February 15th 1944

W.G. Welchman, Esq.

Dear Gordon:

I am sending you, in case you are interested, a paper I have written on a possible stecker knockout machine. The idea seems to me to be rather more feasible than any of the earlier ones that have been tried.

As you will see there are numerous difficulties which neither I nor the people here have been able to clear up as yet, and I thought you might have some ideas about it from your experience with the bombes.

I have been enjoying myself very much here and taking things fairly easy I am afraid.

I hope you are well.

Yours ever,

Hugh

W.G Welchman
(in case you are interested)

STECKER KNOCK OUT MACHINE

1. Statement of Problem

The present method of attack on the E problem, by high speed bombe is only possible if the whole of the machine except the stecker is known. In the event (a) of a new reflector being introduced or (b) of the reflector being pluggable so that it can be changed daily, the bombe attack is impossible and a new method must be devised. At present we have a rather laborious hand method of attack which can be used on a crib of 300 – 400 letters and with a great deal of labour on a crib of 200 – 300 letters (S. K. O with and without equidistances). This is fairly satisfactory for case (a) since this is a rare occurrence and we are prepared to spend a lot of time to clear it up: in case (b) however it involves an impracticable amount of labour and on cribs of under 200 letters is out of the question.

There is strong, though not yet conclusive, evidence that case (b) has occurred on a small but widely spread group of messages on various air force keys and also some evidence that it may be contemplated also in naval keys. In air traffic reliable cribs of over 100 letters are rare. The problem, then, may be stated as follows: to devise a high speed method of breaking on long cribs (I doubt whether lengths of under 100 would be possible) when both Stecler and reflector plugging are unknown.

2. Outline of Method of Attack

To give the general method in its simplest form I shall assume very favourable conditions. Under actual conditions the amount of work might exceed this by a factor of 26^2 but the example chosen shows the basic principle.

Imagine we have (1) Single notch wheels in the two right hand positions. (2) A stretch of 200 letters for which we have an exact crib. (3) No middle wheel (double) turnover in this stretch. (4) Position of turnover of right hand (fast) wheel known.

From (3) we know that the whole of the left hand portion of the machine is fixed throughout the stretch of 200 letters: from (4) we know the relative positions of the two right hand wheels through the crib.

Select from the message and crib all the pairings involving E, assuming there are more occurrences of E than of any other letter. (Note: in more difficult cases it may be necessary to take as many as 3 letters, say E, N, S instead of just E). On a length of 200 there should be about 35 E's – 28 from the plain text and 7 from the cipher. Imagining we have a machine analogous to a bombe, but with only two wheels (the two right hand wheels) per enigma set up the 35 enigmas involved to the correct relative positions corresponding to the positiions of the 35 E's in the crib. Make the assumption E steckered to A: the number of positions to be tested can be divided by 26 if non-reciprocal

(generalized) stecker is used, I.E. stecker E/A does not imply A/E. To avoid confusion assumption will be written E/a.

Put the current into each enigma at the point 'a': at the left hand side of the enigmas have board connected with all 35 enigmas with 325 points corresponding to the possible pairings through the fixed portion of the machine. Suppose N, say, to be the letter most frequently paired with E in the 35 pairings: imagine 4 EN pairings. Then put current in at each of 4 N's corresponding to some random stecker of N, say Nz. Then 4 EN pairings will energize 4 points on the board, say the points CX, DJ, AY, BQ. Now if from any other enigma of the 35 current from the 'a' input has come out at any of points C, X, D, J, A, Y, B, Q we get a further consequence; suppose that where we have a pairing $\frac{E}{T}$ that current going in at 'a' comes out at C: then since CX pairing is being assumed, current will come back from X and if it emerges at "g" on right hand (original input) side of the enigmas we now have $\frac{E}{T}$ Tg stecker. Now if there is any other pairing put current in again at the Tg point and we get a further pairing on left hand side. This process is a cumulative one in much the same way as is the corresponding process of stecker deductions on the present bombe. Sooner or later in the normal case we should get a pairing CY say, on the board involving the output point ('C' in this case) of the current from the "E" of one of the "EN" pairings. This of course will give a new N stecker, say Ny, which has arisen from the original assumption of Nz: Ny will imply Nx, say, in the same kind of way and so on and in the normal wrong position all steckers of N would ultimately be implied. When this happens the hypothesis E/a is disproved; by the same argument as is used when steckers of a letter fill up on the present machine. If all 26 steckers of N are not filled up, then we get a stop. On this method there are 26^2 hypotheses to try out; either all 26 steckers of E in each of 26 positions or any one stecker, say E/a in 676 positions.

3. Miscellaneous points and difficulties.

(a). It may not be sufficient to search on only one letter as I have done in example. With four $\frac{E}{N}$ pairings as in my example 8 of the 26 letters are normally involved which would give on average 9 further steckers immediately, i.e. from remaining 31 E's we would expect 9 occurrences of these 8 letters on the left hand side of the two wheels: this of course would be more than adequate but in unfavourable cases one might get stuck through failure to get consequences. If this happened (as I think it would) in a very small proportion of the cases ---calculation would show the expectancy – it could be met by testing all stops on a stecker assumption for S, say, assuming there were 3 or 4 $\frac{E}{S}$ pairings.

(b). The position of the fast wheel T.O. will normally be unknown. In this case the crib can either be menued in three or four settings if we can afford to discard some of the material or if not it can be run "delayed hoppity" assuming every T.O. position successively.

(c). There may be a double T.O. If the material permits it could be menued into two or more settings. If the message is divided into stretches A, B, C and MWTO is being assumed in B, the most unfavourable case, then A and C could both be used, but two 'boards' on the left hand side of the

wheels would be necessary corresponding to the different pairings through the left hand portion of the machine due to MWTO.

(d). On shorter cribs (e.g. 80 – 100 letters) more than one initial assumption would be necessary simultaneously i.e. it would be necessary to make 26^2 and possible even 26^3 stecker assumptions. However fewer pairings in all are needed when two basic assumptions are being made than when only one is made since pairings involving both the basic letters are peculiarly favourable as they always give pairings to work on. I think 2 assumptions would be sufficient on 100 letter crib.

4. Further points on S.K.O. machine.

Some experimenting on random cribs of 100 letters makes it look as if 4 menus would normally be necessary and 2 basic assumptions. It is not clear what is the best method to use in trying to fail a position The "filling up" method outlined above is not so satisfactory as on the bombe: whereas on the bombe one new on chain stecker produces steckers of all the remaining letters one new UKW pairing produces only one or two consequences if any so one is much more likely to get stuck and fail to fill up completely than on the bombe. The alternative method is to test on EaNy, say, directly (without trying to fill up on the stecker of a third letter) fail it on a single contradicting UKW pairing and if no contradictions are obtained try all steckers of, say, S with Ea, Ny. I find it very difficult to estimate how many individual positions would have to be tested but at a very rough guess I should say 2×26^3 (i.e. allowing for "scritching" S about once in 26 times). If enigmas were set up originally corresponding to all E, N and S pairings only an extremely small proportion would get through with a consistent result Ea, Ng, Sc. These could be tested further (a) by hand or (if too many for this), (b) by having steckers produced scanned for contradictions of Ag, Bg type or (c) a fourth stecker tried by machine. At one per second 2×26^3 positions would take 10 hours – 800 machine hours for a four menu twenty wheel order job. Ten positions a second seems therefore to be the sort of speed necessary to make the thing manageable.

I understand that the two chief difficulties in getting up speed are (1) that the UKW pairings have to be transferred from one enigma to the other without connecting up the machines completely, i.e. if pairing AB is obtained from machine one and then AB must be connected on machine two but A on one must not be connected to B on two. If the "filling up" method is used going to and fro from stecker to UKW and setting up fresh UKW pairings each time is likely to slow up the machine. (2) If the filling up method is not used, then when a contradiction has been obtained the machine has to stop and restart which increases the time again.

I don't know whether one could throw out on either stecker contradictions or UKW contradictions at will or whether it would be better to work on one type of contradiction only.

Another difficulty is how many pairs it would pay to plug up in advance. Presumably if one was testing on steckers of E and N and doing further testing on S where necessary, then all pairs involving E, N, S would be plugged up but it might be worth plugging up even more.

Reciprocal stecker might be worth using – I haven't considered relative merits of this and generalized very carefully.

It is possible but not very likely I think that a machine for use with hand work could be devised. Taking 4 menus there are 104 positions per W.O. to be tested (using generalized stecker) and 26 steckers of E makes 2700 shots per W.O. and it is difficult to see a machine aid making this a practical proposition.

The whole of this paper represents merely an attempt to indicate a new approach to the S.K.O. problem which gives more chance of success by machine attack than the old method and I realize that it leaves all the most awkward questions unanswered.