

verschlüsselt
entschlüsselt

Die entscheidende Schwachstelle der Enigma

Aufgrund von Verbesserungen in der Enigma und ihrer Handhabung – mehr Walzen, mehr Steckerverbindungen, Wegfall der Spruchschlüsselverdopplung – konnte ab 1939/40 die *kryptologische Bombe* nicht mehr eingesetzt werden.

Polen war in der Zwischenzeit von Deutschland besetzt worden. Die polnischen Krypto-Experten übergaben ihre Erkenntnisse an die Briten. Dort entwickelte der Informatiker **Alan Turing** einen Nachfolger der *kryptologischen Bombe*.

Beim Durchprobieren aller 1 014 000 möglichen Schlüssel (Walzenlage und -stellung) war eine weitere Schwachstelle der Enigma äußerst hilfreich: Aus A kann ein B, C, D, ... oder Z werden, aber niemals wieder ein A. Aus B kann niemals wieder ein B werden, aus C niemals ein C usw. Was zunächst wie ein Vorteil aussieht, ist tatsächlich ein entscheidender Fehler.

Angenommen, wir kennen ein Wort aus der verschlüsselten Nachricht. Militärische Meldungen im 2. Weltkrieg enthielten z. B. häufig die Wortfolge „Oberkommandoderwehrmacht“. (Leerzeichen ließ man beim Verschlüsseln weg.)

Da aus einem A niemals wieder ein A wird, aus B niemals ein B usw., können wir sofort sehen, wo sich das Wort „Oberkommandoderwehrmacht“ *nicht* befinden kann:

```
BHNCXSEQKOBIIODWFBTZGCEYHQJJEWOYNBDXHQBALHTSSDPGWG
1 OBERKOMMANDODERWEHRMACHT
2 OBERKOMMANDODERWEHRMACHT
3 OBERKOMMANDODERWEHRMACHT
4 OBERKOMMANDODERWEHRMACHT
5 OBERKOMMANDODERWEHRMACHT
6 OBERKOMMANDODERWEHRMACHT
7 OBERKOMMANDODERWEHRMACHT
8 OBERKOMMANDODERWEHRMACHT
9 OBERKOMMANDODERWEHRMACHT
10 OBERKOMMANDODERWEHRMACHT
11 OBERKOMMANDODERWEHRMACHT
12 OBERKOMMANDODERWEHRMACHT
13 OBERKOMMANDODERWEHRMACHT
14 OBERKOMMANDODERWEHRMACHT
15 OBERKOMMANDODERWEHRMACHT
16 OBERKOMMANDODERWEHRMACHT
17 OBERKOMMANDODERWEHRMACHT
18 OBERKOMMANDODERWEHRMACHT
19 OBERKOMMANDODERWEHRMACHT
20 OBERKOMMANDODERWEHRMACHT
21 OBERKOMMANDODERWEHRMACHT
22 OBERKOMMANDODERWEHRMACHT
23 OBERKOMMANDODERWEHRMACHT
24 OBERKOMMANDODERWEHRMACHT
25 OBERKOMMANDODERWEHRMACHT
26 OBERKOMMANDODERWEHRMACHT
27 OBERKOMMANDODERWEHRMACHT
BHNCXSEQKOBIIODWFBTZGCEYHQJJEWOYNBDXHQBALHTSSDPGWG
```

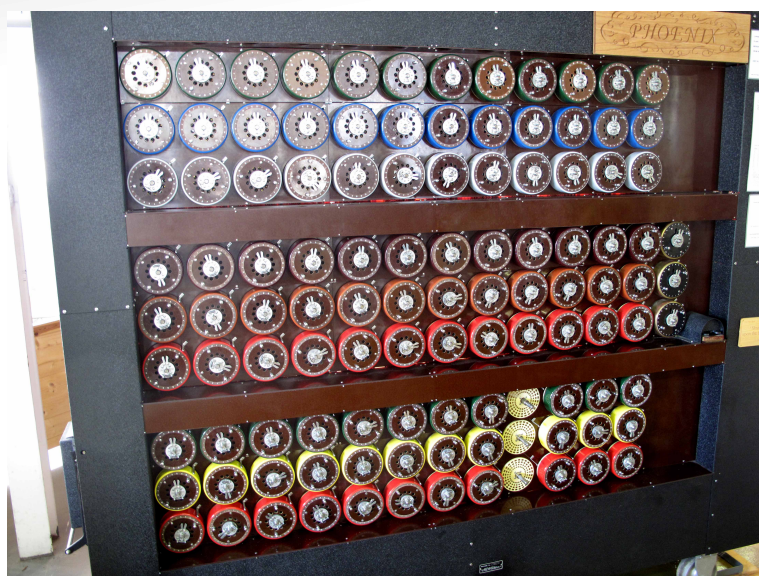
Quelle: [https://de.wikipedia.org/wiki/Enigma_\(Maschine\)](https://de.wikipedia.org/wiki/Enigma_(Maschine))
Verwendung gemäß Lizenz: CC-BY-SA 3.0

Unter Ausnutzung dieser Schwäche gelang es Turing 1940, eine Maschine zu bauen, die alle 1 014 000 verschiedenen Schlüssel innerhalb von ca. 10 Stunden durchprobierte – die **Turing-Bombe**. Sie war noch kein Computer im heutigen Sinne, aber ein wichtiger Meilenstein auf dem Weg dorthin.

Durch den gleichzeitigen Einsatz von 60 *Turing-Bomben* – eine für jede der 60 möglichen Walzenlagen – konnte man nun innerhalb von 10 Minuten jede Enigma-Nachricht entschlüsseln.



Alan Turing (1912–1954)
Bildquelle: https://de.wikipedia.org/wiki/Datei:Alan_Turing_az_1930-as_években.jpg (Ausschnitt, geschärft)
(Urheberrecht abgelaufen)



Nachbau der *Turing-Bombe*, Bletchley Park
Bildquelle: <https://de.wikipedia.org/wiki/Datei:RebuiltBombeFrontView.jpg>
Verwendung gemäß Lizenz: CC0 1.0

verschlüsselt
entschlüsselt



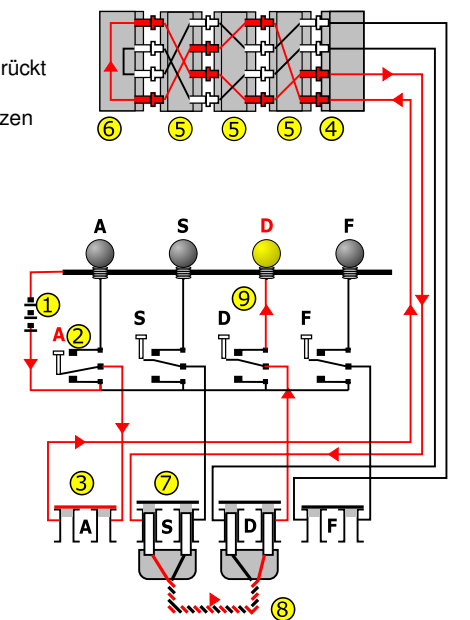
Wie funktioniert die Enigma?

Die Enigma ist eine elektromechanische Maschine zur Ver- und Entschlüsselung von Texten. Sie hat 26 Tasten und 26 Lampen, jeweils mit den Buchstaben des Alphabets beschriftet. Man drückt eine Taste, und eine der Lampen leuchtet.

Die Verdrahtung zwischen den Tasten und den Lampen erfolgt über Walzen, die die Buchstaben wild durcheinanderwürfeln: Aus A wird zum Beispiel D, aus B wird M, aus C wird T usw.

- Nach jedem Tastendruck – also nach jedem verschlüsselten Buchstaben – wird die Walze um einen Buchstaben weitergedreht.
- Der Strom geht danach durch eine zweite Walze, die sich bei jeder vollen Umdrehung der ersten Walze um einen Buchstaben weiterdreht.
- Danach geht es durch eine dritte Walze, die sich noch langsamer weiterdreht.
- Nach den drei Walzen werden die Buchstaben nochmals durcheinandergewürfelt und noch einmal rückwärts durch die drei Walzen geschickt.
- Bevor der Strom zur Lampe gelangt, wird noch ein weiteres Mal durcheinandergewürfelt: Per Steckerverbindung kann man Buchstaben miteinander vertauschen.
- Sender und Empfänger können die Walzen auswählen und anordnen (Walzenlage) und die Anfangsposition der Walzen variieren (Walzenstellung). Auch lässt sich das Verdrahtungsinnenleben der Walzen noch einmal separat verdrehen (Ringstellung). Wenn dies alles sowie die Steckerverbindungen bei Sender und Empfänger gleich sind, kann die Nachricht ver- und wieder entschlüsselt werden.

- 1 Batterie
- 2 Tastatur: Taste „A“ gedrückt
- 3 Steckerbrett ohne Stecker: überbrückt
- 4 Eintrittswalze
- 5 drei wechselbare, rotierende Walzen
- 6 Umkehrwalze (fest)
- 7 Steckerbrett mit Stecker
- 8 Steckkabel vertauscht S ↔ D
- 9 Lampenfeld: Lampe „D“ leuchtet



Bildquelle: https://de.wikipedia.org/wiki/Datei:Enigma_wiring_kleur.svg
Verwendung gemäß Lizenz: GNU FDL 2.1+, CC-BY-SA-NP 3.0 oder CC-BY-SA 2.5

Bildquelle: <https://de.wikipedia.org/wiki/Datei:Enigma-logo.svg>
(Urheberrecht gemäß US-Recht nicht anwendbar)



Copyright © 2018 Prof. Dr. rer. nat. Peter Gerwinski
Hochschule Bochum, Campus Velbert/Heiligenhaus
<http://www.hs-bochum.de/cvh/>

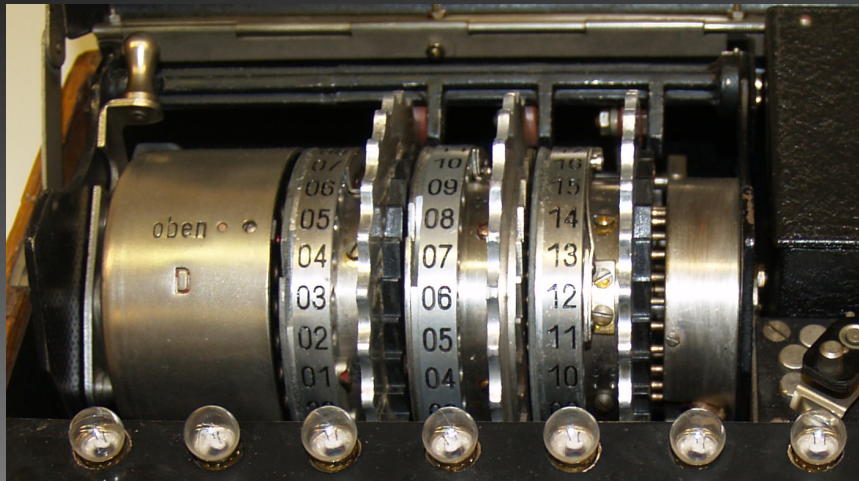
Sie dürfen diesen Text und das oben wiedergegebene Foto der Enigma gemäß den folgenden Lizenzen verwenden, kopieren und weitergeben: CC-BY-SA (Version 4.0) oder GNU GPL (Version 3 oder höher)

Hochschule Bochum
Bochum University
of Applied Sciences



Campus
Velbert/Heiligenhaus

DEUTSCHES SCHLOSS- UND BESCHLÄGEMUSEUM VELBERT
www.museum.velbert.de



verschlüsselt
entschlüsselt

Walzen der Enigma:
rechts die drei rotierenden Walzen,
links die feststehende Umkehrwalze

Copyright © 2018 Deutsches Schloss- und Beschlägemuseum Velbert
Lizenz: CC-BY-SA 4.0

Wie gut ist die Enigma-Verschlüsselung?

Die Enigma-Verschlüsselung beruht nicht allein auf der Geheimhaltung der Walzenverdrahtungen, sondern vor allem auf der Vielzahl der verschiedenen Möglichkeiten, eine Nachricht zu verschlüsseln: der Vielzahl der möglichen **Schlüssel**.

Wie viele verschiedene Schlüssel gibt es?

Walzenlage: Von zunächst drei, später fünf Walzen wählt man drei aus und steckt sie in einer gewählten Reihenfolge in die Maschine. Dafür gibt es $3 \cdot 2 \cdot 1 = 6$ verschiedene Möglichkeiten bei drei Walzen bzw. $5 \cdot 4 \cdot 3 = 60$ bei fünf Walzen.

Walzenstellung: Für jede der drei ausgewählten Walzen wählt man eine von jeweils 26 Anfangsstellungen.

Ringstellung: Für jede der drei ausgewählten Walzen dreht man die innere Verdrahtung in die gewünschte Position. Dies sind wieder 26 Möglichkeiten für jede der drei Walzen.

Steckerverbindungen: Auf dem Steckbrett wurden zunächst 5 bis 8, vom Jahr 1939 an immer 10 Steckerverbindungen gesetzt. Dafür gibt es sehr viele Möglichkeiten, nämlich:

$$\frac{26 \cdot 25}{2} \cdot \frac{24 \cdot 23}{2} \cdot \dots \cdot \frac{8 \cdot 7}{2} = 150\,738\,274\,937\,250$$

Insgesamt erhalten wir

$$\begin{aligned} & (\text{Walzenlage}) && 60 \\ & (\text{Walzenstellung}) && \cdot 26 \cdot 26 \cdot 26 \\ & (\text{Ringstellung}) && \cdot 26 \cdot 26 \cdot 26 \\ & (\text{Steckerverbindungen}) && \cdot 150\,738\,274\,937\,250 \\ & && = 2\,793\,925\,870\,508\,516\,103\,360\,000 \\ & && \text{verschiedene Schlüssel.} \end{aligned}$$

Selbst mit heutigen Computern wäre es aussichtslos, aus all diesen Möglichkeiten den richtigen Schlüssel durch bloßes Ausprobieren zu finden. (Für Experten: Die Schlüssellänge beträgt hier 81,21 Bit, kann aber letztlich auf 19,95 Bit reduziert werden.)

Geheime Kommandoachse		Nr. 00190	
Luftwaffen-Maschinen-Schlüssel Nr. 649			
Achtung! Schlüsselmaterial darf nicht unverschlüsselt in Feindhände fallen. Bei Verlust sofortige Meldung an die vorgesetzte Stelle.			
Walzenlage	Ringstellung	Steckerverbindungen	Steckerverbindungen
040 31 I V III 14 05 24	52 01 DT KU FO RT JN 13 LQ	WXY DEY	445 T2G
040 30 IV III II 03 20 02	13 01 MB RW DT 02 10 00 07	X11 ACW	443 W6U
040 29 III I I 12 25 03	02 AT CV 10 13 05 1W P2 PH 31	10C ACN	44W W4D
040 28 II III V 06 08 16	08 PV A1 DK 07 00 10 11 02	17B C1D	44B T4H
040 27 III I IV 11 01 07	17 EQ HS UV 07 10 07 08 10 17	W4J T4B	441 X1A
040 26 I IV V 10 22 15	V1 AL RT KO GO 11 02 00 P3 PF	X1E K6B	44V T4R
040 25 IV III I 08 25 12	0K PV AD 1Y PK 02 13 05 02	44U 04U	44W 01T
040 24 V I IV 09 10 14	17 45 09 02 20 08 03 01 10	KP1 T4I	441 T1G
040 23 IV II I 24 12 04	0V F8 AK 00 0H 02 02 05 07	04N T4M	44T T1G
040 22 II IV V 01 00 21	10 A1 00 06	04N T4M	44T T1G
040 21 I V II 19 05 15	17 03 K2 04	04N T4M	44T T1G
040 20 III IV V 20 01 10	08 PV A1 DK 07 00 10 11 02	04N T4M	44T T1G
040 19 V III I 17 20 27	03 F8 PV AT 01 01 01 01 01	04N T4M	44T T1G
040 18 IV II V 15 23 26	02 01 1V AQ KW PX RT P5 10 10	04N T4M	44T T1G
040 17 I IV II 21 10 00	18 02 15 00 01 01 01 01 01	04N T4M	44T T1G
040 16 V II III 08 16 13	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 15 II IV I 01 01 01	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 14 IV I V 10 11 00	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 13 I III II 13 20 01	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 12 V II IV 18 10 07	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 11 IV III 02 26 15	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 10 III V IV 23 01 01	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 9 V I III 18 04 05	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 8 IV II V 13 19 20	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 7 III I IV 09 02 22	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 6 V II IV 23 02 24	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 5 IV I II 04 21 05	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 4 III V I 16 14 02	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 3 V I II 19 11 00	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G
040 2 IV V I 16 14 02	05 01 01 01 01 01 01 01 01	04N T4M	44T T1G

Schlüsseltafel aus dem 2. Weltkrieg:
Walzenlage, Ringstellung und Steckerverbindungen
wurden jeden Tag gewechselt.

Bildquelle: https://de.wikipedia.org/wiki/Datei:Enigma_keylist_3_rotor.jpg
(Urheberrecht abgelaufen)

Wie konnte die Enigma „geknackt“ werden?

Bereits ab 1932 gelang es dem polnischen Mathematiker **Marian Rejewski** und seinen Kollegen, die Schlüssel aufgefangener Funksprüche zu rekonstruieren und so die Texte lesbar zu machen. Wie war das möglich?

Walzenlage: Speziell konstruierte Maschinen (das **Zyklometer** und später die **kryptologische Bombe**) halfen, alle möglichen Walzenlagen gleichzeitig durchzuprobieren.

Walzenstellung: Diese wurde für jeden Funkspruch neu gewählt und am Anfang der Nachricht mitgesendet. Dabei wurde sie zweimal hintereinander aufgeschrieben (jeweils 3 Buchstaben) und verschlüsselt.

Diese sog. **Spruchschlüsselverdopplung** war ein entscheidender Fehler: Sie verriet Rejewski zwei verschiedene Verschlüsselungen derselben Buchstabenfolge.

Hinzu kam eine Schwachstelle der Enigma: Wenn aus einem A ein X wird, wird aus einem X ein A. Der Benutzer braucht nicht auszuwählen, ob er ver- oder entschlüsseln will. Das vereinfacht die Bedienung, führt aber zu Regelmäßigkeiten bei der Verschlüsselung.

Diese Fehler zusammen ermöglichten Rejewski, sämtliche Kombinationen von Walzenlage und Walzenstellung durchzuprobieren, auch wenn Ringstellung und Steckerverbindungen noch nicht ermittelt waren.

Ringstellung: Auch bei falscher Ringstellung kann man bereits Teile des Textes lesen. Dadurch konnte Rejewski die Ringstellung nachträglich durch Ausprobieren ermitteln und brauchte sie nicht gleichzeitig mit den restlichen Schlüsseln zu suchen.

Steckerverbindungen: Diese vertauschen lediglich Buchstaben, was durch geschicktes Ausprobieren rückgängig gemacht werden kann.

Tatsächlich müssen also nur die Walzenlage (zunächst 6, später 60 Möglichkeiten) und die Walzenstellung (eigentlich $26 \cdot 26 \cdot 26$ Möglichkeiten, aufgrund einer unwesentlichen Anomalie aber tatsächlich nur $26 \cdot 25 \cdot 26$) durch Ausprobieren ermittelt werden.

Statt 2 793 925 870 508 516 103 360 000 brauchte die **kryptologische Bombe** also „nur“ höchstens

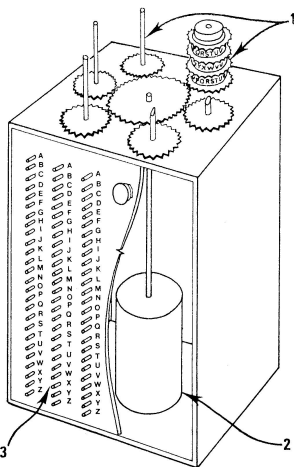
$$\begin{aligned} & (\text{Walzenlage}) && 60 \\ & (\text{Walzenstellung}) && \cdot 26 \cdot 25 \cdot 26 \\ & && = 1\,014\,000 \end{aligned}$$

verschiedene Schlüssel durchzuprobieren.



Marian Rejewski (1905–1980)

Bildquelle: https://de.wikipedia.org/wiki/Datei:Marian_Rejewski.jpg
(Urheberrecht gemäß polnischem Recht nicht anwendbar)



8. Bomba kryptologiczna
(dla przejrzystości ukazano
w górnej części bomby
tylko jeden zestaw
wzruszków szafujących)

Skizze der **kryptologischen Bombe**
(Die Maschine selbst wurde im Krieg zerstört.)

Bildquelle: https://de.wikipedia.org/wiki/Datei:Bomba_full.jpg
(Urheberrecht gemäß polnischem Recht nicht anwendbar)

Innenleben einer Enigma-Walze

Die grünen Drähte vertauschen die Buchstaben und drehen sich nach jedem Tastenanschlag mit der Walze um eine Stelle weiter. Nach einer vollen Umdrehung wird – wie in einem Kilometerzähler – die Nachbarwalze um eine Stelle weitergedreht.

Bildquelle: https://de.wikipedia.org/wiki/Datei:ENIGMA_Wired_Rotor_-_National_Cryptologic_Museum_-_DSC07768.JPG
Verwendung gemäß Lizenz: CC-0 (Version 1.0)

Steckerverbinder einer Enigma
Hier werden S ↔ O und A ↔ J vertauscht.

Bildquelle: <https://de.wikipedia.org/wiki/Datei:Enigma-plugboard.jpg>
Verwendung gemäß Lizenz: CC-BY-SA (Version 3.0)
oder GNU FDL (Version 1.2 oder höher)

