MEDITERRANEAN ENIGMA

1. The bulk of this traffic, called "Sued" by the Germans and "Porpoise" by the British, is enciphered on the 3-wheel naval enigma. The remainder, called "Henno", is believed to be a hand cipher like the R.H.V. The two types are indistinguishable by external characteristics; both are sent in 4-letter groups with the first two groups repeated at the end, and on the same frequency schedules. The users are surface craft and shore stations in the Mediterranean, Aegean, and Black Seas. The traffic averages about 120, 30 and 100 messages per day, respectively for the three areas; Henno probably 20-30.

The enigma keys are changed exactly as in Shark: wheels and rings usually last two days (sometimes only one and sometimes three), while the Stecker and Grundstellung change daily. Keys for the Offizier (called "Winkle") behave exactly as for Limpet. The system is not in the K-book family.

The operator selects a trigram at random, say PYX, at which to encipher the message, i.e. the left-hand wheel will be set at window position P, the middle at Y, and the right-hand wheel at X. To encipher the plain indicator PYX, the operator sets the machine at the Grundstellung in effect and enciphers PYXPYX, getting let us say RGYVMO. He then selects two letters, apparently at random, say U and S, and sends as the two-group indicator: URGY SVMO. Nothing is known about the significance, if any, of these beginning letters of the two indicator groups; it is possible they may serve to distinguish Porpoise from Henno.

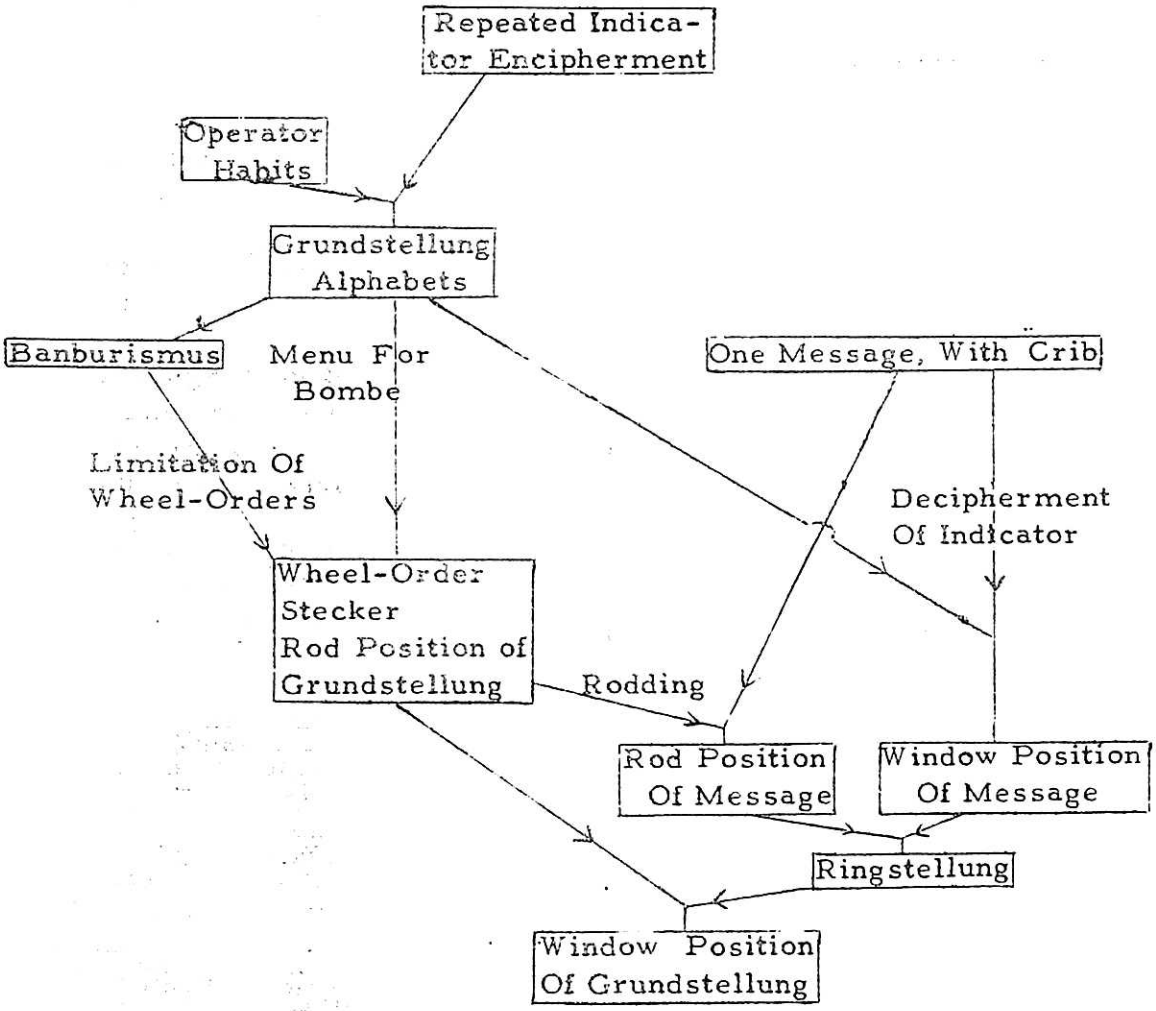
2. From this encipherment of the repeated clear indicator, and the habits of operators choosing trigrams "at random", the six Grundstellung alphabets are found (paragraph 3 below), i.e. those in the first six positions after the Grundstellung. From these a strong menu can be built; in fact they need not be complete for this. Moreover, Banburismus (paragraph 4 below) enables one to find the middle and right-hand wheels, except that VI, VII and VIII cannot be distinguished since their notches are in the same place (after M and Z). Thus the number of wheel-orders to try can be limited to 6, 18 or 36 as the case may be.

The bombe gives the wheel-order and Stecker, of course, and the

rod (i.e. core) position of the Grundstellung. Since we do not know the Ringstellung, the latter is as yet of no use. But all we need do is to rod one message, and the day is ours. For since we know the Grundstellung alphabets, we know at once from the indicator what the window setting of the message is, and this together with its rod position yields the rings.

A diagram of the daily procedure described above is given herewith. The entire job is usually finnished by 0600, leaving six current hours for the day. The paired day (paragraph 5 below) is usually out by 2000, leaving sixteen current hours.

DIAGRAM OF MEDITERRANEAN PROCEDURE



3. The first step in finding the Grundstellung alphabets is to make up a "throw-on" sheet (Exhibit 1.) Suppose the indicators of half a dozen messages are

1.	AYZX	TDAB
2.	VRFT	MXMK
3.	CZKJ	LWTQ
4.	RPOF	BCPG
5.	UYAF	MDEG
6.	VRMC	IXWV

Recall that the significance of the 8 letters is schematically

123	456
XLMR	XLMR

Thus in message #1 the initial letters A and T are dummies (indicated by X); Y and D are the encipherments of the initial window position of the left-hand wheel (L) in the 1st and 4th Grundstellung alphabets; Z and A likewise for the middle wheel (M) in alphabets 2 and 5 respectively; X and B for the right-hand wheel (R) in 3 and 6. On the throw-on sheet one enters D in the Y-row and L-column, A in the Z-row and M-column, and B in the X-row and R-column. These have been starred in Exhibit 1.

From the 250 messages on May 17, all but three squares were filled, and these were readily found. The so-called "duds" - probably mostly Hemno - do not fit the pattern, but they are easily eliminated by their failure to agree with the vast majority.

The second step is to "box" the throw-on sheet. This simply means to find the cyclic components of the three columns (separately). Thus for the L-column we get the cycles:

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

There must always be this pairings off into cycles of equal length. Perhaps the easiest way to see this is to take the correct answer (Exhibit 6) and work backwards. With reference to the L-alphabets 1 and 4 we see that

$$L \xrightarrow{1} R \xrightarrow{4} Z \xrightarrow{1} S \xrightarrow{4} W \xrightarrow{1} X \xrightarrow{4} L$$

It must take an even number of jumps to get back to the starting letter. Moreover, if we pick alternate letters we get L Z W AND R S X. These are the two cycles of length three, except that the second is reversed. This is clarified by breaking the above into two parts

$$L \xrightarrow{14} Z \xrightarrow{14} W \xrightarrow{14} L$$

$$R \xrightarrow{41} S \xrightarrow{41} X \xrightarrow{41} R$$

For the throw-on sheet is the effect of applying Grundstellung alphabet #1 and then #4, while applying first #4 and then #1 yields the inverse thereof.

But these considerations showing the origin of our paired cycles shows also what we must do to recover the constituent alphabets #1 and #4. One cycle must be reversed and larded into its mate. A convenient way of doing this is to write one down in double on one sheet of paper and the other reversed on another, and slide one under the other, thus:

A T Y D Q U G E I J A T Y D Q U G E I J

F N M K V H O C P B

In the above position we think

$$I \xrightarrow{1} F \xrightarrow{4} J \xrightarrow{1} N \xrightarrow{4} A \xrightarrow{1} \ldots \text{ etc.}$$

This is the "correct" position, as can be seen from Exhibit 6. In this way we can read plain-cipher pairings in alphabet #1 very readily - they are the vertical pairs IF, JN, AM, etc. Those in alphabet #4 are so obtained by sliding the bottom strip one place to the right: JF, AN, TM, etc.

Any one of the 10 possible alignments gives a possible (partial) alphabet #1 (and #4), which can be completed by any one of the 3 possible alignments of the cycles of length 3, making 30 possibilities in all. Now comes the job of telling which one is right. This depends