REF ID: A[redacted]

MEMO ROUTING SLIP

NEVER USE [redacted] FOR APPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

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

REMARKS

FROM NAME OR TITLE NSA-314 DATE 3d Nov 42

ORGANIZATION AND LOCATION 17-117 TELEPHONE Ext 391.

DD FORM 1 FEB 50 94 REPLACES NME FORM 94, 1 FEB 49, WHICH MAY BE USED. 16—58363-2 GPO

SECRET

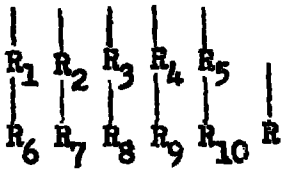
THE PNEUMATIC AUTHENTICATOR OR DEM 498

Reference - 1. Tentative Security Evaluation of AFSAM D498 Brusa 267

2. The Security of the Pneumatic Authenticator (DEM 498) Brusa 616

3. Pneumatic Authenticator Brusa 167

The description of the Pneumatic Authenticator as planned can be found in the references given above.



The authenticator as set up now has two features which place certain limitations on the possible variability of the device. One is the use of a constant input point and the other is the use of 5 groupings of 3 in the reverser. For example suppose each of the 5 groupings of 3 in the reverser is traced to the input end-plate. Only one of the trigraphs obtained would contain the constant input point. This means that for each alignment only one out of 5 of the trigraphic groupings in the reverser is used. With a variable input point any one of the 5 groupings could be used. This means that only 1/5 of the potentiality of the device is being used.

In the above references it has been shown that with planned interrogations certain types of solutions can be found. The possible solutions mentioned made use of a constant input point and the groupings of 3 in the reverser. It was assumed that the enemy would be able to obtain replies for challenges in which all the paired rotors stand except one designated pair. In one solution it was shown how it might be possible to recover the settings of the paired rotors $R_1 - R_6$. The settings of R_5 and R_{10} could be recovered just as easily using the same type of planned interrogation. The output values from R_5 would be a

SECRET

monoalphabetic substitution of the input values into R_{10}. That is the output from R_5 has the same pattern as the input into R_{10}. The constant input point and the groupings of 3 in the reverser can be used effectively to recover such a pattern. In some instances it "snowballs" rather easily and in others it is quite a laborous task.

Suppose we have given the following replies obtained from consecutive settings of R_5 - R_{10} (the settings of the other rotors remain constant).

K C E F K O C F B J G H O I C

G O N O G N D L G G K I F F D

One could assume the input positions into R_5 of the 3 most frequent letters, one of which would be the constant input point A and the other two could be G and F. The initial setting of R_5 would be assumed. The input values for the 3 letters would be enciphered through R_5 at the proper relative settings of R_5. A partial pattern of the output values from R_5 is thus obtained. The initial setting of R_{10} is assumed and trigraphs from the reverser are deciphered at the proper relative settings of R_{10} so as to obtain a partial pattern which agrees with the partial output pattern from R_5. Each partial pattern suggests values for the other so that when all correct assumptions are made the patterns build up very quickly. Contradictions show up in most instances with incorrect assumptions. In some instances if there are not enough repeats in the first partial output pattern from R_5 so as to eliminate some of the possible assumptions from the trigraphs in the reverser, it requires several trials to recover the patterns by hand. With repeats, contradictions show up quickly and eliminate some of the possible trials. (The setting identified for R_5 could only be a relative setting).

There are 15 x 14 x 13 = 2730 possible combinations for the three input positions of A, G and F into R_5. Altogether there are $\frac{15 \times 14 \times 13}{1 \times 2 \times 3} = 455$ different trigraphs. The 455 trigraphs can be listed according to their cyclic interval patterns. There would be 15 trigraphs for each pattern. To illustrate -

Interval pattern	1 - 1 - 13	1 - 2 - 12	1 - 6 - 8
	A B C	A B D	A B H
	B C D	B C E	B C I
	C D E	C D F	C D J
	D E F	D E G	D E K
	etc.	etc.	etc.

There are altogether 31 different interval patterns.

Instead of considering 2730 possible assumptions for the three input positions into R_5 for A, G and F, assume the use of one of the 31 interval patterns. Suppose the interval pattern 2 - 2 - 11 is assumed. The three input positions would then be A - C - D. There would be 3 ways of selecting the input position of the constant input A and 2 for G and F. There would be 6 orders to be considered. Altogether there would be 6 x 31 = 186 assumptions for the three input positions instead of 2730.

Suppose there were 31 people who were assigned to recover the setting (or relative setting) of R_5 and the actual setting of R_{10}. Each individual would have to assume the order of the input positions and the settings of R_5 and R_{10}. There would be a total of 6 x 15 x 15 = 1350 possible assumptions for each person. In most instances if there are two letters of which each appears 5 or more times in the replies the patterns build up more easily and the number of assumptions in most instances are reduced considerably. This solution by no means compromises the device but might lead to other solutions which could compromise the device.

SECRET

Wiring of the reverser -

If two of the trigraphs in the reverser have the same patterned interval and the rotors are moved as a block against the reverser it would be possible to produce a 3 - way lobster effect. For example suppose the two groupings C J N and D H O are used in the reverser. The cyclic interval patterns are 7 - 4 - 4 and 4 - 7 - 4 respectively i.e. they have the same cyclic pattern. This means that an encipherment of the constant input point which comes into the reverser back through the maze by way of C J N at setting S_1, S_2, S_3, S_4, S_5. A second encipherment of the constant input point at setting (S_1+5),(S_2+5),(S_3+5), (S_4+5),(S_5+5) would go through the maze and the reverser by way of D H O. The lobster effect could be recognized in the trigraphs obtained from the two letter replies and the constant input point. If the two replies K M and C F are obtained from the two challenges the lobster effect is detected by the fact that C F A is five positions from M A K as - (M N O A B C);(A B C D E F); (K L M N O A)

The lobster effect cannot be eliminated completely by careful wiring of the reverser. It is true there are 5 patterned intervals which have no repeats as 1 - 1 - 13, 2 - 2 - 11, 3 - 3 - 9; 4 - 4 - 7 and 5 - 5 - 5. But it is impossible to wire a reverser using all five patterned intervals in the same reverser. Consequently all reversers have to include repeats in at least one of the intervals for some of the reverser trigraphs. This means that two-way lobster effects could be produced at the proper offset for the trigraphs which have the repeats. If the offset for two challenges (plus the constant input point) agrees with the offset for two trigraphs which have repeat intervals then it would be possible to associate the replies with the reverser trigraphs that were used in

SECRET

each encipherment, an example of 5 reverser trigraphs and the patterned intervals are

1 - A E J - 4 - 5 - 6

2 - B D K - 2 - 7 - 6

3 - C L N - 9 - 2 - 4

4 - F I O - 3 - 6 - 6

5 - G H M - 1 - 5 - 9

A two way lobster would show up if trigraphs 1 and 2 are used at an offset of one (A is offset one from B, and J one from K).

Stationary rotors interspersed among the stepping rotors could eliminate the possible occurrence of a lobster during a day's traffic. If the stationary rotors are placed only next to the reverser it is possible to increase the occurrences of the lobster effect. This is because the combined effect of the reverser and stationary rotors could produce two or more groupings of three with the same cyclic interval pattern.

To avoid the carry over of the lobster effect from one day's traffic to the next, the relative alignment of the rotors within at least one paired set must be offset from any of the previous day's relative alignments.

How could the use of planned interrogation be eliminated? Or what changes could be made in the use of the device in order to eliminate the possible use of planned interrogation? What could be substituted for the use of the constant input point and the groupings of 3 in the reverser.

Adding rotors will not eliminate the possibility of some of the solutions. Some of the weaknesses of the device might be offset by

~~SECRET~~

1. Double encipherment
2. Varying the position of the input point.
3. Scrambled end-plate; but produce each letter of the reply one at time and read as produced.
4. Eliminate the use of trigraphic reversers.

Amy Norman
NSA-314
June 1954