

# Enigmatyczna historia Enigmy

Barbara Roszkowska Lech

MATEMATYKA DLA CIEKAWYCH ŚWIATA

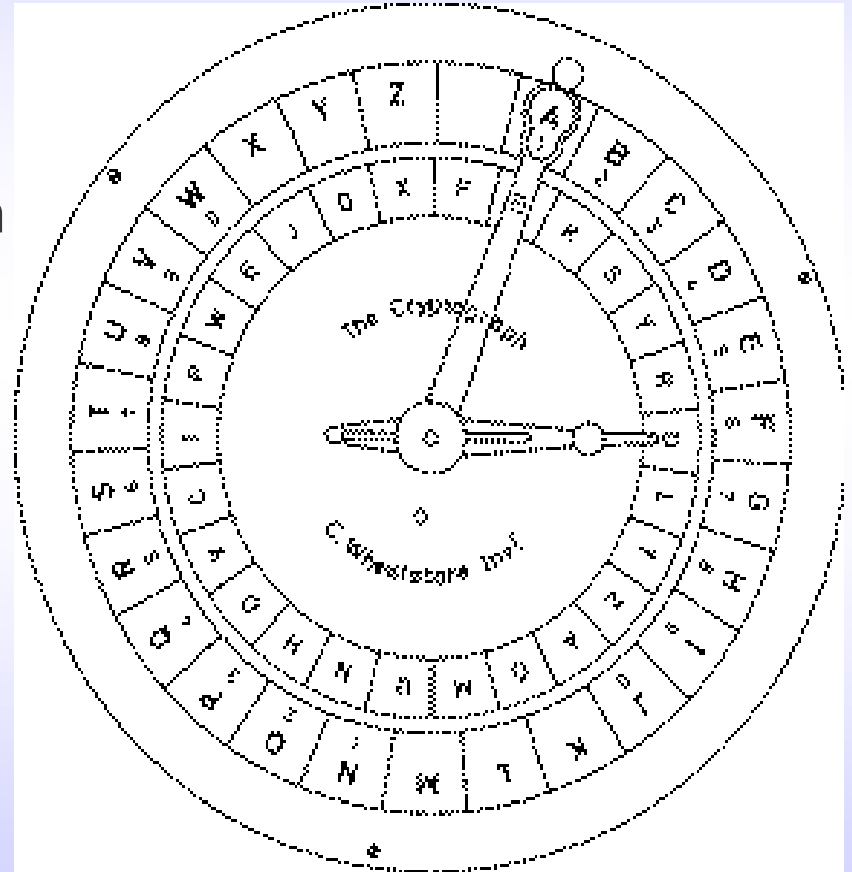


**WYDZIAŁ  
MATEMATYKI I NAUK  
INFORMACYJNYCH**

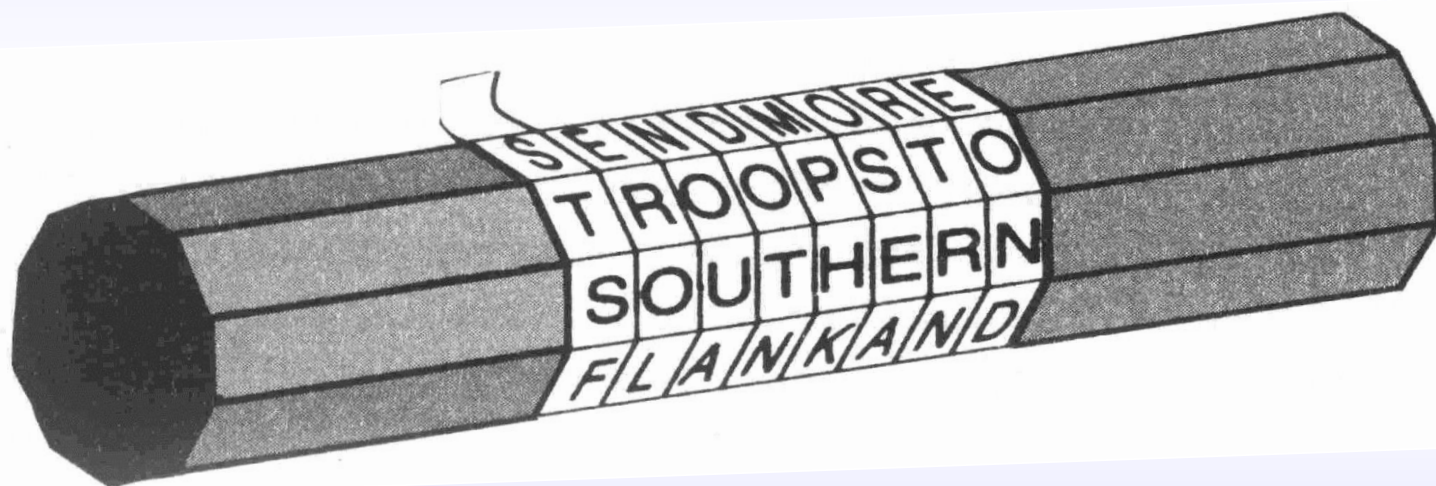


# Szyfry wieloalfabetowe

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

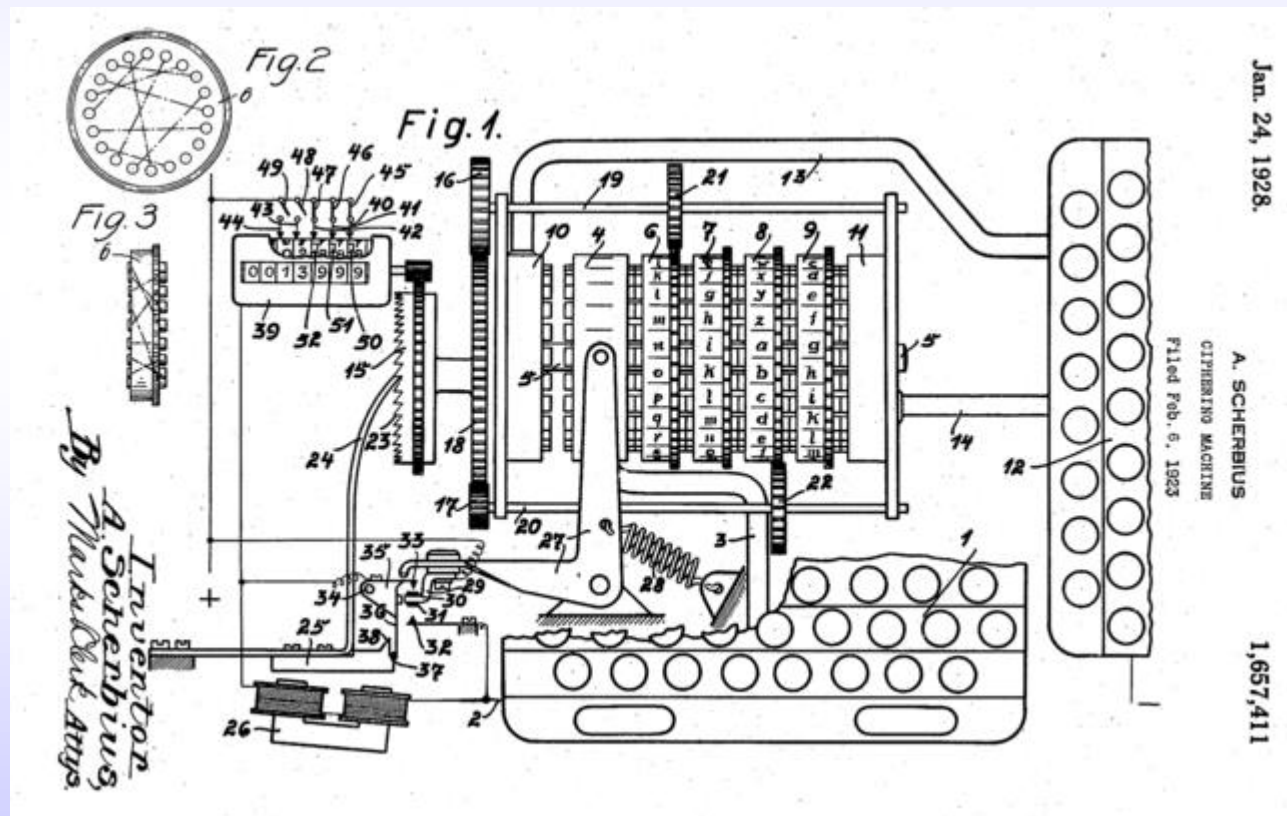


# Scytale urządzenie szyfrujące



# Enigma

Hugo Koch projekt 1918 r maszyna szyfrująca ze zmiennym szyfrem podstawieniowym



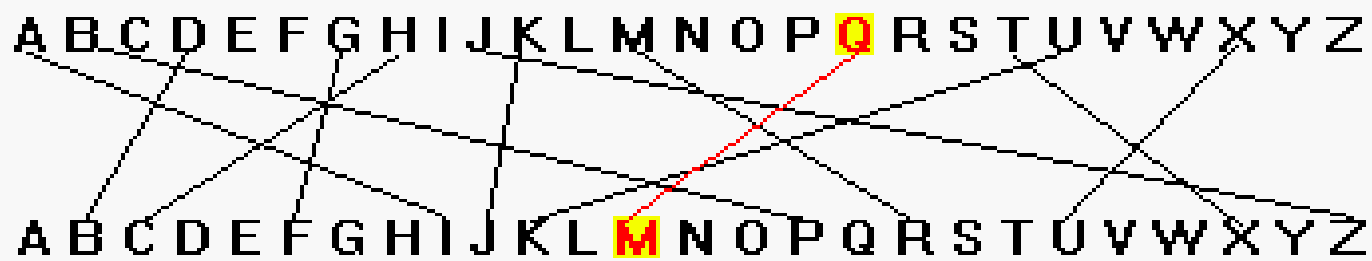
# Enigma

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

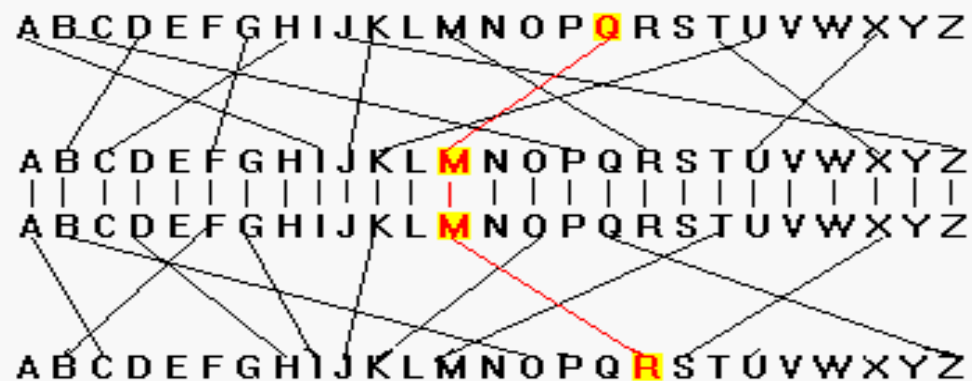
Wersja opatentowana przez Artura Schreibusa w 1918 roku.



(c) 1935, Morton Srimmer



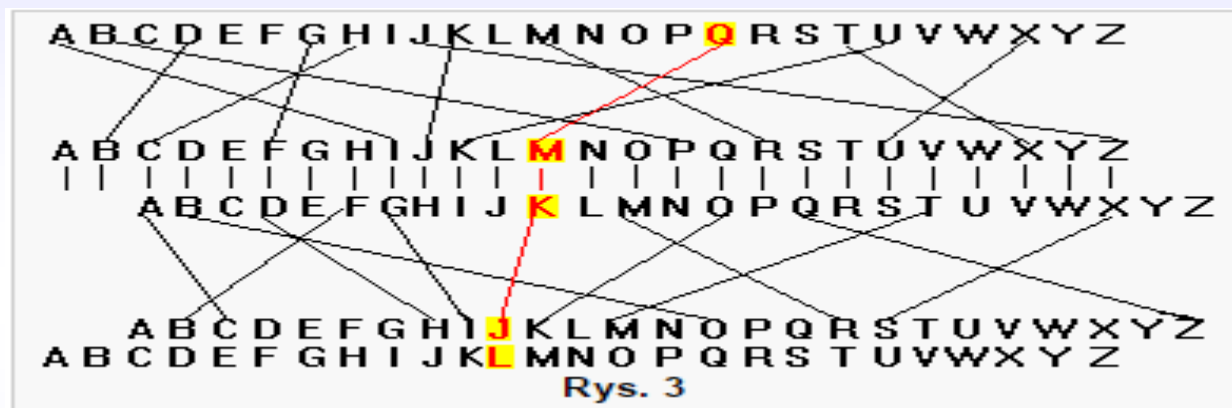
Rys. 1

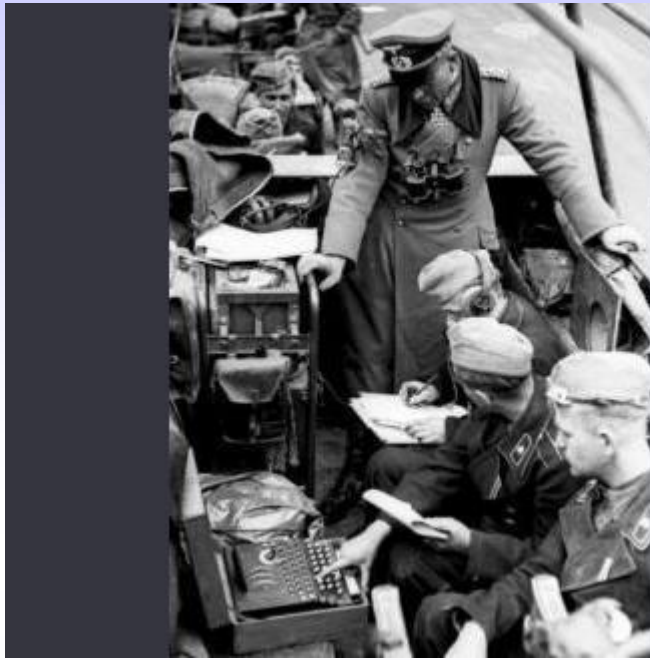


Napięcie przyłożone do końcówki M przechodzi do końcówki R w dolnym wierszu.  
Zatem okablowanie dało w rezultacie zastąpienie znaku Q znakiem M,  
a następnie znaku M znakiem R.

Rys. 2







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

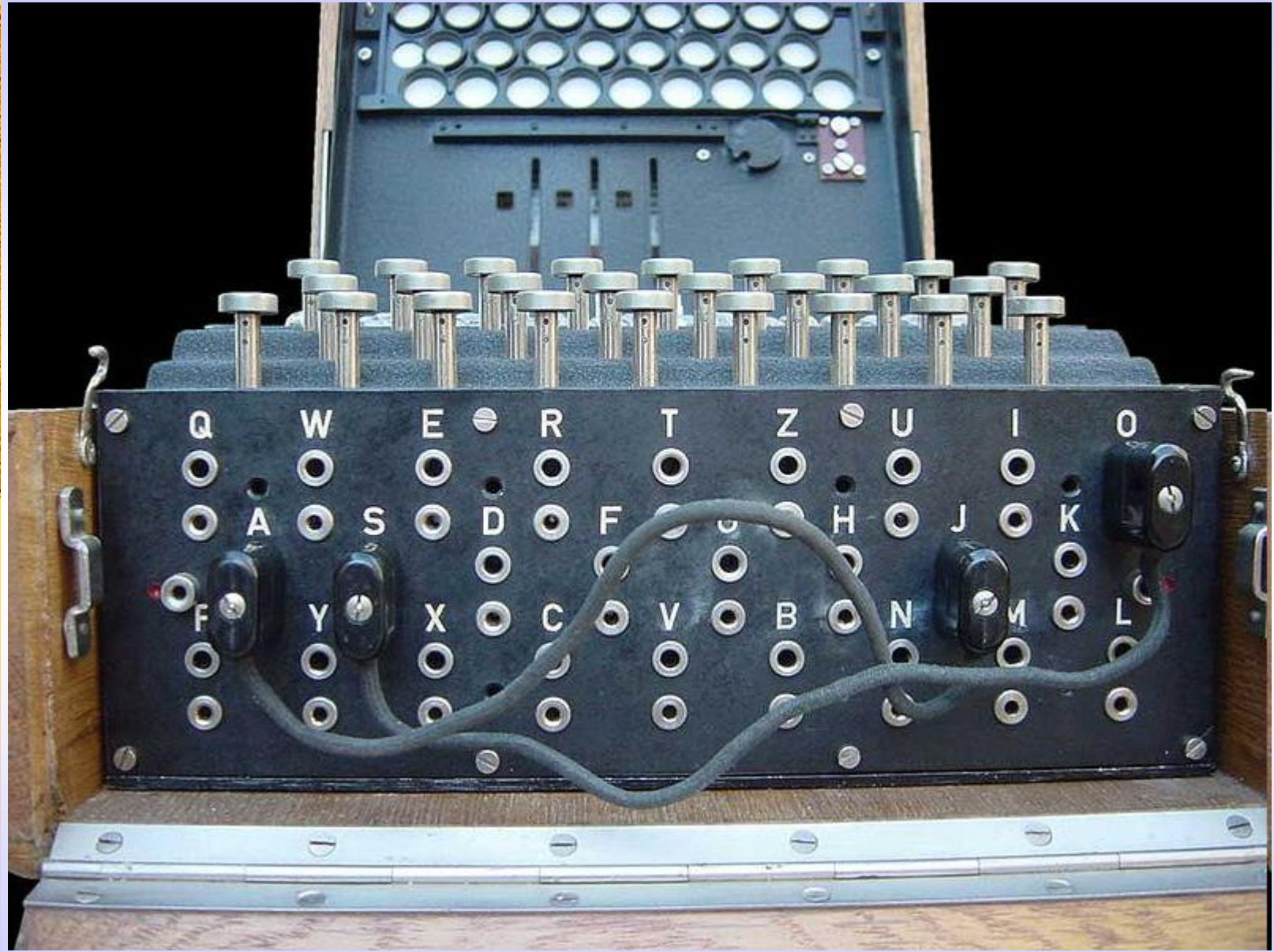


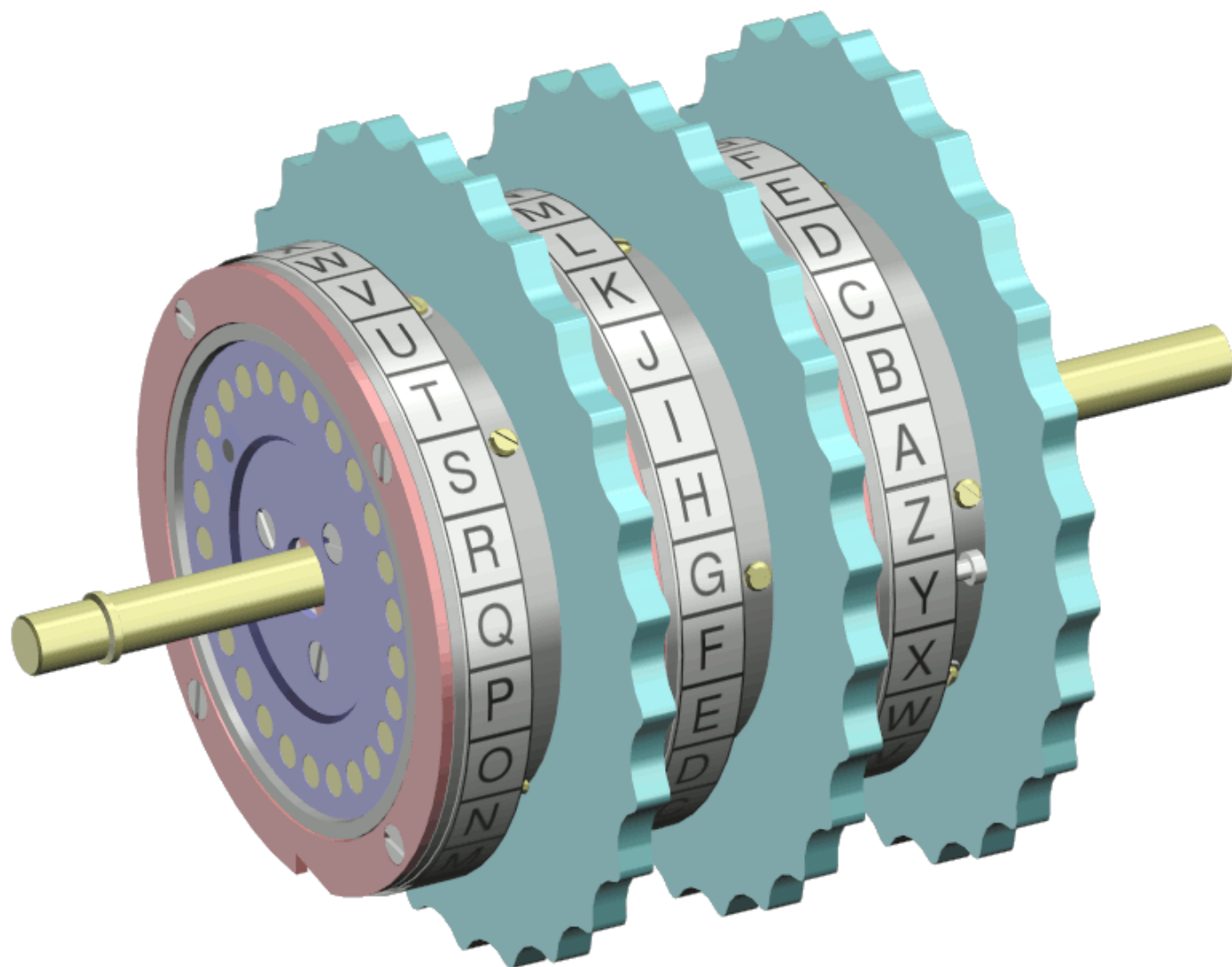


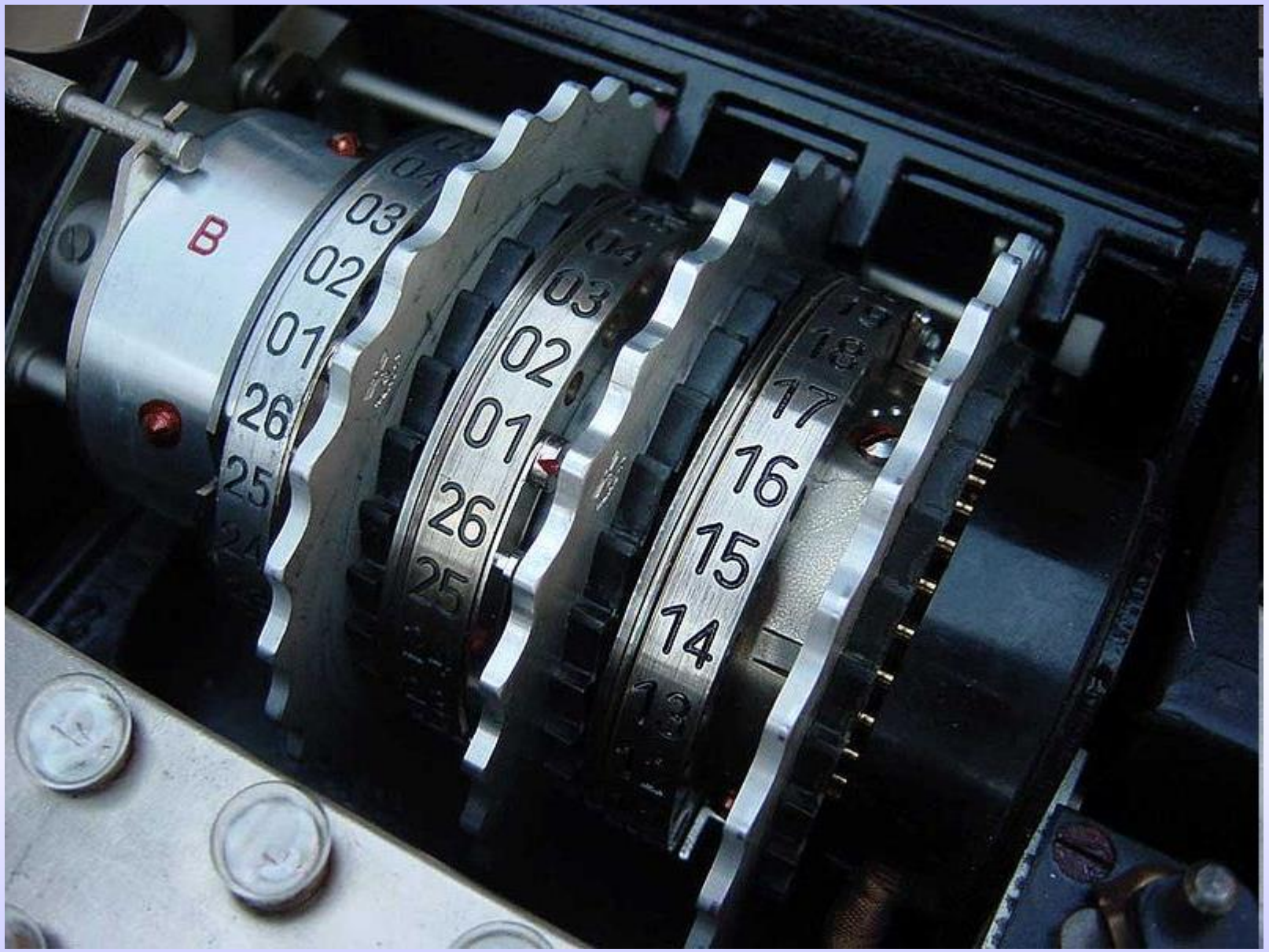
# Budowa

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

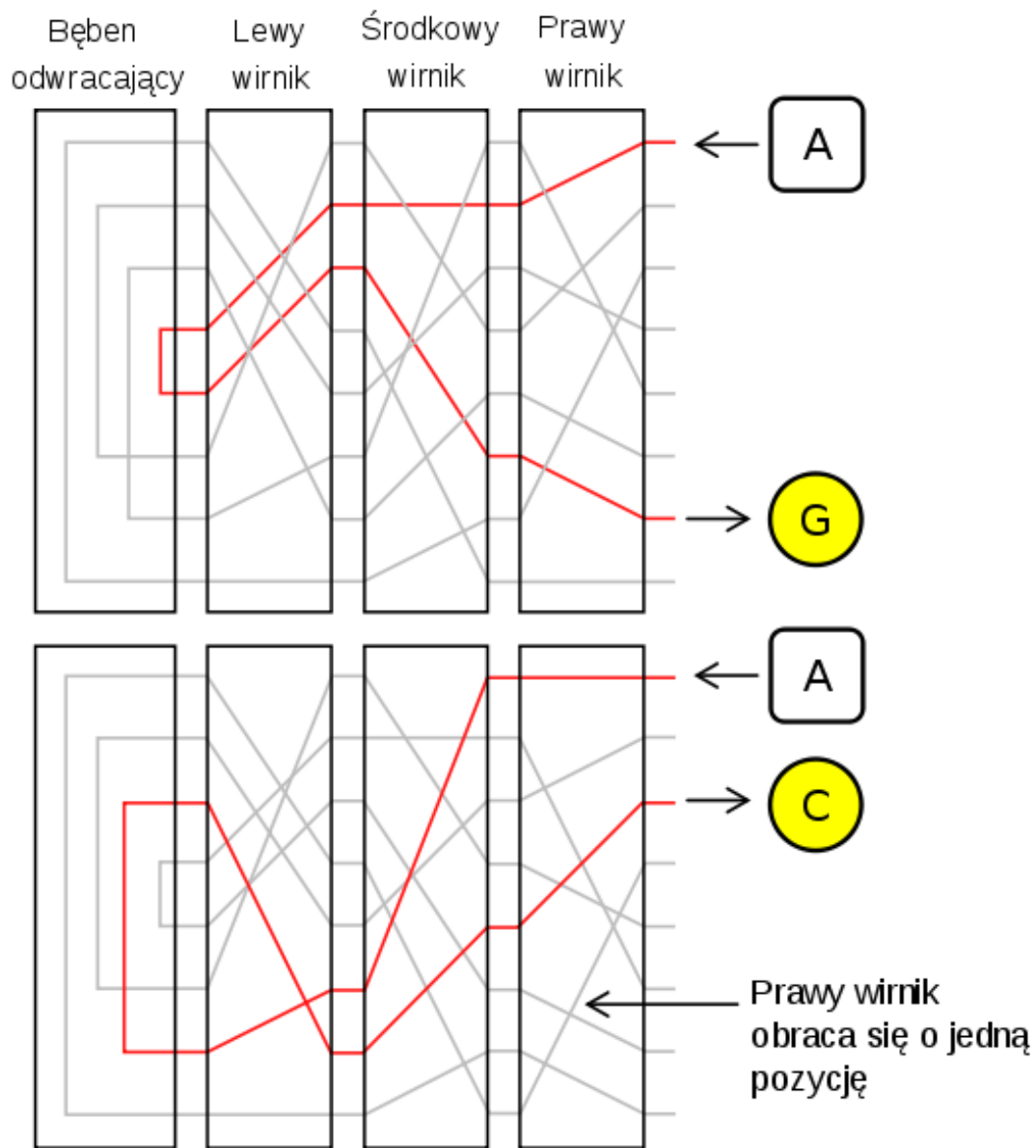














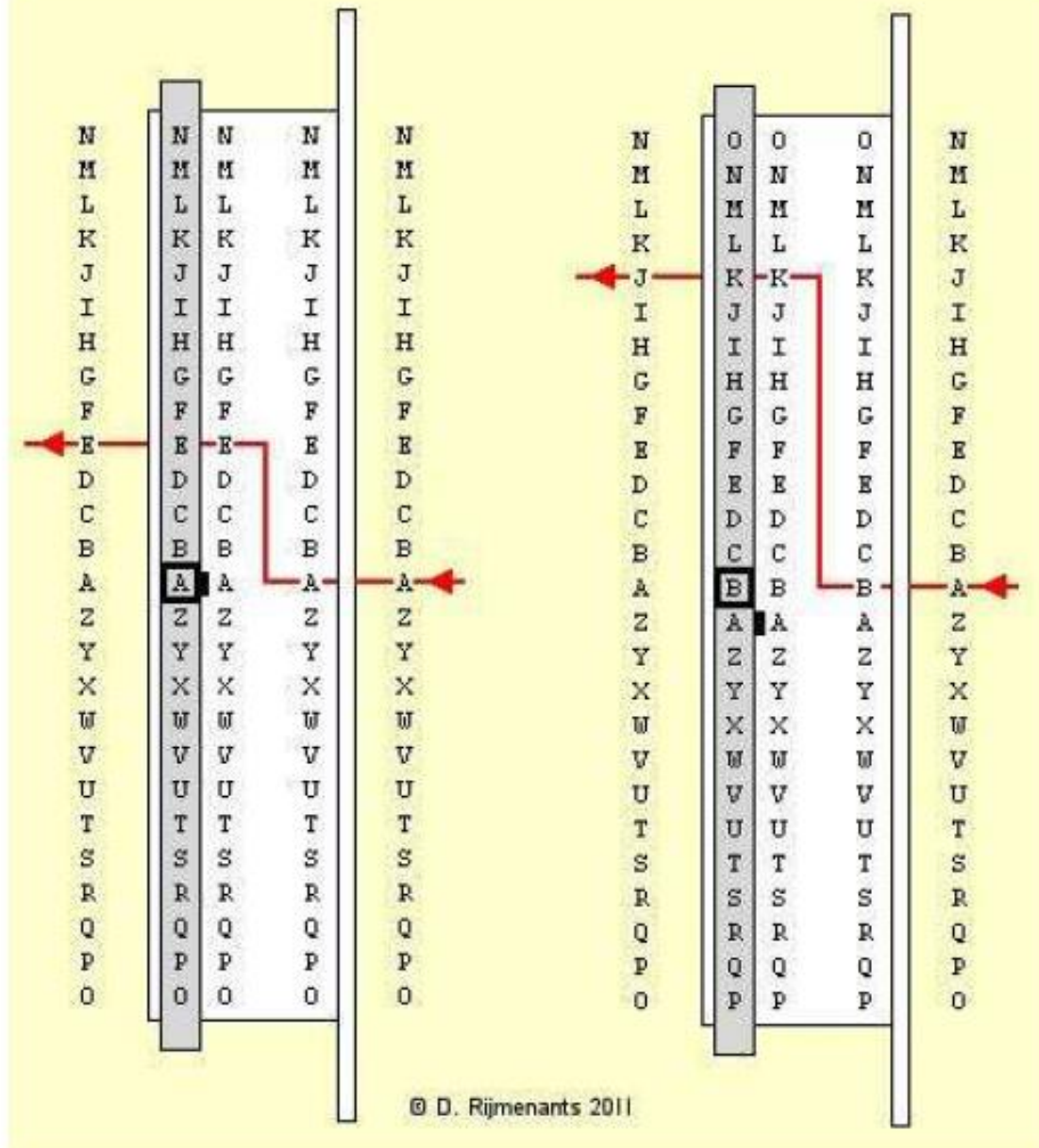


### Rotor wiring Enigma I – M3 – M4

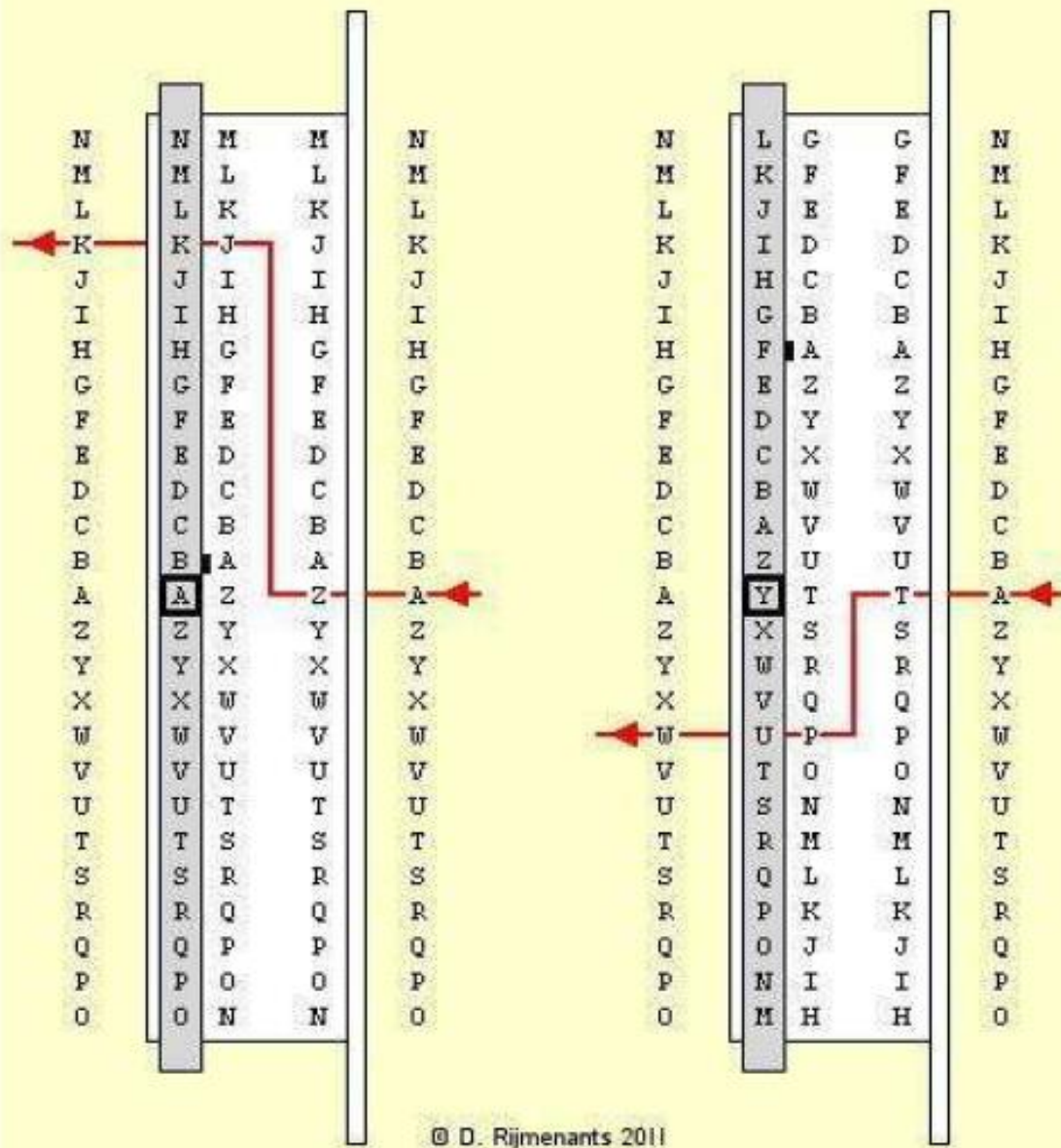
I	II	III	IV	V	VI	VII	VIII	Beta	Gamma
E-A	A-A	B-A	E-A	V-A	J-A	N-A	F-A	L-A	F-A
K-B	J-B	D-B	S-B	Z-B	P-B	Z-B	K-B	E-B	S-B
M-C	D-C	F-C	O-C	B-C	G-C	J-C	Q-C	Y-C	O-C
F-D	K-D	H-D	V-D	R-D	V-D	H-D	H-D	J-D	K-D
L-E	S-E	J-E	P-E	G-E	O-E	G-E	T-E	V-E	A-E
G-F	I-F	L-F	Z-F	I-F	U-F	R-F	L-F	C-F	N-F
D-G	R-G	C-G	J-G	T-G	M-G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

Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel
1	DDJ	ABCK	51	GJR	WOIU	101	PBJ	POER	151	MHV	XARG
2	LWJ	BMUL	52	LTY	YBHO	102	RCV	RGVP	152	NZO	HWOD
3	JEN	BOIT	53	PJE	NSGL	103	SYB	HRMT	153	POB	HXYT
4	PKO	DNBS	54	SAU	COMP	104	UOK	LSOM	154	QQH	RUGT
5	SMP	EBHO	55	WBE	AUPE	105	WKH	RCEI	155	BQK	WUDH
6	UPL	FGAS	56	WYW	LRBG	106	KOB	UZGP	156	VLH	QWFO
7	YOP	GDHT	57	AAE	JAHK	107	ZBD	WKPG	157	WVT	ARSJ
8	AEG	GYVF	58	DBG	RXIT	108	BEH	ATYI	158	KZY	FPTJ
9	FBJ	HTUZ	59	FOV	ZBQO	109	DWH	LXPY	159	CVZ	RXNV
10	KHR	HZNS	60	DHN	IYPO	110	HKT	IGOE	160	AXZ	NGPO
11	KOZ	JFKK	61	GXF	BNOP	111	KWH	TYOK	161	ERQ	KOON
12	NYK	EKUZ	62	JVF	NCEL	112	MKK	UDPT	162	DPL	UAMN
13	REX	EIBS	63	NFD	AHIR	113	QQF	ILVF	163	PUB	XIYP
14	VJF	IYHX	64	QWO	MOAK	114	QJA	PHAE	164	QVD	TBRJ
15	KJH	YDXN	65	TTO	RZDK	115	SDX	THGN	165	JEK	INLJ
16	BHL	TGHP	66	TZO	WOKU	116	TVQ	NPTX	166	KGB	QXER
17	EOJ	VJHA	67	YJK	YMBW	117	WHE	ALWR	167	NGR	EDRG
18	KDE	XHON	68	ZQS	JPLB	118	YDE	HPOO	168	OFV	GETQ
19	LGT	PBYT	69	AVX	BMCN	119	BUX	AGKT	169	QBT	FRBL
20	OWM	RJHP	70	EYH	XQGS	120	FFN	REVT	170	QYQ	CKUT
21	QPG	SAML	71	GNV	JCDK	121	DRW	XIHS	171	TRM	SXZW
22	TUP	PCRR	72	JNX	XDKL	122	GRZ	UBZY	172	OLG	QAVP
23	UDW	HGIM	73	LNZ	RIGX	123	JFZ	TSEN	173	WOM	JTWU
24	GPT	ENTW	74	NJX	QIOW	124	LQC	NRTK	174	XFE	KSTQ
25	KPY	FUCB	75	NTH	ZPKO	125	NDS	OYGN	175	ZFH	RAJR
26	GEN	AKSB	76	RVO	LRYF	126	PCT	IUGK	176	BBE	PJQA
27	MOB	RQNS	77	TJD	DQLE	127	RNF	RHAF	177	COB	TNPD
28	NLZ	OKBH	78	UDE	MOED	128	VCE	GORS	178	FMT	DCOT
29	RRK	ALIK	79	VBP	GNBU	129	YWX	SXKN	179	DMR	OSPL
30	WQO	NGYS	80	YBC	BKHI	130	AKT	OTEF	180	GMO	WFFX
31	KXW	MOEL	81	ZHR	RFOK	131	CKB	PJLB	181	JAL	TGRY
32	CAE	XBJO	82	AEB	KDEW	132	ELB	HXGN	182	HTK	NUZJ
33	DOT	FENR	83	FHE	UTFA	133	GCL	BZSD	183	HME	IJOH
34	HYH	YKHY	84	HTC	TIME	134	HBL	WOFY	184	OOD	DLOG
35	LAN	LPMK	85	KFR	OKZU	135	KCO	XWFO	185	QHZ	RFZY
36	OCS	CFBT	86	KYM	OHFY	136	LZM	GNZO	186	RQJ	ONBX
37	TCZ	AJNE	87	OHX	JNOU	137	NGV	JPIV	187	SXN	GOFG
38	UVH	WPLQ	88	QOF	LKVT	138	QBW	KYPT	188	USO	FWGO
39	TYE	JRPE	89	RKC	UTYO	139	BHN	SADG	189	VRO	LKRN
40	ALN	WLEI	90	VXU	WIZM	140	DYU	OPTO	190	BKN	ISXQ
41	CHM	ZBRK	91	XBG	OPGX	141	WWU	KADU	191	BKK	GJOV
42	BSN	IKWH	92	YST	YGOR	142	XNM	USMP	192	OTE	SUGL
43	HOX	RCZY	93	AFH	TUMY	143	ZOG	KYBE	193	HWP	SJOD
44	MDE	RYOO	94	NEE	BOLH	144	AGZ	BYVC	194	LJV	GOYH
45	...	...	95	...	...	145	...	...	195	OYO	NOFU

Teil A

Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel
201	ANP	TCAM	251	GGL	IHWL	301	KUJ	ELED	351	PZL	
202	CGG	ISBT	252	QEX	MHZP	302	XGP	CHMO	352	RZJ	
203	HDR	DMJT	253	YCD	DVLC	303	YKG	XWFI	353	YCF	
204	LCP	ARBN	254	NNH	GDZJ	304	LZH	MYKR	354	ZJL	
205	OJY	SXXM	255	GPX	FVOO	305	DSZ	KZYH	355	ZKX	
206	WEC	JKUT	256	BAD	BCQP	306	BSW	ZWFKY	356	ZLW	
207	YHJ	LZMO	257	PPP	ASFD	307	MRE	PKDY	357	ZMZ	
208	KMX	HEVR	258	RKQ	MTPX	308	ODT	GBKJ	358	ZNQ	
209	BRU	FEQN	259	VTZ	JKCO	309	UXB	YCGO	359	ZOR	
210	JJT	BPSA	260	HTZ	QPOM	310	KAZ	QAGJ	360	ZPZ	
211	AWY	HIMK	261	ALX	LDUP	311	YFG	OBIR	361	ZRZ	
212	GWE	MENU	262	RJD	SDUW	312	AYA	JIAT	362	ZSZ	
213	GBR	KOHS	263	AJL	ULKO	313	HFF	KVMP	363	ZTJ	
214	UWR	SHPK	264	BAG	VBYO	314	MVJ	PJAD	364	ZUJ	
215	QBR	PISK	265	MJW	FOCG	315	PHY	DGVN	365	ZVJ	
216	TRH	WREB	266	PLN	IRBP	316	VDA	QFM	366	ZWJ	
217	HQE	IYXJ	267	RDW	DFRX	317	KYZ	SCD	367	ZXJ	
218	BYH	YODZ	268	KPO	GOOJ	318	NAL	ISE	368	ZYJ	
219	FXK	APNF	269	DNS	STIH	319	HET	IQ	369	ZZJ	
220	MSY	GTMF	270	GTB	GLKO	320	CRV	DI	370	ZZJ	
221	PGX	ESMJ	271	KLK	CDWF	321	HPY	G	371	ZZJ	
222	UCY	MDNO	272	GPD	KWZK	322	SKD	F	372	ZZJ	
223	YKL	YSQR	273	LBD	UZFH	323	UKF	F	373	ZZJ	
224	BMP	FUSX	274	RTM	PLXZ	324	KED	F	374	ZZJ	
225	DUE	TMBU	275	HFF	OARS	325	LLT	F	375	ZZJ	
226	JSC	PXMY	276	RQW	IOBH	326	RRJ	F	376	ZZJ	
227	LHU	OMUT	277	KUF	DAGH	327	IPK	F	377	ZZJ	
228	OSH	NOAH	278	YKY	GNVF	328	HY	F	378	ZZJ	
229	UQM	LCZS	279	DCH	SLUZ	329	J	F	379	ZZJ	
230	YFQ	WSDG	280	FLB	RFVO	330	J	F	380	ZZJ	
231	ACE	IBEL	281	MWT	XJFU	331	J	F	381	ZZJ	
232	PAB	EGUN	282	HMH	UKHN	332	J	F	382	ZZJ	
233	HCM	SPUD	283	HFF	XMR	333	J	F	383	ZZJ	
234	NMQ	OKPY	284	GLT	EQZR	334	J	F	384	ZZJ	
235	PTK	WRUS	285	NKM	HLCK	335	J	F	385	ZZJ	
236	URZ	TFOD	286	CIN	CJXM	336	J	F	386	ZZJ	
237	ZMO	NHIA	287	DXC	APFK	337	J	F	387	ZZJ	
238	ATV	PXNH	288	HUD	GVJO	338	J	F	388	ZZJ	
239	CHR	BPAL	289	QNC	MTQJ	339	J	F	389	ZZJ	
240	HJB	NILK	290	QAR	KDPT	340	J	F	390	ZZJ	
241	KXJ	LEEN	291	KTB	SGUJ	341	J	F	391	ZZJ	
242	CKN	GOOU	292	WBR	QIFJ	342	J	F	392	ZZJ	
243	BNJ	ENBE	293	FPW	KX	343	J	F	393	ZZJ	
244	UQJ	KAPP	294	RDG	QY	344	J	F	394	ZZJ	
245	YUJ	WGGG	295	DQV	Z	345	J	F	395	ZZJ	
246	FIN	ORIS	296	KEV	Z	346	J	F	396	ZZJ	
247	...	...	297	...	...	347	J	F	397	ZZJ	



**Geheim!** 0

**Sonder-Maschinenschlüssel BGT**

*Nicht im Flugzeug mitnehmen!*

Datum	Wahrsage	Ringstellung	Steckerverbindungen	Keuigruppe
31.	I V III	06 20 24	UA PF RQ SO HI EY DG HL TX ZJ	Jeu nyq aqm
30.	V II III	01 07 12	GF KV JN IB UW LX TD QS NA ZH	ans sds kek
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: OWFWECEVEABSX





# 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 ???

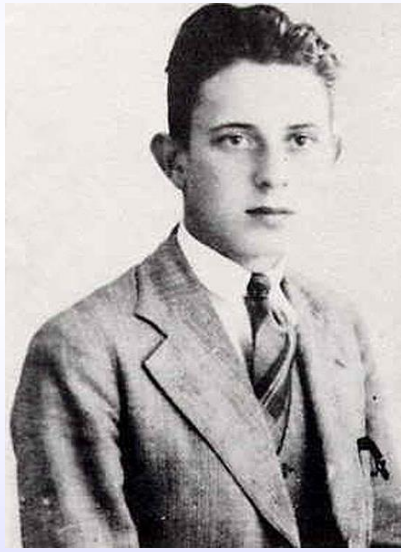


1	AUQ	AMN	23	NXD	QTU	45	TMN	EBY
2	BNH	CHL	24	NXD	QTU	46	TMN	EBY
3	BCT	CGJ	25	NLU	QFZ	47	TAA	EXB
4	CIK	BZT	26	OBU	DLZ	48	USE	NWH
5	DDB	VDV	27	PVJ	FEG	49	VII	PZK
6	EJP	IPS	28	QGA	LYB	50	VII	PZK
7	FBR	KLE	29	QGA	LYB	51	VQZ	PVR
8	GPB	ZSV	30	RJL	WPX	52	VQZ	PVR
9	HNO	THD	31	RJL	WPX	53	WTM	RAO
10	HNO	THD	32	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