Temas para la Educación
revista digital para profesionales de la enseñanza
Nº 10 - Septiembre 2010 | Federación de Enseñanza de CC.OO. de Andalucía | ISNN: 1989-4023 | Dep. Leg.: GR 2786-2008

Enigma: Las Matemáticas ganaron la Segunda Guerra Mundial.

Introducción

Algunos historiadores dirían que este título es exagerado y que el conflicto lo ganó el mayor poder industrial aliado o su gran cantidad de hombres, tanques, aviones y buques. Pero en momentos clave de la guerra las matemáticas permiten a los aliados sobrevivir y evitar el desastre o una Paz negociada del conflicto. Tres son los momentos donde las matemáticas son clave:

- Batalla de Inglaterra
- Guerra antisubmarina
- Bomba atómica

En este artículo se explicará el segundo punto. Se verá como de decisiva, para las bajas de los submarinos, fue el descifrar las claves de la máquina enigma.

En este artículo se expondrá el funcionamiento de la máquina Enigma era un dispositivo electromecánico, lo que significa que usaba una combinación de partes mecánicas y eléctricas. El mecanismo estaba constituido fundamentalmente por un teclado similar al de las máquinas de escribir cuyas teclas eran interruptores eléctricos, un engranaje mecánico y un panel de luces con las letras del alfabeto. Cómo Marian Adán Rejewski fue fundamental en descifrar esta máquina y como afectó a la guerra submarina.

1.- ¿Qué era Enigma?

Enigma era el nombre de una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes.

Su fama se debe a haber sido adoptada por las fuerzas militares de Alemania desde 1930. Su facilidad de manejo y supuesta inviolabilidad fueron las principales razones para su amplio uso. Su sistema de cifrado fue finalmente descubierto, y la lectura de la información que contenían los mensajes supuestamente protegidos, es considerado, a veces, como la causa de haber podido concluir la Segunda Guerra Mundial, al menos, un año antes de lo que hubiera acaecido sin su descifrado.

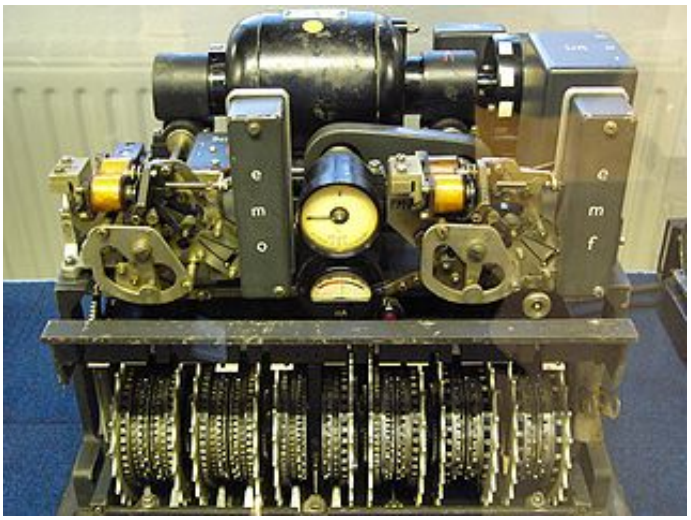
Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

Versiones de la máquina Enigma fueron utilizadas por Alemania y otras potencias del Eje en prácticamente todas las comunicaciones por radio y telégrafo. Incluso la información relativa a las previsiones meteorológicas era cifrada con la máquina Enigma. Una versión comercial sin modificaciones de la máquina se utilizó para cifrar las comunicaciones militares de los españoles durante la Guerra Civil Española y los italianos durante la Segunda Guerra Mundial.

2.- ¿Cómo funciona Enigma?

La máquina Enigma era un **dispositivo electromecánico**, lo que significa que usaba una combinación de partes mecánicas y eléctricas. El mecanismo estaba constituido fundamentalmente por un teclado similar al de las máquinas de escribir cuyas teclas eran interruptores eléctricos, un engranaje mecánico y un panel de luces con las letras del alfabeto.

Los *dispositivos electromecánicos* son los que combinan partes eléctricas y mecánicas para conformar su mecanismo. Ejemplos de estos dispositivos son los motores eléctricos y los dispositivos mecánicos movidos por estos, así como las ya obsoletas calculadoras mecánicas y máquinas de sumar; los relés; las válvulas a solenoide; y las diversas clases de interruptores y llaves de selección eléctricas.



La parte eléctrica consistía en una batería que se conecta a una de las lámparas, que representan las diferentes letras del alfabeto. Se puede observar en la parte inferior de la imagen adjunta el teclado, siendo las lámparas los minúsculos círculos que aparecen encima de éste.

El corazón de la máquina Enigma era mecánico y constaba de varios *rotores* conectados entre sí. Un rotor es un disco circular plano con 26 contactos eléctricos en cada cara, uno por cada letra del alfabeto. Cada contacto de una cara está conectado o cableado a un contacto diferente de la cara contraria. Por ejemplo, en un rotor en particular, el contacto número 1 de una cara puede estar conectado con el contacto número 14 en la otra cara y el contacto número 5 de una cara con el número 22 de la otra. Cada uno de los cinco rotores proporcionados con la máquina Enigma estaba cableado de una forma diferente y los rotores utilizados por el ejército alemán poseían un cableado distinto al de los modelos comerciales.

Dentro de la máquina había, en la mayoría de las versiones, tres ranuras para poder introducir los rotores. Cada uno de los rotores se encajaba en la ranura correspondiente de forma que sus contactos de salida se conectaban con los contactos de entrada del rotor siguiente. El tercer y último rotor se conectaba, en la mayoría de los casos, a un *reflector* que conectaba el contacto de salida del tercer rotor con otro contacto del mismo rotor para realizar el mismo proceso pero en sentido

contrario y por una ruta diferente. La existencia del reflector diferencia a la máquina Enigma de otras máquinas de cifrado basadas en rotores de la época.

Cuando se pulsaba una tecla en el teclado, por ejemplo la correspondiente a la letra A, la corriente eléctrica procedente de la batería se dirigía hasta el contacto correspondiente a la letra A del primer rotor. La corriente atravesaba el cableado interno del primer rotor y se situaba, por ejemplo, en el contacto correspondiente a la letra J en el lado contrario. Supongamos que este contacto del primer rotor estaba alineado con el contacto correspondiente a la letra X del segundo rotor. La corriente llegaba al segundo rotor y seguía su camino a través del segundo y tercer rotor, el reflector y de nuevo a través de los tres rotores en el camino de vuelta. Al final del trayecto, la salida del primer rotor se conectaba a la lámpara correspondiente a una letra, distinta de la A, en el panel de luces. El mensaje de cifrado se obtenía por tanto sustituyendo las letras del texto original por las proporcionadas por la máquina.

Cada vez que se introducía una letra del mensaje original, pulsando la tecla correspondiente en el teclado, la posición de los rotores variaba. Debido a esta variación, a dos letras idénticas en el mensaje original, por ejemplo AA, les correspondían dos letras diferentes en el mensaje cifrado, por ejemplo QL. En la mayoría de las versiones de la máquina, el primer rotor avanzaba una posición con cada letra. Cuando se habían introducido 26 letras y por tanto el primer rotor había completado una vuelta completa, se avanzaba en una muesca la posición del segundo rotor, y cuando éste terminaba su vuelta, se variaba la posición del tercer rotor. El número de *pasos* que provocaba el avance de cada uno de los rotores, era un parámetro configurable por el operario.

Debido a que el cableado de cada rotor era diferente, la secuencia exacta de los alfabetos de sustitución variaba en función de qué rotores estaban instalados en las ranuras (cada máquina disponía de cinco), su orden de instalación y la posición inicial de cada uno. A estos datos se les conocía con el nombre de *configuración inicial*, y eran distribuidos, mensualmente al principio y con mayor frecuencia a medida que avanzaba la guerra, en libros a los usuarios de las máquinas.

El funcionamiento de las versiones más comunes de la máquina Enigma era simétrico en el sentido de que el proceso de descifrado era análogo al proceso de cifrado. Para obtener el mensaje original sólo había que introducir las letras del mensaje cifrado en la máquina, y ésta devolvía una a una las letras del mensaje original, siempre y cuando la *configuración inicial* de la máquina fuera idéntica a la utilizada al cifrar la información.

3.- Orígenes del Criptoanálisis.

La **criptografía** (del griego κρύπτω *krypto*, «oculto», y γράφω *graphos*, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leidos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. Posiblemente, el primer criptosistema que se conoce fuera documentado por el historiador griego **Polibio**: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente **Julio César** lo empleó en sus campañas, uno de los más conocidos en la literatura (según algunos autores, en realidad Julio César no usaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de este método de sustitución ha quedado para los anales de la historia).

En 1465 el italiano **Leon Battista Alberti** inventó un nuevo sistema de sustitución polialfabética que supuso un gran avance de la época.

Otro de los criptógrafos más importantes del siglo XVI fue el francés **Blaise de Vigenère** que escribió un importante tratado sobre "la escritura secreta" y que diseñó una cifra que ha llegado a nuestros días asociada a su nombre.

Durante los siglos XVII, XVIII y XIX, el interés de los monarcas por la criptografía fue notable. Las tropas de Felipe II emplearon durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés **François Viète** consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos.

Por su parte, la reina María Estuardo, reina de Escocia, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

El *descifrado* es el proceso inverso que recupera el *texto plano* a partir del *criptograma* y la *clave*. El *protocolo criptográfico* especifica los detalles de cómo se utilizan los *algoritmos* y las *claves* (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de *protocolos*, *algoritmos de cifrado*, procesos de gestión de claves y actuaciones de los usuarios, es lo que constituyen en conjunto un *criptosistema*, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de *cifras*: los algoritmos que usan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado*, y los que emplean una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Los primeros se denominan *cifras simétricas*, de *clave simétrica* o de *clave privada*, y son la base de los algoritmos de cifrado clásico. Los segundos se denominan *cifras asimétricas*, de *clave asimétrica* o de *clave pública* y forman el núcleo de las técnicas de cifrado modernas.

Por muchos años, los criptógrafos procuraron ocultar las frecuencias usando varias sustituciones diferentes para las letras comunes, pero esto no puede ocultar completamente los patrones en las sustituciones para las letras del texto original. Tales códigos eran descubiertos extensamente hacia el año 1500.

Una técnica para hacer más difícil el análisis de frecuencia es utilizar una sustitución diferente para cada letra, no sólo las comunes. Éste sería normalmente un proceso muy costoso en tiempo que requirió a ambas partes intercambiar sus patrones de sustitución antes de enviar mensajes cifrados.

A mitad del siglo XV, una nueva técnica fue inventada por Alberti, ahora conocida generalmente como cifrado polialfabético, que proporcionó una técnica simple para crear una multiplicidad de patrones de sustitución. Las dos partes intercambiarían una cantidad de información pequeña (referida como la clave) y seguirían una técnica simple que produce muchos alfabetos de sustitución, y muchas sustituciones diferentes para cada letra del texto original. La idea es más simple y eficaz, pero resultó ser más difícil de lo esperado. Muchos cifrados fueron implementaciones parciales del concepto, y eran más fáciles de romperse que los anteriores (p.ej. el cifrado de Vigenère). Tomó varios cientos de años antes de que los métodos apropiados para romper cifrados polialfabéticos de manera confiable fueran encontrados.

Las nuevas técnicas confiaron en la estadística para descubrir la información sobre la clave usada para un mensaje. Charles Babbage, y su **máquina diferencial,** y William F. Friedman están entre los que aportaron la mayor parte del trabajo para desarrollar estas técnicas.

4.- ¿Cómo fue descifrada la máquina enigma?

El uso de rotores múltiples en Enigma brindó un modo simple de determinar qué alfabeto de sustitución usar para un mensaje en particular (en el proceso de cifrado) y para un texto cifrado (en el de descifrado). En este respecto fue similar al cifrado polialfabético. Sin embargo, a diferencia de la mayoría de las variantes del sistema polialfabético, el Enigma no tenía una longitud de clave obvia, debido a que los rotores generaban una nueva sustitución alfabética en cada teclazo, y toda la secuencia de alfabetos de sustitución podía ser cambiada haciendo girar uno o más rotores, cambiando el orden de los rotores, etc., antes de comenzar una nueva codificación. En el sentido más simple, Enigma tuvo un repertorio de 26 x 26 x 26 = 17.576 alfabetos de sustitución para cualquier combinación y orden de rotores dada. Mientras el mensaje original no fuera de más de 17.576 pulsaciones, no habría un uso repetido de un alfabeto de sustitución. Pero las máquinas del Enigma agregaron otras posibilidades. La secuencia de los alfabetos utilizados era diferente si los rotores fueran colocados en la posición ABC, en comparación con ACB; había un anillo que rotaba en cada rotor que se podría fijar en una posición diferente, y la posición inicial de cada rotor era también variable. Y la mayoría de los Enigmas de uso militar agregaron un *stecker* (tablero de interconexión) que cambió varias asignaciones de llave (8 o más dependiendo de modelo). Así pues, esta llave se puede comunicar fácilmente a otro usuario. Son apenas algunos valores simples: rotores a utilizar, orden del rotor, posiciones de los anillos, posición inicial y ajustes del tablero de interconexión.

Por supuesto, si la configuración estuviera disponible, un criptoanalista podría simplemente poner un equipo Enigma a la misma configuración y descifrar el mensaje. Uno podría mandar libros de configuración a usar, pero podrían interceptarse. En cambio, los alemanes establecieron un sistema astuto que mezcló los dos diseños.

Al principio de cada mes, se daba a los operadores de la Enigma un nuevo libro que contenía las configuraciones iniciales para la máquina. Por ejemplo, en un día particular las configuraciones podrían ser poner el rotor n.° 1 en la hendidura 7, el n.° 2 en la 4 y el n.° 3 en la 6. Están entonces rotados, para que la hendidura 1 esté en la letra X, la hendidura 2 en la letra J y la hendidura 3 en la A. Como los rotores podían permutarse en la máquina, con tres rotores en tres hendiduras se obtienen otras 3 x 2 x 1 = 6 combinaciones para considerar, para dar un total de 105.456 posibles alfabetos. Había también un anillo para cada rotor que aún agrega más variaciones. El operador seleccionaría algunas otras configuraciones para los rotores, esta vez definiendo sólo las posiciones o "giros" de los rotores. Un operador en particular podría seleccionar ABC, y éstos se convierten en la configuración del 'mensaje para esa sesión de cifrado'. Entonces teclearon la configuración del mensaje en la máquina que aún está con la configuración inicial. Los alemanes, creyendo que le otorgaban más seguridad al proceso, lo tecleaban dos veces, pero esto se desveló como una de las brechas de seguridad con la que "romper" el secreto de Enigma. Los resultados serían codificados para que la secuencia ABC tecleada dos veces podría convertirse en XHTLOA. El operador entonces gira los rotores a la configuración del mensaje, ABC. Entonces se teclea el resto del mensaje y lo envía por la radio.

En el extremo receptor, el funcionamiento se invierte. El operador pone la máquina en la configuración inicial e introduce las primeras seis letras del mensaje. Al hacer esto él verá ABCABC en la máquina. Entonces gira los rotores a ABC y el resto del mensaje cifrado, descifrándolo.

Este sistema era excelente porque el criptoánalis se basa en algún tipo de análisis de frecuencias. Aunque se enviaran muchos mensajes en cualquier día con seis letras a partir de la configuración inicial, se asumía que esas letras eran al azar. Mientras que un ataque en el propio cifrado era posible, en cada mensaje se usó un cifrado diferente, lo que hace que el análisis de frecuencia sea inútil en la práctica. Con computadoras modernas, las cosas podrían haber sido diferentes, pero con lápiz y papel...

Y también se dice que ellos habían leido algún tráfico codificado italiano con una de las versiones comerciales. Pero cuando la Kriegsmarine (la Armada alemana) empezó a usar la Enigma a mitad de los años 20, nadie pudo leer el tráfico. Cuando el Ejército alemán comenzó a emplear una versión ligeramente diferente en los primeros años 30, tampoco se pudo leer tráfico alguno. Hay informes de que criptoanalistas británicos de la Escuela Gubernamental de Cifrados y Códigos y franceses también se rindieron, considerando a las Enigma militares alemanas como irrompibles.

El esfuerzo que rompió el cifrado alemán empezó en 1929 cuando los polacos interceptaron una máquina Enigma enviada de Berlín a Varsovia y equivocadamente no protegida como equipaje diplomático. No era una versión militar, pero proporcionó una pista de que los alemanes podrían estar utilizando una máquina de tipo Enigma en el futuro. Cuando el Ejército alemán comenzó a usar Enigmas modificadas años después, los polacos intentaron "romper el sistema" buscando el cableado de los rotores usados en la versión del Ejército y encontrando una manera de recuperar las configuraciones usadas para cada mensaje en particular.

Un joven matemático polaco, **Marian Adán Rejewski** fue el matemático y criptógrafo polaco que, en 1932, solucionó la máquina Enigma, el dispositivo de cifrado principal usado por Alemania en la Segunda Guerra Mundial.

El éxito de Rejewski y sus colegas impulsaron a Inglaterra a leer los mensajes de Enigma, y la inteligencia así ganada, llamada código "ultra", contribuyó, decisivamente, a la derrota de Alemania.

Mientras estudiaba matemáticas en la Universidad Poznań, Rejewski había atendido a un curso secreto de criptología conducido por la Oficina de Cifrado del Estado Mayor, con la que se unió a tiempo completo en 1932. La Oficina había alcanzado poco éxito leyendo la Enigma, y a finales de 1932 designó a Rejewski para trabajar en el problema. Después de solamente algunas semanas, él dedujo el cableado interno

secreto del Enigma. Rejewski y dos colegas matemáticos entonces desarrollaron una variedad de técnicas para el desciframiento regular de los mensajes del Enigma. Las contribuciones de Rejewski incluyen la idea del "catálogo de tarjetas", derivado usando su "ciclómetro", y la "bomba".

Cinco semanas antes de la invasión alemana de Polonia en 1939, Rejewski y sus colegas presentaron sus resultados sobre el descifrado del Enigma a los representantes de la inteligencia francesa y británica. Poco después del estallido de la guerra, los criptólogos polacos fueron evacuados a Francia, en donde continuaron su trabajo con la colaboración de Inglaterra y Francia. Rejewski y su compañero matemático Henryk Zygalski huyeron, vía España, Portugal y Gibraltar, a Gran Bretaña. Allí trabajaron en una unidad del ejército polaco, solucionando cifrados alemanes de bajo nivel. En 1946 Rejewski retornó con su familia a Polonia y trabajó como contable, permaneciendo en silencio con respecto a su trabajo criptológico hasta 1967.

Usó técnicas fundamentales de matemáticas y estadística al encontrar una manera de combinarlas. Rejewski notó un patrón que probó ser vital; puesto que el código del mensaje se repitió dos veces al principio del mensaje, podría suponerse el cableado de un rotor no por las letras, sino por la manera que estas cambiaban.

Encontrar las cadenas apropiadas de las 10545 combinaciones era toda una tarea. Rejewski desarrolló un número de métodos de ayuda. Una técnica utilizaba unas tiras en blanco para cada rotor mostrando cuáles letras podrían encadenarse, bloqueando las letras que no podrían encadenarse. Los usuarios tomarían las tiras sobreponiéndolas, buscando las selecciones donde estaban completamente claras las tres letras. Los británicos también habían desarrollado tal técnica cuando tuvieron éxito en romper la Enigma comercial, aunque intentaron (y no lograron) romper las versiones militares del Enigma.

Algunas fuentes sostienen que en 1938 un mecánico polaco empleado en una fábrica alemana que producía las máquinas Enigma tomó notas de los componentes antes de ser repatriado y, con la ayuda de los servicios secretos británicos y franceses, construyeron un modelo en madera de la máquina. Hay también una historia sobre una emboscada hecha por la resistencia polaca a un vehículo del ejército alemán que llevaba una máquina Enigma.

Los polacos, conscientes de que la invasión alemana se acercaba e incapaces de extender sus técnicas con los recursos disponibles, decidieron a mediados de 1939 compartir su trabajo, y pasaron a los franceses y británicos algunas de sus réplicas Enigma, así como información sobre el descubrimiento de Rejewski y otras técnicas que ellos habían desarrollado. Todo eso se envió a Francia en valija diplomática; la parte británica fue a Bletchley Park a 80 km al norte de Londres.

Al inicio de la guerra, el producto del Bletchley Park tenía por nombre en clave 'Boniface' para dar la impresión a los no iniciados de que la fuente era un agente secreto. Tal fue el secretismo alrededor de los informes de 'Boniface' que 'sus' informes se llevaron directamente a Winston Churchill en una caja cerrada con llave, de la cual el primer ministro tenía personalmente la llave. La información así producida fue denominada "Ultra".

Sin lugar a dudas la figura que más destaca es Alan Turing, **Alan Mathison Turing** (1912-1954) fue un matemático, informático teórico, criptógrafo y filósofo inglés.

Desde noviembre de 1942 hasta marzo de 1943, Turing estuvo en Estados Unidos trabajando en colaboración en decodificación y también en un sistema de discurso secreto. Cambios en la forma en que Alemania codificaba sus mensajes llevaron a que Bletchley perdiera su habilidad para decodificar los mensajes. Turing no estuvo involucrado directamente con el quiebre exitoso de estos códigos más complejos, pero sus ideas probaron ser de la mayor importancia en ello. Turing fue premiado con la Alta Orden del Imperio Británico en 1945, por su vital contribución al esfuerzo de guerra.

Para romper los códigos de la máquina Enigma, Turing diseñó la bombe, una máquina electromecánica —llamada así en reconocimiento de la diseñada por los polacos bomba kryptologiczna— que se utilizaba para eliminar una gran cantidad de claves enigma candidatas. Para cada combinación posible se implementaba eléctricamente una cadena de deducciones lógicas. Era posible detectar cuándo ocurría una contradicción y desechar la combinación.

5.- ¿Cómo afectó el descifrar los códigos de la Enigma?

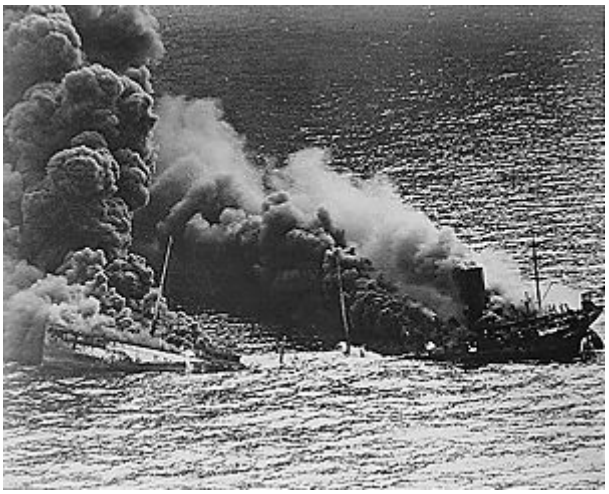
Inicios: septiembre de 1939 - mayo de 1940.
Con una flota de submarinos obsoletos, Alemania no podía hacer mucho. Fueron hundidos 222 barcos mercantes ingleses, que equivalen a 900.000 toneladas, una pérdida que Gran Bretaña estaba preparada para soportar. El almirante Dönitz sabía que a este paso jamás ganarían la guerra y presionaba a Hitler para que construyera más submarinos.

El tiempo feliz: junio de 1940 - marzo de 1941.
La invasión de Francia y la ocupación de Noruega cambiaron el mapa geopolítico de forma adversa a Inglaterra. La ocupación de los puertos noruegos y franceses permitió a los alemanes alcanzar el interior del Atlántico y las costas africanas, hundiendo a buques mercantes desprovistos de escolta aérea. En esta etapa de la guerra fueron hundidos 1.600.000 toneladas de barcos mercantes. Sin embargo, Gran Bretaña se esforzó en aguantar estas pérdidas, ya que sabía que si permitía ser bloqueada, Alemania la invadiría. Los capitanes Otto Kretschmer, Wofgang Lüth y Günther Prien alcanzaron su fama en acciones individuales porque todavía no se implementaba la *manada de lobos*.

Recuperación británica: abril de 1941 - diciembre de 1941.
En 1941, el almirante británico Percy Noble tomó el mando de la campaña antisubmarina en el Atlántico. Noble estaba convencido de la efectividad de los convoyes y adoptó medidas para regularizar la táctica. Ante la falta de buques de escolta, se utilizaron las corbetas, que eran baratas y ejecutaban la tarea de escolta de manera eficiente. Los británicos empezaron entonces a recibir ayuda externa, primero de Canadá, que comenzó a escoltar los buques mercantes desde la mitad de la travesía del Atlántico, luego de Estados Unidos, que empezó a prestar destructores a Gran Bretaña a cambio de bases en el Océano Pacífico.

Al lograr descifrar la máquina alemana Enigma, los británicos se anotaron una gran victoria. En la fotografía se muestran varias máquinas Enigma
En esta época, los criptoanalistas de Bletchley Park lograron desarrollar el programa *Ultra*, que permitía descifrar la máquina criptográfica alemana *Enigma*, una tecnología que sin duda posibilitó a los aliados localizar con mayor facilidad a los submarinos alemanes. Poco después los aliados también pudieron detectar el origen de las transmisiones de radio de los submarinos, consiguiendo otra arma tecnológica importante contra Alemania.
En marzo de 1941, la Kriegsmarine sufrió un duro golpe cuando en un mismo mes, cuatro de los *Ases de los Abismos* - Otto Kretschmer, Joachim Matz, Joachim Schepke y Günther Prien - fueron capturados o muertos en batalla.

El segundo tiempo feliz: enero de 1942 - febrero de 1943.
Aunque Estados Unidos declaró la guerra a Alemania en 1941, su participación en el Atlántico fue casi nula ese año. Sin embargo, el presidente Franklin Delano Roosevelt siempre pensó en ganar la guerra primero en Europa y luego ir contra Japón, por lo que insistió en la necesidad de limpiar el Atlántico de submarinos alemanes antes de enviar a los soldados estadounidenses a Europa.



Inesperadamente, la incursión estadounidense contra Alemania tuvo un efecto contraproducente para los aliados. Los estadounidenses no tenían mucha confianza en la táctica de los convoyes y dudaban en usarlos. Además, los submarinos alemanes ahora podían enfrentarse abiertamente a los buques mercantes norteamericanos, que hasta entonces habían navegado por las aguas del mar Caribe despreocupadamente.

En enero de 1942, la cifra de hundimientos era de 180.000 toneladas, algo inaceptable para la Kriegsmarine. Sin embargo, las cifras de hundimientos por U-Bootes se empezaron a disparar rápidamente, ya que los estadounidenses le dejaban el trabajo fácil a los lobos de mar. Debido a que todavía no se obligaba a apagar las luces de las ciudades costeras de Estados Unidos, los submarinos alemanes encontraban fácilmente los puertos y se detenían en la entrada a esperar que zarpase un buque mercante. De esta manera, a pesar de que sólo doce U-Bootes podían hacer el viaje hasta la costa este de los Estados Unidos, se logró superar en junio la cifra de 700.000 toneladas mensuales, que según Dönitz era suficiente para bloquear a Gran Bretaña.

Aunque el Comandante de la Flota del Atlántico, el estadounidense Ernest King, rechazaba completamente los convoyes asegurando que no disponían de los destructores para poder proteger los convoyes y los transportes de soldados al mismo tiempo, las altas cifras de hundimientos lo obligaron a introducir en julio el sistema de convoyes en el Atlántico, hundiendo inmediatamente siete U-Bootes. Sin embargo, como King temía, se dejaron muchas zonas sin proteger, y los submarinos alemanes se trasladaron al golfo de México y a las costas frente a Venezuela, hundiendo muchos petroleros.

Finalmente, los submarinos alemanes llegaron a sumar 300 en agosto, otorgando a Dönitz los recursos suficientes para poner en práctica "la manada de lobos" a plenitud. De esta manera, las cifras de hundimientos, que habían estado bajando desde la implementación de los convoyes en Estados Unidos, aumentaron de nuevo para noviembre.
El almirante Dönitz logró por fin demostrar la utilidad de los submarinos en la economía de guerra, y eventualmente fue promovido a Gran Almirante de la Flota,

mientras que el almirante Raeder fue depuesto de su cargo al perder varios cruceros en el mar de Barents. Desde entonces, Alemania se dedicó a construir submarinos.

Momento clave: Marzo de 1943.
Los criptoanalistas de Bletchley Park, Inglaterra, la estación X, sede de los servicios secretos británicos, se enfrentan a su peor pesadilla: inesperadamente, los submarinos nazis U-boat han cambiado el código de la máquina enigma que utilizan para comunicarse entre sí y con el alto mando alemán. Un convoy de barcos de mercancías aliado que está cruzando el atlántico con diez mil pasajeros e importantes suministros está en peligro de ataque. Las autoridades recurren a Tom Jericho (Dougray Scott), un brillante matemático y experto descifrador de códigos de la inteligencia británica, el hombre que había conseguido descifrar el anterior código nazi, denominado "shark", empleado por la flota submarina alemana.

Derrota de la Kriegsmarine: mayo de 1943 - septiembre de 1943.
La introducción eficiente de los convoyes acabó con las esperanzas alemanas en la "manada de lobos". En la fotografía un convoy aliado se dirige a Ciudad del Cabo. No obstante, el peligro estaba sobrevalorado, puesto que la mayoría de los mercantes hundidos no se dirigían a Inglaterra, pero el presidente Roosevelt consideraba todavía el Atlántico demasiado peligroso como para enviar a las tropas a Europa.

El almirante Dönitz tenía grandes planes para 1943. Dado que los puertos enemigos se habían vuelto muy peligrosos, decidió enfocarse de nuevo en la brecha del centro del Atlántico. Para marzo de 1943, los submarinos habían hundido 600.000 toneladas de buques, y la inmensa mayoría de estos se dirigía a Inglaterra, lo que confirmaba la confianza alemana.


Morteros antisubmarinos

Sin embargo, al dar Roosevelt la orden de limpiar el Atlántico, se puso al mando de los Accesos Occidentales al almirante Max Horton, que incrementó la protección de los convoyes, y con los buques que sobraban organizó escuadrones "cazasubmarinos" o "Hunter Killer", que rondaban por una zona esperando encontrar un sumergible alemán y hundirlo. Además, se mejoró el sonar y se perfeccionó el lanzamiento de cargas de profundidad, llegándose a lanzar hasta 24 cargas por la proa con mayor precisión. Por último, los nuevos aviones con alta autonomía de vuelo disponían de un potente radar que les permitía localizar fácilmente a los submarinos y, como contaban con sus propias cargas de profundidad, podían atacar a los U-Bootes sin esperar ayuda. Repentinamente, los sumergibles empezaron a ser hundidos rápidamente gracias a la superior tecnología aliada.
El mayor desastre para la Kriegsmarine ocurrió en mayo de 1943. El convoy ONS-5 fue atacado por muchas "manadas de lobos", sumando 50 sumergibles en total, que

libraron una lucha brutal en el Atlántico. Sin embargo, sólo un tercio de los barcos del convoy fueron hundidos, siendo echados a pique 41 U-bootes alemanes. La carnicería fue tan grande que Dönitz retiró a todos los buques de este tipo del Atlántico Norte, ya que, como posteriormente escribió en su diario, se dio cuenta de que Alemania había perdido la batalla del Atlántico.

En septiembre, Alemania contaba con los nuevos torpedos acústicos y una nueva clase de submarinos llamados "clase Walter". Estos avances motivaron que Dönitz intentara suerte de nuevo en el Atlántico Norte, y aunque los U-Bootes obtuvieron algunas victorias, 25 de ellos nunca regresaron a puerto. A principios de 1944, Dönitz volvió a enviar a sus submarinos a la mar, pero esta vez la derrota alemana fue evidente: 37 sumergibles fueron destruidos, hundiendo sólo tres buques mercantes. Lo peor de todo es que la mayoría ni siquiera había podido salir del golfo de Vizcaya, donde estaban la mayoría de los puertos alemanes.

Resultados finales.
Los submarinos alemanes hundieron en total 2.848 buques mercantes, que equivalen a 14.000.000 de toneladas. El desarrollo de nuevas tecnologías y nuevas tácticas en ambos bandos inclinaron la balanza de un lado al otro, pero al final, Alemania no pudo hacer frente a las potencias tecnológicas angloparlantes. Por el lado alemán, el porcentaje de bajas fue alarmente: de los 1.170 U-bootes alemanes que participaron en la Segunda Guerra Mundial, 785 fueron hundidos por los aliados, sin contar los que fueron hundidos en accidentes, capturados o desaparecieron. La llegada tardía de los Submarinos del tipo XXI, no pudo subsanar lo que 6 años de guerra no habían podido hacer. En total, el 75% de los sumergibles fueron hundidos o capturados, un porcentaje de bajas más alto que la de los kamikazes japoneses.

Pérdidas por año de guerra [editar]
- 1939: 9 unidades
- 1940: 24 unidades
- 1941: 35 unidades
- 1942: 87 unidades
- 1943: 237 unidades
- 1944: 242 unidades
- 1945: 151 unidades

TOTAL: 785 submarinos perdidos
Supervivientes: **108 unidades** (12,0%)

Bibliografía

- Webs:

http://www.wikipedia.org
http://www.google.com

- Libros de consulta:

Guzmán, M. y Colera, J. *"Matemáticas II"* Editorial Anaya.
Siglo XX. *"La guerra submarina"* Editorial Orbis.
Imágenes de la Guerra. *"Historia de la II Guerra Mundial"* Ediciones Rialp.