Enigmatyczna historia Enigmy

Barbara Roszkowska Lech

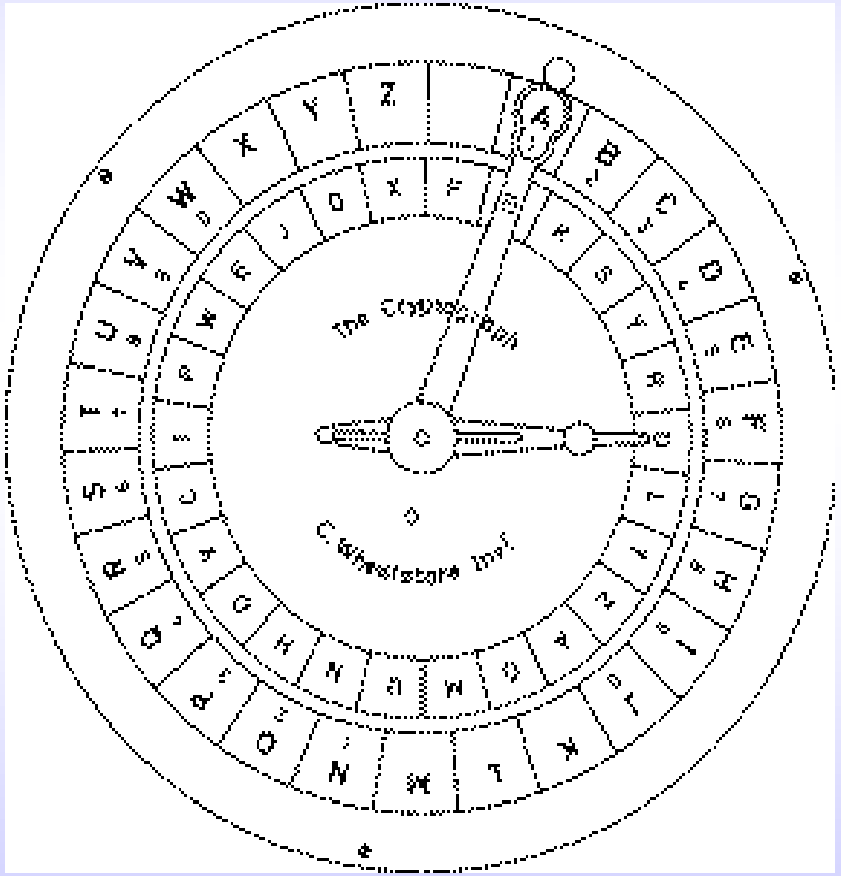
MATEMATYKA DLA CIEKAWYCH ŚWIATA

WYDZIAŁ
MATEMATYKI I NAUK
INFORMACYJNYCH

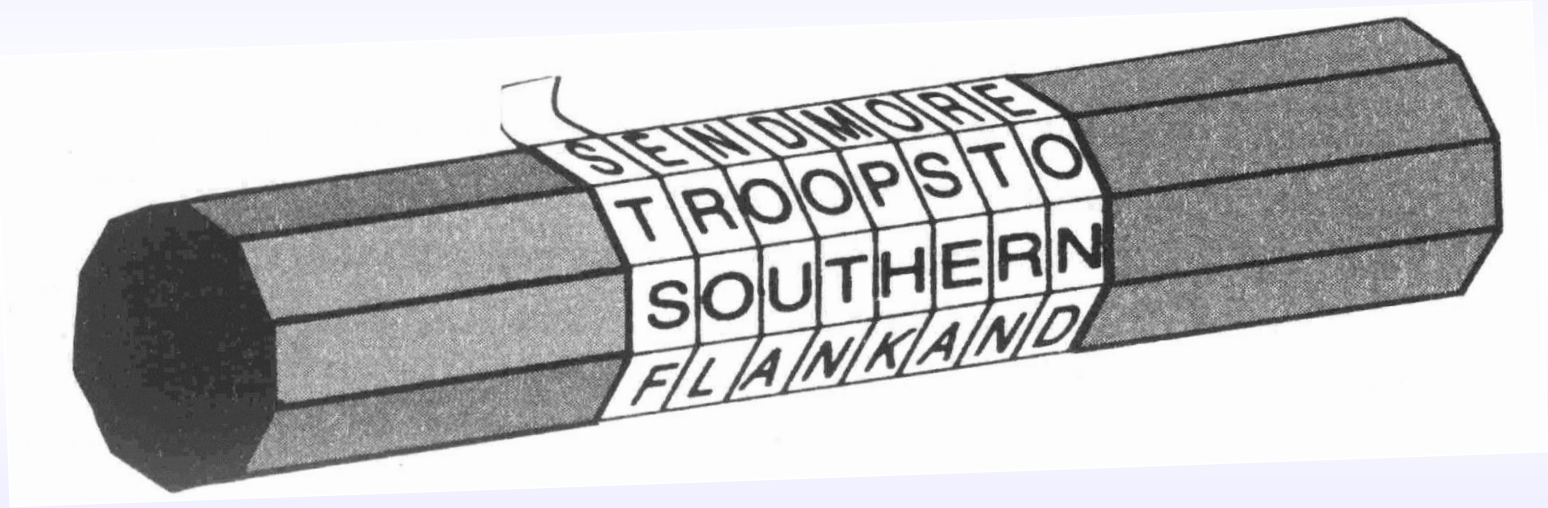

ENIGMA

Szyfry wieloalfabetowe

Ojcem szyfrów wieloalfabetowych był Leon Battista Alberti. Opisał o dysk szyfrowy, podobny do tego na obrazku, umozliwiający wiele podstawień.

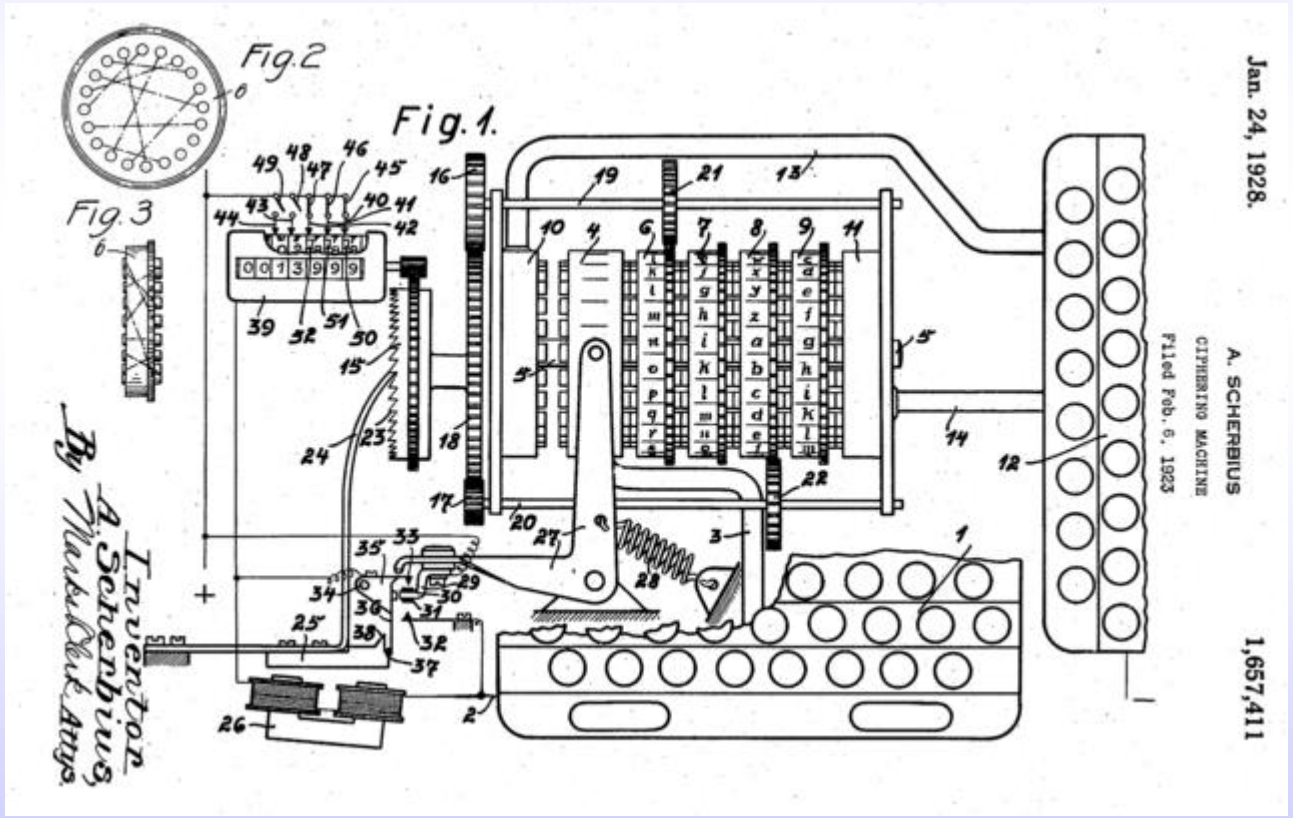


Scytale urzadzenie szyfrujące



Enigma

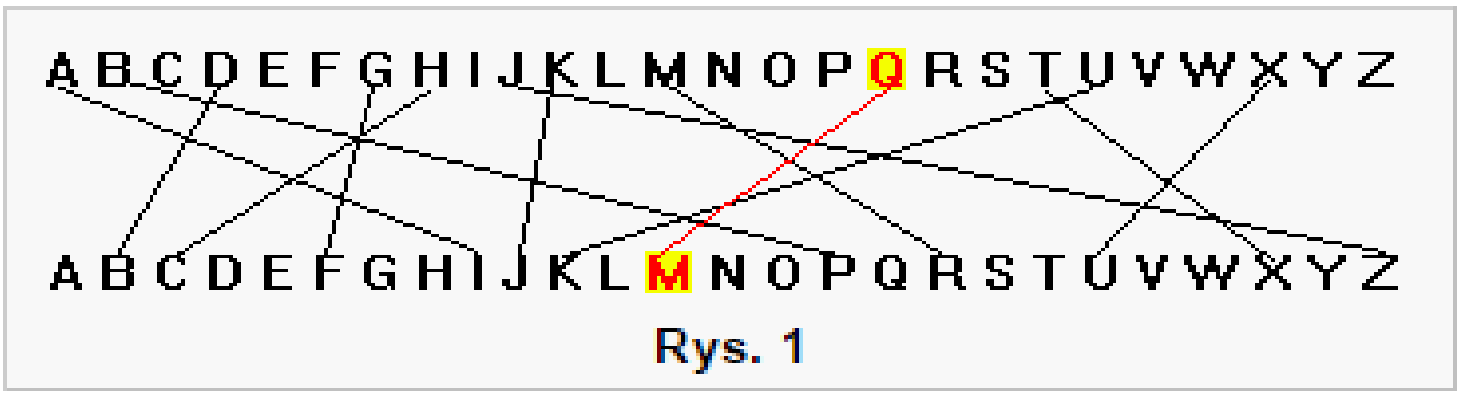
Hugo Koch projekt 1918 r maszyna szyfrująca ze zmiennym szyfrem podstawieniowym



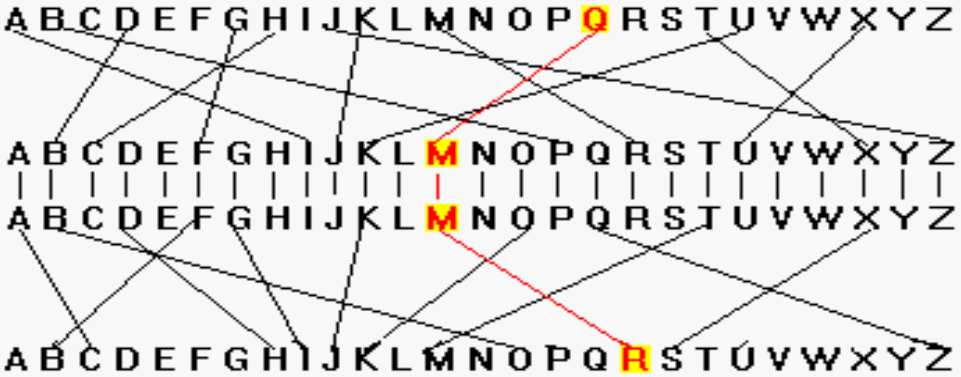
Enigma

Enigma – używana w kilku wersjach w niemieckiej armii od końca lat 20. XX w. do zakończenia II wojny światowej

Wersja opatentowana przez Artura Schreibusa w 1918 roku.

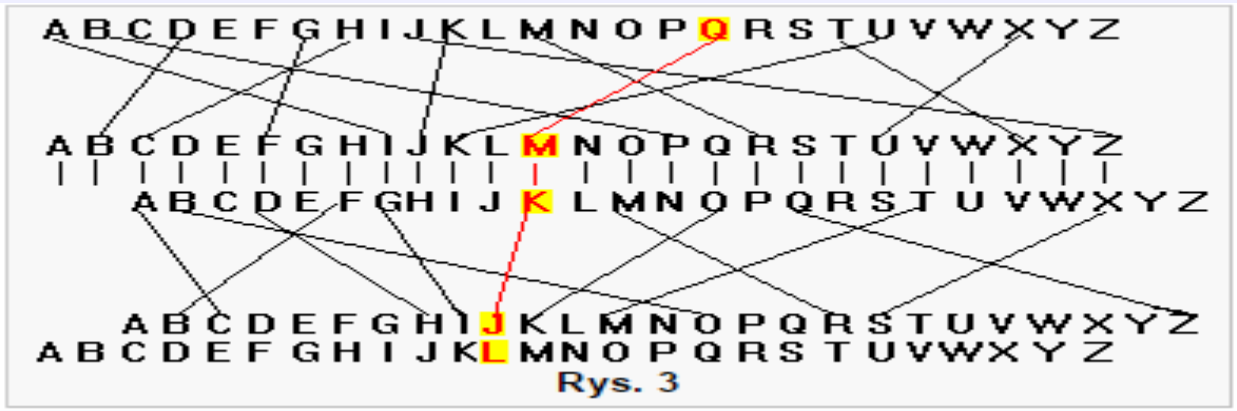

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Rys. 1



Napięcie przyłożone do końcówki M przechodzi do końcówki R w dolnym wierszu.
Zatem okablowanie dało w rezultacie zastąpienie znaku Q znakiem M,
a następnie znaku M znakiem R.

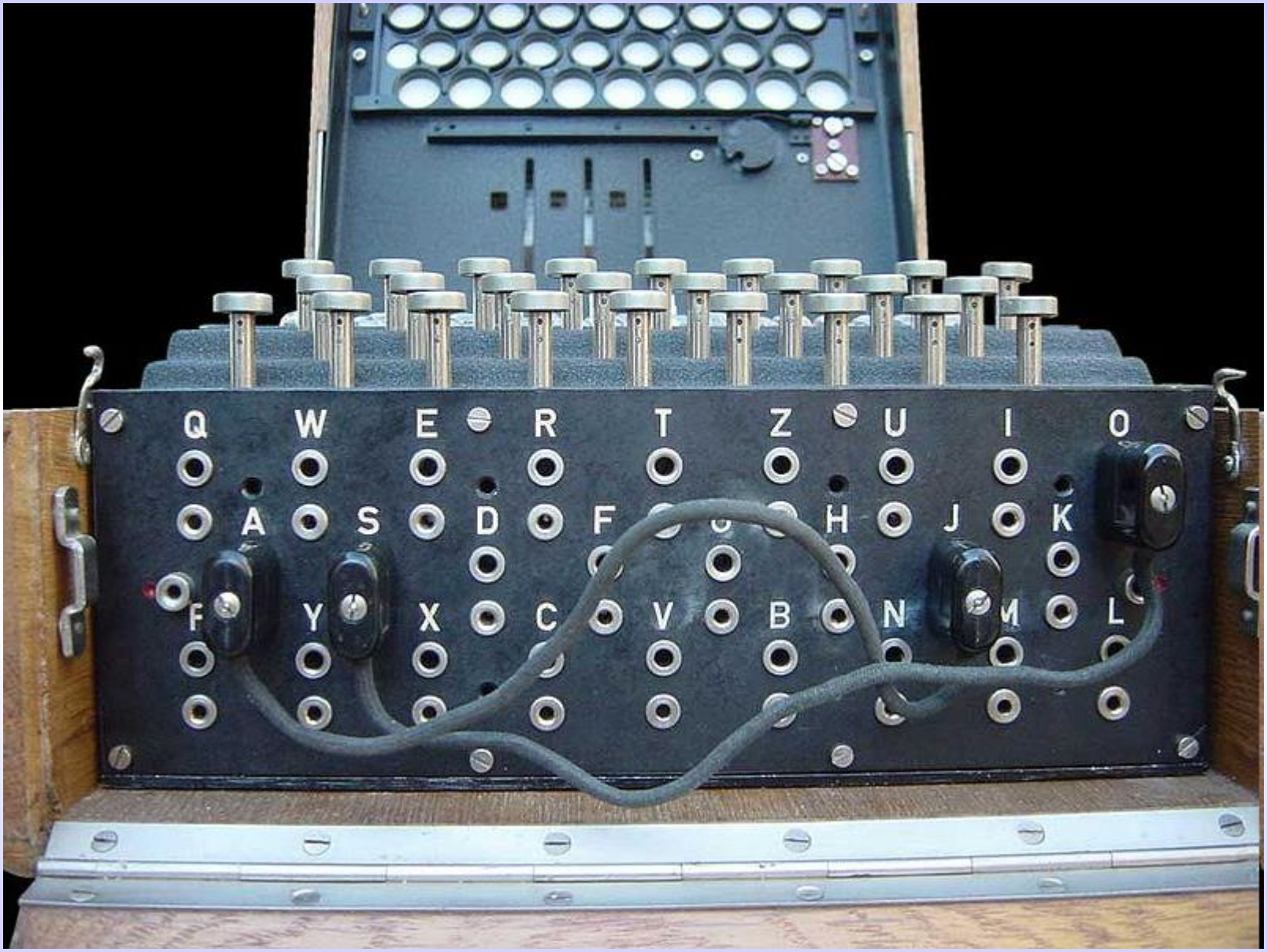
Rys. 2

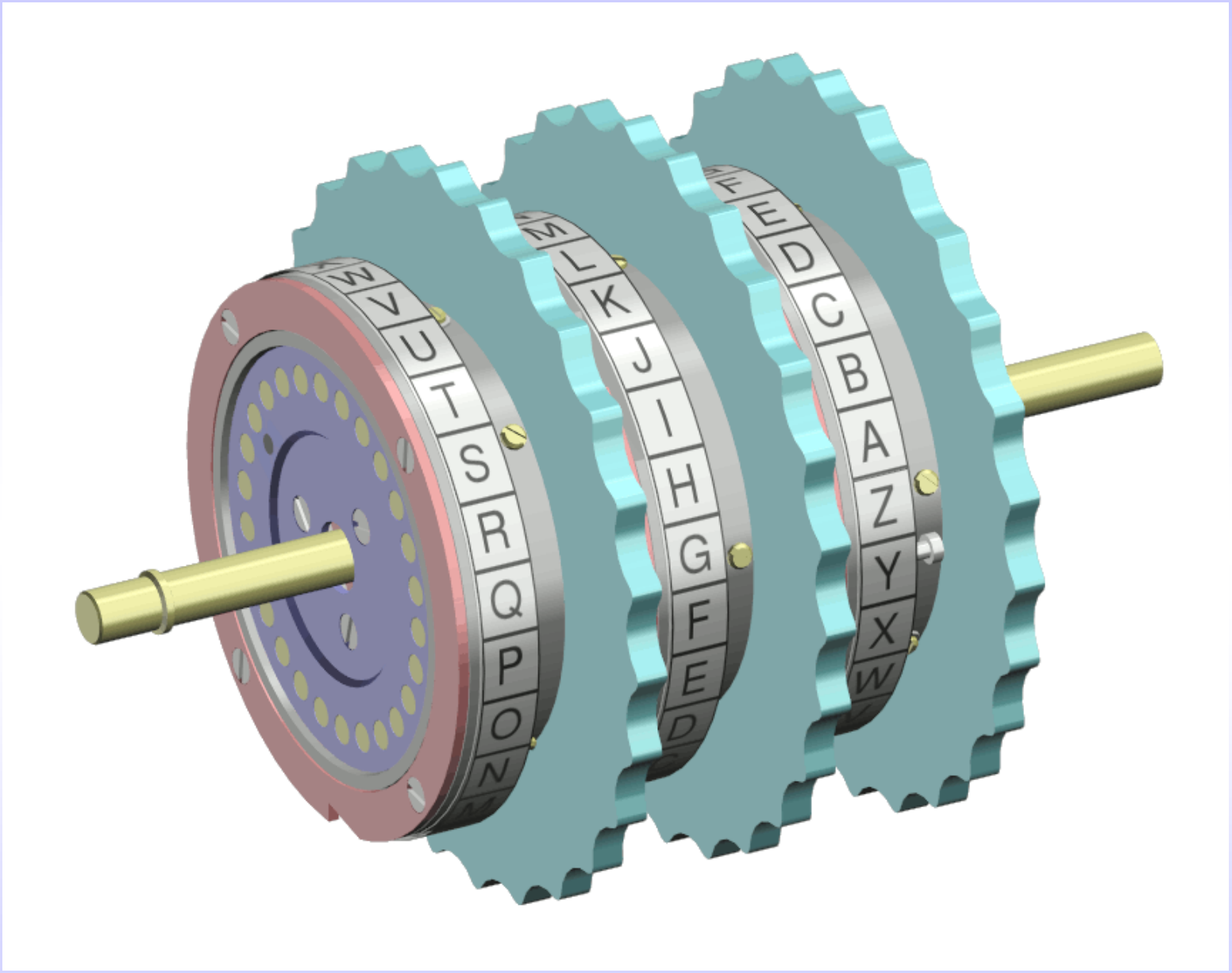

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Rys. 3

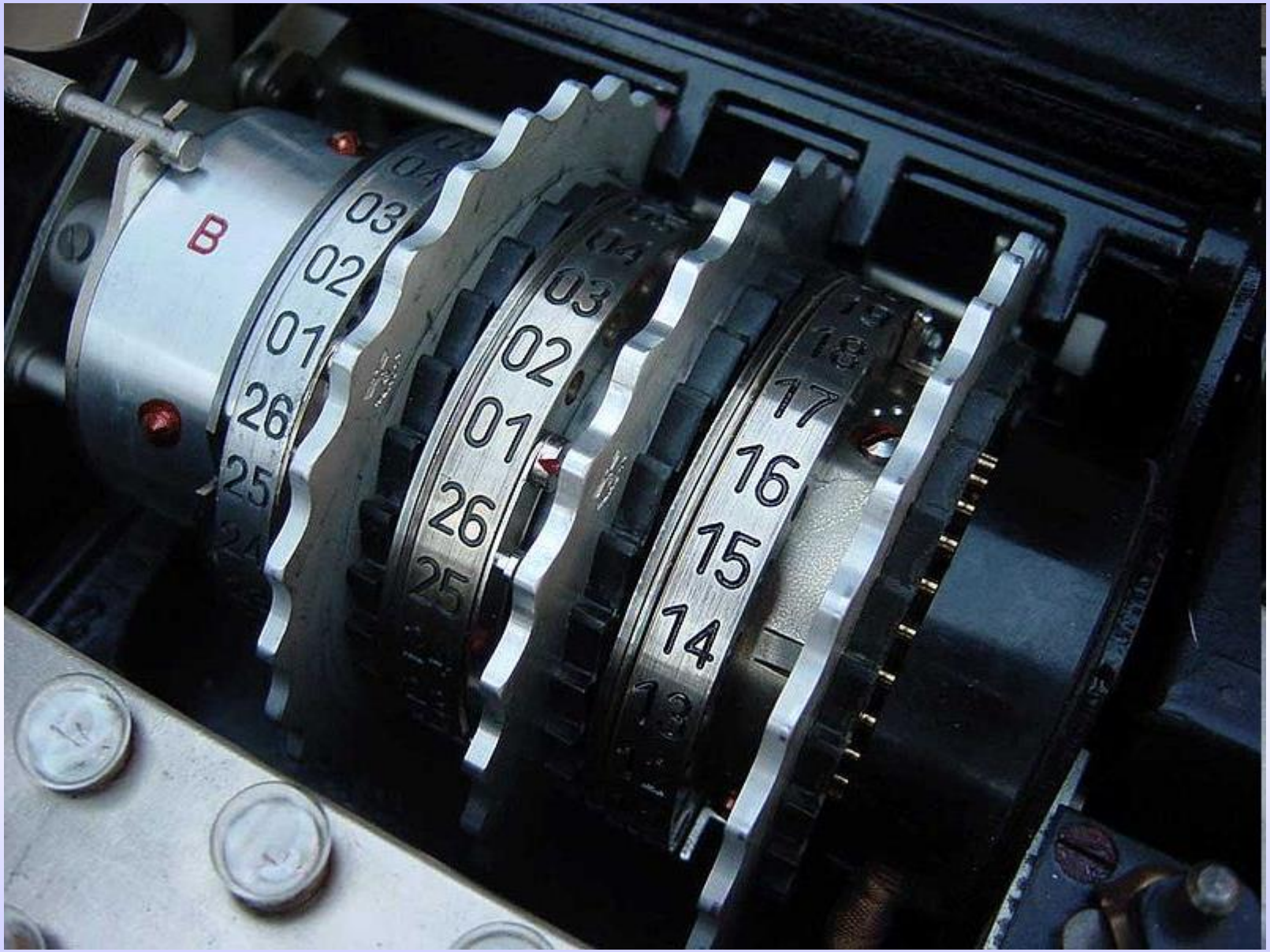
Bundesarchiv, Bild 101I-769-0229-10A / Borchert, Erich

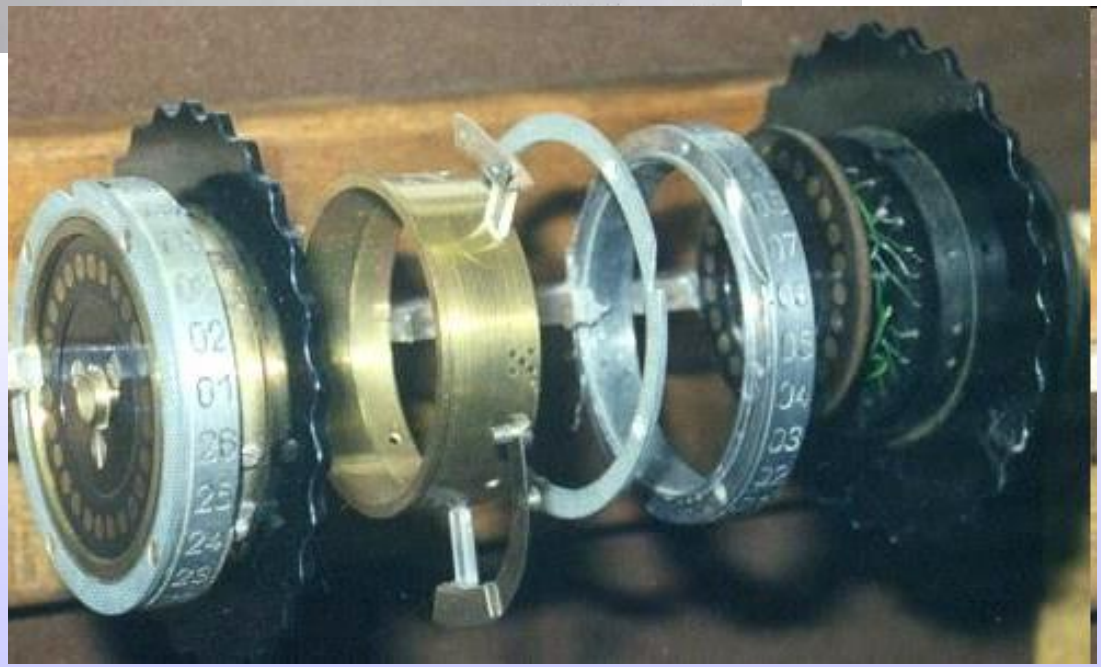
Budowa

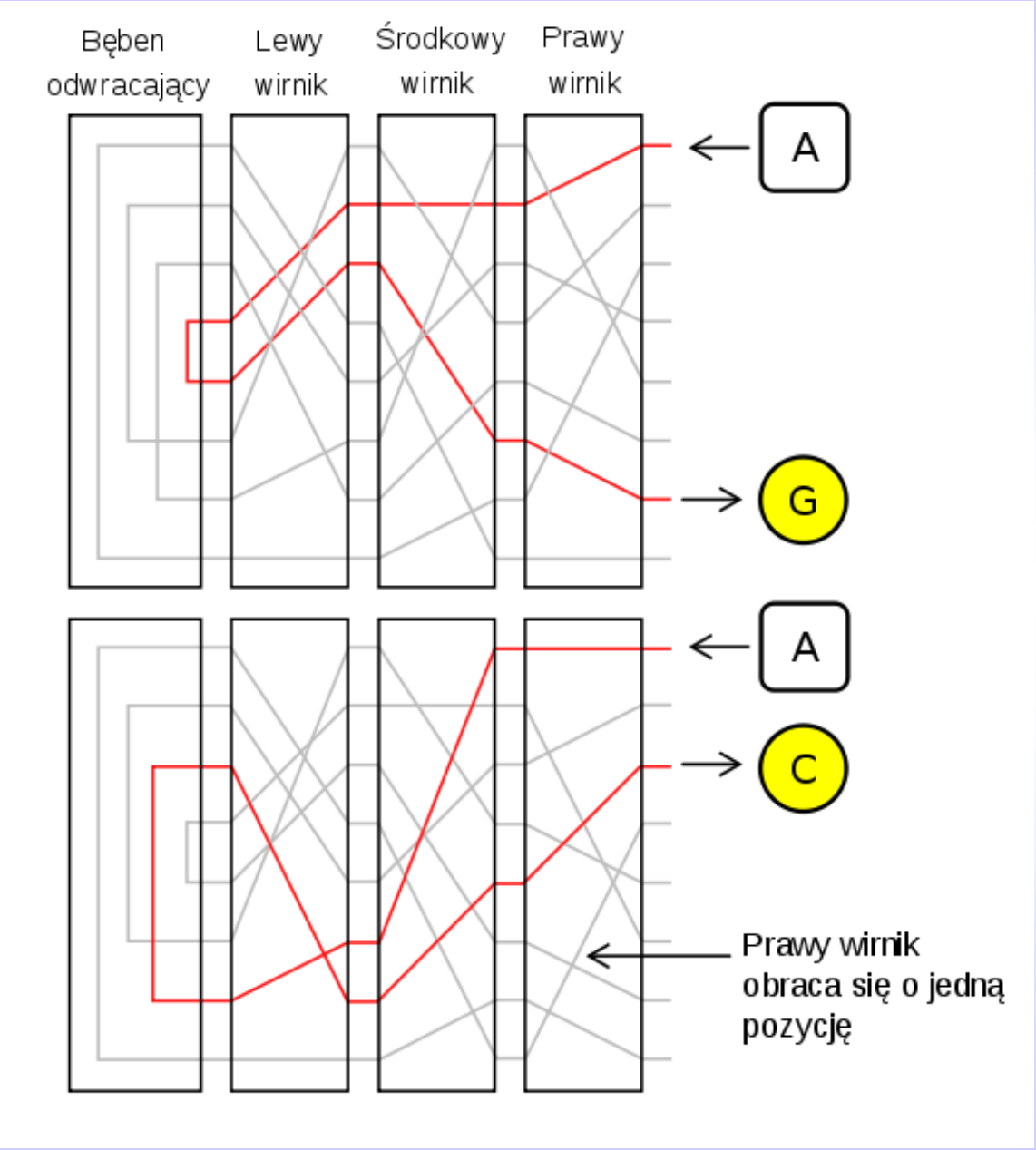
- rotory (wirniki)
- łącznica
- bęben odwracający (reflektor)


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


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

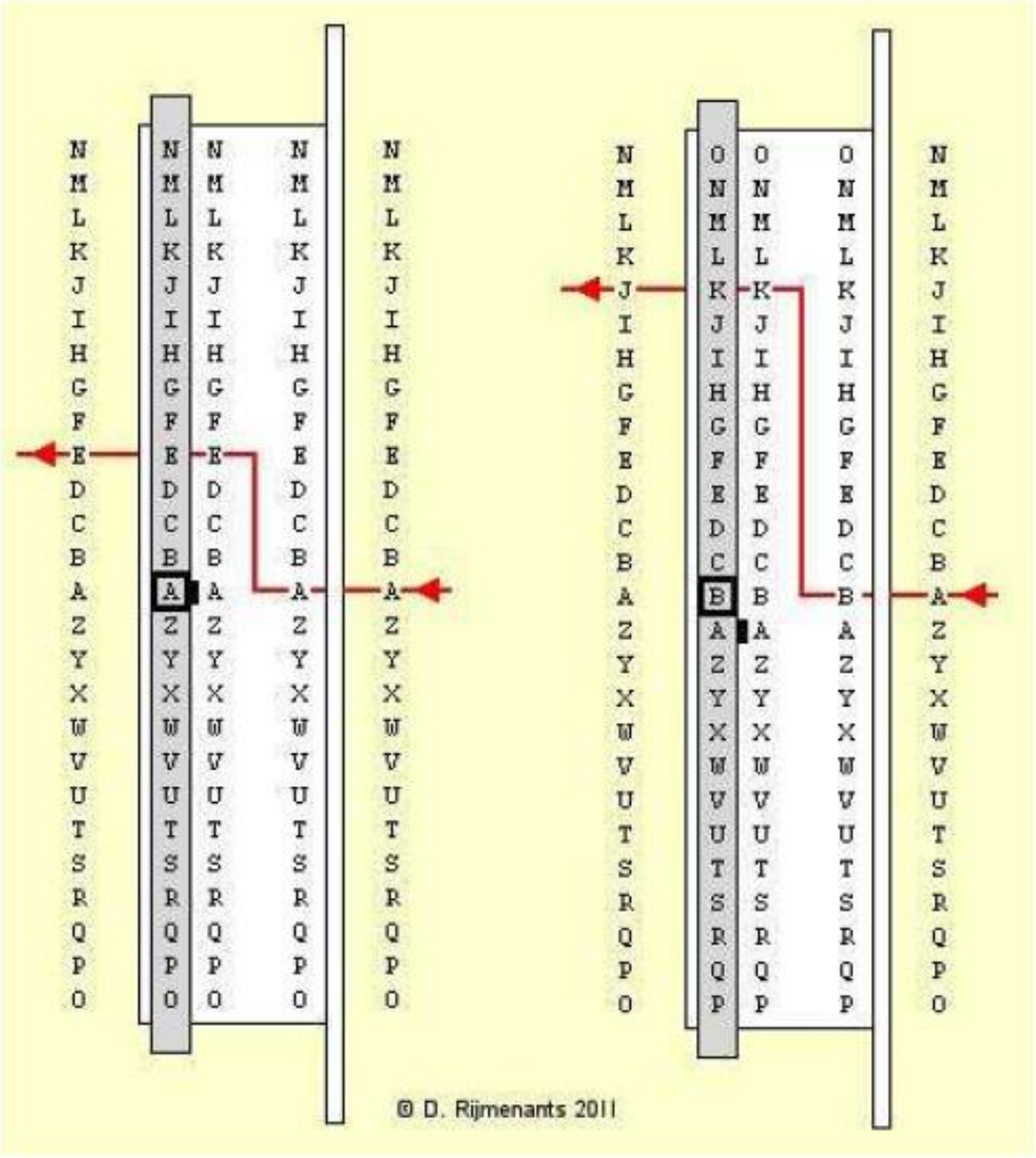

B
03
02
01
26
25
03
02
01
26
25
17
16
15
14



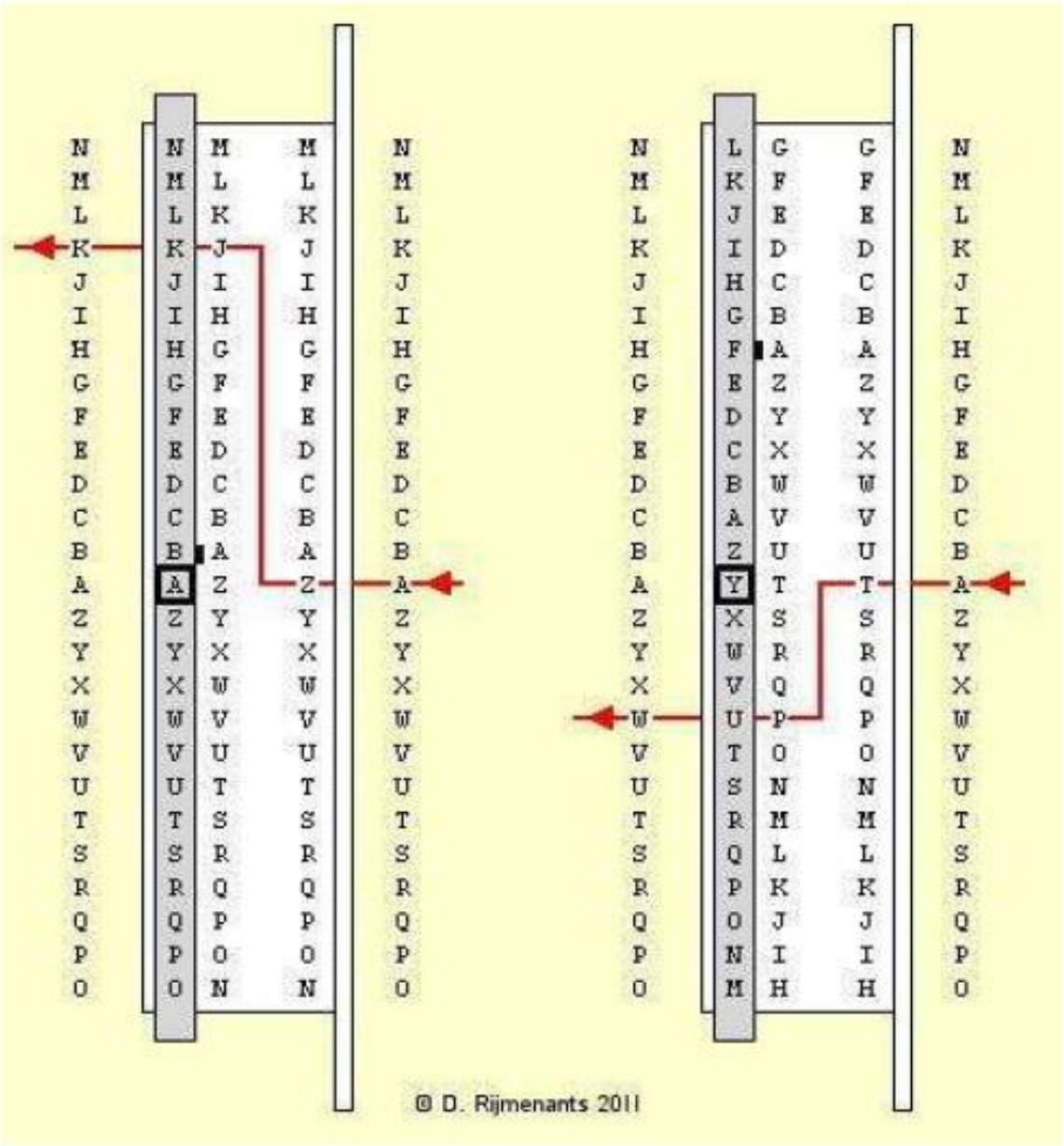

Bęben odwracający
Lewy wirnik
Środkowy wirnik
Prawy wirnik
A
G
A
C
Prawy wirnik obraca się o jedną pozycję

Rotor wiring Enigma I – M3 – M4									
I	II	III	IV	V	VI	VII	VIII	Beta	Gamma
E-A	A-A	B-A	E-A	V-A	J-A	N-A	F-A	L-A	F-A
K-B	J-B	D-B	S-B	Z-B	P-B	Z-B	K-B	E-B	S-B
M-C	D-C	F-C	O-C	B-C	G-C	J-C	Q-C	Y-C	O-C
F-D	K-D	H-D	V-D	R-D	V-D	H-D	H-D	J-D	K-D
L-E	S-E	J-E	P-E	G-E	O-E	G-E	T-E	V-E	A-E
G-F	I-F	L-F	Z-F	I-F	U-F	R-F	L-F	C-F	N-F
D-G	R-G	C-G	J-G	T-G	M-G	C-G	X-G	N-G	U-G
Q-H	U-H	P-H	A-H	Y-H	F-H	X-H	O-H	I-H	E-H
V-I	X-I	R-I	Y-I	U-I	Y-I	M-I	C-I	X-I	R-I
Z-J	B-J	T-J	Q-J	P-J	Q-J	Y-J	B-J	W-J	H-J
N-K	L-K	X-K	U-K	S-K	B-K	S-K	J-K	P-K	M-K
T-L	H-L	V-L	I-L	D-L	E-L	W-L	S-L	B-L	B-L
O-M	W-M	Z-M	R-M	N-M	N-M	B-M	P-M	Q-M	T-M
W-N	T-N	N-N	H-N	H-N	H-N	O-N	D-N	M-N	I-N
Y-O	M-O	Y-O	X-O	L-O	Z-O	U-O	Z-O	D-O	Y-O
H-P	C-P	E-P	L-P	X-P	R-P	F-P	R-P	R-P	C-P
X-Q	Q-Q	I-Q	N-Q	A-Q	D-Q	A-Q	A-Q	T-Q	W-Q
U-R	G-R	W-R	F-R	W-R	K-R	I-R	M-R	A-R	L-R
S-S	Z-S	G-S	T-S	M-S	A-S	V-S	E-S	K-S	Q-S
P-T	N-T	A-T	G-T	J-T	S-T	L-T	W-T	Z-T	P-T
A-U	P-U	K-U	K-U	Q-U	X-U	P-U	N-U	G-U	Z-U
I-V	Y-V	M-V	D-V	O-V	L-V	E-V	I-V	F-V	X-V
B-W	F-W	U-W	C-W	F-W	I-W	K-W	U-W	U-W	V-W
R-X	V-X	S-X	M-X	E-X	C-X	Q-X	Y-X	H-X	G-X
C-Y	O-Y	Q-Y	W-Y	C-Y	T-Y	D-Y	G-Y	O-Y	J-Y
J-Z	E-Z	O-Z	B-Z	K-Z	W-Z	T-Z	V-Z	S-Z	D-Z

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



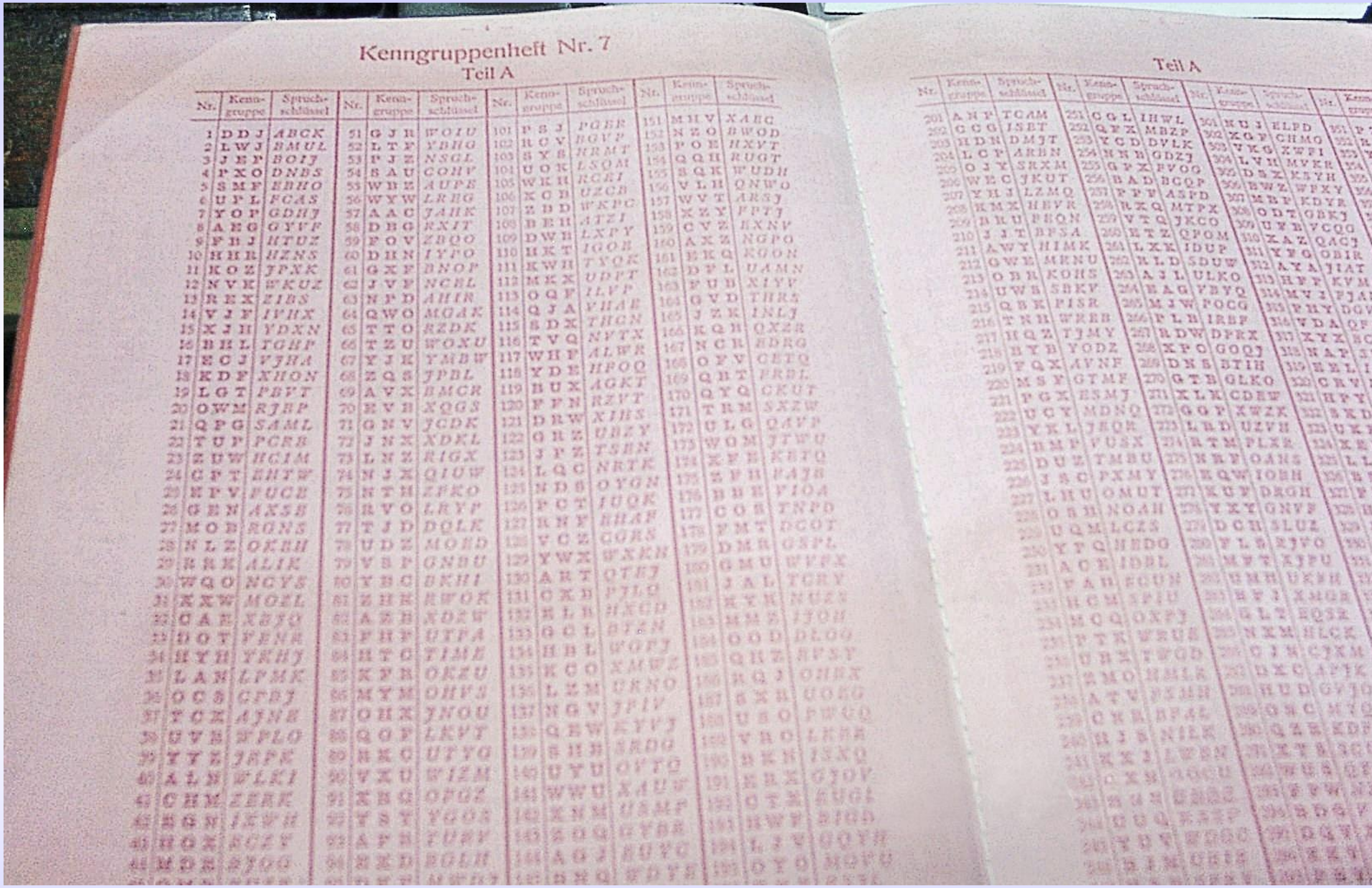
Example 1 - Rotor I with ring setting A



Example 2 - Rotor I with ring setting B and ring setting F

Zawartość klucza

- Kolejność wirników
- Początkowa pozycja wirników
- Ustawienie łącznicy kablowej
- Ustawienia wirników


Kenngruppenheft Nr. 7
Teil A
Teil A

Geheim! 0

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppe
31.	I V III	06 20 24	UA PF RQ SO NI EY BG HL TX ZJ	jeu nyq aqm
30.	V II III	01 07 12	GF KV JM ?B UW LX TD QS NA ZH	azs zds kck
29.	IV I V	11 17 26	CI OK PV ZL HX NB AW DJ FE ST	kap gwh lyx

Geheim! = Tajne! Oto fragment używanego przez Niemców arkusza ustawień

Szyfrowanie

Z klucza dziennego: wirniki II,III,I; reflektor B, pozycja początkowa BEC

A D K A D K → O W F W E C

Zmiana pozycji początkowej na ADK

E N I G M A → V E A B S X

Szyfrogram: OWFWECVEABSX

Złożoność Enigmy

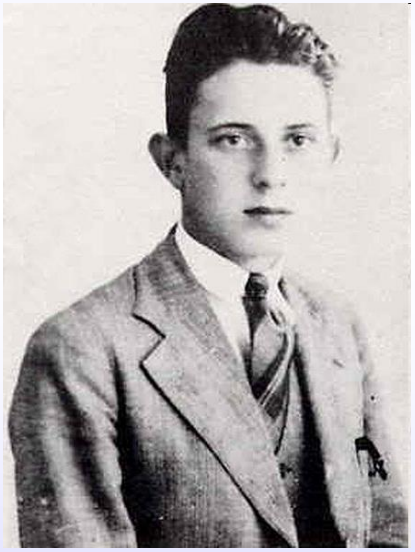
- Obrót wirników $26^3 = 17576$
- Wybór 3 z pięciu wirników i ich kolejności $\frac{5!}{2!} = 60$
- Łącznica $\frac{26!}{6!2^{10}10!}$
- Razem ???

1	AUQ	AMN	23	NXD	QTU	45	TMN	EBY
2	BNH	CHL	24	NXD	QTU	46	TMN	EBY
3	BCT	CGJ	25	NLU	QFZ	47	TAA	EXB
4	CIK	BZT	26	OBU	DLZ	48	USE	NWH
5	DDB	VDV	27	PVJ	FEG	49	VII	PZK
6	EJP	IPS	28	QGA	LYB	50	VII	PZK
7	FBR	KLE	29	QGA	LYB	51	VQZ	PVR
8	GPB	ZSV	30	RJL	WPX	52	VQZ	PVR
9	HNO	THD	31	RJL	WPX	53	WTM	RAO
10	HNO	THD	32	RJL	WPX	54	WTM	RAO
11	HXV	TTI	33	RJL	WPX	55	WTM	RAO
12	IKG	JKF	34	RFC	WQQ	56	WKI	RKK
13	IKG	JKF	35	SYX	SCW	57	XRS	GNM
14	IND	JHU	36	SYX	SCW	58	XRS	GNM
15	JWF	MIC	37	SYX	SCW	59	XOI	GUK
16	JWF	MIC	38	SYX	SCW	60	XYW	GCP
17	KHB	XJV	39	SYX	SCW	61	YPC	OSQ
18	KHB	XJV	40	SJM	SPO	62	YPC	OSQ
19	LDR	HDE	41	SJM	SPO	63	ZZY	YRA
20	LDR	HDE	42	SJM	SPO	64	ZEF	YOC
21	MAW	UXP	43	SUG	SMF	65	ZSJ	YWG
22	MAW	UXP	44	SUG	SMF			

Rysunek 3.5: Tablica identyfikatorów ENIGMY.

Łamanie szyfru

- Polacy – Marian Rejewski, Jerzy Różycki, Henryk Zygalski – 1932, Biuro Szyfrów



- słynne Bletchley Park

Ocalałe egzemplarze w Polsce

- Muzeum Techniki
- Muzeum Wojska Polskiego
- Muzeum Wojska w Białymstoku
- Muzeum Oręża Polskiego w Kołobrzegu

Dziękuję za uwagę