WAR DEPARTMENT

MEMO ROUTING SLIP

1 NAME OR TITLE Mr. Douglas (Ltr over)	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	DATE		CONCURRENCE
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Sent a copy of your report to Dr. Kullback who has been studying this gadget. His first appraisal was pretty low but I don't think he knew all the details. This device seems to present pretty good security for its size. Have you any suggestions for further study as to its possibilities for your own usage?

FROM NAME OR TITLE F	DATE
ORGANIZATION AND LOCATION	TELEPHONE

WD AGO FORM 1 JUN 1946 895

16—48487-1 U. S. GOVERNMENT PRINTING OFFICE

For a low-echelon machine this device would be very difficult to change to keyboard operation including a printer.

For improvements, disregarding the mechanical difficulties, several things can be done.

1. Lengthen the stepping cycle. This can be done by using larger wheels, or steel tapes with punch or no-punch, or link chains with two kinds of links

2. Use two complete alphabets, one for the upper and one for the lower position. The slide would then step 52 positions instead of 26 but each alphabet would be independent and letters could represent themselves.

3. A means of disrupting the regular stepping of the wheels (or tapes, or chains) so that active and inactive pins would be more difficult to set.

I'm rather doubtful that it would be suitable for authentication

JKH

File F

~~TOP SECRET~~

28 December 1949

MEMORANDUM FOR: Mr. Friedman

Subject: Theoretical Security of the "Schlüsselkasten".

1. The security of the Schlussenkasten appears to be fairly high, but I believe that when used in low echelon with a moderate amount of traffic the system will not offer the security required at that level. There follows a brief analysis of the system.

2. The Germans believed that the theoretical security of the Schlussenkasten was equivalent to or greater than the Enigma. Some of the weaknesses, however, which appear to negate the opinion of the Germans are made use of in the analysis.

[redacted]

4. Recovery of the two alphabets presents the most trouble. Cribs and direct depths as well as isomorphs will be the data required. Cribs can be placed since a letter cannot represent itself. As reconstruction progresses additional limitations can be used to place cribs.

a. The reconstruction of the machine can be accomplished, I think, in three steps: (1) Determining the limitations present in each of the two alphabets, i.e., like and unlike substitution values in the upper and lower alphabets; (2) Recovery of the alphabets; and (3) Recovery of the pin wheel patterns.

~~TOP SECRET~~

3128

~~TOP SECRET~~

[redacted]

c. Once the separation is determined the portions of matched plain and cipher text can be divided into three categories - (1) upper alphabet; (2) lower alphabet; and (3) ambiguous. Direct depths and isomorphic depths should help and recovery will be along the usual lines.

d. When the two alphabets are recovered the internal the slide has moved between letters is readily determined from the matched plain and cipher. Since the wheels move regularly, placement of active and inactive pins is relatively simple. As long a crib as possible is desirable, otherwise short cribs may not produce enough pin patterns to permit joining the stepping cycle in relative order. With alphabets recovered, however, and knowing the average interval is about 4, cribs probably can be extended.

e. Isomorphic depths can be helpful in separating the two alphabets and in recovery. The isomorphisms are not as easily recognized as in normal cases since the relation exists as two interlaced isomorphs, each behaving as in the normal case. With sufficient material it seems probable that the isomorphic feature alone might well lead to a complete solution.

James H. Douglas
JAMES H. DOUGLAS

parallel in Indian VIOLET
machine (4 rotors)
— COC.

~~TOP SECRET~~