Detalles Técnicos de la Máquina Enigma
por Dirk Rijmenants.

Traducción y notas por Rafael Padilla.

Diagrama de Cableado

La máquina Enigma es un dispositivo electromecánico. Consta de un teclado (con la disposición QWERTZ alemana), de un panel de bombillas que representa al alfabeto, de un panel frontal de conexiones y de tres o cuatro rotores. Estos rotores avanzan cada vez que se pulsa una tecla. La pulsación de una tecla es convertida, a través de los rotores y del panel de conexiones, en el encendido de una lámpara, la cual representará a la letra ya codificada. La máquina también posee en su interior un compartimento para una batería de 4 voltios y en su exterior también existe una toma de enchufe bipolar para conectar la máquina a una fuente de alimentación exterior o a un transformador de corriente alterna.

El dibujo de la izquierda muestra el cableado. Para simplificar el examen, sólo se muestran 4 de los componentes. En realidad, hay 26 bombillas, teclas, zócalos del panel de conexiones y cables de conexión en el interior de los roto-res. La corriente fluye desde la batería [1] a través del con-mutador bidireccional accionado por la tecla [2], hasta el panel de conexiones [3]. Dicho panel de conexiones permite el re-conexionado del cableado entre el tecla-do [2] y la rueda de entrada fija (*Entreittwalze*, o *ETW*) [4]. A continuación, como se puede ver clara-mente en nuestro ejemplo, la corriente procede a través del zócalo – en este caso cerrado- del panel [3] a través de la rueda de entrada fija [4] hasta el cableado cruzado de cada uno de los tres (Wehrmacht Enigma) o cuatro (Kriegsmarine Enigma) rotores [5] y llega hasta el reflector (*Umkehrwalze* o *UKW*, en alemán) [6]. El reflector devuelve la corriente , por un camino diferente, de regreso otra vez a través de los rotores [5] y la rueda de entrada [4], hasta llegar de nuevo al panel de conexiones, a la toma “S”, que está conectada por el cable [8] (en este caso) a la toma “D” y desde allí, otro interruptor bidireccional [9] la lleva hasta la bombilla. Obsérvese que al pulsar una tecla, primero se mueven los rotores con su mecanismo de avance a continuación se envía la corriente eléctrica hasta la bombilla que corresponda. Si la tecla es soltada, la bombilla dejará inmediatamente de brillar. Por lo tanto, cuando no hay ninguna tecla pulsada, ¡será visible siempre en las ventanas de observación la posición de los rotores correspondiente a la última letra encriptada!

La imagen de arriba representa la disposición mecánica de la Enigma, en vista de perfil derecho, con aproximadamente el mismo diagrama de cableado que el anterior.

Los rotores

Los rotores (*Walzen* en alemán) son los elementos más importantes de la máquina. Estos discos redondos, de aproximadamente unos 10 cm de diámetro, están hechos de metal o de baquelita. Un disco consiste en un alojamiento redondo con una muesca en un lugar fijo y un anillo giratorio con las 26 letras del alfabeto (alemán) o los 26 números correspondientes a las mismas. El centro del rotor consiste en un pequeño disco rotatorio con 26 contactos protuberantes accionados por muelle en el lado derecho, cableados uno a uno de forma mezclada con otros 26 contactos planos en el lado izquierdo. El cambiar la posición del cableado interno en relación con la muesca y con el alfabeto es llamado ajuste de los anillos o *Ringstellung*.

La disposición del cableado interno es diferente para cada uno de los rotores. Este cableado representa a una encriptación por sustitución. La combinación de varios rotores, en posiciones constantemente cambiantes de cada uno en relación con los demás en lo que hace de la encriptación de Enigma algo tan complejo. Cada rotor posee en su lado izquierdo una muestra y en su derecho un trinquete. La combinación de ambos es utilizada por el mecanismo de avance para avanzar los rotores.

La máquina fue introducida con tres rotores. En 1939, el juego de rotores fue ampliado a cinco, usables de tres en tres, marcados con los números romanos, I, II, III, IV y V, todos ellos con sólo una muesca. La Kriegsmarine extendió el juego de rotores al añadir otros tres llamados VI, VII y VIII, estos tres con dos muescas cada uno. En 1942, el modelo M4 de la Kriegsmarine introdujo la posibilidad de usar los rotores de cuatro en cuatro. Para conseguir esto, los rotores anchos “B” y “C” de la versión de tres rotores fueron substituidos por los rotores “B” y “C” de tipo estrecho, dejando espacio para la inclusión del cuarto rotor especial. Los rotores nuevos eran de dos tipos, llamados Beta Gamma, con contactos protuberantes accionados por muelle en ambos lados. Estos dos rotores nuevos eran incompatibles con los otros ocho.

1. Anillo con muesca
2. Marca para el ajuste de anillo en "A"
3. Anillo alfabético
4. Contactos planos

5. Cableado interno
6. Contactos empujados por muelle
7. Bloqueo del anillo de muelles
8. Árbol de soporte
9. Rueda de marcación para el dedo
10. Trinquete

El reflector

El reflector, Umkehrwalze o UKW en alemán, es una característica única de la Máquina Enigma. En el cableado interno de todos los rotores móviles, cada letra está cableada con otra distinta. Una 'A' podría estar cableada con una 'F', mientras que la 'F' pudiera estar cableada con la 'K'. En el reflector, las conexiones de cableado, aunque mezcladas, están realizadas en pares: Si la 'A' está cableada con la 'F', esto implicaría que la 'F' está asimismo cableada con la 'A', dando como resultado una encriptación recíproca. La ventaja de esto para el operador se ve bien clara: La encriptación y la desencriptación se puede realizar con la misma máquina y los mismos ajustes de cableado, sin tener que modificar nada. Desafortunadamente, una letra nunca puede ser encriptada como si misma y esta debilidad abrió las puertas al criptoanálisis, facilitando el trabajo de los analistas de código.

Durante la Segunda Guerra Mundial se utilizaron dos tipos de reflectores, el B y el C. Ambos tenían 26 contactos empujados por muelle en el lado derecho. Las Enigma de cuatro rotores de la Kriegsmarine utilizaban reflectores especiales más estrechos también llamados B y C, pero el cableado de los mismos era diferente del cableado de los reflectores para Enigma de tres rotores de la Wehrmacht y de la Luftwaffe. Sin embargo, si el reflector estrecho B se utilizaba en conjunción con el cuarto rotor llamado "Beta" en posición "A" y con el ajuste del anillo también en posición "A" o si se hacía lo mismo con el reflector estrecho C usado en conjunción con el cuarto rotor llamado "Gamma", estos reflectores se convertían en compatibles con los de las máquinas de tres rotores, permitiendo la comunicación de mensajes entre los distintos tipos de máquinas. Los reflectores estrechos tenían sus contactos planos y se utilizaban en combinación con el cuarto rotor de tipo "Beta" o "Gamma", dado que estos poseían contactos empujados por muelle en ambos lados. En los días finales de la guerra se introdujo un nuevo tipo de reflector, llamado "D". Era un reflector ajustable, con 12 cables y 24 conexiones. El cable 13, con sus dos tomas restantes, era de conexión fija.

Tablas de cableado de los rotores

Para servirnos de un ejemplo de cómo el cableado interno del rotor trabaja como una cifra de sustitución, tomemos al rotor de tipo "I"[1] sin ningún ajuste de su anillo; esto es, con su *Ringstellung* en posición "A". La entrada está en el lado derecho, visto desde el frente de la Enigma. Podremos ver que una 'A' se codifica (-> es cambiada) como 'E', una 'B' se codifica como 'K' y una 'K' se codifica como 'N'. Puede verse que cada letra se codifica como otra diferente. Tras haber pasado por todos los rotores (tres o cuatro, dependiendo de la máquina), la corriente entra en el reflector y tras pasar por este, volverá a recorrer los todos los rotores de nuevo, esta vez en sentido inverso y por otra ruta completamente diferente.

El ajuste del anillo o *Ringstellung* es la posición del cableado interno del rotor (que es fijo) en relación al alfabeto y a la muesca del rotor (posición esta que puede ser variada, dando 26 posibilidades diferentes para el mismo cableado del rotor). Un rotor está compuesto de dos partes principales: En primer lugar, tenemos el anillo exterior, con el alfabeto y la muesca. En segundo lugar, tenemos el núcleo con el cableado interno, que es el sistema de encriptación. Al rotar el ajuste del anillo, cambiaremos por lo tanto las posiciones del cableado del núcleo relativas al punto de avance y a la posición visible del rotor. Pero veámoslo: El rotor tipo "I" en la posición (*ringstellung*) "A"(01) codifica siempre a la letra 'A' como 'E', a la 'B' como 'K' y a la 'C' como 'M'. Pero con su *ringstellung* en "B"(02), todo el cableado ha sido desplazado del núcleo un lugar hacia atrás, con lo que la 'A' se codifica ahora como antes la 'B'; la 'A se codifica ahora como 'K', la 'B' como 'M', la 'C' como 'F' y así sucesivamente. En los rotores, el *Ringstellung* se marca con un punto en el núcleo rotable del cableado. Al cambiar el ajuste del anillo en una posición, el punto de giro del rotor (la muesca, la cual gira con el anillo desplazable del alfabeto) estará aún en la misma posición. Sin embargo, toda la encriptación se habrá desplazado una posición.

Rotores originales de la Wehrmacht, la Luftwaffe y la Kriegsmarine:

[1] En la Enigma, el número que define al tipo de rotor se da siempre en números romanos, desde el I hasta el VIII (*N. del T.*).

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (Rotor/lado derecho)
        ||||||||||||||||||||||||||
I     = EKMFLGDQVZNTOWYHXUSPAIBRCJ
II    = AJDKSIRUXBLHWTMCQGZNPYFVOE
III   = BDFHJLCPRTXVZNYEIWGAKMUSQO
IV    = ESOVPZJAYQUIRHXLNFTGKDCMWB
V     = VZBRGITYUPSDNHLXAWMJQOFECK
```

Rotores adicionales usados sólo por las M3 y M4 de la Kriegsmarine:

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (Rotor/lado derecho)
        ||||||||||||||||||||||||||
VI    = JPGVOUMFYQBENHZRDKASXLICTW
VII   = NZJHGRCXMYSWBOUFAIVLPEKQDT
VIII  = FKQHTLXOCBJSPDZRAMEWNIUYGV
```

Los cuatro rotores especiales, también llamados *Zuzatzwalzen* o rotores Griegos. Utilizados sólo por la Kriegsmarine con reflectores estrechos:

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (Rotor/lado derecho)
        ||||||||||||||||||||||||||
Beta  = LEYJVCNIXWPBQMDRTAKZGFUHOS
Gamma = FSOKANUERHMBTIYCWLQPZXVGJD
```

En la tabla de cableado del reflector, podemos ver que en el reflector normal o ancho, “B”, una ‘A’ se convierte en ‘Y’ y simétricamente, la ‘Y’ se convierte en ‘A’. Existen 13 apareamientos dobles simétricos de esta clase y de ahí el nombre de “reflector”. Los cables están permanentemente conectados formando un bucle entre dos letras.

Reflectores anchos por defecto de la Wehrmacht y de la Luftwaffe:

```
Contactos   = ABCDEFGHIJKLMNOPQRSTUVWXYZ
              ||||||||||||||||||||||||||
Reflector B = YRUHQSLDPXNGOKMIEBFZCWVJAT
Reflector C = FVPJIAOYEDRZXWGCTKUQSBNMHL
```

Reflectores estrechos, sólo en las Enigma M4 de la Kriegsmarine:

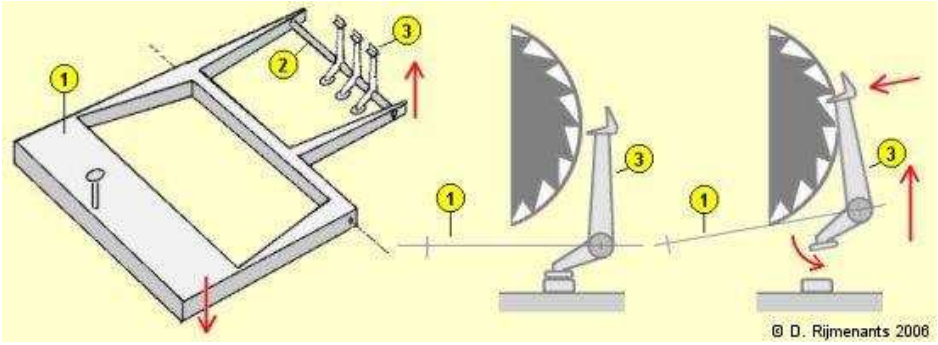
```
          Contactos     = ABCDEFGHIJKLMNOPQRSTUVWXYZ
                          ||||||||||||||||||||||||||
Reflector B Estrecho    = ENKQAUYWJICOPBLMDXZVFTHRGS
Reflector C Estrecho    = RDOBJNTKVEHMLFCWZAXGYIPSUQ
```

Los cableados descritos aquí se refieren sólo a los rotores de las Enigma de la Werhmacht, de la Luftwaffe y de la Kriegsmarine. Los rotores para otras versiones de Enigma difieren y tienen un diferente cableado interno.

El mecanismo de avance

Cada vez que se pulsa una tecla, cambia la posición de los rotores. Esto causa que se utilice una encriptación de sustitución diferente cada vez para la misma letra dada. El primer rotor, el del lado derecho,

avanza un paso con la pulsación de cada tecla. El rotor central avanza un paso por cada 26 avances del primer rotor. El tercero rotor, más lento, avanza un paso por cada 26 avances del rotor central.[2]



El pulsar una tecla desplazará hacia abajo a la barra de avance [1] y al eje común de los gatillos [2] y a sus tres gatillos con muelle [3] hacia arriba. Si el eje común de los gatillos [2] se eleva, todos los gatillos se mueven hacia los rotores. Cada gatillo se apoya a la vez sobre la muesca del anillo del rotor que tiene a su derecha y sobre el trinquete dentado del rotor que tiene a su izquierda. Si un rotor está en su posición de muesca, su gatillo podrá penetrar por ella y acceder a través del hueco que esta le deja hasta el engranaje del trinquete del rotor a su izquierda, moviendo tal rotor un paso hacia delante. Si el rotor a la derecha del gatillo no está en su posición de muesca, el gatillo, viendo su acceso bloqueado, resbalará sobre el anillo del rotor de su lado derecho y le será imposible acceder al trinquete del rotor a su izquierda. Dado que no hay ningún rotor a la derecha del primer rotor, el gatillo más a la derecha siempre activará el avance del primer rotor con cada pulsación de tecla. Si no hay ninguna tecla pulsada, el eje común de los gatillos [2] obliga a los gatillos [3] hacia los asientos en el fondo de la máquina, apartando a los gatillos de los rotores. Esto permite que el operador pueda mover libremente a mano los rotores, en ambas direcciones.

La posición de la muesca es diferente en cada uno de los rotores, En la tabla de abajo podemos ver que el rotor I tiene una muesca sobre la letra Y. Si esta muesca es posicionada frente a uno de los gatillos, se verá la letra Q en la ventanita de los rotores de la máquina. Por lo tanto, el rotor situado a la izquierda del rotor I avanzará un paso cuando el rotor I avance de la Q a la R (los criptoanalistas ingleses utilizaban la frase mnemónica "**R**oyal **F**lags **W**ave **K**ings **A**bove" para recordar las posiciones de los rotores tras el avance). Se debe recordar que los rotores VI, VII y VIII empleados por la Kriegsmarine tenían dos muescas. Esto avanza al rotor a su izquierda dos veces más rápido que el resto de los demás rotores.

Tipo de Rotor	La Muesca está situada sobre la	La letra que aparece en la ventana es la	El rotor a su izquierda salta cuando el rotor avanza de -> a la
I	Y	Q	Q -> R
II	M	E	E -> F
III	D	V	V -> W
IV	R	J	J -> K
V	H	Z	Z -> A
VI VII VIII	H y U	Z y M	Z -> A y M -> N

Nota importante sobre la secuencia de avance: Aunque el mecanismo de avance paso a paso parece trabajar como un odómetro normal, existe una diferencia importante. El rotor central avanza no sólo cuando el rotor a su derecha está en su posición de muesca, sino que también en su propia posición de muesca. Una secuencia que servirá de ejemplo del doble paso: KDO, KDP, KDQ, KER, LFS, LFT (los rotores empleados son, de izquierda a derecha, III, II, I). Este doble paso causa que el comportamiento de los rotores se aparte del de un odómetro normal. El doble paso ocurre como sigue: el primero de los rotores, el más a la derecha, está en su posición de muesca y cuando se pulse una tecla, avanzará y forzará, como se ha visto, el avance de un paso del rotor a su izquierda (el central). Si este rotor central ha caído, por su avance, en su posición de muesca, el tercer gatillo se podrá mover, en el siguiente avance hacia el engranaje del trinquete del tercer rotor (el más a la izquierda). Con este paso siguiente, el tercer gatillo

[2] En las Enigma de 4 rotores, o M4, como se verá más adelante, el cuarto rotor o rotor "griego" Beta o Gamma situado en el extremo más izquierdo, no avanza nunca. Puede definirse su posición inicial, pero no avanza jamás. (*N. Del T.*).

empuja el trinquete del tercer rotor (izquierda) y lo avanza, pero también penetrará en la propia muesca del segundo rotor, avanzando al segundo rotor una segunda vez en la fila.

El mecanismo del doble paso, como se explica arriba, es utilizado en las Enigma de la Wehrmacht y de la Kriegsmarine La enigma de cuatro rotores de la Kriegsmarine, la M4, se deriva de la versión de tres rotores sin cambiar el mecanismo de avance de los rotores, o añadir un cuarto gatillo. Por lo tanto el cuarto rotor no se mueve y sólo puede ser ajustado manualmente. La Enigma-G, utilizada por la Abwehr (Inteligencia Alemana) tiene un mecanismo diferente: La Enigma-G posee un reflector rotativo y tres rotores con múltiples muescas, rotados por un caja de engranajes.

El Tablero de Conexiones (*Stekkerbrett*)

En 1930, el tablero de conexiones, también conocido como *Stekkerbrett,* fue introducido en la primera versión de la Enigma de la Wehrmacht. El tablero de conexiones está situado en el frontal de la máquina. Sin ninguna clavija insertada, la corriente pasa desde los interruptores, controlados por el teclado, directamente hasta el rotor de entrada (también llamado *ETW*, *Entreittwalze*). El insertar un cable entre dos conexiones del panel implica en el intercambio de las dos letras conectadas antes de que al corriente penetre en el rotor de entrada. Cada máquina estaba equipada con un juego de hasta 13 cables de interconexión. El tablero de conexiones fue una mejora importante de la potencia de encriptación de las máquinas.

Cada letra tiene dos conectores. El insertar un cable implica el desconectar el conector superior, que va al teclado y el conector inferior, que va al rotor de entrada. El otro extremo del cable se conecta en la toma de otra letra del panel, invirtiendo las conexiones entre las dos letras. La corriente debe atravesar el panel de conexiones en su camino hacia los rotores y otra vez más, en su regreso hacia las bombillas.

Accesorios

Una elemento muy útil, muy usado en la Kriegsmarine Enigma, fue la *Schreibmax*. Esta pequeña impresora podía imprimir el alfabeto en una pequeña cinta de papel, lo que hacía innecesaria la presencia de un segundo operador leyendo las bombillas y escribiendo las letras. La *Schreibmax* era colocada encima de la Enigma y conectada al panel de bombillas; para instalar la impresora, la cubierta de las bombillas y todas las lámparas, tenían que ser retiradas.

Otro accesorio era el panel de bombillas remoto. Si la máquina estaba equipada con un panel extra, la caja de madera de la Enigma era más amplia y podía almacenarlo. Para que usara el panel extra, la Enigma tenía que ser construida especialmente. Hubo, posteriormente un panel extra que podía añadirse a cualquier Enigma, pero ello requería, al igual que con la impresora *Schreibmax*, que se retirasen previamente el panel de lámparas y todas las bombillas. El panel remoto permitía que una persona (normalmente un oficial) pudiera leer el texto desencriptado sin que el operador de la máquina tuviera acceso al mismo.

En 1944, la Luftwaffe introdujo un panel de conexiones extra, llamado *Uhr* (el reloj). El *Uhr* consistía en una pequeña caja que contenía un conmutador de 40 posiciones. Esto reemplazaba a las conexiones por defecto. Tras conectar los cables, conforme a lo determinado en el libro de códigos para el día, el operador podía girar el conmutador a una de las 40 posiciones, cada una de las cuales con una diferente combinación de cableado. La mayoría de esas conexiones no estaban hechas en pares, a diferencia de las del panel de conexiones principal.