Das Mysterium der Enigma

Tobias Langner

ETH Zurich – Distributed Computing Group – www.disco.ethz.ch

Die Enigma

Die Enigma

- Entwickelt von **Arthur Scherbius** im Jahre 1918

Die Enigma

- Entwickelt von **Arthur Scherbius** im Jahre 1918
- Version für Privatunternehmen als auch Militär

Die Enigma

- Entwickelt von **Arthur Scherbius** im Jahre 1918
- Version für Privatunternehmen als auch Militär
- Initieller Preis betrug ca. **CHF 30'000**

Die Enigma

- Entwickelt von **Arthur Scherbius** im Jahre 1918
- Version für Privatunternehmen als auch Militär
- Initieller Preis betrug ca. **CHF 30'000**
- Zu teuer für die meisten Interessenten

Die Enigma

- Entwickelt von **Arthur Scherbius** im Jahre 1918
- Version für Privatunternehmen als auch Militär
- Initieller Preis betrug ca. **CHF 30'000**
- Zu teuer für die meisten Interessenten
- Deutsche Führung nach **Kryptodebakel** in WK I alarmiert

Die Enigma

- Entwickelt von **Arthur Scherbius** im Jahre 1918
- Version für Privatunternehmen als auch Militär
- Initieller Preis betrug ca. **CHF 30'000**
- Zu teuer für die meisten Interessenten
- Deutsche Führung nach **Kryptodebakel** in WK I alarmiert
- Insgesamt über 30'000 Bestellungen

Exkurs: Verschlüsselung in der Antike

- **Caesar-Chiffre**: Ersetze jeden Buchstaben durch den k-ten Nachfolger im Alphabet

Schlüssel: $k = 2$

W A R S A W $\Rightarrow$ Y C T U C Y

Exkurs: Verschlüsselung in der Antike

- **Caesar-Chiffre**: Ersetze jeden Buchstaben durch den k-ten Nachfolger im Alphabet
- **Monoalphabetische Verschlüsselung**: Ersetze jeden Buchstaben durch einen anderen

Schlüssel: $\mathtt{A} \Rightarrow \mathtt{R}$ $\mathtt{R} \Rightarrow \mathtt{O}$ $\mathtt{S} \Rightarrow \mathtt{X}$ $\mathtt{W} \Rightarrow \mathtt{C}$

$$\mathtt{W\,A\,R\,S\,A\,W} \Rightarrow \mathtt{C\,R\,O\,X\,R\,C}$$

Exkurs: Verschlüsselung in der Antike

- **Caesar-Chiffre**: Ersetze jeden Buchstaben durch den k-ten Nachfolger im Alphabet
- **Monoalphabetische Verschlüsselung**: Ersetze jeden Buchstaben durch einen anderen
- Schwachstelle: **Frequenzverteilung** der Buchstaben unverändert

Schlüssel: $\mathtt{A} \Rightarrow \mathtt{R}$ $\mathtt{R} \Rightarrow \mathtt{O}$ $\mathtt{S} \Rightarrow \mathtt{X}$ $\mathtt{W} \Rightarrow \mathtt{C}$

$$\mathtt{W\,A\,R\,S\,A\,W} \Rightarrow \mathtt{C\,R\,O\,X\,R\,C}$$

Exkurs: Verschlüsselung in der Antike

- **Caesar-Chiffre**: Ersetze jeden Buchstaben durch den k-ten Nachfolger im Alphabet
- **Monoalphabetische Verschlüsselung**: Ersetze jeden Buchstaben durch einen anderen
- Schwachstelle: **Frequenzverteilung** der Buchstaben unverändert
- **Vigenère-Chiffre**: Verschiebe Buchstaben mit Schlüssel

Schlüssel: D E S

D E S D E S

W A R S A W $\Rightarrow$ Z E J V E O

Exkurs: Verschlüsselung in der Antike

- **Caesar-Chiffre**: Ersetze jeden Buchstaben durch den k-ten Nachfolger im Alphabet
- **Monoalphabetische Verschlüsselung**: Ersetze jeden Buchstaben durch einen anderen
- Schwachstelle: **Frequenzverteilung** der Buchstaben unverändert

- **Vigenère-Chiffre**: Verschiebe Buchstaben mit Schlüssel
- Schwachstelle: Verschlüsselung „**wiederholt**“ sich

Schlüssel: `D E S`

`D E S D E S`

`W A R S A W` $\Rightarrow$ `Z E J V E O`

Konzept der Enigma

- Beseitigung der Schwachstellen **monoalphabetischer Verschlüsselungen**:

Konzept der Enigma

- Beseitigung der Schwachstellen **monoalphabetischer Verschlüsselungen**:
- **Polyalphabetische** Verschlüsselung

Konzept der Enigma

- Beseitigung der Schwachstellen **monoalphabetischer Verschlüsselungen**:
- **Polyalphabetische** Verschlüsselung
- **Keine „Wiederholung“** der Verschlüsselung für übliche Nachrichtlängen

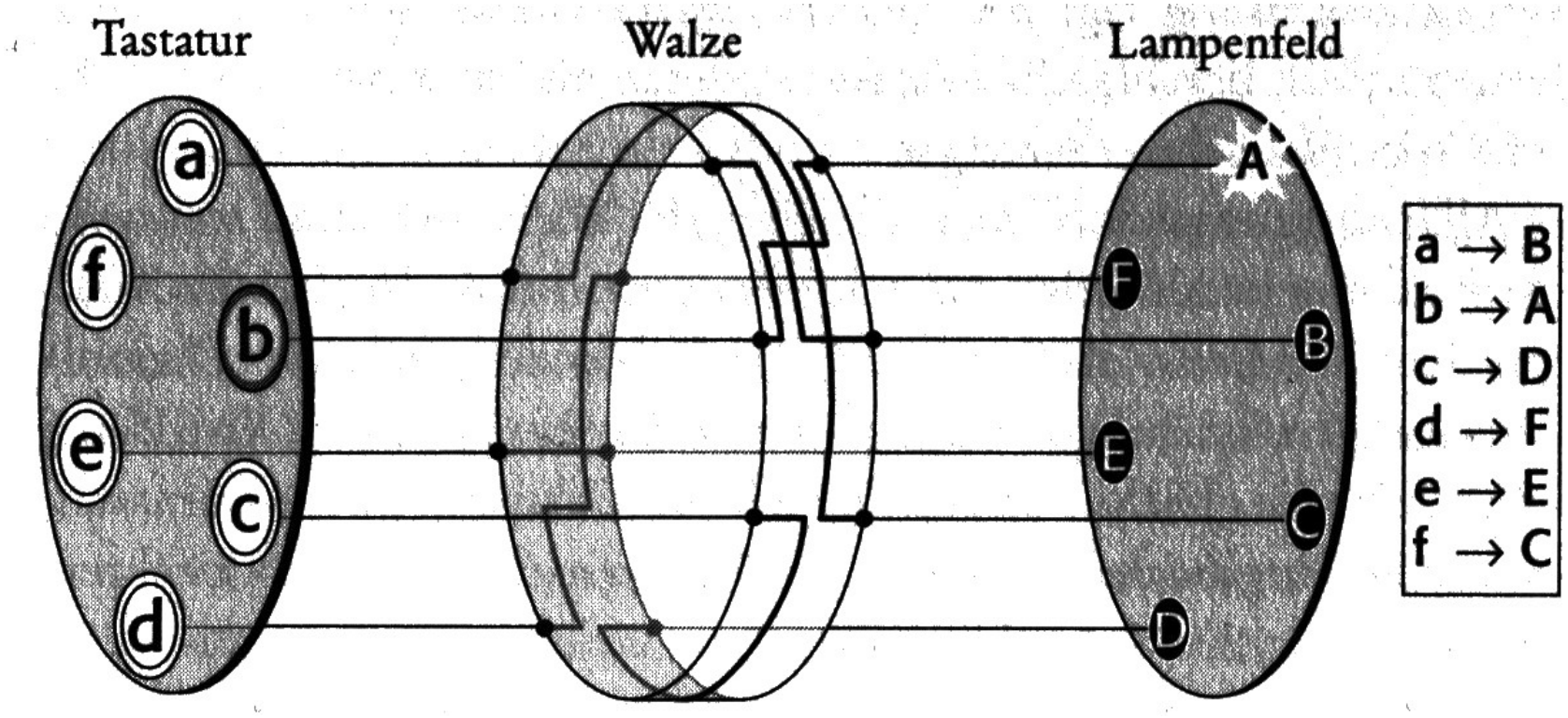
Konzept der Enigma

- Beseitigung der Schwachstellen **monoalphabetischer Verschlüsselungen**:
- **Polyalphabetische** Verschlüsselung
- **Keine „Wiederholung“** der Verschlüsselung für übliche Nachrichtlängen
- **Elektromechanische Verschlüsselung**

Funktionsweise der Enigma

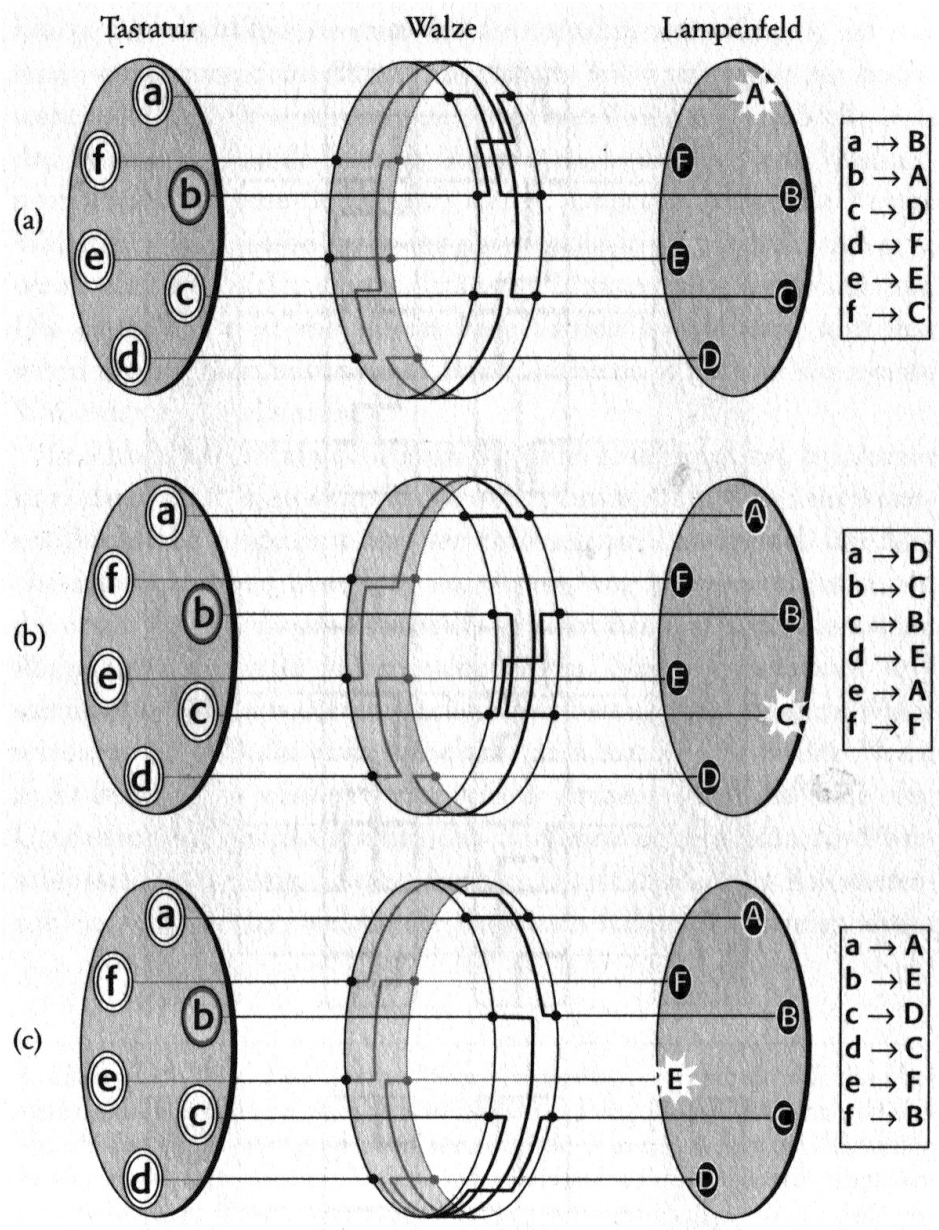
Funktionsweise der Enigma

Funktionsweise der Enigma



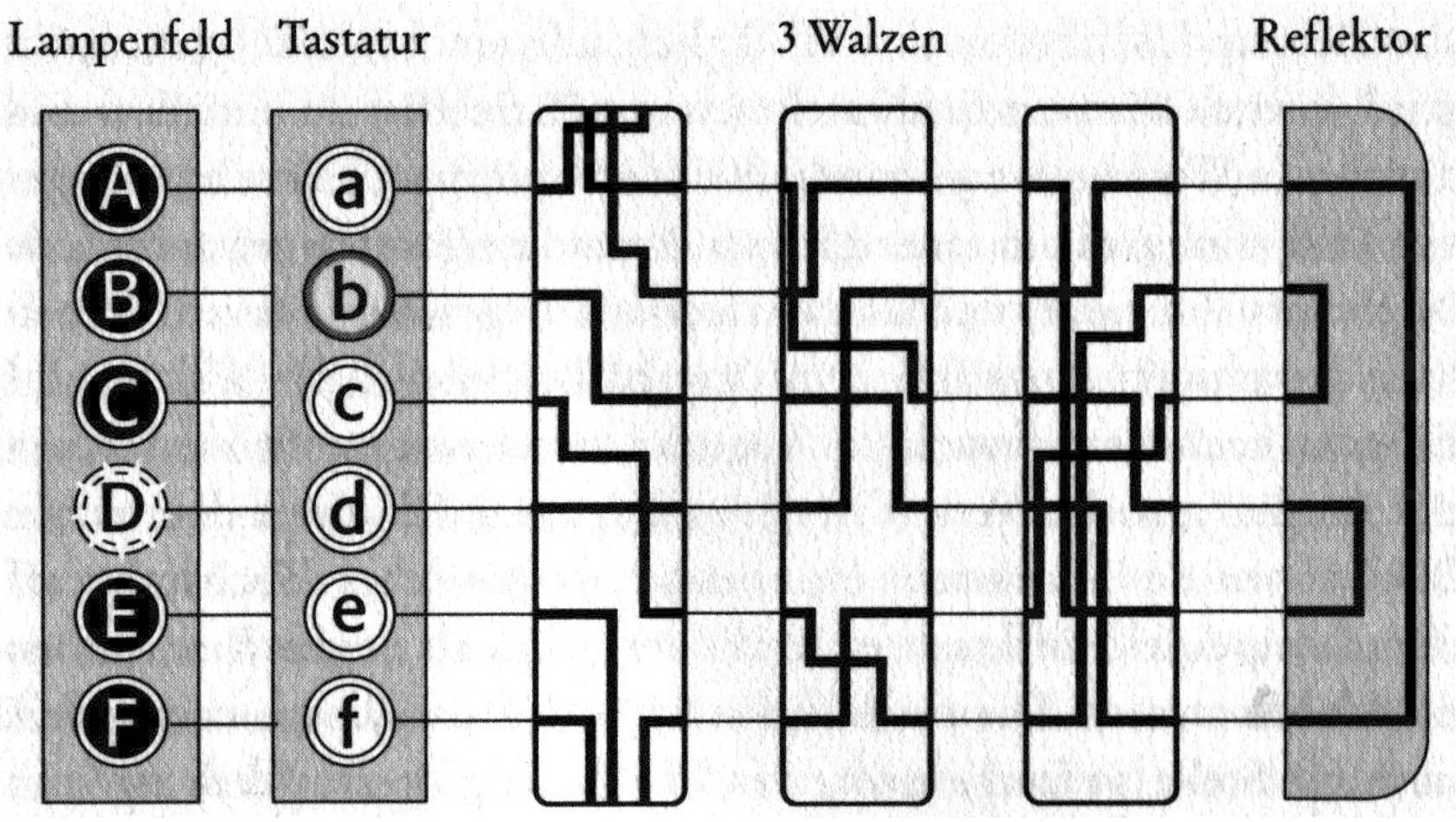
Quelle: Geheime Botschaften, Simon Singh, Deutscher Taschenbuch Verlag

Funktionsweise der Enigma



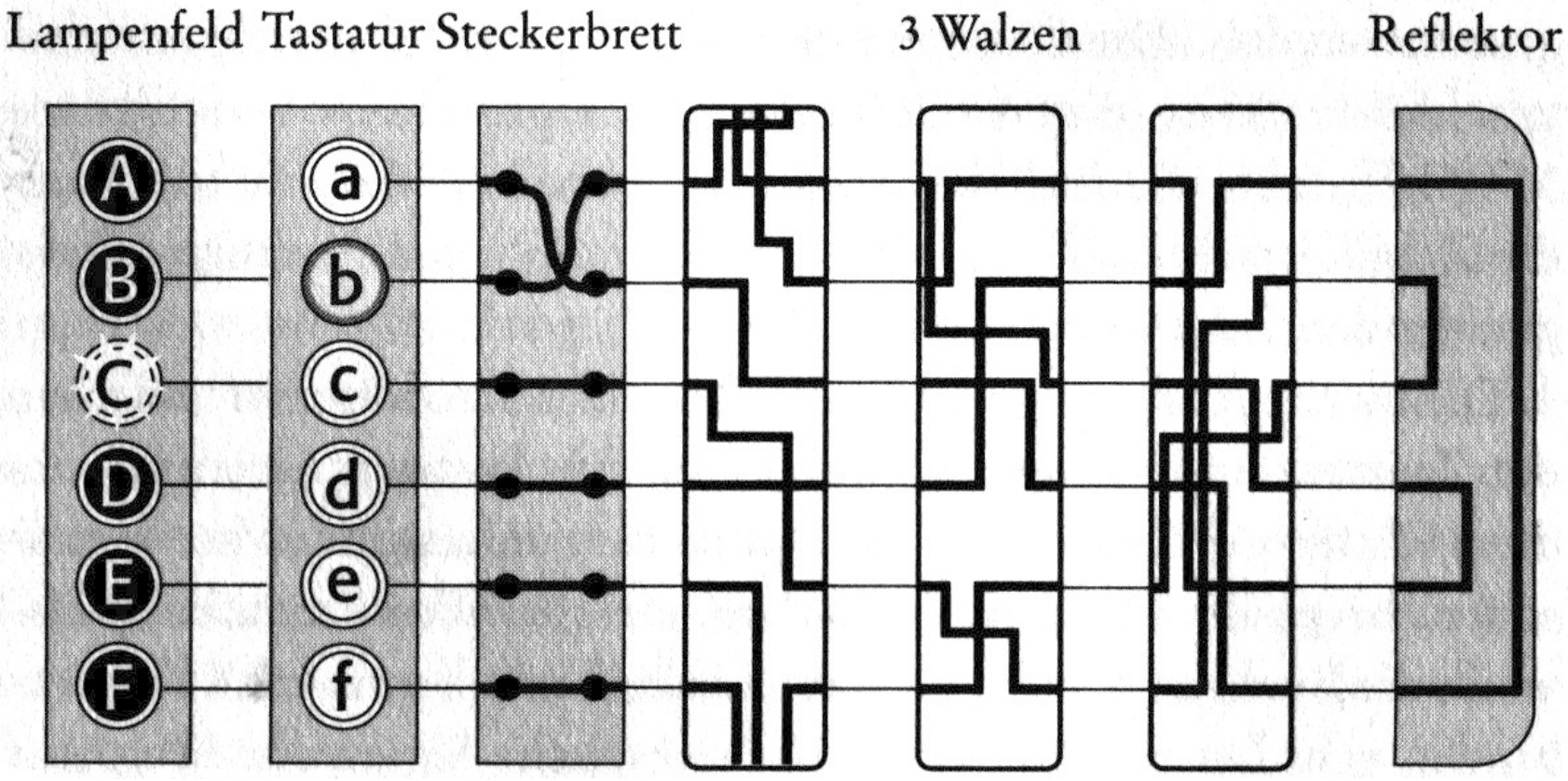
Quelle: Geheime Botschaften, Simon Singh, Deutscher Taschenbuch Verlag

Funktionsweise der Enigma



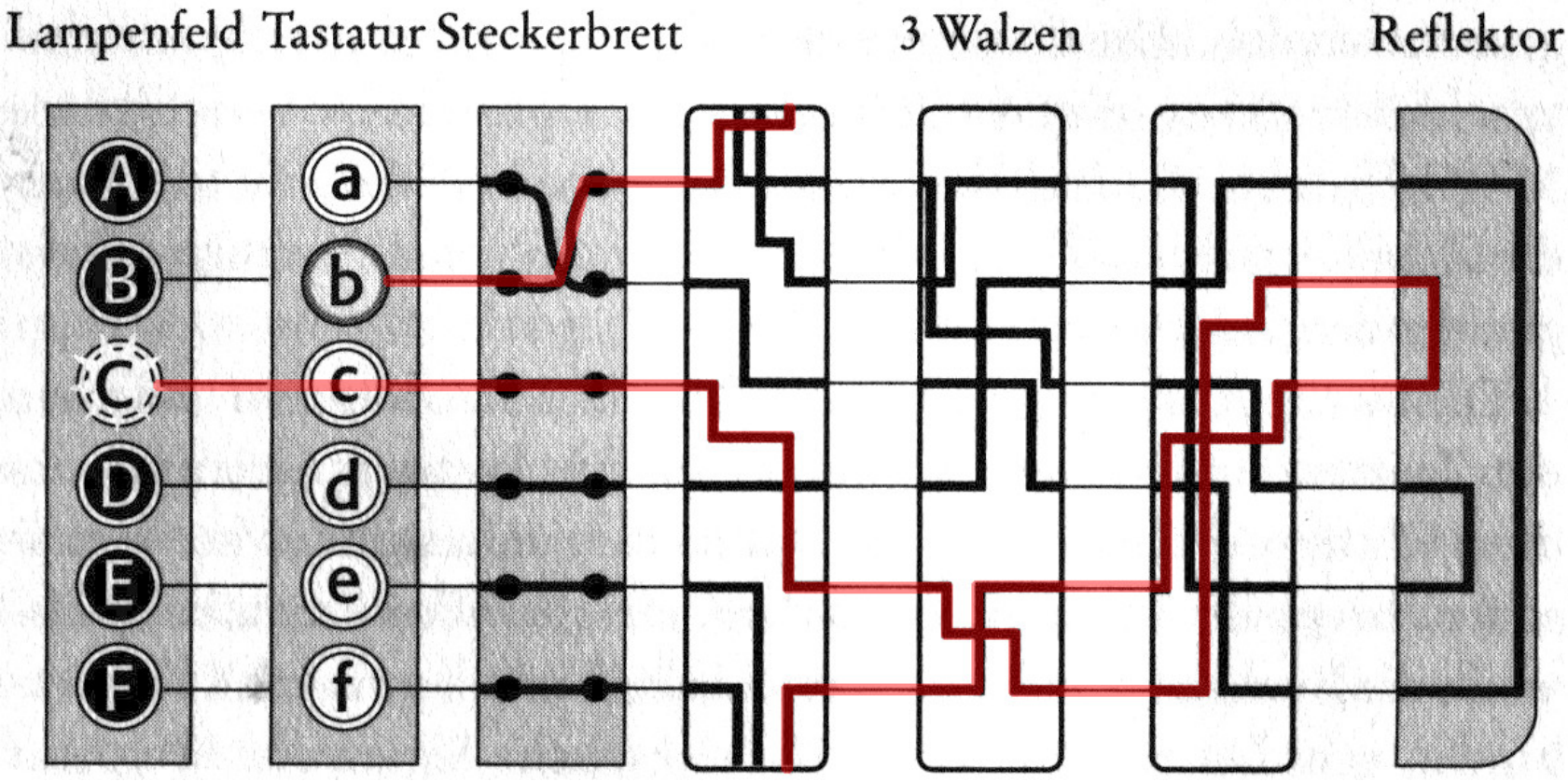
Quelle: Geheime Botschaften, Simon Singh, Deutscher Taschenbuch Verlag

Funktionsweise der Enigma



Quelle: Geheime Botschaften, Simon Singh, Deutscher Taschenbuch Verlag

Funktionsweise der Enigma



Quelle: Geheime Botschaften, Simon Singh, Deutscher Taschenbuch Verlag

Schlüsselkomplexität

- **Walzenlage:** verschiedene Positionen:

Schlüsselkomplexität

- **Walzenlage:** verschiedene Positionen:

$$3! = 6 \text{ Möglichkeiten}$$

Schlüsselkomplexität

- **Walzenlage:** verschiedene Positionen:

$$3! = 6 \text{ Möglichkeiten}$$

- **Walzengrundstellung:** 26 Positionen für jede Walze

Schlüsselkomplexität

- **Walzenlage:** verschiedene Positionen:

$$3! = 6 \text{ Möglichkeiten}$$

- **Walzengrundstellung:** 26 Positionen für jede Walze

$$26^3 = 17.576 \text{ Möglichkeiten}$$

Schlüsselkomplexität

- **Walzenlage:** verschiedene Positionen:

$$3! = 6 \text{ Möglichkeiten}$$

- **Walzengrundstellung:** 26 Positionen für jede Walze

$$26^3 = 17.576 \text{ Möglichkeiten}$$

- **Steckerverbindungen:** 10 Buchstabenpaare vertauschen

Schlüsselkomplexität

- **Walzenlage:** verschiedene Positionen:

$$3! = 6 \text{ Möglichkeiten}$$

- **Walzengrundstellung:** 26 Positionen für jede Walze

$$26^3 = 17.576 \text{ Möglichkeiten}$$

- **Steckerverbindungen:** 10 Buchstabenpaare vertauschen

$$\binom{26}{10} \cdot 11 \cdot 9 \cdot 7 \cdot 5 \cdot 3 = 100.391.791.500 \text{ Möglichkeiten}$$

Schlüsselkomplexität

- **Walzenlage:** verschiedene Positionen:

$$3! = 6 \text{ Möglichkeiten}$$

- **Walzengrundstellung:** 26 Positionen für jede Walze

$$26^3 = 17.576 \text{ Möglichkeiten}$$

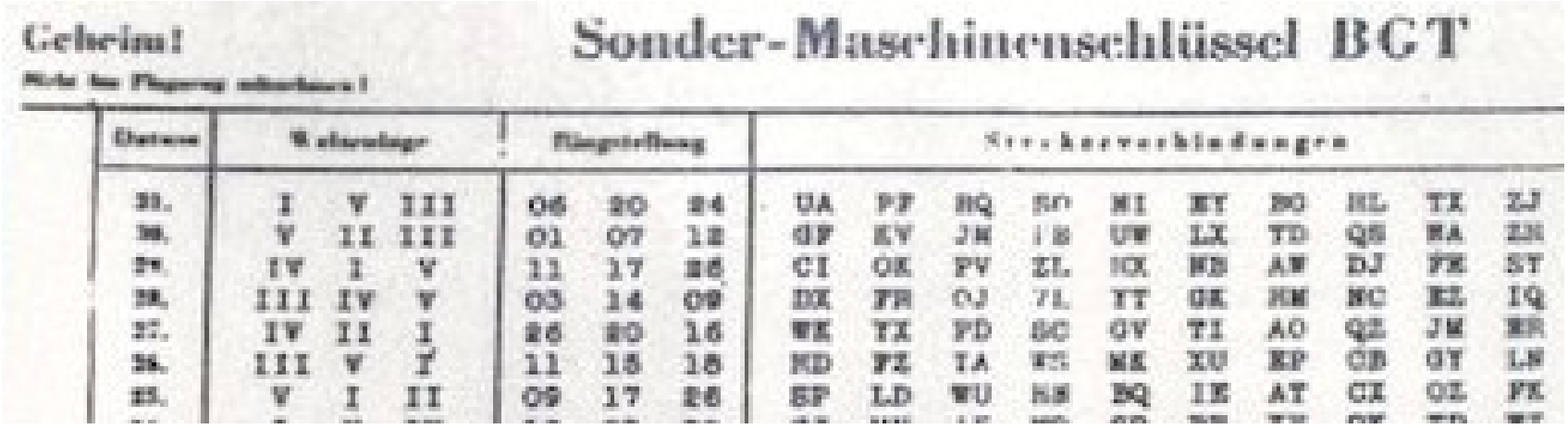
- **Steckerverbindungen:** 10 Buchstabenpaare vertauschen

$$\binom{26}{10} \cdot 11 \cdot 9 \cdot 7 \cdot 5 \cdot 3 = 100.391.791.500 \text{ Möglichkeiten}$$

- **Schlüsselanzahl insgesamt:**

$$\approx 10 \text{ Billiarden}$$

Verwendung der Enigma

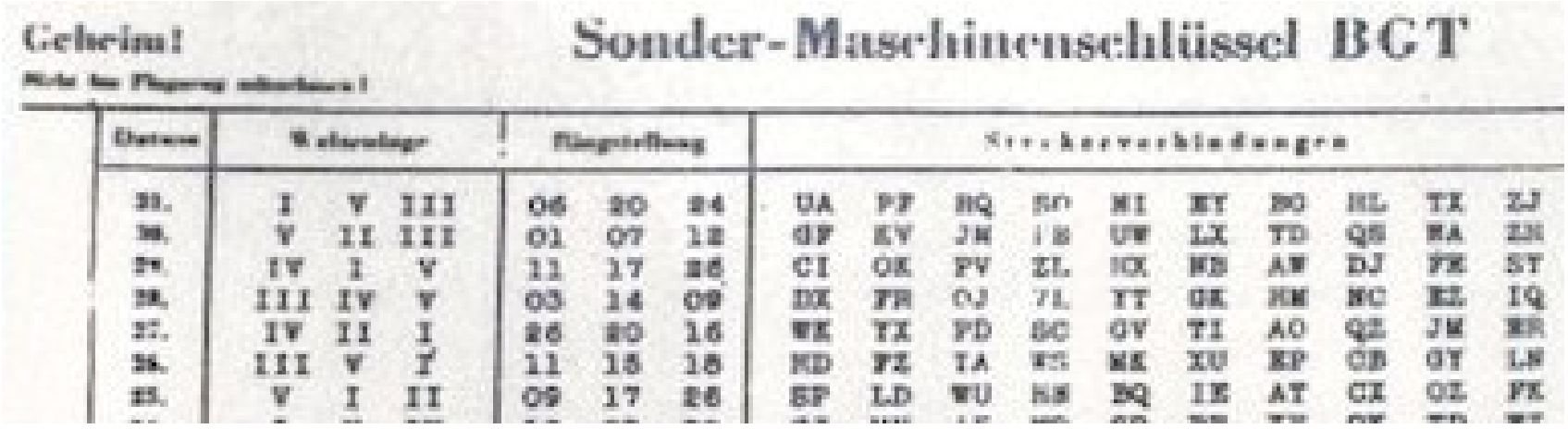


Geheim! Sonder-Maschinenschlüssel BCT

Datum	Walzenlage			Ringstellung			Steckerverbindungen									
31.	I	V	III	06	20	24	UA	PF	HQ	SO	MI	ET	BO	HL	TX	ZJ
30.	V	II	III	01	07	12	GF	KV	JN	IS	UW	LX	TD	QS	RA	ZH
29.	IV	I	V	11	17	26	CI	OK	PV	ZL	HX	RD	AF	DJ	PE	ST
28.	III	IV	V	03	14	09	DX	FR	OJ	YL	TT	GK	HM	NC	BZ	IQ
27.	IV	II	I	26	20	16	WK	TX	FD	SC	GV	TI	AO	QZ	JM	BR
26.	III	V	I	11	15	15	KD	PZ	IA	WS	ME	XU	EP	CB	GT	LN
25.	V	I	II	09	17	26	SF	LD	WU	HS	BQ	IE	AT	CK	GZ	FX

- Nachsehen der **Tageseinstellungen** in Schlüsseltabelle

Verwendung der Enigma

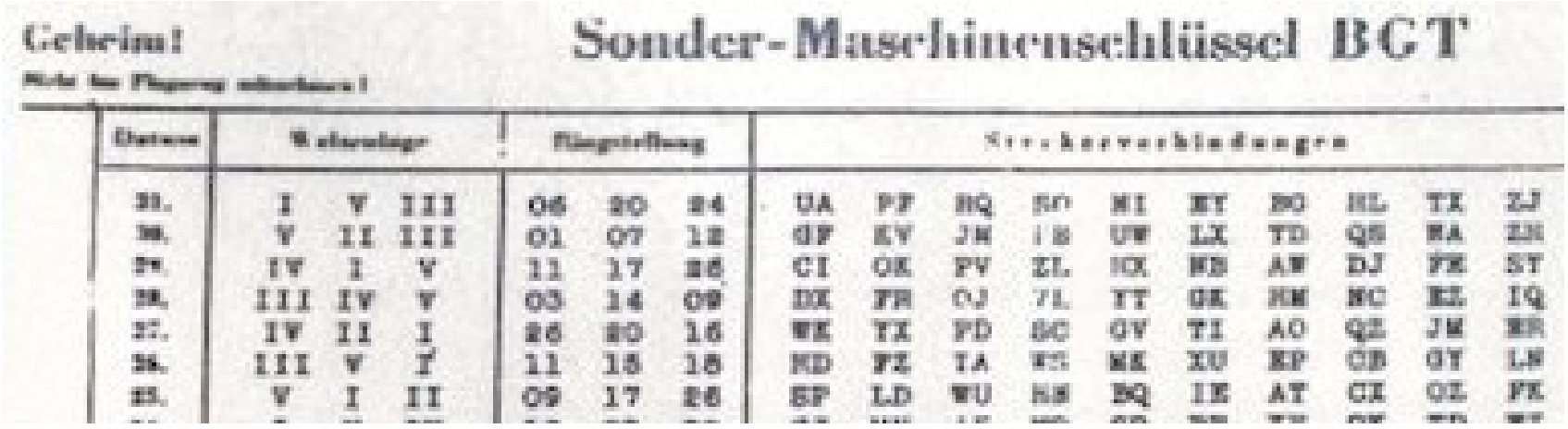


Geheim! Sonder-Maschinenschlüssel BCT

Datum	Walzenlage			Ringstellung			Steckerverbindungen									
30.	I	V	III	06	20	24	UA	PF	HQ	SO	MI	EY	BO	HL	TX	ZJ
29.	V	II	III	01	07	12	GF	KV	JN	IS	UW	LX	TD	QS	RA	ZH
28.	IV	I	V	11	17	26	CI	OE	PV	ZL	HX	RD	AF	DJ	PK	ST
27.	III	IV	V	03	14	09	DX	FR	OJ	VL	TT	GK	HM	NC	EZ	IQ
26.	IV	II	I	26	20	16	WE	YX	FD	BC	GV	TI	AO	QZ	JM	BR
25.	III	V	I	11	15	15	KD	PZ	IA	WS	ME	XU	EP	CB	GT	LN
24.	V	I	II	09	17	26	SF	LD	WU	HR	BQ	IE	AT	CK	OZ	FX

- Nachsehen der **Tageseinstellungen** in Schlüsseltabelle
- Herstellen der entsprechenden Walzeneinstellungen und Steckerverbindungen

Verwendung der Enigma

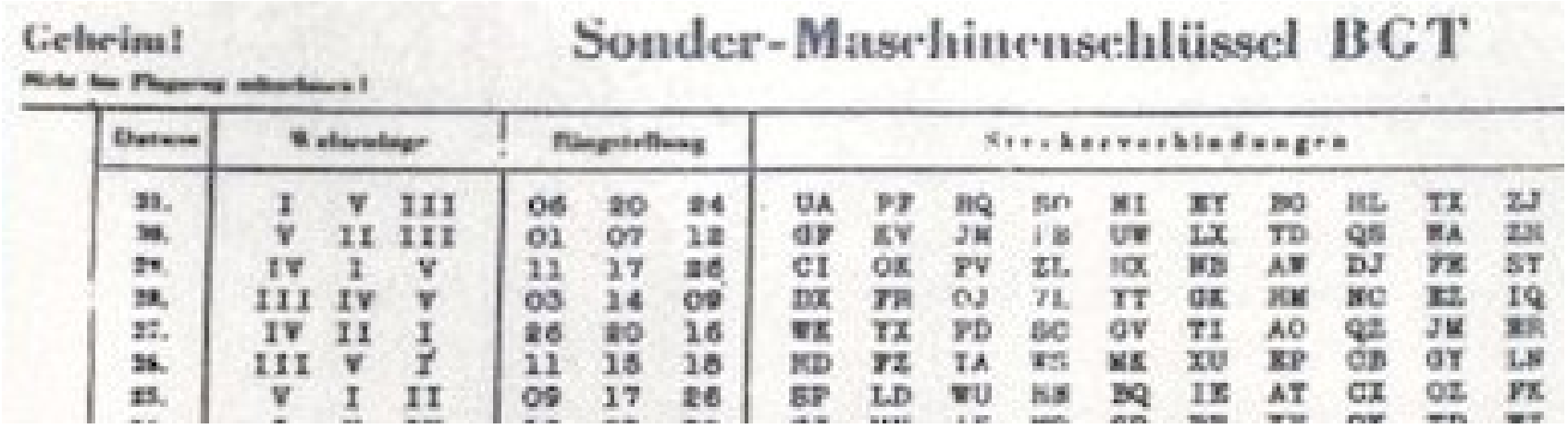


Geheim! Sonder-Maschinenschlüssel BCT

Datum	Walzenlage	Ringstellung	Steckerverbindungen
30.	I V III	06 20 24	UA PF HQ SO MI ET BO HL TX ZJ
29.	V II III	01 07 12	GF KV JN IS UW LX TD QS RA ZH
28.	IV I V	11 17 26	CI OE PV ZL HX RD AF DJ PK ST
27.	III IV V	03 14 09	DX FR OJ VL TT GK RM BC EZ IQ
26.	IV II I	26 20 16	WE TX FD SC GV TI AO QZ JM BR
25.	III V I	11 15 15	RD PZ IA WS ME XU EP CB GT LN
24.	V I II	09 17 26	SF LD WU HR BQ IE AT CK QZ PX

- Nachsehen der **Tageseinstellungen** in Schlüsseltabelle
- Herstellen der entsprechenden Walzeneinstellungen und Steckerverbindungen
- Sender verschlüsselt Nachricht

Verwendung der Enigma



Geheim! Sonder-Maschinenschlüssel BCT

Datum	Walzenlage			Ringstellung			Steckerverbindungen									
30.	I	V	III	06	20	24	UA	PF	HQ	SO	MI	EY	BO	HL	TX	ZJ
29.	V	II	III	01	07	12	GF	KV	JR	IS	UW	LX	TD	QS	RA	ZN
28.	IV	I	V	11	17	26	CI	OE	PV	ZL	HX	RD	AF	DJ	PK	ST
27.	III	IV	V	03	14	09	DX	FR	OJ	VL	TT	GK	RM	NC	EZ	IQ
26.	IV	II	I	26	20	16	WE	YX	FD	BC	GV	TI	AO	QZ	JM	BR
25.	III	V	I	11	15	15	KD	PZ	IA	WS	ME	XU	EP	CB	GT	LN
24.	V	I	II	09	17	26	SF	LD	WU	HR	BQ	IE	AT	CK	OZ	FX

- Nachsehen der **Tageseinstellungen** in Schlüsseltabelle
- Herstellen der entsprechenden Walzeneinstellungen und Steckerverbindungen
- Sender verschlüsselt Nachricht
- Empfänger entschlüsselt Nachricht mit **den selben Einstellungen**

Schwächen der Enigma

Technische Schwächen:

Schwächen der Enigma

Technische Schwächen:

- **Symmetrische** Steckerverbindungen

Schwächen der Enigma

Technische Schwächen:

- **Symmetrische** Steckerverbindungen
- Prinzip der **Umkehrwalze**

Schwächen der Enigma

Technische Schwächen:

- **Symmetrische** Steckerverbindungen
- Prinzip der **Umkehrwalze**

Bedienfehler der Operateure:

Schwächen der Enigma

Technische Schwächen:

- **Symmetrische** Steckerverbindungen
- Prinzip der **Umkehrwalze**

Bedienfehler der Operateure:

- Schlechte Wahl der **Tagesschlüssel**

Schwächen der Enigma

Technische Schwächen:

- **Symmetrische** Steckerverbindungen
- Prinzip der **Umkehrwalze**

Bedienfehler der Operateure:

- Schlechte Wahl der **Tagesschlüssel**
- **Redundanz** in Nachrichten

Schwächen der Enigma

Technische Schwächen:

- **Symmetrische** Steckerverbindungen
- Prinzip der **Umkehrwalze**

Bedienfehler der Operateure:

- Schlechte Wahl der **Tagesschlüssel**
- **Redundanz** in Nachrichten
- „Erratbare“ Nachrichtenteile (sog. **Cribs**)

Die „Erzfeinde“ der Enigma

- Wissenschaftler im **Biuro Szyfrów** in Warschau

Die „Erzfeinde“ der Enigma

- Wissenschaftler im **Biuro Szyfrów** in Warschau
- Junger Mathematiker **Marian Rejewski**

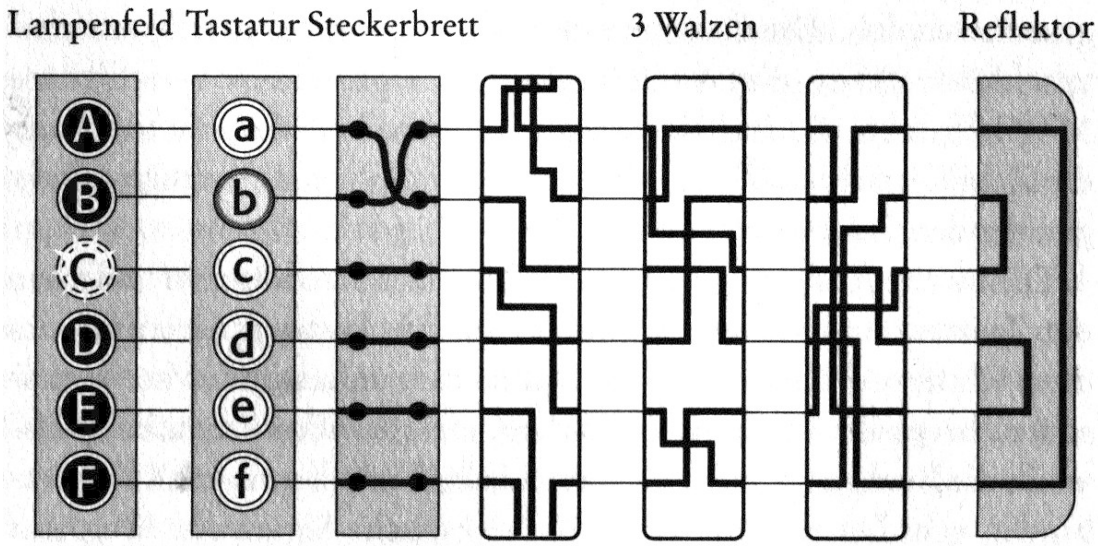
Die „Erzfeinde“ der Enigma

- Wissenschaftler im **Biuro Szyfrów** in Warschau
- Junger Mathematiker **Marian Rejewski**
- Das **Kryptobüro** konnte von 1932 bis 1938 alle Enigma-Nachrichten mitlesen

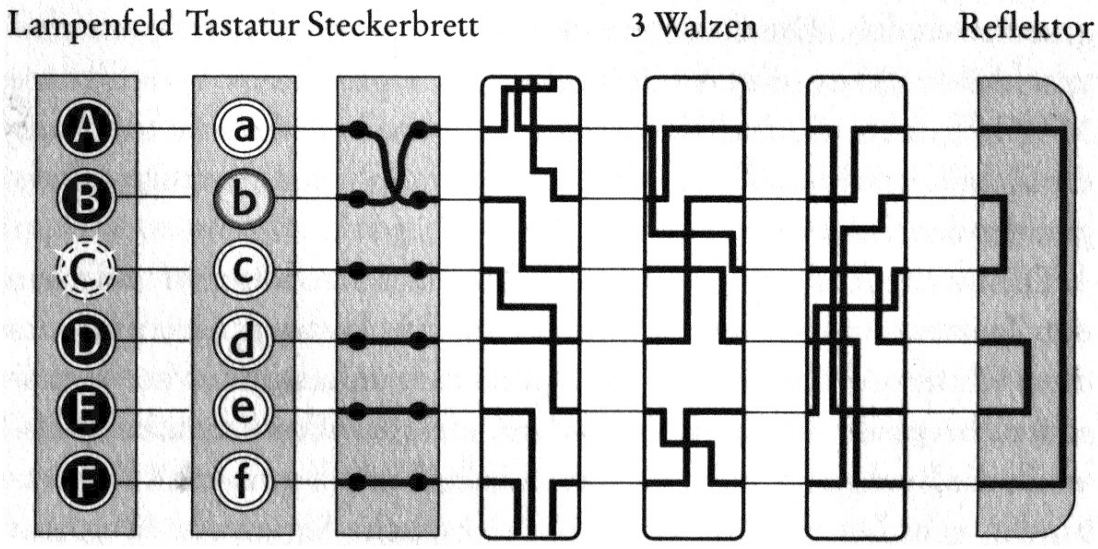
Die „Erzfeinde“ der Enigma

- Wissenschaftler im **Biuro Szyfrów** in Warschau
- Junger Mathematiker **Marian Rejewski**
- Das **Kryptobüro** konnte von 1932 bis 1938 alle Enigma-Nachrichten mitlesen
- Dann erhöhten die Deutschen die **Komplexität** und die Polen suchten Hilfe bei den Briten

Verwendung von Cribs

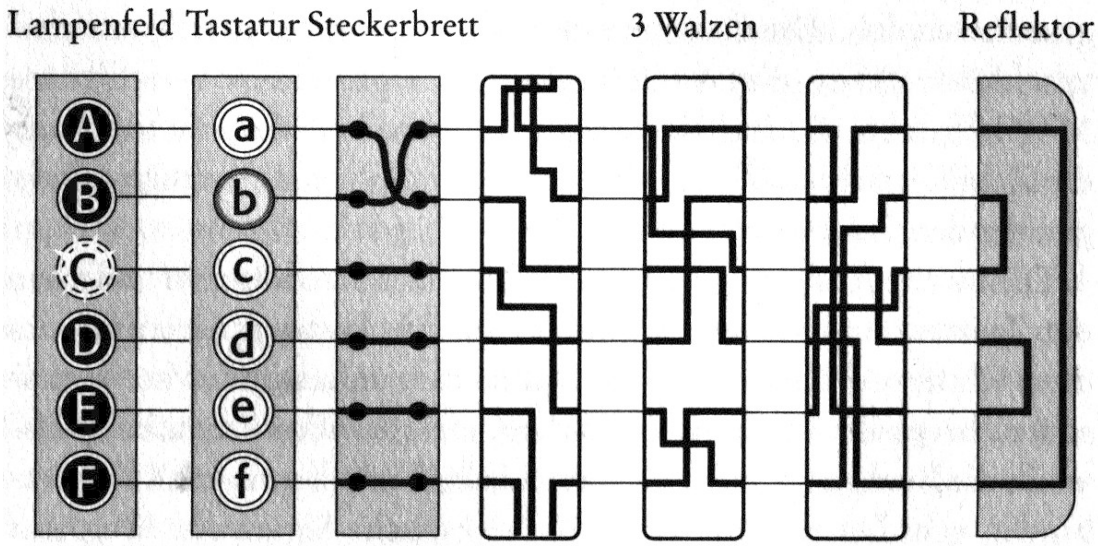


Verwendung von Cribs



- **Umkehrwalze:** Kein Buchstabe wird mit sich **selbst** verschlüsselt

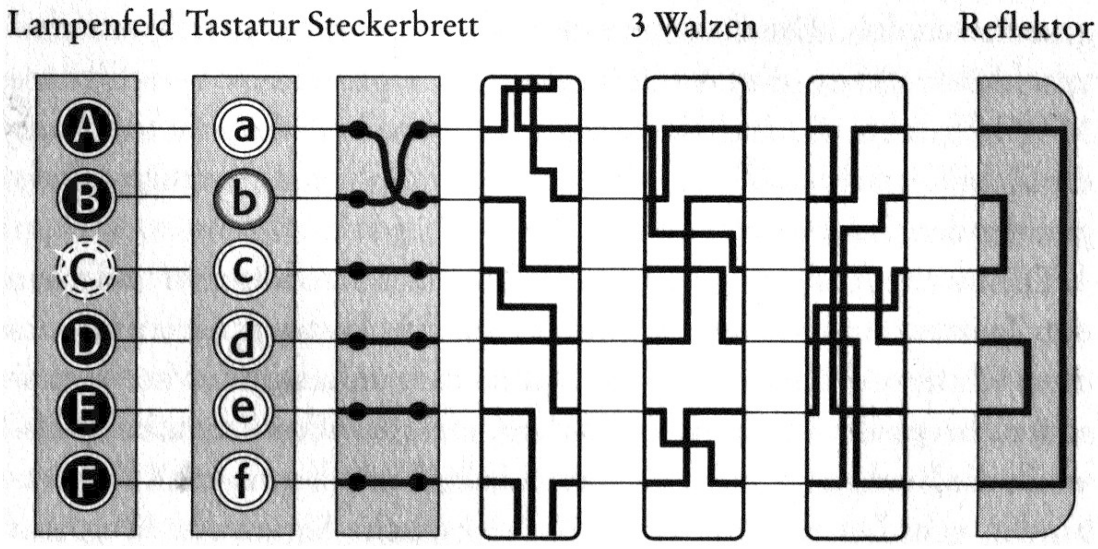
Verwendung von Cribs



- **Umkehrwalze:** Kein Buchstabe wird mit sich **selbst** verschlüsselt

B I L S X G I A D F N Z X D K

Verwendung von Cribs



- **Umkehrwalze:** Kein Buchstabe wird mit sich **selbst** verschlüsselt

```
B I L S X G I A D F N Z X D K

F L U G H A F E N . . . . j
. F L U G H A F E N . . . n
. . F L U G H A F E N . . n
. . . F L U G H A F E N . n
. . . . F L U G H A F E N j
```

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

`D E S D E S` $\Rightarrow$ `J R L P O U`

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

`D E S D E S` $\Rightarrow$ `J R L P O U`

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

`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`

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

```
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
. . . . . . . . . P . . . . . . . . . . . . . . . .
```

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

```
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
. . . . . . . . . P . . . . . . . O . . . . . . . .
```

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

`D E S D E S` $\Rightarrow$ `J R L P O U`

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

```
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
. . . . . . . . . P . U . . . . . O . . . . . . . .
```

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D$$

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

`D E S D E S` $\Rightarrow$ `J R L P O U`

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R$$

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O$$

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V$$

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B$$

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

`D E S D E S` $\Rightarrow$ `J R L P O U`

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F$$

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

$$\texttt{D E S D E S} \quad \Rightarrow \quad \texttt{J R L P O U}$$

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F \Rightarrow A$$

Verwendung von Spruchschlüssel

- Zur Erhöhung der Sicherheit: Verwendung von **individuellem Spruchschlüssel pro Nachricht**
- **Walzengrundstellung** wurde „zufällig“ gewählt (Bsp. `D E S`)
- Spruchschlüssel wird **zweimal** mit Tagesschlüssel verschlüsselt

`D E S D E S` $\Rightarrow$ `J R L P O U`

- **Zusammenhang** von Buchstabenpaar (J,P), (R,O) und (L,U)
- **Beziehungstabelle**

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

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F \Rightarrow A$$

$$C \Rightarrow E \Rightarrow K \Rightarrow S \Rightarrow X \Rightarrow H \Rightarrow L \Rightarrow U \Rightarrow W \Rightarrow M \Rightarrow Z \Rightarrow C$$

$$G \Rightarrow Q \Rightarrow Y \Rightarrow N \Rightarrow J \Rightarrow P \Rightarrow G$$

$$I \Rightarrow T \Rightarrow G$$

Verwendung von Spruchschlüssel

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F \Rightarrow A$$

$$C \Rightarrow E \Rightarrow K \Rightarrow S \Rightarrow X \Rightarrow H \Rightarrow L \Rightarrow U \Rightarrow W \Rightarrow M \Rightarrow Z \Rightarrow C$$

$$G \Rightarrow Q \Rightarrow Y \Rightarrow N \Rightarrow J \Rightarrow P \Rightarrow G$$

$$I \Rightarrow T \Rightarrow I$$

Verwendung von Spruchschlüssel

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F \Rightarrow A$$

$$C \Rightarrow E \Rightarrow K \Rightarrow S \Rightarrow X \Rightarrow H \Rightarrow L \Rightarrow U \Rightarrow W \Rightarrow M \Rightarrow Z \Rightarrow C$$

$$G \Rightarrow Q \Rightarrow Y \Rightarrow N \Rightarrow J \Rightarrow P \Rightarrow G$$

$$I \Rightarrow T \Rightarrow I$$

- **Kettenlängen** $= \{11, 7, 6, 2\}$

Verwendung von Spruchschlüssel

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F \Rightarrow A$$

$$C \Rightarrow E \Rightarrow K \Rightarrow S \Rightarrow X \Rightarrow H \Rightarrow L \Rightarrow U \Rightarrow W \Rightarrow M \Rightarrow Z \Rightarrow C$$

$$G \Rightarrow Q \Rightarrow Y \Rightarrow N \Rightarrow J \Rightarrow P \Rightarrow G$$

$$I \Rightarrow T \Rightarrow I$$

- **Kettenlängen** $= \{11, 7, 6, 2\}$
- **Kettenlängen** werden nur durch **Walzenkonfiguration** bestimmt

Verwendung von Spruchschlüssel

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F \Rightarrow A$$

$$C \Rightarrow E \Rightarrow K \Rightarrow S \Rightarrow X \Rightarrow H \Rightarrow L \Rightarrow U \Rightarrow W \Rightarrow M \Rightarrow Z \Rightarrow C$$

$$G \Rightarrow Q \Rightarrow Y \Rightarrow N \Rightarrow J \Rightarrow P \Rightarrow G$$

$$I \Rightarrow T \Rightarrow I$$

- **Kettenlängen** $= \{11, 7, 6, 2\}$
- **Kettenlängen** werden nur durch **Walzenkonfiguration** bestimmt
- Tabelle: Kettenlängen $\Rightarrow$ Walzenkonfiguration(en)

Verwendung von Spruchschlüssel

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F \Rightarrow A$$

$$C \Rightarrow E \Rightarrow K \Rightarrow S \Rightarrow X \Rightarrow H \Rightarrow L \Rightarrow U \Rightarrow W \Rightarrow M \Rightarrow Z \Rightarrow C$$

$$G \Rightarrow Q \Rightarrow Y \Rightarrow N \Rightarrow J \Rightarrow P \Rightarrow G$$

$$I \Rightarrow T \Rightarrow I$$

- **Kettenlängen** $= \{11, 7, 6, 2\}$
- **Kettenlängen** werden nur durch **Walzenkonfiguration** bestimmt
- Tabelle: Kettenlängen $\Rightarrow$ Walzenkonfiguration(en)
- Noch zu tun: Steckerverbindungen $\Rightarrow$ Cribs & Co.

Verwendung von Spruchschlüssel

- Identifizieren von **Zyklen** in Beziehungstabelle

$$A \Rightarrow D \Rightarrow R \Rightarrow O \Rightarrow V \Rightarrow B \Rightarrow F \Rightarrow A$$

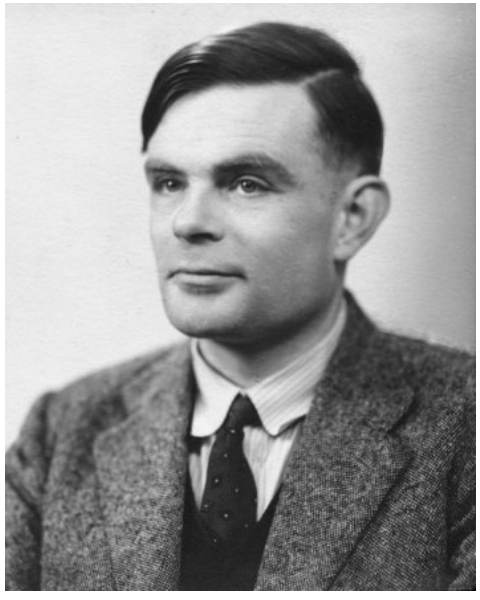
$$C \Rightarrow E \Rightarrow K \Rightarrow S \Rightarrow X \Rightarrow H \Rightarrow L \Rightarrow U \Rightarrow W \Rightarrow M \Rightarrow Z \Rightarrow C$$

$$G \Rightarrow Q \Rightarrow Y \Rightarrow N \Rightarrow J \Rightarrow P \Rightarrow G$$

$$I \Rightarrow T \Rightarrow I$$

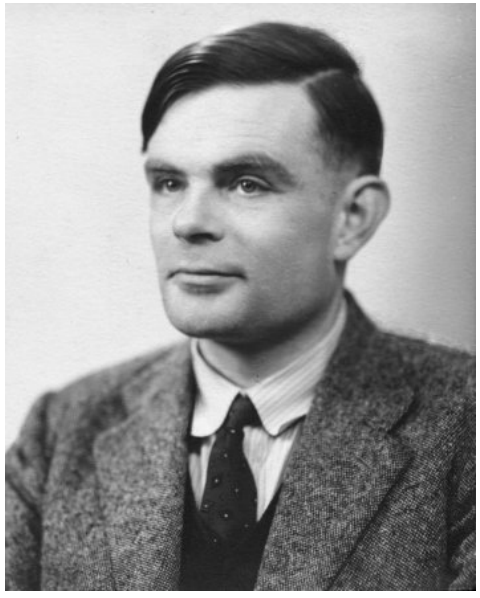
- **Kettenlängen** $= \{11, 7, 6, 2\}$
- **Kettenlängen** werden nur durch **Walzenkonfiguration** bestimmt
- Tabelle: Kettenlängen $\Rightarrow$ Walzenkonfiguration(en)
- Noch zu tun: Steckerverbindungen $\Rightarrow$ Cribs & Co.
- Ergebnis: **Tagesschlüssel für genau einen Tag!**

Alan Turing



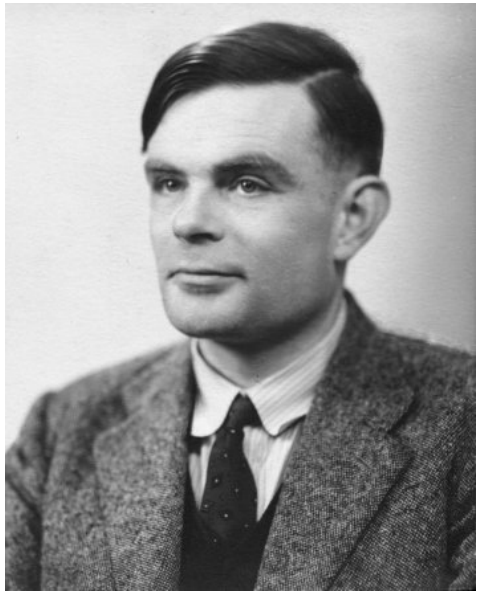
- Deutschland verbesserte die Enigma beständig

Alan Turing



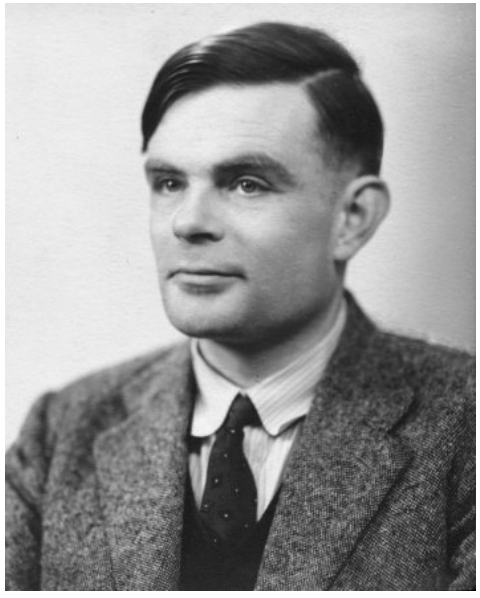
- Deutschland verbesserte die Enigma beständig
- Bestehende **manuelle** Methoden wurden zu aufwändig

Alan Turing



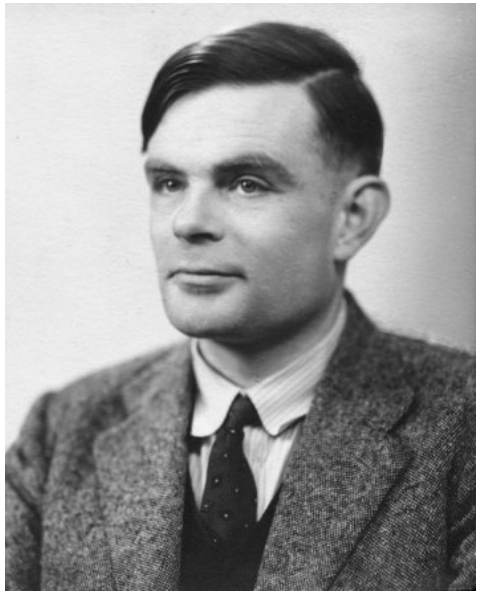
- Deutschland verbesserte die Enigma beständig
- Bestehende **manuelle** Methoden wurden zu aufwändig
- Turing verbesserte Rejewskis „Bomben“ zur **automatisierten Bestimmung** des Tagesschlüssels innerhalb einer Stunde

Alan Turing



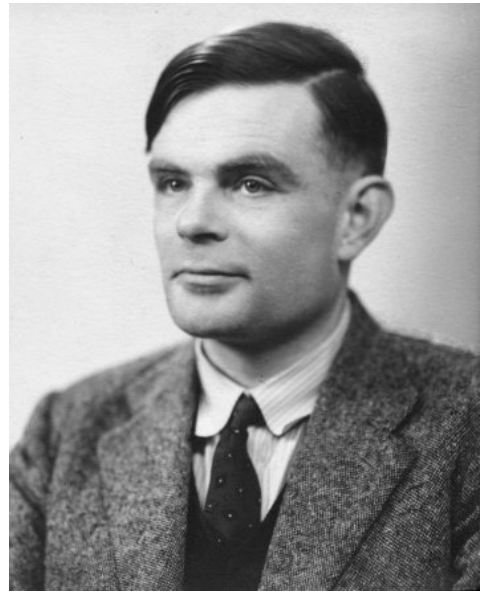
- Deutschland verbesserte die Enigma beständig
- Bestehende **manuelle** Methoden wurden zu aufwändig
- Turing verbesserte Rejewskis „Bomben“ zur **automatisierten Bestimmung** des Tagesschlüssels innerhalb einer Stunde
- . . . und entwickelte weitere bahnbrechende Krypto-Techniken

Alan Turing



- Deutschland verbesserte die Enigma beständig
- Bestehende **manuelle** Methoden wurden zu aufwändig
- Turing verbesserte Rejewskis „Bomben“ zur **automatisierten Bestimmung** des Tagesschlüssels innerhalb einer Stunde
- . . . und entwickelte weitere bahnbrechende Krypto-Techniken
- . . . die für viele Jahre geheim blieben

Alan Turing



- Deutschland verbesserte die Enigma beständig
- Bestehende **manuelle** Methoden wurden zu aufwändig
- Turing verbesserte Rejewskis „Bomben“ zur **automatisierten Bestimmung** des Tagesschlüssels innerhalb einer Stunde
- . . . und entwickelte weitere bahnbrechende Krypto-Techniken
- . . . die für viele Jahre geheim blieben
- Historiker: Knacken der Enigma verkürzte WK II um **mindestens drei Jahre**. . .

Vielen Dank!