, que correspondían con la misma palabra en el texto en claro. Se enfrentaron entonces a un problema más sencillo, y tan solo tenían que resolver un cifrado tipo Vigenère para las vocales, y otro para las consonantes. Pensaron que estaban ante una máquina de rotores, pero

muy sencilla, con un rotor para las vocales y otro para las consonantes. Resolviendo algún que otro problema e imaginando cómo funcionaría la máquina, ya que no tenían ninguna a su alcance ni la habían visto con anterioridad, finalmente fueron capaces de encontrar un procedimiento para descifrar los textos cifrados por la máquina Roja japonesa.

La marina estadounidense, por su parte, tenía a su oficina de cifrado, el OP-20-G, luchando contra el código M1, el usado por su homóloga nipona. Las relaciones entre ambas oficinas norteamericanas, la OP-20-G y el SIS, no era buena y la información no se compartía. En cualquier caso, en febrero de 1939, se capturó un mensaje cifrado por la máquina Roja japonesa, que anunciaba la sustitución de la propia máquina de cifrado por un nuevo modelo. Este nuevo modelo recibiría el nombre en clave de Púrpura y era mucho más complejo y seguro que su predecesora. El primer día de junio de ese mismo año, el código M1 era sustituido por el código AN, que más tarde se denominaría JN-25. Este código también quedaba fuera del alcance de los estadounidenses y los criptógrafos de este país volvían al punto de partida. Si bien la experiencia del SIS era importante, lo cierto es que en un momento en el que la tensión era cada vez mayor en las relaciones entre Estados Unidos y Japón, el SIS se quedaba ciego. De igual forma, el OP-20-G no sabía cómo atacar el AN.

24. Pearl Harbor, Midway y la operación Venganza

Se ha escrito mucho sobre los acontecimientos previos al ataque a Pearl Harbor, e incluso hay una teoría muy extendida que asegura que los estadounidenses conocían con detalle lo que iba a ocurrir y no hicieron nada. Algunos autores hablan de la censura en determinados archivos y de los problemas con los que se encuentran para aclarar la gran pregunta, si los criptógrafos norteamericanos habían roto el código JN-25 de la marina japonesa antes del ataque y por lo tanto sabían qué iba a ocurrir. El segundo gran debate está en torno a si la flota nipona mantuvo el silencio por radio durante los días previos al ataque, tal y como habían ordenado sus superiores, o si este silencio fue roto. De nuevo, la falta de silencio hubiera dado pistas de que un movimiento importante estaba en marcha, camino de Hawái.

Una de las claves está en las comunicaciones diplomáticas. La máquina Púrpura, que gobernaba esas comunicaciones, era más segura y compleja que las Enigma que hemos visto y los procedimientos de los japoneses en su uso aumentaban esa seguridad. Tenía, como motor de cifrado, algo parecido a cuatro rotores y el clavijero, además de algún componente adicional con respecto a Enigma. Por supuesto, también un teclado y una unidad de impresión, por la que salía el mensaje cifrado. Como decíamos, no utilizaba rotores como los de Enigma, sino que eran otro diseño electromecánico, aunque conceptualmente estamos ante algo similar. Su gran inconveniente era el peso y el tamaño, lo que impedía usarla con facilidad en el campo de batalla. Pero para su destino original, las oficinas diplomáticas, esto no suponía un problema.

Era más compleja que la máquina Roja, que se usaba hasta entonces y se destinó tan solo a las comunicaciones diplomáticas más importantes, lo que hacía que el tráfico capturado no fuera muy elevado. Haber roto la máquina Roja, no obstante, permitía a los criptoanalistas estadounidenses conocer el tipo de mensajes que se enviaban, su estructura, algunas palabras y expresiones comunes… y aprovecharon esa información para atacar a Púrpura. El libro de configuraciones, la clave de la máquina, cambiaba cada día y, de forma similar a lo que ocurría en Europa, la ruptura de los mensajes iba y venía por temporadas, en función de la suerte y capacidad para detectar las configuraciones.

Lo cierto es que unos meses antes del ataque, en septiembre de 1940, los estadounidenses consiguieron romper el cifrado diplomático japonés, esto es, Púrpura, lo que no significa que fueran capaces de conocer todo lo cifrado con el mismo sistema. Además, las comunicaciones de la marina japonesa eran otra cuestión diferente y por lo tanto la información no era completa. Con ayuda de dispositivos de IBM y codificando en tarjetas perforadas los mensajes y las posibles configuraciones de la máquina, los estadounidenses buscaban ir

conociendo las claves de configuración y por lo tanto los mensajes. Como vemos, una idea similar a la que se llevó a cabo en Bletchley Park. Si eran capaces de descubrir las claves de un día, y dado que sabían cómo funcionaban las máquinas del enemigo, podrían leer sus mensajes sin problemas. Cada vez que el libro de configuración era modificado, había que empezar de cero, más allá de la experiencia acumulada.

Al acercarse diciembre de 1941, los mensajes diplomáticos de más alto nivel eran cifrados con ese código Púrpura y Estados Unidos tenía una forma de romperlo, cuyo nombre en clave era Magic. Los criptoanalistas norteamericanos habían empleado año y medio en ser capaces de romper Púrpura, pero lo habían conseguido. Eran capaces de deducir la configuración de la máquina y su cableado y de poner los mensajes en claro suficientemente rápido como para que fueran útiles.

El 3 de diciembre de 1941, cuatro días antes del ataque, un mensaje cifrado llegó a la embajada de Japón en Washington, dando orden de destruir los libros de códigos y dos de las máquinas Púrpura que tenían, dejando solo una operativa. Frank Rowlett, un criptoanalista de alto rango del Servicio de Inteligencia de Señales del ejército estadounidense, se encontró en su bandeja de entrada con el mensaje japonés roto gracias a Magic y leyó su contenido con creciente sorpresa y preocupación. Si los japoneses preveían quedarse con una sola máquina Púrpura, obviamente, sería imposible para la embajada continuar su trabajo habitual, por lo que algo debía de estar pasando para que la embajada previera un parón en su actividad, al menos criptográficamente. Cuando lo transmitió a sus superiores, surgieron más preguntas y dudas. Se preguntaban, por ejemplo, si los japoneses habían descubierto que su código no era seguro y por eso destruían los libros y las máquinas. También cabía la posibilidad de que Japón fuera a declarar la guerra y por lo tanto su embajada en Washington tuviera que ser desalojada, por supuesto, sin dejar pistas sobre sus sistemas criptográficos.

Tres días después, la noche del 6 de diciembre, un nuevo mensaje japonés descifrado por Magic ofrecía más pistas. En este caso el mensaje llegó hasta la Casa Blanca. El presidente Roosevelt fue informado de que Japón se disponía a romper relaciones diplomáticas. En un momento de tensión como aquel, se podía intuir que la guerra era inminente, pero no cuándo ni dónde comenzaría.

La facilidad con la que Magic rompía la versión de Púrpura que se utilizaba en el ámbito diplomático no se repetía en el caso de las comunicaciones militares. Los códigos navales japoneses seguían siendo seguros y aunque se conseguía romperlos, se hacía con una demora de meses, lo que convertía la información en prácticamente inútil. El código naval, el JN-25, aunque en aquel momento los estadounidenses lo denominaban AN-1, había sido puesto en funcionamiento el 1 de junio de 1939 y seguía siendo seguro. Cada pocos meses, los japoneses hacían algún cambio en sus libros de códigos y el proceso tenía que volver a comenzar.

El 7 de diciembre de 1941 es conocido popularmente como «El día de la infamia». Al arrancar aquel día, Japón atacó Pearl Harbor y provocó daños enormes a la flota estadounidense. Los dos países no estaban en guerra, a pesar de que la tensión entre ambos iba creciendo desde que en 1931 el ejército japonés comenzó su expansión con la invasión de Manchuria. Ante las acciones niponas de conquista, los estadounidenses, al otro lado del Pacífico, respondían con presión económica y política. Esta tensión hizo que en mayo de 1940 la flota estadounidense en el Pacífico recibiera la orden de permanecer en Pearl Harbor y no regresar a San Pedro, en California, que era su puerto de origen. Esto acabó provocando que, el día del ataque, la concentración de buques en Pearl Harbor fuera favorable a los japoneses.

Tanto es así que el *USS Arizona* y el *USS Vestal* , que estaban anclados en Pearl Harbor aquella dura mañana para los estadounidenses, estaban abarloados, es decir, unidos por el costado. Durante el ataque japonés, y debido a las primeras bombas, el *USS Vestal* , que era un buque taller, sufría un buen número de incendios y los bomberos estaban desbordados a bordo del mismo. A las 08.06 estos buques fueron atacados de nuevo y una de las bombas japonesas llegó hasta la santabárbara del *USS Arizona* , es decir, llegó hasta el lugar en el que estaban las bombas y explosivos del buque. La explosión resultante fue tan brutal que llevó al barco al fondo, pero también apagó todos los fuegos del *USS Vestal* , el buque que tenía al lado.

Isoroku Yamamoto, comandante en jefe de la Flota Combinada de la Armada Imperial japonesa, era reacio a forzar a Estados Unidos a una guerra. Sin embargo, fue el diseñador y director del ataque a Pearl Harbor. El japonés estaba familiarizado con la cultura estadounidense y con su forma de ver el mundo, ya que había estudiado allí, en Harvard, desde 1919 hasta 1921, y había sido agregado naval en Washington. Sabía de la fuerza industrial del país norteamericano y estaba convencido de que la única opción para Japón, en una guerra con el país que él conocía, era una serie de ataques rápidos que destrozaran la flota enemiga antes de que comenzara realmente la guerra.

Cuando llegó el momento de poner el ataque en marcha, en noviembre de 1941, después de meses de preparación, el número de buques involucrados era enorme, con dos acorazados, tres cruceros de combate, nueve destructores y tres submarinos, que escoltaban al núcleo clave del ataque, seis portaaviones. Lógicamente, la situación y todos estos preparativos llevaba a Estados Unidos a estar convencido de que los japoneses acabarían atacándole, aunque no sabía con exactitud cuándo y creía que sería en las Filipinas o en el Sudeste Asiático. En aquellos días previos al ataque la criptografía jugó un importante papel, aunque la falta de desarrollo y seguridad de los norteamericanos acabó siendo una más de las causas del desastre.

La razón por la que el día del ataque a Pearl Harbor se llama «el día de la infamia» está en el discurso del presidente Roosevelt al día siguiente en el Congreso de Estados Unidos. Comenzaba de este modo:

Señor vicepresidente, señor presidente de la Cámara de Representantes, miembros del Senado y de la Cámara de Representantes: ayer, 7 de diciembre de 1941 —una fecha que vivirá en la infamia— Estados Unidos de América fue atacado repentina y deliberadamente por fuerzas navales y aéreas del Imperio de Japón.

El vocablo infamia triunfó y dio nombre al propio discurso, que se conoce como el Discurso de la Infamia (*Infamy Speech*), así como al día del ataque. Esa palabra no estaba en los primeros borradores del discurso, pero en una de las correcciones a lápiz, el propio Roosevelt la incluyó.

Cinco años después del ataque, con la guerra ya finalizada y ganada por los aliados, los criptoanalistas estadounidenses volvieron a intentar descifrar los mensajes que habían capturado a los japoneses antes de aquel día de diciembre de 1941. Con los conocimientos y recursos que tenían ya podían descifrar sin problema los mensajes cifrados con el JN-25. Como era de esperar, los mensajes de la marina japonesa en octubre y noviembre de 1941 hablaban de completar los preparativos para el ataque y de estar listos, el 20 de noviembre, para la guerra total. Se hablaba también de movimientos logísticos que, de haber sido conocidos en el momento, podrían haber dispuesto a Estados Unidos para una mejor defensa de Pearl Harbor.

Más allá de la polémica que continúa viva sobre este hecho, la ruptura de Púrpura hacía esperar algún acontecimiento, pero no se sabía qué, cuándo ni dónde. La información detallada, que se codificaba con el JN-25 japonés, podía haber sido clave, pero parece que Estados Unidos no estaba aún en disposición de romper ese código con facilidad.

Tras el éxito japonés en Pearl Harbor, Yamamoto se había convertido en un ídolo militar y civil en su país. Recibía sacas llenas de cartas del pueblo japonés, donde le mostraban su admiración y le colocaban como el líder militar que debía llevarles al éxito en el nuevo escenario de guerra que se había lanzado con la entrada en liza de Estados Unidos. Esta responsabilidad se mostró apremiante cuando en abril de 1942 los B-25 del teniente-coronel James H. Doolittle bombardearon por primera vez suelo japonés. Habían despegado desde el portaaviones *USS Hornet* y si bien la Incursión Doolittle, como se la conoce popularmente, no causó daños importantes, sí fue un golpe moral para los japoneses, que veían a la guerra llamar a su propia puerta.

Tras aquel ataque, Yamamoto determinó que la isla de Midway era el punto clave para que aquello no volviera a ocurrir. Mientras Midway siguiera en manos de los norteamericanos, el perímetro de seguridad japonés era insuficiente. Había que empujar al enemigo más lejos de aquel punto, los japoneses tenían que tomar Midway. Los detalles del

ataque de Doolittle, aunque Yamamoto no los conociera en aquel momento, le daban la razón. Los B-25 habrían tenido que volar unos 800 kilómetros hasta Japón, lanzar sus bombas, y volar otros 160 kilómetros hasta China, para aterrizar allí. Ese era el plan, pero los aviones tuvieron que hacer más de 300 kilómetros extra, con vientos en contra y el ya de por sí justo combustible para la misión se convirtió en el recurso más preciado y la amenaza más crítica. El resultado fue un desastre para los pilotos y los aparatos estadounidenses de la operación. Varios cayeron en manos japonesas y algunos, incluido el propio Doolittle, salvó la vida de milagro al ser rescatado por la guerrilla china antes de ser capturado por los japoneses. Cinco acabaron en manos rusas y ocho soldados fueron hechos prisioneros por los japoneses, de los que tres fueron ejecutados y otro moriría por las malas condiciones de su cautiverio. Otros tres murieron en los aterrizajes forzosos. Todos los aviones se perdieron.

Como decíamos, Yamamoto no fallaba en su diagnóstico. En cualquier caso, Midway ya era un objetivo prioritario antes de estos acontecimientos. Yamamoto planeó capturar Midway, un pequeño atolón a unas 1.200 millas al oeste de Hawái. Con aquellas dos islas en sus manos, el perímetro de defensa de los japoneses crecía considerablemente y por lo tanto su posición se vería mejorada. En aquel proceso contaban además con asestar otro golpe importante a la flota estadounidense en el Pacífico. El líder japonés no sabía que los criptógrafos estadounidenses, para entonces, ya estaban capturando y leyendo sin muchos problemas parte de los mensajes cifrados con su código JN-25. Esto supuso la diferencia entre la victoria y la derrota, ya que permitió a los norteamericanos adelantarse a los movimientos. No obstante, aquel no fue un trabajo sencillo para los criptoanalistas y mostró, una vez más en la historia, cómo la imaginación y la inteligencia son elementos clave.

En la Estación HYPO, como se conocía al FRUPAC, la Unidad de Radio de la Flota del Pacífico, en Hawái, el comandante Joseph J. Rochefort lideraba el equipo que peleaba contra el JN-25, el código naval japonés. Rochefort acabó en el mundo de la criptografía de manera curiosa, ya que fue su afición a los crucigramas lo que lo provocó. Compartía ese interés con un mando de la nave en la que había servido unos años antes, en 1925, y cuando a aquel mando de la marina, Chester C. Jersey, le preguntaron por personas adecuadas para trabajar con códigos, se acordó de Rochefort. Esto da una idea de la precaria situación de los servicios criptográficos estadounidenses antes de la guerra.

El equipo de Rochefort, en mayo de 1942, descifró parcialmente un mensaje japonés en el que aparecía el texto «fuerza de invasión», y un indicador geográfico al que los japoneses llamaban AF. Una de las posibilidades era que AF fuera Midway, pero si no se sabía con certeza, los movimientos podían ser inútiles y, en el peor de los casos, dejar en mala situación al objetivo real.

Nimitz, responsable de la flota estadounidense en el Pacífico, era uno de los convencidos de que Midway era el objetivo. De hecho, envió órdenes para que tres portaaviones se movieran a la zona y canceló las anteriores a los submarinos con base en Midway para centrarse en el lugar. En el otro lado estaba el mando del OP-20-G, la unidad dedicada a la inteligencia de señales y la criptografía dentro de la marina estadounidense. Desde su sede en Washington creían que los objetivos eran otros, quizás Hawái, Alaska o las Aleutianas, e incluso dudaban de que AF hubiera sido bien descifrado y creían posible que la referencia geográfica fuera en realidad otra cuestión.

En esta situación, y con el tiempo corriendo en su contra, Nimitz convocó una reunión a finales de mayo para tratar el tema. Apostar por la teoría de Rochefort, Midway, supondría dejar desprotegido Hawái, y, por lo tanto, si se equivocaba, el precio podía ser elevado. Uno de los miembros de la Estación HYPO, Jasper Holmes, había trabajado en Midway durante un tiempo y sabía que toda el agua potable de la isla provenía de una única planta desalinizadora. Tuvo una idea para corroborar la teoría de su grupo, el grupo de Rochefort. Por supuesto, la pusieron en marcha. Desde HYPO enviaron un mensaje por cable submarino a Midway con una petición. Desde la isla tenían que enviar una alerta sin encriptar, perfectamente en claro, y con el objetivo de que los japoneses la leyeran. El mensaje de alerta debía indicar que la planta desalinizadora de Midway se había estropeado y que en unos días tendrían problemas por falta de agua potable.

Dos días después de que el mensaje de alerta fuera enviado desde Midway, en la Estación HYPO se capturó y descifró una nueva comunicación enemiga. Los japoneses sabían que AF tenía problemas con su suministro de agua, y lo comunicaban a sus unidades. Esto confirmaba que AF era Midway y por lo tanto colocaba a Estados Unidos en disposición de adelantarse al movimiento. Para que los japoneses no sospecharan que todo aquello era un engaño, como efectivamente era, desde Hawái se respondió al mensaje de Midway, poco después, asegurando que la ayuda para solucionar el problema del agua potable estaba en camino.

Cuando se descifró otro mensaje japonés en la Estación HYPO, y Rochefort lo puso en manos de Nimitz y del resto de mandos navales, la balanza bajó otro poco de su lado. Este nuevo mensaje estaba fechado el 26 de mayo y ordenaba a algunas de las naves que partieran de Saipán el día 28 y navegaran a 11 nudos de velocidad, para llegar a Midway el 6 de junio.

La reunión de Nimitz con sus colaboradores, donde todo esto se puso sobre la mesa fue el 27 de mayo, y ese mismo día la marina japonesa cambió su libro de códigos y además impuso el silencio en las comunicaciones por radio en la flota que se movía hacia Midway. Aquello dejaba sordos a los criptoanalistas estadounidenses, pero estos ya tenían información suficiente para jugar con ventaja.

El 3 de junio de 1942 un avión estadounidense localizó la fuerza japonesa y así comenzó la batalla de Midway, una de las batallas claves de la Segunda Guerra Mundial, en la que, de nuevo, la criptografía otorgó una ventaja clave al vencedor. La guerra del Pacífico sufrió un punto de inflexión y la derrota fue devastadora para Japón, que además de no conseguir su objetivo, perdió cuatro portaaviones y más de 250 aviones, además de miles de hombres. Las pérdidas del bando aliado, en cambio, fueron muchísimo menores: un portaaviones, un destructor, menos de 150 aviones y unos tres centenares de vidas.

Entre los códigos rotos por los aliados dentro del teatro de operaciones del Pacífico, estaba el usado por los mercantes japoneses, el código S, que les permitió a partir de 1943 conocer las rutas y los planes de navegación, las fechas y los destinos de los convoyes y barcos enemigos. La Unidad de Radio de la Flota del Pacífico, FRUPAC, desde su base en Hawái, decodificaba las señales cifradas de los convoyes japoneses e informaba al centro de mando de los submarinos estadounidenses en el Pacífico. En esas señales estaba la información sobre la ruta y en qué punto esperaban estar al mediodía de la siguiente jornada, por lo que los estadounidenses tenían fácil la caza de sus objetivos. De igual forma a lo que pretendía la Ubootwaffe con los británicos, estos ataques a los convoyes japoneses buscaban cortar el abastecimiento y soporte de su enemigo, que se llevaba a cabo básicamente a través de las rutas marítimas que conectaban las diferentes islas bajo su control.

La penetración progresiva en los códigos japoneses a lo largo de la guerra sirvió en no pocas ocasiones para que los estadounidenses se adelantaran a su enemigo y para que tomaran mejores decisiones. Por ejemplo, poco después de que MacArthur invadiera Leyte, la captura de algunos mensajes permitió la destrucción de las tropas de refuerzo japonesas que se dirigían hacia allí. Durante la campaña de Okinawa se interceptaron las órdenes dirigidas al buque japonés *Yamato* , permitiendo a los aliados prepararse para el ataque. El FRUPAC también jugó un papel vital en la operación Venganza.

Casi en la misma medida en la que era un héroe para los japoneses, el almirante Yamamoto era objeto del odio de sus enemigos. En la primavera de 1943 el jefe japonés decidió viajar hasta Rabaul, en el este del mar de Bismarck, para encargarse personalmente de la situación, cada vez peor para su país, en la batalla en torno a las islas Salomón. Japón había sido expulsado de Guadalcanal y sus líneas de suministro estaban cada día más amenazadas, por lo que Yamamoto esperaba organizar un ataque aéreo clave contra los aliados que revertiera la situación o al menos aliviase la de su ejército. Como parte de los preparativos para esta ofensiva aérea, el almirante se propuso hacer un vuelo sobre las islas Salomón e inspeccionar las bases en la zona. También quería levantar la moral de sus pilotos. Las bases japonesas que iba a visitar Yamamoto fueron avisadas de su llegada para que estuvieran listas.

El 13 de abril, el comandante de la Octava Flota japonesa envió un mensaje con los detalles del itinerario que iba a seguir Yamamoto en su viaje de cinco días por las bases, entre cuyos destinos estaban varias unidades aéreas y bases de mando. Precisamente por la variedad de destinatarios del mensaje, en todas esas bases, el código usado para codificar el mensaje por el emisor fue uno de los más generales y distribuidos entre el ejército japonés, en lugar de usar alguno propio de la armada o uno de menor uso. De otro modo, quizás alguno de los receptores del mensaje habría tenido problemas para decodificarlo.

Como bien sabemos, cuanto más común y utilizado es un código más probabilidades hay de que se vea comprometido, ya que no hay nada mejor para un criptoanalista que enormes cantidades de texto codificado. El código usado era uno de los más seguros, pero lamentablemente para Japón los aliados ya lo habían roto y eran capaces de leer sin problemas los mensajes capturados y codificados con ese código. El código había sido actualizado el día 1 de aquel mes de abril, pero a pesar de ello no era ya seguro.

Tras ser interceptado por los aliados, el mensaje fue roto gracias a las máquinas IBM que los criptoanalistas tenían a su disposición. Que el mensaje tuviera un gran número de destinatarios lo convirtió al momento en objeto de interés y por ello fue entregado, para su traducción, a uno de los más capaces entre los traductores que se encargaban de pasar al inglés los mensajes interceptados a los japoneses, el teniente coronel Alva Bryan Lasswell, que había estudiado japonés en Tokio y que desde 1941 formaba parte de la inteligencia estadounidense. Su experiencia y conocimientos ayudaron a completar la descodificación del mensaje y con la ayuda de otros hombres acabó por comprender hasta las referencias geográficas del texto, donde varias islas de las Salomón estaban codificadas como RXZ o RXE, y RR era Rabaul. Con toda esa información debidamente contrastada, se entregó finalmente el mensaje en inglés a los mandos del ejército para que actuaran en consecuencia. El texto del mensaje era el siguiente:

El comandante en jefe de la Flota Combinada inspeccionará Ballale, Shortland y Buin de acuerdo a lo siguiente. (Primero) A las 06.00 salida desde Rabaul a bordo de un avión y escoltado por seis cazas. A las 08.00 llegada Ballale. Inmediatamente salida hacia Shortland a bordo de un submarino (Fuerza de la 1.ª Base, prepara una nave), llegada a las 08.40. Salida de Shortland a las 09.45 a bordo de dicho submarino, con llegada a Ballale a las 10.30. Para propósitos de transporte, tengan preparadas una lancha de asalto en Shortland y una lancha motora en Ballale. A las 11.00 salida de Ballale a bordo de un avión y llegada a Buin a las 11.10. Comida en el Centro de Mando de la Fuerza de la 1.ª Base. El oficial a cargo de la Flotilla Aérea número 26 debe estar presente. A las 14.00 salida de Buin en un avión y llegada a Rabaul a las 15.40. (Segundo) Procedimientos de inspección. Después de que sea brevemente presentado el estado actual, las tropas y pacientes en el hospital de la Fuerza de la 1.ª Base serán visitados. En cualquier caso, no habrá interrupciones en las obligaciones rutinarias diarias. (Tercero)

Los uniformes serán los uniformes del día excepto para los oficiales al mando de las diferentes unidades, que vestirán el atuendo de combate con las condecoraciones. (Cuarto) En el caso de inclemencias meteorológicas, la visita se pospondrá un día.

El almirante Yamamoto tenía fama, al parecer bien ganada, de ser un hombre muy estricto con la puntualidad y, como podemos comprobar, su agenda estaba casi planificada al minuto. Aquel mensaje por tanto tenía un detallado itinerario y horario de uno de los hombres más importantes del ejército japonés, que durante unas horas iba a estar muy cerca de la primera línea de combate y por lo tanto del enemigo, posiblemente tan cerca como no había estado en toda la Segunda Guerra Mundial. Aquella era una gran oportunidad, aunque la decisión a tomar no era para nada sencilla.

El almirante Nimitz, el máximo responsable de la flota estadounidense en el Pacífico, sabía que acabar con Yamamoto sería un hito y un gran golpe para la moral de su enemigo, pero también se debía tener en cuenta quiénes podrían ser los sucesores de Yamamoto una vez eliminado y si el papel de estos sería favorable o desfavorable para el desarrollo general de la guerra. El almirante japonés era el líder indiscutible de la armada japonesa y sus hombres lo habían idealizado. En palabras de Mitsuo Fuchida, el hombre que mandó la primera oleada del ataque a Pearl Harbor, si al comienzo de la guerra se hubiera hecho una votación entre los oficiales de la armada japonesa para decidir quién sería el hombre que debería dirigirlos como comandante en jefe de la flota, hay pocas dudas de que Yamamoto habría ganado por una aplastante mayoría. Además de este liderazgo entre sus hombres, el almirante era definido por los estadounidenses como agresivo, directo, decidido, con gran fe en la capacidad de la fuerza aérea para avanzar en la guerra y capaz de diseñar imaginativos planes y llevarlos a cabo sin dudar. Analizados los posibles sustitutos para el cargo, la conclusión de los aliados fue que cualquiera de ellos sería inferior a Yamamoto y por lo tanto favorable a sus intereses. Se trazó, un plan para acabar con Yamamoto aprovechando la oportunidad que la criptografía había puesto a disposición de los estadounidenses.

El área que iba a visitar el japonés estaba, en el lado aliado, bajo el mando del almirante William Halsey, al que Nimitz envió un mensaje del máximo secreto explicándole los planes de Yamamoto, el detalle de su viaje y dándole autorización para derribar los aviones japoneses en los que se esperaba que estuviera el objetivo, siempre que tuviera capacidad para hacerlo. Halsey estaba en aquel momento en Australia y el mensaje fue recibido por su sustituto en el puesto, el vicealmirante Theodore S. Wilkinson, que respondió a Nimitz comunicándole que tenía capacidad para llevar a cabo la misión, pero que habría que tener en cuenta que la operación pondría de manifiesto para los japoneses que Estados Unidos había roto sus códigos, por lo que sus comunicaciones no eran secretas. Probablemente, tras el ataque contra Yamamoto, los japoneses cambiarían sus códigos y por lo tanto sus comunicaciones volverían a ser seguras y los estadounidenses quedarían ciegos durante

un tiempo, hasta que volvieran a romper el nuevo código, y ese tiempo era difícil de prever. Wilkinson planteaba la duda sobre si acabar con un solo hombre merecía un precio tan alto. Tras algunas discusiones y análisis, Nimitz y sus colabores directos decidieron que el riesgo merecía la pena y que el plan para acabar con Yamamoto debía seguir adelante, aunque tejieron una historia que sirviera de pantalla para los japoneses y les llevara a encontrar otra explicación al ataque, más allá de poner en cuestión la seguridad de los códigos criptográficos que usaban para hacer seguras sus comunicaciones. Además, los criptoanalistas aliados estaban convencidos de que, llegado el peor de los casos, lo único que harían los japoneses para mejorar sus códigos sería desarrollar una nueva versión de su código JN-25, algo que ya habían hecho en otras ocasiones.

El plan de cobertura para hacer creer a los japoneses que el fallo de seguridad estaba en otro punto se basó en los guardacostas australianos. Se haría creer que los guardacostas, que mantenían una buena reputación, habían obtenido la información sobre los movimientos de Yamamoto de alguno de los nativos de la zona de Rabaul afines a los americanos y que la habían enviado por radio al ejército aliado. Si los japoneses se enteraban de algún modo de aquella historia, quizás siguieran confiando en sus códigos. En cualquier caso, no se iba a detener el plan para acabar con Yamamoto y la comunicación final que envió Nimitz a Wilkinson tenía tres partes. En la primera le hacía partícipe de la historia de cobertura y le pedía que llegado el momento se la diera a conocer a todo su personal, esperando que de algún modo fuera filtrada al enemigo. Por otra parte, se ratificó en la autorización, que en realidad era una orden, para llevar a cabo el ataque a los aviones de Yamamoto y, por último, le deseaba buena suerte y buena caza.

En la tarde del 17 de abril de 1943, dos hombres del ejército del aire de Estados Unidos fueron informados en Guadalcanal de la misión y se les entregó un documento, de máximo secreto, con el itinerario que iba a seguir el almirante japonés. Acabar con él mientras cruzaba por el mar entre Ballale y Shortland fue descartado por lo complicado de identificar la lancha exacta en la que viajaba el objetivo. Por lo tanto, el plan sería acabar con él derribando el avión en el que debía viajar. La acción tenía como base la puntualidad de Yamamoto y por lo tanto que este ajustara sus movimientos a la agenda inicialmente trazada por sus asistentes y compartido con las bases que iba a visitar, que era la información que tenían los aliados.

Los pilotos estadounidenses manejaban cazas Lockheed P-38 Lightning, cuya autonomía les permitía llegar hasta Ballale, pero estaba casi en el límite de la misma, incluso con dos tanques extra de combustible que se podían incorporar a los aparatos, por lo que no tendrían mucho margen de maniobra ni tiempo para esperar a que Yamamoto decidiera comenzar su vuelo. El mensaje capturado indicaba que la llegada a Ballale sería a las 08.00, tras dos horas de vuelo, pero según los cálculos de los estadounidenses el avión Mitsubishi que usaría para

llegar hasta allí desde Rabaul tardaría una hora y cuarenta y cinco minutos en completar el recorrido. Ese cálculo encajaba además con otra de las partes del mensaje, que indicaba que tardarían una hora y cuarenta minutos en volar desde Buin de vuelta a Rabaul, un viaje poco más corto que el inicial de Rabaul a Ballale. Aquello significaba que a pesar de lo que afirmaba el mensaje capturado, probablemente Yamamoto llegaría a Ballale quince minutos antes de las 08.00. En el plan daba por hecho que seis aviones escoltarían al del almirante japonés y se determinó el mejor punto para el ataque, teniendo en cuenta las zonas en las que podría haber patrullas niponas, como las cercanías de Buin. Tras todos los análisis, se estableció como hora para el ataque las 07.35, por el lugar en el que se encontraría el avión objetivo en ese momento.

Unas horas después de cerrar el plan, dieciocho aparatos P-38 Lightning despegaban desde el aeródromo Henderson en Guadalcanal, que originalmente había sido construido por los japoneses y cuya toma en octubre de 1942 fue tan importante y dura dentro de la campaña que tiene su propio nombre. La toma se conoce como la batalla por el Campo Henderson. Eran las 07.25 para los americanos y las 05.25 para los japoneses, por lo que faltaban aún algo más de dos horas para el ataque, dos horas de vuelo hasta el objetivo. Treinta y cinco minutos después Yamamoto comenzaba su viaje, fiel como un reloj a su agenda. Los aviones aliados viajaban sin hacer uso de la radio y a baja altura, para no ser detectados por el radar enemigo, volando en semicírculo desde el este hacia el oeste, a unos setecientos kilómetros de las costas de Nueva Georgia, en el suroeste de las islas Salomón. Con una brújula y el indicador de velocidad del avión, los norteamericanos fueron trazando la ruta circular que les llevó tras dos horas y nueve minutos de vuelo a divisar las costas de la isla de Bougainville, donde llevarían a cabo su ataque. La puntualidad y el reloj eran la clave de la operación, ya que el plan se sustentaba en que dos grupos de aviones que partían a más de mil cien kilómetros de distancia y con rutas distintas se encontraran en un punto sobre el océano. Y casi para sorpresa de los aliados, cuando estaban frente a Bougainville, el escuadrón de aviones en el que viajaba Yamamoto apareció en el cielo, a unos ocho kilómetros, como una pequeña mancha negra. El almirante viajaba en un bombardero, acompañado por otro bombardero G4M y escoltados ambos por tres cazas Zero.

Yamamoto fue una de las bajas del combate, pero aún quedaba la comprobación oficial de su muerte, ya que, al haberse estrellado los aviones, era algo muy probable, pero no seguro. En la jungla de Bouganville, al día siguiente del ataque, los japoneses localizaron el punto en el que se había estrellado el avión de Yamamoto y cuando llegaron hasta el aparato encontraron al almirante en su asiento del avión, perfectamente sentado y aferrado con sus guantes blancos a la empuñadura de su catana. Había fallecido. El cuerpo del japonés fue incinerado y el 21 de mayo Japón hizo pública la pérdida de su líder, aunque omitió los detalles y se habló de una muerte en combate. Tal y como Nimitz y sus colaboradores habían previsto, la muerte de Yamamoto dejó consternado al pueblo japonés y a su ejército. El 5 de

junio, sus cenizas recibieron sepultura en Tokio, en una ceremonia en la que estuvo presente el gobierno nipón y en la que, a pesar de las semanas que habían transcurrido desde su muerte, el silencio y la tristeza estuvieron omnipresentes. Mineichi Koga, que fue nombrado sucesor de Yamamoto como comandante en jefe de la Flota Imperial japonesa, dijo tras su muerte que solo existió un Yamamoto y que nadie sería capaz de reemplazarlo, asegurando también que su pérdida era un golpe insoportable para Japón.

El informe estadounidense sobre la operación, escrito una vez concluida, seguía tratando el asunto como un gran secreto y solicitaba expresamente que no se diera a conocer ningún detalle sobre el hecho. El objetivo era hacer dudar a Japón incluso de si el ataque no había sido una mera casualidad, un encuentro rutinario en la zona de combate que por suerte para los aliados había tenido unas consecuencias enormes. Así, la opinión pública estadounidense se enteró del hecho gracias al comunicado del ejército japonés.

Unas semanas después de la operación Venganza contra Yamamoto, uno de los hombres que sería clave en la historia de Estados Unidos en las décadas siguientes estuvo envuelto en una situación complicada, donde también la criptografía tuvo su parte. El 1 de agosto de 1943, una lancha torpedera estadounidense fue atacada por el destructor japonés *Amaqiri* y la partió en dos. La lancha fue dada por perdida, hasta el punto de celebrarse un oficio religioso en honor de sus tripulantes. Pero la tripulación había sobrevivido y consiguió llegar a un islote. Por la noche, uno de sus tripulantes salió nadando al mar para avisar a algunas de las embarcaciones que pasaban por allí, cerca de la costa. Ese nadador era John Fitzgerald Kennedy, el que más tarde sería presidente de Estados Unidos y que acabaría asesinado en Dallas en 1963.

No fue capaz de contactar con ninguna lancha, por lo que regresó nadando hasta el islote, aunque la corriente lo desvió. Cuando volvió a contactar con sus compañeros, trataron de hacer saber que estaban allí, perdidos en un islote, pero con vida. Algunos australianos vigilaban la zona desde posiciones elevadas y habían visto en el estrecho de Blackett, en las islas Salomón, el fuego provocado por el hundimiento de la lancha torpedera. El grupo de Kennedy utilizó el cifrado Playfair, que también era conocido por los australianos, de hecho, era el método de cifrado que solían utilizar, para enviar un mensaje.

La palabra clave, lógicamente, no había sido acordada con anterioridad, por lo que los norteamericanos confiaban en la imaginación de los australianos. Estos probaron con la clave ROYAL NEW ZEALAND NAVY y así pudieron leer el texto en claro: «Lancha PT 109 perdida en acción en Estrecho Blackett dos millas SO Cala Meresu X Grupo de 12 X Pidan cualquier información».

El vigilante australiano comunicó en su escala de mando el mensaje descifrado para que se tomaran las decisiones correspondientes. El

problema principal era que la posición de los estadounidenses estaba tras las líneas enemigas. Los mensajes sobre el grupo de soldados que estaba oculto en la zona japonesa, el grupo de Kennedy, se intercambiaron durante varios días y entre varios puestos australianos, a pesar de lo cual los japoneses no hicieron nada por buscarlos y hacerlos prisioneros. Quizás los japoneses no estaban capturando esos mensajes, o no eran capaces de descifrarlos. También es cierto que ninguno de los mensajes mencionaba la posición exacta, lo que quizás desincentivó a los nipones, que tendrían que buscar a los estadounidenses. Todas las comunicaciones seguían usando la sencilla cifra Playfair, y el número de mensajes y su longitud hubiera permitido descifrarlos sin mucho problema.

Es más, cuando se planeó el rescate, si los japoneses hubieran conocido los planes, podrían haber capturado a los estadounidenses y a los australianos en una sola operación, pero nada de esto ocurrió. La cifra Playfair fue suficiente para que las comunicaciones fueran seguras, en caso de que fueran capturadas, y Kennedy y los demás salieron de aquel trance sin más problemas.

25. Los Navajos en el ejército de Estados Unidos

Si bien a menudo la historia de la criptografía de la Segunda Guerra Mundial gira en torno a la ruptura de la seguridad de las máquinas de cifrado, tanto alemanas como japonesas, lo que es perfectamente lógico, ya que es el punto más relevante del conflicto, también es cierto que dichas máquinas eran relativamente seguras y cumplieron con su cometido. Fue la combinación de diferentes errores y malas costumbres en su uso lo que acabó haciendo que los criptoanalistas vencieran. Las máquinas Tipex y SIGABA, usadas por los británicos y por los estadounidenses, respectivamente, eran más complejas que las Enigma y su uso hizo que se mantuvieran seguras durante toda la guerra. Dicho esto, los estadounidenses pensaron que en determinadas situaciones no era práctico el uso de este tipo de máquinas, ya que su complejidad las hacía lentas para las necesidades del combate. Al final había que escribir el texto en claro, teclearlo en la máquina letra por letra, apuntar el resultado que esta generaba y luego hacer la comunicación. El proceso debía hacerse a la inversa en el lado receptor. Por esto, buscaron alternativas y recurrieron a soluciones más simples y antiguas, pero igualmente eficaces.

En Los Ángeles, en 1942, un ingeniero llamado Philip Johnston quería contribuir de algún modo a que su país venciera en la guerra, pero era demasiado mayor para alistarse. Empezó entonces a trabajar en un método de comunicación seguro. Johnston, que era hijo de un pastor protestante, había crecido en las reservas de indios navajos de Arizona, donde su padre ejercía su labor. Eso le había permitido conocer con suficiente detalle el idioma de esos indios. Tanto es así, que, siendo todavía un niño, acompañó a una delegación de navajos a la Casa Blanca, a la sazón habitada por Theodore Roosevelt, para servir de traductor y hacer llegar al presidente las peticiones de los indígenas. Johnston pensó que si los navajos acompañaban a las unidades del ejército norteamericano y las comunicaciones por radio se hacían entre ellos, dichas comunicaciones serían a todos los efectos secretas, ya que era casi imposible que algún japonés conociera aquella lengua. Por otra parte, los navajos tenían una lengua lo suficientemente rica como para cubrir las necesidades de palabras y expresiones más utilizadas. Un método tan sencillo como práctico, y que otorgaba la rapidez en batalla que el ejército demandaba. A lo largo de la historia se ha usado multitud de veces este tipo de trucos: una determinada lengua se ha utilizado para comunicarse de forma segura. En la Segunda Guerra Mundial volvió a hacerse, y con éxito.

Johnston le contó su idea a un oficial de señales en San Diego y le dijo varias palabras en navajo, para demostrar que era una forma de hablar tan alejada del inglés que nadie podría ni siquiera intuir qué significaba cada palabra. Se ganó el suficiente interés por parte del oficial como para que unos días después le permitieran hacer una demostración con

dos indios navajos. A uno de ellos se le entregaron unas frases en inglés y este las envío por radio, en navajo, a su colega, que llevó de nuevo el mensaje al inglés y lo entregó a los oficiales del ejército que supervisaban la prueba. Funcionaba a la perfección y se diseñó un plan para reclutar indios, entrenarlos e integrarlos en las unidades militares.

En un primer momento la decisión sobre la tribu de la que debían provenir los hombres no estaba tomada, ya que era clave que fuera cual fuera la elegida, debía haber un número suficientemente alto de ellos dispuestos a ir a la guerra. Además debían saber inglés y estar alfabetizados, es decir, saber escribir y leer. Las cuatro tribus más numerosas eran las candidatas obvias: navajos, sioux, chippewa y pima-papagos. Los primeros eran lo más numerosos, pero los que tenían un índice de alfabetización más bajo, mientras que los últimos, los pima-papagos eran los mejor formados, pero los menos numerosos. Lógicamente, se podía trabajar o solventar de alguna forma el problema de la alfabetización, pero era imposible sacar más hombres de una tribu de la noche al día. Por lo tanto, los seleccionados fueron los navajos. Por otra parte, esta tribu había tenido muy poco contacto con el mundo ajeno a ellos, mientras que en otras tribus incluso habían estado conviviendo con estudiantes de otros países, lo que podía suponer un problema en la seguridad, ya que alguien podía conocer su idioma.

Los navajos, por su parte, se mostraron dispuestos a colaborar sin reserva alguna con el ejército de Estados Unidos. Tan solo unas pocas semanas después del ataque a Pearl Harbor, veintinueve indios navajos comenzaron la formación sobre comunicaciones dentro de la Infantería de Marina. La formación de los navajos también incluyó el uso de algunas de sus palabras para referirse a términos militares habituales en aquel momento. Los norteamericanos habían aprendido lo que puede suponer este problema durante la Primera Guerra Mundial, cuando una unidad militar que combatió en Europa, utilizó a ocho indios de la tribu choctaw como operadores de radio, precisamente con la intención de que hablaran en su propio idioma y conseguir la misma seguridad, sencillez y rapidez en las comunicaciones que se buscaba ahora, en la Segunda Guerra Mundial, con los navajos. El problema con los choctaw fue que su idioma no tenía expresiones o palabras para muchos de los términos militares correctos, y por lo tanto los mensajes eran ambiguos o daban lugar a equivocaciones.

La formación que se dio a los navajos buscaba solventar este problema. Se tomaron palabras comunes en el idioma navajo y que se referían a animales o plantas presentes en la naturaleza, pero sin relevancia en la guerra, y se les dio nuevo significado. Así, colibrí quería decir avión caza, el águila ratonera era un bombardero, la ballena un acorazado… De igual forma, los pelotones se nombraban como clanes de barro en el idioma navajo, las fortificaciones como cuevas, y así se fue completando el nuevo diccionario para la guerra moderna dentro del idioma de esos indios.

En cualquier caso, como habitualmente pasa con los nomenclátores y los códigos, donde por muy largo que sea el diccionario siempre hay palabras que quedan fuera y que puede ser necesario utilizar en algún momento, se hubo de idear una solución para hacer posible la comunicación de cualquier palabra y expresión sin abandonar ese idioma navajo. La solución fue crear un alfabeto fonético, donde cada letra correspondía a una palabra, siendo aquella la primera de la propia palabra. Estas palabras sí podían ser dichas en navajo y por lo tanto cualquier mensaje que se quisiera decir, cualquier secuencia de letras, al fin y al cabo, podría ser comunicada como una secuencia de palabras. La A, por ejemplo, correspondía a la palabra inglesa Ant (hormiga en castellano) y en navajo se decía Wol-la-chee. La B se indicaba usando la palabra en navajo para Bear (oso en castellano), que en navajo se decía Shush. Así, si un navajo recibía el siguiente mensaje: *Wol-la-chee Than-zie Wol-la-chee Moasi Klizzie-yazzi* , lo traduciría al inglés como: *Ant Turkey Turkey Ant Cat Kid* , y por lo tanto el mensaje sería *attack* , es decir, atacar. Las palabras seleccionadas eran palabras muy comunes en navajo y en inglés, en el ejemplo: hormiga, pavo, pavo, hormiga, gato y chico.

Cualquier lector que haya llegado a este punto del libro se habrá dado cuenta de la falta de seguridad que supone esta forma de envío de las palabras extrañas para los navajos, donde cada letra se codifica y se manda siempre de la misma forma. Más allá de las complejidades de la transcripción o del entendimiento de las palabras, es obvio que un análisis de frecuencia simple daría al traste con la seguridad, ya que permitiría identificar a qué letra corresponde cada palabra en navajo sencillamente por el número de veces que aparece. Con el fin de evitar esto, el método de codificación creado para los navajos tenía varios homófonos para algunas de las letras, esto es, varias palabras que correspondían a una letra. El uso alternativo de esas opciones hacía algo más segura esa parte de las comunicaciones que no podía hacerse directamente en navajo y que debía deletrearse siguiendo este código.

Los soldados navajos acabaron su formación y fueron examinados, ellos y el propio sistema, antes de enviarlos al frente y hacer descansar la seguridad de las comunicaciones en este método tan sencillo como, *a priori* , efectivo. La misma unidad de la Inteligencia Naval del ejército estadounidenses que había trabajado para romper Púrpura, tuvo varias semanas para enfrentarse a grabaciones de mensajes enviados según el método de los navajos, y no llegaron a entenderlos, ni siquiera a transcribirlos a texto. Aquello era la prueba definitiva de que cumplía con su cometido y veintisiete navajos, ya soldados, fueron enviados al frente integrados en cuatro regimientos que combatían en el Pacífico. Otros dos se quedaron en Estados Unidos para formar a los nuevos reclutas navajos que fueran llegando y aprovechar así todo lo aprendido tras aquel primer ciclo de formación.

En el verano de 1942, los japoneses estaban planificando la construcción de un aeródromo clave en la zona de Guadalcanal, lo que les daría control sobre una parte amplia del Pacífico. El 7 de agosto de

aquel año comenzó la campaña de Guadalcanal, donde los aliados trataban de impedir ese plan japonés, que de conseguirse pondría en serio peligro las líneas de abastecimiento logístico y por lo tanto complicaría la vida al ejército de Estados Unidos, principalmente, que tenía que dotar a sus tropas lejos de su territorio. En aquella campaña, cuyo nombre en clave era operación Torre Vigía, Watchtower, los navajos entraron por primera vez en acción en combate real y el resultado no fue bueno, aunque no porque el método de comunicación no fuera seguro. La cuestión fue que no todos los operadores de radio estadounidenses estaban al tanto de la existencia de los nuevos miembros en la red de comunicaciones y cuando empezaron a escuchar en sus radios un lenguaje que no reconocían ni por asomo, comenzó a correr la idea de que los japoneses estaban emitiendo en las frecuencias estadounidenses. El caos que se formó llevó a los mandos a poner en entredicho si los beneficios generados por el uso del idioma navajo compensaban malentendidos y problemas como los que habían vivido en aquellos primeros momentos. Pero el método navajo funcionaba y era seguro, además de muy rápido. Fue esto último lo que convenció a los más reticentes y poco a poco los comunicadores comenzaron a ser utilizados y se hicieron un lugar, cumpliendo con su cometido. Fueron llegando nuevos miembros, tras su formación en Estados Unidos, y los navajos se ganaron un gran respeto entre los soldados de los batallones en los que estaban integrados. Los que no contaban con ellos, en alguna ocasión los tomaron por enemigos y el malentendido solo se deshizo cuando alguien respondía por ellos.

De nuevo conviene recordar que cierto nivel de desconfianza es necesario y más que recomendable en caso de guerra, y especialmente cuando se trata el tema que nos ocupa, las comunicaciones cifradas. Así no es de extrañar que en alguna ocasión se llegara a dudar de casi todo. Hay una anécdota que ocurrió en la isla de Saipán y que muestra esto. Un grupo de soldados estadounidenses tomó las posiciones en las que habían estado los japoneses hasta poco antes y comenzaron a recibir fuego amigo por parte de compañeros que no sabían que esas posiciones habían sido tomadas. Las primeras comunicaciones por radio para alertar del problema, hechas en inglés, fueron tomadas por una estratagema de engaño japonesa y el fuego no se detuvo. Como decía, cierto nivel de recelo es bueno, aunque a veces se tenga que pagar un precio. Solo cuando un navajo entre los avanzados tomó la radio y emitió un mensaje, los atacantes se dieron cuenta de su error, ya que al momento concluyeron que no había estratagema japonesa posible que les llevara a imitar el idioma navajo.

Durante la batalla de Iwo Jima, ya en febrero de 1945, con la guerra en su recta final, más de 800 mensajes fueron enviados por los navajos, sin errores. Su papel fue relevante y cumplió su cometido. Al final de la Segunda Guerra Mundial más de 400 indios navajos habían formado parte del ejército en ese papel de emisores y receptores de las comunicaciones usando su propio idioma. Pasaron muchos años antes de que dicho papel fuera conocido y reconocido, ya que al finalizar la guerra se les prohibió hablar de lo que habían hecho, lógicamente, por seguridad y para mantener en secreto esa baza, esa forma de

comunicación que podría ser útil en otras ocasiones. Sería en 1968, más de dos décadas después de la guerra, cuando se desclasificara la documentación y se comenzara a reconocer su contribución.

26. La batalla del Atlántico y la balanza de la criptografía

Volviendo a Europa, en la carrera entre el uso de la máquina Enigma naval por parte de los alemanes y el trabajo de los aliados por descifrar sus mensajes, la balanza fue cambiando de lado varias veces a lo largo de la guerra. Las mejoras que introdujo la Kriegsmarine en la máquina y en su forma de uso obligaron a los británicos a emplearse al máximo para conseguir vencerla. Cuando los cifrados de la Luftwaffe, de la diplomacia o del ejército alemán eran ya vulnerables ante los británicos, las comunicaciones marítimas seguían siendo una caja negra para ellos. Y el problema estaba en que la batalla del Atlántico era determinante, y el estrangulamiento de la isla británica por los submarinos alemanes, actuando en grupo, evitando que los convoyes de suministros llegaran a su destino, era una estrategia que funcionaba. Las manadas de lobos de submarinos alemanes, usando la terminología habitual, alcanzaron por momentos un inmenso poder en el mar. Tanto es así que al verano y el otoño de 1940 se los denominaba, ya lo vimos, como los tiempos felices para esos submarinos, donde más de un millón y medio de toneladas fueron enviadas al fondo del océano. Más tarde hubo otros tiempos felices para los hombres de Karl Dönitz, en los que el miedo estaba en el lado aliado y las victorias en el bando alemán, con hombres como Otto Kretschmer, Wolfgang Lüth o Erich Topp al mando de los submarinos. Winston Churchill dejó escrito en su libro sobre la Segunda Guerra Mundial que la única cosa que realmente le asustó durante la guerra fue el peligro de los *U-boote* , los submarinos alemanes. Las mercancías y materias primas que llegaban a las islas británicas eran esenciales para la población y para que la maquinaria de guerra pudiera seguir funcionando, por lo que del mantenimiento de las rutas marítimas dependía seguir respirando o que el país de Churchill se viera abocado a la catástrofe final. En ese pulso el trabajo de Bletchley Park se volvió crítico. Conocer dónde estaban los submarinos permitía a los aliados pasar de la defensa al ataque contra ellos. Del miedo a que en mitad del océano apareciera de repente una estela blanca en el agua, a lanzar barcos con decenas de cargas de profundidad tras haber localizado un submarino.

Más allá de las rutas conocidas o habituales de los convoyes atlánticos, los submarinos alemanes patrullaban el océano durante semanas, buscando objetivos. Cuando detectaban uno de esos convoyes o algún objetivo jugoso, se desencadenaba una serie de comunicaciones que servía para convocar a otros *U-boote* y atacar en grupo. Un submarino podría hundir cuatro o cinco buques de un convoy, pero un grupo de submarinos podría llegar a superar los veinte objetivos abatidos, una pérdida insuperable para el convoy.

Lógicamente, estar tanto tiempo alejados de un puerto y la necesidad de comunicaciones entre ellos, hacían que el tráfico de señales fuera muy intenso. Por otra parte, estas naves pasaban gran parte del tiempo

sumergidas, lo que obligaba al centro del mando en tierra a repetir las señales de manera sistemática para que las naves pudieran recibir los mensajes saliendo a la superficie. Esto hizo que a pesar de que la Kriegsmarine mantuviera un estricto protocolo de seguridad en el uso de Enigma, que además la Ubootwaffe seguía con especial cuidado, los aliados tuviesen su oportunidad de romper el secreto. La versión de Enigma que usaba la marina se denominaba M4 y en marzo de 1941, aunque no de manera continua, los movimientos de los submarinos comenzaron a ser conocidos gracias a Bletchley Park, pues parte de sus mensajes eran descifrados. El hombre de aquel momento fue Francis Harry Hinsley, que se dedicó en cuerpo y alma en el cobertizo 4 a buscar una forma de poner sobre el mapa los puntos donde se encontraban los submarinos, aprovechando el análisis del tráfico de señales, aun sin saber el contenido de las propias comunicaciones. Hinsley, que era un joven estudiante de historia de Cambridge, se convirtió muy pronto, en los primeros meses de guerra, en el principal experto en Bletchley Park en la organización de la armada alemana, sus comunicaciones, sus grupos…

Su labor no era la más relumbrante, *a priori* , y sus informes a menudo pasaban desapercibidos. Pero en junio de 1940 detectó un aumento significativo de comunicaciones que parecían indicar un movimiento de naves desde el Báltico hasta Skagerrak, el estrecho que separa Noruega de la Península de Jutlandia. Avisos como aquel fueron poniéndole a la vista del Almirantazgo, que comprobaba lo útil de la información. El nombre de Hinsley ganó relevancia, llegando al punto de que en algunos casos se enviaban avisos desde el GC&CS en los que remarcarlo a él como la fuente era suficiente para que se tuvieran en cuenta.

Tras la toma de Francia por los alemanes, la base St. Nazaire, en la costa oeste de ese país, permitió que las patrullas de los submarinos partieran más cerca del Atlántico, obteniendo así una gran ventaja, más garantías y mayor tiempo de patrulla efectiva. Dönitz quería que todos los submarinos que se movían por el Atlántico le informaran puntualmente de su situación, de sus éxitos y de sus descubrimientos. De igual modo, el tráfico era continuo hacia el océano desde el centro de mando que Dönitz tenía en Villa Kerillon, en Lorient, en el oeste francés. Estas comunicaciones cifradas desde el centro de mando se repetían cada 2, 6, 12 y 24 horas, debido a que los submarinos pasaban tiempo sumergidos y por lo tanto sin capacidad para recibirlas.

Ya hemos comentado lo estrictos que eran en la marina alemana con el uso de las máquinas Enigma y sus protocolos, complicando así la vida a los criptoanalistas aliados. Tanto es así, que cuando un convoy aliado era avistado por un submarino, primero se codificaba el mensaje utilizando un libro de señales y luego ese mensaje se cifraba con Enigma. Para las comunicaciones de información meteorológica, que fueron claves para que Bletchley Park consiguiera su objetivo contra la marina enemiga, tenían un libro de códigos diferente. Este libro contenía grupos de letras para indicar cualquier variación de la longitud

y la latitud, así como información sobre la temperatura, la presión atmosférica, el viento…

La ocupación de Francia también permitió la captura de más tráfico de información por los alemanes, y dado que podían leer parte de los mensajes codificados por la marina británica y por los barcos mercantes aliados, a menudo los convoyes atlánticos estaban casi condenados. Los británicos y norteamericanos tardaron en darse cuenta de este problema, pero finalmente repararon en ello, fueron conscientes de que sus códigos habían sido comprometidos. La confirmación llegó de la forma más directa. En marzo de 1943, dos importantes convoyes, el HX-237 y el SC-129, salieron de puertos de Nueva York y de Terranova y poco después se interceptaron las comunicaciones de Enigma que situaban dos grupos de submarinos listos para atacarlos. Se envió a los barcos la orden de variar la ruta para evitar a los submarinos alemanes, pero esos mensajes también fueron capturados y descifrados por el B-Dienst alemán, por lo que las dos manadas de lobos nazis modificaron sus posiciones en busca de los convoyes. En Bletchley Park se dieron cuenta de que las nuevas posiciones que el mando aliado había enviado a los convoyes, eran remitidas por los alemanes a sus submarinos poco después. La conclusión era obvia, de igual forma que ellos leían los mensajes alemanes, estos habían roto los códigos aliados. Es más, en aquel momento, en marzo de 1943, la Enigma de la marina era descifrada por Bletchley Park, pero durante mucho tiempo esto no había sido así. Y en ese tiempo pasado, los alemanes sí conocían los códigos británicos. El resultado de la batalla de los submarinos alemanes contra los convoyes HX-237 y SC-129 se saldó con 22 barcos hundidos, con la pérdida de casi 150.000 toneladas y la muerte de unos 300 hombres. Sumando ambos convoyes, la batalla involucró a 90 mercantes y 16 buques de escolta por un bando y 38 submarinos por el otro, de los que tan solo uno se fue al fondo.

Un detalle interesante es la diferencia entre la forma en la que los británicos conocieron la inseguridad de sus códigos y lo que ocurrió en el bando contrario. Como hemos visto, interceptar mensajes enemigos con información propia fue clave para que los aliados repararan en su inseguridad. Los alemanes, en varias ocasiones, se plantearon la posibilidad de que sus máquinas Enigma no fueran seguras, y como hemos comentado, frente a las sospechas, incluían mejoras en la propia máquina o en su uso. Pero una de las razones por las que siguieron confiando en sus Enigma fue que, según ellos mismos, deberían ver en los mensajes que interceptaban a los británicos información proveniente de la captura de sus comunicaciones con Enigma, y eso no ocurría. Esto fue, en gran medida, virtud del buen uso que se hizo de ULTRA. Otro detalle interesante es que los alemanes sabían que los británicos usaban libros de códigos de manera general. Eso les llevaba a pensar que, si no usaban máquinas como sus Enigma, era porque no tenían capacidad para desarrollarlas e implantarlas. Si esto era así, no podrían tampoco desarrollar un método de ruptura de sus Enigma, ya que la tecnología necesaria para ello debería ser muy avanzada. Pero lo cierto es que tanto los británicos como los estadounidenses sí usaron máquinas de rotores, y las utilizaron bien. Las Tipex fueron una herramienta del

ejército y la fuerza aérea británica, y los estadounidenses usaban máquinas SIGABA.

Uno de los hechos importantes de la batalla del Atlántico ocurrió curiosamente lejos de allí, en el Mediterráneo. El 30 de octubre de 1942, en Port Said, en Egipto, un avión de reconocimiento de la RAF localizó al submarino alemán *U-559* . Los buques británicos acudieron a la zona del avistamiento para atacar a la nave, que trató de defenderse, como era habitual, sumergiéndose todo lo posible y esperando que las cargas de profundidad no acabaran con él. El *U-559* no tuvo suerte y se vio obligado por el ataque a salir a la superficie. Desde el *HMS Pettard* se enviaron varios hombres para recuperar del submarino, en estado ya muy maltrecho, toda la información secreta que pudieran. En esta tarea tuvieron éxito, pero el submarino acabó por irse al fondo con dos británicos dentro. Entre la información confidencial que lograron recuperar estaban los libros de códigos que utilizaba la Ubootwaffe para enviar los informes meteorológicos. Los submarinos enviaban todos los días información sobre su posición y la meteorología a la que estaban sometidos. Este libro de códigos fue vital en Bletchley Park. Lógicamente, no porque les permitiera conocer el contenido de esos informes meteorológicos, sino porque estos eran muy repetitivos, es decir, había muy pocas palabras que se repetían de manera recurrente: lluvia, fuertes vientos, temperatura… Estas palabras habituales eran perfectas para que las Bombes las buscaran en los textos cifrados y descubrieran las configuraciones de las máquinas. Una vez descubiertas estas, se podían descifrar mensajes con información mucho más relevante. Gracias a aquella captura del *U-559* , en diciembre de 1942 se podían volver a leer los mensajes cifrados enviados por los submarinos. La clave Shark, como denominaban en Bletchley Park a la usada por los submarinos alemanes, que estos llamaban a su vez Tritón, se podía descifrar.

Este hecho, sumado a que los británicos, conscientes de que sus códigos habían sido comprometidos, los habían modificado, hizo que la situación en la batalla del Atlántico cambiara de forma definitiva. Ahora los alemanes no sabían por dónde se movían los convoyes, pero los británicos sí sabían la localización de los submarinos. En abril de 1943, el convoy SC-127, formado por 57 barcos, partió de Nueva Escocia rumbo a Inglaterra, cargado con armas, explosivos, acero, alimentos… En la ruta que habría seguido de manera natural, había algunos submarinos esperando, pero tras ser localizados por Bletchley Park, se ordenó modificar la ruta del convoy. Ahora los alemanes no eran capaces de conocer esos cambios porque habían perdido la capacidad de leer los códigos británicos, y gracias a todo ello el convoy llegó hasta su destino sin perder un solo barco.

Conocer el lugar en el que estaban los submarinos no solo permitía evitarlos, sino que también hacía posible enviar a la aviación, especialmente, y a otros buques a atacarlos. Una muestra de esto es que fueron hundidos los 14 enormes submarinos de tipo XIV, los conocidos como vacas lecheras, que servían para llevar suministros y combustible

a otros submarinos y así evitar que estos tuvieran que volver a su base en tierra. Entre mediados de diciembre de 1943 y mediados de enero de 1944, diez convoyes cruzaron el Atlántico y ninguno fue atacado por los submarinos alemanes. En los siguientes dos meses de 1944, casi 3.500 barcos llegaron a su destino y tan solo tres fueron hundidos por los alemanes. Un resultado muy distinto al de aquellos tiempos felices de la Ubootwaffe que pusieron en jaque al bando aliado. Los alemanes no fueron capaces de volver a romper los códigos británicos, entre otras razones porque las dotaciones de personal dedicadas a ello cayeron de forma alarmante, ya que cada vez se necesitaban más hombres en el campo de batalla y había menos recursos.

La colaboración entre los británicos y los estadounidenses fue clave para que la guerra criptográfica pudiera llevarse a cabo al ritmo necesario. Llegó un momento en que los británicos sabían qué tenían que hacer y cómo, pero el trabajo era demasiado y los recursos cada vez más escasos. Alan Turing viajó a Estados Unidos a finales de 1942 y la OP-20-G comenzó a trabajar en la creación de las Bombes, poniendo sobre la mesa todos sus recursos, lo que aceleró sobremanera la disponibilidad de las máquinas. El plan consistía en la creación de 336 máquinas para poder acometer con garantías de éxito el descifrado de los mensajes de los submarinos alemanes. Turing compartió las conclusiones e ideas que habían estado generando en el otro lado del Atlántico y el resultado fue un éxito. El intercambio de conocimientos generales, de experiencias, así como de información concreta, hizo que la alianza entre Estados Unidos y Europa potenciara aún más las ventajas que estaban obteniendo de la criptografía.

27. Colossus contra Tunny

Aunque parezca que el éxito en Bletchley Park fue algo continuo y que los aliados conocían con detalle los planes enemigos, lo cierto es que durante la guerra gran parte del tráfico cifrado alemán capturado presentaba problemas para resolverlo y, en ocasiones, cuando se conocía el texto del mensaje, ya era información poco útil por haber pasado demasiado tiempo. Como ya hemos comentado, diferentes entidades dentro de la maquinaria de guerra alemana tenían diferentes versiones de Enigma, distintos protocolos, costumbres de uso… y no siempre el trabajo en Bletchley Park fue un éxito.

Las comunicaciones entre Hitler y sus generales se cifraban utilizando la máquina Lorenz SZ40, un dispositivo más avanzado que la Enigma, con una mayor complejidad y que en lugar de usar morse eran máquinas tipo teletipo. Había comenzado a utilizarse en 1941 y tenía 12 rotores, funcionaba en binario y esa tecnología de teletipo le permitía enviar por radio el mensaje una vez cifrado. El mensaje llegaba del mismo modo y era impreso en el lado del receptor. Había muchas cosas que cambiaban con respecto a Enigma y esos cambios hacían de la SZ40 una máquina más segura para los alemanes y un reto mucho mayor para los criptógrafos aliados. Su uso por parte del máximo nivel jerárquico alemán la convertía en una fuente potencial valiosísima, con información estratégica y sobre las decisiones y planes más importantes.

Los criptógrafos británicos la conocían como Tunny y las Bombes de Bletchley Park se mostraron inútiles contra ella, pero eso no evitó que dos hombres, John Tiltman y Bill Tutte, descubrieran la forma de atacarla. La Lorenz requería que el dispositivo utilizado para romper sus cifrados fuera capaz de un funcionamiento más flexible, con una lógica más compleja de lo que era habitual y conocido en Bletchley Park. Las Bombes clásicas eran capaces de hacer una tarea de manera muy eficiente y a gran velocidad, pero no podían operar de manera flexible. Max Newman, uno de los matemáticos de Bletchley Park, diseñó una forma de aplicar el método de ruptura de Lorenz, aunque, salvo que se hiciera de manera automática, era inútil en términos prácticos, ya que consumía semanas de trabajo. Por supuesto, el contenido de un mensaje semanas después de su captura era a menudo información caducada.

En los primeros meses de 1942 los investigadores de Bletchley Park reunieron todo lo que sabían sobre la SZ40 y Tutte fue capaz de determinar cómo debería ser la máquina, sus rotores y el movimiento de estos. Este sería solo un paso pequeño, ya que hasta más de un año después, en junio de 1943, no se comenzarían a conocer mensajes de las Lorenz. Newman, que se había unido a finales de 1942 al trabajo de los aliados contra la criptografía enemiga, aplicó las ideas de Turing sobre

lo que este había denominado la «máquina universal». Turing acababa de llegar de Estados Unidos y estaba investigando sobre circuitos eléctricos. Compartió algunas ideas con Newman y recomendó a este seguir con la línea de trabajo que había comenzado, y comentarlo con Tommy Flowers, un ingeniero del Servicio Postal de Dollis Hill, en el noreste de Londres, y que ya había participado en la creación de las Bombes. De este grupo de trabajo, en el que había otros personajes destacados como Charles Wynn-Williams, salió la conocida como Robinson, algo así como una máquina Bombe ultrarrápida y más flexible en cuanto a sus capacidades operativas.

El paso de los meses hizo que, para finales de año y comienzo de 1944, muchos mensajes de Lorenz fueran descifrados. Aun así, la Robinson tenía algunos problemas mecánicos que desesperaban a los técnicos, especialmente a Flowers. Este contribuyó a que las grandes ideas de Newman y Wynn-Williams fueran llevadas a la práctica, creando una máquina aún mejor, la Colossus. Tan importante y revolucionaria fue esta máquina, que se suele decir que es la primera computadora de la historia, o al menos uno de los pilares sobre los que arrancó el mundo de los ordenadores y las computadoras. La Robinson utilizaba unas 100 válvulas y la Colossus, en sus primeras versiones, llegaba a las 1.500, aunque alcanzaría las 2.500 en los últimos meses de la guerra. Aquellos que desaconsejaban a Flowers utilizar tal número de válvulas, ya que la convertirían en ingobernable, no le hicieron cambiar de opinión, por suerte para su país.

La Colossus en marcha era un espectáculo que no se había visto en su época. Su complejidad, su tamaño y la energía que requería se concretaban en la velocidad a la que procesaba la cinta de papel y en el resultado, que al final de muchos traqueteos y movimientos ponía la solución a disposición de los operadores. En términos computacionales, esta revolución es curiosamente un uso de las ideas de la máquina universal de Turing para un problema concreto, además, con un cierto componente de ataque al problema por fuerza bruta. Colossus poseía muchas de las características básicas de lo que serían los primeros ordenadores, que llegarían poco después, y algunas de las ideas que han llegado hasta hoy.

El prestigio de Colossus y la ruptura de Lorenz fue otro éxito de los aliados, que les permitió conocer lo que pensaban y planeaban los alemanes al más alto nivel. Sabían así si los planes aliados eran conocidos al otro lado del frente de combate o si sus operaciones de engaño estaban teniendo éxito.

28. EL PROYECTO VENONA

El OKW-Chi alemán sufrió, como todos los berlineses, los bombardeos y las penurias de la última parte de la guerra. En marzo de 1945 su director, Wilhelm Fenner, decidió que había llegado el momento de hacer las maletas y evacuar sus instalaciones, camino de Baviera. Todos los documentos y el equipamiento fueron almacenados en cajas de madera y cargados en camiones. Después de varias semanas de viaje, en la segunda semana de abril, ante una situación desesperada y para evitar que sus documentos y equipamiento cayeran en manos enemigas, todas las cajas fueron arrojadas al fondo de un lago.

Como en otros tantos ámbitos, a medida que las tropas aliadas, británicas y estadounidenses, avanzaban de oeste a este, buscaban hacerse con información alemana y con personajes clave alemanes, antes de que lo hicieran los rusos. Esa labor de cazatalentos desembocó en la Agencia Conjunta de Objetivos de Inteligencia, Joint Intelligence Objectives Agency, JIOA, que creó diferentes grupos especializados para captar los mejores cerebros alemanes y toda la información posible en cada especialidad. Así, había un grupo especializado en información relacionada con temas nucleares, ALSOS; otro que perseguía todo lo relacionado con los cohetes V1 y V2, OVERCAST; otro con el foco puesto en la tecnología de aviación, SURGEON, y, por supuesto, uno cuyo objetivo era investigar, conocer y hacer suyo todo lo relacionado con la inteligencia de señales alemana, haciéndolo además antes de que los rusos fueran capaces de conocer hasta dónde habían llegado. Su nombre en clave era TICOM, Target Intelligence Commitee, y se tenía por cierto que sería un elemento clave para la nueva configuración internacional, donde Rusia pasaría de aliado a enemigo. Asimismo, se sabía de la cercanía entre Japón y la Alemania nazi, por lo que acceder a esa información y convertir en colaboradores a los antiguos nazis que habían trabajado en la inteligencia de señales sería una ventana valiosa para conocer Japón y sus capacidades. De hecho, cuando el proyecto TICOM se puso en marcha en Europa, la guerra en el Pacífico seguía en marcha e información obtenida en un lado podría ser valiosa en la otra parte del mundo.

Uno de los problemas que hubo con la puesta en marcha de TICOM era que las personas que más conocimiento podrían tener en este campo eran en la mayoría de los casos conocedores de ULTRA. Por lo tanto, enviar a estas personas cerca de la línea del frente e incluso más allá de ella, era un riesgo no asumible. Si cayeran en manos enemigas, podrían revelar información crítica. Por ello, una unidad de los marines británicos fue asignada como escolta y protección para los integrantes del proyecto TICOM.

No era extraño que algunos de los antiguos nazis se entregaran voluntariamente a los británicos y estadounidenses, para escapar de los

rusos. Entre ellos estaba uno de los principales oficiales alemanes que habían estado en el OKW-Chi, que al encontrarse con soldados aliados dijo que la guerra estaba finalizada y que ya no había nada que esconder. Aseguró que ahora los norteamericanos eran sus aliados contra los rusos, y entre la información que aportó, puso a los aliados tras la pista de un lago en Baviera donde se había arrojado al agua todo el material. Cuando finalmente dieron con el lago, recuperar del fondo lo que habían hundido los alemanes resultó más complicado de lo que se esperaba. Esta fue solo una de las fuentes del proyecto TICOM, que cumplió con su objetivo e hizo llegar a los británicos y estadounidenses cantidades enormes de información. Todo aquello pasó tiempo en almacenes y no fue consultado a fondo, aunque tenía y tiene información sobre claves británicas, pero también libros de códigos franceses, datos sobre España, códigos rumanos, etíopes…

El Servicio de Inteligencia de Señales del Ejército de Estados Unidos, precursor de la Agencia de Seguridad Nacional, lanzó un programa secreto en febrero de 1943, posteriormente denominado proyecto Venona. La misión de este pequeño programa era examinar y explotar las comunicaciones diplomáticas soviéticas, además de otras labores relacionadas con el espionaje.

Aunque pasaron años antes de que los criptólogos estadounidenses pudieran romper el cifrado KGB y comprometer la información de sus contrincantes en la Guerra Fría, la información obtenida por Venona sí proporcionó a los líderes estadounidenses una perspectiva de los movimientos soviéticos, así como información sobre los ciudadanos o incluso empleados del gobierno de Estados Unidos que colaboraban con el bloque comunista.

En 1995 se comenzó a desclasificar información relacionada con el proyecto Venona, abriendo el acceso a unos 3.000 mensajes de inteligencia soviéticos, así como telegramas y otro tipo de comunicaciones, que habían sido capturados entre 1939 y 1948 a los soviéticos. Una sonda directa al trabajo de espionaje y contraespionaje de los primeros años de la Guerra Fría, entre otros momentos. El proyecto, en el que trabajaron de la mano británicos y estadounidenses, luchó contra los métodos de cifrado de los rusos, que, por culpa de una mala utilización de la clave de uso único, permitieron a los criptoanalistas conocer los textos en claro. Lógicamente en un volumen tan grande de documentos capturados hay información con diferentes niveles de importancia, pero muchas de las comunicaciones importantes entre Moscú y sus hombres, espías o colaboradores en Estados Unidos fueron interceptadas y descifradas. Casos como los de Elisabeth Bentley o Whittaker Chambers, han sido corroborados en los documentos desclasificados. De igual forma, ahora se sabe con certeza que la administración Roosevelt, durante la Segunda Guerra Mundial, tenía brechas en las que se había colado la inteligencia rusa.

El proyecto Venona se mantuvo en el más alto secreto, aunque sí se compartió cierta información con los demás firmantes del Acuerdo

UKUSA, en 1946. El grupo que se formó tras este acuerdo, conocido como Five Eyes, contaba con Estados Unidos, Reino Unido, Nueva Zelanda, Australia y Canadá. Estos países compartirían información de inteligencia de señales, SIGINT. Incluso dentro de las agencias de Estados Unidos con responsabilidad en seguridad nacional e internacional, el proyecto se mantuvo en secreto. Hasta finales de 1952, por ejemplo, la CIA no fue informada de la existencia de Venona. Cuando Kim Philby, quizás el agente doble más famoso de todos los tiempos, que trabajaba oficialmente en el servicio secreto británico, como agente del más alto rango mientras servía a los rusos, visitó Washington, se le prohibió hablar de Venona con cualquier persona de la CIA. Por supuesto, la información sobre el proyecto secreto sí fue comunicada por Philby a la KGB. Así, gracias a Philby y a algún otro agente soviético, los rusos tuvieron conocimiento pronto, en los primeros momentos de la Guerra Fría, de que los criptoanalistas estadounidenses y británicos podían leer su correo.

Cuando en Moscú estuvieron al tanto de la debilidad en sus códigos, que se debía a un mal uso de las claves, que deberían ser de un único uso, pusieron la solución sobre la mesa. Esto hizo que dejara de salir información importante del proyecto Venona y que durante el resto de la Guerra Fría siguiera sin ofrecer capturas y descifrados relevantes. Si bien los principales países envueltos en la Guerra Fría tenían sistemas de cifrado seguros y por lo tanto efectivos, muchos de los países de segunda fila y del Tercer Mundo estaban en manos de los criptoanalistas de cada uno de los bloques, tanto del bloque occidental como del oriental. La colaboración entre el GCHQ, la entidad dentro de la inteligencia británica dedicada al tráfico de señales, y la NSA, reportó información valiosa en muchos de los hechos principales de la Guerra Fría, gracias precisamente a que la cantidad de mensajes que se enviaban y recibían crecía exponencialmente, y por lo tanto el alimento para el SIGINT era continuo. De igual modo, el KGB tenía una capacidad similar, llegando a mediados de los años sesenta del siglo XX a ser capaz de poner en claro más de 150 sistemas de cifrado distintos, utilizados por 72 países.

La Guerra Fría fue una época dorada para el espionaje, y por lo tanto no es de extrañar que la información, las traiciones y la captura de mensajes fueran constantes. Las embajadas rusas en el extranjero eran un punto clave para la captación de agentes e informadores, y Estados Unidos no era una excepción en ese sentido. La KGB y la GRU, el servicio de inteligencia militar ruso, se beneficiaron enormemente de las personas que colaboraban con ellos, por distintas contraprestaciones, pero en muchos casos por puro convencimiento ideológico.

En 1960 dos miembros de la NSA, Bernon F. Mitchell y William H. Martin, desertaron a Moscú. Llevaban unos meses colaborando con el bloque comunista y en septiembre de ese año dieron una rueda de prensa desde la capital rusa. Entre otras cuestiones, los dos desertores explicaron cómo la NSA estaba capturando y desencriptando las comunicaciones de países aliados de Estados Unidos. Italia, Turquía,

Francia, Uruguay… es decir, estaban siendo espiados por la NSA. Se repetía por tanto un escándalo similar al que había desencadenado el libro de Yardley unas décadas antes, que ya hemos comentado. No sería el último, ya que en junio de 2013 Edward Snowden, que había trabajado para la CIA y para la NSA, hizo públicos a través de los periódicos *The Guardian* y *The Washington Post* , documentos clasificados que sacaban a la luz los programas de vigilancia masiva de Estados Unidos, cuyos nombres en clave eran PRISM y XKeyscore. La agencia gubernamental estadounidense estaba accediendo a los registros telefónicos de millones de clientes, a través de sus operadoras, y a los datos que Google y Facebook, entre otros, tenían sobre sus clientes. Bajo el proyecto PRISM, correos electrónicos, chats, historial de búsquedas… de los ciudadanos, eran recabados por la NSA. Snowden reveló que el gobierno de Estados Unidos había estado infiltrándose en los sistemas informáticos chinos durante años. Las Naciones Unidas y la Unión Europa también habían sido espiadas.

29. Espías soviéticos

Igor Gouzenko fue un criptógrafo ruso de la embajada de la URSS en Ottawa, durante la Segunda Guerra Mundial. No era un personaje relevante dentro de la embajada, pero su trabajo le permitía vivir en el país norteamericano de una forma que le resultaba muy agradable. En los primeros días de septiembre de 1945 tuvo conocimiento de que iba a ser enviado de vuelta a la Unión Soviética, lo que le obligaría a dejar atrás su cómoda vida canadiense, tanto a él como a su familia. Decidió desertar y como moneda de negociación para ganarse una posición en Canadá, se llevó de la embajada rusa los libros de códigos y todo el material que pudo relacionado con su trabajo como criptógrafo. Además de esto, llevaba información sobre espías soviéticos que operaban en Estados Unidos, Canadá y Reino Unido.

Sus primeros contactos fueron con la policía canadiense, que se mostró reticente a aceptar la oferta del agente soviético. Esto es lógico, ya que lo que puede parecer un guiño afortunado del destino por ganar una valiosa información, puede ser en realidad una trampa. El juego del espionaje, el gran juego, está lleno de situaciones así, de agentes dobles y de lances que pareciendo una cosa en realidad son la contraria. Gouzenko se quedó, por lo tanto, en tierra de nadie, y aquella misma noche que había desertado, sin protección ni ayuda aún por parte de Canadá, vio cómo los agentes soviéticos llegaban a su casa, irrumpían en ella y rebuscaban por todos lados.

Afortunadamente para Gouzenko, un vecino, un militar canadiense, le prestó ayuda y permitió que él y su familia se ocultaran en su casa aquella noche. Esto le libró de ser capturado y del peor de los destinos, de nuevo, para él y su familia. Poco después la oferta de Gouzenko fue aceptada por Canadá y no tardaron en verse los resultados, incluso públicamente, del material que había proporcionado el criptógrafo ruso. Por supuesto, la información sobre los códigos rusos, así como los métodos criptográficos que utilizaban, y algunas pruebas y experimentos en ese campo, no fue hecha pública, pero fue también un valioso recurso en los primeros años de la Guerra Fría.

La información sobre espionaje que Gouzenko puso sobre la mesa de los enemigos de la Unión Soviética sirvió para detener a una veintena de agentes que operaban en Norteamérica. Entre ellos, miembros destacados del Partido Comunista de Canadá, el físico alemán Klaus Fuchs, el químico Harry Gold, de origen suizo pero afincado en Estados Unidos, David Greenglass, que trabajaba en Los Álamos, y dos de los personajes más famosos de la historia del espionaje del siglo XX: Julius y Ethel Rosenberg. Todos ellos habían estado informando a los rusos del desarrollo de la bomba atómica, de los métodos para construirla, de las investigaciones, de los ensayos…

Como es habitual en este tipo de situaciones, las primeras piezas del puzle del espionaje ruso se colocaron en torno a la información de Gouzenko, pero esas piezas llevaron a otras y se estima en varias decenas los agentes y espías al servicio de la Unión Soviética que cayeron debido a la deserción de Gouzenko.

La Guerra Fría fue, como hemos dicho, una época dorada para el espionaje, y por supuesto, la criptografía era una herramienta básica para su trabajo. En Inglaterra, en 1961, Helen y Peter Kroger hacían labor de espionaje para los rusos, con especial atención a un centro de investigación armamentística que funcionaba en la isla de Portland, en el Canal de la Mancha. No eran los únicos espías rusos en la zona, sino que junto con algunos otros formaban un grupo dirigido por Gordon Lonsdale, aunque eran los Kroger los que se encargaban de las comunicaciones, de hacer llegar a los rusos la información. Eran una pareja normal, a ojos de sus vecinos, con los que se relacionaban normalmente y a los que invitaban a su casa sin mayores problemas. Se dedicaban al mercado y a la subasta de libros, lo que les permitía vivir en casa y viajar en busca de buenos ejemplares de un sitio a otro. Por supuesto, todo era una tapadera.

Lonsdale visitaba regularmente a los Kroger y al final las sospechas cayeron sobre ellos debido a esa relación. Durante el registro de la casa, la señora Kroger pidió que le dejaran alimentar el fuego que mantenía la casa caliente. Los agentes especiales de Scotland Yard tuvieron la precaución de registrar los bolsillos de la espía antes de permitirle acercarse al fuego. Al hacerlo encontraron un pequeño sobre con un papel lleno de números. Aquel papelito era un mensaje cifrado, listo para ser enviado a Moscú. Un mensaje cifrado con una clave de un solo uso que le habían proporcionado los responsables del espionaje ruso.

Era una forma sencilla de usar un cifrado casi perfecto. Con el listado de números, esa clave de un solo uso, que le habían entregado, los Kroger tan solo tenían que tomar cada letra del alfabeto y asignarle un número, que bien podrían ser los números del 1 al 26. Cada letra del mensaje se sustituía por su número y este se sumaba con el siguiente número de la clave, que tenía cuatro cifras. Ese número de la clave no volvía a utilizarse. Efectivo a la vez que seguro.

A los policías les costó localizar el transmisor que usaban para enviar los mensajes. Sus comunicaciones pasaban desapercibidas, ya que su casa no estaba en un lugar cualquiera. Vivían cerca de un aeródromo, por lo que el tráfico continuo de los aviones hacía que sus comunicaciones por radio pasaran desapercibidas si alguien escuchaba en busca de ellas. Además de todo esto, tenían algún otro dispositivo para facilitar el proceso. Como vemos, casi cualquier espía tenía conocimientos y sistemas para asegurar sus comunicaciones de manera sólida.

En los años sesenta, la Casa Blanca comenzó a hacer un uso masivo de SIGINT, encargando a la NSA que se ocupara del tema de manera directa, y con conexión inmediata con el presidente. Algunos presidentes, como Lyndon Johnson, tomaban esta información como vital y la tenían muy en cuenta, apoyando sus decisiones en ella. Otros, como Richard Nixon, fueron menos sistemáticos en la consulta de la información que le proporcionaba la NSA, y si bien la tenían en cuenta, esta quedaba diluida entre otras muchas fuentes.

Como ya hemos comentado, las grandes potencias del bloque contrario, el soviético, habían alcanzado un nivel de seguridad suficiente, no así los países de segunda fila. Gracias a la infiltración de estas comunicaciones, Estados Unidos tuvo información de primera mano sobre los movimientos militares y los enfrentamientos en Oriente Próximo en 1967, tanto antes como durante los propios combates que tuvieron lugar. La invasión de Checoslovaquia en agosto de 1968 por parte del Pacto de Varsovia, por ejemplo, no cogió por sorpresa a los norteamericanos. Los movimientos de tropas y las comunicaciones dentro del Pacto de Varsovia ya habían advertido de que algo iba a ocurrir, si bien los analistas de la CIA, en su mayoría, no creían probable la invasión que finalmente sucedió.

En definitiva, la criptografía siguió presente en el mundo de la Guerra Fría como lo había hecho en toda la historia, e incluso más. Durante gran parte de este tiempo, eso sí, los cifrados parece que han vencido a los criptoanalistas, y las consecuencias, victorias o derrotas, han venido más de las operaciones encubiertas y del espionaje que de la fuerza de la inteligencia contra los códigos.

30. Criptografía y computación, la última revolución

La Segunda Guerra Mundial cambió de manera radical las cosas en muchos ámbitos, y también en la criptografía. A pesar de la pesada cortina que se tendió sobre todo lo que se había hecho en Bletchley Park, llegando incluso a destruir las máquinas de descifrado que se habían creado, los conocimientos que se tenían entonces en torno al incipiente mundo de la computación, fueron clave para el futuro de la criptografía y de la humanidad. El secreto en torno a Colossus hizo que durante años no se tuviera conocimiento de su creación y que otras máquinas, como el ENIAC de la Universidad de Pensilvania, fueran reconocidas como las pioneras. En cualquier caso, los computadores permitían que se pusieran en marcha nuevos métodos de cifrado y nuevas formas de atacar los cifrados. La velocidad de cálculo, la capacidad de implementar procesos complejos y repetitivos y de trabajar con enormes cantidades de información abrieron una nueva era en la criptografía. Al menos fue así en el caso de los gobiernos y los ejércitos. En el ámbito del espionaje, donde lógicamente no podían utilizarse tales recursos, los métodos clásicos, los códigos acordados entre las partes y las soluciones imaginativas fueron la norma.

El conocimiento generado en las primeras décadas del siglo XX hizo que se diseñaran métodos cuya seguridad era muy alta, ya que el saber teórico y práctico había despegado gracias a las guerras mundiales. Ya sabemos la importancia de las claves y cómo una clave suficientemente larga y aleatoria es una forma de blindar en gran medida el cifrado. Por ejemplo, Estados Unidos generaba y distribuía a sus embajadas y centros militares enormes cantidades, toneladas de tarjetas perforadas, cintas de papel, cintas de datos… según el momento histórico, con claves que debían ser utilizadas para cifrar.

Aún quedaba, no obstante, un camino por recorrer para aprovechar todo lo que el nuevo escenario prometía, y los pasos se fueron dando. En los años sesenta, con la llegada del circuito integrado, y en los setenta con la computación, que se hizo popular, llegando a más empresas y entidades, con los precios cada vez más bajos, mientras que por el contrario las prestaciones subían cada vez más. A mediados de los años sesenta, Gordon Moore enunció la conocida Ley de Moore en un artículo de la revista *Electronics* . Esta ley, que no es técnicamente tal cosa, sino más bien una afirmación sobre la velocidad de evolución de la capacidad de computación, aseguraba que cada dos años se duplica el número de transistores en los microprocesadores y por lo tanto la potencia de estos. Hasta la actualidad, el pronóstico de Moore se ha venido cumpliendo más o menos, con lo que ello significa en cuanto a las capacidades de las máquinas. Para hacernos una idea, según unos cálculos de la compañía Intel, un vehículo que hubiera evolucionado al mismo ritmo que los microprocesadores desde el año 1971, en la actualidad sería capaz de moverse a 480.000 kilómetros por hora,

consumiría 4 litros por cada 3,2 millones de kilómetros y su precio rondaría los 3 céntimos.

En las últimas décadas la competición se ha movido entre los avances de las empresas privadas y los de las entidades gubernamentales, como la NSA. Las primeras luchan por desarrollar algoritmos y formas de cifrado irrompibles, mientras las segundas desean evitar esa popularización del cifrado perfecto, ya que impediría en parte su labor.

A comienzos de los años setenta los ordenadores estaban ya lo suficientemente extendidos entre las grandes empresas y entidades como para que se comenzara a hablar de estándares públicos de criptografía. Esto es, de algoritmos que permitieran de forma sencilla las comunicaciones seguras entre esas empresas y entidades. Había que proteger no solo las comunicaciones, sino también el almacenamiento digital de la información, que cada vez era mayor. Lógicamente, si se puede cifrar un texto para que se envíe sin que pueda ser descifrado por otro que no sea su destinatario, también se puede cifrar la información para almacenarla y que nadie, salvo aquel que tenga autorización, pueda descifrarla y consultarla. Esta demanda, como decíamos, era cada vez más alta, y era obvio que en pocos años se extendería aún más y seguiría aumentando. Por esto, la Oficina Nacional de Estándares de Estados Unidos, la NBS en aquel momento y hoy conocida como NIST, por National Institute of Standards and Technology, lanzó un proyecto en 1973 para generar el algoritmo estándar, conocido públicamente y a la vez seguro. En una primera ronda se recibieron pocas propuestas y ninguna se consideró suficientemente buena como para adoptarla como estándar. Un año más tarde se repitió el proceso e IBM presentó un método denominado Lucifer, que sí pasó los exámenes de la NBS. Antes de considerarlo como un estándar a recomendar, la NBS pidió a la NSA, la Agencia Nacional de Seguridad, su opinión y estudio. La NSA, como responsable de mantener la seguridad de las comunicaciones gubernamentales y militares de Estados Unidos y de justo lo contrario con respecto a otros países, tenía una posición privilegiada en el proceso.

En 1975, con el visto bueno de la NBS y la NSA, el cifrado de IBM fue hecho público para la última fase dentro del proceso, su estudio y validación por el resto de la comunidad criptográfica, esto es, investigadores, universidades, empresas privadas… El proceso acabó por fin cuatro años después de su comienzo, en enero de 1977, cuando el cifrado Lucifer de IBM se convirtió en un estándar de cifrado, si bien se le cambió el nombre a DES, Data Encryption Standar. Como estándar que era, poco a poco fue extendiéndose a todos los ámbitos y el *software* comenzó a implantarlo como solución de almacenamiento seguro, mientras distintos productores de *hardware* implementaron chips para aplicar DES a alta velocidad.

Aún hoy continúa la polémica sobre la seguridad del DES y sobre si la NSA, que como hemos visto participó en el proceso de estandarización, pudo analizar, y quién sabe si modificar, el algoritmo para encontrar o

preparar una puerta trasera que le permitiera romperlo. Esto supondría que el DES, usado masivamente tan pronto como se convirtió en estándar, fuera seguro a los ojos de terceros, mientras que la NSA era capaz de descifrarlo de algún modo. De hecho, hubo modificaciones entre el algoritmo Lucifer de IBM y el DES finalmente aceptado. La propuesta original manejaba bloques de 128 bits y claves de 128 bits, mientras que la versión modificada rebajaba el tamaño de los bloques a 64 bits y las claves a 54 bits. Sin entrar en detalles técnicos, un mayor tamaño de bloques y de claves hace el sistema más seguro, sencillamente porque la cantidad de cálculo necesaria para romper el cifrado es mayor. Es cierto que la capacidad de los computadores de los años setenta no era suficiente como para poner en peligro los cifrados realizados con el número de bits que propuso el estándar, pero es posible que la NSA tuviera alguna forma de alcanzar más capacidad de cálculo o sospechara que la alcanzaría en el corto plazo.

La longitud de los bloques y de la clave no fue el único cambio que sufrió el algoritmo tras su paso por la NSA, es decir, en su transformación de Lucifer a DES. No hay confirmación pública de la manipulación del DES por parte de la NSA con el fin de permitirse una forma de romperlo, pero las sospechas han sido constantes durante muchos años. Por otra parte, lo cierto es que DES, en su versión final, contiene modificaciones que lo hacen más seguro que el Lucifer original, por lo que nada en claro se puede decir. Ya en 1976, un año después de su publicación como estándar, había escritos especializados sobre estas dudas.

Un concepto interesante y muy común en el mundo de la criptografía actual es que muchos de los métodos que se utilizan, basados en las características de determinados números, en especial los números primos, y de ciertas operaciones, se saben vulnerables, si bien en la actualidad son seguros. Esto es debido a que el método conocido para romper el cifrado requiere un volumen de cálculo que hoy está fuera del alcance de nuestras capacidades. En ocasiones se duda si fuera del alcance de todos o de casi todos. Estos métodos computacionalmente seguros, lo son a día de hoy, pero serán vulnerables con el paso del tiempo, a medida que los computadores aumenten su capacidad de cálculo.

Esto ya ocurría con el DES, que se sabía vulnerable a un ataque por fuerza bruta, esto es, a un ataque en el que se prueban una a una todas las claves posibles. Por supuesto, en los años setenta se estaba lejos de una capacidad de cálculo que permitiera hacer ese ataque por fuerza bruta en un espacio de tiempo razonable y útil. Hasta dos décadas después, a finales de los años noventa, no llegaría ese momento en el que DES pudiera ser descifrado, aunque no era sencillo y el esfuerzo computacional seguía siendo enorme incluso para las máquinas de la época. En cualquier caso, para entonces la computación había cambiado mucho, así como la criptografía.

Por supuesto, DES no era el único algoritmo criptográfico disponible ni utilizado. Desde los años setenta han aparecido centenares de propuestas de todo tipo, y muchas de ellas se han implementado y utilizado de manera amplia. En enero de 1997 se repitió el proceso de búsqueda de un estándar general en la industria para sustituir a DES.

Sin entrar en detalles técnicos, diremos que las matemáticas han sido capaces de solucionar uno de los problemas principales de la criptografía, como es la distribución o el intercambio de claves. Esta criptografía asimétrica o de clave pública, como se la denomina, unida a los avances que hemos comentado de la computación, hizo que se popularizara la criptografía hasta ser utilizada de manera casi ubicua y transparente, algo que ocurre en nuestros días. El nombre de criptografía de clave pública proviene de que el sistema funciona con dos claves y una de ellas es pública, mientras que la otra es secreta. De igual forma, se denomina asimétrica porque mientras que en el resto de sistemas que hemos visto hasta ahora la clave para cifrar y descifrar es la misma, en este caso son diferentes, por eso conceptualmente el cifrado y descifrado es asimétrico, distinto en origen y destino.

Gracias a las características matemáticas de algunos números y operaciones complejas, se pudo diseñar este sistema. En él existen dos claves, como hemos dicho, una privada, que solo debe conocer su propietario, y otra pública, que puede y debe ser conocida por otros. Cuando una persona, A, desea enviar un mensaje cifrado a otra persona, B, toma la clave pública de B y cifra el mensaje con dicha clave. El cifrado es completamente seguro y no puede ser descifrado salvo que se utilice la clave privada asociada a la clave pública utilizada en el cifrado. En este caso, si se cifró con la clave pública de B, solo se podrá descifrar con la clave privada de B, que conoce solo B, y por lo tanto el método es seguro, ya que solo el destinatario podrá leer el mensaje.

Esta idea fue revolucionaria en el mundo de la criptografía moderna. En 1976 Whitfield Diffie y Martin Hellman, de la Universidad de Stanford, publicaron un artículo con la propuesta de este tipo de criptografía. Ralph Merkle, de la Universidad de Berkeley, estaba trabajando en la misma idea y aunque quedaban aún problemas por resolver, el camino estaba abierto. De nuevo volvemos a la idea de caminar a hombros de gigantes, y estamos ya muy cerca de nuestros días. Si bien estos nombres son los más conocidos y generaron ideas que sirvieron de alimento para otros no son los únicos. Según el director de la NSA de finales de los años setenta, Robert Inman, en la agencia ya se habían hecho avances con la criptografía de clave pública y se había utilizado con éxito, antes de las publicaciones académicas. Es más, hay algunas sospechas de que el británico GCHQ, Govermment Communication Headquarters, ya avanzaba conceptualmente en este campo una década antes.

El algoritmo de clave pública más utilizado y popular es el RSA, siglas que provienen de sus creadores, Rivest, Shamir y Adleman. Estos tres

hombres formaban parte del MIT, del Massachusetts Institute of Technology, y publicaron su propuesta en agosto de 1977. La NSA lanzó una acción jurídica contra la implementación pública del RSA, lo que dio comienzo a una batalla legal que paralizó el desarrollo del sistema durante un buen tiempo.

Finalmente, en 1982 Rivest, Shamir y Adleman crearon una empresa para explotar su idea, la RSA Data Security, con la que obtuvieron un éxito empresarial enorme. Este tipo de criptografía es hoy omnipresente y la utilizamos todos los días, aun cuando no sabemos que está detrás de los protocolos y algoritmos que protegen nuestras comunicaciones.

Cronología de la criptografía en la historia

3600 a. C. - Los sumerios desarrollan la escritura cuneiforme y los egipcios la jeroglífica.

1900 a. C. - Grabado de piedra en la tumba de Menet Khufu, con modificaciones en la escritura jeroglífica.

1600 a. C. - Los fenicios inventan el alfabeto.

500 a. C. - El Atbash comienza a utilizarse.

500 a. C. - En Alejandría se propone el uso de antorchas para enviar mensajes, conocido como Fryctoria.

480 a. C. - En la batalla de Salamina la victoria griega es gracias al aviso de Demarato, usando la esteganografía.

430 a. C. - Heródoto deja constancia del uso de la criptografía en varias de sus historias.

400 a. C. - Eneas el Táctico escribe su tratado militar en el que dedica un capítulo completo a la criptografía.

400 a. C. - Los espartanos usan la escítala para comunicarse con seguridad.

120 a. C. - Polibio crea su cuadrado, su matriz de cinco filas y cinco columnas donde a cada letra le corresponde una celda.

100 - Suetonio escribe su *Vida de los doce césares* , en donde se describen algunas técnicas criptográficas, como el cifrado de Julio César.

300 - Se escribe el *Kama sutra* , que incluye la escritura secreta como una de las artes a conocer por las mujeres.

801 - Nace Al-Kindi, pionero en el análisis de frecuencias.

999 - Accede al papado Silvestre II, que utilizó las tironianas en varios escritos, incluidas dos de sus bulas.

1379 - Gabriel de Lavinde crea los nomenclátores para el Papa.

1401 - Nace el uso de los homófonos en los cifrados.

1450 - Se escribe el *Manuscrito Voynich* , que utiliza algún código aún por descifrar, si bien se sigue trabajando sobre él.

1466 - Leon Battista Alberti, creador del disco que lleva su nombre, inicia la idea de las cifras polialfabéticas.

1474 - Cicco Simonetta publica sus 12 puntos sobre el criptoanálisis.

1500 - Se publica la obra de Tritemio, donde aparecen las tablas que llevan su nombre.

1518 - Se imprime el libro *Poligrafía* , escrito por Tritemio, siendo el primer libro impreso dedicado a la criptografía.

1540 - Nace Philips van Marnix, criptógrafo holandés.

1553 - Bellaso publica varios retos criptográficos, algunos de los cuales aún están por resolver. Describe también una cifra similar a la cifra Vigènere.

1585 - Vigenère publica su tratado, donde describe el método ideado por Bellaso y que será considerado como una cifra indescifrable durante mucho tiempo.

1586 - Tiene lugar la conjura de Babington, que acabó con la condena a muerte de María Estuardo.

1588 - Se publica el libro de cifras de Vigenère.

1626 - Durante el asedio de Realmont, Antoine Rossignol comienza su carrera como criptógrafo.

1671 - Leibniz inventa una máquina calculadora.

1711 - Se crea la Oficina del Gabinete Secreto en Viena.

1753 - Comienza a diseñarse y desarrollarse el telégrafo.

1790 - Thomas Jefferson diseña su rueda para cifrar mensajes.

1791 - Nace Charles Babbage, que rompería la cifra Vigenère y pondría algunos pilares para el avance de la computación y el cálculo automático.

1792 - Claude Chappe presenta el telégrafo óptico, idea similar a la de Agustín de Betancourt, contemporáneo.

1811 - Durante la Guerra de Independencia española, George Scovell rompe la Gran Cifra de París.

1837 - Samuel Morse crea el código que lleva su nombre.

1843 - Se publica *El escarabajo de oro* , de Edgard Allan Poe.

1844 - Se envía el primer mensaje telegrafiado.

1854 - Babbage rompe los cifrados polialfabéticos y la cifra Vigenère.

1854 - Se crea el cifrado Playfair.

1863 - Kasiski publica la ruptura de los cifrados polialfabéticos, sin conocer los trabajos de Babbage.

1883 - Auguste Kerckhoffs escribe *La criptografía militar* y publica el principio que lleva su nombre.

1885 - Se descubren los papeles de Beale, una serie de documentos cifrados que podrían ocultar un tesoro, y que siguen sin descifrarse.

1890 - Bazeries rompe la cifra de los Rossignol, usada por los reyes franceses dos siglos antes. Además, crea un dispositivo similar a la rueda de Jefferson.

1894 - Marconi patenta el invento de la radio.

1903 - Se publica *La aventura de los monigotes* , escrita por Conan Doyle.

1904 - En la guerra ruso-japonesa se emplea por primera vez el análisis de tráfico de señales.

1914 - Los rusos hunden el *SMS Magdeburg* , capturando importantes libros de códigos.

1914 - Gracias a la intercepción de los mensajes rusos, los alemanes vencen en la batalla de Tannenberg.

1915 - William Friedman, uno de los más importantes criptógrafos estadounidenses, avanza en la aplicación de la estadística al criptoanálisis.

1916 - Los franceses comienzan a utilizar los códigos de trinchera.

1916 - Alemania crea su oficina de criptografía, el Abhorchdienst.

1917 - El telegrama Zimmermann es enviado, capturado y descifrado, provocando la entrada de Estados Unidos en la Primera Guerra Mundial.

1918 - Aparece la idea de la cifra irrompible, basada en una clave de longitud infinita.

1918 - Se inventa la máquina Enigma.

1918 - Los indios choctaw sirven en el ejército utilizando su idioma, desconocido para el resto, para asegurar las comunicaciones.

1918 - El cifrado ADFGVX es introducido por Alemania.

1919 - La Alemania de Weimar utilizar la clave de un solo uso para algunas de sus comunicaciones.

1919 - Se patenta la máquina de rotores.

1919 - Vernam patenta el cifrado que lleva su nombre.

1921 - Tiene lugar la Conferencia Naval de Washington donde aprovechan la ruptura de los códigos japoneses.

1925 - Hans-Thilo Schmidt comienza a entregar información a Francia.

1928 - Los alemanes comienzan a usar Enigma.

1929 - Se cancela el Black Chamber estadounidense.

1931 - Se publica el libro de Herbert Yardley, en el que describe el Black Chamber de Estados Unidos y cómo habían espiado las comunicaciones de otros países.

1932 - Los criptógrafos polacos comienzan a romper los cifrados de Enigma.

1935 - Los criptógrafos alemanes rompen el código administrativo naval británico.

1936 - El código Rojo japonés es roto por los estadounidenses.

1938 - Se introducen dos nuevos rotores en la máquina Enigma.

1938 - Los criptógrafos alemanes rompen el código de la marina británica.

1939 - Los japoneses comienzan a usar el código JN-25.

1939 (feb) - El código Púrpura sustituye al código Rojo.

1939 (jul) - Polonia comparte su conocimiento de Enigma con Francia y Reino Unido.

1940 (feb) - Se recuperan dos rotores de Enigma del submarino *U-33* , por parte de los aliados.

1940 (mar) - La Bombe británica comienza a operar.

1940 (may) - El tráfico de la Luftwaffe es descifrado de manera continua.

1940 (sep) - Comienza a romperse el código Púrpura y el JN-25.

1940 (dic) - Entra en uso del JN-25B japonés.

1940 (dic) - Se rompe el código principal de la Abwehr.

1941 (feb) - Se rompen los códigos de la Luftwaffe en África.

1941 (mar) - Se descifran los mensajes de la Enigma naval de febrero gracias a documentos capturados.

1941 (may) - Se captura el submarino *U-110* .

1941 (jun-jul) - Alemania comienza a leer el nuevo código naval británico, utilizado por los aliados para comunicarse con los convoyes atlánticos.

1941 (sep) - Churchill visita Bletchley Park.

1942 (ene) - El tráfico del agregado militar de Estados Unidos en El Cairo comienza a ser leído por los alemanes.

1942 (feb) - Se modifica la Enigma naval (Shark para los británicos) para los submarinos en el Atlántico, con un cuarto rotor.

1942 (mar) - Se lee de forma regular el código JN-25B.

1942 (oct) - Comienza la colaboración de Estados Unidos y los británicos contra Enigma.

1942 (oct) - El *U-559* es capturado.

1942 (dic) - Se rompe la Enigma naval gracias a las comunicaciones meteorológicas.

1943 (abr) - El avión de Yamamoto es derribado.

1943 (jun) - Los aliados cambian sus códigos y los alemanes no pueden conocer el contenido de sus comunicaciones en el Atlántico.

1944 (feb) - La Colossus I es entregada y se encargan cincuenta Bombes adicionales.

1944 (nov) - El proyecto Venona comienza a tomar forma.

1946 - El proyecto Venona rompe los cifrados soviéticos.

1949 - Claude Shannon publica un artículo que da soporte matemático a una cifra indescifrable.

1951 - Se crea la NSA.

1968 - Se desclasifica la información sobre la participación de los navajos en la Segunda Guerra Mundial.

1968 - Se publica la idea de la computación cuántica, por parte de Stephen Wiesner.

1969 - El conocido como Asesino del zodiaco envía mensajes cifrados a varios periódicos.

1973 - Clifford Cocks, dentro del GCHQ, descubre una función que permite la criptografía asimétrica.

1976 - Se acepta el cifrado DES como un estándar.

1976 - Se publica el esquema de cifrado de clave pública de Diffie, Hellman y Merkle.

1977 - Se publica el sistema RSA.

Bibliografía

ANDREW, Christopher, *The Secret World. A History of Intelligence* , Yale University Press, 2018.

BLACK, Jeremy, *Grandes líderes militares y sus campañas* , Blume, Barcelona, 2008.

BUDIANSKY, Stephen, *Battle of Wits* , Penguin Books, 2000.

CARNICER, Carlos y MARCOS, Javier, *Espías de Felipe II* , La Esfera de los Libros, Madrid, 2005.

CEANO, Román, *Ultra: Enigma y Fish* , Escuela Técnica Superior de Ingeniería de Sistemas Informáticos de la UPM, Madrid, 2015.

COPELAND, Jack, *Alan Turing* , Turner, Madrid, 2012.

COWNING, Taylor, *Secret Warriors. Key Scientists, Code-Breakers and Propagandists of the Great War* , Little Brown, 2014.

DIEPENBROEK, Martine, *https://www.academia.edu/20830722/ENIGMA_SECRET_COMMUNICATION_IN_GRECO-ROMAN_WARFARE* , 2017.

FRARY, Mark y PINCOK, Stephen, *Codebreaker: The History of Secret Communication* , Random House Books, 2007.

FRATTINI, Eric, *Los espías del Papa* , Espasa, Madrid, 2011.

GLEICK, James, *La Información. Historia y realidad* , Crítica, Barcelona, 2012.

GORDILLO COUCIERES, José Luis, «La captura del Mar Cantábrico», *Historia y Vida* , 1994.

HAGERTY, Edward J., «The Spy in Hitler's Inner Circle: Hans-Thilo Schmidt and the Intelligence Network That Decoded Enigma», *Journal of Strategic Security* , 2016.

HASTINGS, Max, *La guerra secreta* , Crítica, Barcelona, 2016.

HOLMES, Richard, *Un mundo en guerra* , Crítica, Barcelona, 2008.

IORDANOU, Ioanna, «The Professionalization of Cryptology in Sixteenth Century Venice», *Enterprise and Society* , 2018.

JENNINGS, Christian, *The Third Reich Is Listening* , Osprey Publishing, 2018.

KAGAN, Neil y HYSLOP, Stephen G., *Historia secreta de la Segunda Guerra Mundial* , National Geographic, 2018.

KAHN, David, *The Codebreakers. The Story of Secret Writing* , Macmillan Publishing Company, 1967.

KEEGAN, John, *Intelligence in War* , Alfred A. Knopf, 2003.

LEE, Lucy R., *Cryptography in the First World War* , Massachusetts Institute of Technology (MIT), 2018.

MANN, Chriss, *Grandes batallas de la Segunda Guerra Mundial* , Parragon, 2011.

MICHAEL de LEEUW, Karl y BERGSTRA, Jan (Eds.), *The History of Information Security: A Comprehensive Handbook* , Elsevier Science, 2007.

NORMAN, Bruce, *Secret Warfare. The Battle of Codes and Ciphers* , David & Charles, 1989.

ORDÓÑEZ, Javier, *Ideas e inventos de un milenio (900-1900)* , Lunwerg Editores, Barcelona, 2011.

ORTEGA TRIGUERO, Jesús J., *et al., Introducción a la criptografía: historia y actualidad* , Ediciones Universidad de Castilla-La Mancha, Toledo, 2006.

PELLING, Nick, «Fifteenth Century Cryptography Revisited», *https://www.academia.edu/33813775/Fifteenth_Century_Cryptography_Revisited, 2017* .

PRIETO, Manuel J, *Submarinos* , Redbook Ediciones, Barcelona, 2015.

—, *Operaciones especiales de La Segunda Guerra Mundial* , La Esfera de los Libros, Madrid, 2016.

—, *Curistoria, https://www.curistoria.com* .

QUIRANTE SIERRA, *Los Siete de Camazón* , 2001, *https://naukas.com/2011/02/17/los-siete-de-camazon/* .

—, *Boletín Enigma* , n. 12, 2003, *https://www.ugr.es/~aquiran/cripto/enigma/boletin_enigma_12.htm* .

—, *Boletín Enigma* , n. 14, 2003, *https://www.ugr.es/~aquiran/cripto/enigma/boletin_enigma_14.txt* .

—, *Boletín Enigma* , n. 63, 2008, *https://www.ugr.es/~aquiran/cripto/enigma/boletin_enigma_63.htm* .

REEN WINKLER, Jonathan, *Nexus: Strategic Communications and American Security in World War I* , Harvard University Press, 2008.

SÁNCHEZ MUÑOZ, José Manuel, «Descifrando Enigma. La epopeya polaca», *Lecturas Matemáticas* , 2013.

SINGH, Simon, *Los códigos secretos* , Debate, Barcelona, 2000.

SOLER FUENSANTA, José Ramón, y LÓPEZ-BREA ESPIAU, Francisco Javier, *Mensajes secretos. La historia de la criptografía española desde sus inicios hasta los años 50* , Tirant lo Blanch, Valencia, 2016.

—, *Soldados sin rostro* , Inédita Editores, Barcelona, 2008.

TARANILLA, Carlos, *Criptografía. Los lenguajes secretos a lo largo de la Historia* , Guadalmazán, Córdoba, 2018.

URBAN, Mark, *The Man Who Broke Napoleon's Codes* , Faber and Faber, 2001.

VON ZUR GATHEN, Joachim, «Zimmermann Telegram: The Original Draft», *Cryptologia* , 2007.

VV.AA., *Diccionario Biográfico Español* , Real Academia de la Historia, Madrid, 2019, *http://dbe.rah.es* .

VV.AA., *NSA* , 2019, *https://www.nsa.gov* .

VV.AA. (*Numberphile*), *158,962,555,217,826,360,000 (Enigma Machine)* , 2019, *https://youtu.be/G2_Q9FoD-oQ* .

VV.AA., *Secrets & Spies / The National Archives. http://www.nationalarchives.gov.uk/spies/ciphers/default.htm* .

WILLMOTT, H. P., *La Primera Guerra Mundial* , Inédita Editores, Barcelona, 2004.

Manuel J. Prieto (Vitigudino, Salamanca, España, 1975) es autor de varios libros de divulgación histórica, aunque también ha publicado ensayos en el ámbito de la tecnología así como relatos de ficción.

Él mismo nos cuenta: «No puedo decir que hubo un chispazo o revelación en algún momento de mi vida que me llevara a amar la lectura o la historia, sino que más bien fue algo parecido a la conocida metáfora de la bola de nieve. Aunque mi formación es técnica (Ingeniería Informática, entre otras, para ser exactos), las novelas históricas en un primer momento seguidas de los ensayos fueron poco a poco creando en mí una afición a la historia que ya forma parte de mi día a día, casi literalmente. Llegó un momento en que comencé a escribir un blog, allá por comienzos de 2006, dedicado a la historia. Concretamente a la parte más curiosa, llamativa, anecdótica y amena de la Historia».

Su espacio en la web Curistoria —un neologismo creado a partir de las palabras “curiosidades” e “historia”—, que recoge anécdotas, curiosidades e información de temática histórica desde hace más de diez años, es un referente en la blogosfera española. Ha colaborado con diferentes programas de radio y revistas digitales, y ha sido ganador y finalista en varios certámenes literarios.

Entre sus libros se destacan *Submarinos: relatos de espectaculares y arriesgadas operaciones de la guerra submarina* (2015), *Curistorias de la Segunda Guerra Mundial* (2015) y *Curistoria, curiosidades y anécdotas de la historia* (2008).