

Procedimientos para los mensajes Enigma

por Dirk Rijmenants (<http://users.telenet.be/d.rijmenants/>)

Traducido por Rafael Padilla

Los Libros de Código

Con el propósito de garantizar comunicaciones seguras, el Ejército Alemán utilizó diversos procedimientos para transmitir y recibir mensajes. Para que un mensaje pudiera ser encriptado y desencriptado correctamente, tanto el emisor como el receptor del mismo debían configurar sus Enigma exactamente del mismo modo. Estas configuraciones eran distribuidas en libros de código. Por razones de seguridad, diferentes partes de las fuerzas armadas tenían su propia red, con libros de código diferentes y todo dentro de una red que poseía su propio nombre codificado.

Cada libro de código contenía la información siguiente:

- *Walzenlage*: Elección y orden de las ruedas o rotores.
- *Ringstellung*: El ajuste de los anillos, la posición del cableado del rotor, relacionada con su anillo alfabético.
- *Steckerverbindungen*: Los enchufes de conexión en el Panel de Conexiones.
- *Grundstellung*: Configuración (posición) inicial de los rotores (esto dependía del procedimiento utilizado).

Los libros de código eran distribuidos de antemano y contenían los ajustes básicos para un mes completo, día a día. Por lo general, los libros de código estaban bajo la custodia de un oficial, el cual era el responsable de configurar los rotores, los anillos de la máquina y el panel de conexiones. Tras eso, podía bloquear el frontal de la máquina con una llave. El operador, lo único que podía hacer era configurar la posición inicial de los rotores.

Ejemplo de la tabla de un libro de código:

GEHEIM!			Sonder-Maschinenschlüssel																
Tag	Walzenlage			Ringstellung			Steckerverbindungen									Kennguppen			
31	I	II	V	06	22	14	PO	ML	IU	KJ	NH	YT	GB	VF	RE	DC	XSZ	FDC	LTG
30	III	IV	II	17	04	26	BN	VC	XS	WQ	AZ	GT	YH	JU	IK	PM	CFH	XAP	LOF
29	V	I	III	15	02	09	ML	KJ	HG	FD	SQ	TR	EZ	IU	BV	XC	PEH	MDG	NBX

Puede parecer extraño que el orden de los días esté invertido. La razón es muy simple: cada día, el operador arrancaba la tira correspondiente al día anterior y la destruía para evitar dar pistas sobre los mensajes.

La Clave del Mensaje

Los ajustes de configuración de la máquina eran válidos sólo para un día. El utilizar los mismos ajustes para un gran número de mensajes sería arriesgar la seguridad, al facilitar el criptoanálisis. Por lo tanto, cada mensaje era enviado con un indicador o posición inicial diferente, elegida al azar por el operador. A esto se le llamó "La clave del mensaje".

Antes de 1940, los militares alemanes utilizaban la clave diaria y la configuración inicial de acuerdo al libro de códigos. El operador seleccionaba un mensaje inicial de tres caracteres, que era la clave del mensaje entero. Esta clave del mensaje era encriptada dos veces, para evitar errores. Como ejemplo, el grupo de tres caracteres TGK es encriptado dos veces, dando como resultado XMC FZQ. A continuación, el operador movía los rotores a la posición inicial de GHK y encuitaba el mensaje. Los dos trigramas, siendo la información de la clave inicial del mensaje se transmitían junto con este, normalmente al principio del mismo. El receptor ajustaba su máquina en la configuración prescrita por el libro de códigos y tecleaba los trigramas XMC FZQ, lo que le daba GHK GHK, lo cual era la verdadera clave inicial. A continuación, ponía los rotores en GHK y tecleaba el resto del mensaje, el cual era decodificado.

El seguir este procedimiento implicaba una grieta importante en la seguridad. La clave del mensaje es encriptada dos veces seguidas, lo que por medio del criptoanálisis revelaba una relación entre los

caracteres primero y cuarto, segundo y quinto y tercero y sexto. Aún más, para cada clave inicial de ese día se utilizaban la misma configuración de rotores y la misma clave inicial (las prescritas en el libro de códigos). Esta falla en la seguridad permitió que la Polish Cipher Bureau (La Oficina de Cifra Polaca) rompiera los mensajes Enigma de anteguerra. Sin embargo, desde 1940 en adelante, los alemanes cambiaron los procedimientos para aumentar la seguridad.

Durante la Segunda Guerra Mundial, los operadores alemanes utilizaban los libros de códigos solamente para configurar los rotores y su orden (y la configuración del panel de conexiones). Después de configurar así la máquina, el operador seleccionaba al azar una posición inicial de los rotores, por ejemplo WZA y al azar también, otro trigramo, digamos SXT. Puestos los rotores en WZA, tecleaba "S X T", lo cual sería la clave inicial del mensaje y anotaba el resultado, que digamos era UHL. Una vez anotados WZA y UHL, ponía los rotores en SXT y encriptaba el mensaje. Una vez terminado, incluía en la cabecera que se enviaba antes del mensaje en sí la secuencia = WZA UHL = y enviaba todo. El receptor ponía su máquina en WZA, como le indicaba la cabecera, tecleaba UHL y obtenía SXT. Ponía los rotores en SXT y desencriptaba el mensaje.

Ejemplo de mensaje en cuya primera línea (la cabecera) iba el doble trigramo:

U3F DE C 1820 = 44 = WZA UHL =

QBLTW LDAHH YEOEF PTWYB LENDP MKOXL DFAMU DWIJD XRJZY
DFRIO MFTEV KTGUY DDZED TPOQX FDRIU CCBFM MQWYE FIPUL

Procedimientos y Abreviaturas

La máquina Enigma del ejército sólo utilizaba los 26 caracteres numéricos. Los números se deletreaban o se enviaban en letra. Los signos ortográficos se reemplazaban por combinaciones inusuales de caracteres y los acentos y marcas diacríticas, obviamente no existía. La ò se enviaba como OE y la ù como UE. Los espacios eran omitidos o reemplazados por la letra X. La X se usaba generalmente como indicador de punto y aparte o punto final. Algunos signos diferían en otras partes de las fuerza armadas.. La Wehrmacht reemplazaba a la coma con ZZ y al signo de interrogación con FRAGUE o FRAQ. La Kriegsmarine, sin embargo, reemplazaba a la coma con Y u al signo de interrogación con UD. El grupo de caracteres CH, como en Acht (ocho) o en Richtung (dirección) se reemplazaban con Q (AQT, RIQTUNG). Dos, tres o cuatro ceros se tecleaban como CENTA, MILLE o MYRIA para evitar repeticiones de una palabra (ZERO... ZERO...). La Wehrmacht y la Kriegsmarine transmitían sus mensajes agrupados de cinco en cinco caracteres. La Kriegsmarine, que usaba la Enigma de cuatro rotores, transmitía sus mensajes agrupados en grupos de cuatro letras. Para dificultar aún más el criptoanálisis se prohibía que los mensajes tuvieran una longitud mayor de 250 caracteres. Los mensajes más largos que esto eran divididos en varias partes menores, cada una de ellas transmitida con una clave inicial diferente.

Para hacer del criptoanálisis algo aún más duro, se introdujeron algunas "complicaciones" adicionales en los procedimientos de los mensajes a lo largo de la guerra. Dado que el tercer rotor, el más a la izquierda, sólo avanzaba un paso cada 676 pulsaciones, este rotor no tenía demasiada influencia durante la encriptación. Los mensajes así de largos eran prohibidos por razones de seguridad. Sin embargo, el operador podía cifrar cierto código de cuatro letras dentro del mensaje, por ejemplo CYOP y tras teclearlo, avanzar manualmente el rotor más a la izquierda hasta la letra, en este caso, O. Cuando el receptor encontraba el "CYOP" en el mensaje, se detenía, avanzaba manualmente el rotor más a la izquierda hasta la letra O y continuaba la desencriptación. Otra complicación más, añadida la final de la guerra, era el colocar los rotores "con rotación" cada 8 horas, uno de los rotores, uno dado (normalmente el derecho, que se desplazaba al extremo izquierdo), era 'rotado'. Si los rotores para ese día eran 241, esto cambiaba durante el día primero a 124 y luego a 412. Los ajustes de los anillos (*ringstellung*) de los rotores individuales no cambiaban y se movían con el rotor.

Procedimientos de la Kriegsmarine

Los procedimientos de la Kriegsmarine para el envío de mensajes con la máquina de cifrado Enigma eran bastante más complejos y elaborados que los procedimientos de la Wehrmacht y la Luftwaffe. Las hojas de códigos de la Kriegsmarine consistían en dos partes. La primera hoja, llamada *Schlusselfafel M Allgemein - Innere Einstellung*, contenía los valores de los tres rotores y sus ajustes de anillos. La segunda hoja, llamada *Schlusselfafel M Allgemein - Aussere Einstellung*, contenía la disposición de las conexiones en el panel frontal y la posición inicial de la máquina para cada día del mes. Antes de llevar a cabo la encriptación con la Enigma, el mensaje era encriptado con el libro de códigos *Kurzsignalheft* o código corto de señales, en el que los eventos se indicaban con grupos de número o letras. En otro apartado se detalla más el procedimiento de *Kurzsignal* (señales cortas).

Ejemplo de una hoja de códigos para los ajustes internos de Enigma:

Schlüssel M " T r i t o n "

Monat: Dezember 1943

Prufnummer:

Geheime Kommandosache!

 Schlusselftafel M - Allgemein

 (Schl.T. M All.)
 Innere Einstellung

 Wechsel 1200 Uhr D.G.Z

Monats- tag	Innere Einstellung				
31.	B	Beta	VI	V	III
	A		H	S	W
29.	B	Beta	VIII	IV	I
	A		T	L	A
27.	B	Beta	II	V	VI
	A		X	Z	P

Ejemplo de una hoja de códigos con las indicaciones del Panel de conexiones y la Configuración Inicial:

Schlüssel M " T r i t o n "

Monat: Dezember 1943

Prufnummer:

Geheime Kommandosache!

 Schlusselftafel M - Allgemein

 (Schl.T. M All.)
 Aussere Einstellung

 Wechsel 1200 Uhr D.G.Z

Monats- tag	Steckerverbindungen											Grund- stellung
31.	12/10	15/3	4/9	11/17	2/13	18/6	7/22	26/8	19/14	1/24		X V G K
30.	4/7	11/17	26/3	8/25	14/9	16/1	23/19	12/15	10/6	20/5		A S P I
29.	22/9	15/7	14/23	18/25	9/10	3/19	8/26	13/15	6/2	1/21		L K G V