Genevieve Grotjan's Discovery

Chris Christensen
Department of Mathematics and Statistics
Northern Kentucky University

Friday, 20 September 1940, 2:00 pm

“That’s it!’ Everybody crowded around. Friedman came in. “What’s all the noise about?” he asked. Rowlett showed him Grotjan’s findings. He understood immediately. Grotjan’s discovery verified the team’s theory of how the PURPLE machine worked. It marked the climax of one of the greatest cryptanalyses of all time. David Kahn 1991 “Pearl Harbor and the Inadequacy of Cryptanalysis” *Cryptologia* 15(4), 273 – 294.

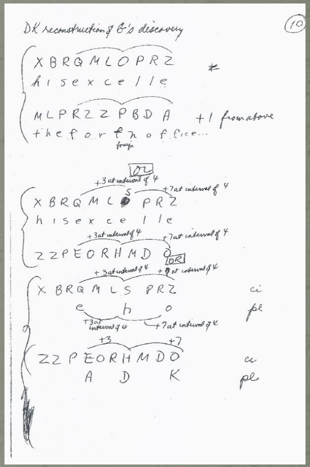
What Grotjan discovered

Frank Rowlett

Rowlett: “… the first case of positive evidence that we were on the proper course to a full recovery of the PURPLE machine.”

The Dr. David Kahn Collection

The Dr. David Kahn Collection



DK reconstruction of G's discovery (10)

XBRQMLOPRZ ≠
hisexcelle

MLPRZZPBDA +1 from above
the for fn of fice...
foreign

OL
+3 at interval of 4 +7 at interval of 4
S
XBRQML PRZ
hisexce lle
+3 at interval of 4 +7 at interval of 4
ZZPEORHMD O
OR
+3 at interval of 4 +? at interval of 4
XBRQMLS PRZ ci
e h o pl
+3 at interval of 4 +7 at interval of 4
+3 +7
ZZPEORHMDO ci
A D K pl

12 May 1991

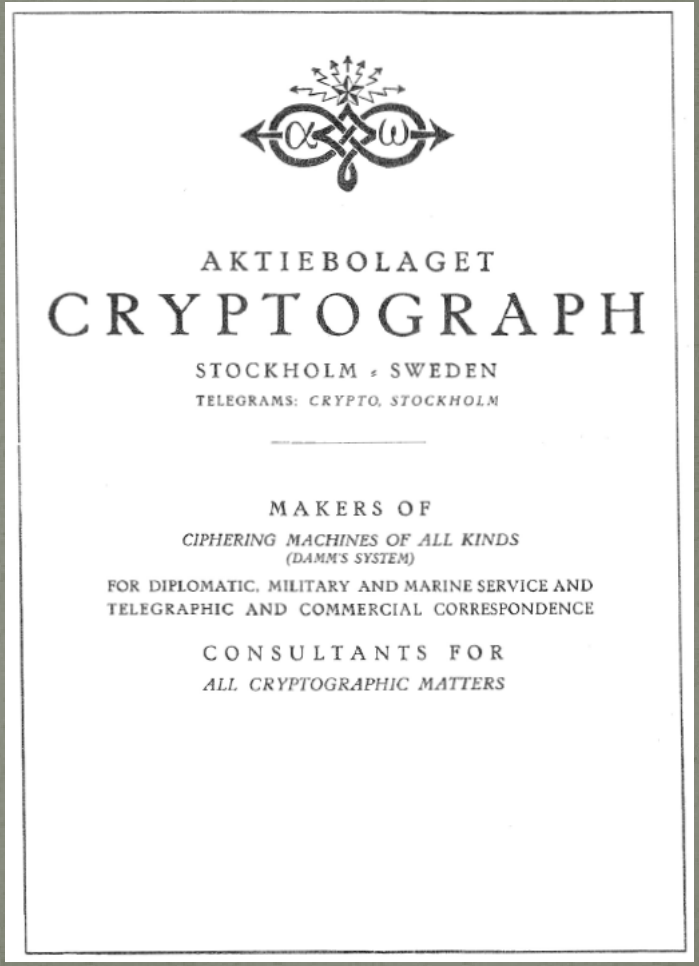
Japanese cipher machines

1931 models

RED, ORANGE, and M-2

Damm’s machines

Pronounceable ciphertext.



AKTIEBOLAGET

CRYPTOGRAPH

STOCKHOLM : SWEDEN

TELEGRAMS: *CRYPTO, STOCKHOLM*

MAKERS OF

CIPHERING MACHINES OF ALL KINDS
(DAMM'S SYSTEM)

FOR DIPLOMATIC, MILITARY AND MARINE SERVICE AND
TELEGRAPHIC AND COMMERCIAL CORRESPONDENCE

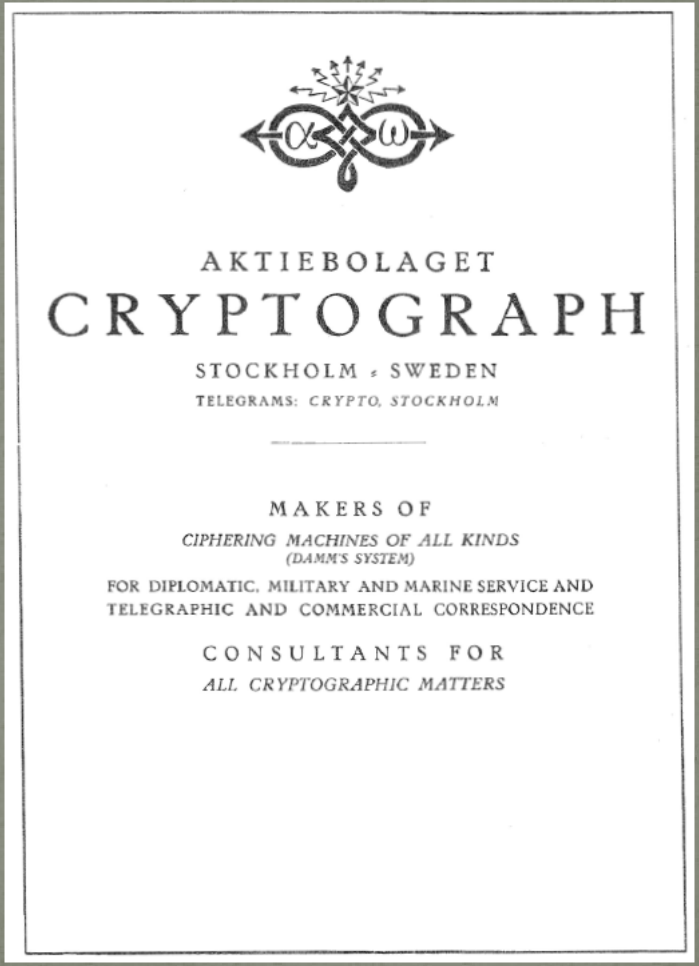
CONSULTANTS FOR

ALL CRYPTOGRAPHIC MATTERS

Damm's machines

Pronounceable ciphertext.

Half-rotor.



AKTIEBOLAGET

CRYPTOGRAPH

STOCKHOLM - SWEDEN

TELEGRAMS: *CRYPTO, STOCKHOLM*

MAKERS OF

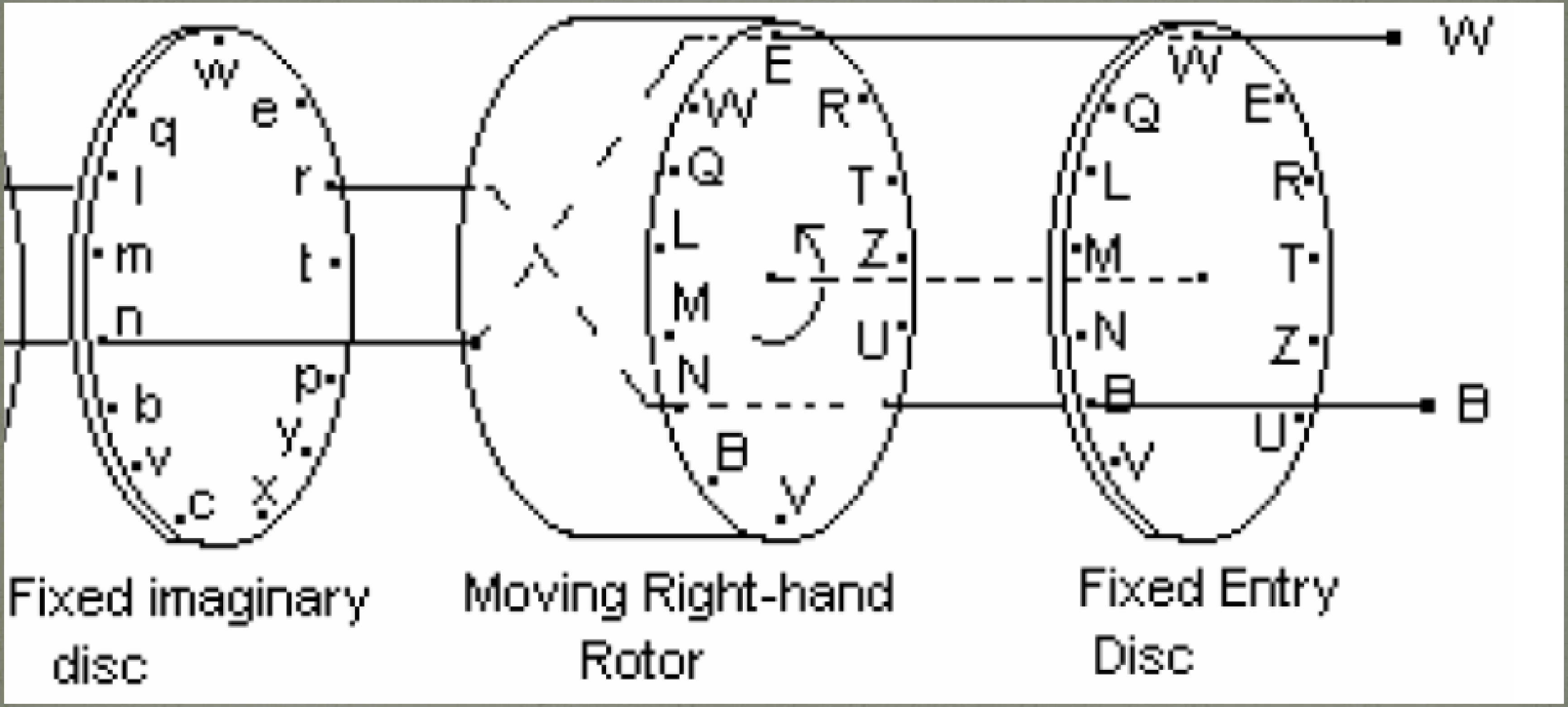
CIPHERING MACHINES OF ALL KINDS
(DAMM'S SYSTEM)

FOR DIPLOMATIC, MILITARY AND MARINE SERVICE AND
TELEGRAPHIC AND COMMERCIAL CORRESPONDENCE

CONSULTANTS FOR

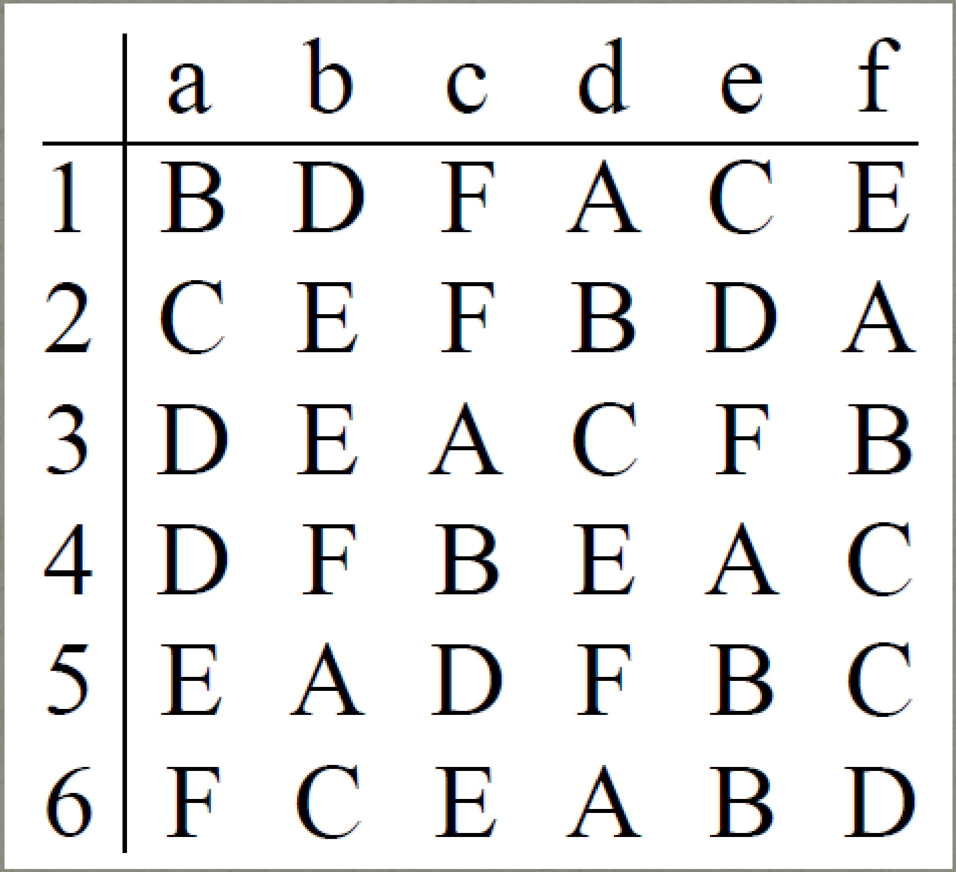
ALL CRYPTOGRAPHIC MATTERS

Full rotor



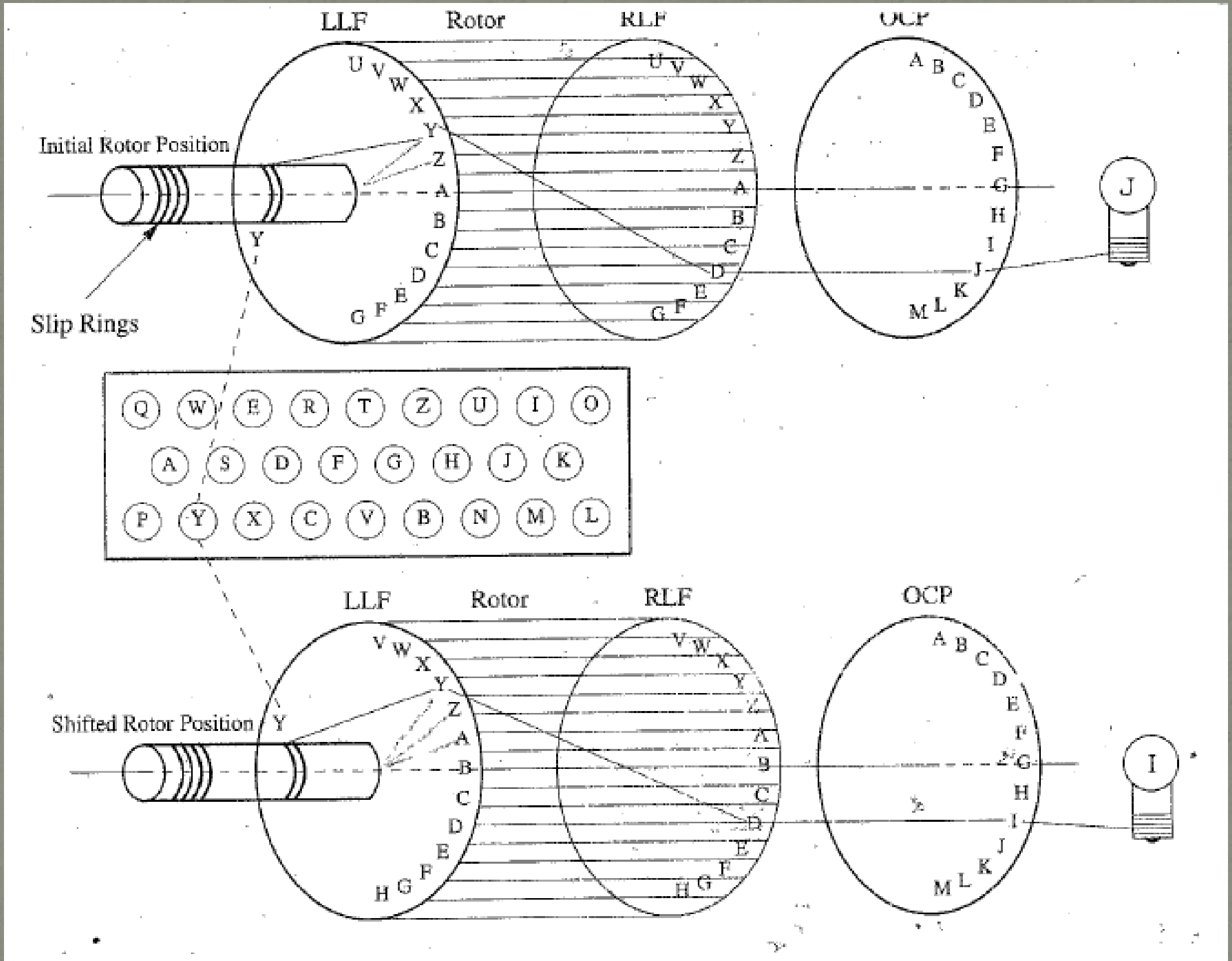
Frank Carter

Full rotor



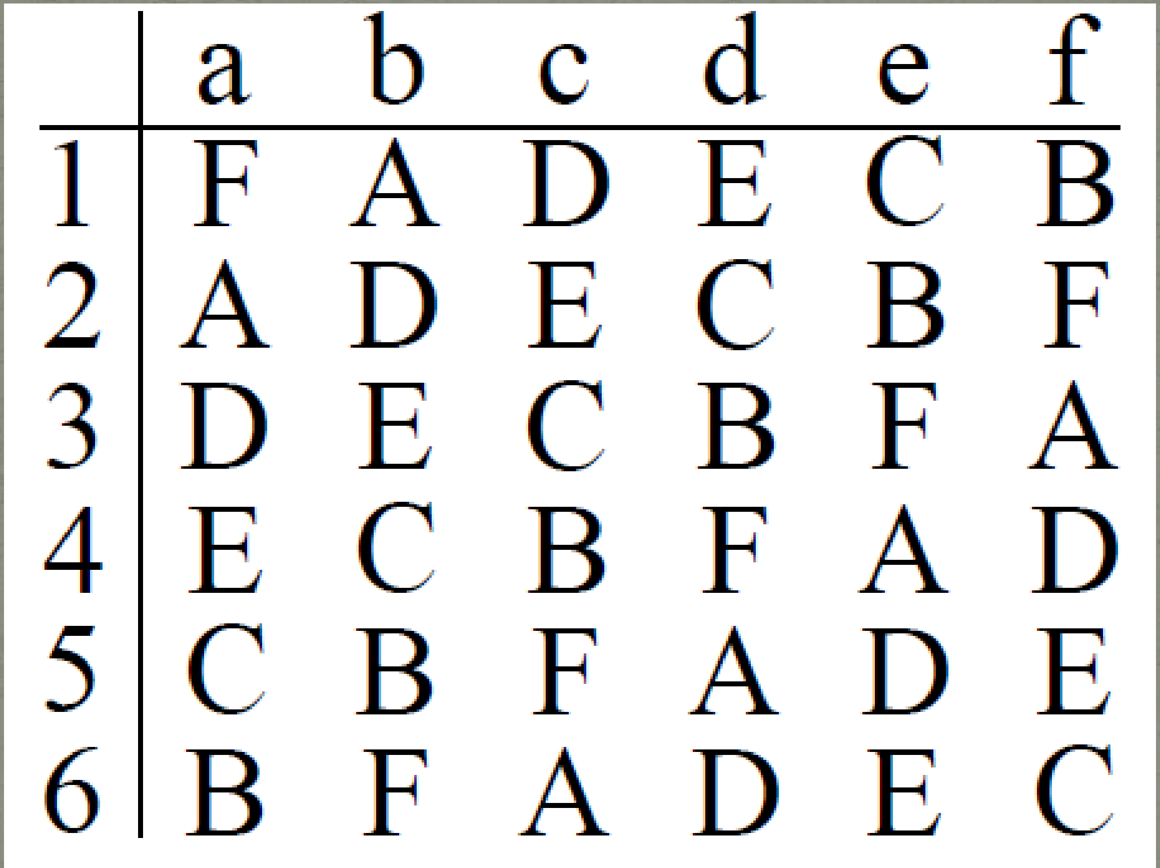
	a	b	c	d	e	f
1	B	D	F	A	C	E
2	C	E	F	B	D	A
3	D	E	A	C	F	B
4	D	F	B	E	A	C
5	E	A	D	F	B	C
6	F	C	E	A	B	D

Damm Half-Rotor



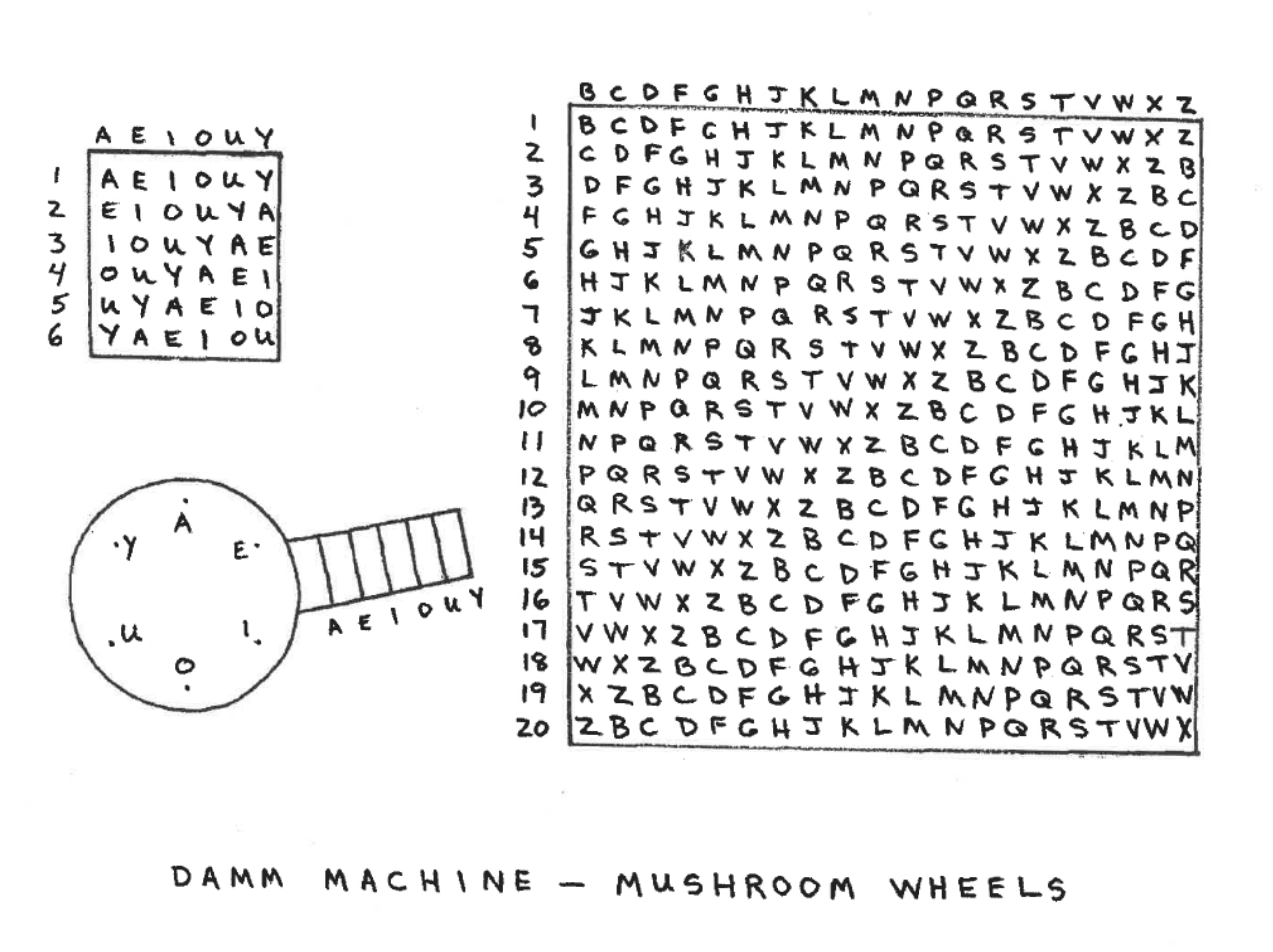
Konheim *Computer Security and Cryptography*

Half-rotor pattern



	a	b	c	d	e	f
1	F	A	D	E	C	B
2	A	D	E	C	B	F
3	D	E	C	B	F	A
4	E	C	B	F	A	D
5	C	B	F	A	D	E
6	B	F	A	D	E	C

6s and 20s



	A	E	I	O	U	Y
1	A	E	I	O	U	Y
2	E	I	O	U	Y	A
3	I	O	U	Y	A	E
4	O	U	Y	A	E	I
5	U	Y	A	E	I	O
6	Y	A	E	I	O	U

	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z
1	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z
2	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z	B
3	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z	B	C
4	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z	B	C	D
5	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z	B	C	D	F
6	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z	B	C	D	F	G
7	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z	B	C	D	F	G	H
8	K	L	M	N	P	Q	R	S	T	V	W	X	Z	B	C	D	F	G	H	J
9	L	M	N	P	Q	R	S	T	V	W	X	Z	B	C	D	F	G	H	J	K
10	M	N	P	Q	R	S	T	V	W	X	Z	B	C	D	F	G	H	J	K	L
11	N	P	Q	R	S	T	V	W	X	Z	B	C	D	F	G	H	J	K	L	M
12	P	Q	R	S	T	V	W	X	Z	B	C	D	F	G	H	J	K	L	M	N
13	Q	R	S	T	V	W	X	Z	B	C	D	F	G	H	J	K	L	M	N	P
14	R	S	T	V	W	X	Z	B	C	D	F	G	H	J	K	L	M	N	P	Q
15	S	T	V	W	X	Z	B	C	D	F	G	H	J	K	L	M	N	P	Q	R
16	T	V	W	X	Z	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S
17	V	W	X	Z	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T
18	W	X	Z	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V
19	X	Z	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W
20	Z	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X

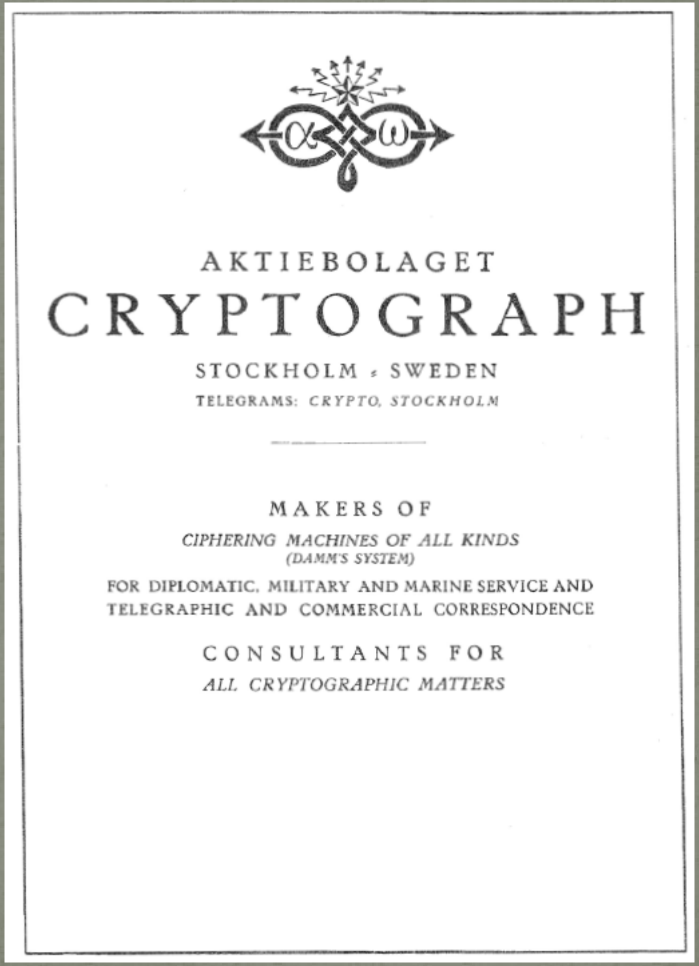
DAMM MACHINE — MUSHROOM WHEELS

Damm's machines

Pronounceable ciphertext.

Half-rotor.

Staggered motion.



AKTIEBOLAGET

CRYPTOGRAPH

STOCKHOLM - SWEDEN

TELEGRAMS: *CRYPTO, STOCKHOLM*

MAKERS OF

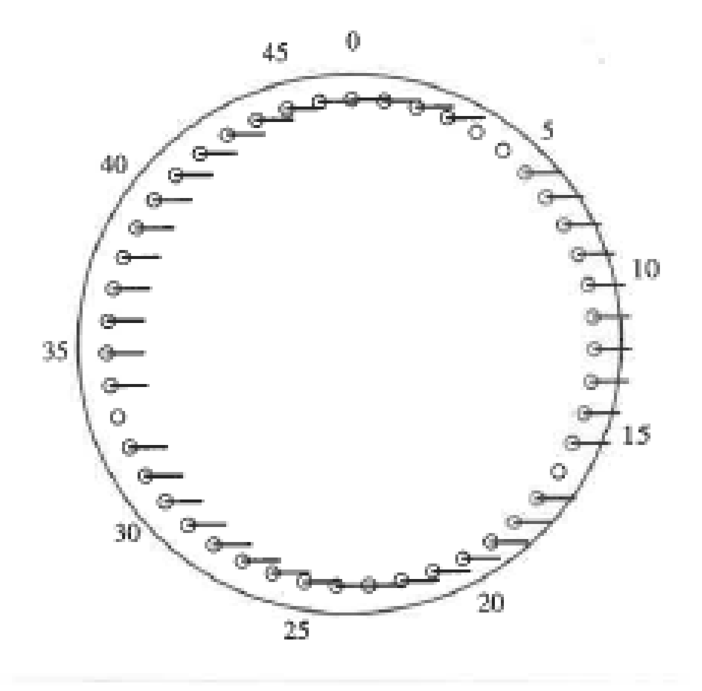
CIPHERING MACHINES OF ALL KINDS
(DAMM'S SYSTEM)

FOR DIPLOMATIC, MILITARY AND MARINE SERVICE AND TELEGRAPHIC AND COMMERCIAL CORRESPONDENCE

CONSULTANTS FOR

ALL CRYPTOGRAPHIC MATTERS

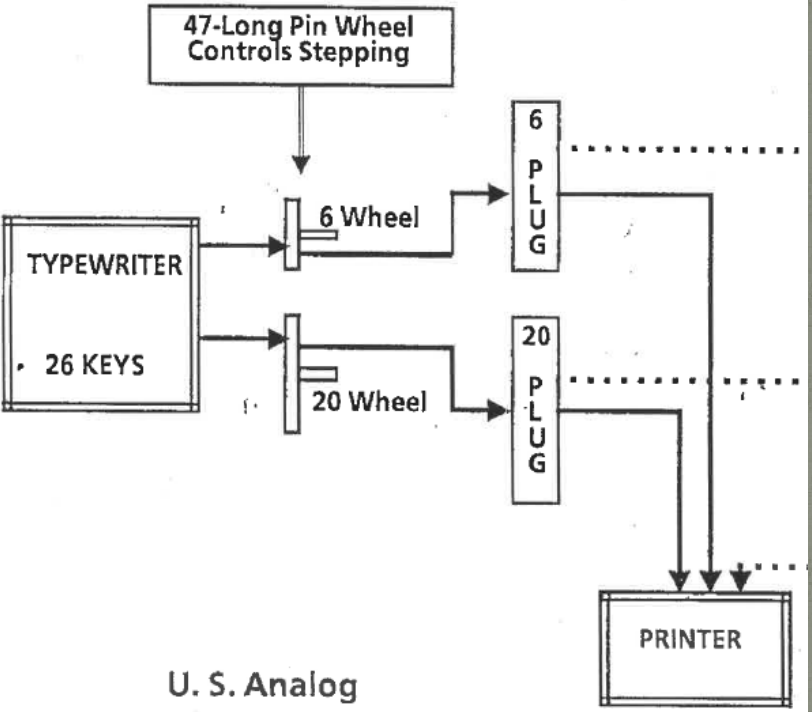
Breakwheel



Konheim *Computer Security and Cryptography*

RED M-3

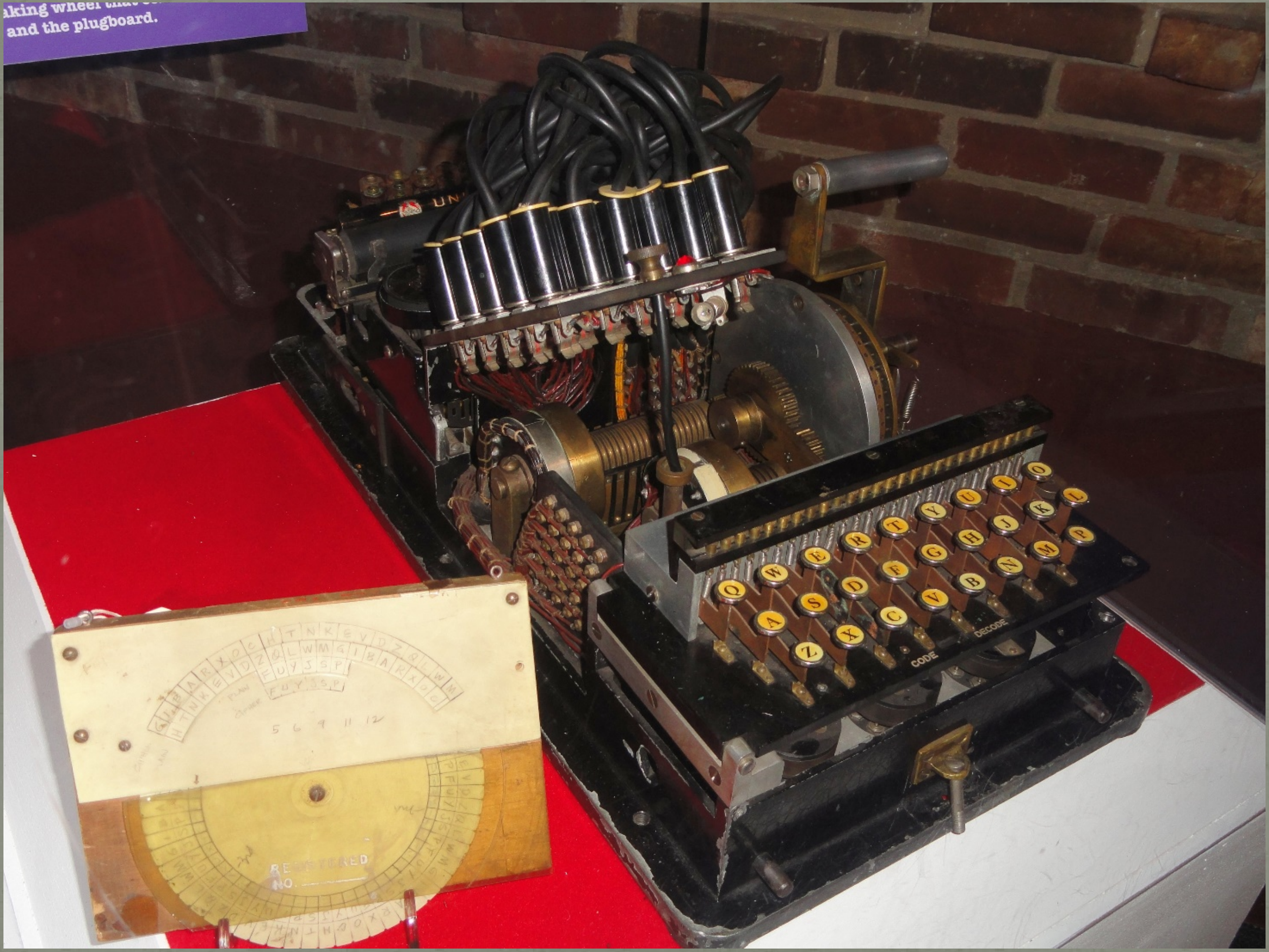
RED



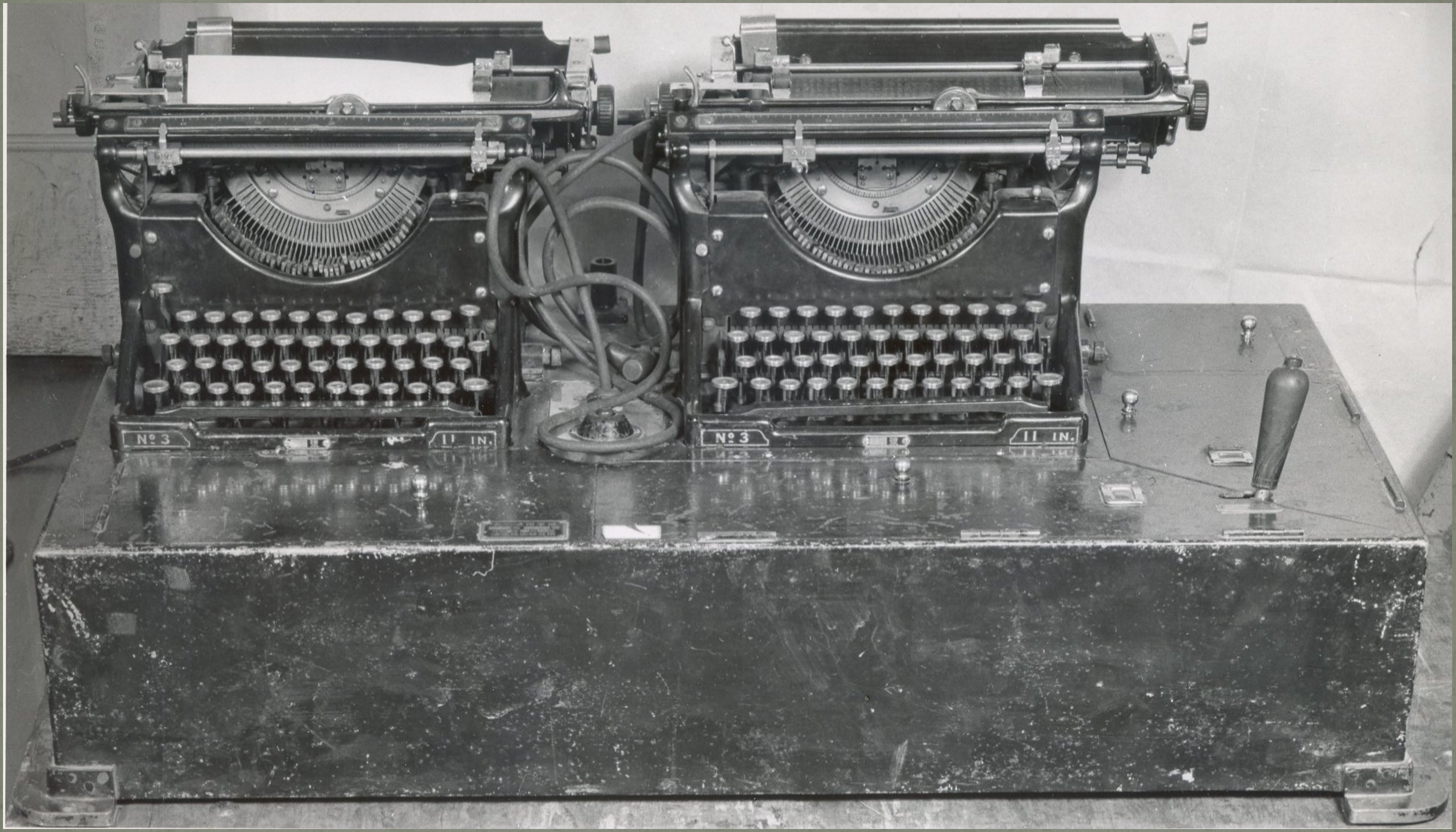
U. S. Analog

6 and 20 wheels step together 1, 2, or 3 times according as 47-wheel has 0, 1, or 2 inactive pins. The 47-wheel steps once per encipherment.
The machine can run in reverse.
Only encipherment paths are shown.

RED analogs


aking wheel that
and the plugboard.
CODE
DECODE
REGISTERED
NO.

ORANGE M-1

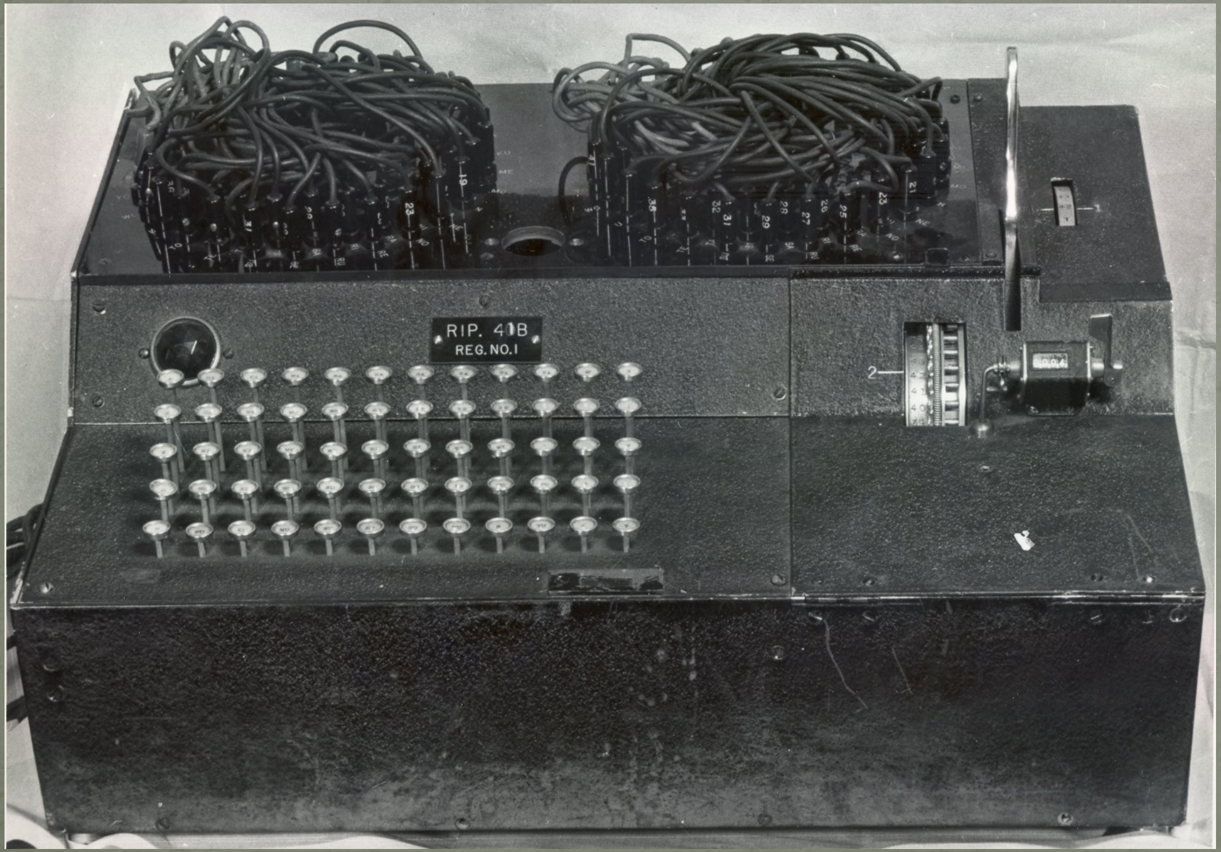


Two machines were capture in Rashin, Korea after World War II.

ORANGE analog

Jack S. Holtwick

Agnes Driscoll



Japanese cipher machines

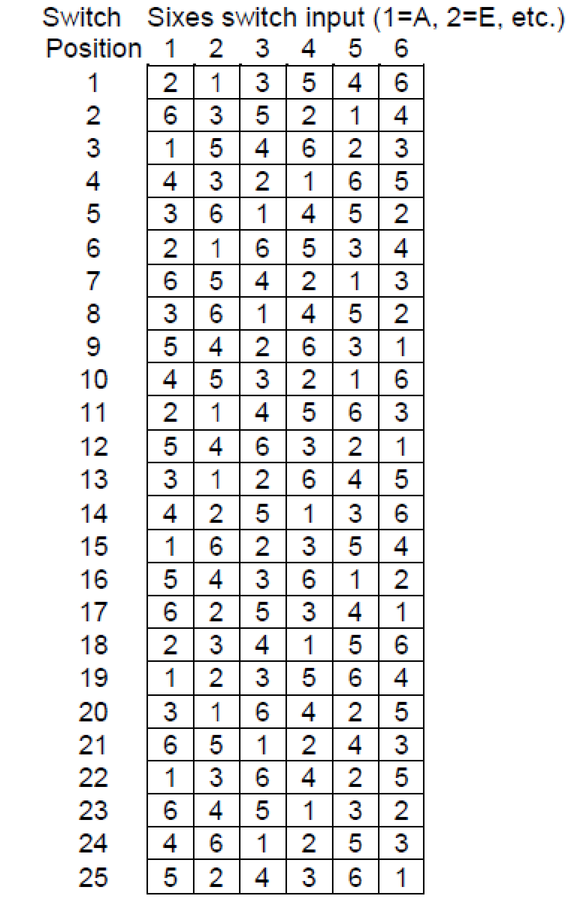
1937 models

PURPLE, JADE, and CORAL

PURPLE

The sixes

The sixes

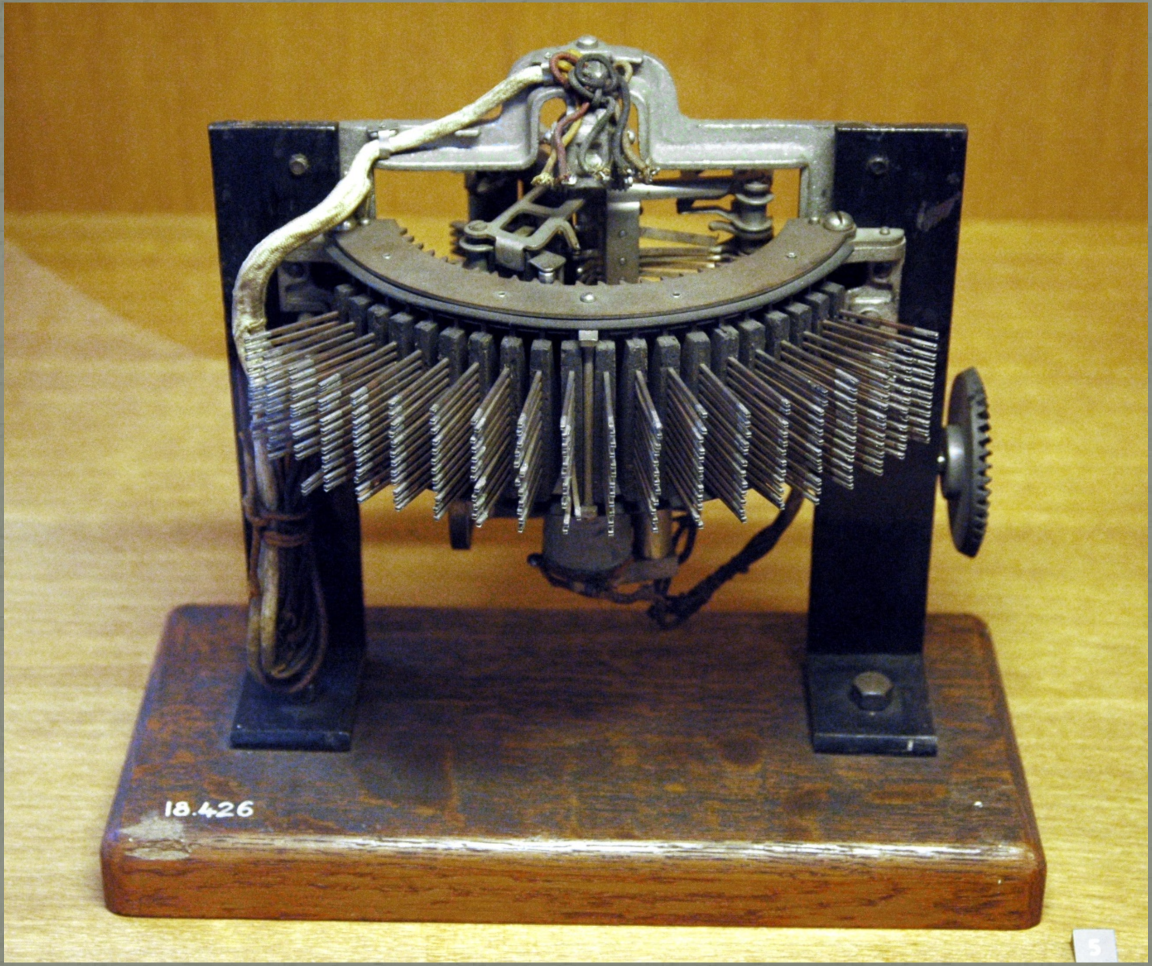


Switch	Sixes switch input (1=A, 2=E, etc.)					
Position	1	2	3	4	5	6
1	2	1	3	5	4	6
2	6	3	5	2	1	4
3	1	5	4	6	2	3
4	4	3	2	1	6	5
5	3	6	1	4	5	2
6	2	1	6	5	3	4
7	6	5	4	2	1	3
8	3	6	1	4	5	2
9	5	4	2	6	3	1
10	4	5	3	2	1	6
11	2	1	4	5	6	3
12	5	4	6	3	2	1
13	3	1	2	6	4	5
14	4	2	5	1	3	6
15	1	6	2	3	5	4
16	5	4	3	6	1	2
17	6	2	5	3	4	1
18	2	3	4	1	5	6
19	1	2	3	5	6	4
20	3	1	6	4	2	5
21	6	5	1	2	4	3
22	1	3	6	4	2	5
23	6	4	5	1	3	2
24	4	6	1	2	5	3
25	5	2	4	3	6	1

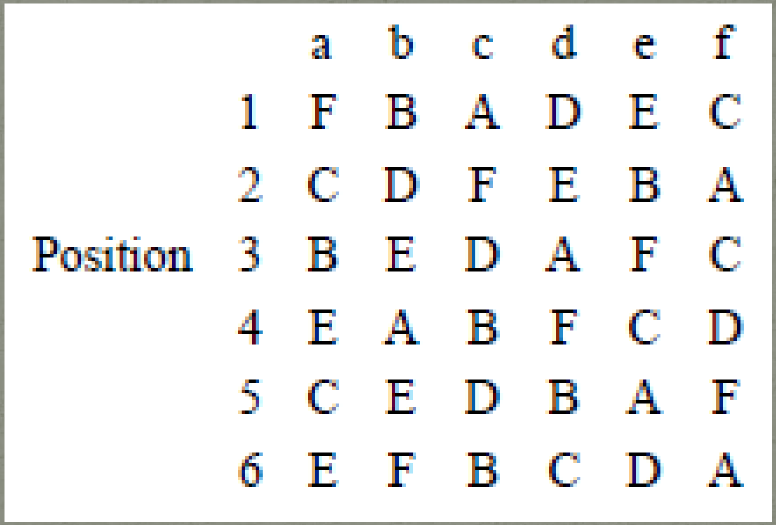
Figure 6. Sixes stepping switch - Decipher mode.

PURPLE Revealed Freeman, Sullivan, and Weierud

Telephone stepping switch



Switch (no) pattern



		a	b	c	d	e	f
Position	1	F	B	A	D	E	C
	2	C	D	F	E	B	A
	3	B	E	D	A	F	C
	4	E	A	B	F	C	D
	5	C	E	D	B	A	F
	6	E	F	B	C	D	A

PURPLE

The twenties

William Friedman 14 October 1940

William Friedman

Enciphering “seemed to start from certain initial settings and to progress absolutely methodically without cyclic repetition of any sort, straight through to the end of the messages”.

Switches

Rowlett: “From the moment that we found that a conventional telephone stepping switch provided a completely satisfactory basis for building a cryptographic mechanism for deciphering the six-letter component, all of us who were working on the Japanese diplomatic cipher machine speculated that the Japanese might have utilized these switches as a basis of the PURPLE machine.”

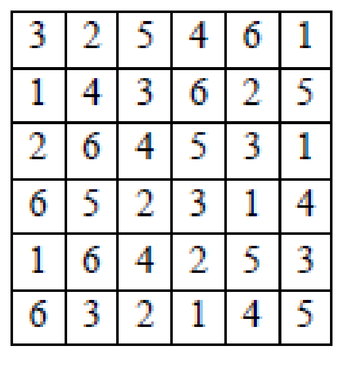
What they were trying to find

Rowlett: "The problem was to search through these messages for a particular phenomenon which we had identified grossly but had to be identified finally by discovery. So we were looking for this phenomenon without actually being aware of precisely what we were seeking."

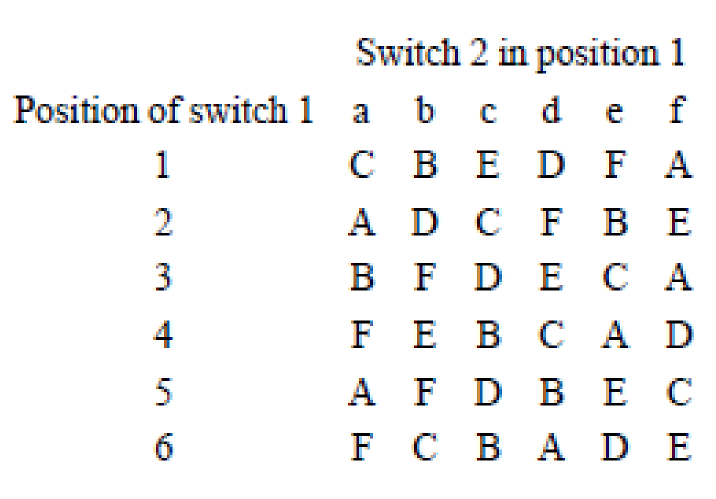
Friedman

Attempt to establish cipher sequences of those found with half-rotors, rotors, and the like.

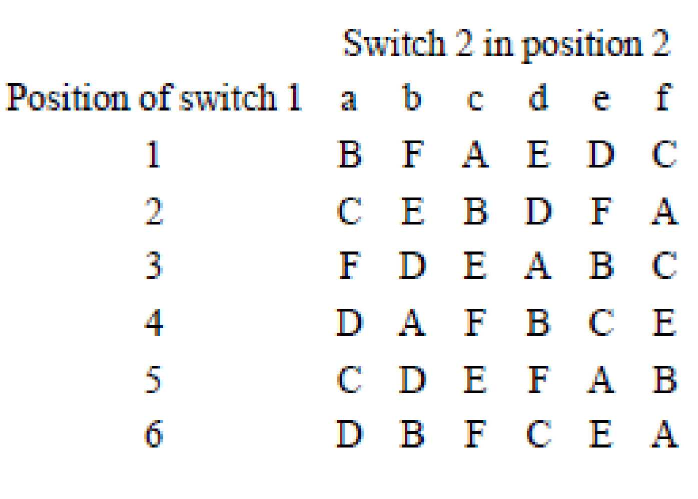
1F2S Isomorphism



3	2	5	4	6	1
1	4	3	6	2	5
2	6	4	5	3	1
6	5	2	3	1	4
1	6	4	2	5	3
6	3	2	1	4	5

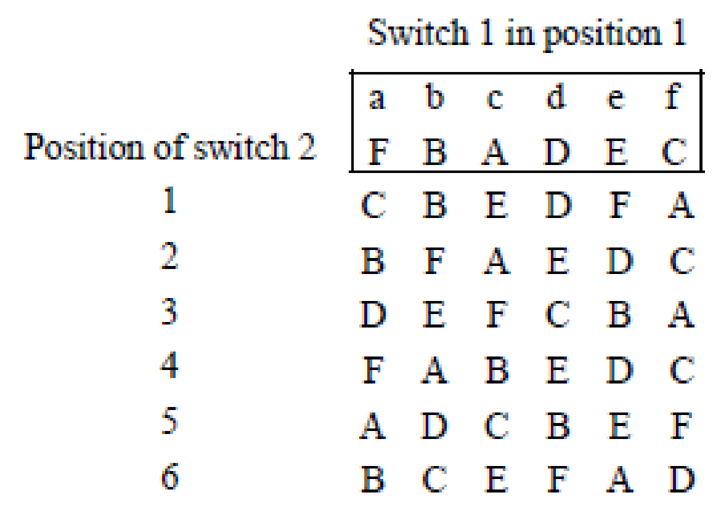


	Switch 2 in position 1					
Position of switch 1	a	b	c	d	e	f
1	C	B	E	D	F	A
2	A	D	C	F	B	E
3	B	F	D	E	C	A
4	F	E	B	C	A	D
5	A	F	D	B	E	C
6	F	C	B	A	D	E

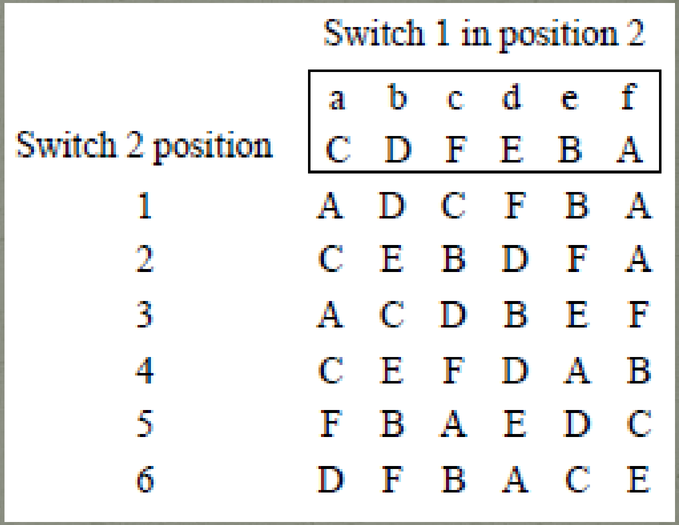


	Switch 2 in position 2					
Position of switch 1	a	b	c	d	e	f
1	B	F	A	E	D	C
2	C	E	B	D	F	A
3	F	D	E	A	B	C
4	D	A	F	B	C	E
5	C	D	E	F	A	B
6	D	B	F	C	E	A

1S2F Repeated columns



	Switch 1 in position 1					
	a	b	c	d	e	f
Position of switch 2	F	B	A	D	E	C
1	C	B	E	D	F	A
2	B	F	A	E	D	C
3	D	E	F	C	B	A
4	F	A	B	E	D	C
5	A	D	C	B	E	F
6	B	C	E	F	A	D



	Switch 1 in position 2					
	a	b	c	d	e	f
Switch 2 position	C	D	F	E	B	A
1	A	D	C	F	B	A
2	C	E	B	D	F	A
3	A	C	D	B	E	F
4	C	E	F	D	A	B
5	F	B	A	E	D	C
6	D	F	B	A	C	E

William Friedman 14 October 1940

Two messages on the same day with identical indicators appeared to be identically enciphered.

William Friedman 14 October 1940

Two messages on the same day with identical indicators appeared to be identically enciphered.

Two messages with identical indicators on different days were absolutely different.

William Friedman 14 October 1940

Two messages on the same day with identical indicators appeared to be identically enciphered.

Two messages with identical indicators on different days were absolutely different.

Two messages with different indicators on the same day were absolutely different.

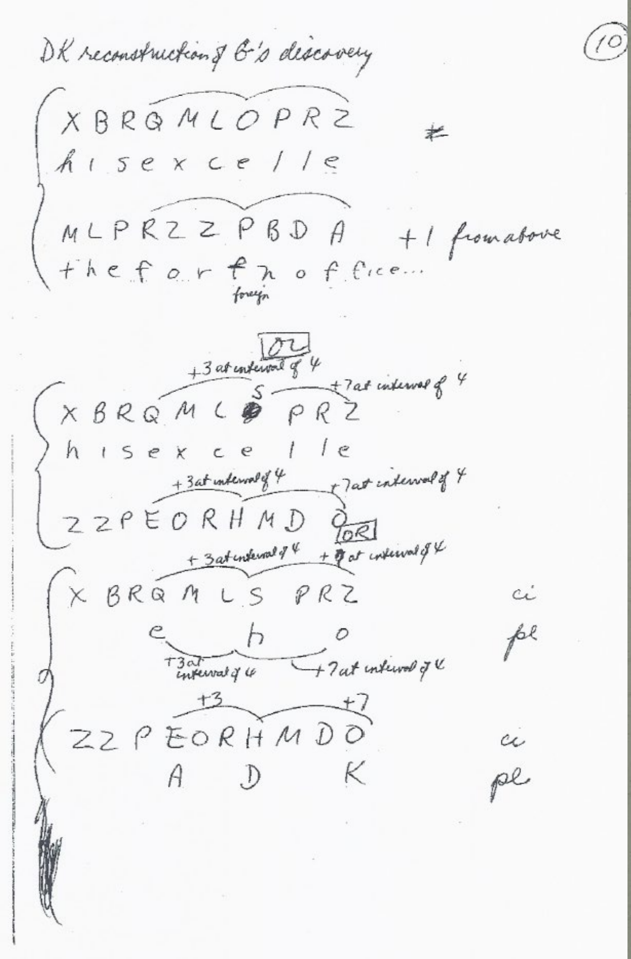
Friedman

It was thought to take messages from different days with the same indicators and reduce them to the same base.

The method succeeded in two cases:

The case of indicator 59173 consisted of 6 messages.

Grotjan's examples



DK reconstruction of G's discovery

(10)

XBRQMLOPRZ ≠

h i s e x c e l l e

MLPRZZPBDA +1 from above

t h e f o r f n o f f i c e...

foreign

OR

+3 at interval of 4

+7 at interval of 4

XBRQMLS PRZ

h i s e x c e l l e

+3 at interval of 4

+7 at interval of 4

ZZPEORHMDO

OR

+3 at interval of 4

+7 at interval of 4

XBRQMLS PRZ ci

e h o pl

+3 at interval of 4

+7 at interval of 4

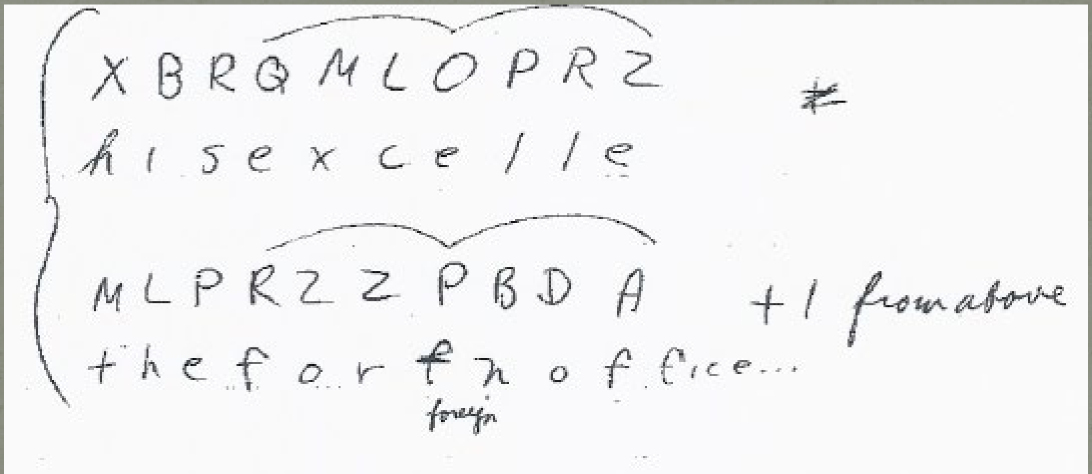
+3

+7

ZZPEORHMDO ci

A D K pl

Example one



X B R Q M L O P R Z ≠

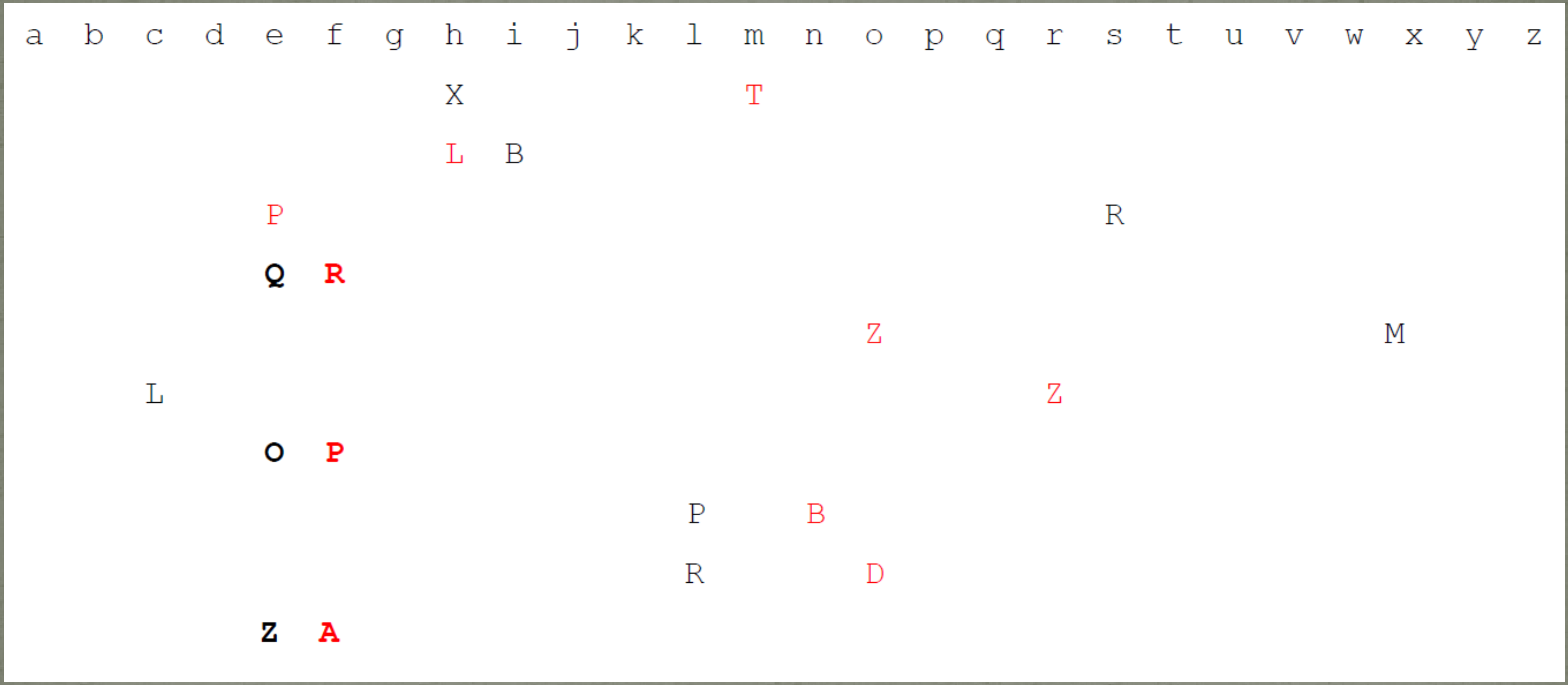
h i s e x c e l l e

M L P R Z Z P B D A +1 from above

t h e f o r f n o f f i c e...

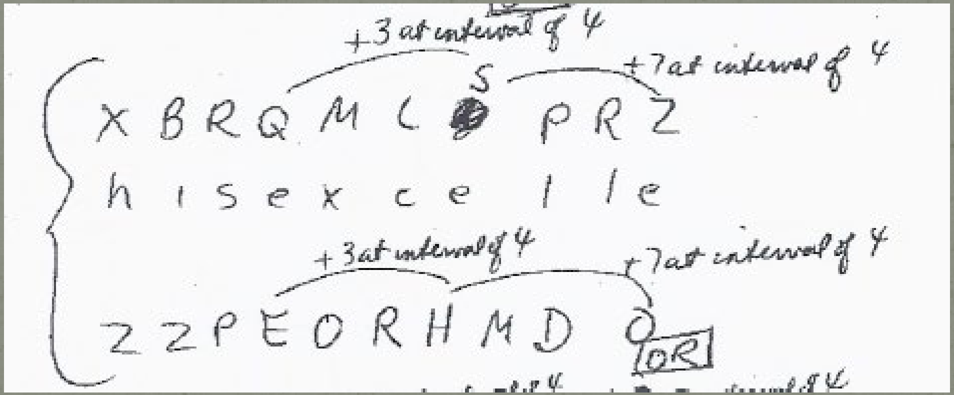
foreign

Example one: "+ 1 from above"



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					T													
							L	B																	
				P														R							
				Q	**R**																				
														Z									M		
		L															Z								
				O	**P**																				
											P		B												
											R			D											
				Z	**A**																				

Example two



+3 at interval of 4

S +7 at interval of 4

X B R Q M L P R Z

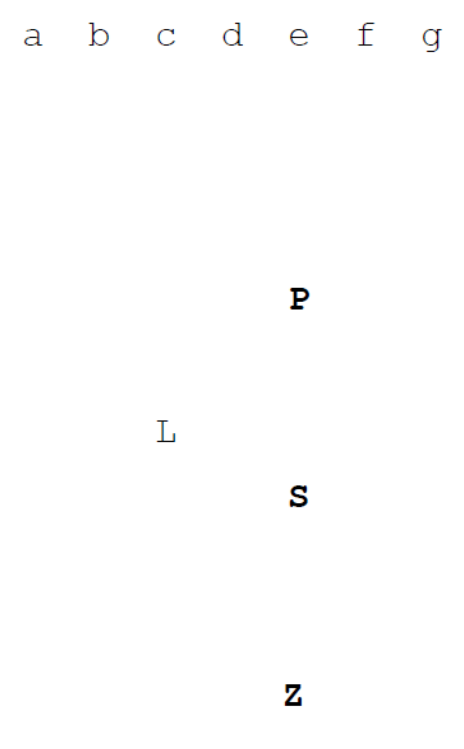
h i s e x c e l l e

+3 at interval of 4 +7 at interval of 4

Z Z P E O R H M D Q OR

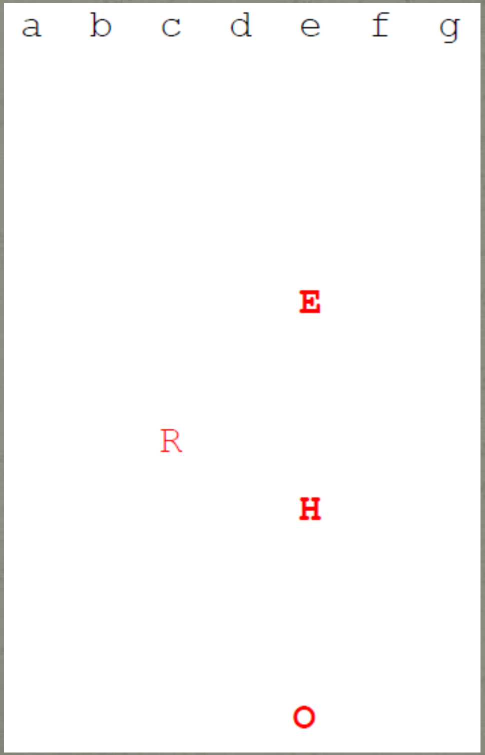
Example two: "+ 3 at an interval of 4, + 7…"

Ciphertext one



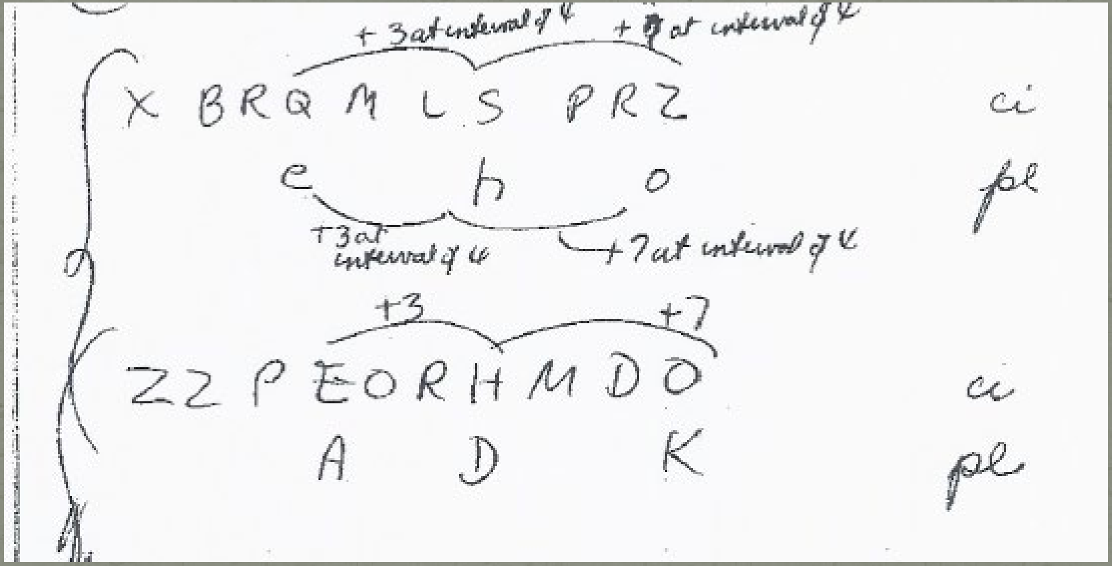
a	b	c	d	e	f	g
				P		
		L				
				S		
				Z		

Ciphertext two



a	b	c	d	e	f	g
				E		
		R				
				H		
				O		

Example three



+ 3 at interval of 4 + 7 at interval of 4

X BRQ M L S PRZ ci

e h o pl

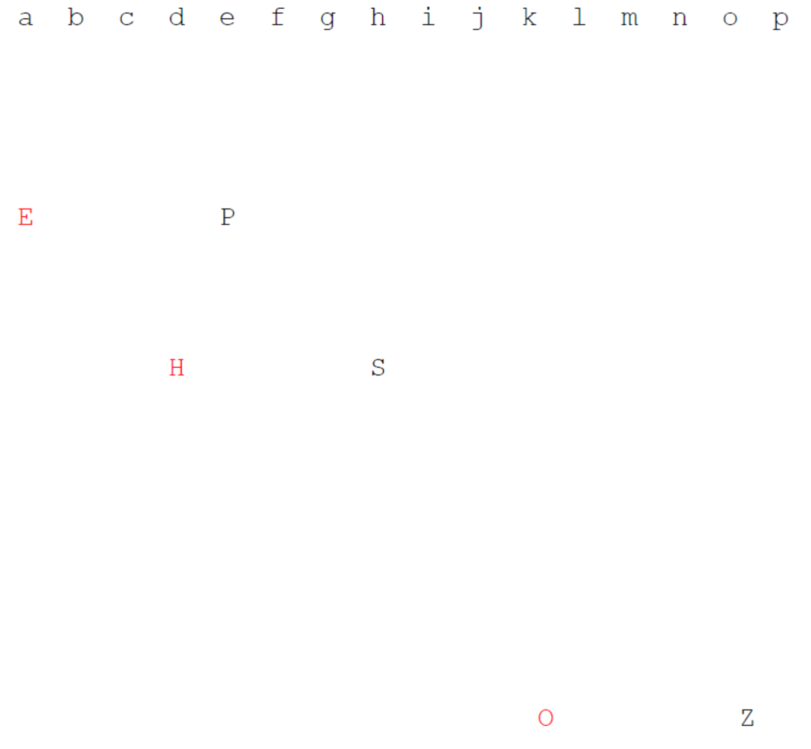
+3 at interval of 4 + 7 at interval of 4

+3 +7

ZZ P EORHMDO ci

A D K pl

Example three: "+ 3 at an interval of 4, + 7..."

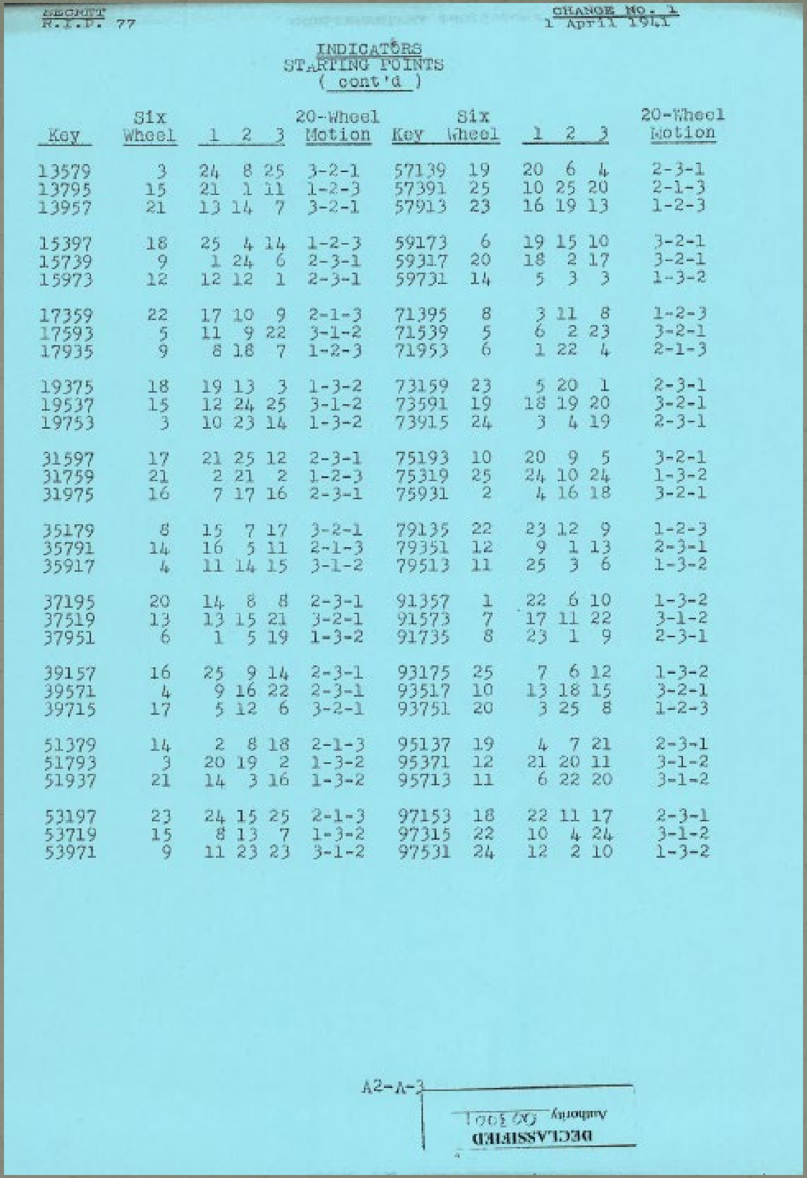


a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
E				P											
			H				S								
										O				Z	

Grotjan

We could see “a” in a certain position, and we could see “a” being enciphered by “B,” in another place by “D” and in another by “E” …, and if we found the same sequence in a different letter, or in a different position with respect to a different letter but spacing of letters the same.

59173



SECRET
R.I.P. 77

CHANGE NO. 1
1 April 1941

INDICATORS
STARTING POINTS
(cont'd)

	Six				20-Wheel		Six				20-Wheel
Key	Wheel	1	2	3	Motion	Key	Wheel	1	2	3	Motion
13579	3	24	8	25	3-2-1	57139	19	20	6	4	2-3-1
13795	15	21	1	11	1-2-3	57391	25	10	25	20	2-1-3
13957	21	13	14	7	3-2-1	57913	23	16	19	13	1-2-3
15397	18	25	4	14	1-2-3	59173	6	19	15	10	3-2-1
15739	9	1	24	6	2-3-1	59317	20	18	2	17	3-2-1
15973	12	12	12	1	2-3-1	59731	14	5	3	3	1-3-2
17359	22	17	10	9	2-1-3	71395	8	3	11	8	1-2-3
17593	5	11	9	22	3-1-2	71539	5	6	2	23	3-2-1
17935	9	8	18	7	1-2-3	71953	6	1	22	4	2-1-3
19375	18	19	13	3	1-3-2	73159	23	5	20	1	2-3-1
19537	15	12	24	25	3-1-2	73591	19	18	19	20	3-2-1
19753	3	10	23	14	1-3-2	73915	24	3	4	19	2-3-1
31597	17	21	25	12	2-3-1	75193	10	20	9	5	3-2-1
31759	21	2	21	2	1-2-3	75319	25	24	10	24	1-3-2
31975	16	7	17	16	2-3-1	75931	2	4	16	18	3-2-1
35179	8	15	7	17	3-2-1	79135	22	23	12	9	1-2-3
35791	14	16	5	11	2-1-3	79351	12	9	1	13	2-3-1
35917	4	11	14	15	3-1-2	79513	11	25	3	6	1-3-2
37195	20	14	8	8	2-3-1	91357	1	22	6	10	1-3-2
37519	13	13	15	21	3-2-1	91573	7	17	11	22	3-1-2
37951	6	1	5	19	1-3-2	91735	8	23	1	9	2-3-1
39157	16	25	9	14	2-3-1	93175	25	7	6	12	1-3-2
39571	4	9	16	22	2-3-1	93517	10	13	18	15	3-2-1
39715	17	5	12	6	3-2-1	93751	20	3	25	8	1-2-3
51379	14	2	8	18	2-1-3	95137	19	4	7	21	2-3-1
51793	3	20	19	2	1-3-2	95371	12	21	20	11	3-1-2
51937	21	14	3	16	1-3-2	95713	11	6	22	20	3-1-2
53197	23	24	15	25	2-1-3	97153	18	22	11	17	2-3-1
53719	15	8	13	7	1-3-2	97315	22	10	4	24	3-1-2
53971	9	11	23	23	3-1-2	97531	24	12	2	10	1-3-2

A2-A-3

F M S
3 2 1

What was found

Friedman: “Careful examination disclosed the presence of repeated sequences, here and there.”

What was found

Friedman: “[C]areful examination disclosed the presence of repeated sequences, here and there.”

Raven: “Finally one of the clerks recording recoveries in the entry book noticed repeating columns and it was immediately obvious to all that the entire machine was wipers.”

Francis Raven

What was found

Grotjan:

“… could fit several enciphering sequences in proper intervals.”

What was found

Grotjan:

“… could fit several enciphering sequences in proper intervals.”

“… it confirmed something about the encipherment – wheel advancement.”

What was found

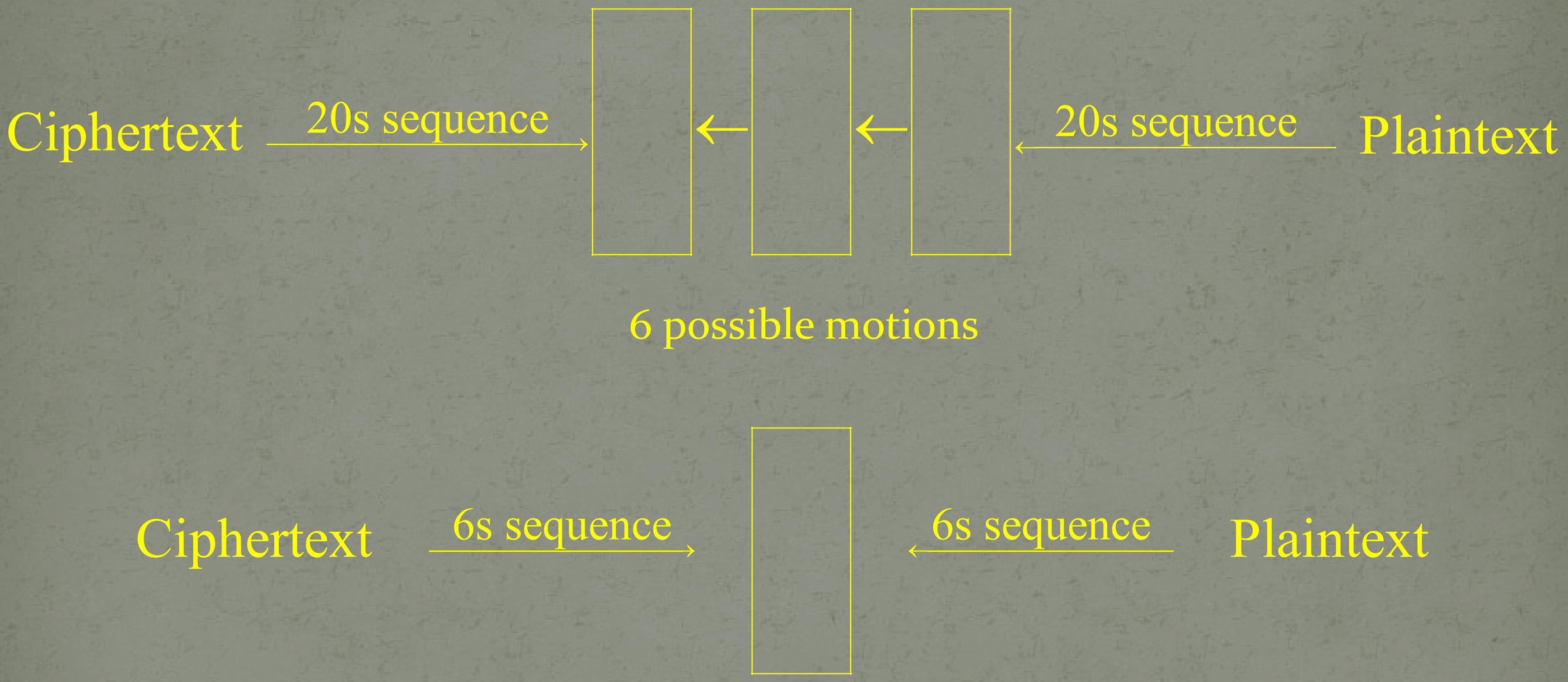
Grotjan:

“… could fit several enciphering sequences in proper intervals.”

“… it confirmed something about the encipherment – wheel advancement.”

“… there was an orderly progression of the encipherment as the message text advanced a letter at a time.”

PURPLE

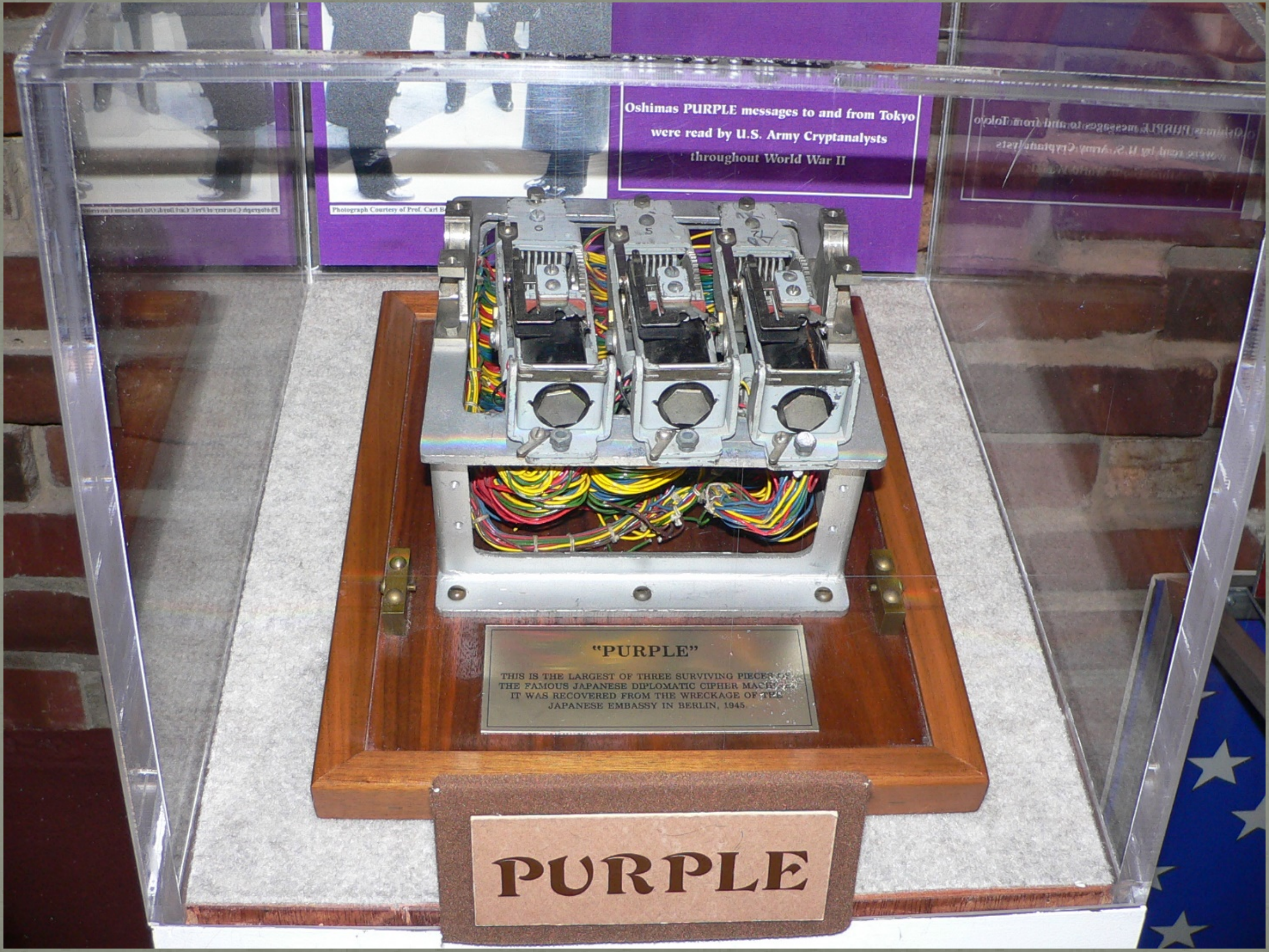


Ciphertext 20s sequence ← ← 20s sequence Plaintext

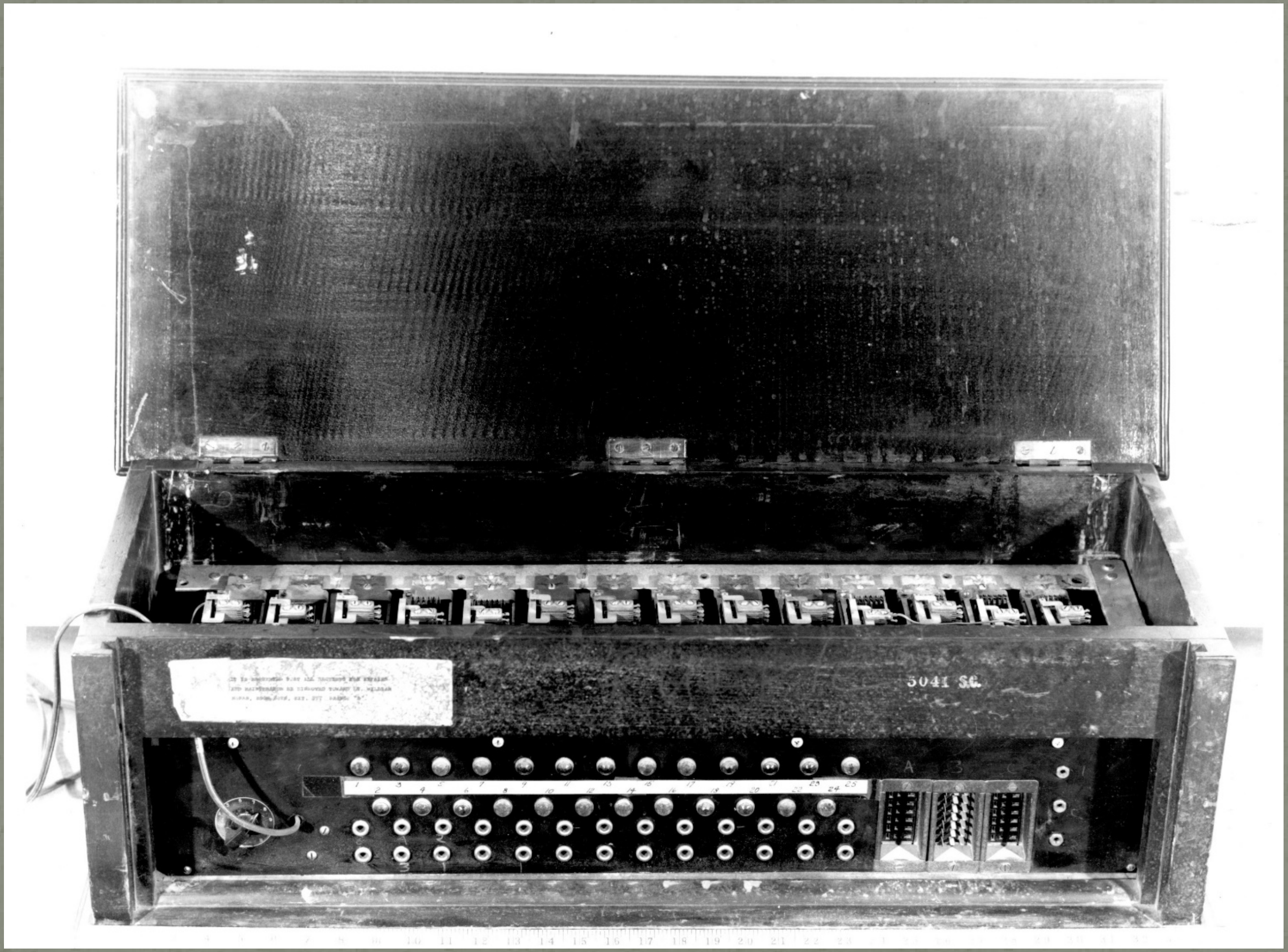
6 possible motions

Ciphertext 6s sequence 6s sequence Plaintext

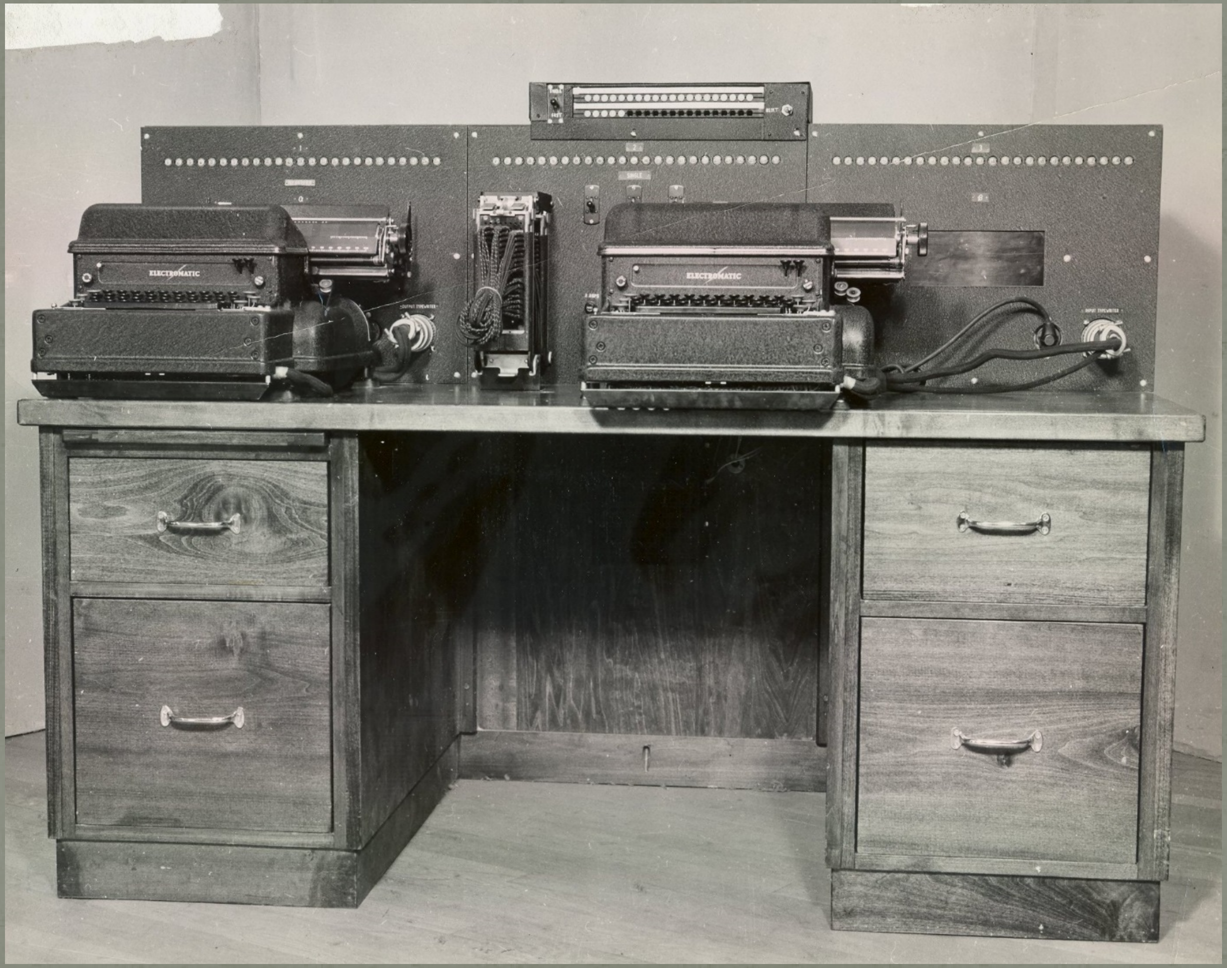
PURPLE


Oshimas PURPLE messages to and from Tokyo
were read by U.S. Army Cryptanalysts
throughout World War II
Photograph Courtesy of Prof. Carl B
"PURPLE"
THIS IS THE LARGEST OF THREE SURVIVING PIECES OF
THE FAMOUS JAPANESE DIPLOMATIC CIPHER MACHINE.
IT WAS RECOVERED FROM THE WRECKAGE OF THE
JAPANESE EMBASSY IN BERLIN, 1945.
PURPLE

PURPLE analog



Advanced PURPLE analog



ありがと

Liza Mundy for the question
Rene Stein for organizing the Kahn Collection