

27 APRIL 2011



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 62647B

11 April 2011

This is our final response to your Freedom of Information Act (FOIA) request submitted via the Internet on 21 August 2010, for "A document or documents that provide a general description of SIGNIN (a WWII era machine)." A copy of your request is inclosed. As previously stated in our letter dated 3 November 2010, for purposes of this request and based on the information you provided, you are considered an "all other" requester. As such, you are allowed 2 hours of search and the duplication of 100 pages at no cost. Since processing fees were minimal, no fees are being assessed.

Your request has been processed under the provisions of the FOIA and the remainder of the material you requested is enclosed.

Sincerely,

for *Sally A. Nicholson*

PAMELA N. PHILLIPS

Chief

FOIA/PA Office

Encls:

a/s

~~TOP SECRET~~

29 May 1940

SIGNIN ~~CRYPTOGRAPHIC~~ PRINCIPLES

Machine is combined teletypewriter and cipher machine. It generates running key, expressed electrically in 5-baud teletype characters, by passage of current through multiple paths in an 8-rotor maze; and applies this key baud-by-baud to plain text to accomplish encryption, addition following the rule "unlike impulses produce mark impluses."

Current input: 1 band of 5 wires on the left endplate.
Key output: 5 bands of 3 wires on the right endplate.

The eight rotors have only the following motion which is accomplished by 5 stepping control notches arranged around the periphery of each rotor in accordance with a standard pattern. NOTE: If a rotor remains on a notched position, the rotor it controls does not keep stepping but steps only the ~~first~~ ^{first} time the notch was effective.

Fast Medium Slow Very Slow (Separator) Fast Slow Medium Fast

Rotors may be inserted in normal position but not in reversed. Rotors may be rewired ~~without~~ without soldering. Mixed-wire separator is permanently located between 4th and 5th rotor positions.

NSA LIBRARY
L-2316 Copy No. 1
F-42

Do Not Destroy. Return to the
NSA Library when no longer needed.
L-2316 Copy No. 1
F-42

RECORD COPY
DO NOT DESTROY OR MUTILATE

Approved for Release by NSA on
03-21-2011, FOIA Case # 62647

~~Top Secret~~

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
Washington 25, D.C.

AFSA-412
A6-3(1)/N36-10()
Summary No. _____
Date: 29 May 1950

SUMMARY SHEET: ATTACK ON SIGNIN SYSTEM

1. GIVEN:

SPECIAL CONDITIONS:

2. RECOGNITION OF THE CASE:

3. RESULT:

4. ESTIMATED TIME TO COMPLETE SOLUTION: Man hours _____ and/or machine hours _____

(a) Existing approved machine methods. _____

(b) Non-existing approved machine methods. _____

(c) Visualized machine methods. _____

(d) Remarks on hand/machine methods:

5. REFERENCES:

6. EVALUATION:

7. SUMMARY OF METHOD:

~~SECRET~~

1540-1
NOV. 1943
copy 4

SIGNIN - Change D

SECTION I
SUMMARY

1. Description: Change D consists of the addition of a band transposition maze to the enciphering unit of SIGNIN. The added maze transposes the bands of the cipher text according to an arbitrary key.
2. Purpose: To test the advisability of adding band transposition.
3. Given: Messages enciphered on SIGNIN with band transposition added as follows:
 - a. Two messages in depth one a stagger of the other.
 - b. Two messages in depth with one probable word given.
4. Results: Even with the addition of the band transposition, two messages in depth can be read though the unique solution for the transposition and substitution is not usually attainable.
5. Conclusions: The addition of band transposition is not recommended for SIGNIN.

Approved for Release by NSA on
03-21-2011, FOIA Case # 62647

~~SECRET~~

~~CONFIDENTIAL~~
~~SECRET~~

10-1238

NOV. 1943

SIGNIN

SUBJECT: Change D.

1. Change D consists of the addition of a transposition maze to the enciphering unit of SIGNIN. This added maze transposes the bands of cipher text according to an arbitrary key. Thus, if the cipher text were: + - - - - it might appear as one of the follow-
ings:

+ - - - -
- + - - -
- - + - -
- - - + -
- - - - +

2. Although it is true that the process of reading messages in depth is complicated by the transposition process, it is still possible that two messages be read. Two tests were run:

a. The plain text of two messages were the same, but staggered by a varying amount. In the numerous depths in traffic studied, this is the case usually found. It is caused by service re-runs in which the same indicator is used.

b. The plain text of the two messages were entirely different, but a probable word was given.

3. Solution is based upon the fact that when two messages are in depth, the key is the same. Given two plain-texts: P₁ and P₂, the enciphering process may be represented by

Message 1: $C_1 = (P_1 + K) T$

Message 2: $C_2 = (P_2 + K) T$

Note: when C = cipher text, P = plain text, K = key; T = transposition.

~~SECRET~~
~~CONFIDENTIAL~~

~~CONFIDENTIAL~~SIGNIN
Change D~~SECRET~~

(cont'd)

The formulas are added, yielding:

$$C_1 + C_2 = (P_1 + K) T + (P_2 + K) T$$

$$C_1 + C_2 = (P_1 + P_2) T + (K + K) T$$

When two identical letters in Baudot Code are added, their effect is cancelled. ✓

$$C_1 + C_2 = (P_1 + P_2) T$$

In enciphering with 32 alphabets, the assumption of a plain-text letter in one message gives one and only one plain-text letter in the other message. When a transposition is added to the cipher text, however, the assumption of a plain-text letter in one message produces a possibility of 1, 5 or 10 plain-text letters in the other message depending on the character of the combined cipher text. The letters of the 32-letter alphabet can be combined into six groups as follows:

1. All transpositions of 2 plusses— A, D, H, I, L, N, O, R, S, Z.
2. All transpositions of 3 plusses— U, J, W, C, P, M, G, B, Y, F.
3. All transpositions of one plus— E, J, 3, 7, T.
4. All transpositions of 4 plusses— K, Q, X, V, Z.
5. All transpositions of 5 plusses— 4.
6. All transpositions of no plus— 6.

✓ Note: See report "Solution of a Teletypewriter System Using Two Endless Key Tapes", paragraph 3 b.

~~TOP SECRET~~
~~CONFIDENTIAL~~

SIGNIN
Range D - cont'd

~~CONFIDENTIAL~~
~~SECRET~~

ASSUMPTION TABLES

Characters
with
3 plusses

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

V

Characters
with
2 plusses

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

Characters
with
4 plusses

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

~~SECRET~~
~~CONFIDENTIAL~~

SIGNIN
 Change D - cont'd
 ASSUMPTION TABLES - cont'd

~~CONFIDENTIAL~~
~~SECRET~~

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

	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	7	5	4	3	2	6	
Characters with 3 plusses	4	M	I	Z	P	V	L	8	J	B	H	T	F	A	R	U	D	7	Y	G	K	O	E	N	5	R	C	Q	X	6	2	3	4

	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	7	5	4	3	2	6	
Characters with no plus	6	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	7	5	4	3	2	6

Example of enciphering two plain-text letters in depth:

		1	2	3	4	5			1	2	3	4	5
P = G =		-	+	-	+	+	B = A =		+	+	-	-	-
K = L =		-	+	-	-	+	K = L =		-	+	-	-	+
(P ₁ + K)	=	-	-	-	+	-	(P ₂ + K)	=	+	-	-	-	+
T	=	2	3	1	5	4	T	=	2	3	1	5	4
(P ₁ + K) T =		-	-	-	-	+	(P ₂ + K) T =		-	-	+	+	-
C ₁	=	-	-	-	+	+	C ₂	=	-	-	+	+	-
C ₂	=	-	-	+	+	-							
C ₁ + C ₂	=	-	-	+	+	+	= M						

In the assumption tables for characters with 3 plusses, if we assume the plain-text letter P₁ = G, we find A is one of the ten possibilities for P₂.

~~SECRET~~
~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
~~SECRET~~

SIGNIN
Change - D -- cont'd

Solution of two messages in depth using Assumption Tables.

Plain 1. SHIP3SAILING3TIME3

Cipher 1. BDKTCKKF3RQW3RVDJH

Combined
Cipher T. OAJUNQYVZITDQHRR6

Cipher 2. XN3QKRGWILGGWVQAEH

Plain 2. DIESEL30IL3TWENTY3

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

~~SECRET~~
~~CONFIDENTIAL~~
5.

SIGINT
Change D - cont'd

Two messages with some plain text with varying amount of stagger:

Plain

1. SHOWER3CITE3RAAGE7557CLASSIFICATION3CONFIDENTIAL3

Cipher

1. A55XWQEU7JRE847DKU5MFVTLIN42YCKB4TE6VY7C7AIZZ3JDPC

Combined

Cipher

1. UZJYYGZT3KCIWF2UEHA0657WCVPFKBOV6YVD366IENY3CKTPA2

Cipher

2. 3WD7IQJ3AUSE7HWCCEH3P2DE7LDPGQSU4SKDDY77DKWY4J24CY

Plain

2. 4H4HOWER3CITE3RAAGE37557CLASSIFICATION3CONFIDENT

Two messages with entirely different plain texts

Plain

1. SHIP3SAILING3TIME3AND3DATE3MUST3NO

Cipher

2. DDKTOIKF3HQW3RVDJH035TCV2MOYQC5HIFK

Combined

Cipher

1. OAJUNQYVZITDQHRRR6TFPAALZ6HKLQLUDGY

Cipher

2. ZE3CHRQWYLUGWVQAEH7DKWFERMRGSLTWHQG

Plain

2. DIXSEL3OIL3TWENTY3WTSMRD3ENG3TGERE3

SECRET

SECRET

~~SECRET~~
~~CONFIDENTIAL~~SIGNIN
Change 2 - cont'd

4. Conclusions: Even with the addition of the transposition, two messages in depth can be read though the unique solution for the transposition and substitution is not usually attained.

The same solution outlined above can be applied to the following cases:

- a. Transposition is applied to plain text before substitution:

$$C_1 = P_1 T + K$$

$$C_2 = P_2 T + K$$

$$C_1 + C_2 = (P_1 + P_2) T + K + K$$

- b. Substitution is followed by transposition which is followed

by a second transposition:

$$C_1 = (P_1 + K_1) T + K_2$$

$$C_2 = (P_2 + K_1) T + K_2$$

$$C_1 + C_2 = (P_1 + P_2) T + (K_1 + K_1) T + K_2 + K_2$$

- c. Transposition is followed by substitution which is followed

by a second transposition:

$$C_1 = (P_1 T_1 + K) T_2$$

$$C_2 = (P_2 T_1 + K) T_2$$

$$C_1 + C_2 = (P_1 + P_2) T_1 T_2 + (K + K) T_2$$

~~SECRET~~
~~CONFIDENTIAL~~

H-3/63

~~TOP SECRET SECURITY INFORMATION~~
~~U. S. EYES ONLY~~

C25.34-503
(52-AFSA-412B3-1)
27 February 1952

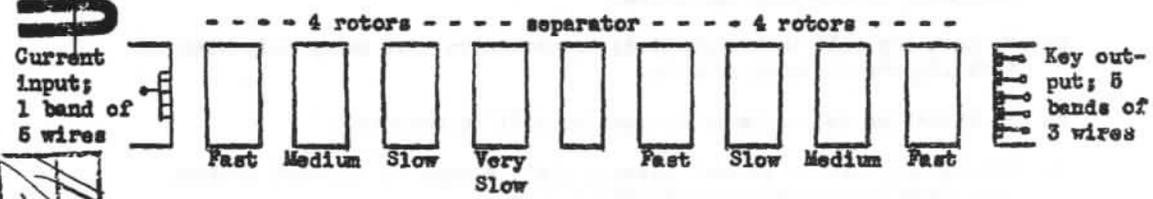
CRYPTOGRAPHIC DATA SHEET

U.S. EYES ONLY

- 1. DESIGNATOR: PANDORA
- 2. SHORT TITLE: SIGNIN (Converter M-294)
- 3. STATUS: Scheduled for use. Category A.
- 4. FUNCTION: Off-line, on-line, and local encipherment and decipherment. May also be used as a teletypewriter for the transmission of plain text.
- 5. CRYPTOGRAPHIC PRINCIPLES: Machine is combined teletypewriter and cipher machine. It generates running key, expressed electrically in 5-baud teletype characters, by passage of current through multiple paths in an 8-rotor maze; and applies this key baud-by-baud to plain text to accomplish encryption, addition following the rule "unlike impulses produce mark impulse".

1-1749-7
NSA LICHT. RY
Copy No. 1

Cryptographic diagram follows:



Do Not Destroy Return to be used as needed
NSA Copy No. 1

Rotors have only the motions indicated. A rotor steps each time the rotor that controls it steps from a notched position. Each rotor has five stepping-control notches arranged around its periphery in accordance with a standard pattern. Rotors are in sets of 10 and wiring is pluggable. All rotors of a set can be interchanged in the eight positions but they cannot be reversed. Current rotors are random wired. A mixed wired separator is permanently located between the 4th and 5th rotor positions. The cycle length is 28^4 .

- KEY LIST DATA: Key lists contain the following information applicable to the operation of the machine for one month:
- a. A regular arrangement of rotors for each 12-hour cryptoperiod of each day.
 - b. Five reserve arrangements with associated reserve system indicators to be used as needed during the month.

RECORD COPY
DO NOT DESTROY OR MUTILATE

Approved for Release by NSA on 03-21-2011, FOIA Case # 62647

~~TOP SECRET~~~~TOP SECRET~~~~U. S. EYES ONLY~~~~U. S. EYES ONLY~~

7 February 1952

- c. A 26-35 check group for each regular rotor arrangement and one for each reserve rotor arrangement.
 - d. A system indicator.
7. INDICATOR SYSTEM: The message rotor alignment is encrypted on a one-time pad to derive a message indicator. The transmitted message set is an eleven letter group. The first three letters indicate the appropriate key-group of the effective one-time pad. The remaining eight letters comprise the message indicator. One-time pads contain approximately 100 pages each. All stations in a particular net hold identical pads. The encipher-decipher cards are Latin squares. Each station in each net is issued a different SEND card. Each receiving station has a RECEIVE copy of that card, identical except in color.
8. SPECIAL PROCEDURES:
- a. A cryptoperiod is 12 hours.
 - b. Messages may be tailed within a 12-hour period; however, rotors will be advanced from 10-35 steps before selecting a new message rotor alignment in off-line operation.
 - c. No pure key will be transmitted; transmission will occur only when intelligence is being passed.
 - d. No bisection and no variable spacing will be required.
 - e. The classification of each message shall always be inserted within the first 25 letters of plain text.
 - f. The first message rotor alignment selected, after any rotor arrangement has been put into effect, may not contain the same letters in positions 1, 5 and 8.
9. CONDITIONS RESULTING IN COMPROMISE OF TRAFFIC ON ONE KEY:
- a. Flagged transmission of message rotor alignment in the clear permits recovery of the rotor arrangement and all traffic for the cryptoperiod can be read.
 - b. Flagged transmission of the 26-35 check group in the clear permits recovery of the rotor arrangement and all traffic for the cryptoperiod can be read.
 - c. Use as a message rotor alignment an alignment closely following the alignment on the rotors at the end of the 25-35 letter check.

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~~~U. S. EYES ONLY~~~~U. S. EYES ONLY~~

27 February 1952

10. CONDITIONS RESULTING IN COMPROMISE OF INDIVIDUAL MESSAGES:

- a. If two or more messages are enciphered in depth, the messages can be read.
- b. If slid depth occurs between messages, it can be located statistically and the overlapping portions of the messages can be read.

11. SPECIAL CONDITIONS:

- a. A plain text crib (approximately 100 letters) can be matched to the cipher text by statistical tests. Pure key is thereby recovered.
- b. If pure key can be obtained for two messages sent with the same rotor arrangement and only one rotor offset between the two encipherments, a basis for rotor recognition exists.
- c. If very long streams of pure key or streams of pure key 26⁵ encipherments apart can be obtained, a basis for rotor recognition exists.

~~TOP SECRET~~