## HOME WATERS ENIGMA

This traffic, called Heimisch (or more recently Hydra) by the Germans, and Dolphin by the British, is on the 3-wheel naval enigma, and is a member of the K-book family. It is used by surface ships in the North Sea and Baltic, and by Arctic subs. The traffic has increased to over 500 messages a day. The Offizier, called Oyster by the British, has keys exactly similar to Limpet.

A diagram of the procedure followed in breaking a new day is given on page 2 below. The banburism begins as soon as the messages start coming in from the registration room, and continues well into the next day. Freeborn does not start sorting and tabulating until the day's traffic is all in, and his catalog starts coming in about 1700 of the next day. The two Grundstellung alphabets are usually complete before 2400, and the menu is sent to the bombes shortly thereafter. The correct stop is usually found by 0400, and the rest is a matter of a few minutes. A menu for the paired day has usually been prepared by that time, and is out by say 0600, leaving six current hours on the paired day. A more detailed description follows, of the determination of the Grundstellung alphabets and the middle and end wheels, the material being drawn from the day May 28.

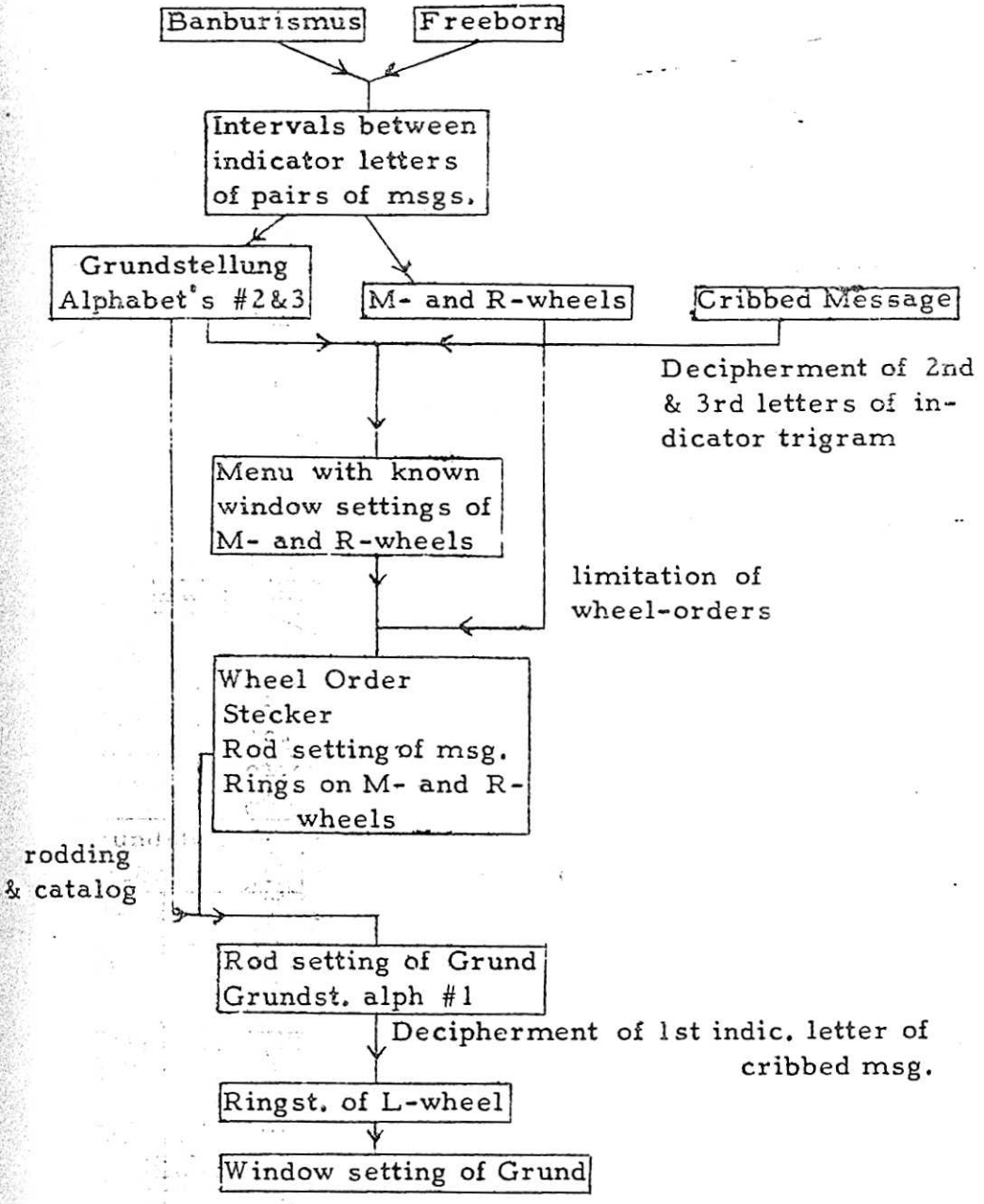
The Dolphin messages are first separated out by K-booking, and registration numbers assigned. The dummyismus percentage for each message is recorded on it, and the Roms Category (see below page 4) in which it falls. Each message is entered on the Foss sheet, and a Banbury sheet is punched up, with the dummy percentage and Roms Category recorded thereon, as well as the enciphered indicator trigram (after bigramming, of course). A blue line is drawn on the Banbury sheet to indicate virtually certain plain text to the left thereof, as dummy messages always begin with plain (even if non-sensical) text for 30 to 60 letters before launching into a string of consonants.

All pairs of messages having their first two indicator letters the same are compared at all positions from -25 to +25. The counts are entered on one of 26 score sheets, namely the one lettered by the earlier of the third trigram letter. Thus the match WEE/WEP is entered on the E-sheet (Exhibit 1). WEE is 132 letters long, with the blue line drawn at 60, and a dummy percentage 65%. WEP has dummy percentage 5%, and (this being so low) has no blue line; its length is 104.

WEE ← - - 60 - → / ← - - - - - - 132 - - - - - - →

WEP ← - - - - 104 - - - - - →

## DIAGRAM OF DOLPHIN PROCEDURE



The upper line (opposite the letters WEE) gives the score at each position as WEP is moved to the right, the overlap decreasing from 59 to 35. The lower line (opposite WEP) gives the score at each position as WEE is moved to the right, the overlap remaining 60. The score is simply the number of coincidences, with a little x indicating a bigram. Thus in the position WEE = WEP + 8 there are 7 coincidences including a bigram, while at WEP = WEE + 24 there are no coincidences. If the dummy percentages are not too bad, scores are made beyond the blue line as well. For example, for RPO = RPE + 16, there are 2 coincidences in an overlap of 45 up to the blue line (on RPO), and 3 in the remaining 51 overlap.

The banbury counts are evaluated from one of three double-entry tables. In the row given by the number of coincidences and the column given by the overlap is found the value (expressed in half decibans) which is entered on the deciban sheet (Exhibit 2). In Table 1 this value is 20 times the log of the ratio of the a posteriori to the apriori odds that the line-up is correct. The values in Table 2 are reduced to allow of a small probability that one or both of the messages be dummy. Those in Table 3 are still further reduced to allow of a large such probability. Before entering the table, to the number of coincidences is added 1 for a bigram, 2 for a trigram, and 4 for a tetragram.

If scores are made only up to the blue line, Table 1 is used. If two scores are made, Table 1 is used for the overlap before the blue line and Table 3 for the overlap after it. If the dummy percentages are small on both messages, the blue line (if any) is ignored and the scores evaluated from Table 2. The table or tables to be used, namely 1, 2, or 1/3, are found entered on Exhibit 1. The values are also found entered there in comparisons of type 1/3, and these are added for entry on deciban sheet.

One sheet is made for each third indicator letter, and each pair is entered twice. Thus WEE/WEP is entered on both the E-sheet (Exhibit 2) and the P-sheet. On the E-sheet, the letter E is written down the center (0-column). In the x-column is entered the value of the score at which WEP = WEE + x (positive to the right, negative to the left). Thus the value contributed by this match to a spatial assumption E. . . . P (x = 5) or P. . . . . E (x = 7) is found by putting E under E and reading off the value above P. The values of the same match on the P-sheet are just the reversal of these, since + and - distance is reversed. Red scores are positive, black negative. Underlining means a trigram. A note is made of especially good line-ups, e,g. those with a repeated tetragram.