José Ramón Soler Fuensanta

Introducción.

Si bien desde el inicio de los conflictos armados organizados ha sido necesario mantener el secreto en las comunicaciones militares, es a partir de la aparición del telégrafo, y sobre todo de la radio cuando éste ha pasado a formar parte importante de las mismas. El enemigo ya no tiene que preocuparse de intentar saber cuando saldrá el correo y su destino para intentar interceptarlo, en el caso de la radio puede obtener el mensaje sentado con el material adecuado, simplemente escuchando. Las ondas de radio no distinguen amigos de enemigos y la seguridad de las comunicaciones depende fundamentalmente de las técnicas de ocultación del significado de los mensajes, es decir, la criptografía. En España en los trabajos dedicados a las comunicaciones de finales del XIX de Lossada[1] y Banus[2] ya aparecen anexos dedicados a este campo de estudio como forma de asegurar el secreto en las comunicaciones. Sin embargo, en ese apartado debemos reconocer que nuestro país, que había sido en el siglo XVI la nación puntera en este campo, estaba a principios del siglo XX en mantillas en comparación con el resto de Europa. La criptografía mecánica que en esa época estaba en el punto de mira de las potencias europeas, era prácticamente desconocida en España. Los dispositivos de cifra más sofisticados de que disponíamos eran la clave norte y el cifrador RF. A pesar de todo, tenemos el dudoso honor de ser el país donde probablemente se utilizó por primera vez la criptografía mecánica en situación de guerra.

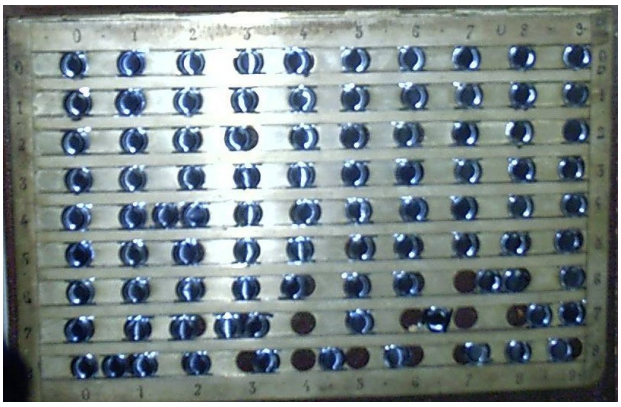


Ilustración 1. Cifrador RF.

Ilustración 2. Clave Norte.

Hablar de la máquina Enigma es fácil, existe una amplia literatura sobre el tema, aunque lamentablemente no en español. Que sepamos solo el libro Ultra secreto, el que descubrió que los británicos habían estado rompiendo Enigma, ha sido traducido y publicado. Sin embargo, este libro no entra en las cuestiones internas de funcionamiento y las características de la misma, quedándose en la relación de hechos en los que el criptoanálisis de Enigma fue, si no determinante, sí importante y haciendo aseveraciones no demasiado correctas desde el punto de vista histórico. Desde ese mismo punto de vista creemos que el libro electrónico que en su día publicó Román Ceano en Kriptopolis es muy superior al de Winterbotham. Sin embargo, en los textos españoles la cuestión técnica de Enigma y su criptoanálisis se ve relegada a algún capítulo de libros dedicados a la criptografía[3].

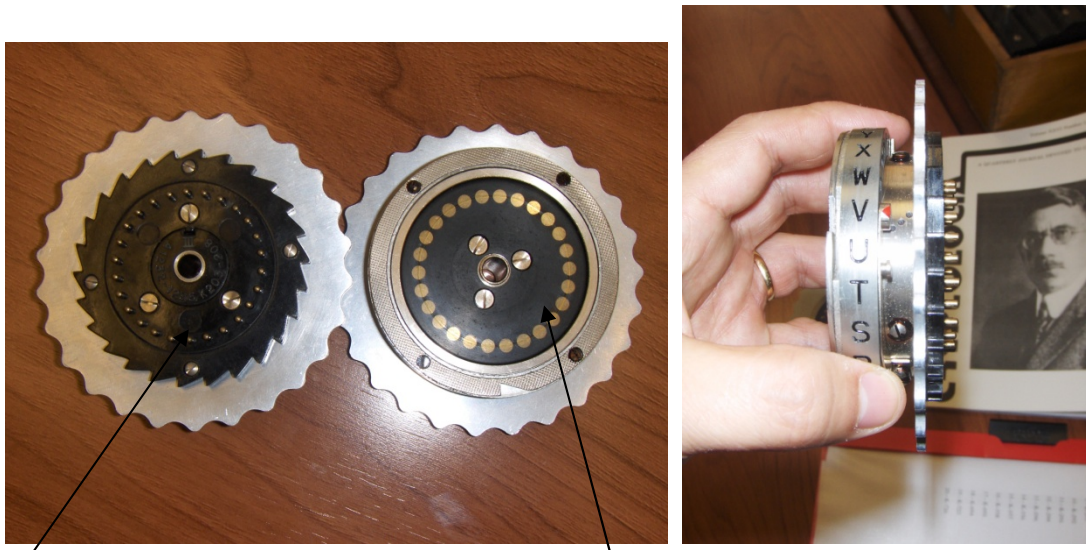
¿Qué hace de Enigma algo especial? Enigma era una máquina bien diseñada, con algunos errores como veremos más adelante, que no pudo resistir el avance de la tecnología. Pensemos que estuvo en funcionamiento en una u otra versión, casi 15 años. Un tiempo muy largo en criptografía. Lo importante no es la máquina en sí, sino su historia, es el ejemplo más claro de que en seguridad no hay nada seguro. Los expertos en criptología suelen hablar de algoritmos fuertes, seguridad

[1] Manual militar de telegrafía. Fernando de Lossada y Sada. Librería de Hernando y Compañía 1898.
[2] Telegrafía militar. Carlos Banús y Tomas. Publicaciones de la Revista Científico-Militar. Barcelona 1897.
[3] Véanse por ejemplo [ORT06] y el más reciente [ENC16].

teórica y conceptos similares. La seguridad teórica de Enigma era muy elevada, pero los alemanes fallaron por considerarla aisladamente, sin tener en cuenta todo lo que se relaciona con ella, uso, distribución de claves, y, sobre todo pensar en que los criptoanalistas enemigos iban a trabajar como los suyos. No tuvieron en cuenta una cosa muy lógica que se puede aplicar a todos los problemas y que Einstein señaló muy acertadamente en su día: "*Si quieres obtener resultados distintos, no hagas siempre lo mismo*". Esa historia más conocida hace que la mayoría de los aficionados asocien la máquina con la guerra mundial y con un determinado modelo de la misma. Lo cierto es que el primer conflicto bélico en el que se utilizó fue en la guerra civil española. Tampoco podemos hablar de la máquina Enigma, sino de las máquinas Enigma. Hubo varios modelos en activo desde su nacimiento hasta su retirada final. En este breve trabajo nos centraremos en los modelos relacionados de una u otra manera con nuestro país.

Convenciones.

Cuando hablemos de las conexiones a los rotores, éstas se considerarán siempre de PIN a PLATE, es decir de los conectores salientes a los conectores planos del rotor. La parte correspondiente al PIN está en sombreado. Si el rotor es alfabético se indican las conexiones y las muescas de salto en forma de letras, en el caso de ser numéricos, se indican los números correspondientes



En la foto superior podemos ver un punto rojo al lado de la V en el rotor. Se trata del marcador de la posición inicial. Si quieren medir el cableado de un rotor, o comprobar los que aparecen a lo largo de este artículo, tendrían que poner la A del anillo en la posición marcada por ese punto rojo. Si lo que desean es determinar el cableado, no les recomendamos abrir el rotor, es mucho más sencillo utilizar un tester normal e ir midiendo desde el Pin al Plate donde pasa la corriente.

El principio básico de las máquinas de cifra, el rotor.

La aparición de las maquinas de cifra puede considerarse el principio de una nueva era en la criptografía y el criptoanálisis. Los tiempos del criptoanalista que en un arranque de genialidad era capaz de romper un código pasaron en el momento en que estas se pusieron en funcionamiento.

Estas máquinas fueron ampliamente utilizadas durante la II Guerra Mundial por todos los contendientes, cada uno con sus variantes, pero utilizando un esquema común, el concepto de rotor. Un rotor no es nada más que una pieza cilíndrica con una serie de contactos en su interior y un conjunto de letras y símbolos en su exterior. Los rotores podían ser de dos clases, cableados o con muescas que podían ser activas o inactivas. En realidad el rotor, en el caso de máquinas electromecánicas, no es más que un conmutador que genera una sustitución entre una letra y otra[4] al pasar la corriente de un conector de una de las caras a otro en la otra cara.

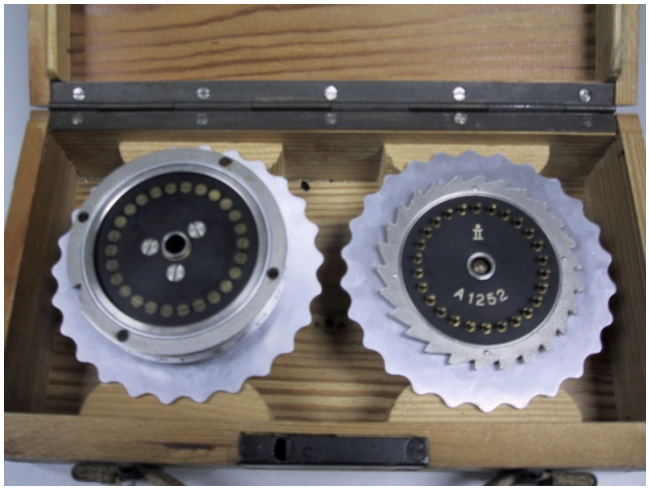


Ilustración 3. Rotores de una Enigma militar.

Para complicar el cifrado, las máquinas de rotor disponían varios rotores en cascada y al hacer que estos se movieran a diferente velocidad se generaba un cifrado de gran complejidad y con un periodo de la clave muy grande.

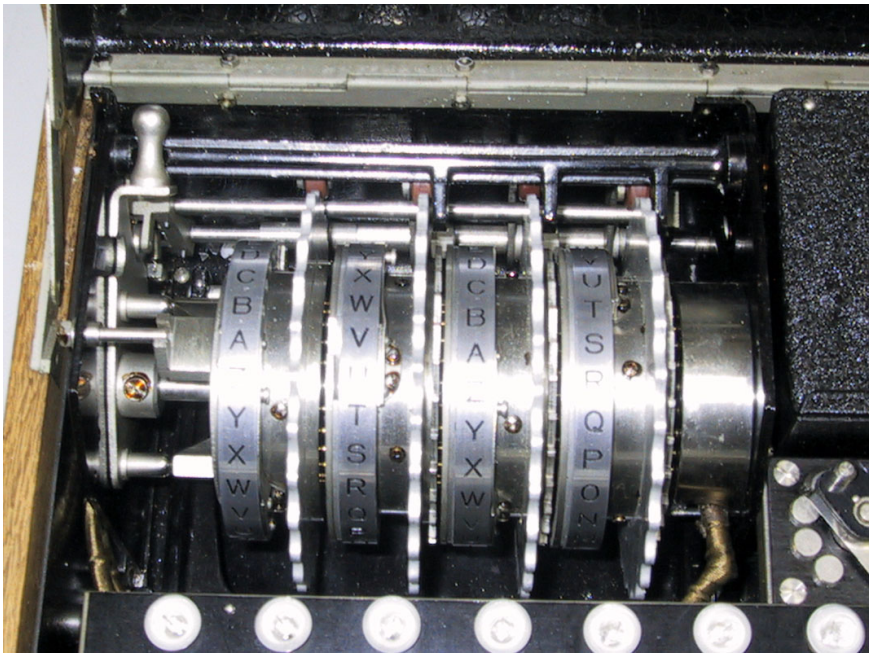


Ilustración 4. Enigma K abierta.

[4] Desde un punto de vista más formal podemos decir que un rotor realiza una sustitución monoalfabética al pasar la corriente de un conector de una de las caras a otro en la otra cara. Las máquinas de rotor lo que hacían era poner varios rotores en cascada y hacer que estos se movieran a diferente velocidad, de esa forma se generaba una sustitución polialfabética de gran complejidad y con un periodo de la clave muy grande. Desde un punto de vista muy simplista podemos decir que las maquinas de rotor pueden considerarse como sistemas que generan cifrados de Vigenère con un periodo muy elevado. En particular con rotores de 26 posiciones, una máquina de *n* rotores tendría un periodo de 26^n.

El concepto de rotor fue desarrollado casi simultáneamente por Arvid Damm en Suecia en 1919, Edward Hebern en Estados Unidos en 1917, Arthur Scherbius en Alemania en 1918 y Hugo Alexander Koch en Holanda en 1919 [BAU99], aunque las ultimas investigaciones sobre el tema parecen apuntar a que la paternidad holandesa correspondería a Th. A. Van Hengel y R. P. C. Spengler, dos oficiales de la Armada holandesa[5]. Todos ellos desarrollaron máquinas que utilizaban una combinación de movimientos mecánicos e impulsos eléctricos generados por los rotores que hacían muy difícil el descifrado. Las más famosas entre estas máquinas fueron la E*nigma* alemana y sus diferentes versiones; la B-21 y su sucesora, la B-211; la serie C de Hagelin, la TYPEX británica y la ECM Mark II o SIGABA americana. La B-21 por ejemplo era una máquina electromecánica con representación del texto cifrado mediante un panel de luces, al igual que en la máquina Enigma. Fue presentada por Boris Hagelin al ejército francés en 1934 que obligó a realizar varios ajustes en la misma antes de adoptarla definitivamente. La nueva máquina, la B-211, era una máquina relativamente ligera, unos quince kilogramos de peso, fabricada por Ericsson en Colombes. De esta máquina se llegaron a construir más de quinientas antes de la guerra y unas cien después. En 1936 Hagelin presenta sus modelos C-36 y C-37, con la particularidad de que permitían la impresión del texto cifrado. De estas máquinas se vendieron más de 50000 unidades a países como Francia, Italia, Japón, Finlandia y Alemania. Solo Francia llegó a comprar más de 5000. En 1940 Hagelin marcha a Estados Unidos donde logra convencer al Servicio de Inteligencia americano (el *Signal Intelligence Service*) de la utilidad de su máquina mejorada, la C-38, que se fabricaría en Estados Unidos por la empresa Smith Corona y que se conocería con el nombre de convertidor M-209 en el Ejército, y CSP-1500 en la Marina.

Ilustración 5. Hagelin M209.

La máquina Enigma.

El proyecto de la máquina *Enigma* fue concebido por Arthur Scherbius un ingeniero eléctrico y E. Richard Ritter en 1918. En ese año Arthur Scherbius patenta la primera máquina *Enigma* con el número de patente 416291. En 1919 Hugo Alexander Koch había patentado también

[5] Para una descripción más detallada véase [LEE03].

su máquina de cifrar (Patente nº. 10700), pero debido a problemas con el diseño, decidió vender la patente a Scherbius en 1923. Scherbius y Ritter montaron una empresa a su nombre e intentaron vender, sin éxito, su máquina de cifrar a la Marina alemana. Posteriormente, a sugerencia del Alto Mando de la Marina, lo intentaron con el Ministerio de Asuntos Exteriores para el cifrado de sus comunicaciones diplomáticas, organismo que no demostró ningún interés en ella. En 1923 Scherbius y Ritter, que no disponían de capital para montar una empresa propia, se asociaron con Willie Korn, transfiriendo la patente a la empresa *Gewerkschaft Securitas* que, el 9 de julio de 1923 crea una compañía llamada *Enigma Chiffiermaschinen Aktien-Gesellschaft* en Berlín para dedicarla a la venta de máquinas de cifra, quedando Scherbius y Ritter como parte de su consejo de administración. Rápidamente se empieza a producir la primera máquina Enigma, en la Steglitzer Strasse nº 2 de Berlin W 35 [PIE92, 10]. A partir de los años treinta la fabricación pasaría a la compañía *Chiffriermaschinen Geselschaft Heimpold un Rinke* aunque varias de las piezas de las máquinas eran fabricadas por otras empresas.

La primera versión comercial de la máquina *Enigma*, la versión A, era una máquina voluminosa y pesada[6]. Producida en 1923, estaba dotada de cuatro ruedas dentadas con periodos de 11 (cinco dientes y seis muescas), 15 (nueve dientes y seis muescas), 17 (11 dientes y seis muescas) y 19 (11 dientes y 8 muescas) respectivamente, con lo que el periodo era de 53295 ($11\times15\times17\times19$). La razón de la elección de esos números es que todos son relativamente primos, con lo que se garantizaba un periodo máximo. Cada una de estas ruedas dentadas tenía asociada un rotor con un alfabeto de 28 letras. Una particularidad de este modelo, muy útil en ambientes comerciales, era que también funcionaba como máquina de escribir. La máquina fue presentada poco antes del congreso de la Unión Postal Internacional en Berna [LEW78, 35], exhibiéndose también en dicho congreso. Más adelante se presentó en la feria de Leipzig y en el Congreso Internacional Postal en Estocolmo, en agosto de 1924, como un sistema para garantizar el secreto de los datos comerciales. La máquina tenía un precio en el mercado de 350 reichmarks. A pesar de su escaso éxito comercial se fabricaron tres modelos más, conocidos como:

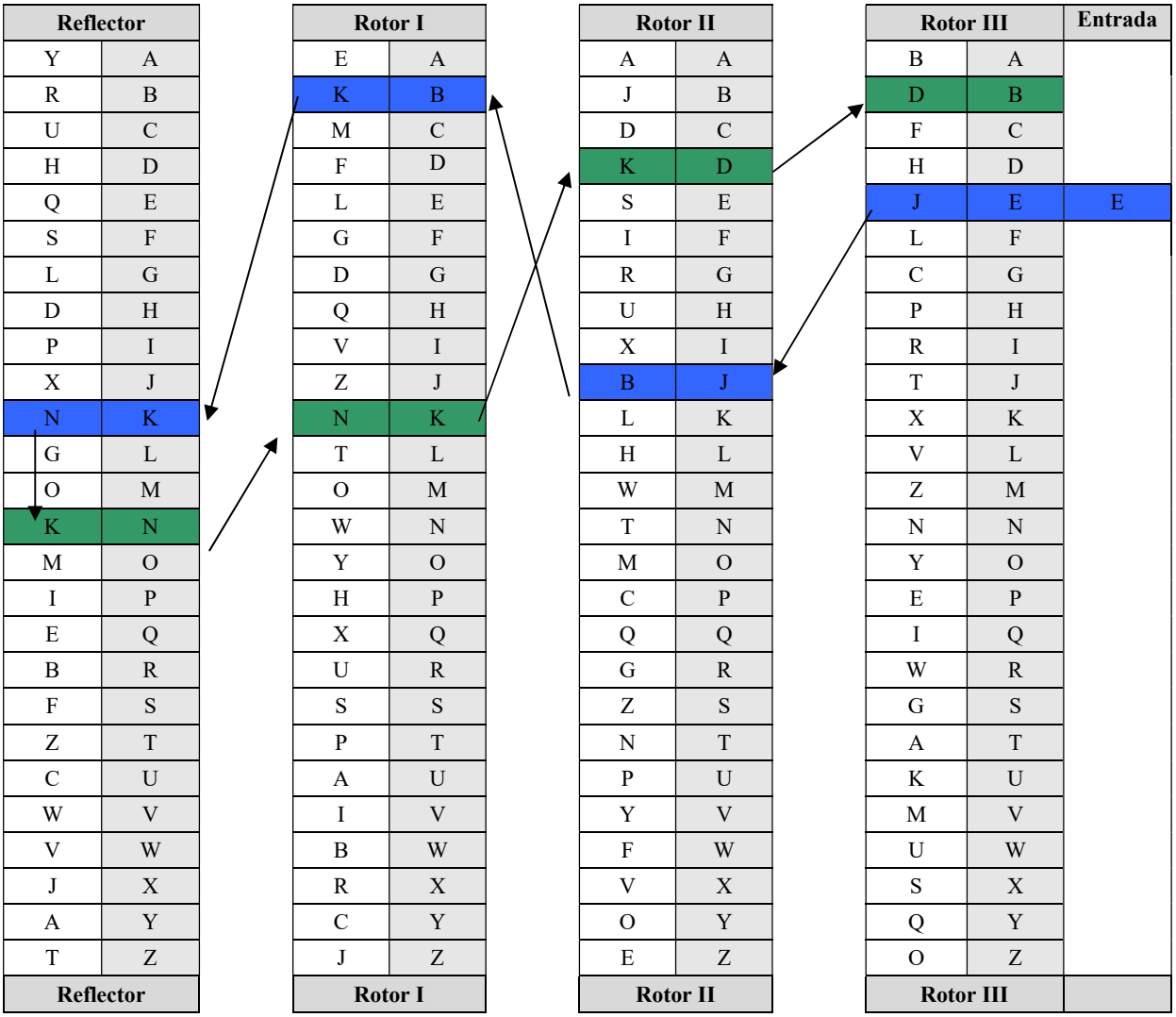
- *Enigma B*, muy similar al modelo *A*, tenía la apariencia de una máquina de escribir y al igual que ésta tenía cuatro rotores, pero de 26 contactos, rotor que sería el utilizado ya a partir de ese momento.
- *Enigma C* y *D*, aparecidas respectivamente en 1925/1926 y 1927, ambas dotadas de tres rotores y reflector (*Umkerwalze*), un rotor especial que devolvía la señal y la hacia pasar otra vez por los rotores siguiendo un camino diferente. Estas y las posteriores ya no disponían de sistema de impresión, sino que la señal aparecía en un panel de luces en la parte superior.

La Enigma K utilizada en la guerra civil Española, de la que hablaremos más adelante, era una versión del modelo D. En la foto siguiente podemos apreciar una máquina de este tipo. Como vemos no aparece el logotipo de Enigma ni ninguna referencia a la marca. Además, si sacásemos los rotores veríamos que en alguna de ellas, en lugar de tener la numeración de la máquina, que también aparece en la tapa, tienen la numeración de toda la serie. Eso ocurre por ejemplo en las máquinas del primer envío. Los rotores vienen marcados con la leyenda K203-208 A1232-1235. En los documentos de Archivo a veces es difícil determinar si ha sido cifrado con Enigma o no. Un indicativo claro de que sí ha sido cifrado con Enigma es el que aparezca la denominación “clave mecánica”.

[6] Tenía unas dimensiones de 65 cm. de longitud, 45 cm. de anchura y 35 cm. de altura con un peso aproximado de 50 kg [KRU02, 5].

Ilustración 6. Máquina K296.

A continuación vemos un ejemplo de cifrado de una letra con una máquina teórica. Para una mejor comprensión de su funcionamiento, haremos dos supuestos, el primero en el que la máquina no adelanta los rotores y otro con el funcionamiento real de la Enigma. El cableado que hemos utilizado es el de una máquina M3 militar. La posición de los rotores es AAA y están puestos en el orden I, II y III. Si nuestros rotores quedan fijos y queremos cifrar la letra E tenemos:



Reflector	
Y	A
R	B
U	C
H	D
Q	E
S	F
L	G
D	H
P	I
X	J
N	K
G	L
O	M
K	N
M	O
I	P
E	Q
B	R
F	S
Z	T
C	U
W	V
V	W
J	X
A	Y
T	Z
Reflector	

Rotor I	
E	A
K	B
M	C
F	D
L	E
G	F
D	G
Q	H
V	I
Z	J
N	K
T	L
O	M
W	N
Y	O
H	P
X	Q
U	R
S	S
P	T
A	U
I	V
B	W
R	X
C	Y
J	Z
Rotor I	

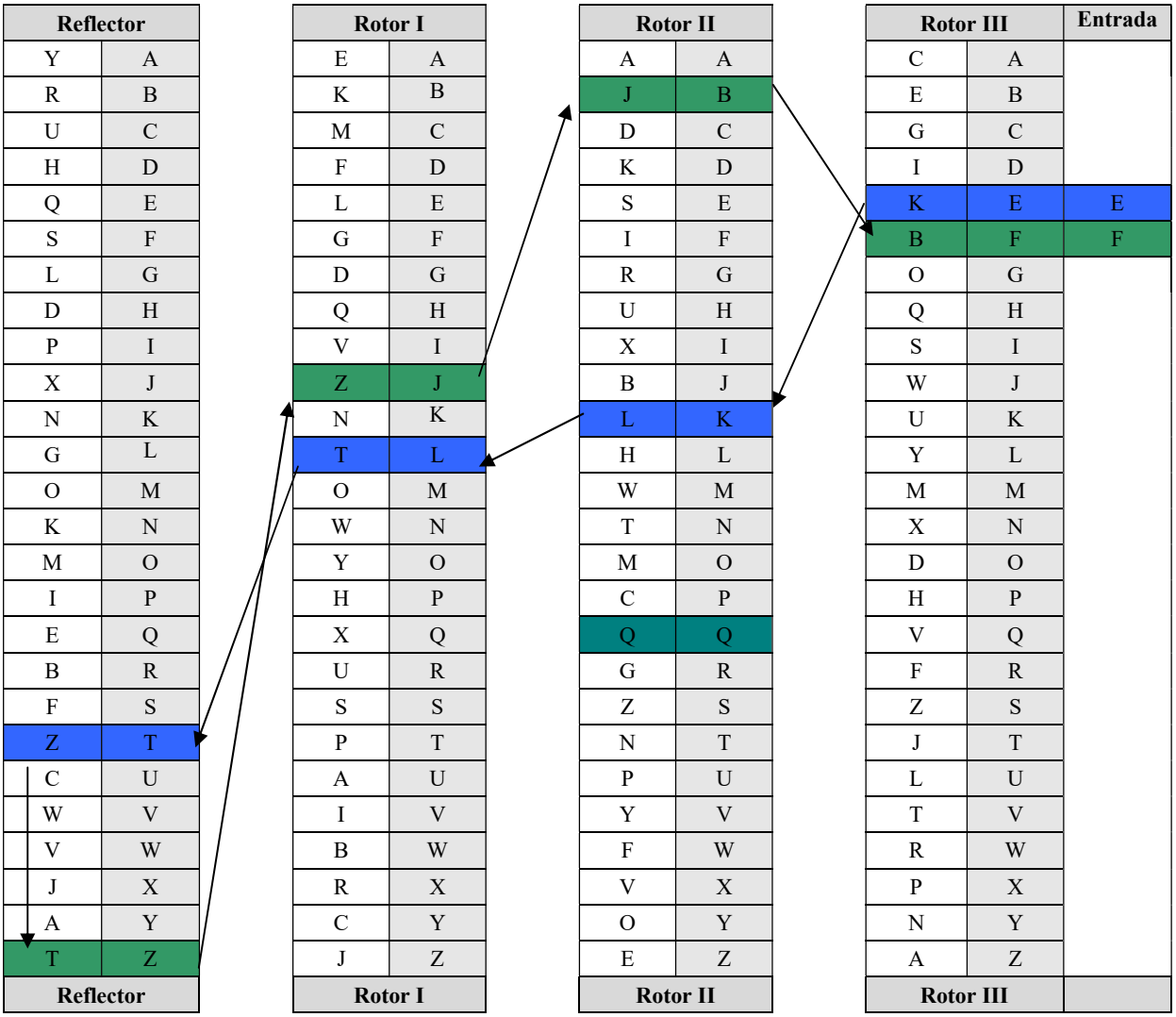
Rotor II	
A	A
J	B
D	C
K	D
S	E
I	F
R	G
U	H
X	I
B	J
L	K
H	L
W	M
T	N
M	O
C	P
Q	Q
G	R
Z	S
N	T
P	U
Y	V
F	W
V	X
O	Y
E	Z
Rotor II	

Rotor III		Entrada
B	A	
D	B	
F	C	
H	D	
J	E	E
L	F	
C	G	
P	H	
R	I	
T	J	
X	K	
V	L	
Z	M	
N	N	
Y	O	
E	P	
I	Q	
W	R	
G	S	
A	T	
K	U	
M	V	
U	W	
S	X	
Q	Y	
O	Z	
Rotor III		

Si ahora ciframos tal como realmente lo hacía la Enigma el resultado es diferente ya que previo a la conexión se realiza un avance del rotor rápido (el derecho). Eso implica un cambio en los enlaces dado que la B del apartado anterior pasaría a ser la A de entrada y las conexiones entre las letras pasarían a ser diferentes. Podemos asumir que, dado que tenemos 26 conexiones en el primer rotor entre las diferentes letras, las nuevas conexiones serían las siguientes aplicando la formula $c_i = l_i + j \bmod 26$, siendo c_i la letra cifrada, l_i la letra en claro y j el desplazamiento. El resultado nos daría una conexión entre las letras como la siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	3	4	5	6	22	8	9	10	13	10	13	0	10	15	18	5	14	7	16	17	24	21	18	15	1
3	5	7	9	11	2	15	17	19	23	21	25	13	24	4	8	22	6	26	10	12	20	18	16	14	1
C	E	G	I	K	B	O	Q	S	W	U	Y	M	X	D	H	V	F	Z	J	L	T	R	P	N	A

Con lo que el cifrado de la letra después de haberse movido el rotor nos daría el siguiente resultado:



El concepto básico de la Enigma, la reversibilidad, es consecuencia del reflector que fue inventado por Willi Korn. Su uso permitía que, si A se cifraba como X con unos determinados ajustes iniciales de la máquina, al teclear X con los mismos ajustes aparecía A como texto en claro. Es decir, el cifrado y descifrado de Enigma era recíproco a partir del modelo C. Tecleando el texto en claro con un ajuste determinado obteníamos el mensaje cifrado, pero inversamente, con ese mismo ajuste al teclear el mensaje cifrado obteníamos el mensaje original. Esa ventaja contaba también con su inconveniente, una letra no podía cifrarse como ella misma, que aunque presentado como una ventaja, era en realidad un fallo criptográficamente hablando. Los modelos *C* y *D* eran prácticamente iguales, pero había pequeñas diferencias que los identificaban:

- El reflector en el modelo C solo tenía dos posiciones, mientras que en el D tenía 26, aunque una vez fijado no podía cambiarse durante el cifrado.

- En el modelo C el teclado y el panel frontal estaba en orden alfabético, mientras que en el D tenía el de un teclado estándar alemán[7], con lo que debía producirse una permutación entre las teclas y los contactos de entrada en los rotores.

La especificación de los rotores en el modelo D, tal como aparece en [KRU02] sería la siguiente[8]:

Entrada	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ETW	J	W	U	L	C	M	N	O	H	P	Q	Z	Y	X	I	R	A	D	K	E	G	V	B	T	S	F
Rotor I	L	P	G	S	Z	M	H	A	E	O	Q	K	V	X	R	F	Y	B	U	T	N	I	C	J	D	W
Rotor II	S	L	V	G	B	T	F	X	J	Q	O	H	E	W	I	R	Z	Y	A	M	K	P	C	N	D	U
Rotor III	C	J	G	D	P	S	H	K	T	U	R	A	W	Z	X	F	M	Y	N	Q	O	B	V	L	I	E
Reflector	I	M	E	T	C	G	F	R	A	Y	S	Q	B	Z	X	W	L	H	K	D	V	U	P	O	J	N

En ambos modelos el rotor rápido era el de la derecha, el medio el central y el lento el de la izquierda. El rotor tenía alrededor un anillo con el alfabeto estándar (A-Z) o los números del 1 al 26. Estos números y letras eran lo que se veían a través de unas oberturas en el panel al lado de las posiciones del rotor.

La máquina militar.

La máquina más conocida es sin duda la Enigma militar con el panel de conexiones frontal. Ésta tenía un tamaño de 28 x 34 x 15 cm. con lo que podía manejarse fácilmente como si fuera una máquina de escribir estándar. La primera en utilizar Enigma para cifrar sus comunicaciones fue la *Kriegsmarine*, que adoptó en 1926 una versión del modelo C con un rotor de 28 contactos para cifrar sus comunicaciones de alto nivel por radio con el nombre de "*Funkschlüssel C*". En esta máquina el reflector podía ser insertado en cuatro posiciones diferentes identificadas con las letras griegas α, β, γ y δ. El ejército de tierra alemán empezó a utilizar una versión modificada, la Enigma G, entrando en servicio la versión definitiva de la máquina, denominada Enigma I, en Junio de 1930. Esta máquina, dotada con tres rotores de 26 contactos y un reflector fijo, se caracterizaba por incluir un panel de conexiones frontal que intercambiaba pares de letras. La máquina militar adoptada por la *Kriegsmarine* desde 1934, la denominada Enigma M, disponía de cinco rotores, de los que se elegían tres, y un panel frontal de conexiones al igual que en la Enigma I. La inclusión del panel frontal fue consecuencia de un estudio encargado a un grupo de expertos por el coronel Fellgiebel sobre la seguridad de la máquina. El resultado fue demoledor, la máquina no era tan segura como se decía e incluso se encontró un método para romperla. El mismo informe indicaba como método para hacerla más segura la inclusión del panel frontal de conexiones. Como medida de seguridad complementaria la Marina alemana introdujo varios tipos de clave con diferentes grados de complejidad en función de los comunicantes: una para tráfico de bajo nivel (*Marinenschlüssel*), otra a nivel de estado mayor (*Stabsschüssel*) y, por último una a nivel de almirantazgo (*Admiralschlüssel*). El primero de agosto de 1935 el ejército del aire empieza también a utilizar Enigma, al igual que la policía y la GESTAPO que lo harán a partir del primero de septiembre de 1937. Una vez adoptada por el resto de las ramas del ejército, se organizaron diferentes redes para cada una de ellas como una medida suplementaria de seguridad, tal como ya había hecho la Marina, de éstas llegaron a existir unas sesenta diferentes. El número de Enigmas creció muy rápidamente; se utilizaba a nivel de División en el *Heer*, a nivel de unidad operacional en la *Luftwaffe* y en cada buque de la *Kriegsmarine*. El número de máquinas en funcionamiento llegó a ser muy elevado, se calcula que el ejército alemán llegó a tener más de treinta mil en

[7] Es decir ABCDEFGHIJKLMNOPQRSTUVWXYZ en el modelo C y QWERTZUIOASDFGHJKPYXCVBNML en el modelo D.
[8] En el artículo hay un par de errores correspondientes al reflector, que en esta tabla hemos corregido.

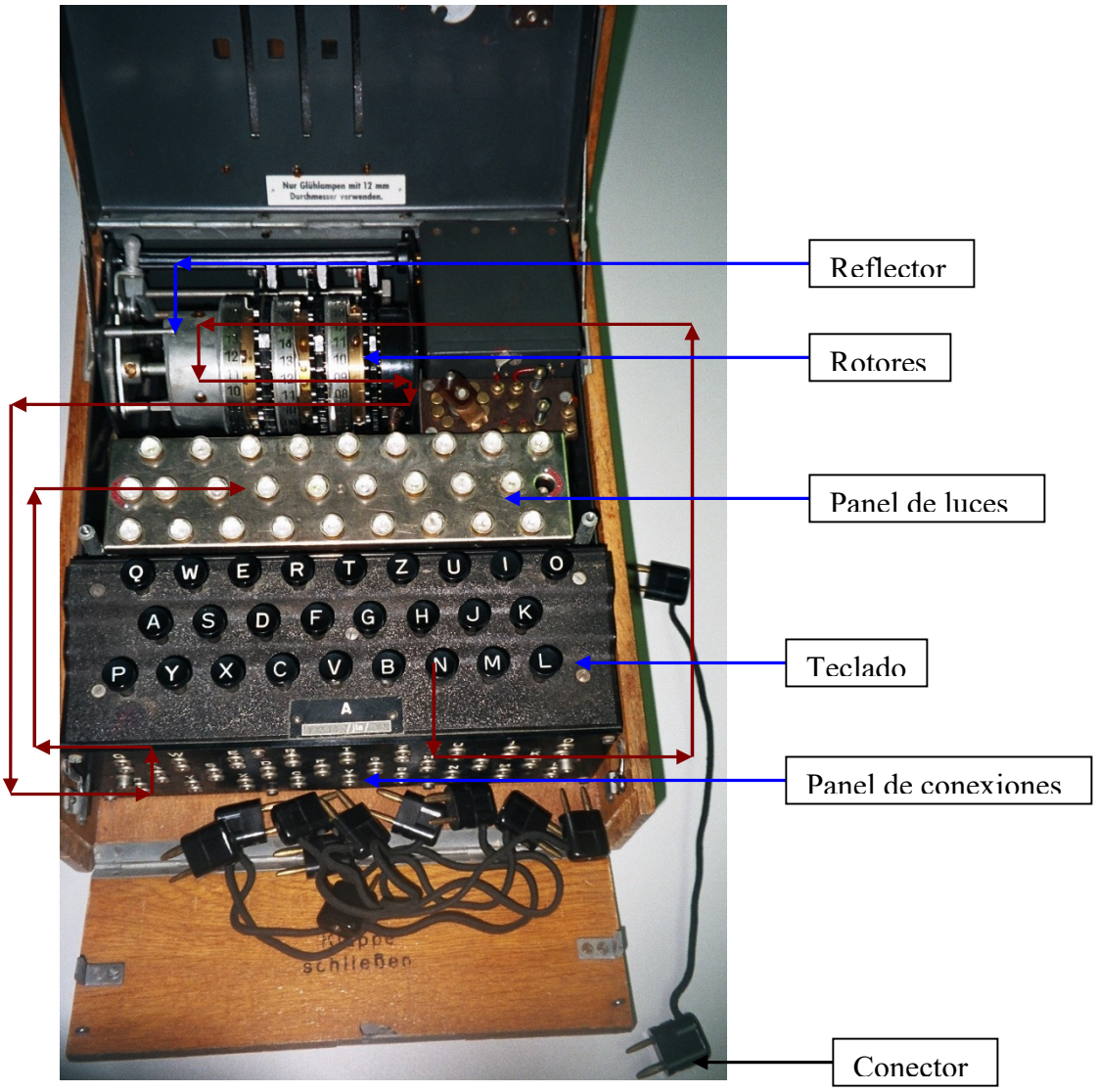
funcionamiento, solo la Marina llegó a utilizar seis mil, mientras que la *Luftwaffe* cerca de veinte mil. Algunos autores calculan que se llegaron a fabricar unas doscientas mil de estas máquinas. No es difícil ver la enorme dificultad que representaba cualquier modificación en una estructura tan grande. Un solo cambio de rotores significaba un problema de logística enorme, aumentado por las distancias que se manejaban y el frecuente cambio de posiciones en ambiente bélico.

En diciembre de 1938 se añaden dos rotores a los tres existentes en la Enigma militar, aunque la Enigma naval, la Enigma M ya hacía tiempo que los utilizaba. Estos dos nuevos rotores incrementaban la dificultar de romper el código, ya que una parte de la clave, consistía en la selección de tres de los cinco rotores y del orden de los mismos. Al parecer durante los años 33 y 34 se empezó a utilizar una variante de la máquina Enigma con ocho rotores intercambiables y con un dispositivo de impresión incorporado, la Enigma II. Sin embargo, finalmente se desechó el modelo debido a sus frecuentes averías. Al parecer hubo más prototipos, o al menos es lo que se desprende del informe realizado en 1931 por el asistente del Agregado Militar Estadounidense en Berlín, el mayor P. W. Evans. En éste se habla de una Enigma con 10 rotores de 5 contactos de unos 90 kg con un dispositivo de impresión en la central de comunicaciones del Ejército y de una máquina con 20 rotores con 50 contactos y unos 200 kg. de peso en la central de comunicaciones de la Armada alemana.

Las medidas de seguridad fueron variando con el tiempo, haciéndose cada vez más duras. La frecuencia de cambio de los rotores aumentó a medida que se hacía más frecuente su uso; al principio los rotores se cambiaban una vez cada tres meses, desde febrero de 1936 una vez cada mes, y desde octubre de ese mismo año, una vez al día. Durante la guerra esa frecuencia llegó incluso a aumentarse; desde el verano de 1942 se cambiaba cada ocho horas. También el número de conexiones frontales sufrió cambios; entre octubre de 1936 y diciembre de 1938 se utilizaban entre cinco y ocho conectores frontales, pasando a partir del mes siguiente a utilizarse entre siete y diez, no siendo nunca un número constante. A finales de 1937 el reflector (*Umkehrwalze)* fue cambiado por un nuevo modelo denominado simplemente reflector B. La más desconfiada, con razón, fue la *Kriegsmarine* que fue incrementando el número de rotores, primero tres de cinco en 1934, pasando a tres de siete en 1938, luego a tres de ocho un año después, y por fin cambiando a una máquina Enigma con cuatro rotores en 1942. En 1943 fue reintroducido en la marina el rotor móvil, que había desaparecido en la Enigma I, de los cuales había tres modelos en uso, los denominados alfa, beta y gamma.

El funcionamiento de la máquina militar.

El funcionamiento de la máquina militar es parecido al de la máquina estándar tipo K que veremos más adelante, pero al contrario que en esa, no había necesidad de poner en posición el reflector dado que éste era fijo. Al igual que el resto de máquinas Enigma, el proceso de cifrado y descifrado era simétrico. El panel frontal de conexiones se encargaba de cambiar pares de letras haciendo una conexión física a través de un cable. Por ejemplo, podía cambiar la letra A por la C, la V por la X, y así hasta, en general, unos diez pares de letras. Con lo que la clave para cifrar un mensaje con la máquina Enigma estaría formada por cuatro operaciones:



1) Selección de la posición del alfabeto del rotor (RINGSTELLUNG). Con tres rotores hay 17576 posibilidades.

2) Colocación de los rotores utilizados, junto con el orden en que estaban colocados en la máquina (WALZENLAGE). Por ejemplo podemos utilizar los rotores III, V y II en este orden de izquierda a derecha. En la práctica se seleccionaban tres de un conjunto de cinco como en el ejército y la aviación alemanes, lo que daba un total de sesenta posibles combinaciones. La Marina alemana, más desconfiada, seleccionaba tres de un conjunto de ocho[9].

3) La posición inicial de los rotores, por ejemplo el rotor III está en la Q, el V en la B y el II en la A. Con tres rotores hay 17576 posibilidades de fijar la posición inicial.

[9] Posteriormente, cuando la Marina añadió el cuarto rotor, se seleccionaban tres de entre los ocho disponibles, más uno entre dos rotores especiales (*zusatzwalze*) de solo 1,2 cm. de anchura en lugar de los 2,5 habituales. Estos no rotaban y eran denominados Beta y Gamma. .

4) El cableado del panel de conexiones frontal. Normalmente un conjunto de diez pares de conexiones (STECKERVERBINDUNG). Con diez pares de conexiones hay 150.738.274.937.250 posibilidades, con once el número se eleva a 205.552.193.096.250.

Los defectos de la máquina Enigma.

Hasta ahora henos hablado de la máquina en sí, de su historia y de su utilización. Ahora hablaremos de los defectos, tanto en su diseño como en su uso. Algunos de ellos permitieron que el cifrado de la máquina fuese roto primero por los polacos y posteriormente por los británicos. Hay que recalcar que los alemanes eran conscientes de algunos de ellos, pero que no llegaron a solucionarlos.

El primer defecto era que la máquina era poco eficiente en su uso. Entendámonos, la máquina estaba diseñada para que el cifrado, o el descifrado según la operación que se estuviese realizando, apareciese en el panel superior como una letra iluminada. Esto hacía que para trabajar con ella se necesitasen dos personas, una encargada de introducir los datos en la máquina y otra que estuviese apuntando los resultados. La falta de un dispositivo de impresión fue señalada por los militares alemanes que hicieron pruebas de una versión (denominada tipo II) con un dispositivo de impresión en 1932, pruebas que resultaron un completo desastre, abandonándose finalmente la idea [SKI92, 4]. Esa misma razón fue esgrimida por la Armada italiana en nuestra guerra civil, que a pesar de que consideraban a la Enigma superior desde un punto de vista criptográfico, preferían las Hagelin por disponer de un dispositivo de impresión [BAR95]. Consecuencia de lo anterior era la baja tasa de texto cifrado que podía generarse por minuto. Al cifrar había que pulsar bastante fuerte la tecla para que girasen los rotores y mantenerse pulsada hasta que se hubiera tomado nota de la letra cifrada equivalente. Esto hacía que se pudiesen cifrar una docena de letras aproximadamente por minuto. Una tasa de cifrado que hoy en día puede parecernos ridícula, pero que en su día se consideró suficiente.

Otro de los problemas que arrastraba la Enigma, en este caso la militar, era la inexistencia de teclas para los números. Esto implicaba que éstos tuvieran que deletrearse lo que hacía que el mensaje se alargase inútilmente. No es necesario destacar que en comunicaciones militares el uso de números es muy frecuente y que eso representaba un claro inconveniente. Curiosamente la Enigma K utilizada en España sí que disponía de números en el teclado, en realidad la tecla tenía dos valores, la Q y el 1, la W y el 2, etc. Para indicar que se trataba de un número se insertaba una combinación de dos letras al inicio del número y otra diferente al final[10], de esta manera quedaba delimitado el número.

Un fallo común a todas las máquinas era el hecho de que la rotación del rotor lento hacía que en algunos casos, en particular cuando el rotor intermedio estaba en la posición de salto, girase éste también tal como podemos ver en la siguiente tabla obtenida del libro de Bauer [BAU13, 253]:

```
ADU
ADV
AEW
BFX
BFY
BFZ
BFA
```

En la máquina K española también se produce este doble salto cuando los rotores derecho y central llegan a sus muescas de salto, en este caso E e Y.

[10] Manual de uso de la Enigma hecho en Salamanca en noviembre de 1936.

III	II	I	Orden de rotores
A	D	W	
A	D	X	
A	D	Y	
A	E	Z	Primer salto
B	F	A	Segundo salto
B	F	B	
B	F	C	

Este doble salto reducía el número de posibilidades de 17576 (26 x 26 x 26) a 16900 (26 x 25 x 26). Evidentemente, al aumentar el número de muescas de salto, este doble salto se producía más frecuentemente y se reducía el periodo real de la máquina.

Finalmente debemos hablar de otro defecto consecuencia del diseño, una letra no podía ser cifrada por ella misma. Esto que se vendió como una ventaja de la máquina era en realidad un claro defecto y un punto de entrada excelente para un ataque por palabra probable. Si en un mensaje cifrado con Enigma sabemos de la existencia de una palabra larga (en alemán son mucho más frecuentes que en español) solo tenemos que buscar los lugares en los que no haya coincidencia en ninguna letra y tomarlos como palabra probable para un ataque. Evidentemente no es una gran debilidad, pero sí es una debilidad, mayor cuanto mayor sea la longitud de la palabra o frase que suponemos aparece en el mensaje.

Lo anterior pude daros una idea por qué una máquina con una cantidad tan grande de posibles combinaciones pudo ser derrotada. Pero no solo hubo fallos de diseño e inherentes a la máquina, sino también en su uso. Resumiendo podemos hablar de debilidades de:

1. La máquina.
    a. Una letra no se cifraba nunca como ella misma. Ya hemos hablado de ella. En realidad era una restricción del diseño como consecuencia del uso del reflector. La corriente no podía volver por un circuito generado por la misma letra o provocaría un cortocircuito.
    b. A pesar de tener un reflector de cableado variable, el *Umkehrwalze D*, no llegó a utilizarse, utilizándose generalmente un único tipo de reflector que ayudó mucho a los criptoanalistas aliados ya que conocían su esquema interno desde 1940.
    c. No se cambiaron los cableados internos de los rotores en toda la guerra. En realidad desmontar un rotor lleva su tiempo y exige una cierta destreza, los alemanes no podían cambiar los cableados de todos los rotores de una forma rápida y uniforme.
    d. El doble salto del rotor central del que ya hemos hablado. Este fallo de diseño se mantuvo incluso cuando se añadieron más muescas de salto.
2. De su utilización.
    a. A pesar de que el número de conexiones frontales era variable, la mayoría de las veces se utilizaban diez pares de conexiones (*steckers*).
    b. Se utilizaban varias versiones de la máquina repitiéndose mensajes entre diferentes redes. Eso hacía vulnerables los mensajes cuando pasaban por una red menos segura. Por ejemplo el *Abwehr* y la *GESTAPO* utilizaban máquinas sin panel de conexiones frontal, más débiles criptográficamente hablando que las militares.
    c. Se hacía un uso frecuente de estereotipos. Esta particularidad de los ambientes militares permitía hacer conjeturas sobre el contenido de un mensaje.

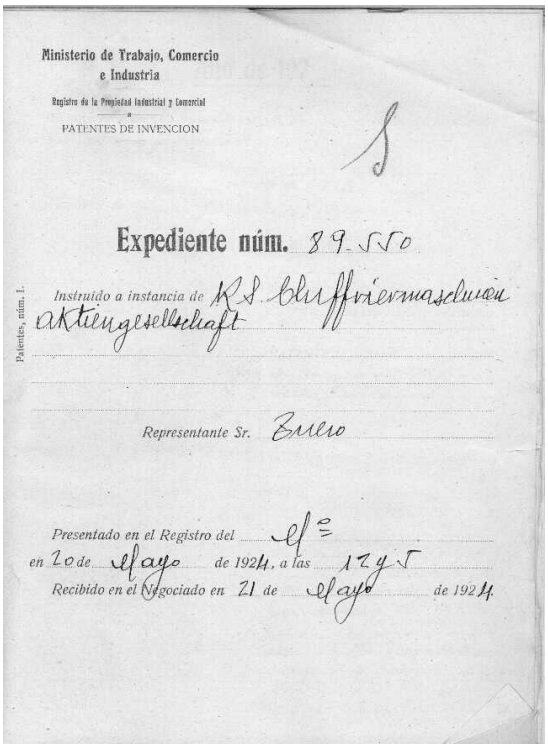
d. Alta frecuencia de mensajes cifrados con la máquina. También en criptografía el silencio es oro. La facilidad que daba la máquina hacía que se cifrasen toda clase de mensajes, aunque muchos podían y debían ser cifrados con cifras de un menor nivel, esto hacía que hubiese muchos mensajes para utilizar en los intentos de criptoanálisis.
e. Longitud excesiva de los mensajes. Entre otros los informes solicitados por Hitler que exigía fuesen muy detallados, y, en consecuencia, muy largos.

Como vemos, la máquina no era perfecta, pero sí una buena máquina de cifra, que bien utilizada podía dar suficiente seguridad.

Enigma en España. Los años previos a la Guerra Civil.

Un archivo a veces poco estudiado pero de una gran importancia en todo lo relacionado con los avances técnicos es sin duda el del Archivo histórico de la Oficina española de patentes y marcas. Allí podemos encontrar detalles de las patentes, entre otras de las máquinas Enigma: 89550, 89546 y 89611; de la Kryha: 9250; y de la de Hebern:109136.

Con respecto a la máquina Enigma que es la que nos interesa las tres patentes son presentadas por un tal Sr. Bueno, aunque la 89456 y la 89611 en representación de *Naamlooze Vennootschap Ingenieursbureau "Securitas"*, mientras que la 89550 lo es en representación de *Chiffriermaschinen Aktiengesellschaft*. La patente 89456 es la misma que la 193035 registrada en Gran Bretaña, mientras que la 89611 parece ser una Enigma A. La más curiosa de las tres es la correspondiente a la tercera patente que hemos comentado, la 89550.


Ministerio de Trabajo, Comercio e Industria

Registro de la Propiedad Industrial y Comercial

PATENTES DE INVENCION

Expediente núm. 89.550

Instruido a instancia de K.A. Chiffriermaschinen Aktiengesellschaft

Representante Sr. Bueno

Presentado en el Registro del ... en 20 de mayo de 1924, a las 12 y 5

Recibido en el Negociado en 21 de mayo de 1924

Ilustración 7. Primera página de la patente 89550

.

La patente corresponde a una patente alemana fechada el 17 de mayo de 1924. Si miramos en el libro de Turkel, las únicas patentes de esa época son la 407804 presentada el 18 de enero de 1924 y patentada el 22 de agosto de 1925 y la 400795 presentada el 18 de agosto de 1923 y patentada el 19 de agosto de 1924. En el libro de Turkel se dice que se trata de una máquina con

bombillas formada por dos dispositivos uno para generar texto cifrado y otro para el texto en claro, [TUR27, 94].

En la descripción de la patente se habla de que "*el objeto del invento es un aparato eléctrico de teclas para cifrar el cual se distingue por una forma de construcción reducida y por consiguiente que ocupa pequeño espacio y una gran seguridad respecto a la técnica del cifrado y que presenta otra ventaja en que un falso servicio del aparato está excluido por una forma de construcción especial de sus distintas partes.*".

El esquema, como podemos ver en el dibujo siguiente, es el de una máquina Enigma con dos rotores con los números del 1 al 28. La máquina dispone de una parte superior muy similar a la de la Enigma comercial, pero con solo dos aperturas para los dos rotores de los que dispone, así como dos para ver los números. Vemos también una tecla un poco mayor, dispuesta en la parte superior derecha y marcada con el número 13 en la figura 2, que bloquea o desbloquea el mecanismo de cifra. El proceso de cifrado consiste pues en pulsar primero la tecla para desbloquear la máquina, cifrar siguiendo el método clásico de la enigma, es decir, pulsando teclas y anotando el texto cifrado aparecido en las bombillas que se encienden, y una vez finalizado el cifrado volver a pulsar la tecla 13 para bloquear otra vez la máquina.

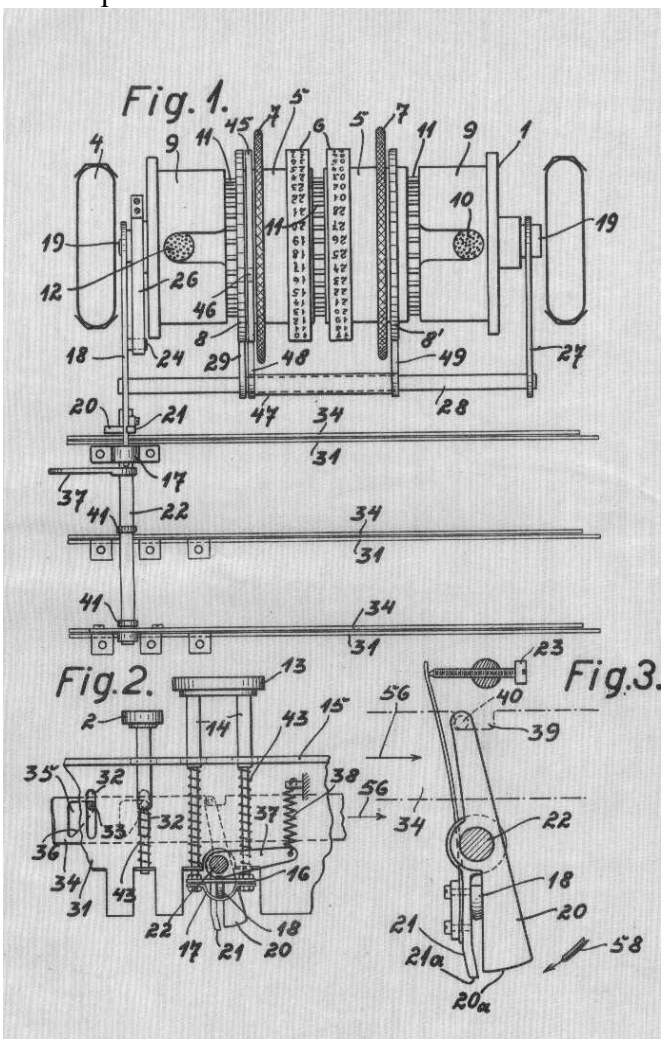


Ilustración 8. Detalle de la máquina

Para cifrar los dos comunicantes se ponen de acuerdo en la posición de los rotores, que puede controlarse en las aperturas superiores identificadas con el número 54 en la figura 3. La seguridad era menor que en los modelos comerciales y militares que conocemos, ya que el período de la clave se reducía, con respecto a otros modelos, a 784. Poca seguridad para aplicaciones

militares y diplomáticas, pero quizás suficiente para aplicaciones de tipo comercial, y seguramente a un coste mucho menor que en la Enigma comercial.

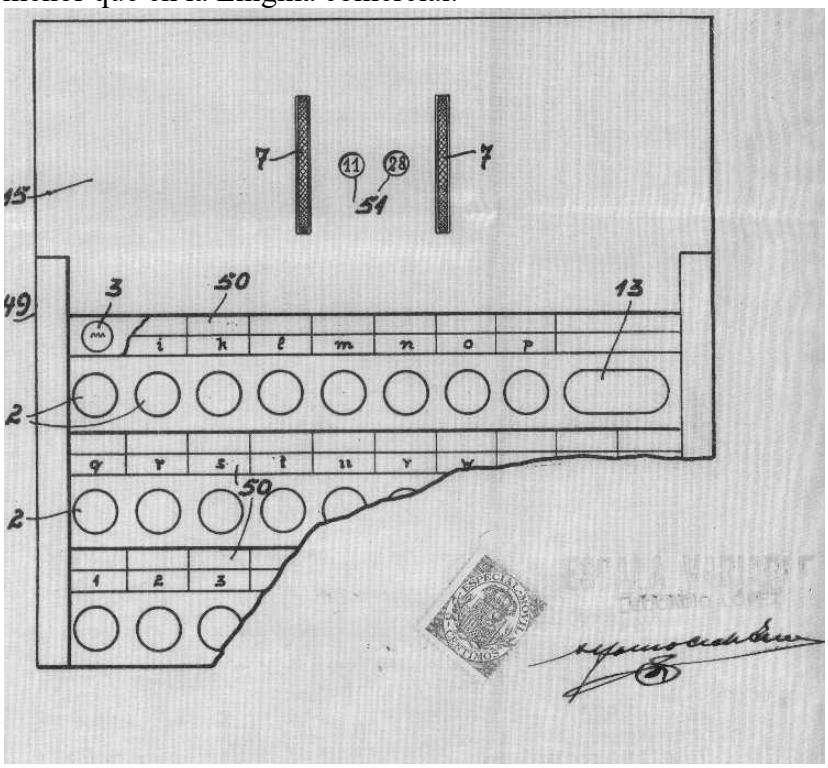


Ilustración 9. Vista superior de la máquina

.

Al final de la memoria se indica que deben existir dos aparatos, uno para cifrar y otro para descifrar. Según la descripción "*De estos aparatos cooperan cada dos aparatos de igual construcción en el transmisor y otros dos en el receptor y uno de los aparatos está en disposición de cifrar y el otro en la de descifrar*". Eso indica que estas máquinas debían venderse, si es que llegaron a fabricarse, en grupos de dos.

Como vemos se trata de una versión reducida de la máquina Enigma. No sabemos si llegó a comercializarse, aunque creemos que no. Al menos no sabemos de la existencia de ninguna máquina de este estilo en España ni hemos oído hablar de ella en ningún otro sitio. Probablemente se trataba, al igual que en el caso de la Enigma Z, de la que hablaremos a continuación, de un prototipo diseñado con la intención de reducir costes en la fabricación de las máquinas, aún a pesar de reducir la seguridad de las mismas. Su destino final debía ser el mercado comercial, no necesitado de tanta seguridad pero más preocupado de la cuestión económica. Sin embargo, como tantos otros modelos de máquinas, seguramente nunca llegó a ver la luz.

La Enigma Z.

El 10 de noviembre de 1931 el Ministerio de Estado hace una petición a la Embajada de Berlín para que solicite información sobre las máquinas de cifra usadas en Alemania. Unos días después se recibe presupuesto de la *Chiffriermaschinen Aktiengesselschaft* de tres máquinas. La Enigma A, la Enigma H, y la Enigma Z [QUI04]. De la primera ya hemos hablado anteriormente. La segunda es un modelo de ocho rotores aparecido en 1929 que tenía como característica diferenciadora el que utilizaba cuatro de ellos como control y cuatro para cifrar, además de contar con un contador al igual que en la Enigma G de la que hablaremos más adelante. De ésta solo se conserva un ejemplar en el Museo Militar de Budapest.

En cuanto a la Enigma Z, se trata de un modelo más pequeño, tanto en tamaño como en peso[11], que la Enigma K, que fue la más ampliamente utilizada en nuestro país. Se trata de un modelo bastante peculiar dado que el teclado solo tenía diez teclas con los números del cero al nueve, al igual que el panel frontal de luces y los rotores. Según el profesor Quirantes disponía de tres rotores y un reflector variable, al igual que en el modelo K. De acuerdo con el folleto de venta de la máquina, ésta tendría un periodo de 10000, lo que parece dar a entender que el rotor, identificado en el folleto comercial como "cilindro de permutación" era móvil y se movía al igual que el resto de los rotores como en la Enigma G, y no era un rotor como el de la Enigma K que, si bien era móvil, una vez puesto en posición no variaba. Por lo que sabemos se construyeron dos versiones de esta máquina, una con los arrastres típicos de Enigma y otra con los de la Enigma G. Algunos países como Chile y Suecia adquirieron ejemplares de la máquina, no así nuestro país, que nosotros sepamos [SOL10]. No parece que haya sobrevivido ninguna, al menos no tenemos conocimiento de su existencia en ningún archivo ni museo.

La Enigma K.

El modelo K fue el utilizado en nuestro país por las fuerzas nacionalistas, en realidad la letra K indicaba que eran modelos con cableados especiales controlados [TICOM M-13]. Este modelo se vendió libremente en el mercado hasta la llegada de los nazis al poder en 1934. Al parecer la adopción de esta máquina por las fuerzas del general Franco fue una recomendación de los alemanes, al menos eso fue lo que nos dijo un buen amigo, que además tenía información de primera mano sobre el tema al ser uno de los hijos del general Sarmiento, la persona encargada de la cifra y contracifra en España durante la Guerra Civil y los primeros años de la posguerra y autor de las instrucciones de uso de la Máquina en Español. Lo cierto es que no hemos podido ver ninguna confirmación documental sobre el hecho, aunque consideramos tal aseveración como muy lógica dado el estado, criptológicamente hablando de los dos bandos al principio de la guerra. No fue la única máquina de cifra utilizada en la contienda, la otra máquina utilizada en cantidades más o menos apreciables fue la Kryha, la famosa "bombonera", en sus dos versiones, la de sobremesa y la de mano, denominada Liliput.

.

Ilustración 10. Máquina Kryha estándar

[11] Tenía unas medidas de 21,6x15,6x11,5 y un peso de 4 kg. las medidas corresponden a la máquina sin la caja.

Las máquinas Kryha ya eran conocidas en España, al menos por el Ministerio de Estado, que a principios de los años treinta adquirió algunas del modelo Liliput en detrimento de la Enigma, muy superior desde el punto de vista de la seguridad. Durante la guerra se intentaron adquirir algunas más. Concretamente en 1938. A pesar de que el Cuartel General del Generalísimo pretendía comprar 24 máquinas, el precio de las mismas hizo que se acabasen comprando, por lo que sabemos, cinco Kryha Estándar por un importe de 5304,75 marcos y tres kryha Liliput por un importe de 2623 marcos (9066,60 pesetas de la época). Poco tiempo después se hace otro pedido de seis máquinas más para el Estado Mayor del Aire, dos estándar y cuatro Liliput. No sabemos de más adquisiciones de estas máquinas, aunque sí de su uso en diferentes fechas en Mallorca, en el Alto Estado Mayor y en Marruecos.

Ilustración 11. Kryha Liliput.

El bando republicano, aunque intentó hacerse con máquinas de cifra, no consiguió adquirir ninguna, a pesar de solicitar información a organismos de países teóricamente neutrales como Inglaterra. Posiblemente ayudara el hecho de que la mayoría de los países europeos estaban rompiendo sus cifras y, posiblemente, no querían dejar de perder esa fuente de información.

Volviendo a la Enigma K, fue utilizada por las marinas nacionalista, alemana e italiana, así como por la Legión Cóndor y por el ejército del general Franco a nivel de Cuerpo de Ejército. En funcionamiento hubo dos o tres anillos de comunicaciones con Enigma, y consecuentemente dos o tres cableados de los rotores, el del Ejército de Tierra, el de la Armada y posiblemente el de la legión Cóndor, aunque este último no hemos podido confirmarlo a día de hoy.

Ilustración 12. Comparación entre la Enigma militar y la modelo K.

La Marina nacionalista utilizó las máquinas Enigma para su inteligencia con sus homólogos italianos y alemanes. A pesar de que estas máquinas eran las menos seguras, dado que, inexplicablemente, utilizaban el cableado estándar en sus rotores, se aumento su seguridad utilizándola como supercifrado de un código de señales. El código, denominado DEI, era una abreviatura de Deutschland, Italia, España y fue concebido por tres oficiales, uno de cada nacionalidad. Lamentablemente, a día de hoy no hemos podido encontrar ninguna copia del mismo.

Cilindro	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Muesca	Ventana
Rotor I	CIAHFQOYBXNUWJLVGEMSZKPDTR	G	Y
Rotor II	KEDXVBSQHNCZTRUFLOAYWIPMJG	M	E
R. III	NUJPHWFMGDOBAVZQTXECLKYSIR	V	N
UKW	IMETCGFRAYSQBZXWLHKDVUPOJN		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

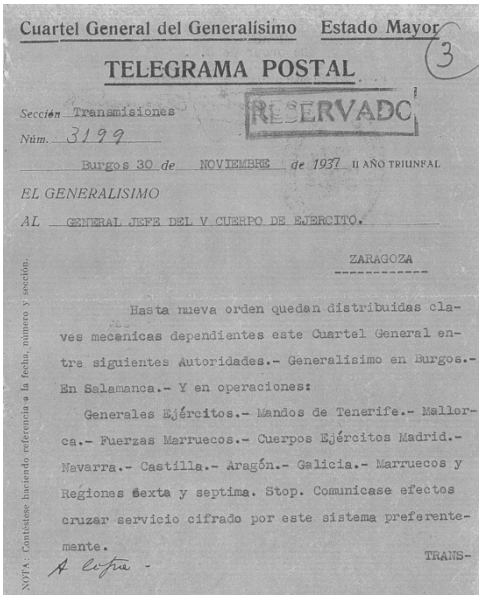
Ilustración 13. Cableado de la Enigma naval española (SNA o D)

El Ejército nacionalista utilizó un cableado diferente, conocido por los criptoanalistas americanos como F, cableado que venía de serie para el grupo de máquinas utilizado por él. Es de notar que, a pesar de haberse comentado en algunos medios la posibilidad de que las máquinas hubiesen sido recableadas, lo cierto es que no lo fueron nunca, manteniéndose el cableado original hasta su retirada. Esa diferencia en el cableado permitió que los británicos no pudiesen romper el código hasta el 12 de diciembres de 1943.

Cilindro	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Muesca	Ventana
Rotor I	HFOTWPDURMCGXJLQEIVZSKBNAY	G	Y
Rotor II	MUHTASIPJYNCVKLOXFDZEGQBWR	M	E
R. III	DKWOJVUNGLFTZCSYIBEARHXQPM	V	N
UKW	IMETCGFRAYSQBZXWLHKDVUPOJN		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

Ilustración 14. Cableado de la Enigma militar española (F)

En la imagen siguiente podemos ver una distribución de máquinas Enigma en noviembre de 1937.



Cuartel General del Generalísimo Estado Mayor

3

TELEGRAMA POSTAL

RESERVADO

Sección Transmisiones

Núm. 3199

Burgos 30 de NOVIEMBRE de 1937 II AÑO TRIUNFAL

EL GENERALISIMO

AL GENERAL JEFE DEL V CUERPO DE EJERCITO.

ZARAGOZA

Hasta nueva orden quedan distribuidas claves mecanicas dependientes este Cuartel General entre siguientes Autoridades.- Generalisimo en Burgos.- En Salamanca.- Y en operaciones:

Generales Ejércitos.- Mandos de Tenerife.- Mallorca.- Fuerzas Marruecos.- Cuerpos Ejércitos Madrid.- Navarra.- Castilla.- Aragón.- Galicia.- Marruecos y Regiones Sexta y septima. Stop. Comunicase efectos cruzar servicio cifrado por este sistema preferentemente.

TRANS-

NOTA. Contéstese haciendo referencia a la fecha, número y sección.

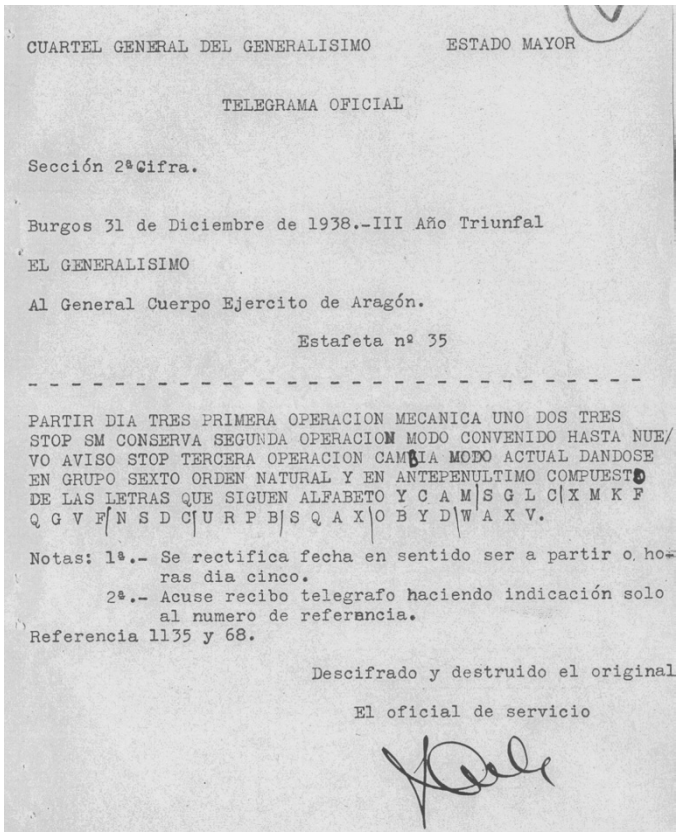
Ilustración 15. Distribución de máquinas Enigma en noviembre de 1937

Acabada la guerra se siguieron utilizando para las comunicaciones con los agregados militares y navales en Roma, Berlín, Vichy y Berna y con la División Azul. Hay que destacar que en cada una de esas legaciones diplomáticas había dos máquinas diferentes, la de Marina y la del Ejército y, por lo que sabemos, las claves utilizadas para las comunicaciones entre Berlín y Madrid, al menos las de los Agregados Militares, eran diferentes de las utilizadas entre Madrid y Roma[12]. Según los británicos los españoles cifraban de una manera infantil, utilizando unas claves muy sencillas. Lo cierto es que las claves utilizadas, así como la periodicidad de cambio de las mismas no era lo adecuada, sin embargo, no debemos culpar en exceso a nuestros compatriotas, que estaban convencidos de que Enigma era un sistema totalmente seguro, o al menos se les había vendido como tal.

En cuanto a la configuración de la máquina, tenemos que destacar que el anillo del rotor variable también podía moverse, con lo cual la configuración incluía la posición inicial del rotor, así como la posición del anillo. En España la configuración inicial se indicaba por el indicativo de primera, segunda y tercera operación. La primera consistía simplemente en poner el orden de los rotores, que aquí se denominaban tambores, es decir por ejemplo poner los rotores en el orden III, I y II de izquierda a derecha. Esta operación se realizaba poco frecuentemente por lo que sabemos.

La segunda operación era la colocación del anillo en los tres rotores y el reflector. Para ello se indicaban cuatro letras y se disponían los anillos en esa posición siempre de izquierda a derecha. Esta operación se realizaba más frecuentemente que la otra.

Por último la tercera operación consistía en la disposición inicial de los rotores una vez cerrada la máquina. Ésta a su vez venía indicada por cuatro letras y se disponían también en el orden marcado de izquierda a derecha.



CUARTEL GENERAL DEL GENERALISIMO ESTADO MAYOR

TELEGRAMA OFICIAL

Sección 2ª Cifra.

Burgos 31 de Diciembre de 1938.-III Año Triunfal

EL GENERALISIMO

Al General Cuerpo Ejercito de Aragón.

Estafeta nº 35

- -

PARTIR DIA TRES PRIMERA OPERACION MECANICA UNO DOS TRES STOP SM CONSERVA SEGUNDA OPERACION MODO CONVENIDO HASTA NUEVO AVISO STOP TERCERA OPERACION CAMBIA MODO ACTUAL DANDOSE EN GRUPO SEXTO ORDEN NATURAL Y EN ANTEPENULTIMO COMPUESTO DE LAS LETRAS QUE SIGUEN ALFABETO Y C A M | S G L C | X M K F Q G V F | N S D C | U R P B | S Q A X | O B Y D | W A X V.

Notas: 1ª.- Se rectifica fecha en sentido ser a partir o. horas dia cinco.
2ª.- Acuse recibo telegrafo haciendo indicación solo al numero de referancia.

Referencia 1135 y 68.

Descifrado y destruido el original

El oficial de servicio

Ilustración 16. Cambio de clave

Los indicadores, al menos desde finales del 43 eran de ocho letras y aparecían como la primer y última letra de los grupos segundo, tercero, cuarto y quinto.

[12] Cryptographic Systems and his solution I. The Spanish Military Attaché Enigma. Documentos cedidos por Ralph Erskine.

La Enigma G del Abwehr.

De este modelo solo sabemos de la existencia de un único ejemplar en España, la G219. A primera vista no parece haber mucha diferencia entre este modelo y el modelo K que hemos visto antes. Al igual que éste tiene tres rotores con letras en su anillo, un reflector variable y no dispone de panel de conexiones frontal. Sin embargo, es un poco más pequeña 25x27x16,5 cm., y tiene un contador en la parte superior derecha de la que la primera carece. Una vez abierta y extraídos los rotores empezamos a ver las diferencias. El rotor tiene un formato muy diferente de las máquinas tipo K. En las fotografías siguientes podemos ver una comparación de ambos. Como vemos el sistema de arrastre era diferente, una simple rueda dentada con 52 dientes, lo que evitaba en estas máquinas el doble salto característico del resto de máquinas Enigma.

Las teclas tienen dos valores en este modelo, uno la letra típica y el otro sirve para números, signos de puntuación, de operaciones matemática y letras especiales.

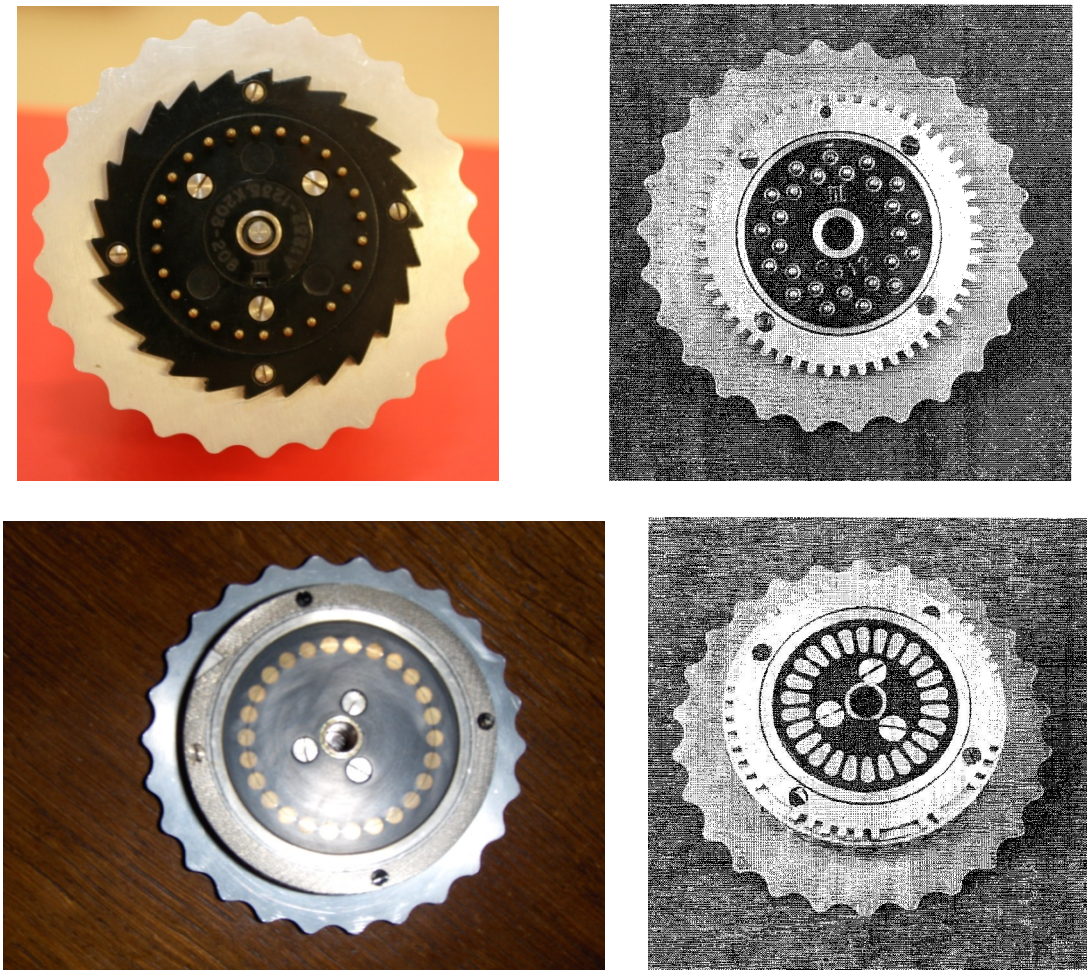


Ilustración 17. Diferencias entre los dos tipos de rotores

Además los rotores son más pequeños, unos 8,5 centímetros de diametro exterior en lugar de los 10 cm de la máquina militar. No acaban aquí las diferencias. Si vemos la entrada del reflector o la de la sustitución inicial (*Eintrittwalze*) vemos que son radicalmente diferentes y, al contrario que en el resto de las máquinas Enigma el reflector actúa como un rotor moviéndose al igual que ellos con lo que el periodo en este caso sería de 26^4 (456976).

El cableado de la Enigma G era el siguiente si ponemos el anillo en la A:

Cilindro	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Muesca	Ventana
Rotor I	DMTWSILRUYQNKFEJCAZBPGXOHV	ACDEHIJKMNQSTWXY	SUVWZABCEFGIKLOPQ
Rotor II	HQZGPJTMOBLNCIFDYAWVEUSRKX	ABDGHIKLNOPSUVY	STVYZACDFGHKMNQ
R. III	UQNTLSZFMREHDPXKIBVYGJCWOA	CEFIMNPSUZ	UWXAEFHKMMNR
UKW	RULQMZJSYGOCETKWDAHNBXPVIF		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

Como vemos hay 17 muescas de salto en el primer rotor, 15 en el segundo y 11 en el tercero. Como vemos se trata de números relativamente primos. Esta particularidad le dio nombre en BP, en la que era conocida como “11-15-17”. Curiosamente, la sustitución inicial corresponde con el orden del teclado. Como vemos, el salto en la muesca corresponde con el desplazamiento de 8 posiciones en orden inverso del alfabeto a lo que se presenta en la ventana.

La Enigma Delta.

Se trata de una máquina militar clásica con un cableado distinto. Su funcionamiento es el clásico de una Enigma militar. Se caracterizaba por que delta en el fondo de la máquina, una vez extraídos los rotores, aparecía una letra similar a la.

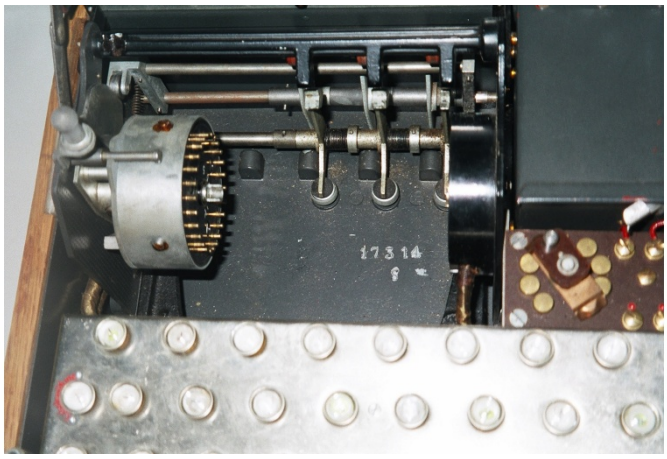


Ilustración 18. Interior de una máquina delta con su indicativo.

Ilustración 19. Máquina delta

El cableado de la misma obtenido de la máquina A-16081 por la unidad TICOM puede verse en TICOM M-3 o bien en el catálogo de máquinas Enigma [HAM54]. Al parecer este modelo fue utilizado por el agregado militar alemán en Zagreb. En España han aparecido también algunas de estas máquinas que, consecuentemente, puede ser fuese utilizada por el agregado militar alemán en España o por los Servicios Secretos alemanes ya que a España no llegó ninguna Enigma militar aparte de las utilizadas por los alemanes. Los únicos países que recibieron máquinas de ese tipo, aparte de la propia Alemania. Fueron: Italia, Rumania, Hungría Eslovaquia y Bulgaria [TICOM/DF-190-AM].

I				II				III				IV				V			
			R				O				T				O				R
A	1	3		A	1	24		A	1	19		A	1	8		A	1	23	
B	2	22		B	2	10		B	2	25		B	2	11		B	2	13	
C	3	6		C	3	7		C	3	9		C	3	20		C	3	7	
D	4	23		D	4	21		D	4	7		D	4	26		D	4	18	
E	5	10		**E**	**5**	18		E	5	24		E	5	4		E	5	11	
F	6	15		F	6	8		F	6	5		F	6	19		F	6	5	
G	7	2		G	7	26		G	7	12		G	7	18		G	7	10	
H	8	24		H	8	13		H	8	4		H	8	6		H	8	21	
I	9	1		I	9	25		I	9	21		I	9	23		I	9	1	
J	10	14		J	10	4		J	10	11		**J**	**10**	16		J	10	26	
K	11	17		K	11	12		K	11	2		K	11	3		K	11	6	
L	12	20		L	12	1		L	12	22		L	12	17		L	12	20	
M	13	4		M	13	20		M	13	15		M	13	10		M	13	15	
N	14	26		N	14	23		N	14	1		N	14	5		N	14	24	
O	15	21		O	15	11		O	15	23		O	15	25		O	15	9	
P	16	13		P	16	19		P	16	20		P	16	24		P	16	14	
Q	**17**	5		Q	17	5		Q	17	26		Q	17	14		Q	17	4	
R	18	25		R	18	16		R	18	8		R	18	22		R	18	25	
S	19	18		S	19	14		S	19	17		S	19	13		S	19	2	
T	20	16		T	20	3		T	20	14		T	20	21		T	20	17	
U	21	19		U	21	17		U	21	6		U	21	7		U	21	22	
V	22	11		V	22	6		**V**	**22**	3		V	22	5		V	22	8	
W	23	7		W	23	15		W	23	18		W	23	12		W	23	12	
X	24	9		X	24	9		X	24	13		X	24	1		X	24	3	
Y	25	12		Y	25	2		Y	25	10		Y	25	15		Y	25	16	
Z	26	8		Z	26	22		Z	26	16		Z	26	2		**Z**	**26**	19	

REFLECTOR							Fijo																		
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
4	15	14	1	10	21	24	20	17	5	12	11	19	3	2	26	9	22	13	8	6	18	25	7	23	16

Laas máquinas aparecidas en nuestro país tienen un cableado diferente a la de Zagreb. Es difícil saber la razón de esta variación de cableado, aunque seguramente éste era el original. Por lo que sabemos nunca fueron recableadas ni utilizadas por los servicios criptográficos españoles. Muy probablemente fuesen, como ya hemos comentado, utilizadas por el Agregado militar o por los servicios secretos alemanes en España. La diferencia de cableado quizás fuese una medida de

seguridad complementaria de manera que las máquinas en España formasen un círculo de comunicaciones específico.

I*				II				III				IV				V			
A17315S			R	A17315S			O	A17315S			T	A17315S			O	A17315S			R
	1	15			1	8			1	24			1	9			1	14	
	2	3			2	23			2	20			2	7			2	24	
	3	8			3	2			3	11			3	20			3	5	
	4	17			4	5			**4**	**6**			4	3			4	11	
	5	26		W	5	15			5	10			5	14			5	21	
	6	13			6	19			6	18			6	17			6	26	
	7	10			7	26			7	13			7	23			7	13	
	8	16			8	6			8	12			8	10			**8**	**17**	
	9	6			9	17			9	7			9	13			9	12	
	10	9			10	13			10	25		W	10	8			10	22	
	11	23			11	20			11	22			11	24			11	3	
	12	5			12	24			12	17			12	6			12	20	
	13	24			**13**	**18**			13	23			13	5			13	9	
	14	20			14	11			14	21			14	26			14	18	
	15	25			15	9			15	2			15	22			15	10	
	16	12			16	7			16	9			16	19			16	25	
W	17	7			17	22			17	5			17	25			17	8	
	18	22			18	10			18	8			**18**	**2**			18	19	
	19	2			19	25			19	1			19	12			19	4	
	20	11			20	16			20	14			20	16			20	7	
	21	4			21	21			21	16			21	18			21	1	
	22	14			22	3		W	22	4			22	15			22	6	
	23	21			23	12			23	19			23	11			23	2	
	24	18			24	14			24	15			24	4			24	16	
	25	**1**			25	1			25	26			25	1			25	23	
	26	19			26	4			26	3			26	21		W	26	15	

REFLECTOR							FIJO																		
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
25	9	15	7	20	24	4	11	2	19	8	22	23	18	3	17	16	14	10	5	26	12	13	6	1	21

¿Cuántas Enigma hubo en España?

Lo cierto es que es difícil saberlo. Aparte de las utilizadas por el Ejército y la Armada, es muy probable que los italianos utilizasen alguna en España para sus comunicaciones con Roma. Además de las que debían utilizar los agregados militares y navales, así como los centros de comunicaciones de los servicios secretos alemanes. Sabemos de la existencia de algunas máquinas Enigma en las Canarias utilizadas por el *Abwehr* y el SD para sus comunicaciones con Berlín, principalmente información sobre movimiento de buques y meteorológica. No sabemos exactamente qué tipo de máquina era utilizada, aunque sí que no era un modelo militar. Al parecer había comunicaciones también entre Villa Cisneros en el Sahara español (actual Dajla o ad-Dajl) y

París utilizando el mismo tipo de máquina. Los agentes alemanes debían tener una máquina en cada una de sus estaciones de espionaje. Aparte de la de las Canarias y las que debían tener en el centro de comunicaciones de la Embajada en Madrid había otras en la estación de Algeciras, Tetuán, Tánger y Ceuta, así como varias en el área del estrecho. Al parecer se trataba de máquinas del tipo K con reflector variable, aunque con un cableado diferente al utilizado por los españoles.

Como vemos es muy difícil discernir cuantas hubo en total en España, pero no debieron llegar al centenar. En nuestros estudios hemos podido clasificar una cuantas e identificar una cincuentena.

Guerra Civil	Cantidad
Ejército de Tierra nacionalista	39 de la cuales dos (k225 y k226) fuesen destinadas a la Marina
Marina nacionalista	Como mínimo 3+1. Probablemente más. Una, la K298 fue utilizada por la Marina italiana durante la guerra. Posiblemente fuesen la K209-K212 ya que éstas mantuvieron el cableado comercial.
Marina italiana	9. Véase nota de la línea anterior.
Marina alemana	Utilizaba máquinas Enigma para enlace con la Marina italiana y nacionalista. No se sabe cuantas.
Aviación nacionalista	No se sabe exactamente. Sabemos de la asignación de la K287, que ha hemos contado con las 39 del Ejército, a la Jefatura del Aire en 1938 y que la aviación utilizó Kryha.
Aviación italiana	Se sabe que utilizó máquinas Enigma con el nombre de clave IBERIA. No se sabe cuantas.
Legión Cóndor	Utilizaba máquinas Enigma. No se conoce el número.
Otros	
Abwehr Enigma	1
Máquinas delta y militares	4

Aparte de estas, tendríamos que tener en cuenta la existencia de las máquinas de tipo K recableadas utilizadas por los servicios secretos alemanes. Se sabe segura la existencia de nueve de esas máquinas, de las que solo conocemos la numeración de dos: la K297 y la K688. Curiosamente la K297 fue utilizada por la Sección de Cifra de la Misión naval italiana en Logroño, lo que parece confirmar que varias de las Enigma fueron devueltas a los alemanes una vez acabada la guerra civil.

A falta de más documentación, como ya hemos comentado, solo podemos especular sobre un número máximo de unas cien unidades de diferentes tipos. Sin embargo, dados los problemas de desclasificación de documentos en diferentes archivos, lo más sensato y agradable es disfrutar de la ventaja de poder ver en diferentes archivos militares estas máquinas que formar parte de nuestra historia y que, afortunadamente, han sobrevivido al paso del tiempo.

Bibliografía.

[2001]. *The Glow-Lamp Ciphering and Deciphering Machine: Enigma*. From the Archives. 2001Cryptologia 25(3): 161-173.
[BAN97] *Telegrafía militar*. Carlos Banús y Tomas. Publicaciones de la Revista Científico-Militar. Barcelona 1897.
[BAR95] *La participación naval italiana en la guerra civil Española (1936-1939)*. Franco Bargoni. Instituto de Historia y Cultura Naval. Madrid. 1995.
[BAU13] *Secret History. The story of cryptology*. Craig P. Bauer. CRC Press 2013.
[BAU99] *An error in the history of rotor encryption devices*. Friedrich L. Bauer. Cryptologia vol. XXIII, número 3. Julio 1999. 229-243.

[ENC16] *La criptografía*. Luis Hernández Encinas. Los libros de la catarata 2016.
[KRU02] *The commercial Enigma: Beginnings of machine cryptography*. Louis Kruh y Cipher Deavours. Cryptologia vol, XXVI, número 1, Enero 2002, pp. 1-16.
[LEE03] *The dutch invention of the rotor machine, 1915-1923*. Karl de Leeuw. Cryptologia vol. XXVII, número 1. Enero 2003.
[LEW78] *Ultra goes to war.* Ronald Lewin. Hutchinson & Co. Ltd. 1978.
[LOS98] *Manual militar de telegrafía*. Fernando de Lossada y Sada. Librería de Hernando y Compañía 1898.
[ORT06] *Introducción a la criptografía. Historia y actualidad*. Jesús J. Ortega Triguero, Miguel Ángel López Guerrero, Eugenio C. García del Castillo Crespo. Ediciones de la Universidad de Castilla-La Mancha. Cuenca 2006.
[PIE92] *Rommel and the secret war in north Africa. 1941-1943*. Janusz Piekalkiewiez. Schiffer Publishing Ltd. 1992.
[QUI04] *Model Z: a numbers-only enigma version.* Arturo Quirantes (2004), Cryptologia, 28: 2, 153 – 156.
[SKI92] *Enigma and its Achilles Heel*. Hugh Skillen. Publicación hecha por el autor. 1992.
[SOL04] *Mechanical cipher systems in the Spanish Civil War*. José Ramón Soler Fuensanta,. 2004. Cryptologia 28(3):265-276.
[SOL08] *Soldados sin rostro*. *Los servicios de información, espionaje y criptografía en la guerra civil española.* José Ramón Soler Fuensanta y Francisco Javier López-Brea Espiau, 2008. Barcelona. Inédita Editores S. L.
[SOL10] *Spanish Enigma: A History of the Enigma in Spain*. José Ramón Soler Fuensanta; Francisco Javier López-Brea Espiau y Frode Weierud (2010), Cryptologia, 34: 4, 301 – 328
[TUR27] *Chiffrieren Mit Geráten und Maschinen* Siegfried Türkel. 1927.. Graz: Ulr. Mosers Buchhandlung.