

הצפנה ודרך פעולתה של מכונת האניגמה במלחמת העולם השנייה

עפר דרורי

offerd@gmail.com

האניגמה התפרסמה כמכונת ההצפנה האולטימטיבית במלחמת העולם השנייה ושימשה את הגרמנים בהעברת מסרים לכוחותיהם.

ראשית המכונה ב-1918 והתבססה על פטנט ישן בן מאות שנים בו בוצעה החלפת אותיות במסר המקורי והחלפה חוזרת במסר המתקבל. שיטה זו נועדה למנוע קריאת המסר ע"י גורם שלישי לא מורשה ע"י שולח המסר, שנחשף למסר.

הצפנה

בעברית כולנו מכירים את צופן הילדים "את-בש" שעושה שימוש באותו רעיון. בשיטת "את-בש" האות הראשונה באלף בית העברי מוחלפת באותו האחרונה של האלף בית. כלומר האות "אלף" מוחלפת באות "תוו" והאות "בית" מוחלפת באות "שין" וכך הלאה.

בטבלה 1 נראה את כל ההחלפות של האלף-בית העברי (לשם הפשטות הוסרו האותיות הסופיות)

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	ק	ר	ש	ת
ת	ש	ר	ק	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

טבלה 1 – מפתח ההצפנה לצופן "את-בש" עם חילוף קבוע של אותיות פעם אחת

כאשר נכתוב את האות "אלף" הצד המקבל יקבל את האות "ת", כאשר נכתוב את האות "ב" הצד המקבל יקבל את האות "ש", ואם נשלח מילה שלמה לדוגמא "אניגמה"

הצד המקבל יקבל את המילה "תחלרטפ" כמובן שלמילה זו אין משמעות, כך שאם הטקסט ייורט ע"י צד ג' הוא יקבל מילה חסרת משמעות "תחלרטפ".

כדי שהצד המקבל יבין מה נשלח אליו הוא יצטרך להשתמש במפתח פענוח. במקרה זה טבלה 1 היא המפתח, המרת כל אות לאות המקורית תניב לו את המילה המקורית "אניגמה".

כמובן שהצפנה זו היא פשוטה ומומחים להצפנה יוכלו לפענח את המסר גם ללא המפתח מכמה סיבות:

1. כל אות במסר הנשלח מוחלפת לאותה אות במסר המתקבל
2. לכל שפה יש תדירות קבועה סטטיסטית, לדוגמא האות "מים" בעברית היא הנפוצה ביותר כך שניתן לשער בטקסט מספיק ארוך מהי האות המחליפה וממנה בהמשך פענוח של אותיות נוספות.

כדי להתמודד עם בעיה זו יצרו סיבוכיות נוספת, כל אות תהיה מוחלפת לאות אחרת והאות האחרת תהיה מוחלפת לאות שלישית. מפתח ההצפנה יראה במקרה זה בטבלה

2. כלומר האות "אלף" תוחלף לאות "בית" כמו קודם ואילו האות "תוו" תוחלף מיידית לאות "שין".

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	ק	ר	ש	ת
ת	ש	ר	ק	פ	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	ק	ר	ש	ת
ש	ר	ק	פ	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	ק	ר	ש	ת	א

טבלה 2 – מפתח ההצפנה לצופן "את-בש" עם חילוף קבוע של אותיות פעמיים

המסר אם כך למילה "אניגמה" יתקבל לאחר ההצפנה "שזכקחע". בתחילה האות "אלף" תוחלף לאות "תוו", האות "תוו" תוחלף לאות "שין". האות "נון" של המילה אנגימה תוחלף בהתחלה לאות "חית" והאות "חית" תוחלף לאות "זין".

ניתן לראות שיש כאן סיבוכיות נוספת אבל השיטתיות בהחלפת האותיות מקלה על הפענוח ולכן ניתן לבצע את אותה הצפנה אבל האותיות המתחלפות תהיינה בדילוג של 3 אותיות לדוגמא שמפתח ההצפנה יראה בטבלה הבאה, 3.

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	ק	ר	ש	ת
ר	ע	מ	י	ז	ד	א	ר	ע	מ	י	ז	ד	א	ר	ע	מ	י	ז	ד	א
דילוג 3	דילוג 6																			
אותיות ימינה מהאות "תוו"	אותיות ימינה מהאות "תוו"																			

טבלה 3 עם חילוף קבוע של אותיות אבל בדילוגים של 3 אותיות

באותה שיטה ניתן לסבך את מפתח ההצפנה, דילוגים של אותיות מספר פעמים ועוד פעמים. יש לזכור שככל שמפתח ההצפנה מורכב יותר פענוח המסר ייקח יותר זמן.

הבסיס של ההצפנה המתוארת של חילופי אותיות קבועים או משתנים הוא הבסיס גם למכונת האניגמה.

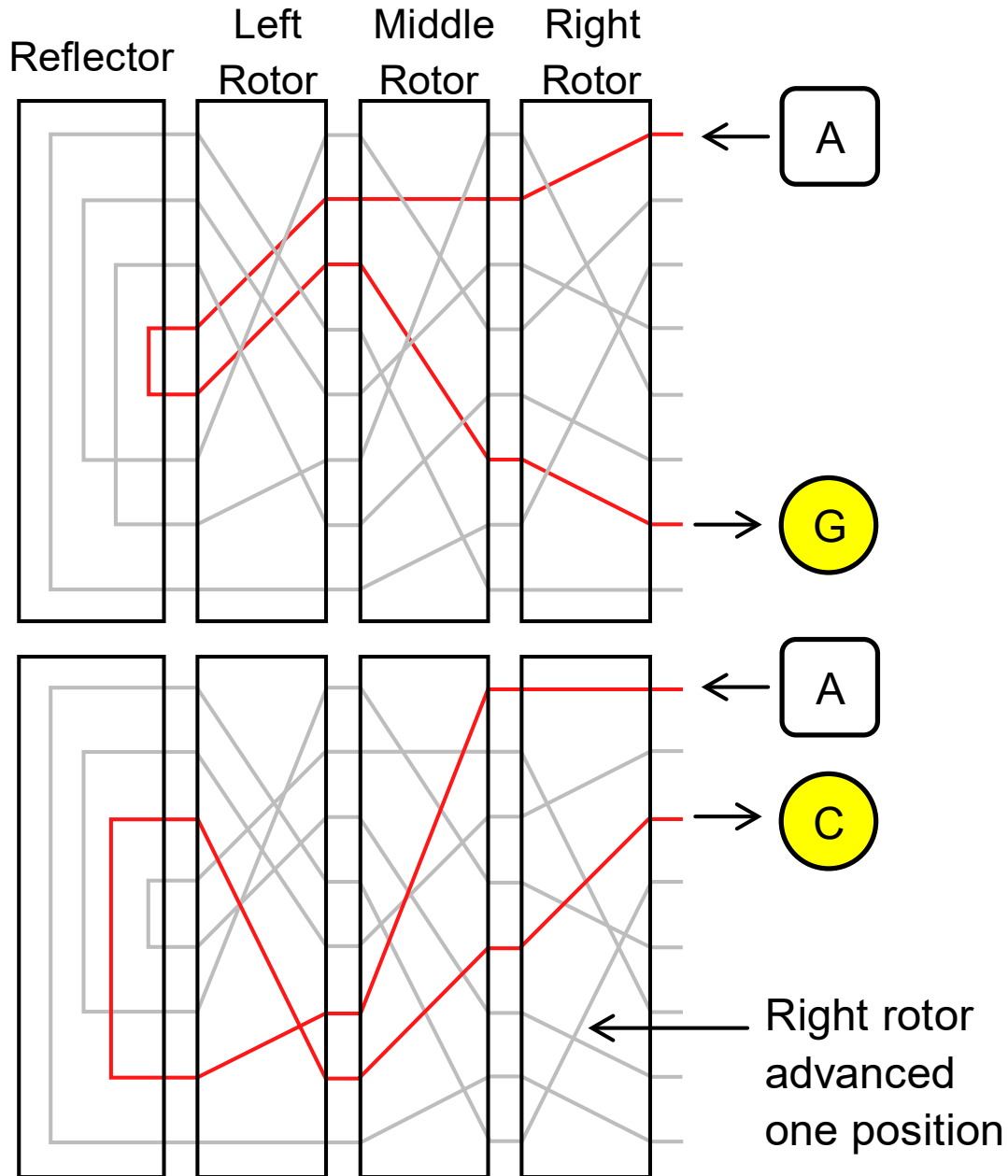
דרך הפעולה של המכשיר

הרעיון המרכזי במכונת האניגמה היה שילוב בין החלפות שונות ומשתנות בכל הקלדה של אות במסר. האניגמה הייתה מכונה אלקטרו מכנית הראשונה להצפנה. בכל הקלדה של אות הסתובב רוטור של אותיות וייצר החלפת אותיות משתנה בכל הקלדה כך שהקלדת אותה אות בפעם החמישית הייתה מייצרת אות חליפית השונה מהאות שהוחלפה בכל ארבעת ההחלפות הקודמות. סיבוכיות נוספת הושגה בשימוש במספר רוטורים כך שגם האות שהוחלפה באות הראשונה ברוטור הראשון הוחלפה לאות חדשה ברוטור השני וככה גם בשלישי.

תהליך השימוש ברוטורים באניגמה מתואר בתרשים כאשר משמאל לשלושת הרוטורים קיים רפלקטור (משקף) שכל תפקידו להעברת התווים המוצפנים דרך 3 הרוטורים בכיוון ההפוך וכל זה כדי להגביר את הסיבוכיות (ניתן היה לעשות שימוש ב-6 רוטורים ברצף

ללא רפלקטור אבל אז גודלה הפיזי של המכונה היה גדול יותר דבר המהווה חסרון במכשיר האמור להיות נייד).

בתרשים המצורף ניתן לראות את מסלול ההמרה של אות מוקלדת במסר עד ליציאתו של אותו תוו לאחר הצפנה.



(זכויות התרשים: מאת MesserWoland - נוצר על ידי מעלה היצירה בהתבסס על:

File:Enigma-action.png by User:Jeanot; original diagram by Matt Crypto, CC BY-SA (3.0, <https://commons.wikimedia.org/w/index.php?curid=1794494>

באמצעות לוח מיתוג חשמלי שהסידור שלו היה משתנה אפשר היה להגביר את כמות הצירופים לכל תוו מוצפן ובכל להגדיל עוד ועוד את היקף הצירופים האפשרי להצפנה.

לוח המיתוג אפשר רמת הצפנה גדולה הרבה יותר מאשר הוספת רוטור נוסף למכשיר. ניתן היה להשתמש בעד 13 זוגות כבלים במכונה.

הכנסת המסר למשלוח נעשתה באמצעות לוח מקשים כמו זה של מכונת כתיבה בזמנו או מחשב בימינו. כל אות שהוקשה הדליקה נורית של אותיות שבפועל הוצפנו. לדוגמא האות A שהוקלדה הדליקה את הנורית של האות Z וכך הלאה לכל אותיות המסר. ראינו שהקלדת אותה אות פעמיים לדוגמא A ולאחריה שוב A הייתה מאירה בפעם הראשונה את האות Z ולאחר מכן לדוגמא את האות L.

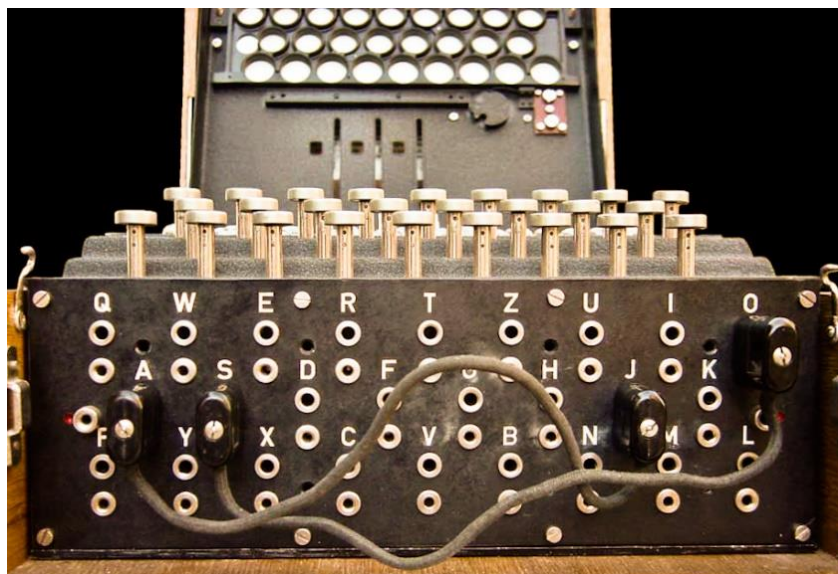
הצד השולח היה מעביר במורס את רצף האותיות כפי שנרשם ידנית ע"י רצף האותיות המוארות ונשלח בצורה גלויה. הקלדת האותיות שהתקבלו בצורה גלויה בצד המקבל למכונת האניגמה הזהה ורישום האותיות המוארות שהתקבלו מהקלדת המסר המוצפן יצרו את המסר המפוענח.

פעולה זו הייתה לוקחת זמן אבל המסר שנשלח באוויר וגם אם היה מיורט ע"י האויב לא אפשרה ליריב לפענח את המסר.

כדי לוודא שכיוון מכונת האניגמה בצד השולח ובצד המקבל זהה היה מסר ראשוני שהשתנה בכל יום אשר הגדיר את מצבי הרוטורים בהתחלה, את מצבי "הגשרים" בלוח החשמלי. רק במצב זהה של שני המכשירים ניתן היה לפענח את המסר המוצפן.

בזמנו נחשבה מכונת האניגמה כבלתי ניתנת לפיצוח ורק צוות של מדענים אנגליים שנמצאו בבבלצ'לי פארק ליד לונדון ובראשם טיורינג נמצאה השיטה לפענוח הקוד. פענוח השיטה היה סוד שמור ביותר אצל האנגלים דבר שגרם לגרמנים להמשיך לעשות שימוש במשך תקופה ארוכה בהודעות מוצפנות מבלי שידעו שהמסרים שלהם מפוענחים ע"י האנגלים. תפיסתה של צוללת גרמנית עם יומן צופן לקביעת המצב הראשוני של האניגמה בכל יום סייעו בפענוח הצופן.

לוח הפלגים עם הגשרים אפשר סיבוכיות נוספת של ההצפנה. גם סידור הפלגים הועבר אחת ליום כדי לכייל את המכשיר באופן תואם בין כל מכשירי הצבא הגרמני.



(תמונת המכשיר: ויקיפדיה)

כמות הצירופים באלף בית האנגלי עמד על 10 בחזקת 20, מספר גדול שלא אפשר פענוח בכלים של אז או בדיוק עפ"י המתמטיקאי האנגלי:

158,962,555,217,826,360,000 (ובעברית: 158 קווינטיליון)

Kenngruppenheft Nr. 7

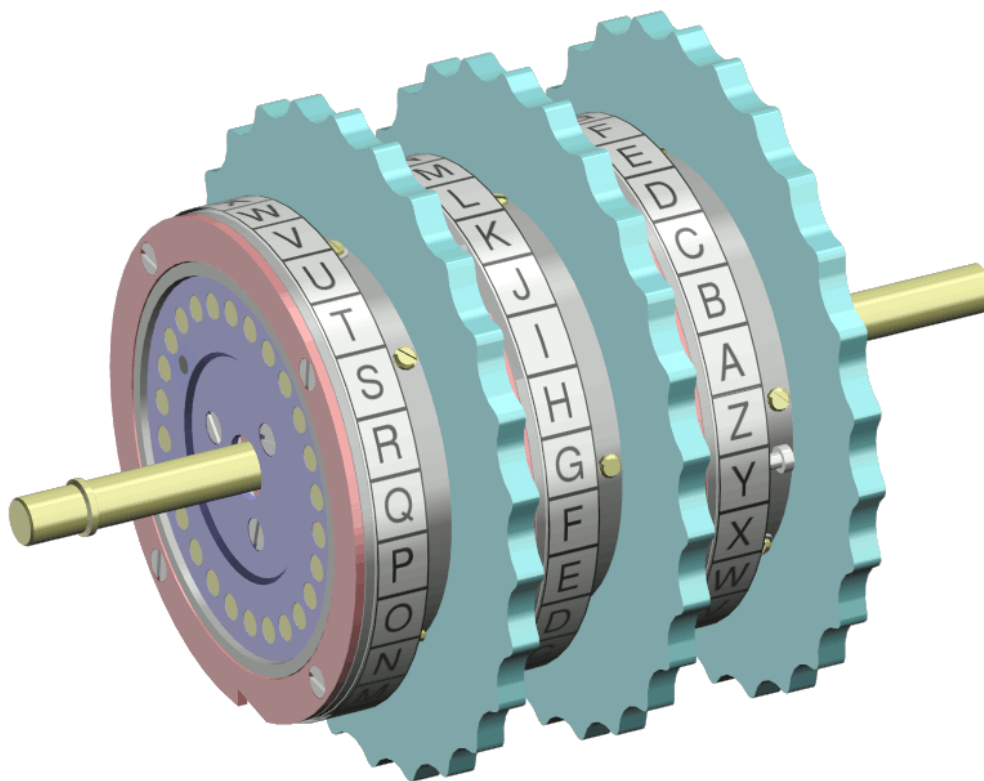
Teil A

Nr.	Kenngruppe	Sprache-schlüssel	Nr.	Kenngruppe	Sprache-schlüssel	Nr.	Kenngruppe	Sprache-schlüssel	Nr.	Kenngruppe	Sprache-schlüssel
1	DDJ	ABCK	51	GJR	WOLD	101	PBJ	POER	151	MIV	XABQ
2	LWJ	BMUL	52	LTP	YBHO	102	RCV	BOVF	152	NZO	BWOD
3	JTY	BOJY	53	PJE	NSGL	103	YGE	TRMT	153	POH	RKXT
4	XOD	DNBS	54	SAU	COHF	104	UOK	LSOM	154	QOH	BUOT
5	SMF	EBHO	55	WBE	AUPE	105	WKR	RCAT	155	BQK	FUDH
6	UPL	FOAS	56	WYV	LRHG	106	KGB	UZCB	156	VLIH	ONFO
7	YOP	GDHJ	57	AAAC	JAHK	107	ZBD	WFKC	157	WVT	ARST
8	ARG	GYPF	58	DBG	KXIT	108	BEH	ATFI	158	XZY	FPTJ
9	FNJ	HTUZ	59	POV	ZBDO	109	DWB	LXFT	159	CVE	KXNF
10	HHH	HZNS	60	DHN	IYTO	110	KKT	IGOS	160	AKX	AGFO
11	KOZ	JFKK	61	GXF	BNOP	111	KWH	TYOK	161	KKQ	KODN
12	NYK	EKUZ	62	JVF	NCGL	112	MKK	UPFT	162	DPL	UAMN
13	REX	ZIRS	63	NFD	AHKK	113	OGF	ILFF	163	FUB	XIYP
14	VJY	IFHX	64	QWO	MGAK	114	QJA	FHGE	164	QVD	THRE
15	XJH	YDXN	65	TTQ	RZDK	115	EDK	THGE	165	JXK	INLJ
16	BHL	TGHP	66	TZU	WOKU	116	TVQ	NFTX	166	KQH	QZER
17	EOJ	YJHA	67	JJK	YMBF	117	WHF	ALWR	167	NCH	SDRG
18	KDF	XHON	68	ZQE	TPBL	118	YDE	HFOO	168	QFT	ERBL
19	LGT	BYFT	69	AVX	BMGR	119	BUX	AGKI	169	QYQ	CKUT
20	OWM	RJRP	70	EVB	XOGS	120	FFN	KZPT	170	TRM	SXZF
21	QPG	SAML	71	GNV	JGDK	121	DWY	KIBY	171	ULG	OJFF
22	TUP	PCRB	72	JNX	XDGL	122	GRZ	UBZY	172	WOM	JTFG
23	DWU	ICIM	73	LMZ	IGXK	123	JPE	TSEN	173	XFB	ESTQ
24	CPT	ENTF	74	NJX	QIUW	124	LQC	NRTK	174	XFB	PATB
25	KPV	FUCE	75	NTH	ZFKO	125	NDS	OYGN	175	BHE	FIOA
26	GEN	AXSB	76	RVO	LRYF	126	PCT	IUGK	176	COB	TNPD
27	MOB	RGNS	77	TJD	DOLK	127	RNF	EHAF	177	FMT	DCOT
28	NLE	OKSH	78	UDZ	MOED	128	VCE	GORS	178	DMR	GSFL
29	RRE	ALIK	79	VBF	ONBU	129	YCW	WAKH	179	GMU	WFFX
30	WQO	NCYS	80	XBC	SKHI	130	ART	OTET	180	JAL	TCEY
31	AXW	MOEL	81	WHR	EFOK	131	CKB	PFIQ	181	KYK	NUZL
32	GAZ	XETO	82	ABH	NOZF	132	MLB	HXGD	182	HMS	IJOH
33	DOT	FEHS	83	FHF	UTFA	133	GCL	STEN	183	OOD	DLOG
34	HYH	YEHY	84	HTC	TIME	134	HBL	WOFJ	184	QHT	AFST
35	LAN	LPMK	85	KFR	OKZU	135	KCO	KMWE	185	QJN	CHST
36	OCS	GFBY	86	MYM	OHFS	136	LZM	URNO	186	RQJ	CHST
37	TCZ	AYNE	87	OHX	JNOU	137	NGV	JFIV	187	KXN	UOEG
38	UVB	FPLE	88	QOF	LEPT	138	QBW	KYFJ	188	USO	FWCG
39	YTF	JAFK	89	RKC	UTYO	139	SHH	SRDO	189	VRO	LEER
40	ALN	FLKI	90	VXU	WIZM	140	YUO	OVTO	190	KAN	ISXO
41	CHM	ZERK	91	KBG	OPGZ	141	WVU	XADU	191	KRE	CTOV
42	SGN	LEWH	92	YST	YGOS	142	KHM	USMF	192	OTE	SUGL
43	HGX	SCZF	93	AFB	TUSY	143	SDG	GYRE	193	HWF	SIGB
44	MDR	BYOG	94	KED	BOLH	144	ADJ	SEYIC	194	LZY	GOYH
45			95			145	BRQ	EDTE	195	OYO	MOFU

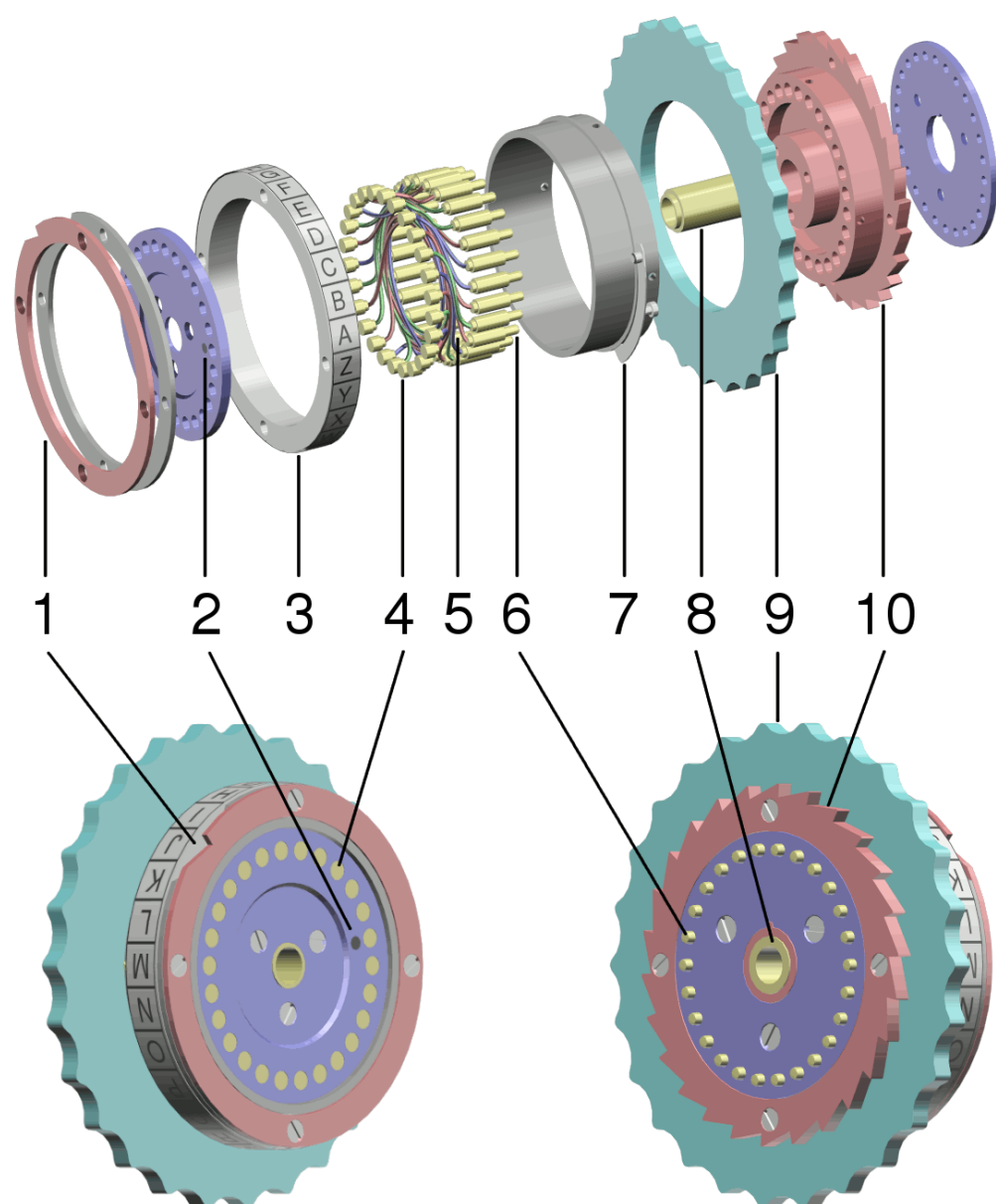
Teil A

Nr.	Kenngruppe	Sprache-schlüssel	Nr.	Kenngruppe	Sprache-schlüssel	Nr.	Kenngruppe	Sprache-schlüssel	Nr.	Kenngruppe	Sprache-schlüssel
201	ANP	TCAM	251	CGI	INFL	301	UJL	ELPD	351	UJL	ELPD
202	CGG	ISRT	252	QFZ	MBZF	302	ZOT	CHMO	352	UJL	ELPD
203	HDB	DMJT	253	YCD	DVLE	303	LYM	ZTFI	353	UJL	ELPD
204	LCP	AREB	254	NHJ	GDZ	304	LYM	ZTFI	354	UJL	ELPD
205	OJY	SRXM	255	QFZ	MBZF	305	UJL	ELPD	355	UJL	ELPD
206	WEC	JKUT	256	RAD	BCOF	306	SWZ	WFEY	356	UJL	ELPD
207	YHJ	LZMQ	257	PPF	ASFD	307	MDR	BYEY	357	UJL	ELPD
208	KMX	HEFE	258	RKQ	MTFX	308	ODT	GBFJ	358	UJL	ELPD
209	RKU	PEON	259	VTQ	JKCO	309	WVW	VCOG	359	UJL	ELPD
210	JTB	BFSA	260	ETZ	OPOM	310	WVW	VCOG	360	UJL	ELPD
211	AWY	HIMK	261	LKR	IDUP	311	YTG	QASZ	361	UJL	ELPD
212	QWR	ARNB	262	RLD	SDUP	312	AYA	FIAT	362	UJL	ELPD
213	OBH	KOHS	263	ALU	PUKO	313	DRF	KYMT	363	UJL	ELPD
214	UWB	SEKF	264	EAG	FVYO	314	WVW	VCOG	364	UJL	ELPD
215	KRE	FISE	265	MWJ	POCG	315	PHY	DGVS	365	UJL	ELPD
216	KNN	WFER	266	FLB	IRFP	316	WVW	VCOG	366	UJL	ELPD
217	HQZ	TJMY	267	BDW	DFEX	317	WVW	VCOG	367	UJL	ELPD
218	BYB	TODZ	268	KFC	GGOJ	318	NAT	WZ	368	UJL	ELPD
219	FQA	ATNF	269	DSE	STIH	319	HEL	IO	369	UJL	ELPD
220	MST	OTMF	270	QTB	GLKO	320	CRV	MD	370	UJL	ELPD
221	UCY	MDNO	271	GGF	KXZF	321	SKD	Y	371	UJL	ELPD
222	YKL	YSQR	272	LBD	UZFH	322	SKD	Y	372	UJL	ELPD
223	BMP	FUSX	273	ATM	FLRX	323	SKD	Y	373	UJL	ELPD
224	DUZ	TMBU	274	KFO	OKHS	324	LLT	Y	374	UJL	ELPD
225	JSC	PKMY	275	EQW	IONH	325	LLT	Y	375	UJL	ELPD
226	LHU	OMUT	276	KUF	DRGH	326	LLT	Y	376	UJL	ELPD
227	ORH	NOAH	277	YXT	GNVF	327	LLT	Y	377	UJL	ELPD
228	QML	LCZS	278	DCH	SLUZ	328	LLT	Y	378	UJL	ELPD
229	YTN	QNEG	279	FLB	IRFP	329	LLT	Y	379	UJL	ELPD
230	ACE	IDBL	280	WVW	VCOG	330	LLT	Y	380	UJL	ELPD
231	PAH	SCOH	281	WVW	VCOG	331	LLT	Y	381	UJL	ELPD
232	HCM	FFID	282	WVW	VCOG	332	LLT	Y	382	UJL	ELPD
233	MCQ	QOFJ	283	GLT	EQSZ	333	LLT	Y	383	UJL	ELPD
234	FTK	WVUE	284	NKM	HLCK	334	LLT	Y	384	UJL	ELPD
235	FRK	ATQD	285	CJN	CTKM	335	LLT	Y	385	UJL	ELPD
236	EMO	HALL	286	DXC	APTK	336	LLT	Y	386	UJL	ELPD
237	ATV	STMH	287	HUD	GVJG	337	LLT	Y	387	UJL	ELPD
238	ONK	BFAL	288	QWC	HYQS	338	LLT	Y	388	UJL	ELPD
239	HJN	SLIK	289	QZB	KDFT	339	LLT	Y	389	UJL	ELPD
240	KXJ	SLAN	290	XTB	SLCU	340	LLT	Y	390	UJL	ELPD
241	KXJ	SLAN	291	WVW	VCOG	341	LLT	Y	391	UJL	ELPD
242	KXJ	SLAN	292	WVW	VCOG	342	LLT	Y	392	UJL	ELPD
243	KXJ	SLAN	293	WVW	VCOG	343	LLT	Y	393	UJL	ELPD
244	KXJ	SLAN	294	WVW	VCOG	344	LLT	Y	394	UJL	ELPD
245	KXJ	SLAN	295	WVW	VCOG	345	LLT	Y	395	UJL	ELPD

דוגמא ללוח הצופן שהכיל את היום בחודש ואת הצירופים שיש לכייל את מכשיר האניגמה לשם יצירת מכנה משותף בכל המכונות ביום מסוים (מקור: ויקיפדיה)



הרוטורים (דיסקיות) במכונת האניגמה בעלת 3 רוטורים, כל תזוזה של רוטור אחד בסיבוב מלא יצרה תזוזה של הרוטור הבא בתור בפסיעה אחת – כלומר תזוזה של אות אחת. כנ"ל בסיום סיבוב של הרוטור השני ותזוזה של אות אחת ברוטור השלישי (צילום: ויקיפדיה)



פירוט החלקים הנעים שהיו מחוברים לרוטורים השונים (מקור: ויקיפדיה).



מכונת האניגמה במבט צידי. ניתן לראות את לוח המקשים של האותיות. מעליו את הנוריות שכל אחת מהן ייצגה את האות המוחלפת. בחזית לוח המתגים עם הגשרים אשר ייצר רמה נוספת של הצפנה וסיבוכיות רבה יותר. מיקום הגשרים כמו מיקום הרוטורים השתנו מידי יום בהתאם לטבלאות הצופן שהועברו בין היחידות השונות.

מומלץ לצפות בסרטון הממחיש את פעולת מכשיר האניגמה שנמצא כאן

https://www.youtube.com/watch?v=G2_Q9FoD-oQ