

מכונת ההצפנה - אניגמה

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 "תו" 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	ע	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	ק	ר	ש
ש	ר	ק	פ	ע	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	ק	ר	ש	ת

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 "תו", האות "תו" תוחלף לאות "שין". האות "נו" 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	אותיות ימינה																	
ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת	ת

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.

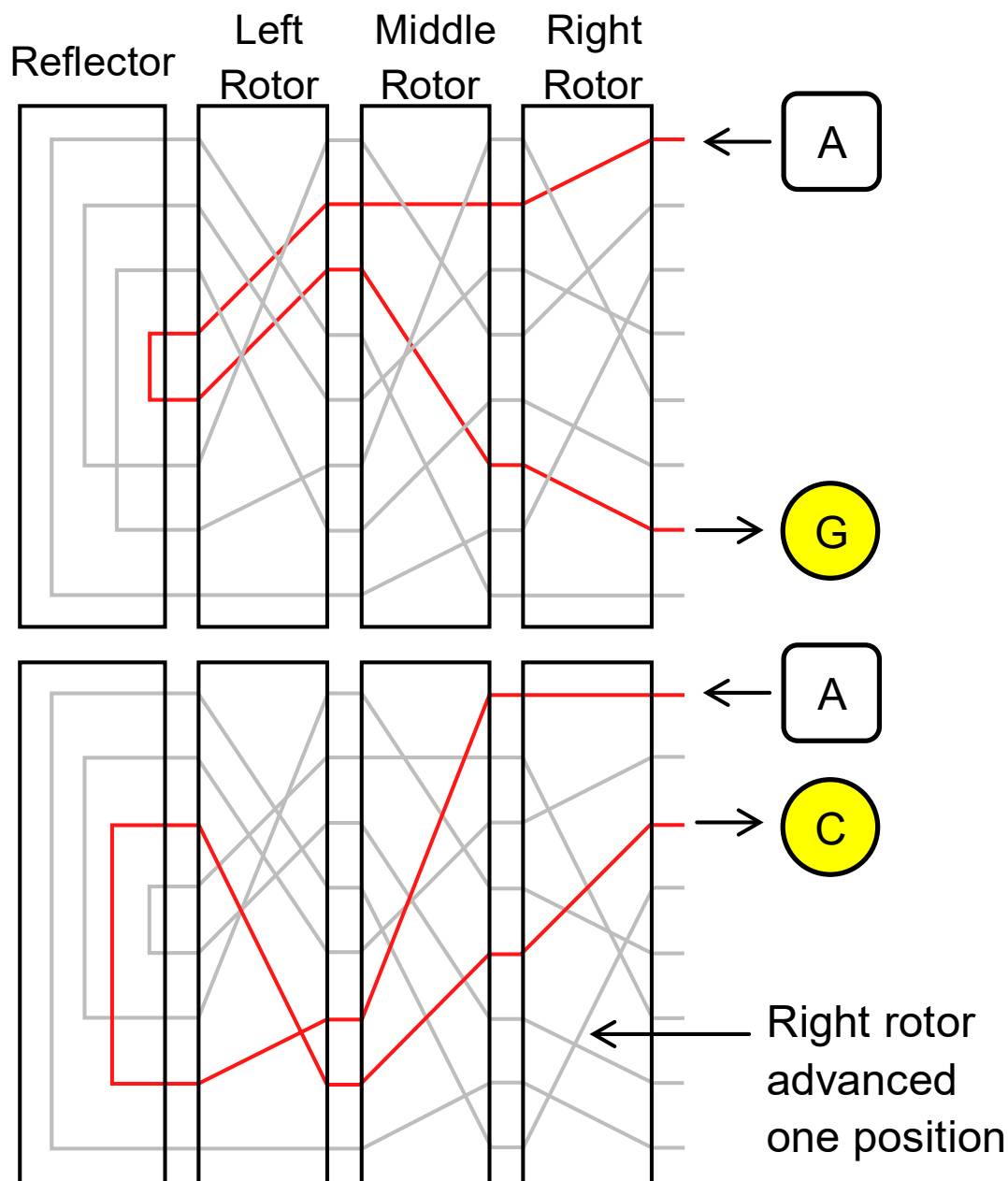
דרך הפעולה של המכשיר

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.

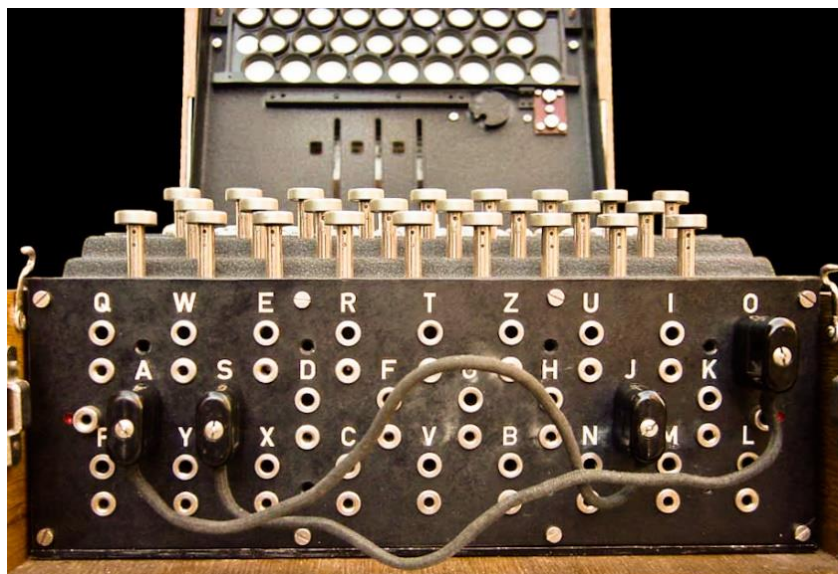
הצד השולח היה מעביר במורס את רצף האותיות כפי שנרשם ידנית ע"י רצף האותיות המוארות ונשלח בצורה גלויה. הקלדת האותיות שהתקבלו בצורה גלויה בצד המקבל למכונת האניגמה הזוהר ורישום האותיות המוארות שהתקבלו מהקלדת המסר המוצפן יצרו את המסר המפוענח.

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 זה של שני המכשירים ניתן היה לפענח את המסר המוצפן.

בזמנו נחשבה מכונת האניגמה כבלתי ניתנת לפיצוח ורק צוות של מדענים אנגליים שנמצאו בבליצ'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 ויום 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.



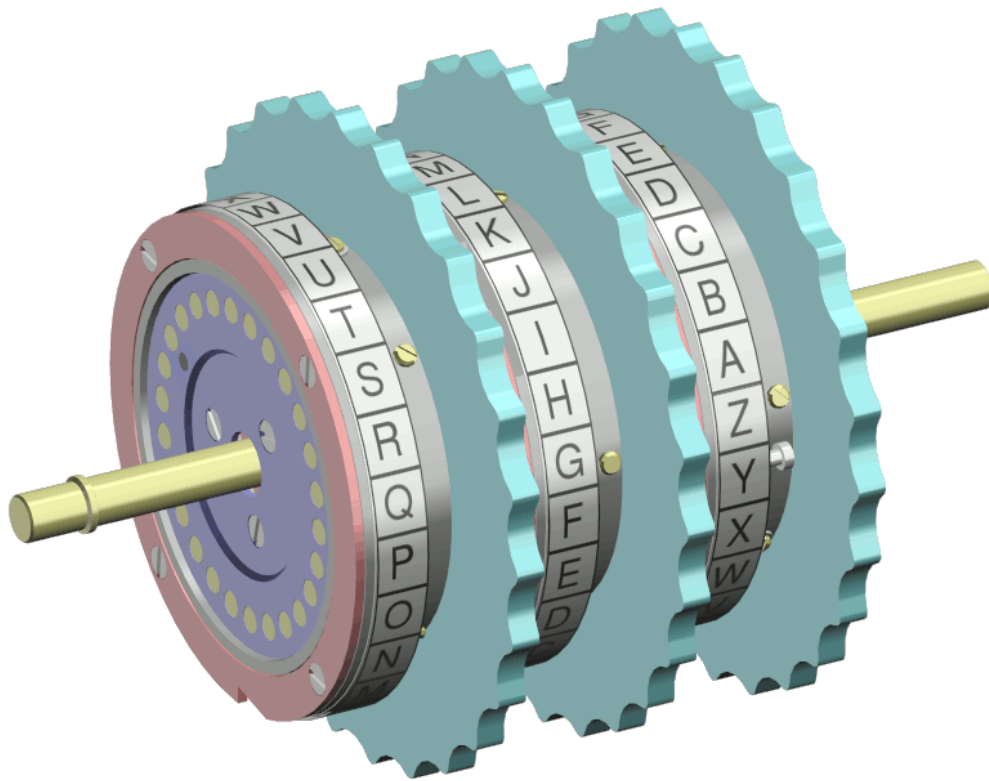
(תמונת המכשיר: ויקיפדיה)

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

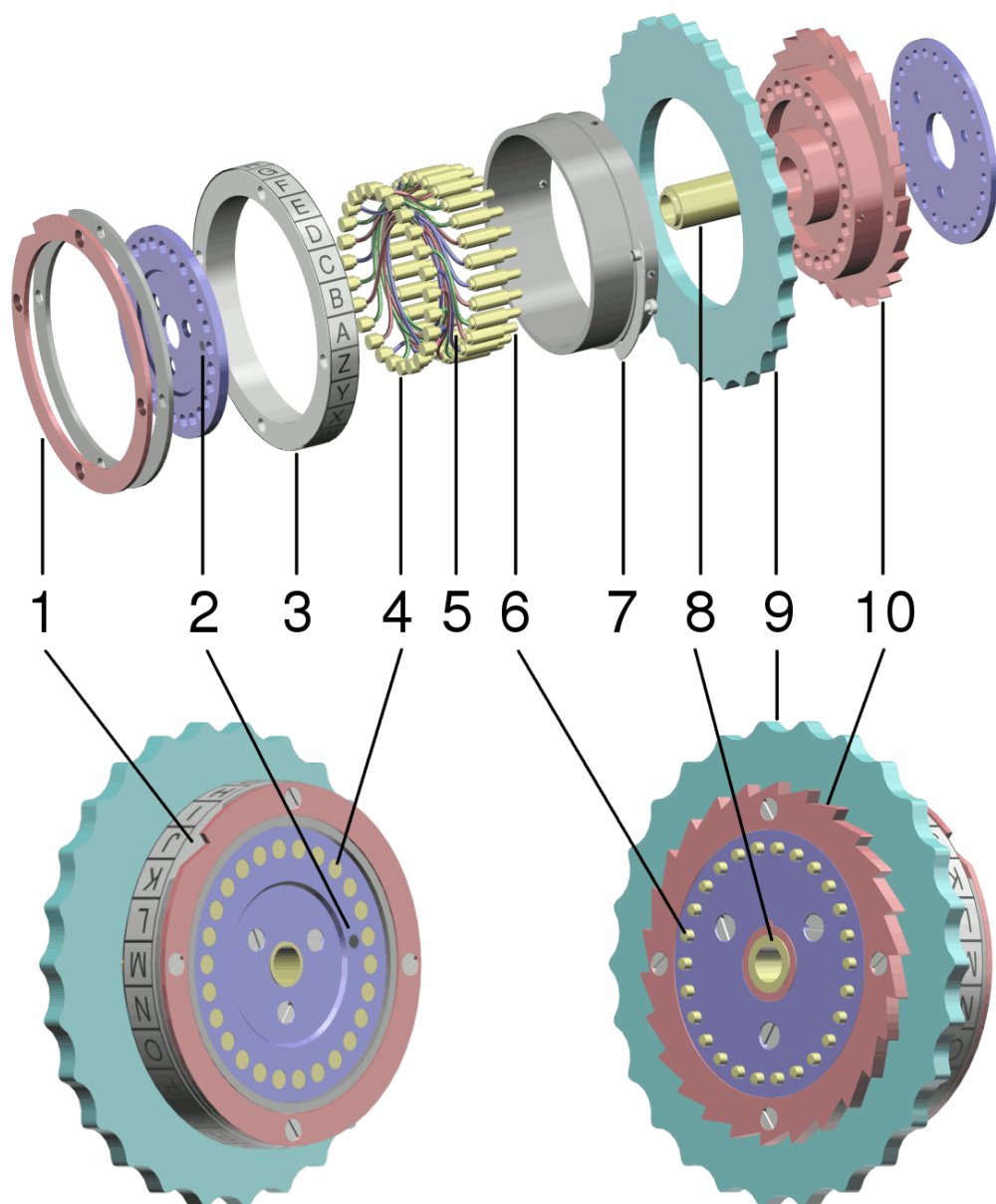
158,962,555,217,826,360,000 (ובעברית: 158 קווינטיליון)

Kenngruppenheft Nr. 7												Teil A											
Kenngruppe						Spruchschlüssel						Kenngruppe						Spruchschlüssel					
Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel
1	DDJ	ARCK	51	GJR	WOLU	101	PBJ	PQER	151	MHV	XABQ	241	AHP	TCAM	291	COL	INHL	341	HUJ	ELFD	391	YZ	
2	LWJ	BMUL	52	LDY	YBHO	102	ROV	BOVP	152	NZO	BBOD	242	COO	ISST	292	QEZ	MBZF	342	KGF	CHMO	392	BA	
3	JHJ	BOJY	53	PJE	NSGL	103	BYB	NEMT	153	POE	HXVT	243	HDB	DMJT	293	YCD	DPLE	343	VKO	ZTFI	393	YK	
4	XOD	DNBS	54	BAU	COHF	104	UOK	LSOM	154	QQR	RUOT	244	LOP	AEEN	294	NNB	ODZJ	344	LVC	ZZFI	394	YK	
5	EMF	ERGO	55	WBE	AUPE	105	WKE	RCEI	155	BQR	FUDH	245	QJY	SEXX	295	QFV	PFVG	345	LVC	ZZFI	395	YK	
6	UPL	FGAS	56	WYU	LRBG	106	KCB	UZCB	156	VLB	OWVO	246	WRC	YKUT	296	BAD	SCGP	346	QFV	PFVG	396	YK	
7	TOP	GDHT	57	AAU	JAHK	107	ZBD	WKNP	157	WVT	ARBJ	247	XHJ	LZMO	297	PFP	ASPD	347	ODT	GBEY	397	YK	
8	ARG	OYTF	58	DEG	EXIT	108	BEH	ATZI	158	KZY	FFTI	248	KMS	HEFE	298	RZQ	MTFX	348	UTY	FCOS	398	YK	
9	THJ	HTUZ	59	POV	ZBOO	109	DWB	LXFY	159	CVE	EKNV	249	BRU	FEON	299	VTQ	JACO	349	ODT	GBEY	399	YK	
10	HHR	HZNS	60	DKN	IYFO	110	HKT	IGOE	160	AXZ	NGPO	250	JJN	TFJA	290	ETZ	QPGM	350	ETZ	QPGM	390	YK	
11	KOZ	JFNK	61	GXF	BNOP	111	KWH	TYOE	161	KKQ	ROON	251	AWY	HIMK	291	LKK	IDUF	351	ETZ	QPGM	391	YK	
12	NYK	ERKZ	62	YVF	NCBL	112	KKX	UPFT	162	DFL	UAMN	252	QWR	AKNU	292	KLD	SDUW	352	ETZ	QPGM	392	YK	
13	REX	ZIBS	63	NPD	AHIR	113	QQF	ILVF	163	GVD	THRT	253	OWB	SEKF	293	AJL	ULKO	353	ETZ	QPGM	393	YK	
14	VJY	IPHX	64	QWO	MGAK	114	QJA	VHAE	164	JZK	INLJ	254	UWS	SEKF	294	AGV	YBYQ	354	ETZ	QPGM	394	YK	
15	KJH	YDKN	65	TDU	REDK	115	DDK	THCN	165	KQR	OXER	255	QSK	PIER	295	MTW	POCG	355	ETZ	QPGM	395	YK	
16	BHL	TDHF	66	TZU	WOKU	116	VQ	NFTX	166	KQR	OXER	256	TNN	SEER	296	PLB	IRRF	356	ETZ	QPGM	396	YK	
17	ECJ	YJHA	67	YJK	YMBW	117	WHF	ALWR	167	NCH	EDRG	257	HQZ	IFJY	297	RDW	DFEX	357	ETZ	QPGM	397	YK	
18	KDF	XHON	68	ZQS	JPBL	118	YDE	HPQO	168	OPV	CETO	258	BTY	YODI	298	PCO	GOOJ	358	ETZ	QPGM	398	YK	
19	LGT	BYFT	69	AVX	BMGR	119	BUU	ALWR	169	QBT	FRBL	259	YQK	ATNF	299	CHS	STIH	359	ETZ	QPGM	399	YK	
20	OWZ	KJHP	70	EVB	XQGS	120	FFN	REPT	170	QYQ	CKUF	260	MSF	GTMF	290	GTR	GLKO	360	ETZ	QPGM	390	YK	
21	QPS	SAML	71	GNV	JGDK	121	DRW	XIHS	171	ULG	QAFP	261	PGX	ESMT	291	XLK	CDEF	361	ETZ	QPGM	391	YK	
22	TDF	PCRB	72	JNX	XDKL	122	GRZ	USEY	172	WOM	JTFU	262	UCY	MDNQ	292	GGP	XWZK	362	ETZ	QPGM	392	YK	
23	ZDW	HGIM	73	LNZ	RIGX	123	JFZ	TSEN	173	XOM	JTFU	263	YLL	YSOR	293	LRN	UIYH	363	ETZ	QPGM	393	YK	
24	GPT	ENTW	74	NJX	QIUW	124	LQC	NETK	174	ZFH	FATB	264	DUE	TMRU	294	ATM	FLER	364	ETZ	QPGM	394	YK	
25	EPV	FUCZ	75	NTU	ZFKO	125	NDS	OYGN	175	BHE	FIOA	265	LNU	OMUT	295	KUF	DRGH	365	ETZ	QPGM	395	YK	
26	GEN	AXSB	76	RYO	LEYF	126	PCT	IUGK	176	COB	INPO	266	ORH	NOAH	296	YCT	GNVY	366	ETZ	QPGM	396	YK	
27	MOB	RGNS	77	TJD	DOLK	127	RNF	SHAF	177	FMT	DCOT	267	UQM	LCZS	297	DCU	SLUJ	367	ETZ	QPGM	397	YK	
28	NLE	OKKH	78	UDE	MOED	128	VCE	CGRS	178	DMR	GKPL	268	YTG	HEGG	298	FLS	BYFO	368	ETZ	QPGM	398	YK	
29	RRK	ALIK	79	VBP	GONBU	129	YWX	WXXH	179	GMS	WFFX	269	YCH	IDBL	299	MTT	JYPU	369	ETZ	QPGM	399	YK	
30	WQO	NCYS	80	YBC	BKHI	130	ART	OTEF	180	JAL	TGRY	270	FAH	ECUN	300	UMH	DEPH	370	ETZ	QPGM	390	YK	
31	KXW	MOEL	81	ZHR	EFOR	131	CKB	PFTO	181	KYH	NUZE	271	HCM	EFID	301	BFJ	XAMG	371	ETZ	QPGM	391	YK	
32	CAE	XSTO	82	AEB	NDZW	132	ELB	HXCH	182	MMZ	JTOH	272	MCQ	OXFJ	302	GLT	EQSZ	372	ETZ	QPGM	392	YK	
33	DOT	FENR	83	FHF	UTFA	133	GCL	STEN	183	OOD	DLOO	273	PTK	VRUE	303	NXM	HLCK	373	ETZ	QPGM	393	YK	
34	HYH	YKHY	84	HTC	TIME	134	HBL	WQFY	184	QHE	AFST	274	URN	TFOD	304	CJN	CTXM	374	ETZ	QPGM	394	YK	
35	LAN	LPMK	85	KFN	OKZU	135	KCO	KMFE	185	RQJ	ONST	275	ZMO	NALA	305	DXC	AFKX	375	ETZ	QPGM	395	YK	
36	OCB	CFBJ	86	MYM	OHVS	136	LZM	CRNO	186	SKH	UOSG	276	ATV	FSMH	306	HUD	GVJO	376	ETZ	QPGM	396	YK	
37	TCZ	AYNS	87	OHX	JNOU	137	NGV	JFIP	187	USO	FWCQ	277	CNR	BFAL	307	QWC	MYQS	377	ETZ	QPGM	397	YK	
38	UVB	WFLQ	88	QOF	LEPT	138	QBW	KYIP	188	VRO	LKRR	278	HJN	FNIL	308	QZL	EDFT	378	ETZ	QPGM	398	YK	
39	YYZ	JAPK	89	RKC	UTYG	139	SHH	ADGO	189	BEH	ISXQ	279	KXJ	LFEN	309	ETZ	QPGM	379	ETZ	QPGM	399	YK	
40	ALN	WLEI	90	VXU	WIZM	140	YUD	OVTO	190	ERE	GJOV	280	KXN	GOOU	310	WUS	EFSE	380	ETZ	QPGM	390	YK	
41	CHM	ZERK	91	ZBG	OPGZ	141	WVU	XAUW	191	OTE	EUGI	281	BNH	WZSS	311	FWF	WZSS	381	ETZ	QPGM	391	YK	
42	SGN	LEWH	92	YST	YGOS	142	XNM	USMF	192	HWF	SIQA	282	UQ	QZSP	312	BDG	VFYK	382	ETZ	QPGM	392	YK	
43	HGN	RCZY	93	ATP	TURV	143	SDG	QYBE	193	LIV	GOYH	283	YUT	WQGO	313	QZL	EDFT	383	ETZ	QPGM	393	YK	
44	MDE	STOG	94	KKD	BGLH	144	ADJ	EUYC	194	OYO	MOFU	284	BNH	WZSS	314	WUS	EFSE	384	ETZ	QPGM	394	YK	

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