Hand Duenna

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 a few cases a superfluous letter(s) has been removed by putting the letter(s) in square brackets preceded by a slash, e.g. [/s]. This particular text is an exceptionally good copy and there are no doubtful passages. Paragraph 9 has been physically reorganised into separate subparagraphs while in the original text the labelled sections (A), (B) and (C) were all run together. The editor feels the present layout gives added clarity to the text. A further 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. Diagrams 1 and 2 are missing in the editor's copy.

The Editor,

Frode Weierud, © June 1998

Source:

Addendum to Captain Walter J. Fried's report No. 62 of 13 July 1944. National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 880, Nr. 2612.

COPYRIGHT

Hand Duenna

A. Introduction.

1. 'Hand Duenna' is a method of breaking a key on a 100 letter crib if the Umkehrwalze is unknown. It uses the same basic method as the machine Duenna now being made at OP 20 G, and is intended as a stop-gap method for use should Uncle D be generally introduced before a sufficient number of Duennas are available.

B. Theory.

2. We will assume that our 100 letter crib has no [S].W.T.O. Imagine that we have found the correct positions of the two right hand wheels. Then we find the Stecker and Umkehrwalze connections as follows:

3. Suppose we have 4 EN pairings in the text, 3 EU's, 2 ES's and 1 NS, 2 EJ's, 2 EQ's, 1 EL and 1 NL, 2 NZ's. Make the Stecker assumptions Ea Nb (we shall use non reciprocal-generalized-stecker for reasons that appear later.) Then for each of the 4 EN pairings we get a pairing through the fixed portion of the machine i.e. the left hand wheel and the Umkehrwalze. (See Diagram 1, in which the pairing is JX). This fixed portion will be referred to as the "reflector" in the rest of this paper.

Suppose these four pairings are JX, LY, AN, BR. Now suppose that for an EJ pairing, say, when we assume E steckered to a, we come through the two right hand wheels to the point N. N has been found to be paired with A through the reflector, so if we work back from A through the 2 right hand wheels and come out at the point S, say, then J must be steckered to S. (Diagram 2). Now that we know the Stecker of J we can use the second EJ pairing to obtain another reflector pairing, say ZT. We continue this process until we reach a contradiction (e.g. had we got ZX instead of ZT this would have failed the position as we already have JX). If no contradiction is reached then we can use the new Steckers we have obtained to fail the position by further testing – if necessary using a stretch outside our menu – on exactly the same lines as those given in Joan Ambler's report on testing Giant stops. There may be a small proportion of positions giving no consequences which it will not be possible to test further without a subsidiary Stecker assumption. Unless these are particularly promising (e.g. having 2 or more confirmations) they will have to be abandoned. The right position will normally show up just as it does on a bombe stop i.e. by confirmations and by absence of contradictions. When the right position has been found the left hand wheel and the true UKW connections can be found just as they are on RED at present when Uncle D is used.

4. This shows how we determine the true Stecker and reflector pairings when we have got the right wheel position. The number of machine positions to be examined is 20 (no. of W.O's) × 26 (possible relative positions of 2 right hand wheels) = 520. We only need

to consider the 26 relative positions of the two right hand wheels (instead of 676 positions) for just the same reason as we only need to consider one position of the right hand wheel when doing the ordinary Stecker knock out with generalized Stecker. If the true position of the 2 right hand wheels is 'XJ' with Stecker E/K, N/R and reflector pairing from this MP, then if we set up right hand wheels at 'OA' we shall get a bogus answer without contradictions. This will be Et, Na reflector pairing VY, since the effect of setting up OA instead of at XJ is to rotate the whole right hand position of the machine 9 places. Therefore we get the true answer with 9 added on to each Stecker and 9 to each reflector pairing.

C. Practice.

5. The crib will have to be menued for R.H.W. turnover just as for an ordinary bombe job. On a fairly favourable 100 letter crib three menus will probably be necessary. For the 20 × 26 positions to be examined on each menu, Mr. Freeborn will send up 20 sets of 26 sheets. Each set corresponds to a wheel order and each sheet within a set to one of the 26 possible relative positions of the two right hand wheels. These 520 sheets therefore are 520 independent units which have to be separately examined and failed.

6. Each sheet has an alphabet A to Z at the top and a series of machine positions written down the side with a scrambled alphabet opposite them.

```
e.g.          A B C D   E F G H   I J K L   ....

     (  LY    R T Q U   F N A E   L V W X   ....
EN   (  MA    S J N U   R X D B   E A W M   ....
     (  NV    N A X R   S Q L V   Y T J Q   ....
     (  MQ    A V S D   E L R J   M F Q C   ....

     (  KJ    R S K A   B G E O   Q J Y V   ....
EU   (  NY    M B E F   U C V W   A N S L   ....
     (  MR    L V K N   G H Z Y   X J T B   ....
```

This tells us that if the two right hand wheels are set up at LY, current put in at A comes through to R, at B comes out at T, C gives Q … and so on. If our 'menu' consisted of 4 EN's, 3 ER's [EU's], 2 ES and 1 NS, 2 EJ, 2 EQ, 1 EL and 1 NL, 2NZ then there would be 4 alphabets in a group (as LY, MA, NV, MQ above) then a gap then 3 more, a gap, 3 more (ES and NS), a gap, 2 more (EJ) and so on.

7. Suppose now we make the assumption Ea Nb. Then for the EN pairings we must discover where current going in at A and B emerges. Looking opposite LY, MA, NV, MQ we get the reflector pairings RT, SJ, NA, AV giving a contradiction – so Ea, Nb is impossible. Suppose we take Ea Nh: we get reflector pairings RE, SB, NV, AJ. This has no contradiction so we try to get further pairings. Look down the A column wherever we have E paired with anything (the H column if it is an N pairing) for one of the letters R,E,S,B,N,V,A or J. Opposite KJ (corresponding to an EU pairing) we see 'R' in the A column, therefore EA takes us through to R at this position. We know R is paired to E,

therefore the U Stecker must take us through to E: but in my example 'E' occurs in column G, therefore we have Stecker Ug, therefore from the other EU pairings we get reflector pairings MV, LZ giving a contradiction with LV. Notice (1) this can be done quite mechanically since all that is necessary having found RE in the EU set is to write down the pairings immediately underneath it: but (2) if one of the pairings had been an NU we should have had to have taken a letter from Col. H (corresponding to Nh) instead of Col. A e.g. had KJ, NY been EU pairings and MR an NU pairing we should have had reflector pairings RE, MV, YZ instead of RE, MV, LZ. Finally, suppose we had taken Ea Ng. This would have given RA, SD, NL, AR – a confirmation. Going to the EU pairings we get RA, MF, IN a second confirmation and if there were no further consequences or contradictions this would be tested on the hand machine by the Giant technique, Steckers Ea, Ng, Ud being known.

8. Without modification, however, this method is too slow. There are 520 sheets per menu each having 26×25 = 650 results to examine and it is not feasible to examine all these. We are therefore obliged to confine ourselves to particularly favourable positions i.e. those giving confirmations each of which has 26 times the normal chance of being right. The effect of this in a typical case is to give 30 to 40 per cent of the chance of the complete method in one tenth to one twentieth of the time.

9. There are various types of confirmations.

(A) On the four basic EN pairings.

(1) The 'beetle' type shown in columns D and K in my example which gives the pairings UW, UW, RJ, DQ. This must be failed two ways round i.e. as Ed, Nk and as Ek, Nd. Also (provided there are no other repeated letters between rows 1 and 2) when these have been failed the four Steckers Ed, Ek, Nd, Nk have been completely failed because Ed implies Nk etc.

(2) The 'starfish' type shown in columns A and G giving RA, SD, IN, AR. This also must be taken as Ea Ng and as Eg Na. When this has been failed Ea, Eg, Na, Ng have not been independently failed as Ea does not imply Ng. Nevertheless the individual shot Ea Ng has as good a chance as Ed Nk each being 26 times as good as the average position.

(B) On subsidiary E or N pairings.

(3) The beetle type. In the EU pairings we see that Ec implies Uj, giving the pairings KJ, EN. Looking at col. C in the EN pairing we see an 'N' and therefore since we must have EN reflector pairing, Ni is also implied. So testing Ec, Ni deals with Ec completely. Also of course KJ, EN might give further reflector pairings from other E pairings: here we are handicapped by having only two basic pairings and not being able to use pairings involving 'N'. Should we get stuck in a case like this it is not worth while considering all values of N in turn, since we are getting no better return from our money than we are from E and N Stecker assumptions with no confirmation – it is merely slightly quicker to fail them as we

have two extra reflector pairings thrown in, but any individual assumption of Stecker for N has no better chance than if there were no confirmation on U.

(4) Starfish type. More or less the same applies. Suppose Ec Uj had given pairings KJ, EN, JK. Then starting from Ec Ni which gives QL, NE, XY, SM we have Uj implied (from EN) and then get a confirmation KJ, JK, therefore Ec Ni is 26 times as likely as the average pair of E, N Stecker, although it is not true that Ec implies Ni, since it does not imply Uj. Owing to the time taken in finding starfish it is a bit doubtful whether these positions are worth failing (as even when found one is quite likely to get stuck). This is a matter for further experiment.

(C) A further type of confirmation has occurred to me while writing this and would also probably be worth looking for. The A column contains an R in the EN section and an R in the EU section. This means that any assumption of Stecker for E and N implies a Stecker U and two more reflector pairings e.g. NL gives RE, SB, NV, AJ which implies Ug and Mv, LZ. We can quickly look for possible confirmations as follows. The first 4 pairings are going to be R,S,N,A with other letters and the second lot R,M,L with other letters, therefore confirmations will arise, if at all, from pairings SM, SL, NM, NL, AM, AL (confirmations on R will be found separately as starfish in (A) or (B). We can deal very quickly with these as follows. SM in row 2 gives RX, and MS in second EU row gives RY[,] failing[/s] the position: if we get a confirmation we again have a position 26 times as good as the random position. It is a matter for experience to see how far it pays to go for these.

10. To find confirmations of the beetly [beetle ?] type is very simple. We look for repeated letters in the same column. Two repeats between the same pair of rows give[/s] a confirmation. Starfish confirmations are more troublesome to find. The best method so far discovered is the simple one of examining each pairing between the two alphabets in question and seeing whether it repeats. To avoid doubling one's work only consider pairings in which the earlier letter in the alphabet comes in the higher row. E.g. taking row 1 and 4 omit pairing one (R is later than A) pairing 2 TV does not repeat because we have VJ in col. 10: when we get to col. 7 AR we pick up a confirmation on RA in col. 1.

D. Further points for consideration.

11. Some points worth further thought by anyone interested are

(1) Is there a better way of finding confirmations? The actual finding of the starfish takes a larger portion of the total time.

(2) Are there any other worth while types of confirmation?

(3) Is it worth listing single pairings i.e. pairings of E or N with letters which are not repeated.[?] These cannot give new reflector pairings but can give further Stecker which will facilitate subsequent testing.

(4) Is it worth listing basic pairings not in the menu, i.e. pairings which must be given two possible settings to allow for turnover.[?]

E. Effectiveness of method.

12. Excluding Type C confirmations we can get about a 1/3rd chance of success with 500 girls hours[.] [W]working 10 girls a shift for 4 days should cover this as they give 960 hours theoretically. Type C confirmations may put this up to as much as half chance with a corresponding increase in time: I am not sure. If so it would be well worth while since 1/3rd chance means on average 2½ cribs tested per success, while a 1/2 chance means 1½ cribs tested.

C. H. O'D. A.

11th July, 1944

Distribution:

A.D.(Mch)
Mr. Milner-Barry
Mr. Wallace
Mr. Fletcher
Miss McLaren
Mr. Lawn
Miss Ambler
Major Babbage
Captain Fried (2)
Lt. Eachus (2)
Major Manisty
Mr. Alexander (2)
Miss Wilson

Editor's Notes

1. Hand Duenna is a powerful method to solve for the Umkehrwalze D wiring by making Stecker assumptions and selecting the 30 or so best constatations from a very long crib of 100 to 150 letters. The Umkehrwalze D (pluggable reflector) was introduced on the German Air Force nets in January 1944.
2. Details about beetle and starfish are to be found in C.H.O'D Alexander's paper "Stecker Knock-Out" from which I have taken the following extract:

   A beetle is a repeated letter on a rod e.g. …ADOQA… and a two-rod starfish is a repeated pairing between two rods with the letters interchanged e.g.

   …FLQRGYC…
   GNMPFTA

   Both beetles and starfish are generalized properties of the rods and hence are basic properties of the different wheel wirings. For an explanation of rods and rod squares see the article by David H. Hamer, Geoff Sullivan and Frode Weierud, "Enigma Variations: An Extended Family of Machines," *Cryptologia*, 22(3), July 1998.
3. W.O. = Wheel Order. The order of the three moving wheels in the machine.
4. T.O. = Turn Over. The turnover of a wheel governed by its right-hand neighbouring wheel.
5. S.W.T.O. = Slow Wheel Turn Over.
6. R.H.W. = Right Hand Wheel.
7. Uncle D is a BP euphemism for Umkehrwalze D. A general abbreviation for Umkehrwalze is UKW.
8. RED was the BP name for the main operational key of the German Air Force (Luftwaffe).