

# verschlüsselt entschlüsselt



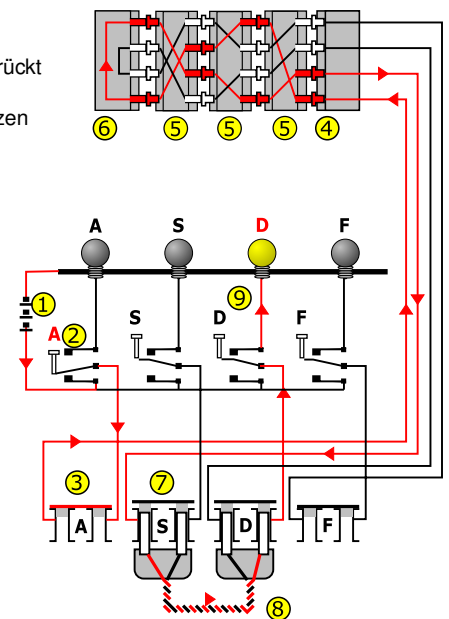
## Wie funktioniert die Enigma?

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](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](http://www.museum.velbert.de)





# 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

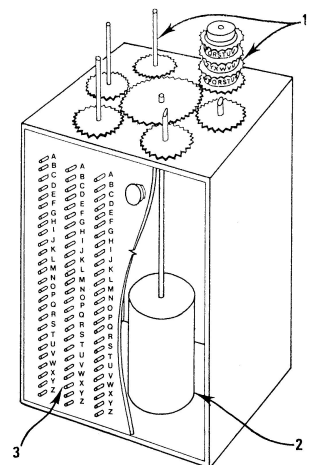
$$\begin{aligned} &(\text{Walzenlage}) && 60 \\ &(\text{Walzenstellung}) && \cdot 26 \cdot 25 \cdot 26 \\ &&& = 1\,014\,000 \end{aligned}$$

verschiedene Schlüssel durchzuprobieren.



Marian Rejewski (1905–1980)

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



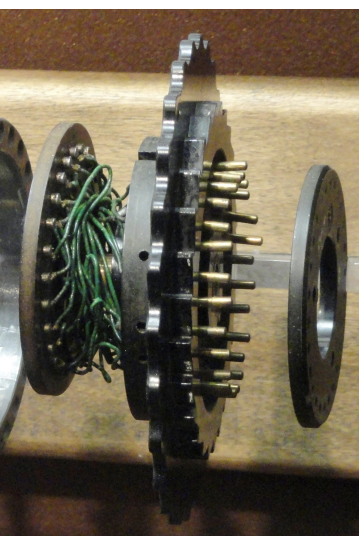
8. Bomba kryptologiczna

(dla przejrzystości ukazano  
w górnej części bomby  
tylko jeden zestaw  
wirników szyfrujących)

1. wirniki,
2. silnik elektryczny,
3. przełączniki

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

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



## Innenleben einer Enigma-Walze

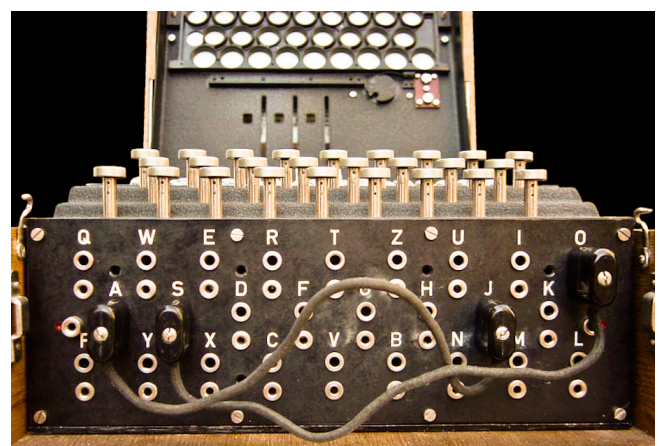
Die grünen Drähte vertauschen die Buchstaben und drehen sich nach jedem Tastenanschlag mit der Walze um eine Stelle weiter. Nach einer vollen Umdrehung wird – wie in einem Kilometerzähler – die Nachbarwalze um eine Stelle weitergedreht.

Bildquelle: [https://de.wikipedia.org/wiki/Datei:ENIGMA\\_Wired\\_Rotor\\_-\\_National\\_Cryptologic\\_Museum\\_-\\_DSC07768.JPG](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  $S \leftrightarrow O$  und  $A \leftrightarrow J$  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)



# 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:

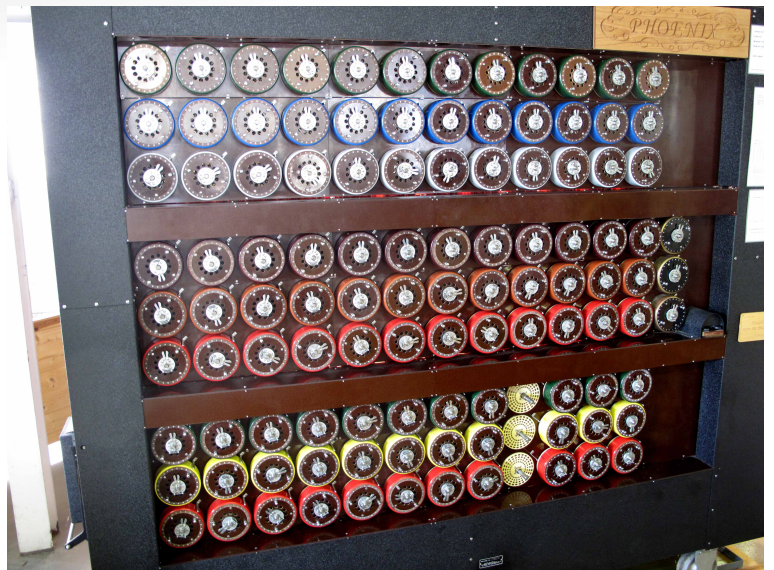
```
BHNCXSEQKOBIIODWFBTZGCEYHQQJEWQYNBDXHQBALHTSSDPWGW
1 OBERKOMMANDODERWEHRMACT
2 OBERKOMMANDODERWEHRMACT
3 OBERKOMMANDODERWEHRMACT
4 OBERKOMMANDODERWEHRMACT
5 OBERKOMMANDODERWEHRMACT
6 OBERKOMMANDODERWEHRMACT
7 OBERKOMMANDODERWEHRMACT
8 OBERKOMMANDODERWEHRMACT
9 OBERKOMMANDODERWEHRMACT
10 OBERKOMMANDODERWEHRMACT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

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



Alan Turing (1912–1954)

Bildquelle: [https://de.wikipedia.org/wiki/Datei:Alan\\_Turing\\_az\\_1930-as\\_években.jpg](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

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.