

Historia de la Máquina de Cifrado Enigma

por Dirk Rijmenants

Traducido por Rafael Padilla.

En la historia de la famosa máquina de cifrado Enigma se combinan una tecnología ingeniosa, la historia militar, el misterioso mundo del espionaje, los criptoanalistas y los servicios de inteligencia en un asunto de verdadero suspense. Nunca antes el destino de tantas vidas se ha visto influenciado por una máquina criptográfica como en la Segunda Guerra Mundial. Enigma es el ejemplo más famoso y atrayente de la batalla entre los creadores de códigos y los criptoanalistas. Enigma mostró la importancia de la criptografía en la inteligencia civil y militar.

Orígenes de Enigma

Con la aparición, a principios de 1900, de las comunicaciones sin hilos, garantizar comunicaciones seguras inalámbricas para uso civil y militar se convirtió en un objetivo primordial. La búsqueda de algo que reemplazara a los poco prácticos y lentos sistemas de cifrado a mano se convirtió en algo esencial. En 1917, el Americano Edward Hugh Hebern desarrolló una máquina de cifrado con discos rotativos, en la que cada disco llevaba a cabo un cifrado de sustitución. La idea de Hebern fue la base para muchas máquinas similares, las cuales se desarrollaron en otros países.



En 1918, el ingeniero Arthur Scherbius patentó una máquina de cifrado que utilizaba rotores. Fueron por él contactadas la Marina de Guerra y el Ministerio de Asuntos Exteriores alemán, pero estos no mostraron ningún interés. En 1923, los derechos de estas patentes fueron a la compañía Chiffriermaschinen-AG, una compañía con Scherbius en el panel de directores, la cual comercializó la máquina. En 1927, Scherbius compró la patente de 1919 de una máquina similar realizada por el holandés Koch, con el objeto de asegurar su propia patente, aprobada en 1925.

La primera máquina de cifrado, la Enigma A, salió al mercado en 1923. Era una máquina grande y pesada, con una máquina de escribir integrada y que pesaba unos 50 Kg. Poco después se introdujo la Enigma B, una máquina muy similar. El peso y el tamaño de estas máquinas las hacía muy poco atractivas para su uso militar. El desarrollo del reflector, una idea del colega de Scherbius, Willi Korn, hizo posible el diseño de la mucho más ligera y compacta Enigma C. Asimismo, la máquina de escribir fue reemplazada por un panel de lámparas. En 1927 fue introducida y comercializada la Enigma D en diferentes versiones y vendida por toda Europa a diferentes servicios militares y diplomáticos.

El Ejército Suizo utilizó la Enigma K. La Marina Italiana compró el modelo comercial de Enigma D, tal como hizo España durante la Guerra Civil Española. Varios servicios de inteligencia tuvieron éxito al romper el cifrado de algunas versiones militares y civiles. Los criptoanalistas británicos, por ejemplo, vencieron a la Enigma española, la cual funcionaba sin un tablero de conexiones. Japón utilizó la Enigma T, también llamada la Enigma Tirpiz, una versión adaptada de la Enigma K. Japón desarrolló también su propia versión, con rotores colocados horizontalmente. Los mensajes de ambos modelos T y K también fueron descifrados.

Versiones Militares

En 1926, la Enigma comercial fue comprada por la Marina Alemana y adaptada para su uso militar. La llamaron Funkschlüssel C. En 1928, el German Abwehr (Servicio Secreto), la Wehrmacht y la Luftwaffe adquirieron su propia versión, la Enigma G, también llamada Zählwerk Enigma debido a su contador en el panel frontal. Este modelo utilizaba una caja de engranajes para avanzar los rotores y un reflector rotativo, pero no tenía panel de conexiones. La Wehrmacht revisó dicha máquina, añadiéndole el panel de conexiones y un sistema diferente de avance de los rotores. Esta versión, la Enigma I, llegó a ser conocida como la Wehrmacht Enigma, siendo introducida a gran escala en el ejército alemán y en las autoridades públicas. La Luftwaffe siguió el ejemplo de

la Wehrmacht en 1935. La Wehrmacht Enigma llevaba inicialmente un juego de tres rotores. A partir de 1939 en adelante, fueron equipadas con un juego de cinco rotores, los cuales se usaban de tres en tres. En 1934, la Marina de Guerra alemana adoptó el modelo de la Wehrmacht con su panel de conexiones más seguro y amplió el juego de posibles rotores hasta ocho. La máquina de la Marina fue llamada Funkschlüssel M ó M3. En 1941, aunque los servicios secretos alemanes (Abwehr) aseguraban que el código de la Enigma M3 era irrompible, el Almirante Karl Dönitz insistió en el mejoramiento de la Kriegsmarine Enigma. A principios de 1942, se introdujo en la Kriegsmarine el famoso modelo de cuatro rotores, la Enigma M4. Se calcula que fueron producidas un total de 100.000 máquinas.

Rompiendo el código

En 1932, el Biuro Szyfrow (Oficina de Cifrado) polaco comenzó con sus intentos para analizar y romper los mensajes Enigma. Aunque el jefe de este servicio recibió copias de los libros de códigos vendidos a la Oficina por el espía alemán Hasn-Thilo Schmidt, él no pasó esta información a sus criptoanalistas. Pensó que el ocultarles esta información serviría para estimular sus esfuerzos. Marian Rejewski, Henryk Zygalski y Jerzy Rozicki tuvieron éxito en romper los códigos Enigma y desarrollaron una máquina electromecánica llamada "Bomba" para acelerar dicho proceso de rotura de códigos. En los procedimientos alemanes de Enigma existían dos debilidades principales: La configuración global y la doble codificación de la clave del mensaje para evitar errores. Estas debilidades abrieron las puertas al criptoanálisis. En 1939, el Bureau ya no era capaz de romper los códigos debido a una aumento de sofisticación del diseño, a los nuevos procedimientos de codificación de la clave principal y a la falta de fondos para pagar a los criptoanalistas. Cuando Alemania invadió Polonia, los conocimientos de los polacos así como varias máquinas Enigma fueron pasadas a los servicios de inteligencia de Francia e Inglaterra.

Bletchley Park

La Escuela Gubernamental de Códigos y Cifra de Bletchley Park inicialmente rompió los códigos de Enigma a mano. En agosto de 1940, comenzaron a usar sus propias "Bombas", diseñadas por Alan Turing y Gordon Welchman. Estas consistían también en un dispositivo electromecánico rotativo, pero funcionaban basándose en un principio completamente diferente al de la Bomba de Rejewski. La "Bomba" de Turing buscaba los ajustes Enigma para un trozo dado de texto, del que disponían de sus versiones en claro y en clave. Cuando era interceptado un mensaje Enigma, los criptoanalistas tenían que buscar "chuletas" en el mismo. Estas "chuletas" consistían en trozos encriptados dentro del mensaje cuyo significado en claro se conocía. Dichos trozos podrían consistir en "An den Oberbefehlshaber", "An Gruppe", "Es lebe der Führer" o cualquier otro trozo de texto estandarizado. Una vez que se había localizado la chuleta (y existían diversas técnicas para ello), se entraban en la Bomba las asociaciones entre las letras del texto cifrado y su versión en claro. La Bomba, que contenía un gran número de tambores, cada uno de ellos replicando a los rotores de Enigma, ejecutaba todos los ajustes posibles para hallar los ajustes clave que correspondían a los trozos cifrados con el texto en claro. Una vez que se hallaban dichos ajustes, todos los mensajes encriptados con los mismos podían ser descifrados.

Toda la información relacionada con el criptoanálisis y el rompimiento de códigos tenía el nombre en clave de "Ultra" y desempeñó a menudo un rol importante –y a menudo decisivo– durante la guerra, principalmente en la Batalla del Atlántico. Toda la información Ultra era utilizada con extremo cuidado para evitar sospechas entre las fuerzas alemanas. En los cuarteles generales y en otros lugares estratégicos se colocaba a oficiales especiales de enlace, entrenados para tratar con este conocimiento valioso pero delicado. Además, nunca se utilizó la información de Ultra a menos que pudiera ser confirmada por una segunda fuente, para evitar dar razones a los mandos alemanes que les hicieran sospechar que sus comunicaciones de seguridad estaban siendo descifradas.

La Kriegsmarine

La Marina de Guerra Alemana –o Kriegsmarine– tuvo mucho éxito en aplicar su Rudeltaktik o "Tácticas de Grupos-Lobo" con los submarinos alemanes o U-Boot. Los Grupos-Lobo se desplegaban individualmente en busca de convoyes. Si un convoy era avistado, lo perseguían ocultos y avisaban a los demás submarinos del Grupo para que se unieran al ataque. Una vez que todos estaban en el lugar, hundían a todos los barcos del convoy gracias a un ataque cuidadosamente coordinado. Esta técnica fue tan devastadora para los suministros aliados que casi llegó a decidir el resultado de la guerra. La comunicación era la clave y los submarinos usaban Enigma para enviar los mensajes de coordinación de sus ataques. Tras algunos tiempos iniciales muy duros, Bletchley Park rompió los códigos navales casi de forma continua. La disminución de la efectividad de sus submarinos hizo sospechar al Almirante Dönitz y aunque la inteligencia alemana le aseguró que sus comunicaciones con Enigma eran seguras, él insistió en mejorar la seguridad de Enigma. A principios de 1942, se introdujo la famosa máquina de 4 rotores en la Kriegsmarine y los complicados códigos llamados 'Shark' causaron una gran crisis en Bletchley Park. La Kriegsmarine se refería a la primavera de 1942 como "los tiempos felices", dado que las fuerzas aliadas fueron incapaces de descifrar sus códigos y los submarinos alemanes fueron capaces de continuar hundiendo convoyes sin demasiada interferencia.

La marea cambia

Por medio del criptoanálisis, los criptoanalistas en Bletchley Park descubrieron que un cuarto rotor había entrado en el campo de batalla de los códigos. Tras diez meses de tensión insufrible por las enormes pérdidas, Bletchley Park tuvo éxito en romper los nuevos códigos 'Shark'. Esto se consiguió gracias a varias razones diferentes. Un factor importante fueron los libros de código Wetter-Kurzschlüssel (libros de código corto meteorológico), recuperados durante ataques a barcos meteorológicos y a submarinos, tales como el famoso ataque al U-599 del Kapitänleutnant Hans Heidtmann llevado a cabo por el barco británico HMS Petard. Tras recibir fuego pesado del HMS Petard, el submarino que se hundía fue abordado por tres marineros británicos. Consiguieron sacar del U-599 la Enigma de tres rotores y los libros de códigos Kurzsignale. Dos de ellos regresaron una vez más para tratar de hallar la Enigma de cuatro rotores, pero se fueron al fondo con el submarino. Esta misión fue un punto crucial para la rotura de 'Shark'.

A veces, debido a la falta de sus 'chuletas', Bletchley Park utilizaba una técnica a la que llamaron 'Jardinería'. Bombarderos británicos arrojaban o plantaban una serie de minas marinas en lugares bien determinados. Los submarinos alemanes, al avistar dichas minas, transmitían mensajes de contacto, aportando así nuevas 'chuletas' a los criptoanalistas. Asimismo, dentro de la red de radio de los submarinos, los mensajes meteorológicos codificados por medio del Wetter-Kurzschlüssel, eran enviados por la Enigma de 4 rotores puesta en el modo M3, que era menos complicado. Esto se hizo así para ser compatibles con la máquina de 3 rotores Enigma M3, la cual era la que usaban los barcos meteorológicos. Las "Bombes" existentes en Bletchley Park, desarrolladas para romper la Enigma de 3 rotores, tardaban más de 20 días en extraer los ajustes de las Enigma de cuatro rotores. Los ajustes de una Enigma de tres rotores, eran extraídos por dichas "Bombes" en menos de 24 horas. Mientras tanto, se desarrollaron nuevas "Bombes" para tratar con las Enigma de 4 rotores. Alrededor de Junio de 1943, la primera "Bombe" de cuatro rotores entró en acción y para finales del mismo año, otras cincuenta y cuatro "Bombes" más de cuatro rotores estaban operacionales en la marina americana. En el otoño de 1943, los mensajes 'Shark' de cualquier clase eran descifrados, por lo general, en menos de 24 horas.

La marea había cambiado para los submarinos alemanes. Excepto por algunos periodos breves, el sistema de comunicaciones alemán al completo era interceptado por un gran número de estaciones de escucha, llamadas Estaciones-Y y los códigos eran descifrados en Bletchley Park, en donde llegaron a trabajar en su cresta unas 7000 personas. Siendo conocidas las posiciones de los submarinos alemanes, los barcos aliados podían ahora evitar al enemigo y comenzó la caza activa de los submarinos. El arma de élite de la Kriegsmarine fue diezmada, dando como resultado pérdidas enormes entre las tripulaciones de los submarinos. Aproximadamente unos 700 submarinos y unos 30000 hombres de sus tripulaciones se perdieron en el mar. El mando alemán relacionó estas pérdidas con las nuevas técnicas de detección, tales como el sonar ASDIC, los aviones cazasubmarinos y a los destructores que escoltaban a los convoyes. Jamás se sospechó nada sobre el criptoanálisis de Enigma.

La información Ultra fue mantenida como de Alto Secreto durante toda la guerra y jugó un rol decisivo, no sólo en el Atlántico. El descifrado de los mensajes de la Wehrmacht y de la Luftwaffe también probó ser crucial. Los criptoanalistas expusieron las debilidades del Afrika Korps del notable Mariscal de Campo Rommel. La rapidez y los éxitos del Afrika Korps les crearon largos pasillos de suministros pobremente defendidos. La información de Ultra ofreció al Mariscal de Campo Montgomery una vital ventaja táctica. En los días previos al Día-D de la invasión de Normandía, la propia Wehrmacht, sin darse cuenta de ello, suministró a las fuerzas aliadas con enormes cantidades de información detallada acerca de las defensas costeras, la localización y fortaleza de las divisiones de tanques alemanes y el movimiento de sus tropas en Francia. Los expertos estiman que el quebrantamiento de Enigma acortó la duración de la guerra en tres años. El número de vidas salvadas no puede ser contado. Alemania siguió utilizando Enigma a lo largo de toda la guerra, sin sospechar nada.

La herencia de Enigma

Tras la segunda Guerra Mundial, Enigma representó la base para el desarrollo de máquinas de codificación más sofisticadas, tales como la suiza NEMA y la rusa M-125 Fialka. Aunque Enigma estaba muy bien diseñada y ofrecía, para aquellos días, una seguridad inquebrantable, su utilización negligente en las Fuerzas Armadas Alemanas y el material de los libros de código comprometido permitió a los criptoanalistas el convertir al mejor secreto de la guerra en un caballo de Troya y dar el pistoletazo de salida para la inteligencia criptográfica. En la actualidad, la Inteligencia de Señales (SIGINT) es considerada como una de las partes más vitales de la guerra moderna.

Páginas en Internet interesantes acerca de la máquina de Cifrado Enigma

Cipher Machines & Cryptology, the Enigma Sim home page:

<http://users.telenet.be/d.rijmenants>

Tom Perera's Enigma Museum:

<http://w1tp.com/enigma>

Frode's Crypto Cellar at CERN:

<http://frode.home.cern.ch/frode/crypto>

David Hamer's cryptology website:

<http://home.comcast.net/~dhamer>

Bletchley Park official site:

<http://www.bletchleypark.org.uk>

Enigma pages by Tony Sale:

<http://www.codesandciphers.org.uk/enigma>

The use of the naval 'Shark' code on U-boats and how it was broken

<http://www.uboat.net/technical/enigma.htm>

Breaking an original message, the double message key and Kenngruppen

<http://home.earthlink.net/~nbrass1/1enigma.htm>

History of solving the Enigma Cipher:

<http://www.enigmahistory.org/enigma.htm>

© Dirk Rijmenants 2004-2008