Die Verschlüsselungsmaschine der Nazis

Velizar Demirev

Computerwissenschaften Salzburg

Table of contents

1. Was ist die Enigma?

2. Geschichte der Enigma

3. Aufbau der Enigma

4. Kleines Beispiel

5. Kryptographische Stärke

6. Kryptographische Schwächen

7. Die Enigma in der heutigen Zeit

8. Time to say goodbye

Was ist die Enigma?

Was ist die Enigma?

Figure 1: Enigma M4

Geschichte der Enigma

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.
- Zunächst versuchte Arthur Scherbius seine Erfindung der Kaiserlichen Marine zu verkaufen, diese winkte aber ab.

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.
- Zunächst versuchte Arthur Scherbius seine Erfindung der Kaiserlichen Marine zu verkaufen, diese winkte aber ab.
- Die erste Enigma (Enigma-A / 1923) wurde kommerziell vermarktet.

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.
- Zunächst versuchte Arthur Scherbius seine Erfindung der Kaiserlichen Marine zu verkaufen, diese winkte aber ab.
- Die erste Enigma (Enigma-A / 1923) wurde kommerziell vermarktet.
- Militärisch gewann die Enigma erst im späteren Verlauf der Geschichte an Bedeutung.

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.
- Zunächst versuchte Arthur Scherbius seine Erfindung der Kaiserlichen Marine zu verkaufen, diese winkte aber ab.
- Die erste Enigma (Enigma-A / 1923) wurde kommerziell vermarktet.
- Militärisch gewann die Enigma erst im späteren Verlauf der Geschichte an Bedeutung.
    - Im Jahr 1926 wurde die Enigma zunächst von der Reichsmarine, zwei Jahre später auch vom Heer versuchsweise eingesetzt.

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.
- Zunächst versuchte Arthur Scherbius seine Erfindung der Kaiserlichen Marine zu verkaufen, diese winkte aber ab.
- Die erste Enigma (Enigma-A / 1923) wurde kommerziell vermarktet.
- Militärisch gewann die Enigma erst im späteren Verlauf der Geschichte an Bedeutung.
    - Im Jahr 1926 wurde die Enigma zunächst von der Reichsmarine, zwei Jahre später auch vom Heer versuchsweise eingesetzt.
    - Mit der Machtübernahme der Nationalsozialisten, stand dem Erfolg der Enigma nun nichts mehr im Wege.

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.
- Zunächst versuchte Arthur Scherbius seine Erfindung der Kaiserlichen Marine zu verkaufen, diese winkte aber ab.
- Die erste Enigma (Enigma-A / 1923) wurde kommerziell vermarktet.
- Militärisch gewann die Enigma erst im späteren Verlauf der Geschichte an Bedeutung.
    - Im Jahr 1926 wurde die Enigma zunächst von der Reichsmarine, zwei Jahre später auch vom Heer versuchsweise eingesetzt.
    - Mit der Machtübernahme der Nationalsozialisten, stand dem Erfolg der Enigma nun nichts mehr im Wege.
- Nahezu der gesamte Funkverkehr der Nazis wurde mit der Enigma verschlüsselt.

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.
- Zunächst versuchte Arthur Scherbius seine Erfindung der Kaiserlichen Marine zu verkaufen, diese winkte aber ab.
- Die erste Enigma (Enigma-A / 1923) wurde kommerziell vermarktet.
- Militärisch gewann die Enigma erst im späteren Verlauf der Geschichte an Bedeutung.
    - Im Jahr 1926 wurde die Enigma zunächst von der Reichsmarine, zwei Jahre später auch vom Heer versuchsweise eingesetzt.
    - Mit der Machtübernahme der Nationalsozialisten, stand dem Erfolg der Enigma nun nichts mehr im Wege.
- Nahezu der gesamte Funkverkehr der Nazis wurde mit der Enigma verschlüsselt.
- Es wird geschätzt, dass etwas mehr als 40.000 Maschinen hergestellt wurden.

Geschichte der Enigma

- Erfunden von Arthur Scherbius und im Jahr 1918 patentiert.
- Zunächst versuchte Arthur Scherbius seine Erfindung der Kaiserlichen Marine zu verkaufen, diese winkte aber ab.
- Die erste Enigma (Enigma-A / 1923) wurde kommerziell vermarktet.
- Militärisch gewann die Enigma erst im späteren Verlauf der Geschichte an Bedeutung.
    - Im Jahr 1926 wurde die Enigma zunächst von der Reichsmarine, zwei Jahre später auch vom Heer versuchsweise eingesetzt.
    - Mit der Machtübernahme der Nationalsozialisten, stand dem Erfolg der Enigma nun nichts mehr im Wege.
- Nahezu der gesamte Funkverkehr der Nazis wurde mit der Enigma verschlüsselt.
- Es wird geschätzt, dass etwas mehr als 40.000 Maschinen hergestellt wurden.
- Galt bis zum Ende des zweiten Weltkrieges als unknackbar auf deutscher Seite.

Aufbau der Enigma

Aufbau der Enigma

Aufbau der Enigma

- Die unterschiedlichen Modelle
- Die Enigma I
- Tastenfeld
- Steckerbrett
- Walzensatz
- Lampenfeld

Die unterschiedlichen Modelle

- Enigma A
- Enigma I (Heer / Luftwaffe)
- Enigma M1-M4 (Kriegsmarine)
- Enigma G (Abwehr bzw. Geheimdienst)
- Enigma T (Kommunikation zwischen Deutschland und Japan)
- Enigma Z (zur Verschlüsselung von Zahlen)

Im weiteren Verlauf der Präsentation beziehen sich meine Angaben auf die Enigma I in der Version mit 3 aus 5 Walzen, der Umkehrwalze B und 20 gesteckerten Buchstaben am Steckerbrett.

Die Enigma I

Figure 2: Enigma I

Tastenfeld

- Besteht aus 26 Tasten die eine Abbildung der 26 Großbuchstaben des lateinischen Alphabets sind.

Tastenfeld

- Besteht aus 26 Tasten die eine Abbildung der 26 Großbuchstaben des lateinischen Alphabets sind.
- Durch das Drücken wird ein elektrischer Stromkreis geschlossen und dadurch wird der gedrückte Buchstabe verschlüsselt.

Tastenfeld

- Besteht aus 26 Tasten die eine Abbildung der 26 Großbuchstaben des lateinischen Alphabets sind.
- Durch das Drücken wird ein elektrischer Stromkreis geschlossen und dadurch wird der gedrückte Buchstabe verschlüsselt.
- Durch den Tastendruck wird ein ”tachoartiges” Drehen der Walzen verursacht.

Steckerbrett

Figure 3: Steckerbrett mit 10 Steckerverbindungen

Steckerbrett

- An der Gerätefront ist das Steckerbrett mit doppelpoligen Steckbuchsen für jeden der 26 Buchstaben angebracht.

Steckerbrett

- An der Gerätefront ist das Steckerbrett mit doppelpoligen Steckbuchsen für jeden der 26 Buchstaben angebracht.
- Durch das Anstecken des doppelpoligen Kabels werden zwei Buchstaben miteinander vertauscht.

Steckerbrett

- An der Gerätefront ist das Steckerbrett mit doppelpoligen Steckbuchsen für jeden der 26 Buchstaben angebracht.
- Durch das Anstecken des doppelpoligen Kabels werden zwei Buchstaben miteinander vertauscht.
- Insgesamt wurden so 20 Buchstaben (10 Verbindungen) paarweise vertauscht.

Steckerbrett

- An der Gerätefront ist das Steckerbrett mit doppelpoligen Steckbuchsen für jeden der 26 Buchstaben angebracht.
- Durch das Anstecken des doppelpoligen Kabels werden zwei Buchstaben miteinander vertauscht.
- Insgesamt wurden so 20 Buchstaben (10 Verbindungen) paarweise vertauscht.
- Der Strom von der Buchstabentaste wird, bevor er die Eintrittswalze erreicht, über dieses Steckerbrett geführt. Nach Durchlaufen des Walzensatzes fließt er ein zweites Mal über das Steckerbrett und bringt schließlich eine der 26 Buchstabenlampen zum Aufleuchten.

Walzensatz

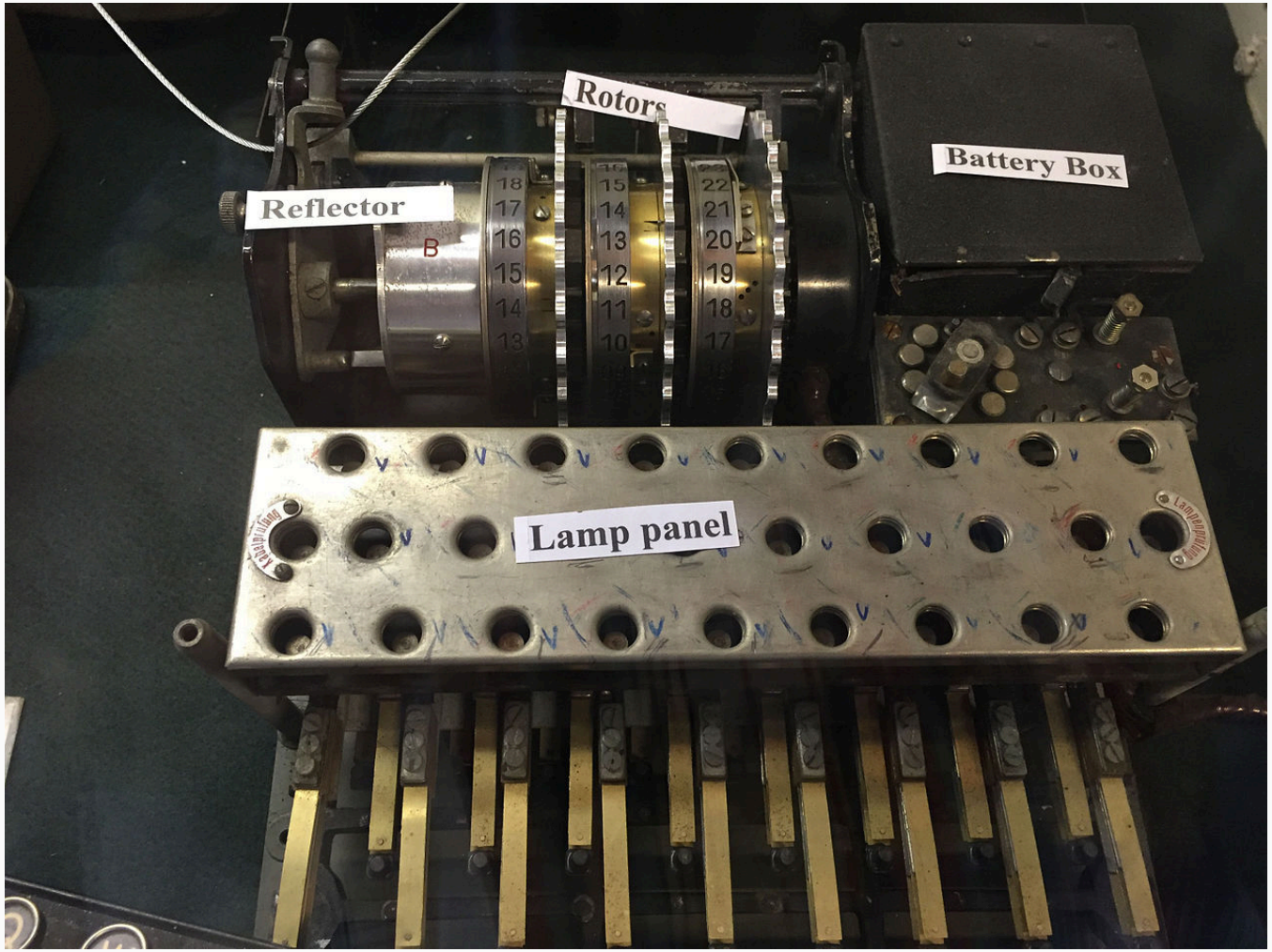


Figure 4: Walzensatz im inneren einer Enigma

Walzensatz

Figure 5: Ausgebauter Walzensatz

Walzensatz

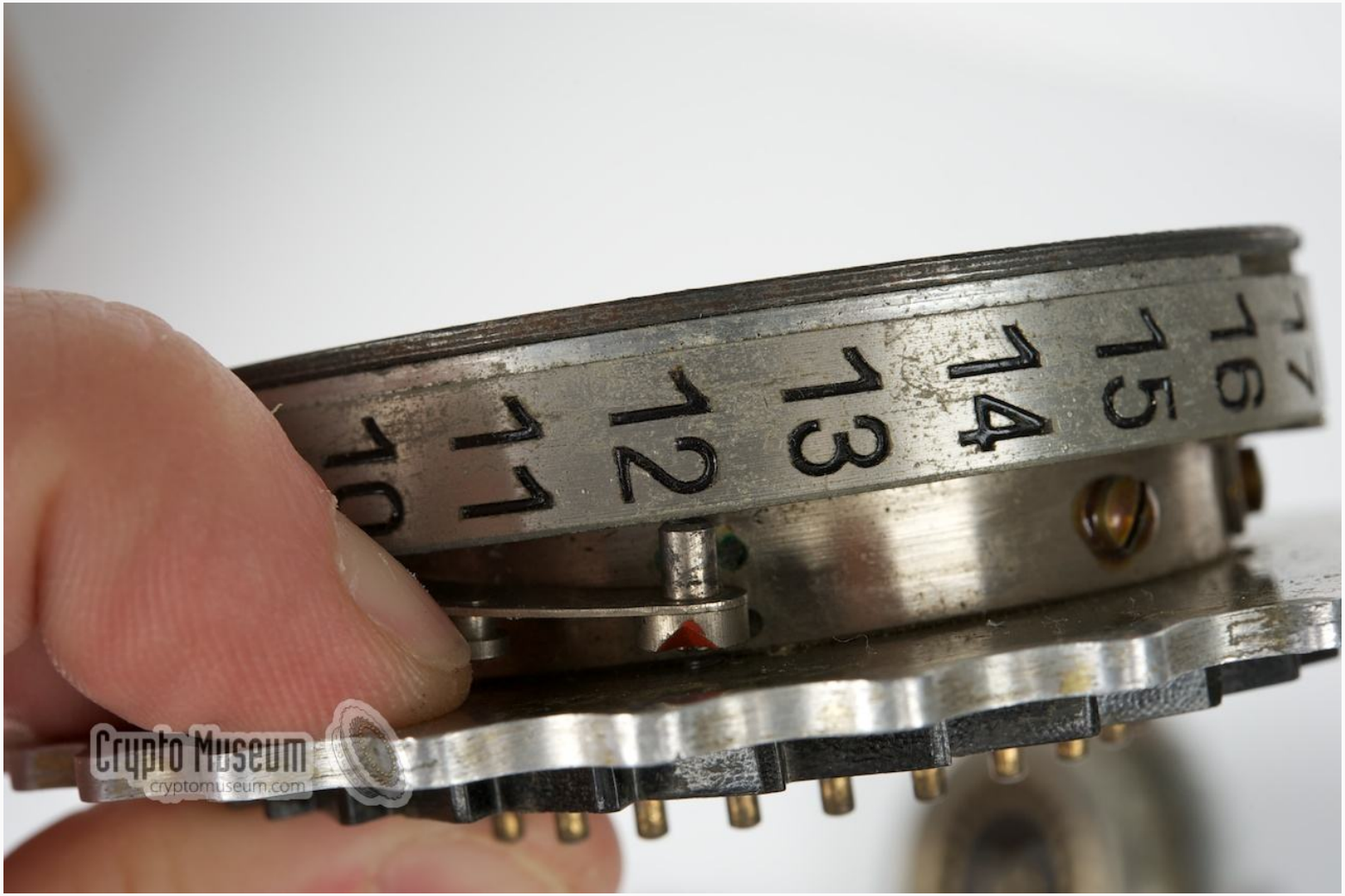


Figure 6: Seitenansicht einer Walze mit Markierung für die Ringstellung

Walzensatz

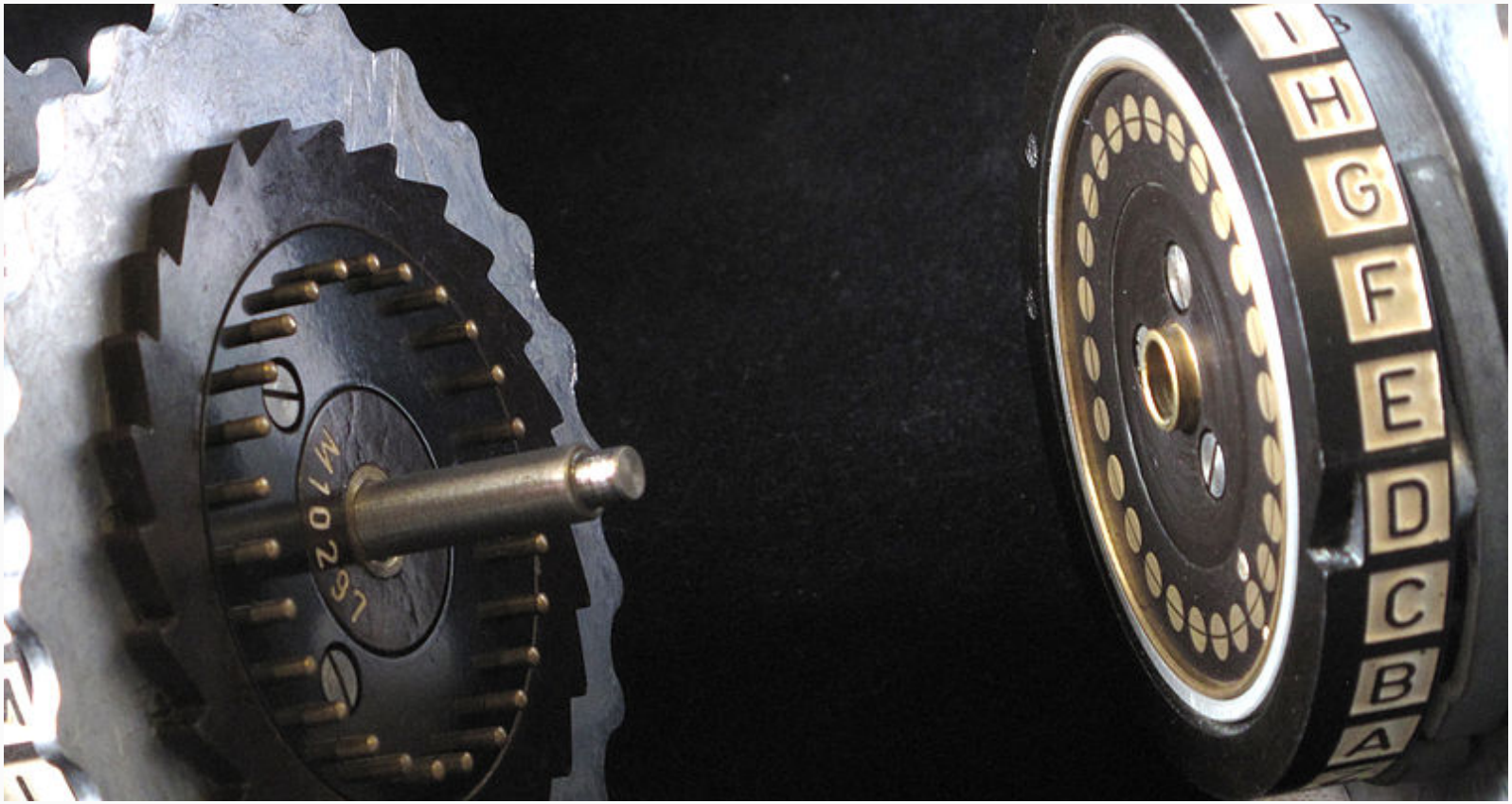


Figure 7: Walzen mit Übertragskerbe

Walzensatz

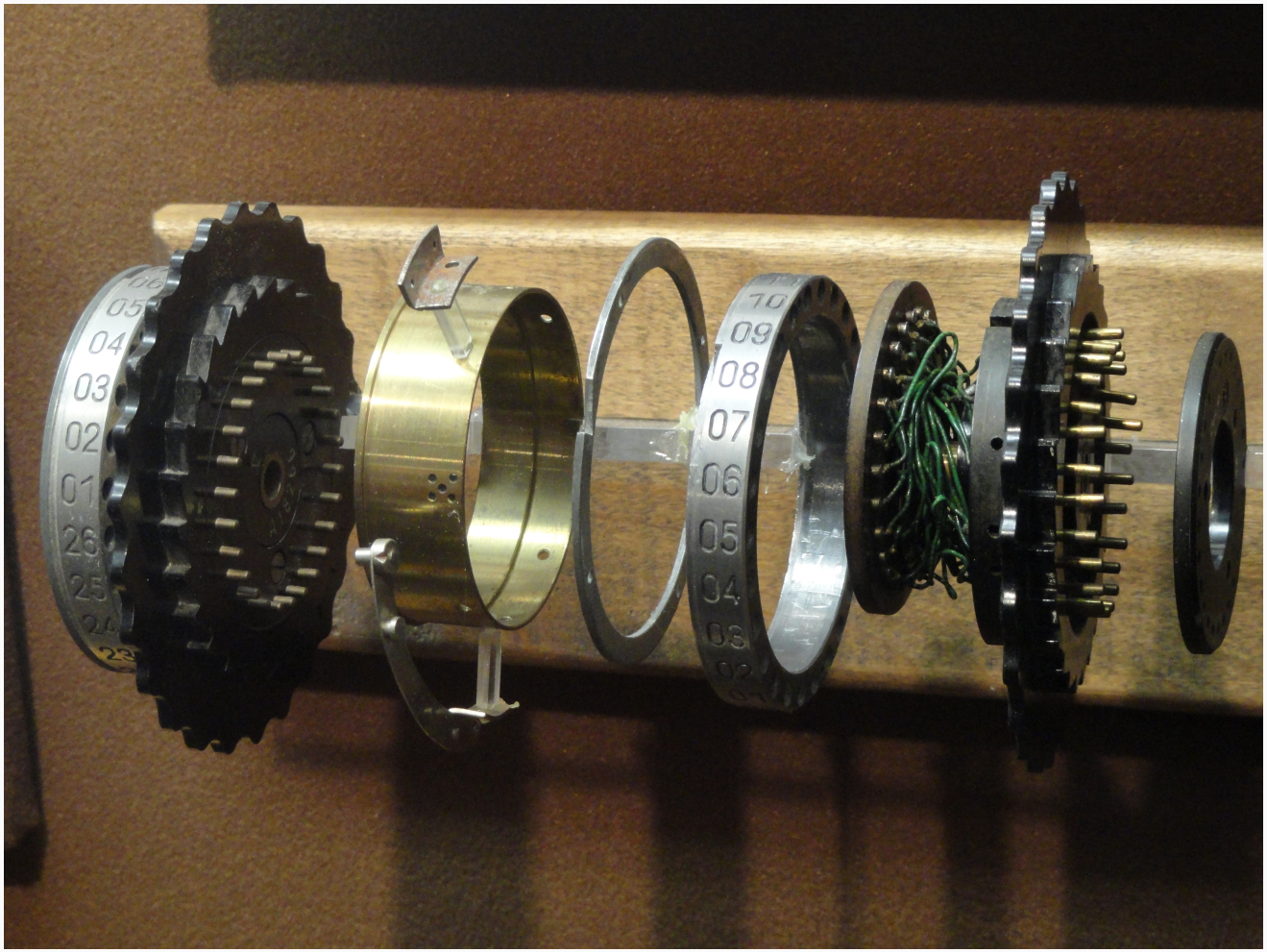


Figure 8: Innenleben einer Walze

Walzensatz 1

- Der Walzensatz ist das Herzstück der Verschlüsselung.

Walzensatz 1

- Der Walzensatz ist das Herzstück der Verschlüsselung.
- Die Enigma I hatte bis zu fünf Walzen zur Auswahl, von denen man 3 in verschiedenster Reihenfolge in die Enigma einsetzen kann.

Walzensatz 1

- Der Walzensatz ist das Herzstück der Verschlüsselung.
- Die Enigma I hatte bis zu fünf Walzen zur Auswahl, von denen man 3 in verschiedenster Reihenfolge in die Enigma einsetzen kann.
- Jede Walze hat auf beiden Seiten 26 Kontakte die miteinander verkabelt sind.

Walzensatz 1

- Der Walzensatz ist das Herzstück der Verschlüsselung.
- Die Enigma I hatte bis zu fünf Walzen zur Auswahl, von denen man 3 in verschiedenster Reihenfolge in die Enigma einsetzen kann.
- Jede Walze hat auf beiden Seiten 26 Kontakte die miteinander verkabelt sind.
- Somit stellt jede Walze eine Permutation des Alphabets dar.

Walzensatz 1

- Der Walzensatz ist das Herzstück der Verschlüsselung.
- Die Enigma I hatte bis zu fünf Walzen zur Auswahl, von denen man 3 in verschiedenster Reihenfolge in die Enigma einsetzen kann.
- Jede Walze hat auf beiden Seiten 26 Kontakte die miteinander verkabelt sind.
- Somit stellt jede Walze eine Permutation des Alphabets dar.
- Der Strom wird vom Steckerbrett über die Eintrittswalze in den Walzensatz geleitet.

Walzensatz 2

- Nachdem der Strom die drei Walzen durchlaufen hat, wird er über die Umkehrwalze (meist UKW B) wieder zurück durch die drei Walzen geleitet und tritt dann von der Eintrittswalze wieder in das Steckerbrett ein.

Walzensatz 2

- Nachdem der Strom die drei Walzen durchlaufen hat, wird er über die Umkehrwalze (meist UKW B) wieder zurück durch die drei Walzen geleitet und tritt dann von der Eintrittswalze wieder in das Steckerbrett ein.
- Bei jedem Tastendruck drehen sich die Walzen wie das Tacho eines Autos um eine Position weiter.

Walzensatz 2

- Nachdem der Strom die drei Walzen durchlaufen hat, wird er über die Umkehrwalze (meist UKW B) wieder zurück durch die drei Walzen geleitet und tritt dann von der Eintrittswalze wieder in das Steckerbrett ein.
- Bei jedem Tastendruck drehen sich die Walzen wie das Tacho eines Autos um eine Position weiter.
- Jede Walze hat eine Ringstellung die den Versatz zwischen der inneren Verdrahtung der Walzen und dem Buchstaben bestimmt, zu dem der Übertrag auf die nächste Walze erfolgt.

Walzensatz 2

- Nachdem der Strom die drei Walzen durchlaufen hat, wird er über die Umkehrwalze (meist UKW B) wieder zurück durch die drei Walzen geleitet und tritt dann von der Eintrittswalze wieder in das Steckerbrett ein.
- Bei jedem Tastendruck drehen sich die Walzen wie das Tacho eines Autos um eine Position weiter.
- Jede Walze hat eine Ringstellung die den Versatz zwischen der inneren Verdrahtung der Walzen und dem Buchstaben bestimmt, zu dem der Übertrag auf die nächste Walze erfolgt.
    - Auf jedem Ring befindet sich eine Kerbe die den Übertrag einer links gelegenen Walze bewirkt.

Walzensatz 2

- Nachdem der Strom die drei Walzen durchlaufen hat, wird er über die Umkehrwalze (meist UKW B) wieder zurück durch die drei Walzen geleitet und tritt dann von der Eintrittswalze wieder in das Steckerbrett ein.
- Bei jedem Tastendruck drehen sich die Walzen wie das Tacho eines Autos um eine Position weiter.
- Jede Walze hat eine Ringstellung die den Versatz zwischen der inneren Verdrahtung der Walzen und dem Buchstaben bestimmt, zu dem der Übertrag auf die nächste Walze erfolgt.
    - Auf jedem Ring befindet sich eine Kerbe die den Übertrag einer links gelegenen Walze bewirkt.
    - Die Ringstellung wurde zusätzlich als Schutz vor Spionage verwendet.

Walzensatz 2

- Nachdem der Strom die drei Walzen durchlaufen hat, wird er über die Umkehrwalze (meist UKW B) wieder zurück durch die drei Walzen geleitet und tritt dann von der Eintrittswalze wieder in das Steckerbrett ein.
- Bei jedem Tastendruck drehen sich die Walzen wie das Tacho eines Autos um eine Position weiter.
- Jede Walze hat eine Ringstellung die den Versatz zwischen der inneren Verdrahtung der Walzen und dem Buchstaben bestimmt, zu dem der Übertrag auf die nächste Walze erfolgt.
    - Auf jedem Ring befindet sich eine Kerbe die den Übertrag einer links gelegenen Walze bewirkt.
    - Die Ringstellung wurde zusätzlich als Schutz vor Spionage verwendet.
- Nach jeder Verschlüsselung bzw. Entschlüsselung einer Nachricht wurden die Walzen wieder in ihre Anfangsstellung zurückgedreht.

Walzensatz 3

Verdrahtung der Walzen I bis VI

```
Eingang = ABCDEFGHIJKLMNOPQRSTUVWXYZ
Walze 1 = EKMFLGDQVZNTOWYHXUSPAIBRCJ
Walze 2 = AJDKSIRUXBLHWTMCQGZNPYFVOE
Walze 3 = BDFHJLCPRTXVZNYEIWGAKMUSQO
Walze 4 = ESOVPZJAYQUIRHXLNFTGKDCMWB
Walze 5 = VZBRGITYUPSDNHLXAWMJQOFECK
```

Verdrahtung der Umkehrwalze B

```
Eing. = ABCDEFGHIJKLMNOPQRSTUVWXYZ
UKW B = YRUHQSLDPXNGOKMIEBFZCWVJAT
```

ACHTUNG: Diese Angaben sind relativ und hängen von der Position (der Verdrehung bzw. der Grundstellung) der Walze in der Maschine sowie von deren Ringstellung ab!

Walzensatz 4

Royal Flags Wave Kings Above - Die Übertragskerben

Walze	*Übertragskerbe*	*Fenster*	*Weiterdrehen des linken Rotors*
1	*Y*	*Q*	$Q \rightarrow R$
2	*M*	*E*	$E \rightarrow F$
3	*D*	*V*	$V \rightarrow W$
4	*R*	*J*	$J \rightarrow K$
5	*H*	*Z*	$Z \rightarrow A$

Lampenfeld

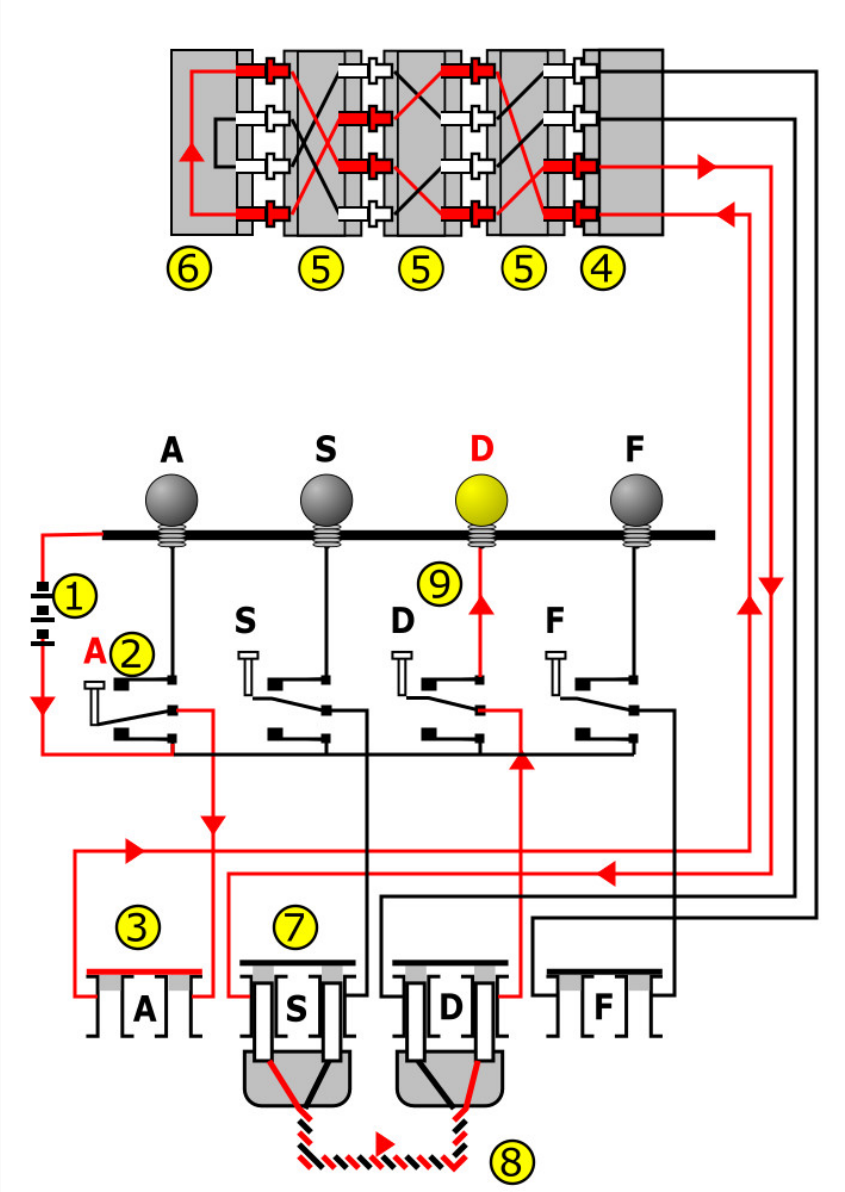
Figure 9: Lampenfeld direkt über der Tastatur

Lampenfeld

- Der Strom der aus dem Steckerbrett austritt, gelangt schlussendlich in das Leuchtfeld und einer der 26 Buchstaben leuchtet auf. Dieser Buchstabe ist dann der kodierte bzw. enkodierte Buchstabe.

Kleines Beispiel

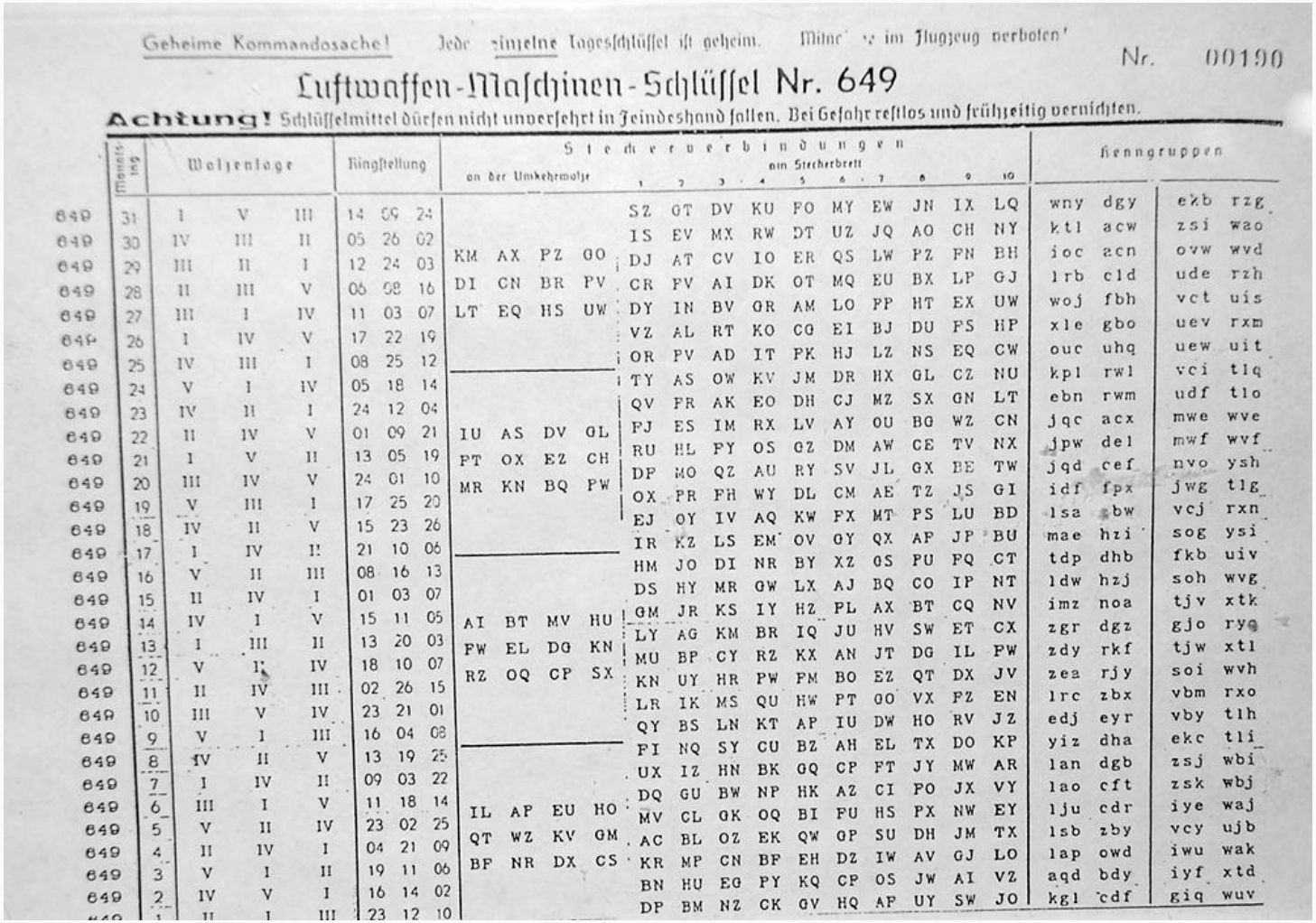
Kleines Beispiel



1. Batterie
2. Tastatur
3. Steckerbrett
4. Eintrittswalze
5. Walzensatz
6. Umkehrwalze
7. Steckerbrett
8. Steckkabel
9. Lampenfeld

Figure 10: Beispiel entnommen von www.wikipedia.com

Kleines Beispiel



Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

	Monats-tag	Walzenlage			Ringstellung			Steckerverbindungen an der Umkehrwalze	Steckerverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen	
649	31	I	V	III	14	09	24		SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny dgy	ekb rzg
649	30	IV	III	II	05	26	02		IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl acw	zsi wao
649	29	III	II	I	12	24	03	KM AX PZ GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc acn	ovw wvd
649	28	II	III	V	06	08	16	DI CN BR PV	CR	PV	AI	DK	OT	MQ	EU	BX	LP	GJ	lrb cld	ude rzh
649	27	III	I	IV	11	03	07	LT EQ HS UW	DY	IN	BV	GR	AM	LO	FP	HT	EX	UW	woj fbh	vct uis
649	26	I	IV	V	17	22	19		VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle gbo	uev rxm
649	25	IV	III	I	08	25	12		OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc uhq	uew uit
649	24	V	I	IV	05	18	14		TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl rwl	vci tlq
649	23	IV	II	I	24	12	04		QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn rwm	udf tlo
649	22	II	IV	V	01	09	21	IU AS DV GL	PJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jqc acx	mwe wve
649	21	I	V	II	13	05	19	PT OX EZ CH	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpw del	mwf wvf
649	20	III	IV	V	24	01	10	MR KN BQ PW	DP	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd cef	nvo ysh
649	19	V	III	I	17	25	20		OX	PR	FH	WY	DL	CM	AE	TZ	JS	GI	idf fpx	jwg tlg
649	18	IV	II	V	15	23	26		EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa cbw	vcj rxn
649	17	I	IV	II	21	10	06		IR	KZ	LS	EM	OV	GY	QX	AP	JP	BU	mae hzi	sog ysi
649	16	V	II	III	08	16	13		HM	JO	DI	NR	BY	XZ	GS	PU	FQ	CT	tdp dhb	fkb uiv
649	15	II	IV	I	01	03	07		DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	ldw hzj	soh wvg
649	14	IV	I	V	15	11	05	AI BT MV HU	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz noa	tjv xtk
649	13	I	III	II	13	20	03	FW EL DG KN	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr dgz	gjo ryq
649	12	V	II	IV	18	10	07	RZ OQ CP SX	MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW	zdy rkf	tjw xtl
649	11	II	IV	III	02	26	15		KN	UY	HR	PW	FM	BO	EZ	QT	DX	JV	zea rjy	soi wvh
649	10	III	V	IV	23	21	01		LR	IK	MS	QU	HW	PT	GO	VX	FZ	EN	lrc zbx	vbm rxo
649	9	V	I	III	16	04	08		QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj eyr	vby tlh
649	8	IV	II	V	13	19	25		FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz dha	ekc tli
649	7	I	IV	II	09	03	22		UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	lan dgb	zsj wbi
649	6	III	I	V	11	18	14	IL AP EU HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao cft	zsk wbj
649	5	V	II	IV	23	02	25	QT WZ KV GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lju cdr	iye waj
649	4	II	IV	I	04	21	09	BF NR DX CS	AC	BL	OZ	EK	QW	GP	SU	DH	JM	TX	lsb zby	vcy ujb
649	3	V	I	II	19	11	06		KR	MP	CN	BF	EH	DZ	IW	AV	GJ	LO	lap owd	iwu wak
649	2	IV	V	I	16	14	02		BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd bdy	iyf xtd
649	1	II	I	III	23	12	10		DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO	kgl cdf	giq wuv

Figure 11: Schlüsseltafel

Kryptographische Stärke

Kryptographische Stärke

- Kryptographische Stärke
  - Kryptographisch seiner Zeit voraus
  - Schlüsselraum
  - 150 Millionen Millionen Millionen

Kryptographisch seiner Zeit voraus

- Die kryptographische Stärke ist durch den rotierenden Walzensatz gegeben.

Kryptographisch seiner Zeit voraus

- Die kryptographische Stärke ist durch den rotierenden Walzensatz gegeben.
- Durch die Drehung der Walzen wird eine polyalphabetische Verschlüsselung erreicht.

Kryptographisch seiner Zeit voraus

- Die kryptographische Stärke ist durch den rotierenden Walzensatz gegeben.
- Durch die Drehung der Walzen wird eine polyalphabetische Verschlüsselung erreicht.

  $\Rightarrow$ Mit jeder Drehung wird jeder Buchstabe mit einem neuen Alphabet verschlüsselt. OTTO $\rightarrow$ PWMC

Kryptographisch seiner Zeit voraus

- Die kryptographische Stärke ist durch den rotierenden Walzensatz gegeben.
- Durch die Drehung der Walzen wird eine polyalphabetische Verschlüsselung erreicht.
  - $\Rightarrow$ Mit jeder Drehung wird jeder Buchstabe mit einem neuen Alphabet verschlüsselt. OTTO $\rightarrow$ PWMC
  - $\Rightarrow$ Unangreifbar durch linguistische Entschlüsselungsverfahren bzw. Analysen.

Kryptographisch seiner Zeit voraus

- Die kryptographische Stärke ist durch den rotierenden Walzensatz gegeben.
- Durch die Drehung der Walzen wird eine polyalphabetische Verschlüsselung erreicht.
  - $\Rightarrow$ Mit jeder Drehung wird jeder Buchstabe mit einem neuen Alphabet verschlüsselt. OTTO $\rightarrow$ PWMC
  - $\Rightarrow$ Unangreifbar durch linguistische Entschlüsselungsverfahren bzw. Analysen.
- Die Enigma konnte mit der gleichen Einstellung Texte entschlüsseln. PWMC $\rightarrow$ OTTO

Kryptographisch seiner Zeit voraus

- Die kryptographische Stärke ist durch den rotierenden Walzensatz gegeben.
- Durch die Drehung der Walzen wird eine polyalphabetische Verschlüsselung erreicht.
  - $\Rightarrow$ Mit jeder Drehung wird jeder Buchstabe mit einem neuen Alphabet verschlüsselt. OTTO $\rightarrow$ PWMC
  - $\Rightarrow$ Unangreifbar durch linguistische Entschlüsselungsverfahren bzw. Analysen.
- Die Enigma konnte mit der gleichen Einstellung Texte entschlüsseln. PWMC $\rightarrow$ OTTO
- Für heutige Verhältnisse, eine immer noch sehr starke Verschlüsselung mit einer Schlüssellänge von ungefähr 76 bit.

Schlüsselraum - Definitionen

Schlüsselraum - Definitionen

Definition - Schüsselraum

Der Schlüsselraum bezeichnet die Menge N aller für ein Verschlüsselungsverfahren möglichen Schlüssel.

Schlüsselraum - Definitionen

Definition - Schüsselraum

Der Schlüsselraum bezeichnet die Menge N aller für ein Verschlüsselungsverfahren möglichen Schlüssel.

Definition - Schlüssellänge in Bit

$$Schlüssellänge = log_2(|N|)$$

Schlüsselraum

Der Schlüsselraum lässt sich aus dem Produkt folgender Punkte berechnen:

Enigma Schlüsselraum:

Anzahl aller möglichen Walzenanordnungen $*$
Anzahl aller möglichen Ringstellungen $*$
Anzahl aller möglichen Walzenstellungen $*$
Anzahl aller möglichen Steckerbrett – Verbindungen

Schlüsselraum - Anzahl aller möglichen Walzenanordnungen

3 aus 5 Walzen

Schlüsselraum - Anzahl aller möglichen Walzenanordnungen

3 aus 5 Walzen

$\Rightarrow$ Variation ohne Wiederholung

Schlüsselraum - Anzahl aller möglichen Walzenanordnungen

3 aus 5 Walzen

$\Rightarrow$ Variation ohne Wiederholung

Anzahl der möglichen Walzenanordnungen

$$V_k^n = \frac{n!}{(n-k)!} = 3 * 4 * 5 = 60$$

Schlüsselraum - Anzahl aller möglichen Ringstellungen

26 Ringstellungen für jede Walzen

Schlüsselraum - Anzahl aller möglichen Ringstellungen

26 Ringstellungen für jede Walzen

$\Rightarrow$ Variation mit Wiederholung

Schlüsselraum - Anzahl aller möglichen Ringstellungen

26 Ringstellungen für jede Walzen

$\Rightarrow$ Variation mit Wiederholung

Anzahl der möglichen Ringstellungen

$$^{r}V_{k}^{n} = n^{k} = 26^{3} = 17.576$$

Schlüsselraum - Anzahl aller möglichen Ringstellungen

26 Ringstellungen für jede Walzen
$\Rightarrow$ Variation mit Wiederholung

Anzahl der möglichen Ringstellungen

$$^{r}V_{k}^{n} = n^{k} = 26^{3} = 17.576$$

Der Ring der linken Walze ist kryptographisch bedeutungslos, da ihre Übertragskerbe kein Fortschalten einer noch weiter links befindlichen Walze bewirkt.

Schlüsselraum - Anzahl aller möglichen Ringstellungen

26 Ringstellungen für jede Walzen
$\Rightarrow$ Variation mit Wiederholung

Anzahl der möglichen Ringstellungen

$$^{r}V_{k}^{n} = n^{k} = 26^{3} = 17.576$$

Der Ring der linken Walze ist kryptographisch bedeutungslos, da ihre Übertragskerbe kein Fortschalten einer noch weiter links befindlichen Walze bewirkt.

Korrigierte Anzahl der möglichen Ringstellungen

$$^{r}V_{k}^{n} = n^{k} = 26^{2} = 676$$

Schlüsselraum - Anzahl aller möglichen Walzenstellungen

26 Walzenstellungen für jede Walzen

Schlüsselraum - Anzahl aller möglichen Walzenstellungen

26 Walzenstellungen für jede Walzen

$\Rightarrow$ Variation mit Wiederholung

Schlüsselraum - Anzahl aller möglichen Walzenstellungen

26 Walzenstellungen für jede Walzen

$\Rightarrow$ Variation mit Wiederholung

Anzahl der möglichen Walzenstellungen

$$^{r}V_{k}^{n} = n^{k} = 26^{3} = 17.576$$

Schlüsselraum - Anzahl aller möglichen Walzenstellungen

26 Walzenstellungen für jede Walzen
$\Rightarrow$ Variation mit Wiederholung

Anzahl der möglichen Walzenstellungen

$$^{r}V_{k}^{n} = n^{k} = 26^{3} = 17.576$$

Es gibt eine Anomalie beim Fortschaltmechanismus der linken Walze die den Schlüsselraum der Walzenstellung auf $26 * 25 * 26 = 16.900$ reduziert, **vorausgesetzt** die Ringstellungen sind bekannt.

Beispiel einer Anomalie

Mit den Walzen 1, 2, 3 und den jeweiligen Ringstellungen 01.

$$ADU \rightarrow ADV \rightarrow AEW \rightarrow BFX \rightarrow BFY$$

Schlüsselraum - Anzahl aller mögl. Steckerbrett - Verbindungen

Es werden 10 Steckerverbindungen zwischen den 26 Buchstaben hergestellt.

Schlüsselraum - Anzahl aller mögl. Steckerbrett - Verbindungen

Es werden 10 Steckerverbindungen zwischen den 26 Buchstaben hergestellt.

Anzahl der möglichen Steckkombinationen, n=10

$$\frac{1}{n!} \prod_{i=1}^{n} \frac{(26-2i+2)(26-2i+1)}{2} =$$

Schlüsselraum - Anzahl aller mögl. Steckerbrett - Verbindungen

Es werden 10 Steckerverbindungen zwischen den 26 Buchstaben hergestellt.

Anzahl der möglichen Steckkombinationen, n=10

$$\frac{1}{n!}\prod_{i=1}^{n}\frac{(26-2i+2)(26-2i+1)}{2} = 150.738.274.937.250$$

Schlüsselraum

Enigma Schlüsselraum:

$60 * 676 * 17.576 * 150.738.274.937.250 = 107.458.687.327.250.619.360.000$

Das sind ausgesprochen Hundertundsieben Trilliarden.

Schlüsselraum

Enigma Schlüsselraum:

$60 * 676 * 17.576 * 150.738.274.937.250 = 107.458.687.327.250.619.360.000$

Das sind ausgesprochen Hundertundsieben Trilliarden.

Enigma Schlüssellänge:

$Schlüssellänge \approx 76Bit$

150 Millionen Millionen Millionen

Die gelegentlich zu hörenden „150 Millionen Millionen Millionen“ Kombinationen, beispielsweise in den Spielfilmen „Enigma – Das Geheimnis“ und „The Imitation Game – Ein streng geheimes Leben“, basieren auf dem Weglassen der Ringstellungen. Die genaue Rechnung ergibt in diesem Fall:

150 Millionen Millionen Millionen

Die gelegentlich zu hörenden „150 Millionen Millionen Millionen“ Kombinationen, beispielsweise in den Spielfilmen „Enigma – Das Geheimnis“ und „The Imitation Game – Ein streng geheimes Leben“, basieren auf dem Weglassen der Ringstellungen. Die genaue Rechnung ergibt in diesem Fall:

Hollywood-Schlüsselraum:

$$60 * 17.576 * 150.738.274.937.250 = 158.962.555.217.826.360.000$$

Kryptographische Schwächen

Kryptographische Schwächen

Kryptographische Schwächen

- Involutorische Permutationen
- Die Methode des Wahrscheinlichen Worts

Was bedeutet Involution?

Definition:

Eine Abbildung $f : A \to A$ mit übereinstimmender Definitions- und Zielmenge A heißt genau dann eine Involution, wenn für alle $x \in A$ gilt: $f(f(x)) = x$.

Involutorische Permutationen

Permutationen von ABCD

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

Involutorische Permutationen

Permutationen von ABCD

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

Involutorische Permutationen

Permutationen von ABCD

----	----	----	----	----	----
----	BADC	----	BCDA	BDAC	----
----	CADB	----	----	CDAB	CDBA
DABC	----	----	----	DCAB	DCBA

Involutorische Permutationen

Permutationen von ABCD

----	----	----	----	----	----
----	BADC	----	BCDA	BDAC	----
----	CADB	----	----	CDAB	CDBA
DABC	----	----	----	DCAB	DCBA

Involutorische Permutationen

Permutationen von ABCD

```
----  ----  ----  ----  ----  ----
----  BADC  ----  ----  ----  ----
----  ----  ----  ----  CDAB  ----
----  ----  ----  ----  ----  DCBA
```

Involutorische Permutationen

Bei einem Alphabet mit den vier Buchstaben {A,B,C,D}, hat man mit jedem Tastendruck eine der drei involutorischen Permutationen für die Verschlüsselung zur Verfügung.

Involutorische Permutationen

Eine involutorische Permutation von ABCD

$$f(ABCD) = (BADC)$$

Beweis

Fall 1 $f(A) = B$ *und* $f(B) = A$, *oder* $f(f(A)) = A$

Fall 2 $f(B) = A$ *und* $f(A) = B$, *oder* $f(f(B)) = B$

Fall 3 $f(C) = D$ *und* $f(D) = C$, *oder* $f(f(C)) = C$

Fall 4 $f(D) = C$ *und* $f(C) = D$, *oder* $f(f(D)) = D$

Involutorische Permutationen

Bei der Enigma mit ihren 26 Buchstaben bewirkt diese Beschränkung, dass statt der 26! (ungefähr $4 * 10^{26}$) insgesamt möglichen permutierten Alphabete lediglich 25!! (etwa $8 * 10^{12}$) echt involutorisch permutierten Alphabete genutzt werden können.

Durch die Umkehrwalze verschenkt man so den Faktor von etwa $5 * 10^{13}$ an Möglichkeiten – eine gigantische Schwächung der kombinatorischen Komplexität der Maschine.

Definition Doppelfakultät

$$n!! = \begin{cases} n * (n-2) * (n-4) * \ldots * 2 & \text{für } n \text{ gerade und } n > 0, \\ n * (n-2) * (n-4) * \ldots * 1 & \text{für } n \text{ ungerade und } n > 0, \\ 1 & \text{für } n \in \{-1, 0\} \end{cases}$$

Involutorische Permutationen

Figure 12: Marian Rejewski

Mit diesem Wissen und zahlreichen Analysen abgefangener deutscher Nachrichten gelang es dem Polen Marian Rejewski und seinem Team die Enigma nicht nur zu knacken sondern auch die geheime Verdrahtung der Walzen herauszufinden. Während die Briten und Franzosen die Enigma noch als unknackbar einstuften.

Enigma-Gleichung

$$c_i = R_z(p_i) = (S \circ W_z \circ U \circ W_z^{-1} \circ S^{-1})(p_i)$$

Rejewskis Team hatte zudem den Vorläufer der Touringbombe gebaut, die Bomba.

Die Methode des Wahrscheinlichen Worts

Ein seit Jahrhunderten bekanntes und bewährtes Entzifferungsverfahren ist die „Methode des Wahrscheinlichen Worts“. Hierbei errät, vermutet oder weiß der Angreifer, dass im Text eine bestimmte Phrase (englisch Crib) auftritt, beispielsweise „FUEHRER“.

Die Methode des Wahrscheinlichen Worts

```
   XAEMYAEBHRIG
1  FUEHRER
2   FUEHRER
3    FUEHRER
4     FUEHRER
5      FUEHRER
6       FUEHRER
   XAEMYAEBHRIG
```

Die Methode des Wahrscheinlichen Worts

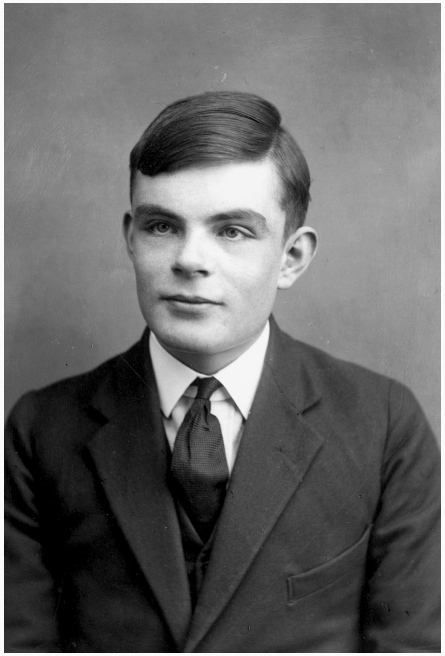


Figure 13: Alan Turing

Das britische Dechiffrierteam rund um Alan Turing baute im geheimen Bletchley Park die sogenannte Turing Bombe. Die Turing Bombe benötigte zum Knacken des jeweiligen Tagesschlüssels ein Crib. Meistens nutzten sie den täglichen Wetterbericht der Nazis. Es wurden auch Vorfälle hervorgerufen um Funknachrichten mit speziellen Cribs zu provozieren.

Crib Beispiele:

OBERKOMMANDODERWEHRMACHT, WETTERVORHERSAGE

Die Enigma in der heutigen Zeit

Die Enigma in der heutigen Zeit

Obwohl die Enigma aus heutiger Sicht veraltet wirkt, ist ihre kryptographische Stärke nicht zu unterschätzen. Das M4 Message Breaking Project benötigte 2006 für das Entschlüsseln von 2 aus 3 mit der Enigma M4 verschlüsselten original Nachrichten des U-Bootes U264 mehrere Tausend vernetzte Computer und ungefähr einen Monat. 2013 gelang es schließlich die dritte Nachricht zu entschlüsseln. Dies zeigt eindrucksvoll, dass die Enigma auch mit modernen kryptanalytischen Angriffsmethoden und der heutigen weit fortentwickelten Rechnertechnik nicht einfach zu knacken ist, sondern noch immer eine harte Nuss darstellt.

Time to say goodbye

Time to say goodbye

Vielen Dank für Ihre Aufmerksamkeit!

Quellenangabe

Logo https://commons.wikimedia.org/wiki/File:Enigma-logo.svg

Fig. 1 https://commons.wikimedia.org/wiki/File:Bletchley_Park_Naval_Enigma_IMG_3604.JPG

Fig. 2 https://commons.wikimedia.org/wiki/File:Enigma_beschriftet_cropped.jpg

Fig. 3 http://www.cryptomuseum.com/crypto/enigma/working.htm

Fig. 4 https://commons.wikimedia.org/wiki/File:Enigma_insides.agr.jpg

Fig. 5 https://commons.wikimedia.org/wiki/File:Enigma_rotor.jpg

Fig. 6 http://www.cryptomuseum.com/crypto/enigma/working.htm

Fig. 7 https://commons.wikimedia.org/wiki/File:Enigma_rotors_and_spindle_showing_contacts_rachet_and_notch.jpg

Fig. 8 https://commons.wikimedia.org/wiki/File:ENIGMA_Wired_Rotor_-_National_Cryptologic_Museum_-_DSC07768.JPG

Fig. 9 http://www.gotopnews.com/technology-science/the-enigma-machine/

Fig. 10 https://commons.wikimedia.org/wiki/File:Enigma_wiring_kleur.svg

Fig. 11 https://commons.wikimedia.org/wiki/File:Enigma_keylist_3_rotor.jpg

Fig. 12 https://commons.wikimedia.org/wiki/File:MR_1932_small.jpg

Fig. 13 http://www.nybooks.com/articles/2015/02/05/saving-alan-turing-his-friends