Stecker Knock-Out

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]. In this particular text complete words have been added in square brackets to enhance the flow of the text. There is one exception to this rule and that concerns the German word ‘stecker’. The editor has decided to adopt the German spelling of the word ‘Stecker’ with a capital, however, the constructed verb ‘steckered’ has been left in its original form.

The Editor,

Frode Weierud, © July 1998

Source:

Addendum to Captain Walter J. Fried’s report No. 8 of 23 March 1944. National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 880, Nr. 2612.

COPYRIGHT

Stecker Knock-Out

1. Methods of Attack

There are two methods of attack on a Stecker knock-out job. (1) By generalized Stecker in which the diagonal property of the rod square is used to enable the work to be done by testing only one position instead of 26. In this case the Stecker is non-reciprocal and the assumption A in the message steckered to B on the rods must be distinguished from B in the message steckered to A on the rods: the usual notation is to write A/b and B/a in the two cases. Given a set of generalized Stecker say A/b, B/d, C/z, D/a, E/x, F/e, G/y, H/c there are 26 possible sets of true Stecker got by adding 0–25 in turn to the small letters; the true position, if there is one, usually shows up very clearly on confirmations and self Stecker e.g. in this case add 3 to each of the small letters and we get A/E, B/G, C/C, D/D, E/A, F/H, G/B, H/F which is obviously right and the correct rod position is three back from the one which gave the generalized Stecker. (2) By non-generalized Stecker in which each rod position is tried in turn and the Stecker used (being true Stecker) are reciprocal.

2. Relative Merits of Gen & Non-Gen.

Which method is preferable depends on the data available. Suppose that on a particular hypothesis the Stecker of E implied the Stecker of N and of I: in this case you could normally put down a particular generalized Stecker assumption say E/a, N/g, I/k pretty nearly as easily as the non-generalized Stecker assumption E/A, N/G, I/K since E, N, I occur so frequently that they will give further consequences without difficulty (note, incidentally, that only results for the form E/<u>a</u>, G/<u>a</u> constitute a contradiction on generalized Stecker) and as your generalized assumption covers 26 reciprocal Stecker assumptions it must pay to do it. On the other hand suppose E is not connected with any other letter: then the assumption E/a gets you nowhere as a rule and you would have to make the 26 subsidiary assumptions for (say) N and even then you would quite often get stuck. In the non-generalized case E/A gives you two letters and you may well be able to fail it without further assumption. In the generalized case you have 26 assumptions in one position for one E Stecker each giving you the generalized Stecker for the two best letters E, N: in the non-generalized case you have one assumption in 26 different positions (E/A in pos: 1, E/B in pos: 2 etc. … corresponding to E/a generalized) each giving you the reciprocal Stecker for two letters one of which may be unfavourable. In favour of the respective methods are (1) for Generalized: you always have the Steckers of the two most favourable letters (2) for Non-Generalized: (a) as soon as you get a consequence you have the Steckers of 2 more letters so that you are less likely to get stuck subsequently (b) owing to reciprocal confirmations and self-steckers the right position shows up much sooner if you reach it and therefore it is less likely to be missed through error, boredom or corruption. On the whole I think non-generalized is superior in this case, provided it can be done without scritching and that there is no good chain available for use with the generalized E Stecker (see C below).

3. General Policy

There are some hypotheses which offer a very much better return for money than others owing to only taking a tenth or a twentieth of the time to put down while giving an equal amount of information. For this reason it is very uneconomical to plough systematically through all possible Steckers of E, say, in all possible rod positions. All the more troublesome positions should be left until last and should be abandoned altogether if there is another re-encodement available to work on. Broadly speaking I think the programme should be (1) Prepare all suitable charts (2) Fail all the more favourable hypotheses that can be done by generalized Stecker (3) Fail all the more favourable hypotheses that can be done by non-generalized Stecker.

4. Beetles and Starfish

A beetle is a repeated letter on a rod e.g. $\cdots\underline{A}DOQ\underline{A}\cdots$ and a two-rod starfish is a repeated pairing between two rods with the letters interchanged e.g. $\cdots\begin{smallmatrix}F&L&Q&R&G&Y&C\\ \underline{G}&N&M&P&\underline{F}&T&A\end{smallmatrix}\cdots$ Both beetles and starfish are generalized properties of the rods (i.e. if there is a beetle at distance 6 on one rod so there is on all the other rods, running down the diagonal) and are of great use (particularly beetles) in doing Stecker knock-out. The number of beetles varies greatly per wheel (12, 7, 8, 3, 2, on wheels I to V – a deliberate attempt to avoid them must have been made on wheels IV, V) and for this reason wheels I and III are always easier to work on than wheels IV, V.

The fact about a beetle that makes it useful is this: suppose in the message we have $\begin{smallmatrix}L&R&Q&J&T&N\\ E&I&N&S&S&E\end{smallmatrix}$ and that there is a beetle at distance 5 on the rods. Then if we make a Stecker assumption which means that the E's go with beetle, it follows that the Steckers of L and N imply each other as they must come on the same rod.

```
e.g.   Message    (L R Q J T N
                  (E I N S S E

       Rod        (A F Y T N A   E/A means that Stecker of L
         pairing  (X T Q V P Y   implies the Stecker of N, e.g.
                                 if L/X then N/Y.
```

The two-rod starfish give not a definite implication but a favourable combination of Steckers when there is a female in the message.

```
e.g.   Message    (V T Q P J V
                  (E I N S S E

       Rods       (X L Y T R N
                  (N J U P V X
```

E/X does not imply V/N but if we assume E/X, V/N (or E/N, V/X) and lay the rods for the first EV pairing we get a confirmation on the 2nd EV pairings.

5. Charts

Most if not all charts are connected with beetles and starfish. The following are a list of charts which it seems to be well worth having: quite likely there are others also worthwhile.

A. Permanent Beetle and Starfish Charts.

This chart would show what beetle and starfish exist on each wheel

e.g. Beetle	WHEEL	LETTER	DISTANCE	Rod on which Beetle begins in Position I
	I	Y	2	C

This says that on wheel I there is a beetle at distance 2, that on the C rod this beetle occurs between the 1st and 3rd letter and that the repeated letter is Y. (From this of course it follows that on the B rod, there is a beetle between the 2nd and 4th letters, the letter being X etc. etc.) This, I think, is the only permanent chart that is essential. The remaining charts are concerned with the particular message being worked on and one will be needed for each wheel.

B. Impossible and Consequential Beetles and Starfish.

This chart would show consequences arising from assuming generalized Stecker which gave rise to beetles and starfish in the message at positions at which there was a female. An actual example should make this clear.

Suppose that we have a female $\genfrac{}{}{0pt}{}{N}{E}\cdots\cdots\genfrac{}{}{0pt}{}{N}{E}$ in the message in positions 18 and 25. On I rods there is a beetle at distance 7 and this appears as T·········T in positions 18 – 25 on W rod; therefore, if we are doing generalized Stecker and laying the rods with rod position 1 under message position 1 (we only have to lay the rods in one position for generalized Stecker and this is the natural one to choose) the assumption E/t implies the two E's on the same rod and therefore the two N's on same rod. There is not, however, a second beetle and therefore this is impossible, so we enter in square ET "18/25 X" meaning generalized assumption E/t— a T.O. between 18 and 25. Had there been a second beetle, say J······J in positions 18······25 we should have entered "18/25 N/j" in the ET square, "18/25 N/t" in the EJ square, "18/25 E/j" in NT and "18/25 E/t" in NJ since E/t······N/j provided there is no T.O. in 18/25. In the same way starfish are listed. Suppose that we had a two-rod starfish $\genfrac{}{}{0pt}{}{A}{B}\cdots\cdots\genfrac{}{}{0pt}{}{B}{A}$ in positions 18, 25. Then the generalized Stecker assumption E/a and N/b gets a confirmation and we should enter "18/25 N/b s" in "EA" square and "N/a s" in "EB" square etc.

To prepare this chart it is simply necessary to discover (by [F]oss sheeting pairings) all females in the message and hence what beetles and two rod starfish are possible.

C. Chains on E beetles.

Whenever we have $\genfrac{}{}{0pt}{}{A}{E}\cdots\genfrac{}{}{0pt}{}{B}{E}$, then if E has generalized Stecker K say which gives a beetle the Stecker of A implies the Stecker of B. Supposing $\genfrac{}{}{0pt}{}{E}{A}$ to be in line 4 pos: 11, $\genfrac{}{}{0pt}{}{E}{B}$ in line 4 pos: 17 we should enter "B 11/17 4" in square KA and "A 11/17 4" in square KB meaning that, provided no T.O. in 11/17, then, if E/R the Stecker of A implies Stecker of B. Suppose now that we have in K line (i.e. corresponding to E/k generalized Stecker) entry A 11/17 4 and also N 13/22 7 in square KB: this means that if E/k then Steckers of A, B and N are connected so that if we assume a Stecker for one the Stecker for the other two follow and this gives us a powerful method for attacking the assumption E/k by means of 25 subsidiary assumptions each of which gives 4 generalized Stecker (those of E, A, B, N).

D. Chains on other beetles.

As other beetles are less frequent than E beetles there will be fewer entries here and they could all be got on one chart. I would suggest construction on [the] following plan. Wheel I will be taken as example.

There is a beetle at distance 2 on Wheel I, and it occurs in 1st and 3rd positions on rod C as Y.Y (therefore as X.X. in 2nd and 4th positions on rod B etc.) Run down columns 1 and 3 of the message for constatations involving a repeated letter: suppose we get $\genfrac{}{}{0pt}{}{V}{N}\cdots\genfrac{}{}{0pt}{}{N}{M}$ in line 4 – then enter in square NY the entry 4VM 1/3, meaning that if generalized Stecker N/y then Stecker of V implies Stecker of M provided no T.O. 1/3 and pairings are to be found line 4 and associated Stecker on 1st and 3rd columns of rod square. Then go to columns 2 and 4: suppose repeat $\genfrac{}{}{0pt}{}{L}{K}\cdots\genfrac{}{}{0pt}{}{K}{Q}$– then enter LQ etc. in square K$\underline{X}$ since if beetle is Y.Y in rod positions 1, 3 it will be X. X in positions 2, 4. Go through all columns at distance 2: this completes entries for beetle at distance 2 – then go on to beetle at distance 3 etc. etc.

This chart should help considerably in downing stories on chains (section C above). Suppose we have E/k, A/l, B/t, N/r: then if any squares AL, BT, NR contains an entry connecting E, A, B, or N with any other letter we get a further consequence immediately.

E. E Consequences giving impossible beetles.

Suppose $\genfrac{}{}{0pt}{}{A}{C}\cdots\genfrac{}{}{0pt}{}{E}{C}$ are pairings 4 apart. For wheel I there is no beetle at distance 4. Therefore it is impossible for the Steckers of the 2 C's to be on the same rod; therefore the Steckers of A and E cannot be on the same rod; therefore for each generalized Stecker of E there is one impossible Stecker of A. These impossible Steckers corresponding to various E Steckers can be very easily listed by running down the appropriate columns on the rod square. The chart when made then shows a set of immediate contradictions which should enable a number of stories (particularly when scritching a chain associated with an E Stecker) to be put down quickly.

F. E Consequences for non-generalized Stecker assumptions.

Suppose we have a pairing $\overset{E}{K}$ in the text followed 4 places later by another E (a similar argument holds if the letter is a K, the other letter of $\overset{E}{K}$ pairing) then the Stecker assumption (non-generalized) of $\overset{E}{K}$ will give an immediate consequence if rod with E on it in position corresponding to the $\overset{E}{K}$ pairing has K on it 4 places later: for then we have this position

Message	(E ··· L)	
	(K ··· E)	
	)	It is clear that the Stecker
Rods	(E ··· K)	L/Q is implied
	(K ··· Q)	

In order for the assumption E/K to produce a direct consequence, therefore, it is necessary for a rod to exist with K···E on it and for this to happen there must be two letters 4 apart on the rods and 20 apart in letter value (E - K = 20). If we have listed the difference in letter values for various rod distances (which is a permanent chart for the wheel) then the Steckers of E which do produce consequences in appropriate rod positions can quickly be listed – entries would take [the] form 2 L 4/7 in square S 14 (numbering 1 – 26 across top of chart) implying that if E/S in rod position 14 then Stecker of L followed provided no T.O. in 4/7 by laying rods for line 2.

The method of construction of this chart is a bit troublesome to get hold of at first but once a few entries have been made it becomes very quick and easy to do. (Probably about a shift for complete chart).

6. Programme

This has been discussed elsewhere and the following are remarks about various methods of attack to give some idea of the relative returns for money offered by various procedures.

A. Generalized Stecker.

1) Beetles, 2-rod Starfish and E-chains with closures are worth putting down whenever possible. Each has 1/130th chance n.a.f. turnover and as there are about 100 beetles or starfish each of which can be taken in two ways (i.e. A/x, B/y or A/y, B/x) the total chance on these alone is of the order of 50%.

2) Good open chains on E-Steckers. With the aid of charts C,D,E above it should be possible to put these down fairly quickly. A 3 chain associated with a given E Stecker would nearly always give enough consequences to fail it: the main question is how long it takes to reach a contradiction. Charts D and E should be very useful here: "D" will give a number of jumping-off points and help to avoid unnecessary laying of rods and "E"

should put out 10 or 20 per cent of the positions at a fairly early stage. It may well be that it is quite feasible to scritch two chains if they involve favourable (i.e. common) letters: should this be so then a very large proportion of the E Steckers can be put down generalized.

If results of scritching are favourable and compare well with work on non-reciprocal Stecker it might be worth while scritching for three beetles and starfish which it has not been possible to fail in (1).

B. Non-Generalized Stecker.

I should think that it would be better not to do any systematic work on non-generalized Stecker until everything worthwhile has been done on the generalized, since generalized results automatically cover a number of non-generalized results while the converse is not true; therefore by doing non-generalized first, duplication work is risked unnecessarily.

3) Beetles and Starfish with confirmations. Suppose there has been a beetle position A/k, B/j which it has not been possible to fail generalized. Then in rod position 10 this gives A/B, B/A i.e. the Stecker A/B in rod position 10 is confirmed: this is therefore worth failing if it can be done without scritching.

4) E-Steckers that don't involve scritching. Chart F will show these up and they are most worth doing of any non-generalized Steckers since (a) they will be easiest to put down, being Steckers of E (b) they are part of a systematic E programme and therefore have a better cumulative chance.

5) Other Steckers that don't involve scritching. These can be obtained in a variety of different ways, assuming (as will normally be the case) that when we have 2 non-generalized Stecker we shall get a consequence. Some of the ways of getting such Stecker are (a) Aitken's method of getting two self-stecker or cross steckered pairs on the same pair of rods (b) examining beetles and starfish non-generalized (c) preparing charts similar to F for other common letters besides E and testing positions with consequences (d) taking positions of chains associated with E (or other) Stecker that have a confirmation, e.g., suppose E/k implies a N–L chain and that one position of the N – L chain gives N/a L/c then for rod position 16 we have E/V and the N–L chain has position N/L with confirmation.

Not allowing for any cumulative effect (such as you get from examining a series of E Steckers) every individual shot in (4) or (5) has exactly the same chance. In choosing between them the following seem to be points to be borne in mind (1) Are they part of a general plan i.e. is there any appreciable cumulative effect (2) How easy are they to obtain (3) How easy are they to put down? (1) favours the doing of E Steckers and to a very much smaller extent a subsequent attack on Steckers of other common letters. (2) is uncertain since different types of labour are needed in different methods: in any case it is not a major point because the time involved is small in comparison with the time of failing results. (3) favours the Steckers of common letters but is not a major point because if a position produces no consequence one can abandon it without much harm being done.

Another point in favour of E Steckers is that one might be able to use the generalized charts to help in the non-generalized case.

On the whole my own inclination would be to do the maximum possible on E in (4) and (5) (d) and after that I can see little to choose between (5) (a), (b) & (c).

American Method of Rodding

The Americans at OP-20-G have a method of using inverse rods instead of direct rods for the failing of individual positions which they say saves a considerable amount of time. They use it when the T.O. is known – or at any rate a sufficient stretch known to be without T.O. exists on an equidistance. To make the explanation clearer [/and/] [I] will assume first known T.O. occurring at the beginning of each alphabet. Their procedure is as follows.

First they punch up the pairings on a mask (as for an ordinary rod crib) using a separate mask for each alphabet – so that one would have 9 masks for the Greenshank R.E. Suppose the generalized Stecker assumptions A/x, B/t are being made. They have a flat open box lettered A to Z down the side to hold the inverse rods and they now insert the x rod in the A row and the t rod in the B row. Now suppose the first alphabet has a pairing $\genfrac{}{}{0pt}{}{A}{B}$ in it and later on A’s and B’s paired with different letters. Then if we lay the mask for the first alphabet on the inverse rod box we shall get a rod pairing, say $\genfrac{}{}{0pt}{}{l}{m}$, showing up for $\genfrac{}{}{0pt}{}{A}{B}$ and isolated rods showing up through the holes in the mask for the other A’s and B’s. Suppose a second l shows up then since we know $\genfrac{}{}{0pt}{}{l}{m}$ is the correct pairing this implies a further Stecker i.e. we must now put in the box in the correct position the rod which will give us a second $\genfrac{}{}{0pt}{}{l}{m}$ pairing. We lay each of the masks in turn continuing to get a fresh Stecker until we reach a contradiction. (If reciprocal Stecker are being used we can lay two rods instead of one each time).

The advantage of this method is that all one’s information is available all the time. Suppose we have A/x, B/t, J/k, L/m, N/a. Then with our present method we can only lay one pair of rods at a time and may lay many useless pairs before we get one giving a consequence. With the American system however, laying the alphabet mask produces all consequences from all rod-pairings immediately. They say they take less than half the time by this method than they do by the other and I certainly think it would save that amount of time and be much less tiring.

With no turnover information, the only modification necessary is to have the box double width and the inverse rods double length and then to punch up a double alphabet on each mask i.e. pairings from alphabets 1 and 2 on mask 1, from alphabet 2 and 3 on mask 2 and so on.

I would strongly recommend that rods and boxes be made to use this method. They will represent a permanent asset and will be extremely useful if we ever have to do Stecker knock-outs in the future quite apart from the present emergency. It is essential that the boxes should be really well made and that the rods should fit into them easily and firmly and a detailed explanation of the method of use and need for convenience and accuracy given to whoever has to make them. Probably it [would] be worthwhile having special paper as well and some form of holder for the various masks which would fit onto the boxes. The rods should be strongly made and not liable to warp.

C. H. O’D. A.

Editor's Notes

1. The document is not dated but it is known to have been written in the end of February or beginning of March 1944. The "Report on the S.K.O. Experiment" which is dated 4 March 1944 refers to Mr. Alexander's paper on S.K.O. The Stecker Knock-Out procedure is a hand method to allow for Stecker and Umkehrwalze D wiring to be solved simultaneously. The Umkehrwalze D (pluggable reflector) was introduced on the German Air Force nets in January 1944. In the beginning of March 1944 a worrying message was intercepted. It concerned the possibility of extending the use of Umkehrwalze D to much larger part of the German Air Force networks.
2. 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, pp. 211-229.
3. T.O. = Turn Over. The turnover of a wheel governed by its right-hand neighbouring wheel.
4. R.E. = Re-encodement, a given message enciphered again on a different key or in a different system.
5. n.a.f. = The Editor supposes this stands for "not accounting for".
6. Foss sheet was a form consisting of a 26 by 26 matrix with alphabets as co-ordinates along the sides.
7. Female is a BP expression for a given constatation to appear in two different places in the message usually at a relatively short distance. A constatation is the association of a cipher letter with its assumed plaintext equivalent.
8. Scritching is a BP term used for the procedure of testing an assumption by examining its implications in a sequential manner with other assumptions, eliminating contradictions and scoring confirmations. This procedure was later automated by Arlington Hall with their machines the Autoscritcher and the Superscritcher.
9. Greenshank was the BP name for the Army Staff key for Germany.