Thema: Die Enigma

Dominik Oepen, Sebastian Höfer

Seminar: Geschichte der Verschlüsselung

14.11.2006

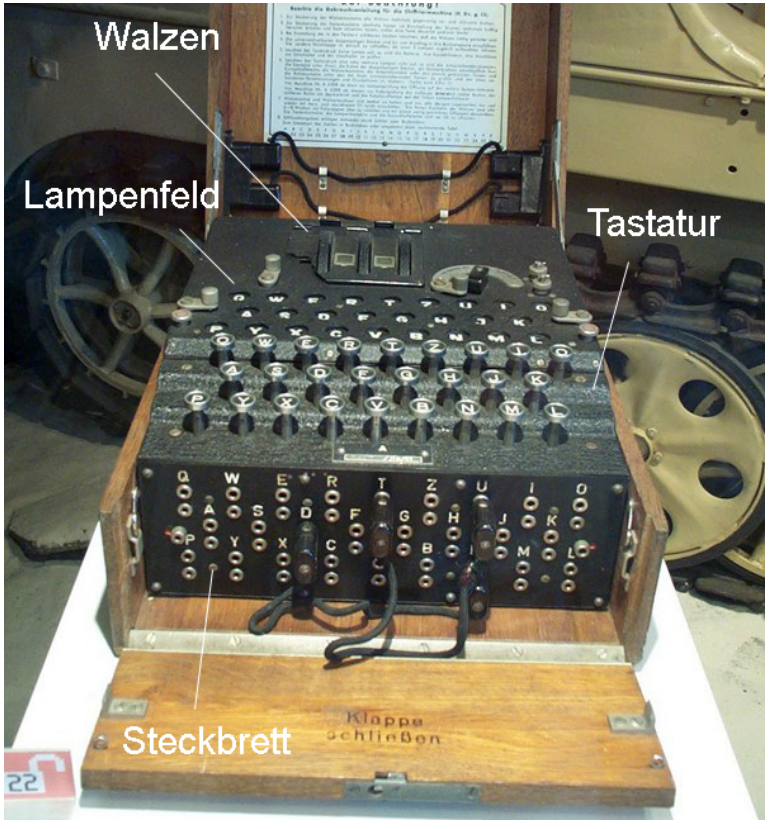
Gliederung

Entstehungsgeschichte

- Ab 1918: Mehrere Ansätze zum Bau von Rotormaschinen zur Verschlüsselung
- Arthur Scherbius reicht am 23.2.1918 Patent für die Enigma ein
- Kommerzielle und militärische Variante
- 1923 enthüllt Churchill Geheimnis um Entschlüsselung des Zimmermann-Telegramms

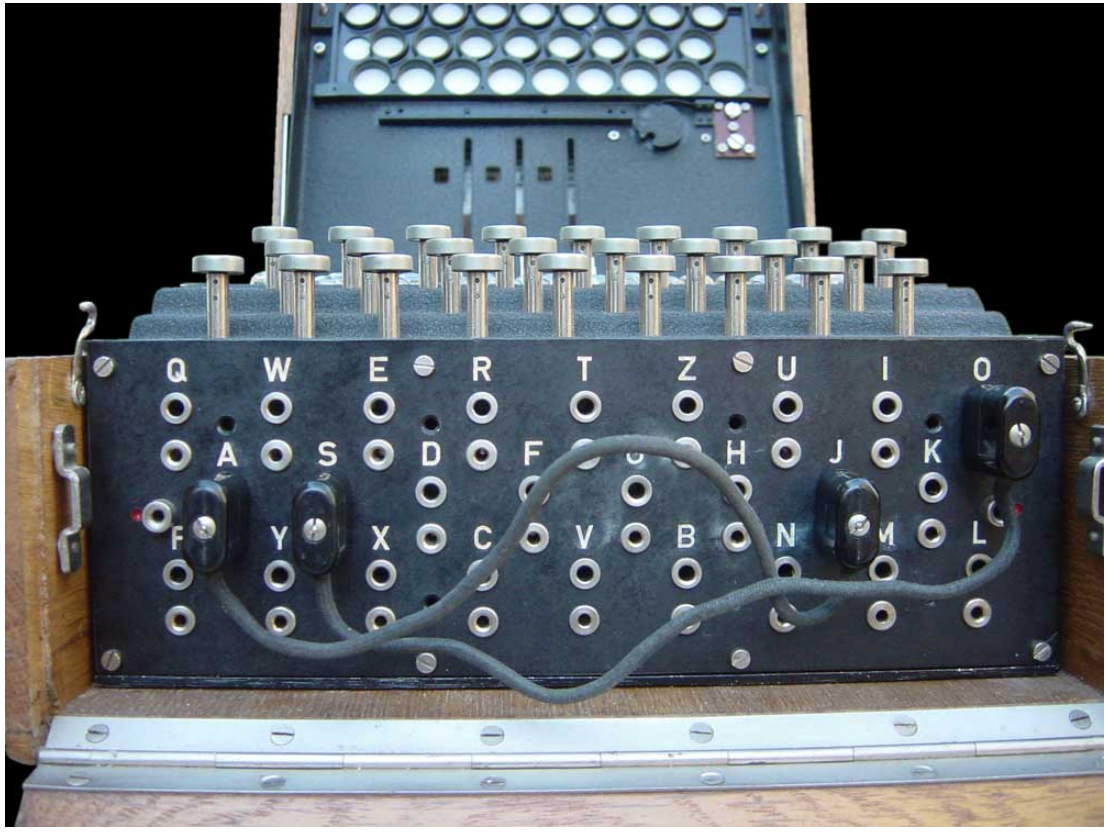
Abbildung: Arthur Scherbius

Die Enigma



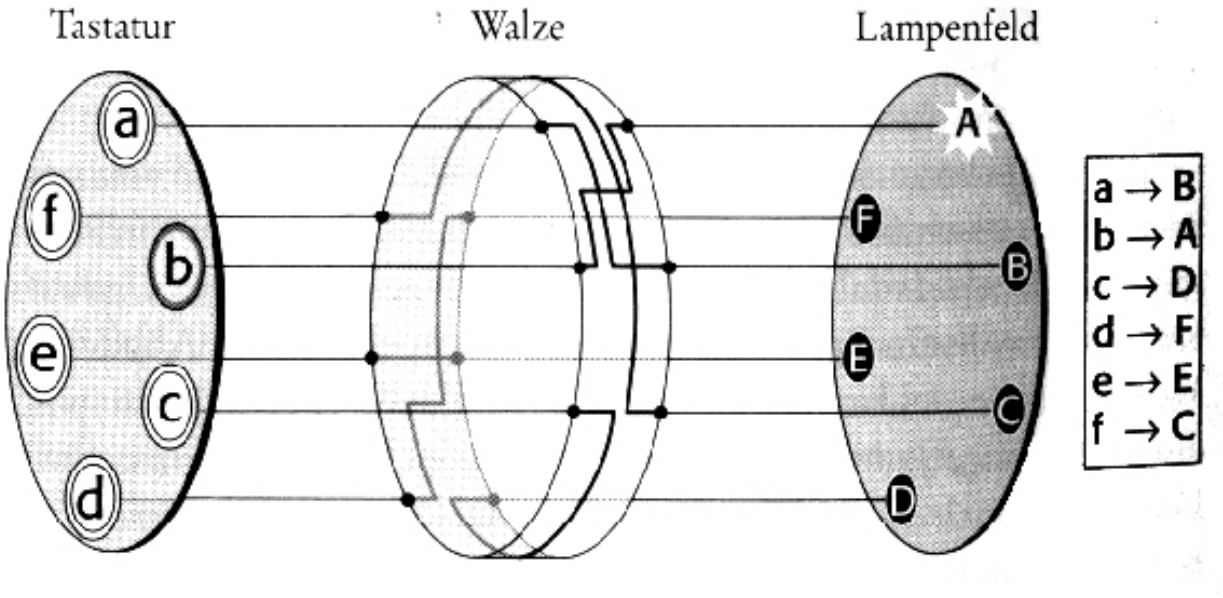
Batteriebetriebene, handliche elektrische Rotorchiffriermaschine

Steckbrett



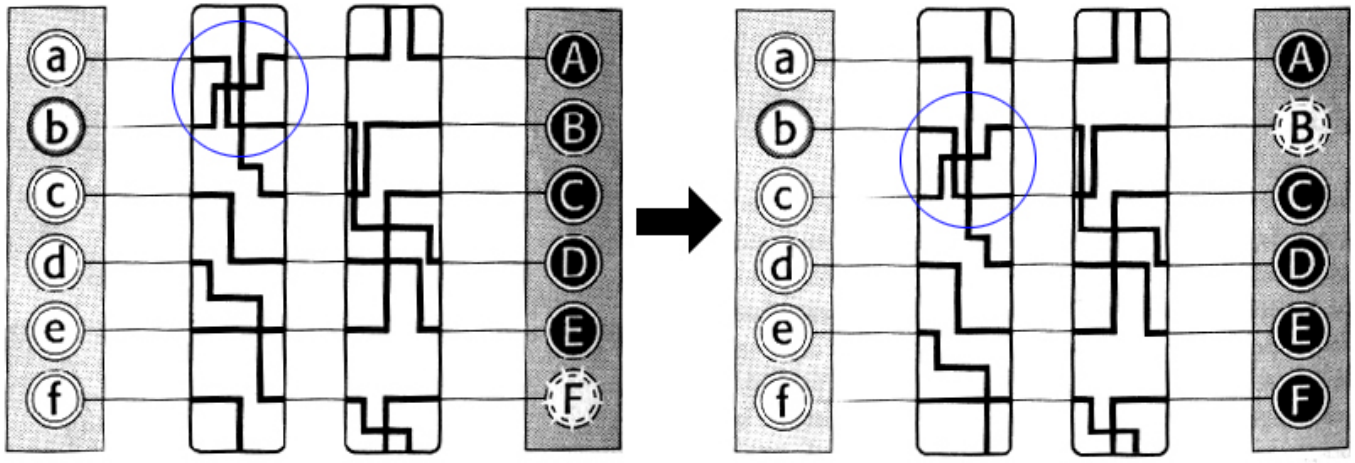
- Vertauschung von Buchstaben durch Verkabelung
- **Monoalphabetische** Verschlüsselung durch diese Komponente

Walzen und Ringe



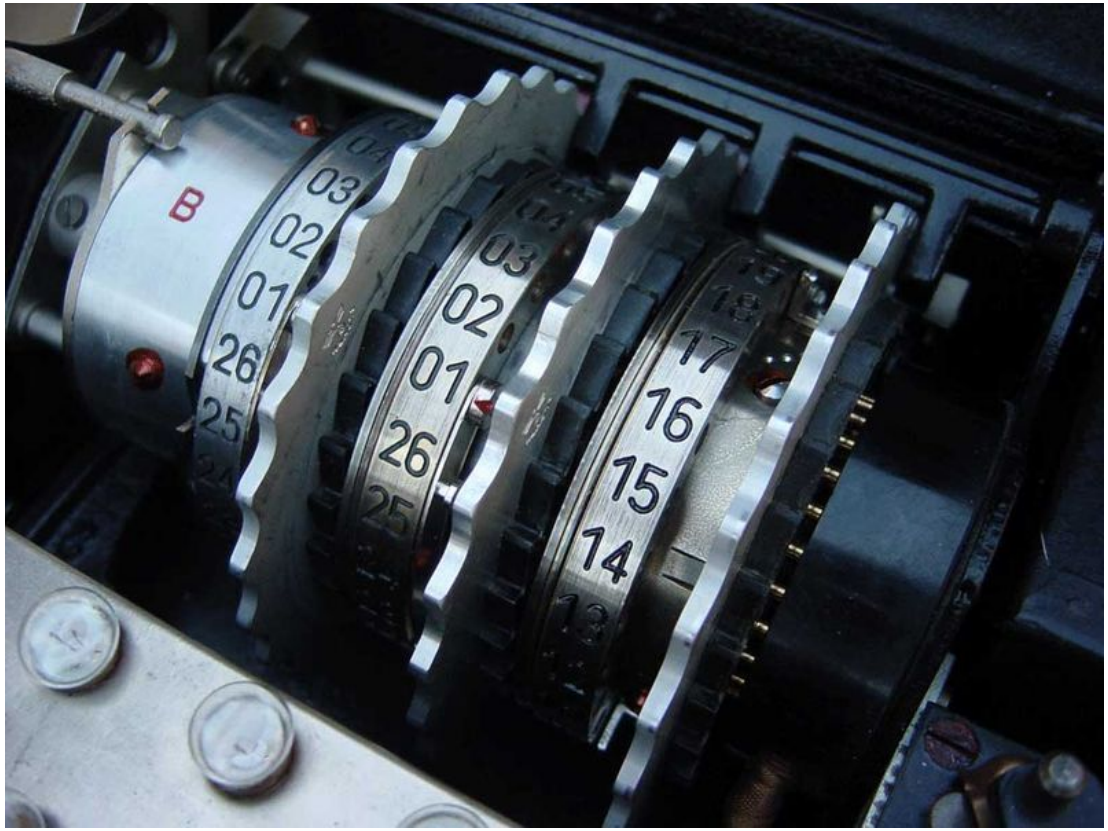
- 3 Rotationswalzen pro Maschine (später auch 4)
- Walzen austauschbar
- Bis zu 8 verschiedene Walzentypen
- Reihenfolge und verwendete Walzentypen müssen Sender und Empfänger bekannt sein

Walzen und Ringe



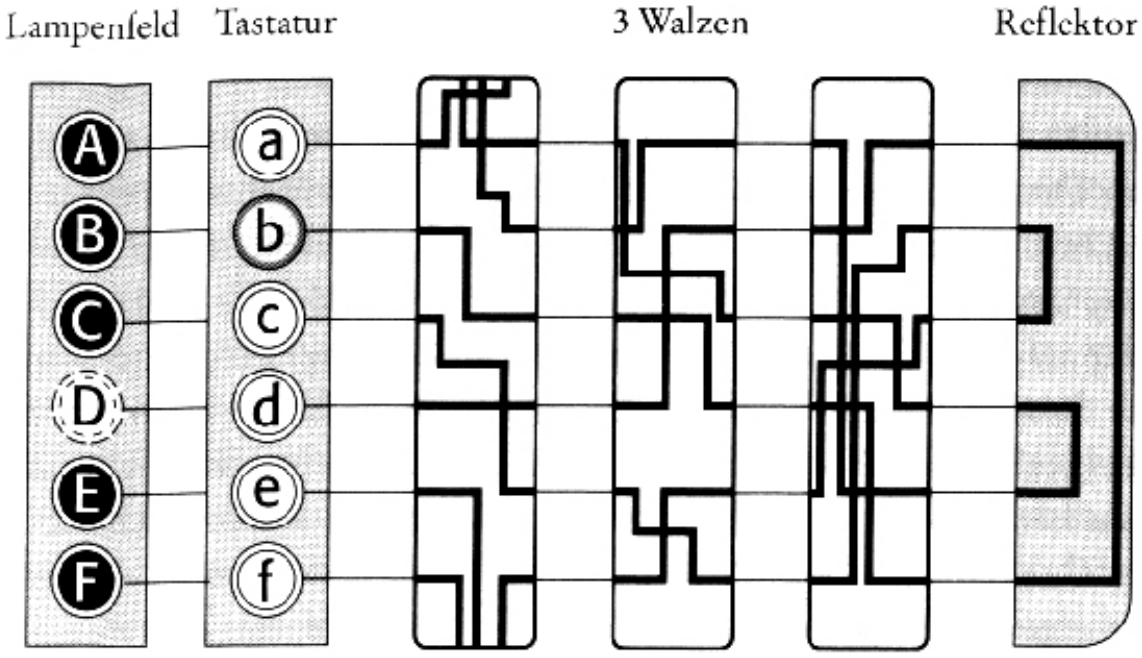
- Walzen rotieren während der Eingabe
- 1. Walze nach jedem Zeichen, 2. Walze alle 26 Zeichen, usw.
- **Polyalphabetische** Verschlüsselung

Walzen und Ringe



- Die Ziffern bzw. Buchstaben, die oben stehen, bestimmen die Walzenausgangsstellung
- Im Bild: 02 02 16 bzw. BBP

Umkehrwalze (Reflektor)



- Elektrischer Strom wird durch die Walzen wieder zurückgeleitet
- Vorteile:
  - Höherer Verschlüsselungsgrad
  - **Verschlüsselungsvorgang = Entschlüsselungsvorgang!**

Verwendung

- Schlüsselbücher und Tagesschlüssel
- Spruchschlüssel

Schlüsselbücher und Tagesschlüssel

Tag	UKW	Walzenlage	Ringstellung	---- Steckerverbindungen ----
31	B	I IV III	16 26 08	AD CN ET FL GI JV KZ PU QY WX
30	B	II V I	18 24 11	BN DZ EP FX GT HW IY OU QV RS
29	B	III I IV	01 17 22	AH BL CX DI ER FK GU NP OQ TY

- Schlüsselbücher mit *Tagesschlüsseln* für einen Monat
- Durften Feind nicht in die Hände gelangen
- Vorteil:
  Schlüssel für mehrere Monate auf wenigen Blättern Papier
- Nachteil:
  Ein einziger Tagesschlüssel für eine riesige Fülle an Nachrichten
  Lösung: Spruchschlüssel

Spruchschlüssel

- Funker wählt zufällige Walzenstellung
- Die Buchstaben, die bei Walzenstellung oben stehen, werden als *Spruchschlüssel* verwendet
- Spruchschlüssel wird mit Tagesschlüssel verschlüsselt
- Rest der Nachricht wird dann mit neuem Spruchschlüssel verschlüsselt

- Anfangs wurde der Spruchschlüssel verdoppelt übermittelt

Entschlüsselung

- 1931-1939 Polnische Entschlüsselungsarbeit
- 1939-1945 WWII und Betchley Park

Polnische Entschlüsselungsarbeit

- Entschlüsselung vorrangig im polnischen *Biuro Szyfrów*
- *Biuro Szyfrów* wirbt Mathematiker der Universität Posen an, u. a. Marian Rejewski
- Hans-Thilo Schmidt verkauft Frankreich Anleitungen der Enigma, welche Polen zukommen

Abbildung: Marian Rejewksi

Polnische Entschlüsselungsarbeit

- Rejewski erschließt interne Verdrahtung der Walzen
- Er nutzt die Spruchschlüsselverdoppelung aus, um Tagesschlüssel zu rekonstruieren
  $\Rightarrow$ Divide & Conquer: Komplexitätsreduktion durch Trennung von Steck- und Walzenkonfiguration!

Polnische Entschlüsselungsarbeit

Beispiel Kettenbildung:

- Abgehörte Spruchschlüssel:
  `LOK RGM, MQR XZH, JBG MOK, DFO PWE`
  Paarung von Zeichen 1 und 4:
  `(L, R), (M, X), (J, M), (D, P)`

erster Buchstabe	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
vierter Buchstabe				P									M					R	X							

Polnische Entschlüsselungsarbeit

Beispiel Kettenbildung:

- Abgehörte Spruchschlüssel:
  `LOK RGM, MQR XZH, JBG MOK, DFO PWE`
  Paarung von Zeichen 1 und 4:
  `(L, R), (M, X), (J, M), (D, P)`

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

Polnische Entschlüsselungsarbeit

Beispiel Kettenbildung:

- Abgehörte Spruchschlüssel:
  `LOK RGM, MQR XZH, JBG MOK, DFO PWE`
  Paarung von Zeichen 1 und 4:
  `(L, R), (M, X), (J, M), (D, P)`

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

- Kettenbildung

A → F → W → A	3 Verknüpfungen
B → Q → Z → T → V → E → L → R → I → B	9 Verknüpfungen
C → H → S → O → Y → D → P → C	7 Verknüpfungen
J → M → X → G → K → N → U → J	7 Verknüpfungen

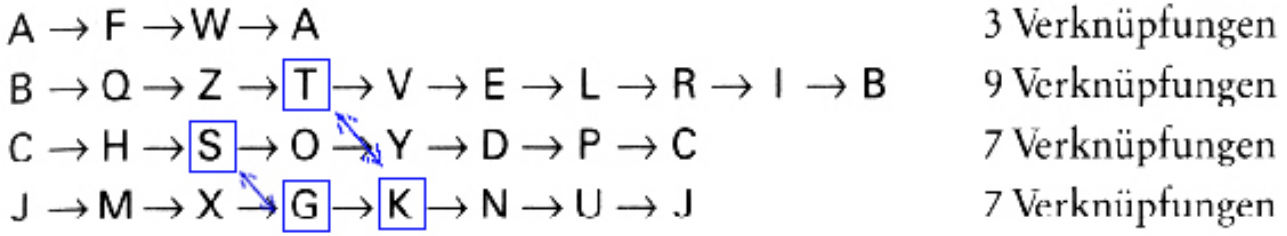
Polnische Entschlüsselungsarbeit

Beispiel Kettenbildung:

- Abgehörte Spruchschlüssel:
  `LOK RGM, MQR XZH, JBG MOK, DFO PWE`
  Paarung von Zeichen 1 und 4:
  `(L, R), (M, X), (J, M), (D, P)`

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

- Kettenbildung (Streckbrettverbindung spielen keine Rolle!)



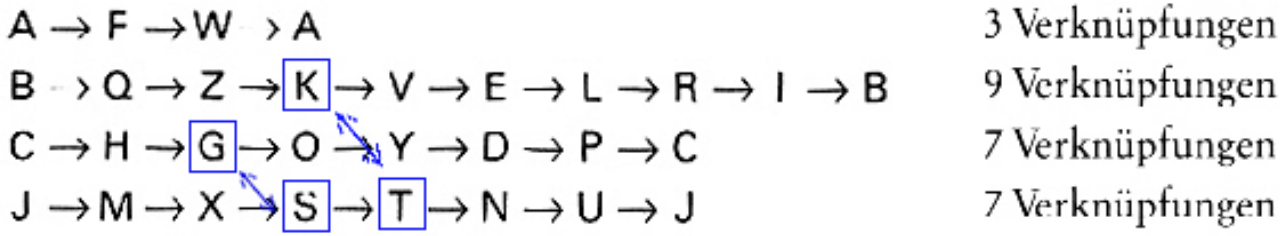
Polnische Entschlüsselungsarbeit

Beispiel Kettenbildung:

- Abgehörte Spruchschlüssel:
  `LOK RGM, MQR XZH, JBG MOK, DFO PWE`
  Paarung von Zeichen 1 und 4:
  `(L, R), (M, X), (J, M), (D, P)`

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

- Kettenbildung (Streckbrettverbindung spielen keine Rolle!)



Polnische Entschlüsselungsarbeit

- Steckerverbindungen zu finden ist mit gefundenem Tagesschlüssel einfach
- Entwicklung von Entschlüsselungsmaschinen: *Bomba*, *Zyklometer*
- Aber: Polnische Entschlüsselung schlägt bei Einführung neuer Walzen und weiterer Steckverbindungen fehl (Ende 1938)
- Polen geben Ergebnisse ihrer Forschung im Juli 1939 an die Briten und Frankreich weiter

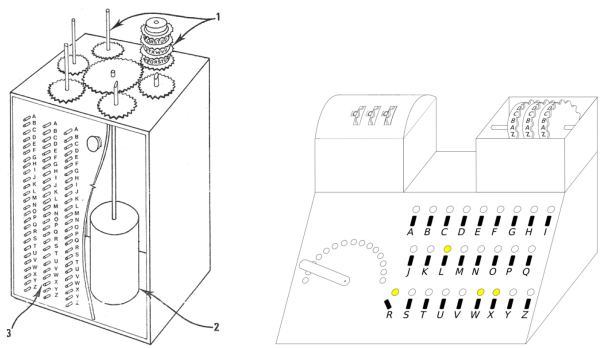


Abbildung: Bomba und Zyklometer

WWII und Bletchley Park

- Briten setzen ab Herbst 1939 Arbeit der Polen fort
- Zunächst Ausnutzung von einfach zu erratenden Spruchschlüsseln, *cillies*
- Ebenso wurden erbeutete Tagesschlüsselsätze verwendet

Cribs

- Turing: Annahme wahrscheinlicher Wörter im übermittelten Text, sog. *Cribs*
- Ausnutzung der *Invultorik* der Enigma
- Invultorik: Kein Buchstabe kann in sich selbst verschlüsselt werden
- Automatisierung der Entschlüsselung durch *Turing-Bombe*

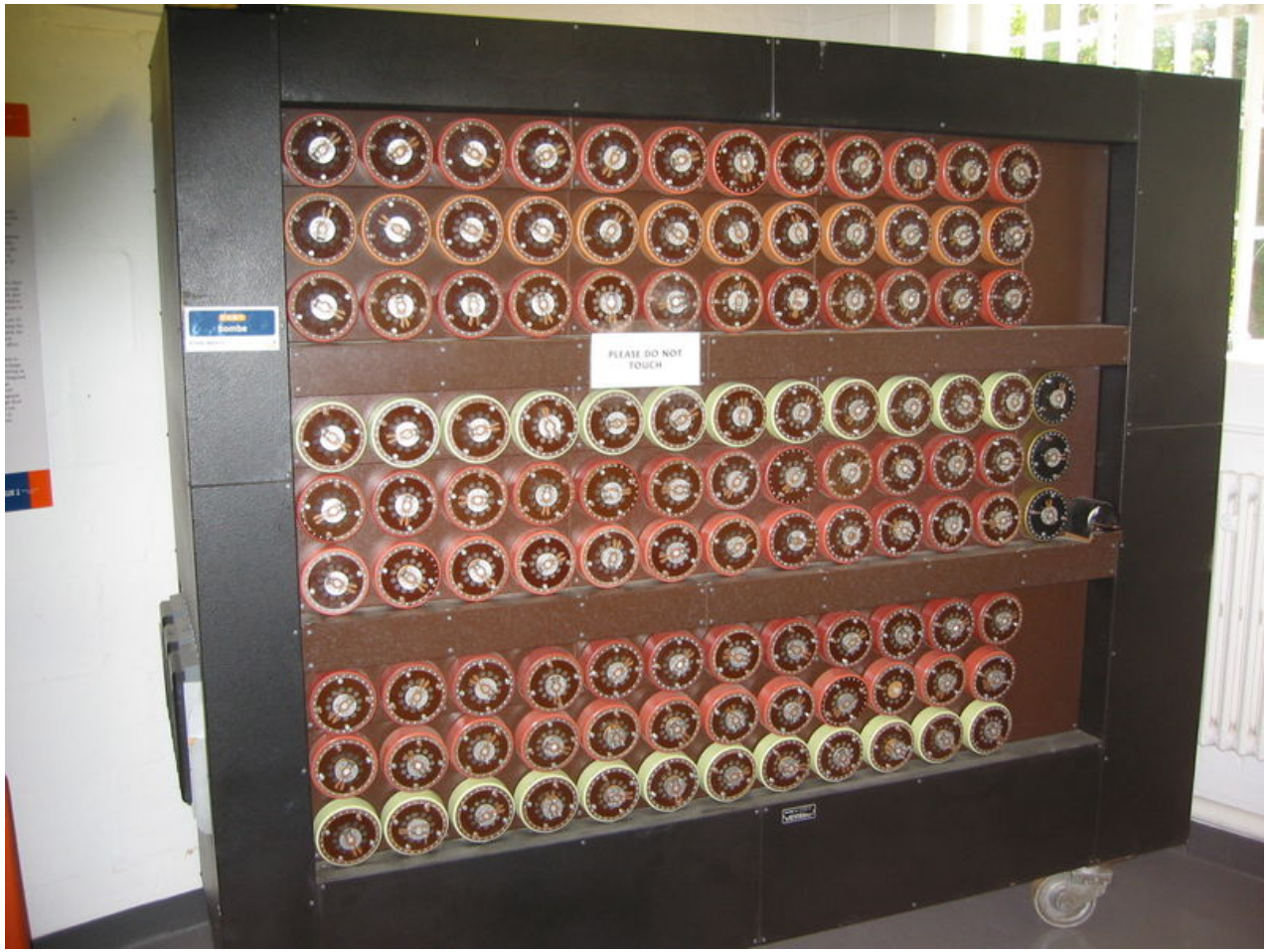
Abbildung: Alan Turing

Beispiel: Cribs

```
  BHNCXSEQKOBIIODWFBTZGCYEHQQJEWOYNBDXHQBALHTSSDPWGW
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
  BHNCXSEQKOBIIODWFBTZGCYEHQQJEWOYNBDXHQBALHTSSDPWGW
```

Turing-Bombe

- Automatisierung der Entschlüsselung durch die *Turing-Bombe*



Bedeutung der Verschlüsselung

- Im zweiten Weltkrieg gewann die Kommunikation zwischen den Truppenteilen an Bedeutung
- Blitzkriegtaktik der Deutschen
- Jede Division verfügte über ein eigenes Signalbatallion

Auswirkungen der Entschlüsselung

- Codename *Ultra*: Informationsgewinnung durch Entschlüsselung
- Ultra-Informationen wurden genutzt bei:
  - Battle of Britain (1940)
  - Afrikafeldzug (1941)
  - Deutsche Invasion in Griechenland (1941)
  - Vor allem: Seeschlachten zwischen England und Deutschland
- Ohne Entschlüsselung hätte der Krieg womöglich 2-3 Jahre länger gedauert
  - Mehr Tote auf allen Seiten
  - Atombombe auf Deutschland?
- Große Leistung der Engländer: Geheimhaltung von Ultra bis in die 1970er

Weiterführende Literatur

- **Historischer Roman**
  - Robert Harris - *Enigma*
- **Bletchley Park**
  - Gordon Welchman - *The Hut Six Story*
- **Allgemein**
  - Simon Singh - *Geheime Botschaften*
  - David Kahn - *Codebreakers*
  - Deutsche und englische Wikipediaartikel