The *Kenngruppenbuch* Indicator System Used with the Main Wartime Naval Enigma Ciphers

by Ralph Erskine

The main wartime naval Enigma ciphers such as Hydra (called Dolphin by Bletchley Park) used the *Kenngruppenbuch* (indicator group book) system to spell out message keys - the rotor starting positions for enciphering a specific signal. When enciphering a signal, an operator had to let the recipient know what the actual message key was without revealing it to the enemy.

At the start of each cipher day (often 1200 hrs, DGZ, German legal time), a naval Enigma operator set up his machine. If it was the first day of a pair in a keylist, an officer had first to insert the rotors in the order set out in the keylist, after setting the rotor rings to the letters indicated in the list. The operator then set the external connections (*Stecker*) on his machine in accordance with the keylist

The *Kenngruppenbuch* system required operators to choose message keys from a random list in the book. This prevented them choosing guessable sequences such as ABC or WER (from the keyboard). Part A of the *Kenngruppenbuch* listed all 17,576 three-letter groups (trigrams – 'BSY' and so on) in random order. Each standard naval Enigma signal had its own message key. However, some naval Enigma ciphers did not use the *Kenngruppenbuch,* and there was a separate system for short signals.

To encipher a message with the *Kenngruppenbuch* system, the operator–

(a) looked up an allocation list to see which columns in Part A had been assigned to his cipher (e.g. columns 91–110 or 361–410 for Hydra in July 1944), selected a three-letter group in a column at random for the *Schlüsselkenngruppe* (cipher indicator group), and wrote it on a special cipher form;

(b) picked any column at random and chose another trigram (say VFN) as the *Verfahrenkenngruppe* (procedure indicator group, but actually the message key), and wrote it in the form under the first group;

(c) inserted a letter as a null (say X), as the first letter in the *Schlüsselkenngruppe* giving XHYU;

(d) added another null letter (say K) as the last letter of the *Verfahrenkenngruppe,* making VFNK. He then had–

```
XHYU
1234
VFNK
```

(e) encoded the vertical bigrams (XV, HF and so on) with bigram tables which substituted pairs of letters. XV and HF here gave BM and OG, for example. Written horizontally, these resulted in–

BMOG as the first indicator group
PYUD as the second indicator group.

He then went to his machine, and–

(f) turned the rotors to the *Grundstellung,* say GRD, set out in the keylist: each naval keylist contained a series of daily *Grundstellungen,* which were employed for all signals using the cipher in question;

(g) obtained the message key by typing the unencoded version of the *Verfahrenkenngruppe* (VFN) once, giving e.g. SPL;

(h) set the rotors to SPL as the message key,

(i) keyed the plain text of the signal, writing down each cipher text letter as its lamp lit up (often a two-man operation).

The cipher text was transmitted in four-letter groups, preceded by BMOG PYUD, although a few naval Enigma ciphers used five-letter groups. A typical message is set out below. The indicator groups were repeated at the end to reduce deciphering mistakes, making naval Enigma signals instantly recognisable to friend and foe alike.

A hand cipher, known as *Reservehandverfahren*, also employed similar repeated indicators to make it look like Enigma.

To decipher a message, the receiving operator went through the above steps in reverse (assuming that his machine was already set to the daily key for the cipher in question), first decoding the indicator groups using the relevant bigram tables to obtain the enciphered message key, VFN. By typing it, he obtained SPL, to which he set his rotors. He then typed the cipher text, and wrote down the resulting letters as they lit up.

The *Kenngruppenbuch* system was much more secure than the indicating system for army and air force Enigma, except for its use of a common daily *Grundstellung*. Together with different turnover notches in rotors I to V, the common *Grundstellung* enabled the Bletchley codebreakers to reduce the number of rotor combinations to be tested from 336 to as few as 18 by a process known as Banburismus. This saved an immense amount of bombe time, and was a vital part of breaking three-rotor naval Enigma (M3) from 1 August 1941 until mid-1943, when bombes became available in large numbers.

Typical naval Enigma signal, as intercepted

MMA’[1]   0141/4/370[2]   22[3]

HNMX[4] UOLP[4] FZNM HSNS CENH VHKQ TDEB XMTR GSRK DJYP XUKWQ SWED NTET MWVI AUXP XXDK TYQF QBZO DDND ULDA HNMX[4] UOLP[4]

0812[5] 6790[6]

1. Call sign of shore transmitting station. A’ was Ä (A in Morse with a ‘bar’ or dash added).
2. Time of origin, date and serial number.
3. Group count.
4. Indicator groups.
5. Time of intercept.
6. Frequency in kHz.