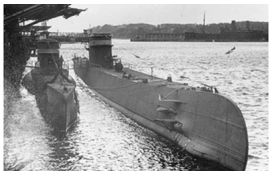


Manuel P. Villatoro

La máquina Enigma fue una de las armas que otorgó una ventaja definitiva al Tercer Reich en la monumental batalla del Atlántico. Gracias a su sistema de cifrado, tanto las manadas de lobos grises (el nombre que recibían los grupos de submarinos nazis) como los «U-boot» solitarios camparon a sus anchas por los océanos acechando a los convoyes que llevaban armamento, munición, alimentos y un largo etc. desde Estados Unidos hasta Gran Bretaña. Ya lo dijo el premier Winston Churchill: «Lo único que me asustó de verdad durante la guerra fue el peligro de los submarinos. Me sentía aún más desasosegado por esta batalla que por el glorioso combate aéreo conocido como la batalla de Inglaterra».

Utilizada para enviar órdenes a los submarinos desde el alto mando de forma segura, así como para intercambiarse ubicaciones entre los propios «U-Boote», la máquina Enigma fue, en definitiva, un elemento clave en la Segunda Guerra Mundial. O, como explica Pere Cardona a ABC (autor de la página « **Historias Segunda Guerra Mundial»** y de varias obras sobre el conflicto como «Lo que nunca te han contado del Día D»), «fundamental para que los alemanes pudieran entorpecer el tráfico marítimo en el Atlántico». Como bien señala, las Enigma, en sus múltiples modelos, «posibilitaron la supremacía germana» durante los primeros años de la contienda. Para ser más concretos, hasta que los Aliados lograron profanar sus secretos tras asaltar el U-110 y hacerse con una de ellas.

«Al principio, el sistema de cifrado que usaban entre los submarinos, un código de transmisión de radio llamado “shark”, que se usaba también con las Enigma, era un enemigo difícil de vencer. Lo mismo pasaba con las transmisiones generales. Pero a partir de la captura del U-110 se hicieron con toda la codificación. Karl Dönitz no entendía por qué los convoyes esquivaban a sus sumergibles. Hasta tal punto le desquiciaba que pensó que había un traidor entre ellos», añade Cardona. Pero no era ningún traidor. El honor correspondía al criptógrafo Alan Turing y a su equipo, los magos que habían desvelado el truco de las transmisiones teutonas.

Los orígenes de Enigma

Para hallar los orígenes de la máquina Enigma es necesario viajar en el tiempo hasta la Primera Guerra Mundial, época en la que los agentes secretos ya habían comenzado a hacer sus «pinitos» en el mundo del espionaje ayudados por todo tipo de curiosos artefactos (los cuales tenían poco que envidiar, con la salvedad del tiempo, a los usados por James Bond). Además de estos «juguetitos», los servicios secretos contaban también con varios sistemas para evitar que sus mensajes secretos fueran captados por el enemigo. Eran las llamadas técnicas de criptografía y permitan que, si los contrarios se apoderaban de dicho correo, no entendieran ni jota de lo que había en su interior.

En aquellos años, sin embargo, los sistemas de codificación de mensajes se basaban básicamente en la sustitución de las palabras o letras por números. Así pues, el emisor y el receptor tenían que contar con un libro de códigos en el cual se explicaba qué cifra se correspondía con cada carácter. Era un encriptación, por lo tanto, que no se parecía en nada a la que se lleva a cabo hoy en día mediante el ordenador. Por el contrario, se basaba en el lápiz y el papel y era bastante sencilla de descifrar si era descubierto por el enemigo.

Todo ello cambió con la llegada del siglo XX, una época en la que la criptografía se hizo mayor de golpe gracias a las primeras máquinas de cifrado. Éstas lograban modificar, de forma automática, un mensaje convirtiendo un texto legible en una amalgama de números y letras al azar. De esta forma se lograba que el enemigo tuviera que exprimirse la mollera para descubrir lo que realmente se estaba escribiendo. «Estas máquinas permitían a los criptógrafos mecanizar el proceso de cifrado, pero aumentando enormemente el número de posibilidades de encriptación, haciendo prácticamente inaccesibles las tareas de aquellos que intentaban desentrañar qué se escondía tras los mensajes cifrados con dichos mecanismos», explica el investigador José Manuel Sánchez Muñoz en su dossier **«Descifrando Enigma. La epopeya polaca».**

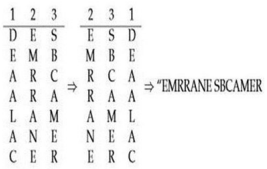
A pesar de que el funcionamiento de estas máquinas era mecánico, su objetivo era exactamente el mismo que aquellos primitivos métodos de encriptación utilizados en contiendas anteriores: lograr esconder una letra haciéndola pasar por otra o por un número. A su vez, pretendían conseguir que ese carácter fuera cifrado mediante un sistema contra más complejo mejor. Así pues, si –por ejemplo- el sistema de codificación consistía en sumar a cada letra del mensaje tres posiciones dentro del alfabeto («A» equivaldría a «D») estos aparatos eliminaban la necesidad de hacer esta cuenta a mano y la cambiaban

automáticamente.

Esconder mensajes

El ejemplo anterior es sólo uno de los métodos utilizados en la encriptación de mensajes. Concretamente, es el conocido como sistema de sustitución. «El primer ejemplo documentado de un método de sustitución de encriptación fue utilizado por Julio César en la guerra de las Galias para enviar un mensaje a Cicerón, que estaba sitiado y a punto de rendirse, sustituyendo las letras romanas por griegas haciendo ininteligible el mensaje. Para cifrar un mensaje mediante el Cifrado de César, cada letra de dicho mensaje era remplazada con la letra de tres posiciones después en el abecedario. Por tanto, la A sería reemplazada por la D, la B por la E, la C por la F, y así sucesivamente», determina Muñoz en su dossier: «Historias de Matemáticas criptología nazi. Los Códigos Secretos de Hitler».

Con todo, existen multitud de sistemas (los cuales fueron evolucionando con el paso de los años). Otro de ellos, como bien señala el experto, es el denominado método de transposición: «Pongamos un ejemplo; imaginemos que tanto el emisor del lenguaje cifrado como el receptor consideran en principio un número menor de nueve dígitos como clave, por ejemplo el 231. Dicha clave ponía de manifiesto que el texto debía ser escrito en tres columnas (en principio sin considerar espacios entre palabras). De este modo el emisor codificaría la frase “DESEMBARCAR AL AMANECER” como “EMRRANE SBCAMER DEAALAC”».



Nace Enigma

Con el paso de los años, los expertos fueron perfeccionando estos aparatos de cifrado consiguiendo inventar máquinas que realizaban por sí mismas complicadas permutaciones en las letras. Precisamente uno de los grandes avances del cual nacería la máquina Enigma fue la

invención de los «rotores», unas ruedas que –dependiendo de la posición en la que se encontraran- hacían que cada letra se convirtiera en otra. La primera de ellas fue inventada por el estadounidense Edward Hugh Hebern en 1917, la cual fue mejorada posteriormente en múltiples ocasiones.

Sin embargo, la gran revolución de las máquinas de cifrado de mensajes llegó de manos de Arthur Scherbius. «El 23 de febrero de 1918 Scherbius solicitó la primera patente de la máquina comercial Enigma con el fin de crear una máquina que mantuviera en secreto las principales transacciones de información en el mundo empresarial. Enigma era relativamente fácil de transportar y muy potente, rápida y cómoda a la hora de generar mensajes cifrados. La primera versión comercial, conocida con el nombre de Enigma A, fue puesta a la venta en 1923», añade el experto español. Por entonces, este germano no se imaginaba que su invento iba a ser utilizado a gran escala por el ejército nazi para lograr ocultar a los aliados los movimientos de sus tropas.

La armada alemana (o Kriegsmarine) fue la primera en adoptar esta máquina de encriptado en febrero de 1926. A los marinos les hizo sin duda un buen servicio, pues gracias a ella las manadas de «lobos» (como eran conocidos los grupos de submarinos nazis) podían atacar a los convoys ingleses y americanos que trataban de entrar y salir de las islas británicas. Luego fue asumida por la Wehrmacht, donde fue utilizada para coordinar los asaltos masivos de carros de combate sobre el enemigo (la llamada « guerra relámpago»). La fuerza aérea (Luftwaffe) tampoco se quedó atrás y adquirió su propio dispositivo mediante el que pudo mantener en secreto sus operaciones de bombardeo.

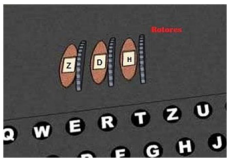
Así funcionaba

¿Cómo funcionaba la máquina que ayudó a los nazis a dominar los campos de batalla? Para empezar, la Enigma contaba con una forma similar a la de una máquina de escribir, aunque no usaba papel y se alimentaba a base de baterías. Sus dos partes principales eran un teclado con las 26 letras del alfabeto (en el que el emisor escribía el mensaje que quería cifrar) y un panel en el que se hallaban también cada uno de los caracteres del abecedario. Cuando el emisor pulsaba una de las teclas, y mediante un complejo mecanismo, la máquina la convertía en otra (la cual aparecía iluminada en el cuadro de luces). El receptor, por su parte, debía tener un aparato similar configurado de igual manera que el primero para que el sistema hiciese el recorrido inverso.

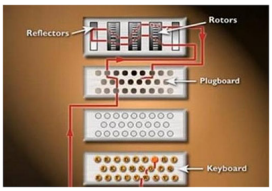
El mecanismo interior era bastante complejo. Cuando se pulsaba una tecla, la máquina enviaba un impulso eléctrico que pasaba en primer lugar a través de un clavijero bajo el teclado. Éste era el primer elemento encargado de modificar la letras, ya que el emisor podía conectar dos caracteres haciendo que uno equivaliera a otro (de esta forma, si se unía la «A» y la «Z», una se permutaría por la otra). ¿Complicado? Pues sólo es el comienzo del sistema que inventaron los nazis para que la inteligencia aliada fuera sorda y ciega ante sus ataques y no pudiera interceptar sus mensajes.

En segundo lugar, el impulso eléctrico llegaba hasta tres rotores (o hasta cinco dependiendo del modelo de Enigma). Éstos podían colocarse a su vez en 26 posiciones diferentes –nuevamente, correspondiendo con cada una de las letras del abecedario-. Cuando el impulso eléctrico enviado por la letra que había sido pulsada pasaba a través de ellos, era modificada en otra dependiendo de cómo estuvieran configuradas las ruedas. De esta forma, si la «A» circulaba por los mecanismos ubicados en las posiciones «C-D-A», el resultado que se obtendría no sería el mismo que si estuvieran dispuestos como «H-T-L»).

El emisor y el receptor debían configurar de igual forma las posiciones de los rotores (por ejemplo «C-S-T») para que el mensaje pudiera ser enviado de forma satisfactoria. Si esta disposición previa no era igual, era imposible descifrar los datos adjuntados. Por otro lado, la descodificación también variaba dependiendo de la situación que tuvieran las ruedas (que eran extraíbles) antes de comenzar a escribir. De esta forma, el resultado no era el mismo si el engranaje número uno se hallaba en el centro de las tres posiciones en las que se podía encajar dentro de la máquina que se si encontraba a la izquierda o la derecha.



Las posiciones previas en las que debían estar los rotores eran enviadas, en principio, todos los días una vez a los operadores de radio y, en tiempos de guerra, llegaban a modificarse hasta en tres ocasiones por jornada. Por otro lado, y con el paso de los años, las tres letras necesarias para conocer la combinación inicial de las ruedas terminaron siendo diferentes en cada mensaje y eran seleccionadas por los propios operadores. Por lo tanto, el receptor siempre recibía tres caracteres sin cifrar al principio de cada mensaje codificado (los cuales se enviaban a través de código MORSE). Éstos se correspondían con la forma en la que debían ser colocados los mecanismos para que se pudieran descodificar las palabras de forma exitosa.



El complejo sistema de la Enigma no se quedaba en este punto, sino que, además, el rotor ubicado más a la derecha giraba una posición cada vez que se pulsaba una letra. Esto hacía que el sistema modificara la letra por enésima vez de una forma diferente y complicaba aún más si cabe la posible descodificación por parte de los aliados. Para terminar, y una vez que el primer mecanismo daba una vuelta completa, el segundo (el ubicado a su izquierda) giraba una posición, ofreciendo nuevas posibilidades de cifrado. La ingente cantidad de combinaciones existente provocó que los nazis creyeran indescifrable a la Enigma. No era para menos, pues el total era de casi 160.000.000.000.000.000.000.

El homosexual que venció a Hitler

La presunta invulnerabilidad de este aparato quedó destruida gracias a Alan Mathison Turing, un británico nacido en 1912 que –desde su más tierna infancia- había destacado por su capacidad innata para las matemáticas. Este inglés fue reclutado por el servicio secreto de su país en 1939 para tratar de descubrir los códigos alemanes. Por entonces era profesor en Cambridge y ya había sido reconocido por sus revolucionarios teoremas sobre la computación.

Con todo -y como señala Jesús Antonio Espinosa (Profesor Titular del Departamento de Tecnología Informática y Computación de la Universidad de Alicante) en su dossier **«Turing,**

el hombre que sabía demasiado»

-

el equipo británico no partía de cero, pues contaba con los grandes avances realizados por los polacos. Y es que varios expertos de este país habían logrado descifrar antes de la contienda los mensajes enviados por los nazis e, incluso, construir su propia Enigma (algo que no pudieron seguir haciendo después de que éstos mejoraran la máquina sucesivamente).

Desde ese año, Turing trabajó en Bletchnet Park, la sede oficial del gobierno inglés para códigos y cifrado, con el objetivo de acabar con la Enigma y su código. En aquella mansión victoriana reconvertida en cuartel general este británico pasó horas y horas con el objetivo de descubrir qué secretos había detrás de las, aparentemente, letras aleatorias de los mensajes alemanes que eran interceptados por los operadores de radio aliados. Como él, más de 10.000 personas (distribuidas en tres turnos diferentes) se enfrentaron a este reto, desde genios matemáticos, hasta expertos jugadores de ajedrez.

En los años posteriores, este británico modificó las máquinas utilizadas por los polacos para descifrar los mensajes antes de las evoluciones de la Enigma (las llamadas «Bombas») y creó su propia versión, la «Bombe». Mediante este aparato (que utilizaba complejos cálculos matemáticos y estadísticos para establecer las posiciones de los rotores), logró al fin desentrañar este misterioso código. Con el paso de los meses, el uso de este artilugio se generalizó hasta tal punto que se llegaron a descodificar miles y miles de mensajes enviados por los nazis. «En 1942, el descifrado de los mensajes alemanes se ejecutaba tan veloz que, a veces, dudaban de que los alemanes no se dieran cuenta», determina el experto español.

Esa no fue su única aportación a la lucha contra Hitler pues, a partir de 1940, Turing colaboró en el proyecto «Colossus». En este caso, el británico participó en la creación de una máquina lo suficientemente potente como para luchar contra los aparatos de cifrado alemanes SZ40/42. A su vez, este experto también realizó durante la contienda grandes avances en lo referente a la inteligencia artificial e, incluso, en proyectos que derivarían en la creación posterior del ordenador.

No obstante, ser uno de los artífices de la caída de Hitler no le sirvió para la condena que, en 1952, se le impuso por ser homosexual: la castración química. Según los expertos, este fue el detonante que, dos años después, le llevó a suicidarse. «Oficialmente Turing se suicidó. Su hastío por la vida a la cual lo llevaron constituye motivo suficiente para un suicidio. En julio de 1954 no le queda nada, después de menoscabar sus teorías, a principio de 1952 todo fue un cúmulo de mala suerte: le roba su amante, lo acusan de ultraje a la moral pública, lo condenan a la castración química, lo echan del trabajo… Sólo había una manzana, encima de la mesilla,

junto a la cama donde dormía, con un mordisco y rociada en una solución de Cianuro», completa Espinoza.

Fuente: ABC