A Method for Breaking Into JNA-20 Traffic

C.H.O’D. Alexander

Editor's Preface

This document is one of seven papers in a series of documents written by the late Conel Hugh O'Donel Alexander while he worked as a cryptanalyst at Bletchley Park during the Second World War. The documents have been obtained from the US National Archives and permission has been obtained from the Controller of Her Majesty's Stationary Office to publish the papers on the editor's personal Web Page. The documents have been faithfully retyped by the editor with help from Ralph Erskine. The original documents were typed and had the style and layout of a typewritten document of that period. To make the re-edited presentation more pleasing the documents have been both left and right justified and a more modern type font has been used. Apart from these modifications to the layout the documents have the appearance of the original.

Where there are obvious typing errors these have been corrected in square brackets. In this particular text where the editor's copy is quite faint at places there are some numbers that can not be determined with certainty. These numbers have been marked in the text with an asterisk enclosed in square brackets, e.g. 60[*]. Further 'JNA 20' has been changed to JNA-20 throughout the text. Another modification is the adoption of the German spelling of the word Stecker with a capital, however, the constructed verb 'steckered' has been left in its original form. Tables 1, 2 and 3 are missing in the editor's copy.

The Editor,

Frode Weierud, © June 1998

Source:

Addendum to Captain Walter J. Fried's report No. 78 of 19 August 1944. National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 880, Nr. 2612.

COPYRIGHT

Crown copyright is reproduced with the permission of the Controller of Her Majesty's Stationery Office.

A Method for Breaking Into JNA-20 Traffic

1. This is a description of a method of breaking into JNA-20 when the indicators change i.e. a method of getting out a message with unknown sequence and set-up.

A. General Description of Method.

2. The method consists of:

(1) An application of the crash method to reduce the number of possible positions to something of the order of 1000

(2) A further reduction to 5 or 10 positions (or even less) by a frequency count of the bigrams in a ‘Yoxallismus’ (Erack) at each position.

3. ‘CRASH’ METHOD.

If O (possibly L might be tried as well – no other letters are sufficiently common in clear text) is steckered to J say, then at every machine position at which J encodes as J with no sequence, we shall have O encoding as O in this particular case. Suppose there are n O's in the message text, then if we compare the J crash tape (i.e. a tape showing at which machine positions J encodes as J) with a ‘message tape’ with J’s punched wherever O occurs, we shall have an average number of clicks of n/26 in a wrong position. Since we have 3 motions and 26 possible Steckers of O there are about 1,200,000 positions in all to examine and Table 1 shows the probability of picking up the right answer and the number of wrong stops to be tested for different numbers of O’s in a message.

4. YOXALLISMUS.

For any position obtained as in (3) which has to be further tested we know the assumed Stecker of O. If we list all the bigrams resulting from assuming every letter of the clear text to be O and comparing the result with the cipher text we get more squares with a large number of entries in the right case than in a wrong case, since in the right case one eighth of all the entries (those where there really is an O in the clear text) go into 26 of the 676 squares. Table 2 shows the distribution for messages of 676 and 900 letters in typical right and wrong cases and gives a scoring system for showing how good any particular position is. On 900 letters the test is sufficiently powerful to so eliminate all but a small number of positions; on 676 letters 10 or 20 per cent might require further testing but few of the messages will be as short as this.

B. Detailed Application of Method.

5. The best policy to pursue seems to be to be prepared to make a number of shots at the problem assuming each time that the right position is a very favourable one (i.e.

Crown Copyright

giving one's self a fairly small chance each time, but drastically restricting wrong stops). This enables us to use a much larger number of messages than would otherwise be possible. In September 1943 there were 28 suitable messages (working on O only). Accepting 150 stops per message one could get a 90% chance with a 44% chance in the first week, with 370 stops a message a 95% chance and 55% in the first week, with 800 stops a 99% chance and a 70% in the first week.

6. The best way of examining the 1,200,000 positions a message seems to be by the I.C. Plate Comparator. A typical group of comparisons would be an A crash tape with an A message tape, the latter consisting of A's punched in the positions where O occurs in the messages. The I.C. plate method would be to construct a message plate and a series of crash plates and run these against each other. At first sight there seems to be a serious practical difficulty in that our message may be over 1200 letters long and the present I.C. machine can only take a stretch 200 long (allowing for overlap). This can be got over as follows. Have the crash plate prepared as follows: if it has an A in position X, then record also a B in position 300 + X, C in position 600 + X, D in position 900 + X. Now to prepare the A message plate record an A in position Y (O<Y≤300) if there is an O in position Y, record a B in position Y if there is an O at position 300 + Y, a C in position Y if there is an O in position 600 + Y and D if there is O at 900 + Y. In this way the O's in the message are recorded in a stretch of 300 length and when this stretch is compared with the crash plate we get all the coincidences that occur in the full stretch of 1200 and we get no others. (Note: there is no difficulty about recording several different letters at the same position as will happen e.g. if we have A's at position 112, 412, 1012). A rate of comparison of 15 positions a second will enable us to get through the 1,200,000 positions in a day. Actual running time is small and the chief time taken is in changing plates and recording stops. Using two I.C. plate machines however it seems as if one should be able to manage this average speed (which is 20 seconds per plate of [or] 40 seconds per plate with the two machines). Altogether it looks as if provided that the crash plates are prepared between now and September (see Para 9) that the whole of this stage would not take more than a day per attempt and there will probably not be more than an average of one suitable example a day on the letter O.

7. Having got our stops these have got to be further tested and for this purpose 'Mike' (cf. N.L.R. #7, para. 1. JNS.) seems to be ideal. Suppose we have prepared in advance encode tapes for every letter at all machine positions. Then given a stop on O/J, say, run the message tape against the J tape (the latter starting at the position given by the stop) and record the bigrams on the digraph counter board. If possible it would be convenient (though not at all essential) for a light or some other indication to show which totals were (say) 7 or more. The number of scores of 7 or better would be taken down and the great majority of positions would obviously be no good and could be rejected without further examination, see Table 2. The few positions which were not obviously hopeless could be more carefully examined by hand. Mike does about 450 bigrams a minute so it would take 2 minutes to record all bigrams and allowing another 8 minutes for setting up and looking at answers etc., we still get a time of 10 minutes per position or 144 a day; as can be seen from Para 5 much better results can be obtained if we can deal with more than

this but 144 would be enough to make the method practicable; for detailed figures on this see Table 3.

8. If the September 1943 figures are a reliable guide, then, it appears that with Mike and two I.C. plate machines used without any modifications, one should have about an even chance of a break in the first week of the new period, taking a fairly conservative rate of working and a 90% chance in the first month.

C. Preparatory Work Needed.

9. (1) 78 sets (3 motions, A to Z for each motion) of crash plates (about 60[*] plates in a set) each corresponding to the crashes in a particular letter for a particular motion. A typical crash plate (say the J plate) will have, corresponding to a J crash in position X, and A in position X, B in position X - 300, C in position X - 600, D in position X - 900. Since each crash plate only uses four rows of the plate, there is no reason why, if it is any convenience, 8 sets should not be put on the same series of crash plates - A crash on A to D, B crash on E to H etc. The only objection to this would be if the I.C. Plate machine was not sufficiently sensitive to distinguish between 6 and 7 points of light, say, in which case one might have to repeat the holes several times on the same plate so as to give, say, 48 and 56 points of light instead of 6 and 7. Preliminary investigations however seem to indicate that this would not be necessary. In any case I feel that this is a matter on which the Americans might well know best through greater experience of handling equipment of this type.

> (2) 78 sets of encode tapes for doing the Yoxallismus on Mike. It would also be worth while having some sets of decode tapes for frequency dotteries on assumed Steckers when testing stories further. Here also I think the Americans would have the best idea of what to do.
>
> (3) It might be worth while (though I rather doubt it) having I.C. Plates one foot instead of six inches long, thus giving 3 times as great a length of comparison per plate (900 instead of 300). This would also need only a third of the number of plates in a set. (It is also possible that Hypo might be used instead of I.C.).

The preparatory work to be done, assuming we wish to be ready by Sept 1st, amounts to making one set of crash plates and one encode and one encode tape a day from now on.

C. H. O'D. A.

Crown Copyright

Editor’s Notes

1. The document is not dated but it is known to have been prepared some time before 19 August 1944. There are also some indications that this is not the latest version of the document.
2. JNA-20 is the designator for the traffic generated by Coral, the cipher machine used by the Japanese Naval Attachés. The machine is made out of 3 banks of 26 position telephone selectors which move with cyclometric stepping. The machine is equipped with plugboards at each end and was apparently used with the same sequence at both ends. Only three of the six possible “wheel” orders were used. The machine is cryptographically stronger than Purple but the use of the machine was relatively weak. For more details on Coral and Purple see Cipher A. Deavours and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis*; Norwood MA: Artech House, 1985.
3. The I.C. Plate machine, belonging to the RAM (Rapid Analytical Machinery) family, was performing optical I.C. (Index of Coincidence) measurements on two specially prepared photographic plates. A later model was the I.C. Film Projector or HYPO which used two photographic films instead of plates and which was more automated than the I.C. Plate machine.
4. Mike was a cryptanalytical aid made by the National Cash Register Company (NCR). It was used to count digraphs and consisted of a great number of electromechanical counters which are said to have filled a whole wall. For further details about Mike and the RAM see Colin Burke, *Information and Secrecy: Vannevar Bush, Ultra and the Other Memex*; Metuchen, N.J. & London: The Scarecrow Press Inc., 1994.
5. Dottery was a hand method for determining the Stecker plugging when wheel order, Ringstellung and message key had been determined. The name is derived from the dots that were used as tallies next to each letter on a frequency counting sheet.
6. Yoxallismus, named after its inventor Leslie Yoxall, is a similar process to the Dottery based on a statistical approach to find the Stecker connections. The method assumes that every letter of a message is the most frequent letter in the alphabet, E. In the case of Japanese this would be the letter O.