NAVY DEPARTMENT
Office of the Chief of Naval Operations
Washington

Op-20-G/rwb
Serial 0843120

May 15, 1943

MEMORANDUM

From: The Assistant Director of Naval Communications, (Op-20-G).

To : Colonel W. P. Corderman.

Subject: Suggested Solution of Commercial Enigma

Reference: (a) Memo of Apr. 5, 1943 on the above subject.

Enclosure: (A) Reference (a).

1. The subject method of solution was discussed at a conference at the Naval Communications Annex on May 4, 1943. The Army representatives present were Major Rosen, Captain Seaman, Captain Dunwell, Mr. Ferner, and Mr. Small. The Navy representatives were Lieutenant Commander H. T. Engstrom and Lieutenant Commander R. B. Ely.

2. Research on a machine which will carry out the suggested operation as well as other more general processes was initiated by the Navy in September, 1942. General designs were completed in January, 1943, and a model of the equipment is now under construction. Delivery is expected in about one month.

3. Discussions at the conference showed complete agreement on the general design of the equipment.

4. The proposal of the reference in handling turn-over points is sound. It is intended, however, to check the operation of a single unit before considering tandem operations.

5. Your cooperation in submitting the reference is appreciated.

E. E. STONE
Captain, U. S. Navy

SUGGESTED GENERAL SOLUTION FOR THE COMMERCIAL ENIGMA, WHERE ONLY THE END PLATE AND WHEEL WIRINGS ARE KNOWN

***

By the method to be described, we should be able to "break" any average message enciphered by the commercial enigma, in an hour's testing time, even though the indicators are not known.

This method uses high speed analytic machinery already developed.

No plain text assumptions are necessary.

1. Basic principles underlying solution:

Suppose a development sheet is made up by enciphering only the letter "E" at every possible setting of the commercial enigma. The other 25 letters are left undeveloped.

Then by superimposing an unknown message against this development and noting "hits," the setting where most "E's" are possible can readily be determined.

Such a setting is not necessarily the proper one however, unless many hundred letters of message text were used in the test.

Now suppose that a development sheet has been made by enciphering the nine highest frequency letters at each setting--so that when any given letter of the message to be tested is

slid against this development, a "hit" at any position of this development means that either an "E" or a "T" or an "0" etc., could have been enciphered at this position. A no-hit means that a medium or low frequency letter would have been enciphered at this point.

If thirty-six consecutive letters of the message are slid simultaneously, and their hits totaled, the proper setting should give an estimated total of 26 hits (on average). Only seven improper cases (out of 2,400,000 tests needed in the commercial enigma) will equal or exceed this average value. (See paragraph 3 below.) Such a test is therefore practical if the tests can be made speedily.

2. Equipment to be used:--A high speed index of coincidence analyzer is needed. This machine should give the total number of coincidences for a superimposition 36 letters wide, at each setting. Furthermore, at each setting, each of the 36 letters should be tested in its own column against a 26 letter alphabet whose individual frequencies are either "1" or "ø". This can be accomplished by a tape with 26 levels or more, in which the frequency of "1" is indicated by "punch", and of "ø" is indicated by "no-punch". Speed is assumed to be 120,000 positions per minute. We understand this equipment is forthcoming soon.

3. Mathematics involved:--Given N identical variates (in this case N = 36, since our test is 38 letters wide) with

any one of the variates to be indicated by "x" and to take on the following values with the probabilities associated thereto:

Random case:		Causal case:	
x	p	x	p
1	9/26*	1	71/100*
Ø	17/26	Ø	29/100

*For English, if it is one of the letters E, T, O, A, N, I, R, S, H

Expected value x (random) = 9/26 or .346

Variance x (random) = .475

Expected value x (causal) = .710

Question: What is the probability that the random value will be greater than the average causal value, given a total test N variates wide?

The inverse of this probability was looked up in the standard normal-curve charts, wherein x_t (the value for x as it appears in the tables) was:

$$x_t = \frac{.710 - .346}{.475} \sqrt{N}$$

We found that for $x_t = 4.5$, the probability that it would equal or exceed is only 3/1,000,000; and for x_t to equal 4.5, N must be exactly 36 letters. (Assuming 10% inaccuracy however this would require 54 letters.)

4. Effect of the ringstellung:--The above calculations were made considering the second-wheel turnover point, or

"ringstellung", to occur at the end of the first 26 letters in each message, and after each set of 26 thereafter.

Different ringstellungs can be provided for, however, by several methods, all practical.

Perhaps the simplest is to use two high speed analytic machines, wired in parallel to the same counting mechanism.

The "master" "development" tape is then prepared in duplicate, as follows:

Each cycle of 26 alphabets generated by the first wheel between motions of the second wheel, is repeated immediately after itself before the kick over takes place.

Eighteen consecutive letters of the message text are then set up on one of the analytic machines; the 27th to 44th letters are set up on the second machine. The tape on the second machine is advanced 52 positions with referance to the tape on the first machine. The two machines are then run in synchronism, their outputs being wired in parallel. The result is a test of 2 x 18 or 36 letters, as required. The proper setting can be found if the breakover occurs somewhere between the 18th and 27th letters of the message, these not having been set up on the test board. Supposing the breakover to have occured however between the 27th and the 34th letters, then we should have started with the 9th letter to set up our test. A second run is therefore made, setting up the machines beginning at the 9th and 35th letters.

A third run is made at the 17th and 43rd letters. This covers practically every possibility in just three runs.

Since we expected 7 bad settings per run, the total number of bad settings equalling or exceeding the average good value is therefore only 21.

If it is desired to use just one machine, we will require a tape of ten million positions, run through three times. The tape is made up as follows: the basic tape is spread out to every other position, and its duplicate advanced 52 positions and printed in between. The combined tape is then put in the analyzer. The first 18 letters are then set up across the test strip at every other position, and the 27th to 44th letters set up in between. Five million interspersed settings of the master tape will of course be impossible settings, and the effective length of the tape as far as number of comparisions goes will therefore be only the remaining 5,000,000, and half of these are duplicates. So for three runs we must still deal with only 21 bad settings above the average good value.

Another method of using a single machine consists of making a tape only 5,000,000 long, and making three runs with the two 18 letter groups starting in each of three positions for each run. (Not to be described here.)

Less letters would have to be taken into the test of course, if all 26 could be used in each alphabet and accurate frequency values "punched" into the tape by varying the sizes of the holes "punched".* This is not considered necessary, since the 36-wide test should be possible with standardized machinery.

It should be noted that rapid analytic apparatus is used throughout; the times of testing are exceptionally short; bad cases as high as the average good are not too numerous, and can be lessendd withlanguages other than English; and best of all, no plain text guesses are required.

The bottleneck, if any, is in preparation of the development tapes. We have not been informed as to the exact nature of the machines accomplishing tape manufacture, and cannot estimate times here.

Possibilities for solving Orange and Yellow traffic may develop out of this proposed Indigo method.

---

*For German, approximately 25 letters.

Section B III F

Extra

REF ID:A4146658

~~SECRET~~

SPSIS 3115.-Gen. SPSIS-3

1st Memo Ind.

Director of Communications Research, 3 July 1943.

To: Commanding Officer, Arlington Hall Station

1. In a paper dated 5 April 1943, the SSS described a "Suggested General Solution For The Commerical Enigma Where Only The End Plates And Wheel Wirings Are Known". The basic idea was entirely conceived and elaborated by SSS personnel, independently of any contact with the Navy. The title of the paper was unnecessarily limited, because the principles are applicable to the steckered Enigma also. It presented possibilities for a purely statistical method of solution, not requiring any cribs.

2. In view of our previous relations with the Navy in regard to technical research and development, as soon as the proposed new solution appeared to offer possibilities, a conference was arranged with the Navy for the purpose of disclosing the idea to them and possibly initiating a joint project for incorporating modifications in an existing Navy RAM known as "Tetra-Tessie" with a view to trying out the new statistical method conceived by SSS personnel. This conference was held on May 4, and is the one referred to in the Navy memorandum dated May 15. Inasmuch as I was away on a mission, I was not present at that conference.

3. It was only at the end of the conference, after our representatives had disclosed the basic principles of our proposed method of statistical solution, that the Navy representatives saw fit to disclose to our representatives at the conference the fact that they had under development a new piece of equipment known as "Hypo", which was intended to operate along somewhat new lines in connection with E solution activities but still required the use of "cribs". They indicated however that they were aware of statistical possibilities along lines similar to ours.

4. After some discussion, during which our representatives pointed out how the "Tetra-Tessie" machine might be modified, the Navy representatives thought that the "Hypo" machine might be used for the type of statistical solution proposed by SSS.

~~SECRET~~

Thereupon our representatives left with the Navy the memorandum dated April 5, to which reference was made in the first paragraph above, for the purpose of closer study by the Navy to determine the feasibility of the solution by use of a suitably modified "Hypo" machine. It was jointly agreed not to initiate an additional development project for equipment specifically designed to operate according to the principles disclosed in the above-mentioned memorandum.

5. At no time during this conference did the Navy mention the fact that although they had disclosed "Tetra-Tessie" to the British they had withheld this technical development relating to the "Hypo" machine from the British. This fact developed only during a conversation between Commander Wenger and myself on the evening of June 17. I must admit that I was considerably astonished to learn this fact, and it should also be stated that our representatives at that conference were also taken aback when they learned that the "Hypo" development, although dating from September 1942, had not been previously disclosed to SSS.

6. Only general features were discussed and few details of the "Hypo" equipment were made available at the conference. After more mature thought and deliberation, keeping in mind the fact that the proposed "Hypo" machine is intended for "crib" operation, it was not and is still not clearly apparent to us how the "Hypo" machine can be directly applied to the statistical method proposed by us; however we are still not cognisant of all constructional and operating details of the "Hypo" machine and no effort has been made by us to secure these details. It was decided to wait until the proposed equipment has been reduced to practice before going further into the matter. This did not seem to be long off, for delivery of the "Hypo" machine was indicated as being only about a month off.

7. In view of the foregoing, it is clear that the SSS is not under any obligation to the Navy for any of the ideas involved in the SSS proposed statistical method of solution as disclosed in the above-mentioned memorandum of 5 April 1943.

8. There is now considerable doubt in our minds as to whether the proposed "Hypo" apparatus can be readily modified to accomplish the type of statistical solution proposed by us,

and we are undertaking studies independently of the Navy, with a view to initiating a project for the construction of a machine that will accomplish it.

9. Although it is realized that this question involves matters of policy, I feel nevertheless warranted in making the recommendation that we abide strictly by the terms of our recent agreement with the British in respect to a complete interchange of technical information, especially in regard to the "E" problem. This may not be the time to make a disclosure to the British but I feel that we may want to be free to make a disclosure should our preliminary investigations prove the feasibility of our proposal.

10. In view of the fact that Captain Seaman and Mr. Ferner are unaware of the situation raised by your memorandum of June 28, and inasmuch as they are still awaiting transportation it may be desirable to communicate with them with a view to giving them proper instructions in the premises.

William F. Friedman
Director of Communications
Research

~~SECRET~~

SPSIS 3115.-Gen. SPSIS-3

1st Memo Ind.

Director of Communications Research, 3 July 1943.

To: Commanding Officer, Arlington Hall Station

1. In a paper dated 5 April 1943, the SSS described a "Suggested General Solution For The Commerical Enigma Where Only The End Plates And Wheel Wirings Are Known". The basic idea was entirely conceived and elaborated by SSS personnel, independently of any contact with the Navy. The title of the paper was unnecessarily limited, because the principles are applicable to the steckered Enigma also. It presented possibilities for a purely statistical method of solution, not requiring any cribs.

2. In view of our previous relations with the Navy in regard to technical research and development, as soon as the proposed new solution appeared to offer possibilities, a conference was arranged with the Navy for the purpose of disclosing the idea to them and possibly initiating a joint project for incorporating modifications in an existing Navy RAM known as "Tetra-Tessie" with a view to trying out the new statistical method conceived by SSS personnel. This conference was held on May 4, and is the one referred to in the Navy memorandum dated May 15. Inasmuch as I was away on a mission, I was not present at that conference.

3. It was only at the end of the conference, after our representatives had disclosed the basic principles of our proposed method of statistical solution, that the Navy representatives saw fit to disclose to our representatives at the conference the fact that they had under development a new piece of equipment known as "Hypo", which was intended to operate along somewhat new lines in connection with E solution activities but still required the use of "cribs". They indicated however that they were aware of statistical possibilities along lines similar to ours.

4. After some discussion, during which our representatives pointed out how the "Tetra-Tessie" machine might be modified, the Navy representatives thought that the "Hypo" machine might be used for the type of statistical solution proposed by SSS.

~~SECRET~~

Thereupon our representatives left with the Navy the memorandum dated April 5, to which reference was made in the first paragraph above, for the purpose of closer study by the Navy to determine the feasibility of the solution by use of a suitably modified "Hypo" machine. It was jointly agreed not to initiate an additional development project for equipment specifically designed to operate according to the principles disclosed in the above-mentioned memorandum.

5. At no time during this conference did the Navy mention the fact that although they had disclosed "Tetra-Tessie" to the British they had withheld this technical development relating to the "Hypo" machine from the British. This fact developed only during a conversation between Commander Wenger and myself on the evening of June 17. I must admit that I was considerably astonished to learn this fact, and it should also be stated that our representatives at that conference were also taken aback when they learned that the "Hypo" development, although dating from September 1942, had not been previously disclosed to SSS.

6. Only general features were discussed and few details of the "Hypo" equipment were made available at the conference. After more mature thought and deliberation, keeping in mind the fact that the proposed "Hypo" machine is intended for "crib" operation, it was not and is still not clearly apparent to us how the "Hypo" machine can be directly applied to the statistical method proposed by us; however we are still not cognisant of all constructional and operating details of the "Hypo" machine and no effort has been made by us to secure these details. It was decided to wait until the proposed equipment has been reduced to practice before going further into the matter. This did not seem to be long off, for delivery of the "Hypo" machine was indicated as being only about a month off.

7. In view of the foregoing, it is clear that the SSS is not under any obligation to the Navy for any of the ideas involved in the SSS proposed statistical method of solution as disclosed in the above-mentioned memorandum of 5 April 1943.

8. There is now considerable doubt in our minds as to whether the proposed "Hypo" apparatus can be readily modified to accomplish the type of statistical solution proposed by us,

and we are undertaking studies independently of the Navy, with a view to initiating a project for the construction of a machine that will accomplish it.

9. Although it is realized that this question involves matters of policy, I feel nevertheless warranted in making the recommendation that we abide strictly by the terms of our recent agreement with the British in respect to a complete interchange of technical information, especially in regard to the "E" problem. This may not be the time to make a disclosure to the British but I feel that we may want to be free to make a disclosure should our preliminary investigations prove the feasibility of our proposal.

10. In view of the fact that Captain Seaman and Mr. Ferner are unaware of the situation raised by your memorandum of June 28, and inasmuch as they are still awaiting transportation it may be desirable to communicate with them with a view to giving them proper instructions in the premises.

William F. Friedman
Director of Communications
Research