MEMORANDUM FOR RECORD. 1 July 1954

TO: Mr. Friedman

FROM: Mr. Snyder, R/D 3501

SUBJECT: SUPERFLEX

1. I am forwarding the material on SUPERFLEX, about which I telephoned you the other day, so that you can get a full picture of the background actions since the original proposal in August 1946, for study as your own schedule permits.

2. I understand that results of recent field testing of the "507" reveal, among other things, difficulties due to variations in the length of electrical paths through the rotors. This will certainly influence the engineering evaluation of SUPERFLEX. The seriousness of this trouble, and the likelihood of an eventual solution should be re-evaluated if cryptographic evaluation of SUPERFLEX indicates that it is worthy of serious consideration.

3. I would appreciate your comments as to the potentialities of this system, apart from engineering considerations. Particularly what possibilities there are in one of its small embodiments.

S. S. Snyder

S. S. SNYDER
R/D 3501

Incl:
SUPERFLEX File

Declassified and approved for release by NSA on 10-15-2014 pursuant to E.O. 13526

REF ID:A4146724

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE DR KULLBACK	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION R/D	DATE		COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Mr. Snyder thinks there are features here which ought to be studied once more. In the light of developments since 1946, when he first suggested the ideas on which his SUPERFLEX is based, is there any reason to change the evaluations put on this system?

FROM NAME OR TITLE Friedman	DATE 10 Sept 54
ORGANIZATION AND LOCATION	TELEPHONE

DD FORM 1 FEB 50 95 Replaces DA AGO Form 895, 1 Apr 48, and AFHQ Form 12, 10 Nov 47, which may be used. 16—48487-4 GPO

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION ~~3??~~	DATE		COORDINATION
2			FILE
314 see comment below MRE			INFORMATION
3		X	NECESSARY ACTION
31 MC			NOTE AND RETURN
4			SEE ME
30			SIGNATURE

REMARKS

Comment please

From a security point of view the potentialities of superflex are great if the superflexing features are pluggable but this creates great problems for the development engineers and great trouble for the potential operators. WHEaskins.

FROM NAME OR TITLE [signature]	DATE 13 Sept
ORGANIZATION AND LOCATION 13	TELEPHONE

DD FORM 1 FEB 50 95 Replaces DA AGO Form 895, 1 Apr 48, and AFHQ Form 12, 10 Nov 47, which may be used. 16—48487-4 GPO

REF ID:A4146724

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

1. NAME OR TITLE / ORGANIZATION AND LOCATION	INITIALS / DATE		
1.			CIRCULATE
			COORDINATION
2 Mr. Friedman			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4 ~~SECRET~~ ATTACHED			SEE ME
			SIGNATURE

REMARKS
Snyders proposal is essentially a brute force solution. The multiplicity of plugging & plugboards would entail an engineering problem and practical operational problem. ~~[illegible]~~ We ~~[illegible]~~ need more ingenious ideas which are easy to engineer and operate & yet provide the security of thousands of pluggable leads.

FROM NAME OR TITLE: S Kullback
DATE: 27 Sept 54
ORGANIZATION AND LOCATION: RD
TELEPHONE:

DD FORM 1 FEB 50 95 Replaces DA AGO Form 895, 1 Apr 48, and AFHQ Form 12, 10 Nov 47, which may be used. 16—48487-4 GPO

REF ID:A4146724

DISPATCH
NSA - R/D
MAIL ROOM

1954 SEP 28 3 00

BY ____________

COM-
MENTS
ACTIONS

15 September 1952

MEMORANDUM

TO: Dr. Kullback

FROM: S. S. Snyder

SUBJECT: SUPERFLEX

1. You may recall the time in 1946, when I developed the idea and the suggested embodiment for the cryptographic device called SUPERFLEX. It was born of a desire for a device which would thwart the classic methods of entry into wired rotor systems, namely, either by "stripping" one rotor at a time, or by dividing the machine in half. Such methods are possible primarily because, in the classic rotor maze, current entering at a given point follows a path through a series of rotors in turn and always in the same order. My proposal varies the point of entry, the order and the number of rotors in the path, according to change of setting and also according to plain text entry point. The method of accomplishing this includes, in the most likely embodiment, the use of printed circuit "cards" as a means of varying the machine setup or specific key. Possession of the machine, the rotors, and the cards would not constitute a compromise, without knowledge of the selection of cards and order of assembly in a specific key. In fact, it is possible, subject to verification by security study, that clear indicators could be used for rotor settings.

2. Under the then Projects Section, CSGAS 76C, a certain amount of study was devoted to this. A handtester was put together using SIGABA baskets and SIGHEK pluggable stators; with this it was possible to simulate various plugging setups, and much was learned about its potentialities and limitations. Also, the subsection heads all wrote comments on SUPERFLEX, and Miss Phyllis Metcalf made a fairly complete study of a representative situation. These comments and the security study are attached with be original paper and its amendments, as well as a paper by Frank Proschan on the number of paths of various lengths possible under different conditions. Dick Chiles, particularly, made valuable contributions, suggested several improvements, and helped put together the handtester. As far as I know, the idea for this device never was given enough backing to be forwarded to any higher echelons, nor were there any strong objections which would throw it out of consideration for eventual adoption.

3. Since I am still of the opinion that this device could be of potential value, and since I am sure it does no good to be resting in my file unevaluated, I am offering it to the Agency through you, for enough research to evaluate its potentialities. I understand that the newly constituted branch 314 will have opportunity to give greater emphasis to such security studies, and it may be that this is the time and the right place to reopen this matter. I only hope that during the past six years there have not been occasions when this device could have satisfied some Agency need.

S. S. SNYDER
Procedures Branch, 351

SECRET

SECRET SECURITY INFORMATION

361D - AHS
Mr. S. S. Snyder

25 Jul 52

412B

Superflex

1. Herewith is the folder we discussed recently.

2. Our studies on this indicate that the ideas might easily be developed into a secure system if the various features can be made practical. There is, of course, a question of whether another system built along more conventional designs representing the same complexity and same amount of equipment would provide security as great as this principle. This we were not able to answer. In my own opinion, unless a system built along the lines of Superflex would block solution based on known stepping of rotors, I am inclined to think that security would not be substantially greater than that from a more conventional machine of comparable complexity. Putting it another way, if the use of this principle would permit transmission of message rotor alignments in the clear, safely, this would be a step forward.

3. I have been at a disadvantage on this system by not knowing what the engineers would consider practicable in terms of equipment features. This is a type of research for which all deadline jobs seem to take precedence; consequently, whenever we started the study of any specific application of the system, there seemed always to be a deadline job coming up that forced this one to wait. I apologize for having so little to report.

R. A. PAGE
Head, AFSA-412B

SECRET

REF ID: A4146724

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE 412B	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	DATE		COORDINATION
2			FILE
			INFORMATION
3		X	NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Complete evaluation, please.

Priority Z. Deadline 25 Jan 1951 or better if you can.

FROM NAME OR TITLE RHS (signed)	DATE 5/8/50
ORGANIZATION AND LOCATION 412	TELEPHONE

DD FORM 1 FEB 50 95 Replaces DA AGO Form 895, 1 Apr 48, and AFHQ Form 12, 10 Nov 47, which may be used. 06—16—48487-4 GPO ☆

SECRET

17 July 1950

Abe:

As per our conversation the other day, I am sending herewith a folder containing a file copy of my proposal for SUPERFLEX, together with other papers bearing on the subject. I would appreciate an evaluation of the basic theory, and an appraisal of its suitability for inclusion in an official device.

The proposal is described in the basic paper, which was in the form of a memorandum to Projects Section on 6 August 1946. Mr. Chiles, who was in that Section at the time, became interested in it, and made valuable contributions, including a suggested embodiment which is described in his paper dated November 1946. Also he was primarily instrumental in constructing a 'hand-tester' which turned out to be invaluable both for testing variations of the device and for producing cipher text for study. Sets of sliding strips can be used for this, and for detailed check of the actual rotor paths, but the process is extremely slow for mass encipherments.

A later suggested embodiment, dated 19 September 1947, introduced the idea of a 'commutating cylinder' which if engineeringly feasible, would add considerably to the security by changing stator plugging at each encipherment.

The security study included herein was made by Miss Metcalf, and is the only extensive effort along this line. Certainly other analysis is necessary to get a complete evaluation.

Thank you very much for your consideration.

SAM (signed)
S. S. SNYDER
AFSA 351D
Ext. 377 (AHS)

CSGAS-70 10 October 1947

COMMENTS ON SUPERFLEX

1. The system which has been proposed was based on the assumption, among others, that security would be enhanced because additional items need be either captured or obtained in other ways by an enemy. Considering our present rotor systems, we may say that the following components of a system must be protected:

a. The key list
b. The rotors
c. The basic system.

2. The basic system, however, usually must be considered as known to the enemy. That leaves, then, only the key list and rotors to be safeguarded. If either is compromised security depends upon the continued uncompromised status of the other. With the addition of another component to the system, security of traffic, presumably, would continue even after the loss of any two components.

3. It should be noted in this connection that if there is a loss by capture one can not be certain that all components have not been lost. If there is a compromise through espionage one must expect all components to be lost. At least, these are the safest assumptions to make.

4. There is an advantage when shipping systems to holders in having many components in a system. Then, if one component is lost in transit the remaining uncompromised components should assure security until replacement of the lost component can be made. One simple way of increasing the number of components in our present systems is to divide the key list into separate parts, all parts together then being needed to operate the system. Loss in transit on one component would not necessarily endanger security. As a practical matter, compromised key lists can be replaced with less strain on production facilities and with less expense than can rotors or other components more difficult and expensive to produce. The frequency of changing the different components and the length of time they remain effective affects the relative importance of the components.

5. Four rotors are recommended for the system, mainly to assist in reducing the weight and size of the machine. No motion is specified for the four rotors. Because the type of motion contributes a great deal to the security or insecurity of a system no definite statement can be made on the security of this system. If straight-forward predictable motion is used, even with five rotors, it seems quite probable that methods of solution can be found. In considering possible motions for the machine, thought must be given to the effect of clear indicators, one rotor off (if this should be dangerous to security use of only four rotors will allow such a condition to arise more often than a greater number of rotors), tailing, etc.

6. The study of reflexing is, as yet, scarcely begun and it seems reasonable to believe that techniques will be found for handling reflexed systems which can be applied to this system. As it stands now a considerable amount of time

and effort will b e needed to give a proper evaluation of the security of the system.

7. It would seem to be true that if a strong motion is needed for security, regardless of other factors, then most effort should be concentrated on finding a strong motion and depending on it for the principal security safeguards.

JAMES H. DOUGLAS

CSGAS-76

9 January 1947

COMMENTS ON SUPERFLEX

Noted. The using forces will not stand for plugging. Therefore this problem should be licked first. Secondly, much more security study must be done before this idea can be circulated.

A. I. DUMEY
Cryptologic Branch

COMMENTS ON SUPERFLEX

1. The limitation on motion, suggested in paragraph 2 d of the description, which would insure that none of the rotors would be stationery for more than two successive encipherments would greatly increase the difficulty of guaranteeing a long cycle on the machine. The limitation was introduced to suppress repeats in the cipher which come from repeats in the plain. Such a limitation would increase consecutive letters ~~repeats~~ in the cipher which come from successive letters in the plain, $AB_p = CD_c$. This would happen when ever all wheels USED turned between such a plain text pair. Any further limitation of motion cuts down the number of trials the enemy cryptanalyst must make. The suggested limitation would not entirely suppress consecutive repeats ~~repeats~~ which come from consecutive repeated letters.

2. The test messages enciphered by the machine show a large percentage of two-wheel encipherments. The following percentages were enciphered by two wheels only:

25.5% of Test 1
33.7% of Test 2
30.0% of Test 3
24.0% of Test 4

The following characteristics of the machine are suggested as offering a possible statistical solution because of the number of two-wheel encipherments.

The following wheel orders are the only ones possible in a two-wheel encipherment with the machine set up as in the example.

1 and 4
2 and 4
2 and 5
3 and 4
3 and 5

The cipher text may be divided into two classes, those letters which are the output of Rotor 4 and those letters which are the output of Rotor 5. In the example 13 letters come from wheel 4 and 13 letters come from wheel 5. If all entry points are equally possible then 3/5 of the two-wheel encipherments are going to leave the machine at wheel 4. If high frequency letters are plugged into wheel 1 then this percentage will become larger. On the basis of frequency it might be possible to classify the cipher text as outputs of wheel 4 or wheel 5 which will begin to give an entry into the machine for bombing with fewer trials.

The basis for classification of cipher text is a result of the limitation which does not allow the wheel order 1 and 5 as a

(Comments on SUPERFLEX)

two-wheel encipherment. This was introduced to cut down the number of two-wheel encipherments. A different set of stator plugging which did not use one as an entry point and 5 as an exit point might be devised to overcome the frequency attack, which is an attack and not a solution.

3. If this machine is suggested to fulfill Basic Military Requirements II, III or IV the consideration of inter-communication may become very complicated unless all three devices employ similar principles.

4. The machine would be subject to error in setting up the key whether cards or plugs were used to vary the stator wiring. Frequent changes of key would certainly not be practical.

Mary MacNeill

27 August 1946

I suggest (a) a security study based on fixed stator wiring (which is probably what will be the case, anyway) to see what can be done about getting the wheels and identifying them, and (b) consideration of reflexed machine, which would permit the removal of the limitations on motion (to some extent).

DANIEL M. DRIBIN

11 September 1946

Some improvement in the means of "plugging" seems to be indicated if this idea is to be useful - and I don't like the idea of fixed stator wiring. Certainly, also, the suggestion should be developed to eliminate the necessity for the motion restrictions. Perhaps a simpler device including the re-entrant feature should be studied first.

Warren H. Turner, Jr.

13 January 1947

The 2-wheel encipherment danger can be circumvented by introduction of a reflector ~~so~~ that one endplate is used; of course, bridged elements are still highly doubtful. Plugging is a difficulty which must be faced realistically

Daniel M. Dribin

(Comments on SUPERFLEX)

9 November 1946

It should be pointed out that the idea of assembling 26 cards from a deck of 108 containing possible printed circuits permits more flexibility than is indicated in paragraph 1E and Figure 3. Since the choice of number and position of entering rotors (from LFS) and exit rotors (to RFS) is not fixed, these can be varied by printing of new sets of cards. Presumably new cards would be issued at the time new sets of rotors were sent out. This, therefore, increases further the variability, and is an additional advantage over the plugging method mentioned in paragraph 1E which would have 108 stator wirings built into the machine and only allow variation of plugging.

Mary Neely Rosebro

Research on the basic security of simple reflexed cipher systems has pointed up the fact that the first step in any solution effort is to separate those elements whose encipherments involve one channel (one trip through the maze) from those whose encipherment involves several channels. Moreover any use of a reflexed element requires specific assumptions as to the number of trips through the maze. In the light of the above study SUPERFLEX solution would require an effort to separate the elements into classes according to the specific wheel order (i.e., wheels 1-2-2-3 etc.) for the elements being used. This effort would be a major one except possibly for the 2-wheel encipherments and the physical difficulty of changing the stators.

The fact that in 5 to 10% of the cases a specific two-wheel encipherment may be involved ~~with~~ gives a wedge for solution if the identification of which elements are of this type is possible.

If wheels 4 and 5 are made fairly fast moving wheels in order to complicate this identification then it may be possible to set wheels 4 and 5 and then wheels 2 and 3 in turn by assumptions made an encipherment by wheels 2 and 4 and verified by 2 and 5 encipherments. The two-wheel encipherments. Addition of another wheel or two would make it possible to guarantee that no two-wheel encipherments occur.

Unless the stator "cards" are changed frequently the insecurity of the two-wheel encipherments will engulf the basic security advantages of the "superflexing".

Perhaps a 7-wheel device as suggested below which eliminates 2-wheel encipherments would provide more security. This device sacrifices the variablity provided by the cards for the assurance

(Comments on SUPERFLEX)

that the minimum 3-wheel encipherments will occur in less than 11% of the cases. Moreover the security due to variability of the cards will be partially regained by the possibility of more frequent changes of the stators.

In the description below the inputs of stators are described as being connected to the outputs of stators by multiple position switches instead of cards. i.e., if the input of stator C is connected to the output of stator A_1 then the encipherment would have involved wheel 2 and then wheel 1 in that segment of its path.

STATOR A | C.W. 1 $\boxed{1}$ | STATOR B | C.W. 2 $\boxed{2}$ | ETC. C $\boxed{3}$ D $\boxed{4}$ E $\boxed{5}$ F $\boxed{6}$ G $\boxed{7}$ H

LET INPUTS OF STATOR	A	BE CONNECTED TO OUTPUTS OF STATORS A, B, OR C
	B	A, B, OR C
	C	A, B, OR C
	D	D
	E	E
	F	F, G, OR H
	G	F, G, OR H
	H	F, G, OR H

Let 3, 4, 5 be the most rapid wheels - for example let 4 be fast and either 3 or 5 move every time. Let successive wheels move in opposite directions. Let the cards be replaced by 52 - six position switches and a daily key list furnish the settings of these switches. (The key list could be prepared so that for high frequency letters the stator A be connected only to A or B thus guaranteeing encipherments by a minimum of 4 wheel on high frequency letters.

The wiring task on the chassis of any SUPERFLEX will be a gigantic production problem and therefore very strong recommendations will have to be made before it will be adopted. Devices of comparable security.

William H. Erskine

(Comments on SUPERFLEX)

23 October 1946

I like the basic contribution which this device makes to cipher machine technology, but believe it would be better if certain practical defects or difficulties could be eliminated. One is the complexity of the internal wiring job, which is apparently a neccessary corallary to the inclusion of the feature of pluggable stators. Another possible criticism is the fact that within any key period (same stator plugging) there is a consistent entering rotor associated with each plain letter, and likewise a consistent exit rotor associated with each cipher letter. The following variation in the design is offered as a means of eliminating both, and also, in line with Dr. Erskine's suggestion, it insures at least a three-rotor encipherment for every plain-text character. A further advantage is that the necessity for inserting the twenty-six cards in slats to change the stator plugging is eliminated, this change being effected merely by substituting a new plastic cylinder for the one formerly in use, as described below.

The cipher maze of the machine would consist of the following elements:

(1) Seven rotors (preferably of the plastic printed-circuit type). These rotors would be in the form of rings approximately 3" or 3½" in diameter, depending on the number of contact points, with a 2" hole in the center of each instead of the usual ¼" or 3/8" shaft hole.

(2) Eight stators separating the rotors, of special construction as shown in Figure 1.

(3) A cylinder, 2" in diameter and equal in length to the length of the rotor-stator assembly. This cylinder will have circuit paths printed on its surface which serve to inter- connect the input and output contacts of the stators (see Figure 2), effecting the same result as the stator wirings of SUPERFLEX. In addition this cylinder serves as the shaft about which the rotors move and itself is moved independently (possibly opposite in direction to the movement of the rotors). This would have the effect of not only shifting the points of contact of plain and cipher letters with each encipherment, but also of adding to the variability which results from the basic idea of stator plugging.

As shown in Figures 2 and 3, stators A, B, C, and D are inter-connected by the circuit paths printed on the rotating cylinder, and in the same way stators E, F, G, and H are inter-connected. This arrangement is merely an adaptation of Dr. Erskine's suggestion, and if the circuit paths for each set of four stators are arranged so that at least one rotor from the

(Comments on SUPERFLEX)

group 1, 2 and 3 and one from the group 5, 6 and 7 is used in every path (rotor 4 being used every time), a minimum three-rotor encipherment is assured for each plain-text character. It will be noted that the cylinder may be cut in half and each half moved independently, if this is thought desirable.

If the above limitation is used to assure at least a three-rotor encipherment, there are eighteen possible circuit arrangements for each set of four stators. All eighteen circuits are shown on the cylinder in Figure 2. If the same tolerances which were used in planning printed rotor circuits are maintained, all of these paths can be easily arranged on a cylinder 2" in diameter with the rows of contact points spaced $\frac{1}{4}$" apart.

J. R. Chiles

STUDIES OF SUPERFLEX

An exhaustive security study has not been made of all embodiments of SUPERFLEX. Such methods of solution as could be devised and carried through by hand have been tried for the simplier embodiments of the machine. No method of attack is at hand for the most complicated version of SUPERFLEX which includes mixed level stator wiring. A detailed report of the embodiments studied, the materials used, and the results obtained follows.

I Original Embodiment

A. Description.

1. 5 Hebern type rotors with 26 points each

2. Orange type motion - cascading multiple notch

3. 6 stators.

a. Variable by plugging (26 point IBM jacks) or printed circuit cards.

b. No mixed levels in stator wiring.

c. Limitations.

(1) Minimum 2-rotor encipherment insured by designating 3 rotors as entrance rotors and the remaining 2 as exit rotors.

(2) 5 possible 2-rotor encipherments (1-4, 2-4, 2-5, 3-4, 3-5)

B. Frequency Counts

1. 200 letters of matching plain - cipher

a. Plain frequencies

(1) 32 occurrences of X (word-spacer)

(2) 27 occurrences of E

(3) 0 occurrences of K, Q, Z

b. Cipher frequencies

(1) 12 occurrences of D, E to

(2) 3 occurrences of S

(3) no blanks.

c. Number of rotors involved

(1) 51 2-rotor encipherments

(2) Average encipherment was through 5 rotors

(3) Maximum encipherment was 22 rotors

2. Same as B 1 above but with different motion pattern.

a. Plain frequencies - see above

b. Cipher frequencies

(1) 15 occurrences of S to

(2) 2 occurrences of R

(3) no blanks.

c. Number of rotors involved

(1) 67 2-rotor encipherments

(2) Average encipherment through 5 rotors

(3) Maximum encipherment was 23 rotors

3. 100 encipherment of "E" which entered fast moving rotor

a. Cipher frequencies

(1) 8 occurrences of L to

(2) 1 occurrence of D, P, Z

b. Repeats

(1) no consecutive occurrence of identical enciphering paths

(2) 4 cases of consecutive cipher repeats derived by different paths.

4. 100 encipherments of "R" (entering slowest entrance rotor)

(Studies of SUPERFLEX)

a. Cipher frequencies

(1) 12 occurrences of O to

(2) 0 occurrence of C, W, Z

b. Repeats

(1) 1 pentograph (KKKKK) due to identical enciphering paths occurring consecutively and caused by no motion of enciphering wheels involved.

(2) 5 trigraphs as above

(3) 9 digraphs as above

C. Attempts at Solution

1. Given motion, setting, order, and wiring of rotors, an attempt was made torecover stator wiring with 200 letters of cipher text.

a. Method: Plains "E" and "X" were assumed to enter Rotor 3. Every cipher letter was assumed to have come from plains E and X and was deciphered through every possible combination of 2 wheels. A table was kept of the stator wirings implied by each of these possible encipherments. Analysis of confirmations and contradictions in this table yielded 13 correct wires and one incorrect wire in stators D, E, and F. Decipherments through these established wires gave insufficient clues for cribbing in additional plain text.

b. An attempt was made to recover plain text by removing rotor 5, where wires derived in (a) above made it possible, and deciphering through rotors 2 and 3. An attempt to assign plain text letters to the entrance points of these wheels on the basis of frequencies gave insufficient data to warrant continuation of such an approach.

2. Given setting, motion, order, and wiring of rotors. An attempt was made to recover stator wiring with 200 letters of matched plain-cipher.

a. Method - All stator wiring implied by possible 2-rotor encipherments was tabulated. Confirmations were sufficient in 34 cases to accept the derived wires as a basis for obtaining additional ones from 3-rotor encipherments. All stator wiring was recovered. (It is probable that this could not have been accomplished with 200 letters of matched plain-cipher from a machine with simple metric motion if there were no turnover of 3rd, 4th, and 5th wheels.) A tabulation of wiring implied by all possible 2-rotor encipherments of the same 200 matched plain-cipher pairs with rotors set incorrectly gave results with sufficient contradictions to reject the setting.

II Second Embodiment

A. Description

1. 5 Hebern-type rotors (26point)

2. Simple metric motion - 1 notch per wheel.

3. 6 stators (same as in Original Embodiment)

B. Frequency Counts

1. 255 plain-cipher pairs

a. Number of 2-rotor encipherments:

(1) 17.9% before turnover of 3rd wheel.

(2) 61% (in only 26 pairs) after 3rd wheel break.

b. Plain-cipher constatations show break-point approximately. It was possible to determine to a large extent which plain letters were enciphered through rotor 1 and any combination of rotors 1, 2, 3, 4, 5; which were not enciphered through 1; and which were not enciphered through 1 or 2.

C. Attempts at Solution

1. Given 10 consecutive cipher alphabets, known rotor order, setting, wiring, and simple metric motion with turnover of 2nd wheel only between the 5th and 6th alphabets. An attempt to recover stator wiring on the basis of 2-rotor encipherments was made. 36 correct stator wires were recovered. These produced insufficient decipherments in a message to suggest

cribbing or recovery of additional stator wires, even when rotor wiring, motion, and setting of the message were known.

III Third Embodiment

A. Description

1. 10 Hebern-type rotors (26 point Sigrotes)

2. Simple metric motion - (Some sample encipherments made with simple metric motion in 2 sets of 5 rotors each.)

3. 10 stators

   a. Mixed-level wiring.

   b. No variation of stator wiring.

   c. Minimum 2-rotor encipherment guaranteed by having plain pass through rotor 1 before entering stator A where variation in wheel order is initiated; by having no connection from stator A direct to cipher output.

B. Observations

1. Given 10 messages in depth - show that frequencies between breakpoints of 2nd fast wheel can be exploited as well as column frequencies to derive plain text.

2. Given 2 messages with same plain and in depth on all but 6th wheel. The sample shows that wheel 6 was involved in 198 of the 327 encipherments (60.6%. This would seem to imply that reading text by setting and deciphering on fewer than all ten wheels might be impractical.

3. Given 25 cipher alphabets and all elements of the machine except stator wiring. No method of solution devised.

IV Fourth Embodiment

A. Description

1. 4 Hebern-type rotors (26 point)

2. Orange type motion - cascading multiple-notch. (In

(Studies of SUPERFLEX)

final version perhaps notch pattern could be permanently attached to wheels. Delayed cycle-motion suggested by Dr. Erskine was considered but it may be unnecessarily complicated)

3. 5 stators

a. Mixed levels

b. Variable by printed circuit cards changing plugboard connections. The plugboard would have 13 x 20 hubs for wires from the stators. Ten circuit cards would be pulled from a deck of, say, 50 and placed on the face of the plugboard according to the key. Each card would connect two columns of 13 hubs in the plugboard. Approximately 10^{15} trials would be necessary to recover stator card assembly.

c. Limitations

(1) Minimum 2-rotor encipherment (enter rotors 1 and 2; exit rotors 3 and 4) or

(2) Minimum for final version is 1-rotor encipherment.

B. Attempts at Solution

1. Given 200 letters of matched plain-cipher; known rotor wiring, setting and motion. No method of attack for recovering stator wiring was suggested - (Exhaustive trials about 10^{15})

2. Given matched plain-cipher, rotor wiring and notch patterns, and stator wiring. An attempt to set rotors for a message was made. To split the machine and set two rotors initially, 3, a fast and exit rotor, and 1, 2nd fast and entrance rotor were chosen as they were the only two completely independent of other rotors with respect to motion. All plain-cipher constatations with plain entering rotor 1 and cipher leaving rotor 3 were selected from the crib; 34 crib pairs yielded 13 such constatations requiring two correct 2-rotor encipherments for a "stop" when trying the 13 pairs, gives about 38 random stops per wheel order and a 25% chance of missing the correct stop entirely. Therefore, since the number of trials for setting four wheels simultaneously is no greater than for setting two at a time, and crib required

(Studies of SUPERFLEX)

would undoubtedly be shorter, splitting is a less practical and less reliable method of wheel setting.

3. A deck of 50 cards was made in order to determine time required for changing stator cards according to a key. Average time for withdrawing 10 and inserting 10 other cards was less than 3 minutes.

Conclusions:

I. A small, easily operated, and secure SUPERFLEX is practical if printed circuit cards can be developed to vary stator wiring. Without variable stators the mixed level embodiment would be secure until compromise of stators; thereafter solution of wheel order and setting would be comparable to that for a Hebern-type machine with the same number of rotors and the same type motion. No conclusions were reached concerning comparable difficulty of solving rotor wiring.

II. Assuming development of printed circuit cards, issuing a deck of 50 such cards of which 10 could be selected for a daily key, would place solution by means of exhaustive trials beyond any present means. No other solution has been found for mixed level stators. Since stator cards can be changed in 3 minutes, daily change is not impractical.

III. Impracticability of solving stators removes necessity for complicating other elements of the machine. It is conceivable that in the fourth embodiment motion notch patterns be permanently fixed in the rotors and only a settable alphabet ring be added to allow sending indicators in the clear - provided a days traffic is not sufficiently heavy to allow reading depths on frequencies alone. There should be sufficient motion to suppress plain-text characteristics evident from successive encipherments between which there is no motion. Present opinion is that something approximating Orange-type motion would be necessary.

(Studies of SUPERFLEX)

IV. For use in lower echelons a less secure machine could be made to have a Hebern maze with separators varied daily. An adapter which would make this intercommunicable with SUPERFLEX should be feasible.

MARY NEELY ROSEBRO
M.A.C. Subsection

MARY MacNEILL
Cryptographic Plan
Subsection

SNYDER
IMPR.
EMBODI-
MENT

WDGAS 76-C

SECRET

19 September 1947

SUBJECT: SUPERFLEX Commutating Unit

TO : CIC, Projects Section

1. One possible cryptographic weakness of the SUPERFLEX embodiment employing ten printed circuit slides, is suggested by the fact that during an entire daily key setup, any given plain (or cipher) letter remains in direct contact with an associated entry (or exit) point on a particular rotor. The modification proposed herewith is designed to eliminate this weakness, by varying the "plugging" setup during the encipherment of each message, in an unpredictable manner.

2. Instead of having the spring contacts of the reflexing plugboard arranged along a plane surface against which the set of ten printed circuit slides are to make contact, let the spring contacts be arranged in ten pairs of rows around the surface of a bakelite cylinder (Figure 1). Let the plugboard slides be inserted in slots in the inner face of a "sleeve" (Figure 2) which is designed so that points on these slides make good electrical connection with the spring contacts of the cylinder. Motion bumps are provided on the outer surface of the sleeve, to effect its motion; after any step of the sleeve around the cylinder, a complete shift of the ten slides with relation to the spring contacts will have been made. Provision should be made for this motion to be related to the motion control scheme for the rotors themselves, so that it is fairly irregular, and would vary according to different daily key setups, notch rings, etc. Assuming that printed circuit slides can be made approximately the same size as in the original proposal, the whole enciphering process can probably be accomplished within a simple unit similar to that shown diagrammatically in Figure 3.

3. In the design of the plugboard ~~ring~~ sleeve shown in Figure 2, the slides are shown as having a slightly curved face and edges cut at an acute angle. It is felt that this type of slide would lend itself reasonably well to manufacture on a mass-production basis. A process for making printed circuits has been perfected commercially, using steatite; it is felt that this material would be satisfactory for this purpose. One of the best reasons for using that material is the fact that circuits printed on it have shown remarkable resistance to abrasion.

4. Consideration has been given to the idea of using more rotors to effect practically the same result. Such a plan, for example, might employ nine rotors and accomplish "superflexing" to approximately the same extent as the proposed four-rotor version with rotating plugboard ring. This was rejected for the following reasons:

a. One of the powerful arguments for a device like SUPERFLEX has been the fact that a stock of fifty to one-hundred printed-circuit slides would be on hand, from which ten would be selected for the daily key setup.

SECRET

This was felt to be practical because such slides were considered readily producible in large quantities. Also once distributed, they would not have to be reissued, and in fact would hardly have to be classified secret. But preparation and issue of the corresponding numbers of rotors to each holder would probably be prohibitive in expense and bulk.

b. The use of rotors to accomplish the shift of enciphering path from letter to letter is probably weaker cryptographically than the use of a cylinder with slides. The reason is that, using rotors, successive letters will be related in their path because they still contact points on the same rotor. Using the cylinder, with its rotating sleeve, however, each motion brings into position a new circuit.

5. It is felt that use of the device as proposed would be proof in case of capture of the device, provided specific keys are not compromised. It is recommended that the plan of wiring the spring contacts be such as to guarantee a minimum enciphering path of two rotors.

6. It is also to be kept in mind that SUPERFLEX can be fairly easily designed so that its plugging setup, in effect, be altered to convert it to a simple Hebern device with no "reflexing" or "bridging". This might be desirable if it becomes necessary to render it communicable with a device in a lower echelon which is a simple Hebern type machine.

S S Snyder
SAMUEL S. SNYDER
CIC, Cryptographic Plan Subsection

SECRET

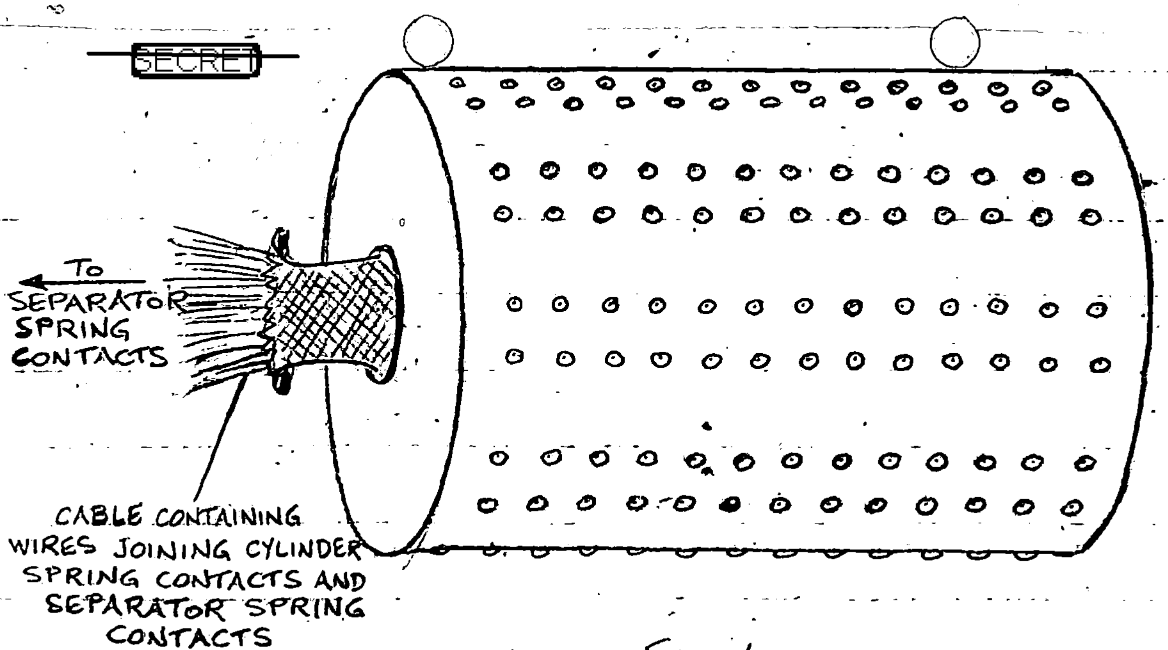
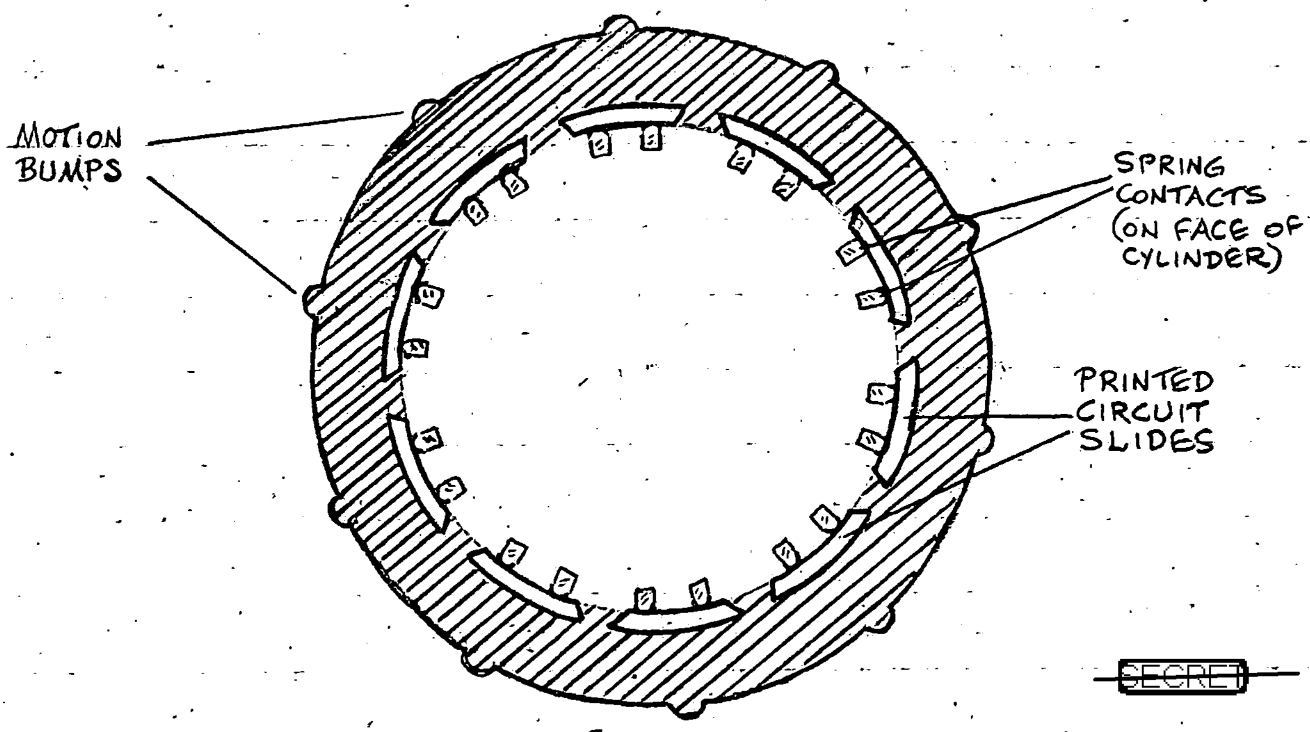


FIG. 1.

COMMUTATING CYLINDER,

SHOWING PAIRED ROWS OF SPRING CONTACTS



SECRET

FIG. 2

COMMUTATING SLEEVE (END VIEW)

SHOWING HOW SPRING CONTACTS OF CYLINDER MAKE ELECTRICAL CONNECTION WITH POINTS ON SLIDES

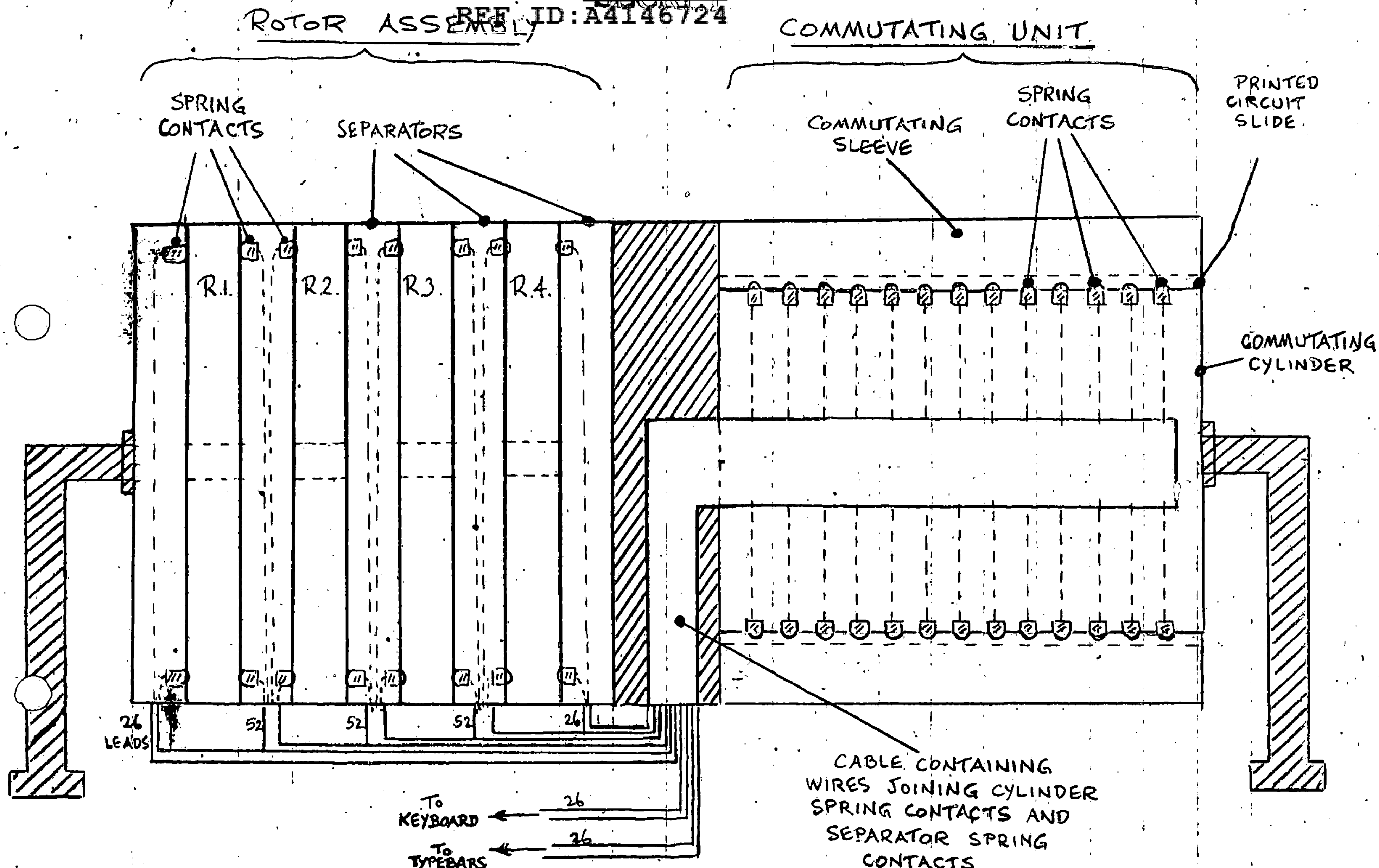


FIG. 3.
(DIAGRAMMATIC) SUPERFLEX ENCIPHERING UNIT - (ACTUAL SIZE)
(MOTION CONTROL MECHANISMS NOT SHOWN)

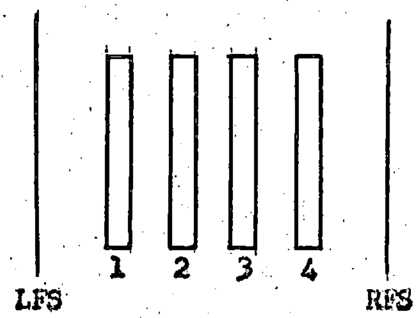
PROB
STUDY
ON
PATHS

WDGAS 76-C 16 September 1947

PROBABILITY OF VARIOUS LENGTH PATHS THROUGH SUPERFLEX

1. Four Rotor Superflex.

Consider a four rotor Superflex (see Mr. Chiles' paper of November 1946 on the Superflex)



where the path LFS to RFS is impossible but any other path is possible. What is the probability that the path of an encipherment goes through one rotor, two rotors, three rotors, etc?

Let us first determine the relative proportion of wires from LFS to Rotors 1, 2, 3, and 4, and from Rotor 1 to Rotor 1, 2, 3, 4, and LFS, etc. We know that LFS may be wired to 1, 2, 3 or 4, and, we assume, with equal probability. Hence we consider $\frac{1}{4}$ of the points of LFS go to Rotor 1, $\frac{1}{4}$ to Rotor 2, $\frac{1}{4}$ to Rotor 3, and $\frac{1}{4}$ to Rotor 4. Now Rotor 1 may be wired to any of the remaining 3/4 of Rotor 1, any of the remaining 3/4 of Rotor 2, any of the remaining 3/4 of Rotor 3, any of the remaining 3/4 of Rotor 4, and to any of RFS. Hence we assume the 26 points of Rotor 1 are wired to Rotors 1, 2, 3, 4, RFS in same proportions as listed above, i.e., 3/16 to Rotor 1, 3/16 to Rotor 2, 3/16 to Rotor 3, 3/16 to Rotor 4, and 4/16 to RFS. By this reasoning we prepare the following table.

WDGAS 76-C (16 September 47)

		Enters				
		1	2	3	4	RFS
	LFS	1/4	1/4	1/4	1/4	0
	1	3/16	3/16	3/16	3/16	1/4
Leaves	2	3/16	3/16	3/16	3/16	1/4
	3	3/16	3/16	3/16	3/16	1/4
	4	3/16	3/16	3/16	3/16	1/4

Table of Probabilities

This table means that the probability of current leaving Rotor 2 going into Rotor 4 is 3/16, going to RFS is 1/4, etc. Incidentally, in our calculations we make the approximation that the probability of a path from any rotor to any other rotor (or to RFS) remains unchanged at each stage. This is not strictly true, since as we fill up more and more points on the rotors, the probabilities of paths change, but the error will be small.

Let us denote by P(i) the probability of the current leaving the machine after passing through i rotors. Then

$$P(1) = 1/4$$

$$P(2) = 3/4 \cdot 1/4$$

$$P(3) = 3/4 \cdot 3/4 \cdot 1/4$$

....

$$P(i) = (3/4)^{i-1}\, 1/4$$

Some values are listed below

P(1) = .2500	P(6) = .0593
P(2) = .1875	P(7) = .0445
P(3) = .1406	P(8) = .0334
P(4) = .1055	P(9) = .0250
P(5) = .0791	etc.

To determine the mean length of path, E(i), we sum i·P(i). Hence

$$E(i) = \sum_{i=1}^{104} i\ P(i).$$

Let us use the infinite sum instead - the difference will be negligible.

Then

$$E(i) = \sum_{i=1}^{\infty} i\ 1/4\ (3/4)^{i-1} = 1/4 \sum_{i=1}^{\infty} i\ f^{\,i-1} \text{ where } f = 3/4.$$

$$\int E(i)\,df = 1/4 \sum_{i=1}^{\infty} f^{i} = 1/4 \left[\frac{1}{1-f} - 1\right]$$

Hence $$\frac{d\left(\int E(i)\,df\right)}{df} = E(i) = 1/4 \frac{1}{(1-f)^2} = 1/4\ \frac{1}{(1-3/4)^2} = 4.$$

Hence E(i) = 4 approximately.

To get $\sigma(i)$, the standard deviation, we first determine $E(i^2)$. By definition

$$E(i^2) = 1/4 \sum_{i=1}^{\infty} i^2 f^{\,i-1} \quad \text{where} \quad f = 3/4.$$

$$\int E\,df = 1/4 \sum_{i=1}^{\infty} i\,f^{i} = 1/4 \sum_{i=1}^{\infty} (i+1)f^{i} - 1/4 \sum_{i=1}^{\infty} f^{i}$$

$$= 1/4 \left[\sum_{i=1} i\,f^{\,i-1} - 1\right] \quad - \quad 1/4 \left[\frac{1}{1-f} - 1\right]$$

$$= 1/4 \left[\frac{1}{(1-f)^2} - 1\right] - 1/4 \left[\frac{1}{1-f} - 1\right] = 1/4 \left[\frac{1}{(1-f)^2} - \frac{1}{1-f}\right]$$

$$\frac{d\left(\int E\,df\right)}{df} = E = 1/4 \left[\frac{2}{(1-f)^3} - \frac{1}{(1-f)^2}\right] = 1/4 \left[2 \cdot 64 - 16\right]$$

$$E(i^2) = 28$$

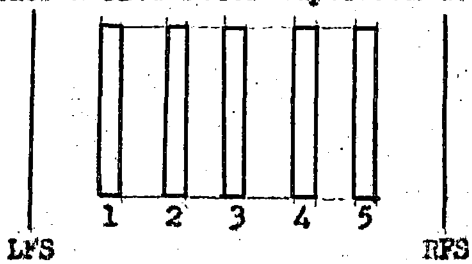
Hence $$\sigma^2 = E(i^2) - \left[E(i)\right]^2 = 28 - 16 = 12 \qquad \sigma = 3.464.$$

WDGAS 76-C (16 September 47)

Since the series was not infinite we drop the 64 and conclude that $\sigma = 3.4$ approximately.

2. Five Rotor Superflex.

Now consider a five rotor Superflex device with the following restrictions:



1. LFS may be wired only to Rotors 1, 2, or 3.

2. Rotor 1 may be wired only to 1, 2, 3, or 4.

3. Rotors 2, and 3 may be wired to 1, 2, 3, 4, or 5.

4. Rotors 4 and 5, may be wired to any rotor or RFS.

With these restrictions we may set up a table of probabilities of current out of LFS or Rotor i going into Rotor j or RFS, as before.

	1	2	3	4	5	RFS
LFS	1/3	1/3	1/3	0	0	0
1	2/9	2/9	2/9	1/3	0	0
2	4/27	4/27	4/27	6/27	1/3	0
3	4/27	4/27	4/27	6/27	1/3	0
4	4/54	4/54	4/54	1/9	1/6	1/2
5	4/54	4/54	4/54	1/9	1/6	1/2

As before, we make the assumption that these probabilities remain unchanged at various stages of the path.

Let us now define this additional symbol:

$P(j,i)$ = probability that current enters Rotor j after it has been through i rotors.

Then we may set up recursive equations as follows: Current may enter RFS from Rotor 4 or Rotor 5 with probability 1/2 each. Stated symbolically:

ADGA 76-C (16 September 47)

$$P(i) = P(4,i-1)\ 1/2 + P(5,i-1)\ 1/2 \quad .$$

Similarly, current may enter Rotor 5 from Rotor 2 with probability 1/3, from Rotor 3 with probability 1/3, from Rotor 4 with probability 1/6, and from Rotor 5 with probability 1/6. Hence:

$$P(5,i) = P(2,i-1)\ 1/3 + P(3,i-1)1/3 + P(4,i-1)\ 1/6 + P(5,i-1)\ 1/6$$

Similarly $P(4,i) = P(1,i-1)\ 1/3 + P(2,i-1)\ 2/9 + P(3,i-1)\ 2/9$

$$+ P(4,i-1)\ 1/9 + P(5,i-1)\ 1/9$$

For $i > 0$

$$P(3,i) = P(1,i-1)\ 2/9 + P(2,i-1)\ 4/27 + P(3,i-1)\ 4/27$$

$$+ P(4,i-1)\ 2/27 + P(5,i-1)\ 2/27$$

$$P(2,i) = P(1,i) = P(3,i)$$

By the use of these recursive equations we build up the following table.

	P(1,i)	P(2,i)	P(3,i)	P(4,i)	P(5,i)	P(i)	Σ P(i)
0	.3333	.3333	.3333	0	0	0	
1	.1729	.1729	.1729	.2592	.2222	0	
2.	.1253	.1253	.1253	.1880	.1955	.2407	
3	.0934	.0934	.0934	.1401	.1475	.1918 -	
4	.0697	.0697	.0697	.1046	.1102	.1438	
5	.0521	.0521	.0521	.0781	.0823	.1074	
6	.0389	.0389	.0389	.0583	.0615	.0802	
7	.0291	.0291	.0291	.0436	.0459	.0599	
8	.0217	.0217	.0217	.0326	.0343	.0448 -	.8238
9	.0162	.0162	.0162	.0243	.0256	.0334 +	
10	.0121	.0121	.0121	.0181	.0191	.0249 +	
11	.0090	.0090	.0090	.0135	.0143	.0186	.9269
12	.0067	.0067	.0067	.0101	.0106	.0139	
13	.0050	.0050	.0050	.0075	.0079	.0104 -	.9697
14	.0038	.0038	.0038	.0056	.0059	.0077	
15	.					.0057 +	
							.9831

Average = 5

$\sigma = 3.3$

WDGAS 76-C (16 September 47)

We then calculate the mean length of path and the standard deviation directly from the values of P(i), getting

$$\text{Mean} = 5 \text{ rotors}$$

$$\sigma = 3.3 \text{ rotors} \quad .$$

FRANK PROSCHAN
Cryptologic Research Subsection

SECUR-
ITY
STUDY

~~SECRET~~

CSGAS-76C

8 October 1947

SUPERFLEX SOLUTION, GUARANTEED TWO ROTOR ENCIPHERMENT

Given: A. 1000 letters of matched plain and cipher text, Figure 1.

B. Rotor wirings and order of rotors:

I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	I	V	O	K	C	U	G	P	F	H	Q	E	T	D	L	Z	X	R	B	M	Y	J	S	A	W	N
II	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	O	Q	P	E	U	J	T	B	F	I	Z	L	G	M	H	R	W	D	N	C	K	X	A	V	S	Y
III	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	J	I	W	H	U	X	M	Q	E	N	D	T	Z	Y	A	B	L	V	S	P	K	G	R	C	F	O
IV	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	N	H	P	D	L	M	F	Y	Z	U	V	Q	B	R	T	C	W	I	A	G	O	K	S	J	E

C. Notch patterns:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
II	X	.	X	.	X	X	.	X	X	X	.	.	.	X	X	.	X	X	.	X	.	X	X	X	X	.
III	X	X	.	.	X	.	.	.	X	X	X	X	.	X	X	X	X	.	X	.	X	.	X	X	X	.
IV	X	X	X	X	X	.	X	.	X	.	X	.	X	.	X	X	X	.	.	.	X	X	X	.	X	.

X = Effective Notch
. = No Effective Notch

D. Initial setting of rotors: A H F S

E. Plugboard: Figure 2.

F. The plugging was such that each letter of plain was guaranteed to be enciphered through at least two rotors. C.C.M. type motion was used in encipherment with rotor IV the fast rotor.

Result: The notch rings were set and the plugging was recovered.

Method of Solution: The matched plain and cipher was written out on a width of 26 (Figure 1) because the fast rotor moved once for each encipherment. Since there were 16 notches on each rotor, rotor III moved 16 times for each complete cycle of the fast rotor. After 13 cycles of the fast rotor, rotor III would have had 8 cycles and the setting of rotors III and IV would have been the same as at the beginning. The setting of rotor III at the beginning of each cycle of rotor IV was known because each notch on rotor IV was active only once.

~~SECRET~~

SECRET

CSGAS-76C (8 October 47)

Figure 1

Setting Rotor IV	1	27	53	79	105	131	157	183	209	235	261	287	313	339	365	391	417	443	469	495	521	547	573	599	625	651	677	703	729	755	781	807	833	859	885	911	937	963	989
S	L	E	T	R	I	R	L	O	M	U	I	I	B	A	B	X	S	X	P	S	Y	R	H	O	S	X	S	L	E	A	X	O	A	E	T	T	X	A	T
	Q	P	Q	L	L	O	D	L	T	Q	M	W	C	L	S	P	U	I	X	Q	Z	G	Q	K	A	G	Y	Y	U	R	I	L	R	W	W	A	Y	R	N
R	O	S	X	M	C	E	E	X	I	C	G	N	R	N	I	M	X	S	L	E	X	S	E	N	P	D	H	E	R	X	A	P	T	M	X	O	Q	P	H
	O	H	U	C	S	L	R	T	R	C	Z	K	R	J	P	T	J	T	K	C	Q	L	N	B	P	P	G	J	P	X	K	C	Y	O	J	O	C	J	S
Q	N	X	R	E	H	A	X	M	C	H	H	E	I	D	L	I	O	X	I	L	F	X	X	X	R	E	X	E	N	G	X	L	I	E	Z	X	U	E	E
	Z	G	P	F	R	X	R	F	J	A	N	A	X	Z	E	K	Y	L	B	G	L	D	L	Y	X	K	V	J	N	K	E	K	P	H	J	E	D	F	C
P	D	S	E	D	X	C	A	E	X	X	T	T	T	X	L	L	F	E	E	L	I	F	S	S	E	N	T	X	M	E	N	E	V	R	X	A	E	R	X
	M	B	G	X	N	I	G	K	L	N	C	T	G	L	Z	N	H	Y	M	V	H	F	K	Q	V	S	B	R	M	Q	X	X	F	X	N	G	G	Y	W
O	O	A	D	X	C	H	S	E	C	A	X	X	I	D	I	L	X	C	D	I	N	O	X	T	A	I	H	A	E	N	E	X	E	G	A	X	S	X	H
	Z	G	E	V	L	O	X	V	Z	L	P	Q	F	W	A	Z	B	J	L	N	P	A	T	K	N	V	A	G	J	D	N	G	B	X	D	Y	R	L	Z
N	N	I	U	F	O	I	X	T	R	N	B	D	A	O	O	I	T	O	X	N	A	R	F	O	D	E	A	P	N	E	W	O	X	E	T	R	T	R	O
	S	G	I	Q	D	N	U	R	V	T	K	O	B	H	X	R	T	A	G	A	U	X	Z	I	R	C	N	M	F	B	Z	Z	F	Z	S	O	Y	R	E
M	X	D	C	O	U	N	A	X	I	X	E	E	N	L	N	O	H	N	C	G	N	X	U	C	X	D	T	O	T	R	X	R	P	N	T	O	I	E	U
	H	R	Z	D	B	B	N	C	V	U	M	K	J	U	U	H	Y	R	L	X	T	Y	O	U	J	S	X	U	T	O	D	N	H	G	J	P	S	W	J
L	A	X	E	R	L	G	X	A	S	A	X	C	X	L	X	N	E	O	O	X	C	T	T	K	A	X	X	S	X	A	M	X	A	C	L	U	O	P	S
	X	I	D	H	W	D	Z	P	C	V	M	H	V	L	I	L	K	F	E	Z	A	V	F	K	W	V	C	Z	P	A	Q	B	S	L	E	Z	P	B	K
K	U	T	X	C	D	X	W	X	I	C	C	I	A	A	F	X	X	M	M	C	I	H	U	X	G	A	P	T	M	L	A	I	R	Y	E	T	N	O	E
	J	X	W	Y	V	P	K	Y	U	B	H	A	P	B	R	A	Y	N	N	U	A	E	I	M	J	M	A	W	H	Z	T	P	G	N	T	S	D	G	C
J	T	O	T	E	X	E	O	P	S	T	O	S	P	R	I	D	N	I	M	O	A	E	R	M	A	U	R	R	I	X	N	N	T	X	E	I	X	R	X
	Y	J	X	W	T	F	Y	S	J	S	E	D	S	I	Y	G	X	G	N	S	G	N	O	K	A	G	I	T	I	N	L	I	I	D	U	N	F	F	M
I	H	D	H	S	H	F	R	R	X	I	U	I	O	X	V	O	A	C	A	M	L	X	E	A	I	T	I	O	G	E	D	V	Y	C	X	N	B	T	O
	F	H	C	W	S	G	H	C	P	R	H	X	I	X	F	M	O	M	W	Q	T	C	K	D	E	P	D	X	Y	B	T	Z	U	L	C	I	V	O	L
H	O	A	E	X	A	F	L	O	T	O	P	O	S	R	E	L	T	X	X	M	X	N	X	R	N	H	M	P	H	L	A	I	X	O	C	E	A	X	F
	U	R	L	X	E	Z	D	T	K	N	N	R	T	X	V	M	F	E	E	O	M	L	W	S	V	Z	P	L	N	E	S	F	D	A	K	Z	I	F	G
G	R	Y	X	D	V	E	D	S	H	N	L	N	T	E	X	L	I	T	A	A	W	A	C	K	X	O	E	H	T	E	T	T	T	A	O	X	S	C	X
	W	B	Q	F	O	C	N	I	N	P	G	P	I	S	D	M	Q	S	T	E	F	T	O	F	N	S	Y	S	B	N	C	T	O	E	H	P	A	C	Q

SECRET

Figure 1 - Continued

Setting Rotor IV	14	40	66	92	118	144	170	196	222	248	274	300	326	352	378	404	430	456	482	508	534	560	586	612	638	664	690	716	742	768	794	820	846	872	898	924	950	976
F	I	X	S	A	E	C	Z	P	I	X	E	X	R	S	H	A	O	R	X	X	Q	T	O	E	D	R	X	F	X	C	E	E	O	L	M	P	E	O
	D	D	F	Z	O	B	T	W	B	Y	V	G	G	U	G	K	W	Z	J	L	J	M	P	X	E	C	Q	W	L	O	W	W	S	P	W	R	W	B
E	T	B	I	S	X	T	P	E	S	U	D	T	O	E	U	R	N	O	N	A	I	I	M	T	A	I	M	X	E	T	X	X	Z	I	M	A	D	M
	Z	P	J	S	H	G	N	R	U	D	T	K	E	N	B	A	B	U	K	T	J	W	U	Q	M	E	J	Z	K	I	I	Q	K	A	P	X	N	X
D	A	R	Z	H	F	S	O	C	X	L	X	O	P	R	N	S	X	U	E	T	T	O	M	S	S	T	I	S	I	J	F	T	J	T	A	R	X	M
	L	S	W	S	S	A	W	D	G	U	Q	J	G	Z	S	R	Q	E	F	M	V	I	W	B	X	L	V	M	V	C	X	D	Q	Y	J	T	B	X
C	T	I	E	X	A	X	W	T	W	T	W	X	H	V	D	X	A	B	W	T	E	N	A	X	H	A	N	K	T	O	R	H	O	I	X	L	O	A
	Y	V	Z	S	A	L	P	K	I	K	J	O	R	S	X	N	V	Y	O	B	J	G	G	L	A	Z	L	E	Y	K	Q	W	J	F	X	C	I	J
B	I	T	X	A	R	O	B	I	I	I	I	D	E	E	H	Z	P	L	X	R	E	X	K	Z	X	T	I	L	H	N	O	E	I	O	R	I	N	Z
	X	Q	H	Y	O	Q	Q	P	N	G	W	U	T	G	M	U	B	F	R	O	H	D	R	D	M	F	E	G	M	A	Q	V	P	L	K	T	Y	D
A	V	I	O	X	X	N	R	V	N	M	T	I	X	X	E	X	O	E	W	I	S	A	H	X	A	I	S	A	E	X	M	X	N	N	E	A	X	S
	X	J	E	F	X	K	Y	O	C	I	U	K	Z	L	U	T	R	U	O	A	E	H	G	S	Z	B	O	Z	N	X	Q	B	Z	B	F	S	P	B
Z	E	A	F	S	H	X	X	F	T	A	H	F	S	O	D	A	S	S	A	B	X	P	I	N	H	V	T	B	A	T	X	C	X	X	P	M	A	A
	O	B	I	W	D	S	R	W	H	H	T	F	D	G	Q	N	R	O	B	P	O	K	V	O	H	U	C	S	O	F	G	S	E	K	K	K	H	K
Y	X	N	X	T	Y	H	D	X	E	T	X	X	X	F	X	S	T	X	V	U	T	O	T	U	D	E	E	O	X	O	T	O	I	C	L	E	X	I
	H	O	J	H	J	J	H	N	R	Y	F	F	I	E	C	P	H	H	F	X	Z	H	Q	N	X	D	W	S	J	V	V	E	A	N	P	M	F	W
X	S	X	H	E	P	E	A	E	R	E	A	I	O	X	S	K	R	M	E	T	O	S	Y	M	X	L	R	R	C	X	H	H	N	A	Y	N	N	D
	O	K	J	H	E	L	J	E	O	X	Q	W	D	Q	A	B	E	G	I	X	X	O	Z	R	D	F	S	C	A	P	G	C	I	J	G	K	M	Z
W	O	M	E	P	H	R	S	C	X	L	X	N	O	T	I	S	O	U	X	E	X	T	L	O	W	Y	X	X	A	S	E	S	X	B	I	T	E	X
	L	U	J	N	W	Y	N	N	B	B	T	H	L	B	Q	H	C	N	D	O	W	F	I	J	D	D	U	J	I	S	V	C	V	R	O	K	C	A
V	U	I	R	X	E	X	H	O	Z	Y	C	T	L	E	X	I	P	L	O	D	F	R	O	R	E	X	A	G	L	E	X	E	A	I	N	A	W	I
	C	Y	Y	D	M	G	V	A	A	R	K	C	K	W	C	V	C	Y	E	C	U	X	M	M	J	F	K	E	Y	E	B	K	S	O	H	T	Z	V
U	R	G	X	W	N	R	X	N	X	X	A	O	D	O	T	G	H	T	F	X	E	O	N	S	R	D	T	O	L	E	P	E	N	S	G	R	S	N
	I	C	G	O	Y	R	F	Y	Z	X	Z	R	E	B	Z	H	G	P	G	M	C	A	H	V	T	U	Z	D	T	N	K	D	X	M	P	X	P	S
T	C	H	A	H	X	O	T	O	S	M	B	X	X	X	Y	N	F	I	X	B	A	P	D	X	E	A	T	V	X	K	E	V	X	E	X	Y	P	X
	O	K	R	R	L	Y	E	V	P	I	U	S	L	R	I	C	L	U	T	K	C	U	B	G	Z	F	K	P	V	A	W	E	X	W	O	M	Q	H

SECRET

CSGAS-76C (8 October 47)

Figure 2

PLUGBOARD

1		2		3		4		5		6		7		8		9		10	
I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II
A	A	B	B	C	C	D	D	A	B	B	A	D	A	C	B	B	C	A	D
LFS	1	LFS	1	LFS	1	LFS	1	1	2	1	2	2	RFS	2	RFS	2	RFS	2	RFS
F	E	E	F	G	G	H	H	U	D	V	C	H	E	G	F	F	G	E	H
LFS	1	LFS	1	LFS	1	LFS	1	1	2	1	2	2	RFS	2	RFS	2	RFS	2	RFS
I	I	J	J	K	K	L	L	W	F	X	E	L	I	K	J	J	K	I	L
LFS	1	LFS	1	LFS	1	LFS	1	1	2	1	2	2	RFS	2	RFS	2	RFS	2	RFS
M	M	N	N	O	O	P	P	Y	H	Z	G	P	M	O	N	N	O	M	P
LFS	1	LFS	1	LFS	1	LFS	1	1	2	1	2	2	RFS	2	RFS	2	RFS	2	RFS
Q	Q	R	R	S	S	T	T	A	Z	B	Y	T	Q	S	R	R	S	Q	T
LFS	1	LFS	1	LFS	1	LFS	1	4	3	4	3	2	RFS	2	RFS	2	RFS	2	RFS
U	U	V	V	W	W	X	X	C	X	D	W	X	U	W	V	V	W	U	X
LFS	1	LFS	1	LFS	1	LFS	1	4	3	4	3	2	RFS	2	RFS	2	RFS	2	RFS
Y	B	Z	A	H	Y	G	Z	F	V	E	U	B	T	A	S	Z	Y	Y	Z
LFS	4	LFS	4	4	1	4	1	4	3	4	3	3	3	3	3	2	RFS	2	RFS
C	C	D	D	E	E	F	F	G	N	H	M	F	L	E	K	D	J	C	I
1	4	1	4	1	4	1	4	1	2	1	2	3	2	3	2	3	2	3	2
I	O	J	H	K	I	L	J	M	T	N	S	J	R	I	Q	H	P	G	O
1	4	1	4	1	4	1	4	1	2	1	2	3	2	3	2	3	2	3	2
O	K	P	L	Q	M	R	N	S	Z	T	Y	N	X	M	W	L	V	K	U
1	4	1	4	1	4	1	4	1	2	1	2	3	2	3	2	3	2	3	2
I	O	J	P	K	Q	L	R	M	R	N	Q	R	P	Q	O	P	N	O	M
4	4	4	4	4	4	4	4	4	3	4	3	3	3	3	3	3	3	3	3
T	S	S	T	R	U	Q	V	P	L	O	K	V	J	U	I	T	H	S	G
4	4	4	4	4	4	4	4	4	3	4	3	3	3	3	3	3	3	3	3
Z	W	Y	X	X	Y	W	Z	V	F	U	E	Z	D	Y	C	X	B	W	A
4	4	4	4	4	4	4	4	4	3	4	3	3	3	3	3	3	3	3	3

I = Output
II = Input
1 = Rotor I
2 = Rotor II

LFS - Left Fixed Sequence
RFS - Right Fixed Sequence
3 - Rotor III
4 - Rotor IV

In each of the 10 boxes any one of the 13 outputs may be plugged to any of the 13 inputs in that box.

SECRET

CSGAS-76C (8 October 47)

The matched plain and cipher at each setting of rotor IV was examined at an interval of 13 for hits. Ten such hits were found.

Hit	Positions	Setting of Rotor IV
$X_p = I_c$	443 - 781	S
$A_p = G_c$	31 - 707	O
$X_p = I_c$	34 - 372	L
$X_p = Z_c$	164 - 502	L
$X_p = V_c$	320 - 658	L
$R_p = I_c$	348 - 686	J
$P_p = K_c$	566 - 904	Z
$X_p = J_c$	73 - 749	Y
$T_p = H_c$	99 - 473	Y
$X_p = F_c$	281 - 957	Y

These hits were assumed to have been caused by encipherment through rotors III and IV once each. The hits $X_p = I_c$ which appeared at settings S and L were examined first. It was assumed that these must be caused by parallel wires in rotor IV and rotor III being at the same setting, or different outputs from rotor IV and different settings of rotor III. Examination of possible inputs of X from the L.P.S. to rotor IV at the two designated settings and possible outputs from rotor IV which could be plugged directly to an entrance point of rotor III was made.

Possible Pluggings of X on L.P.S. to Rotor IV	P	J	N	R	V	Z
Output of Rotor IV						
Setting L	<u>B</u>	Z	X	<u>F</u>	J	L
Setting S	<u>I</u>	<u>V</u>	<u>P</u>	<u>G</u>	J	W

At setting L of rotor IV, if X on the L.P.S. is plugged to input P of rotor IV, the output from rotor IV is at B, and at setting S, the output is at I. The underlined letters are outputs from rotor IV which can be plugged directly to inputs of rotor III. No possible input of X to rotor IV has outputs from rotor IV at both settings, L and S, which can be directly plugged to rotor III so the first assumption was incorrect.

Another hit, $P_p = K_c$ at setting Z of rotor IV, was chosen for examination as a single $P_p = K_c$ occured at position 805 setting U of rotor IV.

Possible Pluggings of P on L.F.S. to Rotor IV	F	J	N	R	V	Z	
Output of Rotor IV							
Setting U	P	K	I	L	J	V	
Setting Z	A	T	H	N	L	J	

If P on the L.F.S. was plugged to input F on rotor IV, the output from rotor IV at settings U and Z could both be plugged directly to an entrance point of rotor III.

Another hit, $A_P = G_C$ at setting O of rotor IV, was examined together with other $A_P = G_C$ at positions 160 and 914 with setting P of rotor IV, at position 530 with setting J of rotor IV, at position 589 with setting C of rotor IV, and at position 546 with setting T of rotor IV.

Possible Pluggings of A on L.F.S. to Rotor IV	B	C	G	K	O	S	W
Output of Rotor IV							
Setting O	P	Y	W	U	C	G	I
Setting P	X	Z	W	U	P	N	Q
Setting J	N	W	U	G	R	E	Y
Setting C	C	X	Q	E	K	I	G
Setting T	R	S	Q	L	J	M	K

There were 3 possible pluggings of A on the L.F.S. to rotor IV (B, K, and S) which would give outputs at 3 of the 5 settings which could be directly plugged to an entrance point on rotor III.

First, A on the L.F.S. was assumed plugged to input K on rotor IV, so that the output from rotor IV at both settings O and P would be U. Table I was made to show the setting of rotor III at positions 31, 160, 914 and 589, assuming all possible settings of the notch ring on rotor IV. Figure 3 shows the possible inputs to rotor III from output U on rotor IV and the exit points from rotor III which can be plugged directly to G on the R.F.S. at each of the possible settings of rotor III. Since, from Table I, position 31 and 160 could not have the same settings of rotor III, there was no possible plugging of output U on rotor IV to an input of rotor III which could make $A_P = G_C$ at positions 31 and 160 or 914 two rotor encipherments.

CSGAS-76C (8 October 47)

Figure 3.

Possible Settings of Rotor III at Position		Possible Pluggings of Output U on Rotor IV to an Input on Rotor III: E	K	Q	U	W	Y
31 & 707	L	-	-	-	-	-	P
	M	-	-	L	-	P	-
	N	-	-	X	-	-	D
	O	-	-	-	-	-	-
160	K	P	-	-	-	L	-
	L	-	-	-	-	-	P
	M	-	-	L	-	P	-
	N	-	-	X	-	-	D
914	O	-	-	-	-	-	-
	P	-	X	-	L	-	-
	Q	-	-	-	-	-	-
	R	-	-	-	-	-	-

CSGAS-76C (8 October 47)

TABLE I

Possible Notch Ring Settings on Rotor IV at Beginning of Message	Settings of Rotor III at Positions 31	160	914	530	589	805	904
1	N	L	P	S	I	F	W
2	M	L	P	R	H	F	W
3	M	K	O	Q	H	F	V
4	L	K	O	Q	G	E	V
5	L	K	O	Q	G	E	U
6	M	L	P	R	H	E	V
7	M	L	P	Q	H	E	U
8	N	M	Q	R	H	E	V
9	N	L	P	Q	G	E	V
10	N	M	Q	R	G	E	W
11	N	L	P	R	G	E	V
12	N	M	Q	S	H	E	V
13	N	L	P	S	H	E	V
14	N	M	Q	T	H	F	V
15	N	L	P	S	H	F	V
16	M	L	P	S	G	E	V
17	M	K	O	R	G	D	U
18	M	L	P	S	H	D	V
19	N	M	Q	S	I	E	V
20	O	N	R	T	J	F	W
21	O	M	Q	S	J	F	W
22	N	L	P	S	I	E	W
23	M	K	O	R	I	E	W
24	M	L	P	S	I	E	X
25	M	L	P	S	I	E	W
26	N	M	Q	T	I	F	X

Next, A on the L.F.S. was assumed plugged to input B on rotor IV so that at setting O the output from rotor IV was at P. This was the same output as when P on the L.F.S. was plugged to F on rotor IV at setting U. Table I was extended to show the settings of rotor III at positions 530, 589, 805, and 904, assuming all possible settings of the notch ring on rotor IV. Figure 4 shows the possible inputs to rotor III from rotor IV and the exit points from rotor III which can be plugged directly to G or K on the R.F.S. at each of the possible settings of rotor III. The $A_P = G_C$ at position 589 was not consistent with $A_P = G_C$ at positions 31 and 530 and $P_P = K_C$ at positions 805 and 904. Therefore, it was assumed that $A_P = G_C$ at positions 589 was not a two rotor encipherment. From Figure 4, the output P on rotor IV was assumed plugged to input X on rotor III and output A on rotor IV plugged to input R on rotor III. G on the R.F.S. would be plugged to output H on rotor III and K on the R.F.S. would be plugged to output L of rotor III.

Figure 4.

Possible Settings of Rotor III at Position / Possible Pluggings of Output P on Rotor IV to an Input on Rotor III

Position	Setting	F	L	R	V	X	Z
31 & 707	L	-	-	-	-	-	-
	M	-	T	-	-	-	-
$A_P = G_C$	N	-	-	-	-	H	T
	O	X	-	-	-	-	-
805	D	-	-	-	-	L	-
$P_P = K_C$	E	-	P	-	-	L	-
	F	P	-	X	-	-	D

Possible Pluggings of Output N on Rotor IV to an Input on Rotor III

Position	Setting	E	K	Q	U	W	Y
530	Q	-	-	-	-	-	-
	R	-	-	-	-	-	-
$A_P = G_C$	S	-	-	-	-	H	P
	T	-	-	H	-	-	D

Possible Pluggings of Output C on Rotor IV to an Input on Rotor III

Position	Setting	F	L	R	V	X	Z
589	G	-	-	-	-	-	-
	H	-	D	-	-	-	-
$A_P = G_C$	I	-	L	-	-	-	-
	J	-	-	-	-	-	-

Possible Pluggings of Output A on Rotor IV to an Input on Rotor III

Position	Setting	F	L	R	V	X	Z
904	U	-	-	-	-	-	-
	V	T	-	L	-	X	-
$P_P = K_C$	W	T	H	-	-	P	-
	X	-	-	-	-	H	-

Also from Figure 4, the setting of rotor III at position 31 must be N, at position 805 E or D, at position 530 S or T, and at position 904 V. All settings of the notch ring on rotor IV were eliminated which produced other settings of rotor III at those positions. The notch ring on rotor IV could be set at position 12 or 19 at the beginning of the message. Also at position 805 the setting of rotor III would be at E and at position 530 the setting of rotor III would be at T which would cause the output of N on rotor IV to be plugged to input W on rotor III. These assumptions were tested on position 328, setting D of rotor IV where $P_P = G_C$. At this setting if P of the L.F.S. was plugged to input F of rotor IV, the output was P of rotor IV which was assumed plugged to input X on rotor III. If the notch ring on rotor IV was set at position 12 at the beginning of the message, rotor III would be at setting M at position 328. At setting M of rotor III an input at X would give an output at O. If the notch ring on rotor IV was set at position 19 at the beginning of the message, rotor III would be at setting N at position 328. At setting N of rotor III an input at X gave an output at H. It had been assumed that G on the R.F.S. was plugged to output H on rotor III so that assumption was confirmed and the setting of the notch ring on rotor IV was 19 at the beginning of the message. Position 982, $A_p = K_c$, at setting Z on rotor IV gave an output at U on rotor IV when A of the L.F.S. entered rotor IV at B. Since it was assumed that the notch ring on rotor IV was at 19 at the beginning of the message, rotor III would be at setting Z at position 982. If the output of rotor IV at U was plugged to input E on rotor III, the output of III at setting Z would be K. From the plugboard it was possible for output U on rotor IV to be plugged to input E on rotor III. Thus it was assumed that the reasoning thus far was correct and the setting of rotor III for each position was written out.

Hits of $X_p = L_c$ appeared at positions 445 and 575, setting Q of rotor IV; at positions 212 and 342, setting P; at positions 508 and 742, setting F; at positions 147 and 615, setting G; and positions 130 and 338, setting T. These were assumed possible 2 rotor encipherments through rotors II and IV. A single $X_p = L_c$ appeared at setting O, position 967 and also at setting A, position 357.

Output of Rotor IV Possible Inputs of X from L.F.S. to Rotor IV

Setting	J	N	R	V	Z
Q	T	O	M	P	N
P	T	B	F	H	G
G	D	B	N	Y	L
T	X	B	D	G	E
F	Q	S	M	O	U
O	M	Z	T	K	N
A	Y	B	H	L	J

It was assumed that X on the L.F.S. was plugged to input N of rotor IV since four of the seven settings at which $X_p = L_c$ gave output at B of rotor IV which could be plugged directly to an input of rotor II. The setting of rotor II at these positions was assumed to be the same or to have parallel wires effective.

It was noted that $X_p = L_{cc}$ which occurred at positions 338 and 342, settings T and P respectively, could have the same setting of rotor II if F on rotor III had no effective notch. This was assumed to be true and so limited the possible settings of the notch ring on rotor III to 10. Namely, F set at 3, 4, 6, 7, 8, 13, 20, 22, or 26. Table II showed that there were 7 to 12 possible changes of setting of rotor II between positions 342 and 357, depending upon the setting of the notch pattern on rotor III.

Figure 5 showed that there were no settings of rotor II at an interval of 7, 8, or 11 which would allow $X_P = L_C$ at positions 342 and 357 to be 2 rotor encipherments. At an interval of 9 there were 7 possible settings of rotor II which would allow $X_P = L_C$ at positions 342 and 357 to be 2 rotor encipherments. At an interval of 10 there were 2 possible settings of rotor II and also 2 at an interval of 12. These were as follows:

TABLE II

Position in Message	Setting of Rotor III	Setting of Notch Ring on F of Rotor III									
		3	4	6	7	8	13	18	20	22	26
338	F	.	.	.	.	.	.	.	.	.	.
339	F	.	.	.	.	.	.	.	.	.	.
340	F	.	.	.	.	.	.	.	.	.	.
341	F	.	.	.	.	.	.	.	.	.	.
342	E	X	.	X	.	.	X	X	X	X	X
343	D	X	X	.	X	.	X	X	.	.	X
344	C	.	X	.	.	X	X	X	X	X	X
345	C	.	X	.	.	X	X	X	X	X	X
346	B	X	.	X	.	.	X	X	X	.	.
347	B	X	.	X	.	.	X	X	X	.	.
348	A	X	X	X	X	.	.	.	X	X	X
349	A	X	X	X	X	.	.	.	X	X	X
350	Z	X	X	.	X	X	.	X	X	X	.
351	Z	X	X	.	X	X	.	X	X	X	.
352	Y	.	X	X	.	X	.	X	.	X	X
353	Y	.	X	X	.	X	.	X	.	X	X
354	X	X	.	X	X	.	X	X	X	X	.
355	W	.	X	X	X	X	.	X	X	.	X
356	V	X	.	.	X	X	.	.	X	X	X
	Total Changes -	10	10	9	8	8	7	12	12	11	10

Figure 5.

Setting of Rotor II	Input to Rotor II Which Can Be Plugged to Output B or Rotor IV	Output From Rotor II Which Can Be Plugged to L on the R.F.S.
A	G	M
	S	Y
B	C	Q
C	M	Y
	Y	U
D	S	U
	Y	E

CSGAS-76C (8 October 47) Figure 5 (Continued)

Setting of Rotor II	Input to Rotor II Which Can Be Plugged to Output B of Rotor IV	Output From Rotor II Which Can Be Plugged to L on the R.F.S.
E	C	I
	G	Q
	S	M
F	E	A
	S	Q
	Y	M
G	-	-
H	C	Y
	E	E
I	C	M
	Y	E
J	S	Y
K	E	Q
L	A	A
	G	E
	Y	U
M	G	M
	Y	I
N	Y	Y
O	A	M
	G	Q
	M	I
	S	Y
P	C	A
	A	I
Q	C	I
	G	A
R	A	Y
	G	E
	M	A
S	C	M
	E	Y

CSGAS-76C (8 October 47) Figure 5 (Continued)

Setting of Rotor II	Input to Rotor II Which Can Be Plugged to Output B of Rotor IV	Output From Rotor II Which Can Be Plugged to L on the L.F.S.
T	C	E
U	Y	E
V	C	A
	G	M
W	A	U
	E	A
	S	E
	Y	I
X	A	Y
	G	U
	M	I
	Y	A
Y	C	Y
Z	C	I
	M	M
	S	Q

At an Interval of 9

Setting of Rotor II Position 342	Setting of Rotor II Position 357	Input to Rotor II To Which Output B On Rotor IV is Plugged	Output of Rotor II To Which L on R.F.S. is Plugged
D	U	Y	E
F	W	E	A
H	Y	C	Y
J	A	S	Y
L	C	Y	U
V	M	G	M
Z	Q	C	I

At an Interval of 10

E	O	G	Q
W	M	Y	I

At an Interval of 12

A	O	S	Y
U	I	Y	E

The six possible settings of the notch ring on rotor IV which would allow 9, 10, or 12 changes of setting on rotor II between positions 342 and 357 were tested on positions 130 and 147. Table III showed that the number of changes of setting between positions 130 and 147 could be 9, 11, 12, 13, or 14. Using Figure 5 it was found that there were no settings of rotor II at an interval of 11 or 13 which would allow $X_p = L_c$ at positions 130 and 147 to be 2 rotor encipherments. At an interval of 9 and 12 the same settings and pluggings were possible as were possible ~~as were~~

TABLE III

Position in Message	Setting of Rotor III	Setting of Notch Ring on F of Rotor III: 3	4	6	18	20	26
130	D	X	X	.	X	.	X
131	D	X	X	.	X	.	X
132	D	X	X	.	X	.	X
133	D	X	X	.	X	.	X
134	C	.	X	.	X	X	X
135	B	X	.	X	X	X	.
136	A	X	X	X	.	X	X
137	A	X	X	X	.	X	X
138	Z	X	X	.	X	X	.
139	Z	X	X	.	X	X	.
140	Y	.	X	X	X	.	X
141	Y	.	X	X	X	.	X
142	X	X	.	X	X	X	.
143	X	X	.	X	X	X	.
144	W	.	X	X	X	X	X
145	W	.	X	X	X	X	X
146	V	X	.	.	.	X	X
	Total Changes -	12	13	9	14	11	12

~~possible~~ between positions 342 and 357. At an interval of 14 the following settings and pluggings were possible.

Setting of Rotor II Position 130	Setting of Rotor II Position 147	Input to Rotor II to Which Output B On Rotor IV is Plugged	Output of Rotor II To Which L on R.F.S. is Plugged
A	M	G	M
E	Q	C	I
I	U	Y	E
A	O	S	Y

If the notch ring of rotor III was set so that 3 was on F, there were 10 changes of setting of rotor II between positions 338 and 357 and 12 changes of setting of rotor II between positions 130 and 147. The intervals of 10 and 12 had no settings which would allow the same plugging of output B on rotor IV to an input of rotor II and L on the R,F.S. plugged to the same output of rotor II. The same was true for position 26 on the notch ring. Position 6 of the notch ring was possible because the number of changes of setting between positions 338 and 357 and positions 130 and 147 were both 9 and the settings could be identical for each pair. Position 18 was also possible because there were 12 changes of setting between positions 338 and 357 and 14 changes of setting between positions 130 and 147 and the intervals 12 and 14 had one setting and plugging in common. Namely, rotor II would have to be at setting A for positions 338 and 130 and at setting O for positions 357 and 147. However, this was impossible. When the setting of the notch ring on rotor III was assumed as position 18 at F and the motion was followed through from the beginning of the message, position 130 was at setting F.

When the setting of the notch ring on rotor III was assumed as position 6 at F, the setting of rotor II at position 130 was L. This setting was possible and so was assumed correct. Therefore, output B on rotor IV was plugged to input Y on rotor II and output U on rotor II was plugged to L on the R.F.S. At positions 212, 338, and 342, rotor II was at position L and at positions 147, 357, and 615, rotor II was at position C. In all six positions X_p was enciphered through the same path of rotors II and IV.

Other pluggings were placed by assuming the following plain to be two or three rotor encipherments.

Plain	Cipher	Position	Settings II	III	IV	Plugging Output	Assumed Input
X	L	445	D	T	Q	O - IV	S - II
		575	D	R	Q		
X	E	783	H	T	Q	D - II	E - R.F.S.
		913	H	R	Q		
X	R	159	T	N	Q	S - II	R - R.F.S.
X	Y	601	M	B	Q	R - II	Y - R.F.S.
X	R	706	Y	O	P	S - II	R - R.F.S.
X	N	108	Z	S	P	W - II	N - R.F.S.
		238	Z	Q	P		
X	N	888	T	G	P	W - II	N - R.F.S.
X	N	407	Z	Q	C	W - II	N - R.F.S.
X	W	992	J	U	P	F - II	W - R.F.S.
X	O	303	H	C	C	B - II	O - R.F.S.
X	O	910	H	R	T	B - II	O - R.F.S.
X	X	901	N	Y	C	Y - II	X - R.F.S.
X	S	617	B	Q	A	J - II	S - R.F.S.
X	P	97	F	Y	A	M - II	P - R.F.S.
		955	F	Q	A		
X	T	409	X	O	A	A - II	T - R.F.S.
X	E	95	G	A	C	X - II	L - II
X	E	719	O	G	C	Z - II	P - II
X	H	988	J	V	T	F - II	H - R.F.S.
R	T	926	X	J	D	R - L.F.S.	A - IV
R	O	122	O	J	B	M - IV	D - II
		512	O	D	B		

CSGAS-76C (8 October 47)

Plain	Cipher	Position	Settings II	Settings III	Settings IV	Plugging Output	Assumed Input
R	I	348	I	A	J	F - III	I - R.F.S.
		686	M	A	J		
X	I	443	D	T	S	O - III	M - III
		781	H	T	S		
R	S	42	G	H	D	X - II	L - II
R	F	972	R	C	J	E - III	F - R.F.S.
R	G	841	W	J	K	O - II	C - III
A	B	46	F	D	Z	A - III	B - R.F.S.
A	B	488	E	R	Z	A - III	B - R.F.S.
A	H	956	E	P	Z	W - III	H - R.F.S.
A	H	254	N	F	Z	V - III	D - III
A	N	410	W	N	Z	J - III	R - II
X	H	70	U	P	B	W - III	H - R.F.S.
X	R	486	F	T	B	M - III	Q - II
X	R	590	R	H	B	J - III	R - II
X	D	564	I	X	B	S - III	D - R.F.S.
X	P	391	H	Z	S	D - III	V - II
X	Y	937	S	B	S	M - III	Q - II

There was one inconsistency in the preceding assumptions. $X_p = W_c$ at position 992 gave the output of F on rotor II as plugged to W on the R.F.S. $X_p = H_c$ at position 988 gave the output F on rotor II as plugged to H on the R.F.S. Since this was impossible, these positions were not two rotor enciphermernts and output F could not be plugged to any letter on the R.F.S.

In the matched plain and cipher there were four instances where two consecutive plain letters were identical and the cipher letters were identical. These were $L_p = M_c$ at positions 402 and 403, $M_p = N_c$ at positions 477 and 478, $E_p = J_c$ at positions 704 and 705, and $M_p = X_c$ at positions 977 and 978. These were assumed to be 2 rotor encipherments through rotors I and II and that the rotors had not moved between the 1st and 2nd encipherment of each hit. When the settings of rotor II were inspected to see if rotor II had remained stationary at these consecutive positions, it was found that it had remained stationary at B for positions 402 and 403 and stationary at M for positions 477 and 478, but had moved between positions 704 and 705 and positions 977 and 978. It was then assumed that the notch ring on rotor II was set so that B and M had no effective notch so that rotor I would remain stationary between positions 402 and 403 and positions 477 and 478. When the notch pattern was examined to see if the notch ring could be set so that both B and M could have no effective notch, it was found that there were three possible settings of the notch ring. B could be at setting 2, 19, or 26 of the notch ring.

The matched plain and cipher was rewritten so that the positions enciphered at each setting of rotor II were written together. Figure 6 shows the positions enciphered at setting M and I of rotor II.

CSGAS-76C (8 October 47)

Figure 6.

Setting M

Position	36	80	124	125	126	127	128	129	167	207	257	291	335	378	427	476	477	478	516	559	601	639	686	727	774	820	859	902	944	985
Plain	O	M	H	Y	P	H	E	N	R	N	L	X	O	H	A	O	M	M	T	A	X	A	R	O	T	E	E	R	O	X
Cipher	J	C	D	J	E	W	M	Y	H	Y	B	Q	L	G	O	E	N	N	A	T	Y	M	I	D	F	W	W	K	P	A

Setting I

Position	40	89	138	139	140	178	221	263	301	348	389	436	482	521	564	606	647	692	735	778	779	826	827	828	863	864	908	909	948	949	950	993	994
Plain	X	S	G	X	E	A	H	H	T	R	T	S	X	Y	X	K	W	I	T	E	E	C	O	N	G	E	N	G	A	S	E	H	O
Cipher	D	W	D	P	F	J	N	N	K	I	Z	R	J	Z	D	K	D	V	T	E	H	S	E	C	X	Z	H	P	I	A	W	Z	E

At setting M positions 820 and 859 were both $E_p = W_c$ and at setting I positions 221 and 263 were both $H_p = N_c$. It was assumed that these were two rotor encipherments between rotors I and II and that rotor I was at the same setting at positions 820 and 859 and at positions 221 and 263. The 3 possible notch ring settings on rotor II were tested between these positions to see if they would allow just 26 changes of setting of rotor I between these positions. From Table IV it was noted that when position 2 of the notch ring was set at B of rotor II, there were 26 changes of setting of rotor I between positions 820 and 859 and positions 221 and 263. Therefore, it was assumed that the notch ring on rotor II was set at 2 on B and the settings of rotor I were written for each position of text.

The hit $E_p = W_c$ at positions 820 and 859, setting M of rotor II and I of rotor I was assumed to be a two rotor encipherment. W on the R.F.S. could be plugged to output F, N, or V of rotor II, but at setting M of rotor II, output N was the only one which would allow the input to be plugged directly to an output of rotor I. At setting I of rotor I, E on the L.F.S. could be plugged to input B of rotor I which would cause output N of rotor I to be plugged to input M of rotor II or E could be plugged to input R of rotor I which would cause output H of rotor I to be plugged to input M of rotor II. These possible pluggings of E were tested on $E_p = W_c$ at positions

CSGAS-76C (8 October 47)

TABLE IV

Position in Message	Setting of Rotor II	Setting of Notch Ring on B of Rotor II: 2	19	26
820	M	.	.	.
821	L	.	X	X
822	K	.	.	X
823	K	.	.	X
824	J	X	X	X
825	J	X	X	X
826	I	X	.	.
827	I	X	.	.
828	I	X	.	.
829	H	X	X	X
830	G	.	X	X
831	F	X	X	.
832	E	X	X	X
833	D	.	.	.
834	C	X	X	X
835	B	.	.	.
836	A	X	X	X
837	A	X	X	X
838	Z	.	X	X
839	Y	X	.	X
840	X	X	X	X
841	W	X	X	.
842	V	X	.	X
843	U	.	.	.
844	T	X	.	X
845	T	X	.	X
846	T	X	.	X
847	T	X	.	X
848	T	X	.	X
849	T	X	.	X
850	S	.	X	X
851	S	.	X	X
852	S	.	X	X
753	R	X	X	.
854	Q	X	X	X
855	P	.	.	X
856	O	X	X	.
857	O	X	X	.
858	N	X	X	.
		26	21	26

Position in Message	Setting of Rotor II	Setting of Notch Ring on B of Rotor II: 2	19	26
221	I	X	.	.
222	H	X	X	X
223	G	.	X	X
224	F	X	X	.
225	F	X	X	.
226	E	X	X	X
227	D	.	.	.
228	C	X	X	X
229	C	X	X	X
230	C	X	X	X
231	B	.	.	.
232	A	X	X	X
233	A	X	X	X
234	Z	.	X	X
235	Z	.	X	X
236	Z	.	X	X
237	Z	.	X	X
238	Z	.	X	X
239	Y	X	.	X
240	X	X	X	X
241	W	X	X	.
242	V	X	.	X
243	U	.	.	.
244	T	X	.	X
245	T	X	.	X
246	T	X	.	X
247	S	.	X	X
248	R	X	X	.
249	Q	X	X	X
250	P	.	.	X
251	O	X	X	.
252	N	X	X	.
253	N	X	X	.
254	N	X	X	.
255	N	X	X	.
256	N	X	X	.
257	M	.	.	.
258	L	.	X	X
259	L	.	X	X
260	L	.	X	X
261	K	.	.	X
262	J	X	X	X
		26	30	27

CSGAS-76C (8 October 47)

806 and 884, setting U of rotor I and T of rotor II. If E on the L.F.S. was plugged to input B of rotor I, the output H of rotor I could be plugged to input A of rotor II. If E was plugged to input R of rotor I output U of rotor I could not be plugged to input A of rotor II. Therefore it was assumed that E on the L.F.S. was plugged to input B on rotor I, output N of rotor I was plugged to input M of rotor II and output H of rotor I was plugged to input A of rotor II. This plugging was verified by $E_P = T_C$ at position 330, setting 1 of rotor I and setting R of rotor II.

Thirty-nine of the 130 pluggings had been recovered. The rest of the pluggings were recovered by taking several matched plain and cipher pairs for a particular plain letter and tracing through paths which would give consistent pluggings.

Plain	Cipher	Position	Settings I	II	III	IV	Plugging Output	Assumed Input
C	O	768	P	P	C	F	C - L.F.S.	K - I
C	S	106	K	Z	T	R	V - I	G - II
C	O	26	I	U	P	T	O - I	S - IV
C	B	144	S	E	W	F	M - I	V - III
C	C	236	S	Z	R	R	P - III	C - R.F.S.

The complete recovered plugging is given in Figure 7.

Conclusions: It is not known whether this solution would have been possible if the rotor order and initial settings of the rotors had not been known. A study will be made to see if they could have been recovered.

The number of trials which would have to be made to set the notch rings could be greatly increased by making the notch rings removable so that any notch ring could be used on any rotor.

Rotor IV used in this study had four wires which were parallel and this was very helpful in that it gave many repeats caused by the same path. Rotor wirings should be limited to pairs of parallel wires.

PHYLLIS METCALF
Cryptographic Plan Subsection

CSGAS-76C (8 October 47)

Figure 7

PLUGBOARD REARRANGED TO SHOW PLUGGINGS

1		2		3		4		5		6		7		8		9		10	
I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II
A	B	B	V	C	K	D	D	A	H	B	Q	D	E	C	W	B	O	A	T
LFS	4	LFS	1	FLS	1	LFS	1	1	2	1	3	2	RFS	2	2	2	RFS	2	RFS
F	O	E	B	G	Y	H	X	U	Z	V	G	H	A	G	S	F	N	E	I
LFS	4	LFS	1	LFS	4	LFS	1	1	3	1	2	2	RFS	2	3	2	3	2	2
I	C	J	D	K	O	L	V	W	Z	X	U	L	J	K	O	J	S	I	U
LFS	4	LFS	4	LFS	1	LFS	4	1	2	1	3	2	3	2	3	2	RFS	2	2
M	E	N	T	O	Y	P	F	Y	T	Z	E	P	T	O	C	N	W	M	P
LFS	1	LFS	4	LFS	1	LFS	4	1	2	1	2	2	3	2	3	2	RFS	2	RFS
Q	U	R	A	S	C	T	P	A	R	B	Y	T	M	S	R	R	Y	Q	O
LFS	1	LFS	4	LFS	1	LFS	1	4	3	4	2	2	RFS	2	RFS	2	RFS	2	2
U	G	V	P	W	W	X	N	C	F	D	C	X	L	W	N	V	B	U	L
LFS	4	LFS	4	LFS	1	LFS	4	4	3	4	2	2	2	2	RFS	2	3	2	RFS
Y	A	Z	H	H	E	G	Z	F	F	E	K	B	P	A	B	Z	P	Y	X
LFS	1	LFS	4	4	4	4	1	4	2	4	3	3	3	3	RFS	2	2	2	RFS
C	Q	D	F	E	M	F	Z	G	L	H	A	F	I	E	F	D	V	C	G
1	1	1	1	1	4	1	4	1	3	1	2	3	RFS	3	RFS	3	2	3	3
I	W	J	J	K	S	L	L	M	V	N	M	J	R	I	I	H	G	G	A
1	4	1	1	1	1	1	1	1	3	1	2	3	2	3	3	3	RFS	3	3
O	S	P	X	Q	G	R	R	S	N	T	Y	N	U	M	Q	L	K	K	Z
1	4	1	4	1	1	1	4	1	2	1	3	3	RFS	3	2	3	RFS	3	RFS
I	M	J	R	K	U	L	J	M	D	N	W	R	X	Q	K	P	C	O	M
4	1	4	1	4	4	4	4	4	2	4	3	3	2	3	2	3	RFS	3	3
T	K	S	L	R	Q	Q	H	P	X	O	S	V	D	U	J	T	H	S	D
4	4	4	4	4	4	4	1	4	3	4	2	3	3	3	RFS	3	3	3	RFS
Z	I	Y	N	X	I	W	T	V	B	U	E	Z	Q	Y	V	X	J	W	H
4	1	4	1	4	4	4	1	4	2	4	3	3	RFS	3	RFS	3	2	3	RFS

This arrangement of the plugboard has been written so that each output is opposite the input to which it is plugged. A on the LFS is plugged to the input at B of rotor IV, F on the LFS is plugged to the input at O of rotor IV, and etc.

CHILES
EMBOD
MENT

The following-described embodiment of SUPERFLEX is felt to have the advantages of (1) mixed-level stator wiring, (2) smallness and compactness, and (3) ease of changing daily key. It employs a rotor basket of special design, using only 4 rotors (26-point rotors will be assumed, but other size rotors would not seriously alter the design). The rotor basket has two endplates and three separators, (see Fig. 1) with 26 spring contacts built into each of the 8 faces (designated a through h) which contact a rotor surface. The spring contacts are connected, according to a wiring plan like that of Fig. 2, to the bank of spring contacts on a "reflexing plugboard". (Fig. 5 is a diagrammatic representation of the face of the plugboard, and shows connections between plugboard pins and points on the contact faces of the rotor basket.) This "plugboard" (see Fig. 3) has 260 spring contacts, arranged in a rectangle 13x20, and is fitted with a hinged panel into which 10 "slides" can be placed. (A similar "plugboard" containing such spring contacts is in use on the SIGJIP.) Each slide consists of bakelite or other suitable insulator on which appear two rows of 13 points arranged to contact 26 of the spring contacts on the plugboard; these points are connected by printed circuits on the face (or both faces) of the slide, to form actually 13 circuits (See Fig. 4). By inserting a set of ten slides, selected from a stock of some 50, according to a daily key list, a complete change of stator wiring will in effect be obtained. With only 4 rotors to be assembled from perhaps 5 or 10 kept on hand, the daily machine setup is kept relatively simple for a device of its security.

The motion control scheme need not be especially complicated, since the same considerations apply as have been discussed in the original paper, and in the various comments attached thereto. Also, it might be felt adequate to have movable alphabet rings, and dispense with movable notch rings, using clear indicators, if traffic is kept low enough to prevent too great depths.

It will be noticed from Fig. 2 that the contacts of the separators are wired to different stators, and in such a way that a plain letter impulse must pass through at least one rotor to effect encipherment.

J.R. CHILES
November 1946

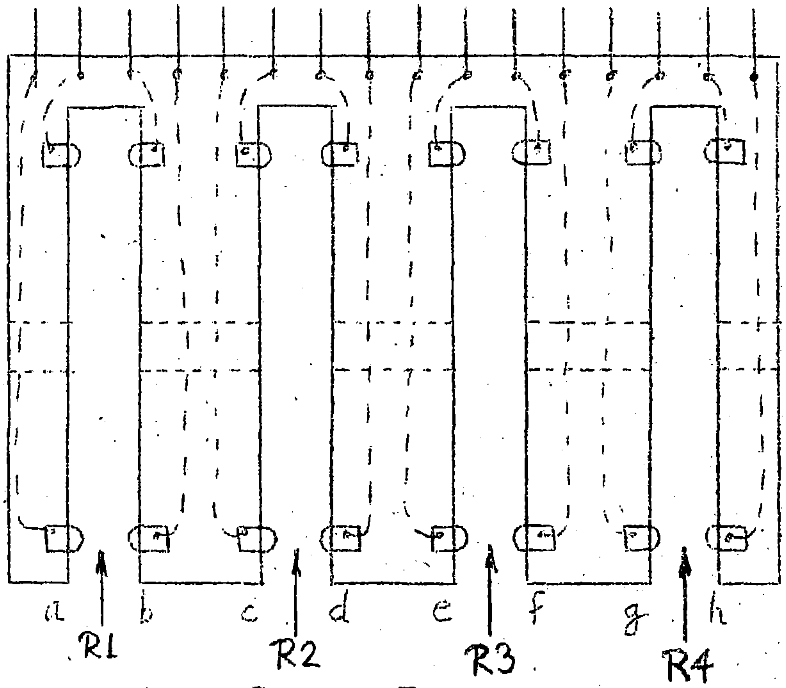
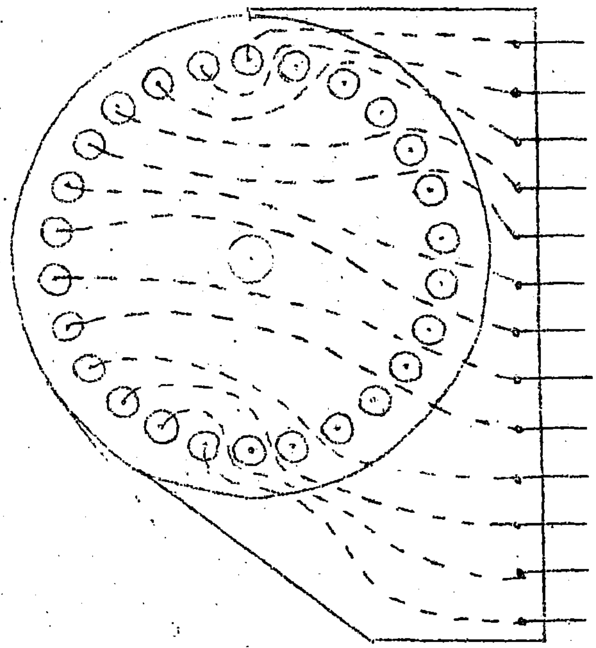
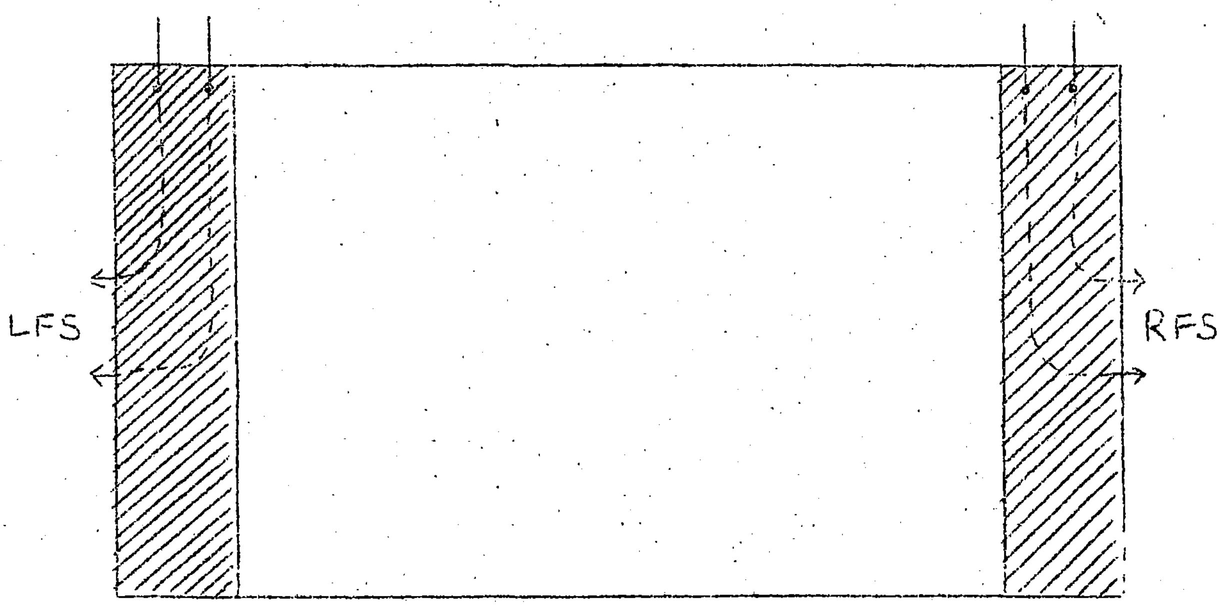


FIG. 1. ROTOR BASKET
CROSS-SECTION—TOP VIEW



SIDE VIEW



ROTOR BASKET HOUSING
CROSS-SECTION—TOP VIEW

FIG. 2. PLAN OF ROTOR BASKET
Showing Connections to Points on Reflexing Plugboard

Contact Faces: to Plugboard Positions:	LFS L	a R	b L	c R	d L	e R	f L	g R	h L	RFS R
A	1	1	1	1	1	1	1	1	1	6
B	2	2	2	2	2	2	2	2	2	7
C	3	3	3	3	3	3	3	3	3	8
D	4	4	4	4	4	4	4	4	4	9
E	5	5	5	5	5	5	5	5	5	Ø
F	1	6	6	6	6	6	6	6	6	6
G	2	7	7	7	7	7	7	7	7	7
H	3	8	8	8	8	8	8	8	8	8
I	4	9	9	9	9	9	9	9	9	9
J	5	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø
K	1	1	1	1	2	1	1	1	1	6
L	2	2	2	2	3	2	2	2	2	7
M	3	3	3	3	4	3	3	3	3	8
N	4	4	4	4	5	4	4	4	4	9
O	5	5	5	5	6	5	5	5	5	Ø
P	1	6	6	6	7	6	6	7	6	6
Q	2	7	7	7	8	7	7	8	7	7
R	3	8	8	8	9	8	8	9	8	8
S	4	9	9	9	Ø	9	9	Ø	9	9
T	5	Ø	Ø	4	6	5	Ø	Ø	Ø	Ø
U	1	1	6	1	7	1	6	1	6	6
V	2	2	7	2	8	2	7	2	7	7
W	3	3	8	3	9	3	8	3	8	8
X	4	4	9	4	Ø	4	9	4	9	9
Y	5	5	Ø	5	Ø	5	Ø	5	Ø	Ø
Z	1	Ø	9	1	6	2	7	3	8	6

(The inverse of this chart is given in Fig. 5)

LFS = Left Fixed Sequence
a = Input Rotor 1   b = Output Rotor 1
c = " " 2   d = " " 2
e = " " 3   f = " " 3
g = " " 4   h = " " 4
RFS = Right Fixed Sequence

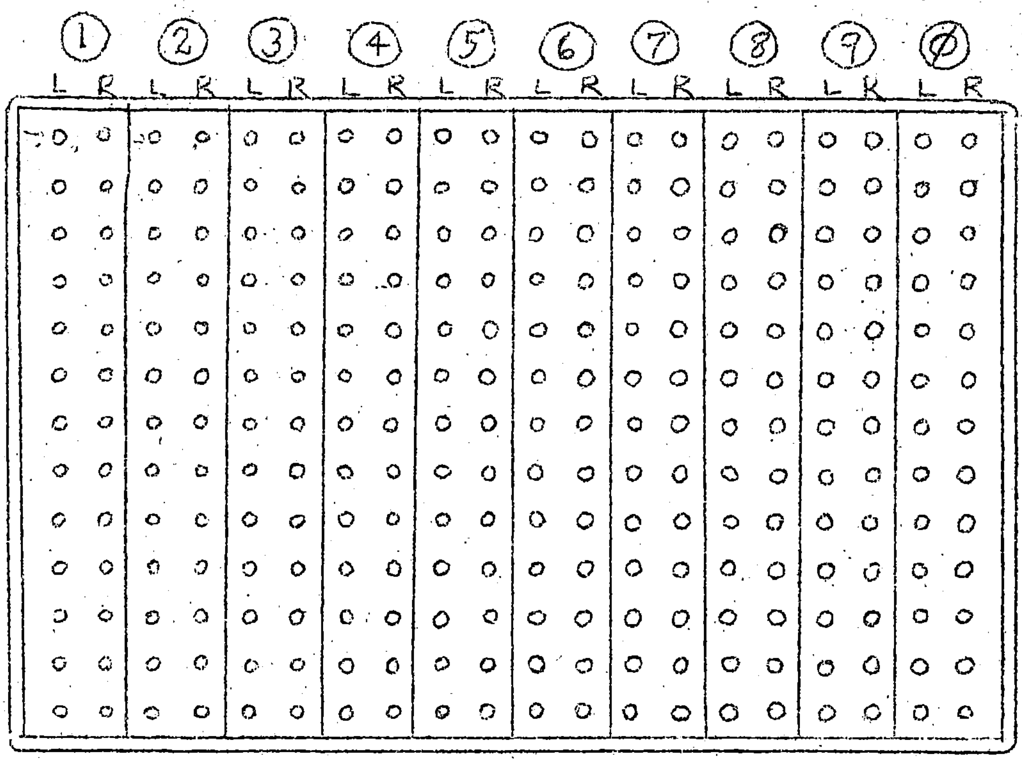
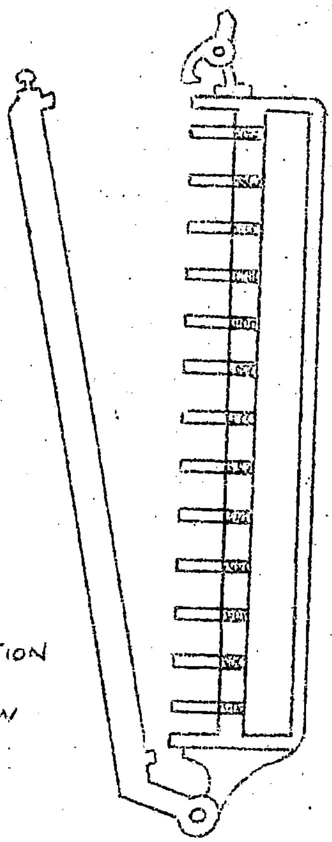


FIG. 3. REFLEXING PLUG BOARD
FACE VIEW



CROSS-SECTION
SIDE VIEW

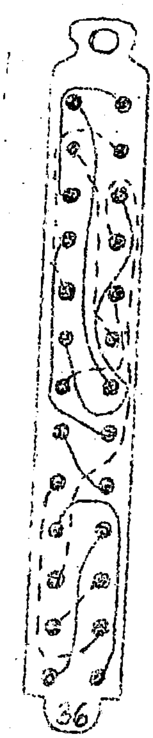


FIG. 4. SLIDE.
SHOWING PRINTED CIRCUIT
(DOTTED LINES PRINTED ON REVERSE SIDE)

FIG. 5. REFLEXING PLUGBOARD,
Showing Actual Connections to Positions in Rotor Basket
(According to Wiring Plan of Fig. 2)

1		2		3		4		5		6		7		8		9		Ø	
L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R
A LFS	A a	B LFS	B a	C LFS	C a	D LFS	D a	E LFS	E a	P h	F a	Q h	G a	R h	H a	S h	I a	T h	J a
F LFS	K a	G LFS	L a	H LFS	M a	I LFS	N a	J LFS	O a	U h	P a	V h	Q a	W h	R a	I h	S a	J h	T a
K LFS	U a	L LFS	V a	M LFS	W a	N LFS	X a	O LFS	Y a	U f	A RFS	V f	B RFS	W f	C RFS	X f	D RFS	Y f	Z a
P LFS	A c	Q LFS	B c	R LFS	C c	S LFS	D c	T LFS	E c	Z d	F c	Z f	G c	Z h	H c	X h	I c	Y d	J c
U LFS	K c	V LFS	L c	W LFS	M c	X LFS	N c	Y LFS	O c	T d	P c	U d	Q c	V d	R c	W d	S c	X d	E RFS
Z LFS	Z c	K d	Z e	L d	Z g	M d	T c	N d	T e	O d	F RFS	P d	G RFS	Q d	H RFS	R d	I RFS	S d	J RFS
A b	U c	B b	V c	C b	W c	D b	X c	E b	Y c	F b	K RFS	G b	L RFS	H b	M RFS	I b	N RFS	J b	O RFS
K b	A e	L b	B e	M b	C e	N b	D e	O b	E e	P b	F e	Q b	G e	R b	H e	S b	I e	T b	J e
A d	K e	B d	L e	C d	M e	D de	N e	E d	O e	U b	P e	V b	Q e	W b	R e	X b	S e	Y b	S g
K h	U e	L h	V e	M h	W e	N h	X e	O h	Y e	F d	P RFS	G d	Q RFS	H d	R RFS	Z b	S RFS	Y h	T RFS
A h	A g	B h	B g	C h	C g	D h	D g	E h	E g	F h	F g	G h	G g	H h	H g	I d	I g	J d	J g
A f	K g	B f	L g	C f	M g	D f	N g	E f	O g	F f	Z RFS	G f	P g	H f	Q g	I f	R g	J f	T g
K f	U g	L f	V g	M f	W g	N f	X g	O f	Y g	P f	U RFS	Q f	V RFS	R f	W RFS	S f	X RFS	T f	Y RFS

BASIC
PAPER

SECRET

WDGAS-76 C   6 August 1946

TO: CIC Projects Section
FROM: MR. SNYDER
SUBJECT: Suggested Cipher Machine, SUPERFLEX

1. Cryptologic Principles.

a. The cipher machine design submitted herewith embodies what is considered to be one of the most general applications of the principle of reflexing. It results in effecting a change in the number and order of rotors, with each letter enciphered. Thus, using 5 conventional Hebern-type rotors, and with certain restrictions described below, a letter is enciphered in effect by passage through any number of rotors from two to 78, with an average path of about 5, and in practically any order.

2. Cryptography.

a. The machine consists of five conventional Hebern-type notched rotors (numbered 1 to 5, Fig. 1), and six stators, (numbered A to F, Fig. 1). One stator is on each end of the assembly, and between successive pairs of rotors. The stators are each equipped with 26 input contact points and 26 output contact points, each point connected by wire to a plugboard outlet. The outlets are arranged in 26 sets of 12 points, (6 input and 6 output) corresponding to the 26 positions of the rotor-stator assembly, so that each set can be readily plugged

SECRET

up, 6 inputs to 6 outputs.

b. A letter is enciphered by depressing a key, say E, which sends an impulse through the corresponding input point of separator (stator) A, through the plugboard to output of stator C to enter rotor 3 (See Fig. 2). At the particular setting shown in the example, rotor 3 is at a setting such that the "E" impulse enters that rotor at G; following the wire through the rotor reveals that the impulse leaves rotor 3 to contact a point on the stator which takes it to rotor 2, which it enters at L. Again the impulse is taken through the rotor to leave at a point on stator C which is wired to enter rotor 5. Entering rotor 5 at W, the impulse leaves at a point which is plugged to go to rotor 3 at B, then to rotor 2 at N, to rotor 5 at O, and then through "right fixed sequence" to typebar F. (Digit 6 is used to represent R.F.S., in the plugging diagrams.)

c. To insure passage of current through a minimum of two rotors, stator A (which is in contact with plain letters on the input side) should be wired, on its output side, to only 3 of the 5 rotors; none of these three must be allowed to go straight out to cipher. The result of applying these limitations is shown by Fig. 3, which lists all the possible stator wirings, and the conditions set up to control plugging possibilities.

d. The change in rotor settings between successive encipherments is not limited to any particular type of motion, but should be some irregular motion system that will insure that none of the five rotors may be stationary for more than two successive encipherments. This insures against encipherments of too many pairs of identical letters through identical rotor maze.

e. The plugging should be set up in some form to facilitate frequent changes requiring a minimum of effort and training of operators. A suggested scheme is to have a file of 108 cards, approximately 3 by 3 inches, each having one of the 108 wirings of 6 inputs to 6 outputs of stators printed on its surface with conducting ink. Insertion of a selection of 26 cards (according to key lists, etc.) in 26 "slots" or contact positions would be the equivalent of wiring up the 6 stators at all 26 positions. (See Fig. 4.) Another method might be to have the 26 sets of six input positions of the stators terminate in 26 six-pronged plugs. These to be inserted into the particular 26 of the 108 six-hole outlets terminating on the face of the plugboard, according to key list. This would eliminate the necessity of having to prepare, issue, and store sets of cards containing printed circuits.

3. Encipherment of Test Messages.

a. In order to investigate the effects of encipherment by this system, two 200-letter encipherments of identical plaintext were prepared, using rotor motions similar to Orange machine motion. While these were admittedly on too small a scale to constitute what might be called a security study, these tests and the two other tests next described gave enough clear results to serve a s a guide to planning proper use of the device.

b. In Test 1, the cipher text was reasonably flat, individual letter frequencies varying from three to 12 occurrences, with all 26 letters represented. (Frequencies of plain text letters in the example showed 3 blanks and highs of 32 for X (word separator) and 27 occurrences of letter E.) There were 51 encipherments through 2 rotors, 30 three-rotor and 25 four-rotor encipherments, and 94 involving five or more. Longest path was 22 rotors, and the average was about five. There was one case of two identical plain letters (separated by one letter) which yielded identical cipher letters and used the same rotor path.

c. The cipher text obtained from test 2 was found to be flat, and contained no significant repetitions. There were 67 encipherments involving passage of current through two rotors, 24 three-rotor encipherments, 26 four-rotor, and 82 involving 5 or more rotors. The largest number of rotors involved was 23. The average path was five rotors.

d. Test 3 was the encipherment of 100 E's, in which the wiring of stator A was directly to the fast moving rotor.

Consequently there were no consecutive encipherments through the same rotor path, to yield identical cipher. But there were four cases of identical consecutive cipher derived through different paths. There were 30 two-rotor encipherments, 18 three-rotor, 11 four-rotor, and 41 encipherments involving five or more rotors. The longest path was through 22 rotors.

e. Test 4 was the encipherment of 100 R's, in which the wiring of stator A was directly to slow-moving rotor. This was rotor 2 in this case, and had motion only 42% of the time. Due to no motion of the enciphering rotors between certain successive positions, there were 9 digraphs (doublets), 5 trigraphs, and 1 pentagraph involving the same cipher letter; i.e. identical enciphering paths in successive positions. There were two cases of identical consecutive cipher pairs derived through different paths. There were 24 two-rotor encipherments, 16 three-rotor, 12 four-rotor encipherments, XX and 48 encipherments through five or more rotors.

4. Evaluation.

a. It is felt that the principal contribution of the SUPERFLEX is the great variability in the number and order of rotors constituting the path of each enciphering impulse. In other words, assuming knowledge of rotor wirings, in addition to identifying rotor order, ~~and~~ setting, AND MOTION, the enemy must reconstruct stator wiring, to reproduce the factors in encipherment. The wiring of the 26 stator positions may be done in $108!/82! = 2.8 \times 10^{51}$ ways, assuming adoption of the rules set forth in Fig. 3.

b. The fact that design and construction of the SUPERFLEX introduces a minimum of new mechanical or electrical principles is considered a great advantage. The only feature which can be said to be new is the stator plugging device, which can be handled in a choice of several ways, all fairly simple. Rotor design, notch setups, motion planning, and indicator encipherment schemes can be chosen from among known, tried techniques.

c. Since no exhaustive security studies have been carried out, any statements made here are subject to the strictest review. But it is considered possible that the introduttion of irregular reflexing, as proposed here, may conceivably make it possible to relax certain features of security regulations which usually control the use of most other cipher machines. For example, further study will reveal whether the machine will permit use of "clear" indicators, and under what conditions; also, whether re-encipherments may be permitted, etc.

5. Acknowledgment.

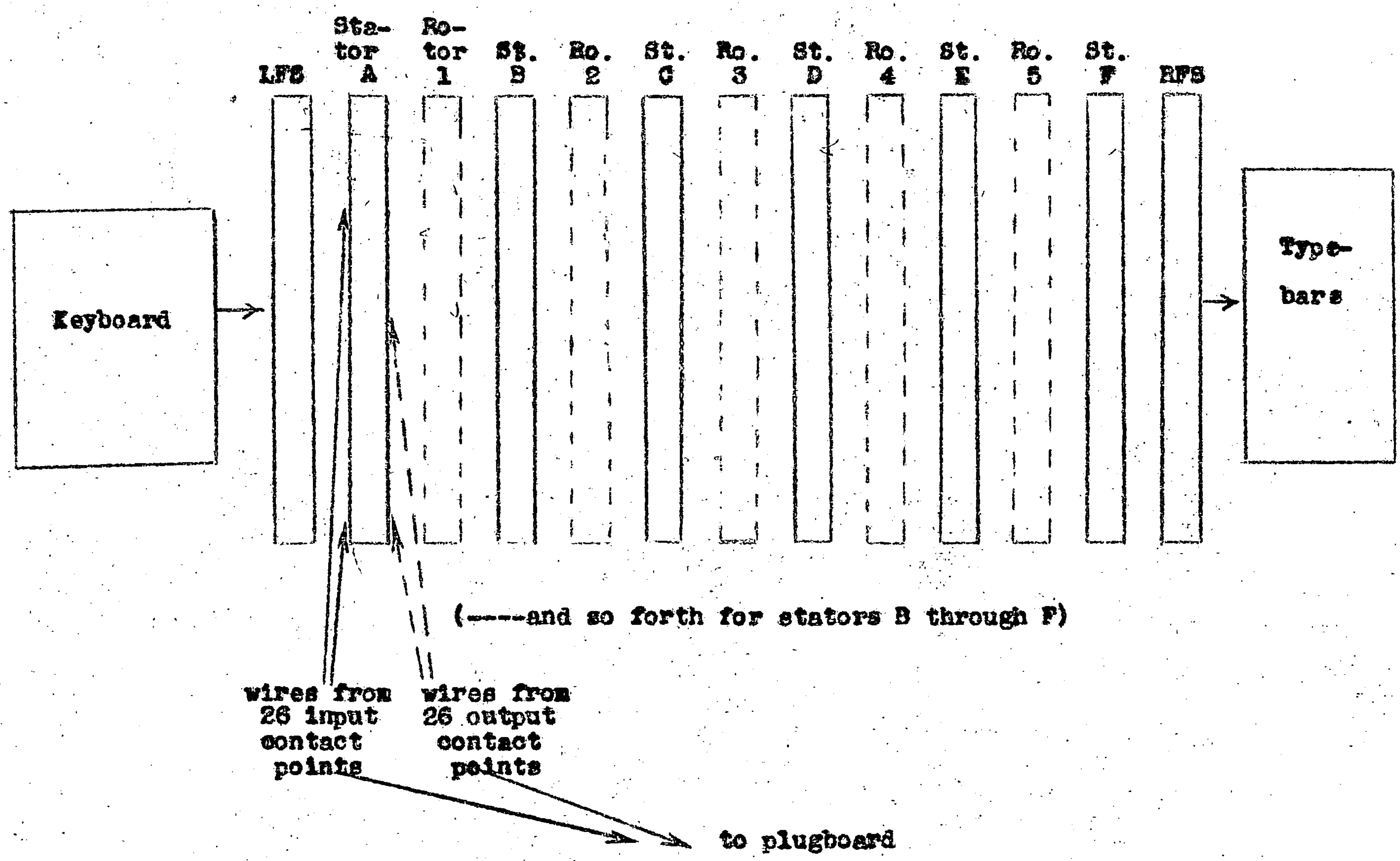
a. The undersigned hereby acknowledges the helpful suggestions and constructive criticisms of the following individuals, during the development of the ideas contained

~~SECRET~~

herein: Major Dumey, Mr. Barlow, Mr. Ferner, Miss Rosebro, and Mr. Gordon and other members of Projects S ection.

S.S.SNYDER

Fig. 1. Schematic Diagram of SUPERFLEX



Setting: A B C D E

Keyboard(LFS): A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Stator A 1 3 2 1 3 2 2 3 3 3 3 2 1 1 2 3 1 2 3 1 1 3 2 3 1 2

Rotor 1 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
N E X I M W L B A U V K T G J S C F O Q Z D Y P R H

Stator B 2 2 1 3 4 1 3 2 1 4 4 4 3 4 4 4 4 1 1 2 3 1 1 2 3 4

Rotor 2 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C W O V I E P K R D X N F J H Q U T B L Y A S Z G M C

Stator C 3 5 4 6 5 4 5 4 4 1 5 1 5 5 5 2 3 5 5 5 2 4 5 4 5 1

Rotor 3 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
F K E U N T I Y C L R M G S B A Q J Z V O X H D W P F K

Stator D 4 4 5 2 1 5 4 5 5 5 2 5 2 3 1 5 2 4 4 4 5 5 3 5 4 5

Rotor 4 B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
D U A P J Z G H N R B X I F Q T L C M W S E K Y V O D U

Stator E 5 6 6 4 6 3 6 1 6 2 6 3 6 6 3 1 5 6 2 6 4 2 6 6 2 6

Rotor 5 C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
Z W J A U D T O B M F I C S H L V R E X Q Y N P K G Z W

Stator F 6 1 3 6 2 6 1 6 2 6 1 6 4 2 6 6 6 3 6 3 6 6 4 1 6 3

Typebars(RFS): A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Stator wirings assembled as follows (See fig. 3):

1, 98, 44, 21, 106, 43, 60, 91, 80, 99, 108, 63, 22, 36, 69, 103, 29, 48, 83, 12, 15, 79, 46, 92, 23, 64

Fig. 2.

Fig. 3. List of Stator Wirings

1. A rotor number appearing under a given stator in the list below means the preceding rotor (immediately to the left) is wired to input of that rotor number. For example, a "5" under stator C means that output of rotor 2 is wired to input of rotor 5 at that level, or rotor position.

2. Stator A may be wired to only three rotors; in the present instance, rotors 1, 2, and 3.

3. Only two stators may be wired to typebar, or Right Fixed Sequence ("rotor" 6); in the present instance, stators E and F.

4. Output of stator B has been limited to four rotors, in order to reduce the percentage of short (2- or 3-rotor) paths; in the present instance, rotors 1, 2, 3, and 4.

5. Tabulation of possible stator-to-rotor wirings:

1 5

	Stators: A	B	C	D	E	F
may go	1	1	1	1	1	1
to	2	2	2	2	2	2
rotors:	3	3	3	3	3	3
		4	4	4	4	4
			5	5	5	5
					6	6

6. List of all possible rotor-stator-rotor wirings, using above limitations:

#	A	B	C	D	E	F	#	A	B	C	D	E	F	#	A	B	C	D	E	F
1	1	2	3	4	5	6	13	1	3	2	4	5	6	25	1	4	2	3	5	6
2	1	2	3	4	6	5	14	1	3	2	4	6	5	26	1	4	2	3	6	5
3	1	2	3	5	4	6	15	1	3	2	5	4	6	27	1	4	2	5	3	6
4	1	2	3	5	6	4	16	1	3	2	5	6	4	28	1	4	2	5	6	3
5	1	2	4	3	5	6	17	1	3	4	2	5	6	29	1	4	3	2	5	6
6	1	2	4	3	6	5	18	1	3	4	2	6	5	30	1	4	3	2	6	5
7	1	2	4	5	3	6	19	1	3	4	5	2	6	31	1	4	3	5	2	6
8	1	2	4	5	6	3	20	1	3	4	5	6	2	32	1	4	3	5	6	2
9	1	2	5	3	4	6	21	1	3	5	2	4	6	33	1	4	5	2	3	6
10	1	2	5	3	6	4	22	1	3	5	2	6	4	34	1	4	5	2	6	3
11	1	2	5	4	3	6	23	1	3	5	4	2	6	35	1	4	5	3	2	6
12	1	2	5	4	6	3	24	1	3	5	4	6	2	36	1	4	5	3	6	2

(continued)

Fig. 3. List of Stator Wirings (continued)

#	A	B	C	D	E	F	#	A	B	C	D	E	F	#	A	B	C	D	E	F
37	2	1	3	4	5	6	49	2	3	1	4	5	6	61	2	4	1	3	5	6
38	2	1	3	4	6	5	50	2	3	1	4	6	5	62	2	4	1	3	6	5
39	2	1	3	5	4	6	51	2	3	1	5	4	6	63	2	4	1	5	3	6
40	2	1	3	5	6	4	52	2	3	1	5	6	4	64	2	4	1	5	6	3
41	2	1	4	3	5	6	53	2	3	4	1	5	6	65	2	4	3	1	5	6
42	2	1	4	3	6	5	54	2	3	4	1	6	5	66	2	4	3	1	6	5
43	2	1	4	5	3	6	55	2	3	4	5	1	6	67	2	4	3	5	1	6
44	2	1	4	5	6	3	56	2	3	4	5	6	1	68	2	4	3	5	6	1
45	2	1	5	3	4	6	57	2	3	5	1	4	6	69	2	4	5	1	3	6
46	2	1	5	3	6	4	58	2	3	5	1	6	4	70	2	4	5	1	6	3
47	2	1	5	4	3	6	59	2	3	5	4	1	6	71	2	4	5	3	1	6
48	2	1	5	4	6	3	60	2	3	5	4	6	1	72	2	4	5	3	6	1
73	3	1	2	4	5	6	85	3	2	1	4	5	6	97	3	4	1	2	5	6
74	3	1	2	4	6	5	86	3	2	1	4	6	5	98	3	4	1	2	6	5
75	3	1	2	5	4	6	87	3	2	1	5	4	6	99	3	4	1	5	2	6
76	3	1	2	5	6	4	88	3	2	1	5	6	4	100	3	4	1	5	6	2
77	3	1	4	2	5	6	89	3	2	4	1	5	6	101	3	4	2	1	5	6
78	3	1	4	2	6	5	90	3	2	4	1	6	5	102	3	4	2	1	6	5
79	3	1	4	5	2	6	91	3	2	4	5	1	6	103	3	4	2	5	1	6
80	3	1	4	5	6	2	92	3	2	4	5	6	1	104	3	4	2	5	6	1
81	3	1	5	2	4	6	93	3	2	5	1	4	6	105	3	4	5	1	2	6
82	3	1	5	2	6	4	94	3	2	5	1	6	4	106	3	4	5	1	6	2
83	3	1	5	4	2	6	95	3	2	5	4	1	6	107	3	4	5	2	1	6
84	3	1	5	4	6	2	96	3	2	5	4	6	1	108	3	4	5	2	6	1

Fig. 4. Detail of Printed Circuit Representing Wiring # 63 (See Fig. 3)