LA CLAVE ENIGMA

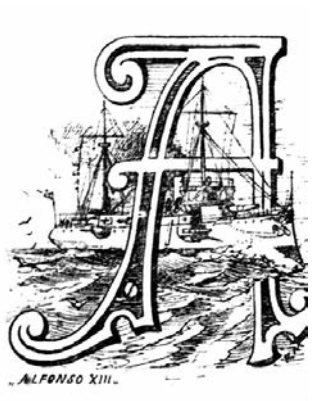
Antonio BARRO ORDOVÁS

(RE)

La guerre est un métier pour les ignorans, et une science pour les habiles gens.

Maurice de Saxe (1696-1750), *Mes Rêveries*.

Arthur Scherbius



ARTHUR Scherbius nació en Francfurt en 1878. Hijo de un hombre de negocios, estudió Electricidad en las universidades de Munich y Hannover, acabando su formación en 1903. Al año siguiente recibió el doctorado en Ingeniería. En 1918 fundó la empresa Scherbius & Ritter. Su fama se extendió pronto por Alemania por sus múltiples inventos, especialmente los relacionados con los motores asíncronos.

El 23 de febrero de 1918 patentó una máquina de cifrar basada en unas ruedas giratorias interconectadas eléctricamente por elementos conductores que hacían contacto con ellas al girar, y que fue conocida como la Rotor-Schlüsselmaschinen o Rotor-Chiffriermaschinen. Scherbius la comercializó con el nombre de Enigma, y en principio la utilizaron algunas compañías comerciales para cifrar sus comunicaciones. La Armada alemana de entreguerras, la Reichsmarine (Kriegsmarine desde 1935), adquirió una versión modificada en 1926. Años después, en 1928, el Ejército alemán (Reichswehr hasta 1935, posteriormente Heer) también adoptó la máquina, pero en una versión diferente a la de la Reichsmarine. En 1935 lo hizo la Luftwaffe.

Scherbius murió en 1929 en un accidente cuando viajaba en un coche de caballos.

El Biuro Szyfrów

Marian Rejewski. (Foto: *www.wikipedia.org*).

El Biuro Szyfrów era la agencia del Estado Mayor de las Fuerzas Armadas polacas encargada de la criptografía (el uso y estudio de cifras y códigos con el propósito de descifrarlos) en el período de entreguerras.

En 1929, el mismo año en que murió Scherbius, los polacos interceptaron una máquina Enigma en versión comercial que había sido enviada de Berlín a Varsovia, y que no se protegió, por error, como equipaje diplomático. Años más tarde, cuando el Reichswehr empezó a usar la Enigma militarizada, el Biuro Szyfrów intentó descifrar «el sistema», tratando de reconstruir el cableado de los rotores de la máquina militar y recuperar las configuraciones usadas en los mensajes.

En 1932, tres jóvenes matemáticos que trabajaban para el Biuro Szyfrów, Marian Rejewski, Jerzy Różycki y Henryk Zygalski, pudieron determinar el cableado de los rotores que utilizaban las máquinas del Reichswehr/Heer, consiguiendo descifrar gran parte de los mensajes que transmitía el Ejército alemán hasta los comienzos de la Segunda Guerra Mundial. Para ello construyeron un artificio que venía a ser «Enigma en paralelo» y que llamaron *bomba kryptologiczna*. Con independencia de sus trabajos, recibieron también ayuda de la inteligencia militar francesa.

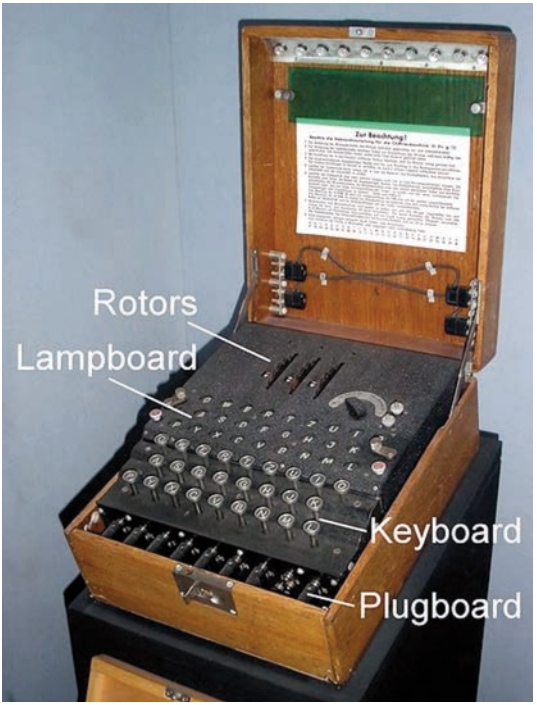
A partir de 1938, los alemanes fueron añadiendo modificaciones cada vez más complejas a sus máquinas, por lo que el descifrado de los mensajes se hacía más y más difícil, necesitándose de más medios y personal del que los polacos podían aportar. En julio de 1939, estos mostraron a los representantes de la inteligencia militar francesa y británica en Varsovia sus conocimientos sobre Enigma, incluyendo la *bomba kryptologiczna*, y les entregaron algunas de sus réplicas de la máquina. Esta información fue valiosísima para los alia-

dos, y en ella se basaron los futuros logros de los servicios de criptoanálisis británicos ubicados en Bletchley Park.

Cuando los alemanes invadieron Polonia el 1 de septiembre de 1939, la mayoría del personal del Biuro Szyfrów consiguió escapar a Francia, donde siguió trabajando con los servicios de la inteligencia militar francesa. Tras la invasión de Francia el 10 de mayo de 1940, algunos de los matemáticos polacos escaparon al Reino Unido.

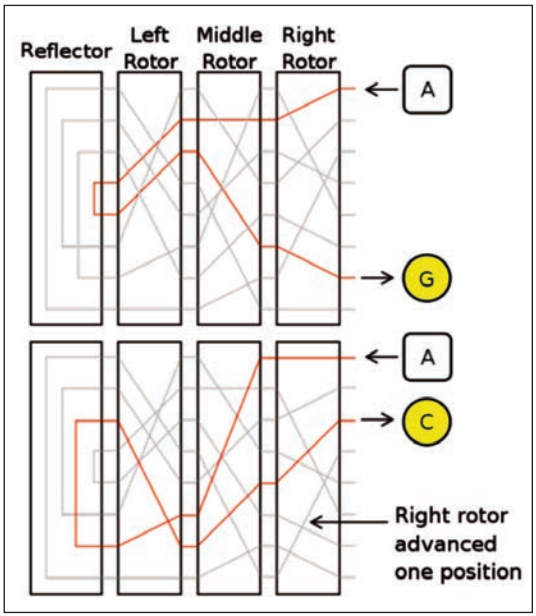
El funcionamiento de Enigma

La máquina Enigma consistía básicamente en un teclado como el de una máquina de escribir; un poco más hacia arriba, había un panel con letras que se iluminaban al pulsar las teclas, y más allá del panel había tres o cuatro ranuras, dependiendo del tipo de máquina, donde se introducían los correspondientes *walzen,* o rotores, con 26 posiciones cada uno, que se podían «configurar inicialmente», a mano, en una posición relativa determinada por las letras que aparecían en unas ventanillas delante de cada rotor. Al configurar la máquina, se podían intercambiar los rotores, de los que algunas disponían de cinco, seis, siete y hasta ocho en total para intercambiar entre las tres o cuatro ranuras, aumentado así el número de combinaciones de rotores, que iban numerados en romanos del I al VIII. A la derecha de los rotores había una batería. En la parte frontal se encontraba el Steckerbrett o panel de interconexión (*plugboard*), que conectaba las letras por parejas, haciendo cambalaches entre ellas (hasta seis pares de letras en la mayoría de las máquinas) para aumentar aún más la complejidad del cifrado.



Enigma de tres rotores. (Foto: *www.wikipedia.org*).

El Heer y la Luftwaffe tenían modelos de tres ranuras (tres rotores en funcionamien-



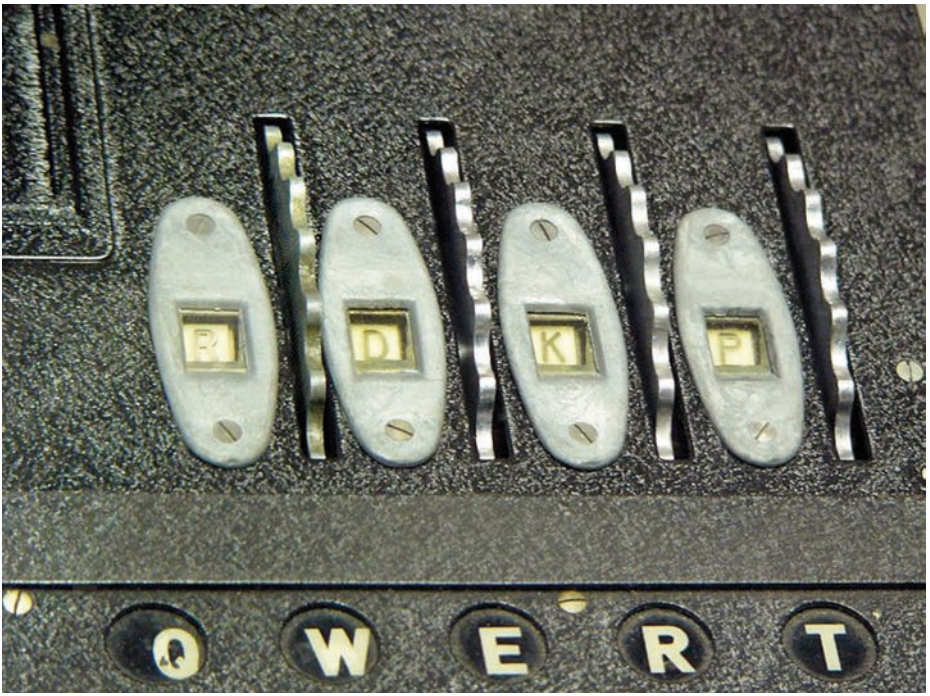
Funcionamiento del cableado de los rotores al pulsar dos veces la A. (Autor: Messer Woland). (Foto: *www.wikipedia.org*).

to) y cinco para intercambiar. La Kriegsmarine al principio tenía máquinas de tres ranuras y seis rotores para intercambiar, que luego aumentaron a siete y ocho; posteriormente cambió a las de cuatro ranuras, llamadas también de cuatro rotores, aunque seguían teniendo los ocho rotores para intercambiar.

Los rotores tenían una serie de conectores en cada cara, interconectados por un cableado interior (la disposición exacta de la interconexión de los cables era uno de los secretos de la máquina) que era diferente para cada rotor. Los conectores de los rotores conectaban a estos entre sí y la corriente cerraba el circuito a través de una rueda o rotor fijo, llamado *umkehrwalze* (rotor de inversión) por los alemanes o *reflector* por los británicos, situada en un extremo de los rotores, que hacía que la corriente eléctrica volviera a circular otra vez por estos, pero siguiendo un camino diferente al inicial.

Cuando se pulsaba una tecla, se cerraba el circuito y se iluminaba una de las letras del panel, que nunca coincidía con la letra pulsada, tras lo cual el rotor de la derecha giraba una posición de las 26, haciendo que al presionar otra vez se encendiera otra letra distinta, aun cuando la pulsada en la tecla fuera la misma. Cuando este rotor había girado 26 posiciones, el siguiente rotaba una posición, cambiando la configuración relativa de los rotores. Cuando el segundo había girado a su vez 26 posiciones, el tercero lo hacía una posición, y así sucesivamente.

Al comienzo del mensaje había un grupo de seis letras en las máquinas de tres rotores (ocho en las de cuatro) que indicaba la posición relativa de estos para ese mensaje determinado. En realidad era un grupo de tres letras repetido (o cuatro en las de cuatro rotores). Por ejemplo, si se quería que la posición relativa de los rotores fuera RDKP, el transmisor del mensaje tecleaba RDKPRDKP y en el panel de luces se iluminaban ocho letras distintas, por ejmplo, LANCXJIH; esos caracteres eran los que se transmitían por radio al comienzo del texto. Al recibirse el mensaje, el operario ponía los rotores en



Máquina de cuatro rotores con configuración RDKP. (Foto: *www.wikipedia.org*).

una «configuración inicial», leía la hoja con el mensaje cifrado y tecleaba LANCXJIH, encendiéndose las luces RDKPRDKP; a continuación giraba a mano los rotores a las posiciones R, D, K y P y continuaba tecleando el resto del mensaje con esa configuración y apuntando en una hoja de papel las letras iluminadas correspondientes. Existían unos libros de edición mensual en los que entrando con la fecha del día se obtenía la «configuración inicial» o «posición base» (*Grundstellung*) correspondiente.

Para hacer aún más difícil el descifrado, los rotores tenían otro «truco» que consistía en girar unos anillos interiores (*Ringstellung*) con las 26 letras, con respecto a sus propios conectores eléctricos, es decir podían cambiar hasta 26 veces la interconexión del cableado que unía los conectores de un lado y otro del rotor. En resumen, se podían hacer los siguientes cambios:

— Decidir cuáles de los cinco u ocho rotores había que escoger, y establecer su orden en las ranuras (*Walzenlage*).
— Cambiar la posición de los conectores de un lado del rotor respecto a los del otro lado (*Ringstellung*).

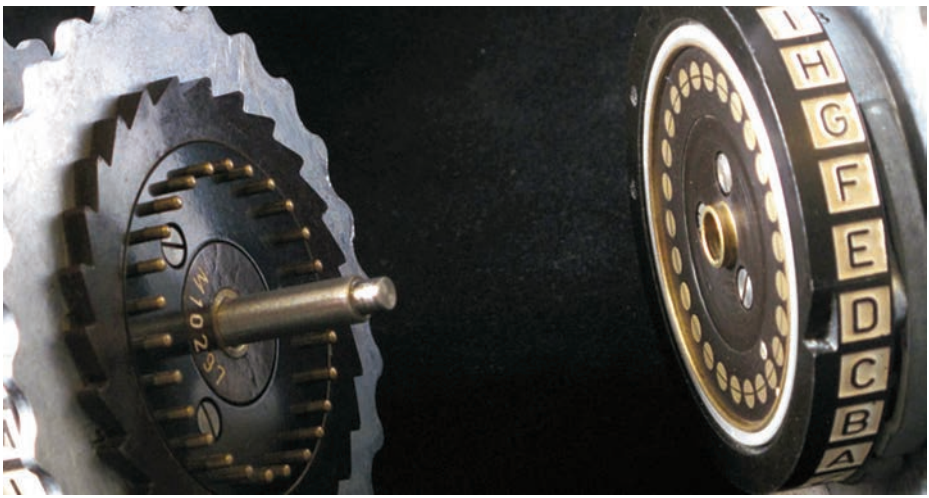
— Configurar las conexiones de las seis (o más, según la máquina) parejas de letras en el Steckerbrett o panel de interconexión frontal (*Steckerverbindungen*).
— Determinar la «configuración inicial» de los rotores para poder definir a su vez la configuración de los mismos para un mensaje específico (*Grundstellung*).

Naturalmente, para hacer todo esto se necesitaban unos códigos. Los códigos navales eran unos libros de pastas rojas, de tinta soluble en agua sobre papel rosado, de forma que fueran fáciles de destruir en caso de emergencia.

Un ejemplo de una página de un código militar alemán de una Schlüsselmaschinen de tres rotores (para simplificar se supone que no hay rotores para intercambiar) podría ser el siguiente:

DATUM	*WALZENLAGE*	*RINGSTELLUNG*	*STECKERVERBINDUNGEN*	*GRUNDSTELLUNG*
01	III I II	0 X R	DO RZ XO UP LS QN	RDK
02	II III I	R T I	UX KI SW TA OR NU	TLF
03	III II I	A K P	HR DY BN SK AT VT	DSE

Las combinaciones que se pueden hacer de acuerdo con la tabla para un día determinado serían:



Rotores mostrando los conectores de uno y otro lado, y el *Ringstellung* a la derecha. (Foto: *www.wikipedia.org*).

— Combinaciones de rotores (*Walzenlage*): 6.
— Posición de los conectores (*Ringstellung*): 26 x 26 x 26 = 7.576.
— Parejas de letras (*Steckerverbindungen*): 100.391.791.500.
— «Configuración inicial» de rotores (*Grundstellung*): 26 x 26 x 2 = 17.576.
— Total de combinaciones: 1.06×10^{16}.

Normalmente los mensajes se reducían a unos cuantos cientos de letras, por lo que no había ninguna posibilidad de que se repitiera alguna posición combinada de rotores, negando así a los expertos en análisis criptográfico las pistas necesarias para descifrar según la técnica llamada «análisis de frecuencia».

Si la máquina tenía cuatro rotores, y además había otros para intercambiar, las combinaciones posibles eran muchísimo mayores.

En general, los procedimientos y códigos de la Kriegsmarine (Kenngruppenheft o Kenngruppenbuch, código de los *U-boote*) eran más elaborados y seguros que los del Heer y la Luftwaffe. Esta es una de las razones por las que los británicos tardaron más en descifrar la Enigma naval, aparte de la mayor utilización de rotores, y de que en febrero de 1942 se cambió a una máquina de cuatro rotores (con ocho para intercambiar).

En la mayoría había que escribir a mano el resultado que indicaban las luces; no obstante, algunas de cuatro rotores utilizaban una pequeña impresora llamada Schreibmax, que estaba situada en la parte superior de la Enigma y que era capaz de imprimir el texto del mensaje en una estrecha cinta de papel.

Bletchley Park y Ultra

Bletchley Park era una mansión inglesa construida en el siglo XVIII y situada a 80 km al noroeste de Londres. En mayo de 1938 el almirante Sir Hugh Sinclair, jefe del Secret Intelligence Service (SIS o MI6) adquirió la finca para que la utilizase el Government Code and Cypher School (GC&CS). El jefe del GC&CS desde 1919 hasta 1942 fue el capitán de fragata Alastair Denniston, que se instaló en Bletchey Park en 1938. Cuando Gran Bretaña declaró la guerra a Alemania, Denniston solicitó personal civil para apoyar al GC&CS, gente con perfil de profesor de Matemáticas, pero también jugadores de ajedrez e incluso expertos en crucigramas. De las universidades de Oxford y Cambridge llegaron matemáticos, como Peter Twinn, Alan Turing y Gordon Welchman, entre los que destacaría posteriormente Turing. Durante la guerra, para ocultar la existencia de Bletchley Park se la denominaba de diferentes formas, tales como: BP, Station X, London Signals Intelligence Centre y Government Communications Headquarters.

Los británicos comenzaron sus trabajos basándose en la información proporcionada por los matemáticos polacos del Biuro Szyfrów y desarrollaron

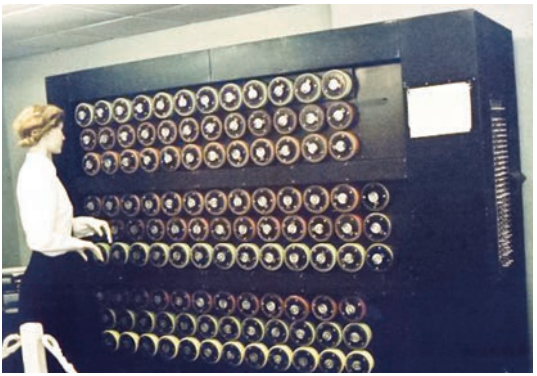
Bletchley Park. (Foto: *www.wikipedia.org*).

una máquina electromecánica, llamada *bombe,* basada en la *bomba kryptologiczna,* pero más compleja y elaborada. La *bombe* era una máquina de forma paralelepípeda de 2,1 x 0,61 x 2,1 m, que pesaba aproximadamente una tonelada, tenía 108 rotores que simulaban los de las máquinas alemanas y tres tambores indicadores, y equivalía a 36 Enigmas; había sido diseñada por Alan Turing con la ayuda de Gordon Welchman y construida por la British Tabulating Machine Company. Su función era descubrir los ajustes diarios de la Enigma, es decir, los rotores en uso, sus posiciones relativas en la máquina, la posición de los conectores y el cableado del panel frontal.

El primer código que empezaron a descifrar los británicos fue el de la Luftwaffe, luego el del Heer, y no fue hasta 1941 —en que se capturaron el pesquero armado *Krebs*, el *U-110* y dos buques meteorológicos— cuando se empezaron a leer los mensajes de la Kriegsmarine. Cuando esta introdujo la Enigma de cuatro rotores, en febrero de 1942, hubo un «apagón» informativo de diez meses, hasta diciembre de 1942, en que se reanudó el descifrado gracias a la captura de los códigos del *U-559* en el Mediterráneo (octubre 1942).

El sistema de descifrado británico se parecía básicamente al polaco, aunque modificado de acuerdo con la evolución de las máquinas, y era bastante complejo. Se basaba en errores del sistema Enigma, como por ejemplo que al pulsar una tecla determinada la letra correspondiente a dicha tecla no aparecía nunca en el panel de luces; o bien en la repetición de los formularios para ciertos tipos de mensajes, como los informes meteorológicos de los *U-boote*. A veces eran fallos de los operadores alemanes que, por pereza,

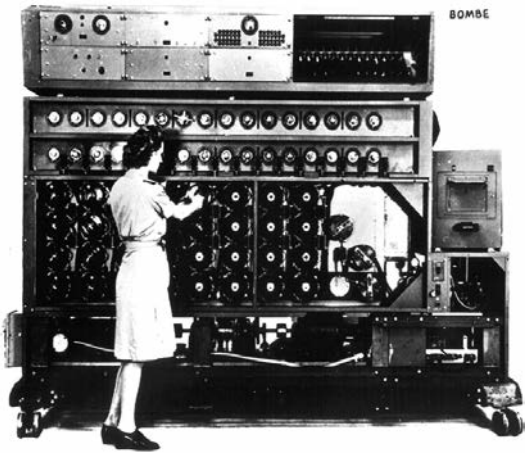
usaban siempre las mismas configuraciones de rotores para cifrar los mensajes. Se aprovechaban los estereotipos, frases como «sin novedad» u otras parecidas que se repetían con frecuencia. Estas técnicas se basaban pues en suposiciones, y cuando una de ellas era acertada se denominaba *crib;* a partir de ahí, la configuración de rotores y otros parámetros que daba la *bombe* se introducían en la máquina Enigma capturada y se podían leer los mensajes hasta las 24:00, hora en que los alemanes cambiaban la configuración.



Maqueta de *bombe* británica. (Autor: Sarah Hartwell). (Foto: *www.wikipedia.org*).

A partir de junio de 1941, la British Military Intelligence empezó a denominar Ultra al descifrado de mensajes enemigos por el GC&CS en Bletchley Park.

Con ayuda de los británicos, los americanos consiguieron desarrollar sus propias *bombes,* que eran mucho más rápidas que sus contrapartes británicas. La US Navy tuvo lista su primera máquina el 3 de mayo de 1943. Sus dimensiones eran 3 x 0,61 x 2,1 m y pesaba 2,5 t. La producción de *bombes* de la US Navy llegó a alcanzar un ritmo de dos por semana y se construyeron 121 hasta septiembre de 1944. Las americanas descifraron mensajes especialmente difíciles y transmitían constantemente su información al Reino Unido por cable haciendo uso de una máquina de cifrar combinada angloamericana.



Bombe de la US Navy. (Foto: *www.wikipedia.org*).

Algunas consecuencias de los logros de Bletchley Park

En verano de 1940, durante la Batalla de Inglaterra, los británicos leían a diario los informes que enviaban los mandos de la Luftwaffe desde canal de la Mancha a Berlín, por lo que sabían el número exacto de

aviones alemanes derribados por los cazas británicos, que no coincidía con el que se apuntaban los pilotos de la RAF, que era bastante más elevado que el real y además se publicaba en los periódicos. Si bien la RAF derribaba por lo general más aviones alemanes que estos a los británicos, las cifras no eran tan abultadas y eran sobre todo de bombarderos, pero no de cazas, ya que en la lucha caza contra caza iban ganando los *Messerschmitt Me-109,* y el Fighter Command se estaba quedando sin pilotos (1).

El mando británico se planteó la posibilidad de decir la verdad, pero consideró que esto afectaría negativamente a la moral de la nación y decidió apuntar a los pilotos los derribos que ellos decían y publicar dichas cifras en los periódicos.

Durante la ocupación alemana de la URSS, unidades del Heer descubrieron en el bosque de Katyn, cerca de Smolensk, unas fosas con 4.421 (2) cadáveres de militares polacos fusilados, la mayoría de ellos oficiales. Los alemanes identificaron los de los oficiales que habían sido internados en el campo de concentración de Kozelsk antes de abril de 1940 y transmitieron por radio el hallazgo a Berlín, transmisión que fue descifrada por Ultra. El 13 de abril de 1943, el ministro de Propaganda del III Reich, Joseph Goebbels, aprovechó este hecho para introducir una brecha entre los aliados occidentales y la URSS, pero los soviéticos echaron las culpas de la matanza a los alemanes, acusándolos de haber asesinado a los polacos tras la invasión de esa zona en julio de 1941. Los británicos, aunque sabían la verdad porque habían descifrado el mensaje del Heer a Berlín, callaron para no comprometer a sus aliados soviéticos, a pesar de las protestas del Gobierno polaco en el exilio, que hicieron que el Gobierno soviético rompiera relaciones con los polacos el 25 de abril de 1943.

El 13 de octubre de 1990, Mijaíl Gorbachov reconoció que la responsabilidad de las matanzas de Katyn había sido soviética.

Antes de la ofensiva de Kursk (Operación ZITADELLE), el GC&CS de Bletchley Park informó a los soviéticos del ataque alemán, lo que se complementó con los informes del espía Rudolf Roessler (*Lucy*), refugiado alemán en Suiza al servicio de los aliados. Los soviéticos tuvieron tiempo de preparar las defensas alrededor de Kursk para desgastar a las divisiones alemanas durante el inicio de la ofensiva, pasando al contraataque tras una semana de combates.

---

(1) Las cifras de derribos de cazas durante los cuatro meses de la Batalla de Inglaterra fueron: 219 *Spitfire* derribados *versus* 180 *Messerschmitt,* y 272 *Hurricane* derribados *versus* 153 *Messerschmitt* (*Messerschmitt Bf 109 in action. Part 1*. BEAMAN, John R.; CAMPBELL, Jr. & Jerry L., 1980).

(2) El número total de polacos asesinados por los soviéticos, incluyendo los de otras fosas y campos de concentración, además de los de Katyn, fue de 21.857. (*Paracuellos-Katyn, un ensayo sobre el genocidio de la izquierda*. VIDAL, César. Libros Libres, abril de 2005).

Ultra y la Batalla del Atlántico

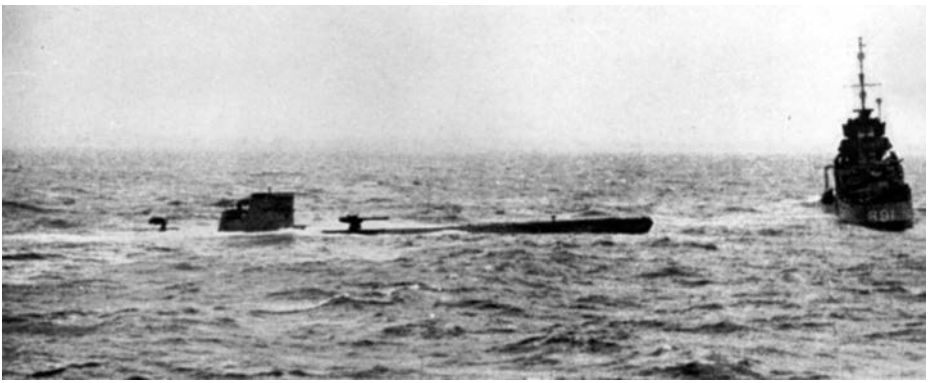
En marzo de 1941 la Royal Navy capturó el pesquero armado alemán *Krebs* en aguas de Noruega, apoderándose de la máquina Enigma y de los correspondientes códigos. A partir de entonces Bletchley Park empezó a leer los mensajes de la Kriegsmarine.

El 7 de mayo de 1941 cuatro *U-boote* (*U-94, U-110, U-201* y *U-556*) avistaron el convoy *OB-318* en el Atlántico Norte y lo atacaron durante cuatro días. El *U-110* (Kptlt. Fritz-Julius Lemp) había hundido los mercantes británicos *Bengore Head* y *Esmond,* pero el día 9 fue atacado con cargas de profundidad por los destructores HMS *Broadway,* HMS *Bulldog* y la corbeta HMS *Aubretia*, obligándole a emerger con averías.

Una vez en superficie la dotación del *U-boot* abandonó el buque, y a continuación el *Bulldog* mandó un bote con un trozo de abordaje que capturó una máquina Enigma con un mensaje listo para transmitir y varios códigos y libros confidenciales. El submarino fue llevado a remolque por el destructor, pero se hundió el 11 de mayo. Para completar estos apresamientos, la Royal Navy capturó también los buques meteorológicos *München* y *Lauenburg* al nordeste de Islandia en mayo y junio de 1941 respectivamente.

El descifrado de la Enigma naval a partir de la primavera de 1941 posibilitó a los convoyes aliados seguir rumbos de evasión de las líneas de patrulla de los *U-boote,* haciendo que estos consiguieran pocas interceptaciones, con lo que disminuyeron las cifras de hundimientos de mercantes durante el resto del año y los alemanes empezaron a sospechar que los británicos leían sus mensajes.

Las cosas cambiaron en febrero de 1942 por dos razones: en primer lugar el B-Dienst (servicio criptográfico alemán) consiguió descifrar la clave de la



El *U-110* y el HMS *Bulldog*, que capturó una máquina Enigma y los códigos de cifrado. (Foto: *www.wikipedia.org*).

Royal Navy (British Naval Cypher N.º 3), con lo que el BdU (3) fue capaz de leer el 80 por 100 de los mensajes navales británicos y, por consiguiente, dirigir a los *U-boote* a interceptar las rutas de los convoyes dadas por el Almirantazgo; en segundo lugar, el BdU introdujo un cuarto rotor en las máquinas Enigma navales durante el mismo mes de febrero, con lo que Bletchley Park dejó de leer los mensajes alemanes durante los diez meses siguientes.

El 30 de octubre de 1942, el *U-559* fue atacado con cargas de profundidad por cinco destructores británicos a unas 60 millas al NE de Port Said y tuvo que salir a superficie con averías. Cuando la dotación abandonó el buque, un bote del destructor HMS *Petard* envió un trozo de abordaje que consiguió recuperar los códigos Enigma antes de que el *U-boot* se hundiera.

Gracias a esto, Bletchley Park fue capaz de volver a leer los mensajes de la Kriegsmarine desde mediados de diciembre de 1942. No obstante, esta ventaja fue anulada temporalmente por el hecho de que el B-Dienst seguía descifrando los de la Royal Navy cifrados con la British Naval Cypher N.º 3, y por consiguiente los alemanes podían saber cuáles eran las rutas evasivas de los mercantes y a su vez dar nuevos rumbos a sus *U-boote* para interceptar a los convoyes aliados.

El *U-505* tras ser capturado por el USS *Guadalcanal*. (Foto: *www.wikipedia.org*).

(3) *Befehlshaber der Unterseeboote* (BdU): comandante en jefe de los *U-boote,* aunque BdU se utilizaba también para nombrar al Estado Mayor del almirante o a su cuartel general.

El 10 de junio de 1943, los británicos adoptaron la British Naval Cypher N.º 5, clave que los alemanes fueron incapaces de descifrar durante el resto de la guerra, con lo que ya no pudieron leer los mensajes con las rutas evasivas de los convoyes.

El 4 de junio de 1944, el portaaviones de escolta USS *Guadalcanal* y cinco destructores capturaron en el Atlántico al *U-505,* apoderándose de sus códigos, que ayudaron al descifrado de la Enigma naval durante el período de validez de los mismos.

Algunas consideraciones

El descifrado de las claves Enigma de la Kriegsmarine en 1941 y 1942, tras haber capturado la Royal Navy algunas máquinas y los códigos de los distintos buques alemanes, ayudó a desviar algunos convoyes, especialmente en la segunda mitad de 1941; pero, como se dijo anteriormente, desde febrero de 1942 el B-Dienst también leía la British Naval Cypher N.º 3, y por tanto fue capaz de contrarrestar la labor de Ultra hasta el 10 de junio de 1943. En cualquier caso la información de Ultra sirvió tanto para evitar hundimientos de mercantes como para ayudar a localizar submarinos; pero lo que en realidad hizo ganar la Batalla del Atlántico, y por ende la guerra, fue la conjunción de aviones de patrulla marítima (especialmente el *B-24 Liberator*), los grupos *Hunter Killer* (un portaaviones de escolta y varios destructores) y los *support groups* o grupos de apoyo de escoltas, cuyo cometido era atacar a los submarinos alemanes que se encontraban en las proximidades de los convoyes, dejando el cuidado del destacamento a sus escoltas. Esta gran cantidad de buques y aviones consiguió cambiar las tornas de la Batalla del Atlántico en mayo de 1943, fecha en que el número de submarinos alemanes hundidos (41) fue superior al de los entregados (26) por los astilleros a la Kriegsmarine. Este mes fue llamado *Schwarzer Mai* (Mayo Negro) por el propio BdU, y los alemanes todavía leían la British Naval Cypher N.º 3. El 10 de junio, cuando los británicos cambiaron a la British Naval Cypher N.º 5, que los alemanes fueron incapaces de descifrar durante el resto de la contienda, la guerra submarina ya estaba sentenciada a pesar del canto de cisne de los *Unterseeboote* en septiembre de 1943.

Por otra parte, el conocimiento de los movimientos del enemigo no siempre aseguraba la victoria. Ejemplos de esto se dieron varias veces:

— En julio de 1942, el convoy *PQ-17*, que llevaba material de guerra para la URSS por la ruta del Ártico, recibió una orden de dispersión prematura, originada por el First Sea Lord, almirante Sir Dudley Pound, pese a que este había sido avisado por Ultra de que los buques pesados alemanes no habían abandonado los fiordos noruegos. Como

consecuencia de la citada orden de dispersión, los *U-boote* y aviones de la Luftwaffe basados en Noruega hundieron aproximadamente el 65 por 100 de los buques del convoy.

— En septiembre de 1943, una línea de 19 *U-boote* se encontraba desplegada hacia el oeste de los convoyes *ON 202 y ONS 18*; no obstante, a pesar de que los británicos tenían la clave Enigma, los servicios de inteligencia de la Royal Navy fueron incapaces de informar a tiempo de la presencia de los submarinos alemanes, por lo que no pudieron desviar a ambos convoyes de la barrera de buques enemigos, que acabaron con seis mercantes y cuatro escoltas por la pérdida de tres submarinos.

Otro fallo similar fue la Operación MARKET GARDEN (septiembre 1944) en Holanda, en la que la Primera División Aerotransportada británica y la Primera Brigada Paracaidista polaca independiente tenían la misión de capturar el puente de Arnhem. El mando de la operación había sido informado por *Ultra* de que en las inmediaciones de la ciudad se encontraban las 9.ª y 10.ª divisiones Panzer de las SS. A pesar de la información, la operación aliada fue un desastre.

Conclusiones

Los verdaderos pioneros de los trabajos aliados que condujeron al descifrado de la clave Enigma fueron los matemáticos polacos Marian Rejewski, Jerzy Różycki y Henryk Zygalski, especialmente el primero, aunque Alan Turing y otros británicos, y posteriormente norteamericanos, consiguieron completar y llevar a buen término los desarrollos de las *bombes* y los correspondientes éxitos de Ultra.

Si bien la información obtenida por esta última fue una contribución muy importante en la consecución de la victoria aliada, especialmente en la Batalla del Atlántico, no está del todo claro hasta qué punto fue decisiva, a pesar de que algunos aseguran que acortó considerablemente la guerra. Winston Churchill, una vez finalizada la contienda, le dijo al rey George VI: *It was thanks to Ultra that we won the war* (4); pero para lograr la victoria, además de información, hacían falta medios.

En definitiva, el descifrado de la clave Enigma fue una valiosa ayuda para el esfuerzo bélico aliado, pero lo que en realidad hizo que se ganara la batalla del Atlántico, y por consiguiente la guerra, fue la colosal producción industrial americana.

---

(4) *http://www.history.co.uk/study-topics/history-of-ww2/code-breaking*.

BIBLIOGRAFÍA

JONES, R. V.: *Most Secret War*. Wordsworth Editions Limited, 1998.
TARRANT, V. E.*: The U-Boat Offensive, 1914-1945*. Año 1989.
IRVING, David: *The Destruction of Convoy PQ-17*. St. Martin's Press Edition, October 1989.
BEAMAN, John R.; CAMPBELL, Jerry L.: *Messerschmitt Bf 109 in action. Part 1*. Squadron/Signal Publications, Inc. 1980.
VIDAL, César: *Paracuellos-Katyn, un ensayo sobre el genocidio de la izquierda*. Libros Libres.
http://en.wikipedia.org/wiki/Bletchley_Park
http://en.wikipedia.org/wiki/Ultra
http://www.history.co.uk/study-topics/history-of-ww2/code-breaking
http://en.wikipedia.org/wiki/Enigma_machine
http://es.wikipedia.org/wiki/Enigma_(máquina)
http://en.wikipedia.org/wiki/Arthur_Scherbius
http://es.wikipedia.org/wiki/Bombe
http://en.wikipedia.org/wiki/German_submarine_U-505
http://www.uboat.net:8080/boats/u110.htm
http://en.wikipedia.org/wiki/German_weather_ship_Lauenburg
Encyclopaedia Britannica (*Micropaedia, t. 6*). The University of Chicago, 1985.
The inner workings of an Enigma Machine. Perimeter Institute for Theoretical Physics *(YouTube)*.
Bletchley Park Tour (YouTube).