

Kurzsignalen en los U-Boot alemanes.

Por Dirk Rijmenants

Traducido por Rafael Padilla.

Orígenes del Kurzsignale

Durante la Segunda Guerra Mundial, los U-boot (submarinos) alemanes utilizaban el *Kurzsignale* o el código de Mensajes Cortos para enviar sus mensajes. El *Kurzsignale* era una parte importante del complejo sistema de comunicaciones de la Kriegsmarine. En general, el *Kurzsignale* consistía en grupos de cuatro letras los cuales representaban a toda clase de frases relacionadas con información táctica, tal como curso, informes sobre el enemigo, cuadrículas de posición o informes meteorológicos. Una razón importante para que la Kriegsmarine utilizase el *Kurzsignale* era que los aliados utilizaban los Sistemas de Radio Detección de Alta Frecuencia (*High Frequency Direction Finding*) o abreviado, Huff Duff. Este sistema permitió que las fuerzas aliadas pudieran determinar la posición del origen de las transmisiones de radio alemanas. Esto representó una importante ventaja táctica en el atlántico, al revelar las posiciones de los barcos y los submarinos alemanes. El uso del *Kurzsignale* redujo muchísimo la longitud de los mensajes en telegrafía, reduciendo con frecuencia el tiempo de retransmisión a menos de un minuto. De este modo, la marina alemana hizo más difícil el fijar sus posiciones por medio del Huff Duff.

(Más adelante, se tratará sobre el sistema de transmisión de *Kurzsignale* conocido como “*Kurier*”)

Kurzsignale en los U-Boot

Los procedimientos de la Kriegsmarine para el envío de mensajes por medio de la máquina de cifrado Enigma, eran de lejos mucho más complejos y elaborados que los procedimientos de la Wehrmacht y de la Luftwaffe. Por supuesto, el hecho de que sus comunicaciones fueran seguras era una parte vital de la supremacía de la Kriegsmarine en el Atlántico. Los *U-boot* dependían completamente de sistemas seguros de comunicación para recibir sus órdenes, coordinar sus patrullas en el mar y para sus tácticas de “Ataque de Lobos”. Si las comunicaciones resultaban comprometidas, ello revelaría las posiciones navales alemanas y resultaría en la aplicación de contramedidas tácticas por parte de los aliados o en la caza activa de los *U-boot*. Durante la guerra, se emplearon varios sistemas de *Kurzsignale* en los submarinos. Hasta 1942, se utilizaron las señales de clase *Alpha*. Una señal *Alpha* consistía en un pequeño mensaje, conteniendo usualmente un solo grupo de cuatro letras. Desde 1942 en adelante, los submarinos alemanes utilizaban comúnmente las señales *Beta*. Durante la guerra se utilizaron varias ediciones del *Kurzsignalhefte*, los Libros de Código de Señales Cortas. Cada mensaje de *Kurzsignal* o señal *Beta*, tenía un formato estricto, conteniendo una introducción, una identificación a la clave y el mensaje en sí, encriptado con la máquina de cifrado Enigma.

Los Libros de Código

Para aplicar las *Kurzsignale*, la Kriegsmarine utilizó varios libros de códigos diferentes. Los dos libros más importantes de códigos eran el *Kurzsignalheft*, para toda clase de mensajes de operación y el *Wetterkurzschlussel*, para los informes meteorológicos. El *Kurzsignalheft* contenía tablas con las que se convertían frases en grupos de cuatro números. Se listaban en él toda clase de expresiones relacionadas con muchos tópicos diferentes. Asuntos logísticos, como repostaje y encuentros con barcos de suministros, posiciones y listados de la cuadrícula, nombres de puertos, países, armas, condiciones meteorológicas, posiciones enemigas y barcos, tablas de fechas y de horas. Se listaban todas las situaciones y tópicos posibles. Otro de los libros de código contenía los *Kennguppen* y los *Spruschlussel*, esto es las claves de identificación del responsable y la clave del mensaje, esto es, la posición inicial de los rotores de Enigma. Los libros de código estaban impresos en papel especial con tinta roja soluble en agua. Si se veía que los libros de código estaban en riesgo de ser capturados, se destruían con sólo arrojarlos al agua.

El Kurzsignale o Mensaje Corto

En nuestro ejemplo, mostraremos un Mensaje Corto, codificado con la edición de 1944 del Kurzsignalheft. Esta edición era más compleja que la anterior. El Kurzsignalheft 44 consistía en dos partes, Heft I y Heft II. El Heft I contenía el *Satzbuch* o libro de frases para convertir frases en grupos de cuatro números y también contenía el *Schlüsselzahltafel* o la tabla de números clave. El Heft II, llamado *Buchgruppenheft*, se utilizaba para convertir grupos de cuatro números en palabras de cuatro letras. Además, para firmar los mensajes o para identificar a otros submarinos en un mensaje, la Kriegsmarine utilizaba un libro de códigos llamado el *Marinefunknamenliste* o listado de indicativos navales. Este consistía en una lista con todos los submarinos existentes y sus trigramas. Un trígama era un grupos único de tres letras asignado a cada submarino. Por desgracia para la Kriegsmarine, esta edición más compleja de 1944 no entró en servicio a tiempo de cambiar la suerte de la para entonces diezmada flota de submarinos en el Atlántico. Vayamos ahora al ejemplo.

El mensaje que debía enviarse digamos que era:

```
GELEITZUG 16-20 DAMPFER
Quadrat CA 91 33 (CA 90 und 133)
U-999
```

Traducción: *Avistado Convoy de 16 a 20 barcos de vapor en la retícula CA 9133. Firmado, U-999.*

En primer lugar, las tres frases son convertidas en números a través del *Satzbuch* :

```
GELEITZUG 16-20 DAMPFER = 0512
Quadrat   CA 90           = 4545
           133            = 8152
```

A continuación, a estos tres valores numéricos se le suma un número, sin acarreo, esto es, *sin llevar* si pasa de la decena, obtenido de la *Schlüsselzahltafel*:

```
  0512 4545 8152
+ 0384 0384 0384
-----
 0890 4829 8436
```

Finalmente, los números resultantes son convertidos en grupos de cuatro letras por medio del *Buchgruppenheft* y el mensaje es firmado con el trígama que representa al submarino emisor, tomado de la *Marinefunknamenliste*:

```
0890 = ZLDP
4829 = OYAK
8436 = WIKW
U999 = LQX
```

No sólo los procedimientos de transmisión y el formato de los mensajes de la Kriegsmarine eran diferentes de los de la Wehrmacht y de la Luftwaffe. Las hojas de claves para los ajustes de la Enigma eran también diferentes. La Wehrmacht utilizaba una tabla de códigos con indicaciones de los rotores, ajustes de los anillos, conexiones en el panel frontal e indicativos de identidad (Kennguppen) para cada uno de los días del mes, todo ello en una hoja única. Las hojas TRITON de código de la Kriegsmarine consistían en dos partes. La primera hoja, llamada

Schlusselfafel M Allgemein - Innere Einstellung, contenía los tres rotores y su ajuste de anillos, el rotor delgado Beta o Gamma y el reflector y esto para todos los días impares de un mes entero. La segunda hoja, llamada *Schlusselfafel M Allgemein - Aussere Einstellung*, contenía las conexiones del panel frontal y la configuración inicial o *Grundstellung* para cada día del mes. La *Kriegsmarine Sonderschlüssel M*, utilizada para conversaciones privadas entre el Comandante de la Flota de Submarinos y un U-Boot en particular, tenía una hoja especial de códigos con sólo tres ajustes internos y tres ajustes para el panel de conexiones, cada uno con una validez de diez días, y una lista de *Spruchschlüssel* o claves de mensaje, designadas por una palabra de código. La *Sonderschlüssel M* era similar a la *Schlusselfafel M Offizier* de TRITON. Hay ejemplos de las claves usadas por la Kriegsmarine en la sección de "Procedimientos".

Con el objeto de preparar el mensaje para su transmisión, el operador tenía que cifrarlo con la Máquina de Cifrado Enigma. Seleccionaba al azar un *Kennguppe* y un *Spruchschlüssel* de su libro de códigos Kennguppenheft. El Spruchschlüssel o clave del mensaje era la posición inicial de los rotores de Enigma antes de la encriptación. Un Kennguppe era un trigrama que permitía identificar el Spruchschlüssel elegido al operador receptor. En nuestro ejemplo, el operador seleccionó el Kennguppe RDF con el Spruchschlüssel MKDF.

Los grupos, ya cifrados con Enigma:

QRLE ATMG SIKR ODX

El mensaje completado contenía la información siguiente:

- La señal de introducción $\beta\beta$ (beta beta)
- El trigrama del Kennguppe, sin encriptar
- Todos los grupos de señales, cifrados
- La firma, cifrada
- El Kennguppen sin encriptar, repetido

El mensaje completo de Kurzsignal, listo para ser transmitido:

$\beta\beta$
RDF
QRLE ATMG SIKR
ODX
RDF

Un operador de radio experimentado podría transmitir fácilmente este mensaje en Morse en unos 20 segundos.

Al final, el operador ¡ha utilizado 7 tablas u hojas de claves para cifrar su mensaje! El Kurzsignalheft Heft I con su Satzbuch para convertir las frases en grupos de cuatro números y el Schlüsselzahltafel para sumar sin acarreo al número clave, el Heft II con el Buchgruppenheft para convertir los grupos de cuatro números en grupos de cuatro letras, el Marinefunknamenliste para identificar a los submarinos, las dos hojas del Schlusselfafel M para los ajustes internos y externos de la máquina Enigma y finalmente, el Kennguppenheft para seleccionar la clave del mensaje. No es de extrañar que tuvieran confianza en la

seguridad de sus comunicaciones. A pesar de esto, los criptoanalistas aliados tuvieron éxito en romper las comunicaciones de los submarinos, como se puede leer en el apartado de "Enigma y la guerra submarina".

El Sistema Kurier

En Agosto de 1944, la Kriegsmarine comenzó las pruebas de un sistema experimental llamado "Kurier", el cual se diseñó como una contramedida que combatiera los sistemas de Búsqueda de Dirección en Alta Frecuencia de los aliados. Era un sistema basado en un principio hoy conocido como codificación en un impulso. El dispositivo Kurier era conectado a un radiotransmisor. El componente principal del Kurier era el generador de pulsos KZG 44/2, un tambor con 85 barras ajustables. Cada barra representaba a un pulso de señal. Al activar el dispositivo, un brazo con un elemento magnético efectuaba una sola rotación, pasando secuencialmente por las 85 barras predispuestas. Cada pulso que se generaba tenía una duración de 1 ms, con un intervalo de 3 ms entre pulsos. En total, con los pulsos de inicio y las pausas, la transmisión de un mensaje completo nunca tardaba más de ¡460 milisegundos!, El código de Kurzsignal que tenía que transmitirse era convertido a código Morse. Cada punto se enviaba por el Kurier como un solo pulso y las rayas como dos pulsos seguidos. Entre puntos y rayas había una pausa de un pulso de longitud y entre letras, de dos pulsos. El receptor Kurier KGR-1 convertía los pulsos en un haz de luz el cual era proyectado en un tambor rotatorio con papel fotosensible (hay más detalles técnicos en la Web dedicada a los sistemas alemanes de comunicación).

El sistema Kurier iba a ser utilizado en la transmisión de Kurzsignalen y de Wetterkurzsignalen, combinado además con un complejo esquema de cambios de frecuencia, con saltos de frecuencia de en más o en menos 200 KHz. Cada Wetterkurzsignalen Kurier tenía una longitud de siete letras. Cada letra correspondiente era sacada de una tabla en el libro de códigos Kurier. Por ejemplo: Si la primera letra de la Wetterkurzsignal era la G, ello quería decir una presión atmosférica de 1034 milibares. Como siempre con las Kurzsignalen, el mensaje era previamente codificado con Enigma previamente a su transmisión por medio del dispositivo Kurier.

Composición de la Wetterkurzsignal Kurier:

PDF WBBU

P Presión Barométrica
D Dirección del Viento
F Intensidad del Viento

W Nubes
BB Punto de Observación (tabla de bigramas)
U Identificación del área marina (Cuadrícula meteorológica)

A finales de 1944, Berlín hizo de las pruebas del Kurier una prioridad, pero el programa fue interrumpido antes de que el sistema Kurier estuviera operativo en la flota de submarinos. Los acontecimientos sobrepasarían todo y el final de la guerra detuvo la posibilidad de experimentos posteriores. Si el programa Kurier hubiera sido operativo en estadios más iniciales de la guerra submarina, ello hubiera resultado en consecuencias muy serias. La inteligencia aliada se hubiera encontrado sin sistemas de radiolocalización y de monitorización de los mensajes de Kurzsignalen. Esto no hubiera sólo implicado la pérdida del conocimiento de las posiciones de los submarinos alemanes, sino que habría también privado a los criptoanalistas en Bletchley Park de las cribas o "chuletas" necesarias para romper las claves de Enigma, utilizadas por la Kriegsmarine para encriptar su tráfico de mensajes. Todo ello podría haber cambiado el resultado final de la guerra en el Atlántico.