Enigma

PD Dr. Reinhard Bündgen
buendgen@de.ibm.com

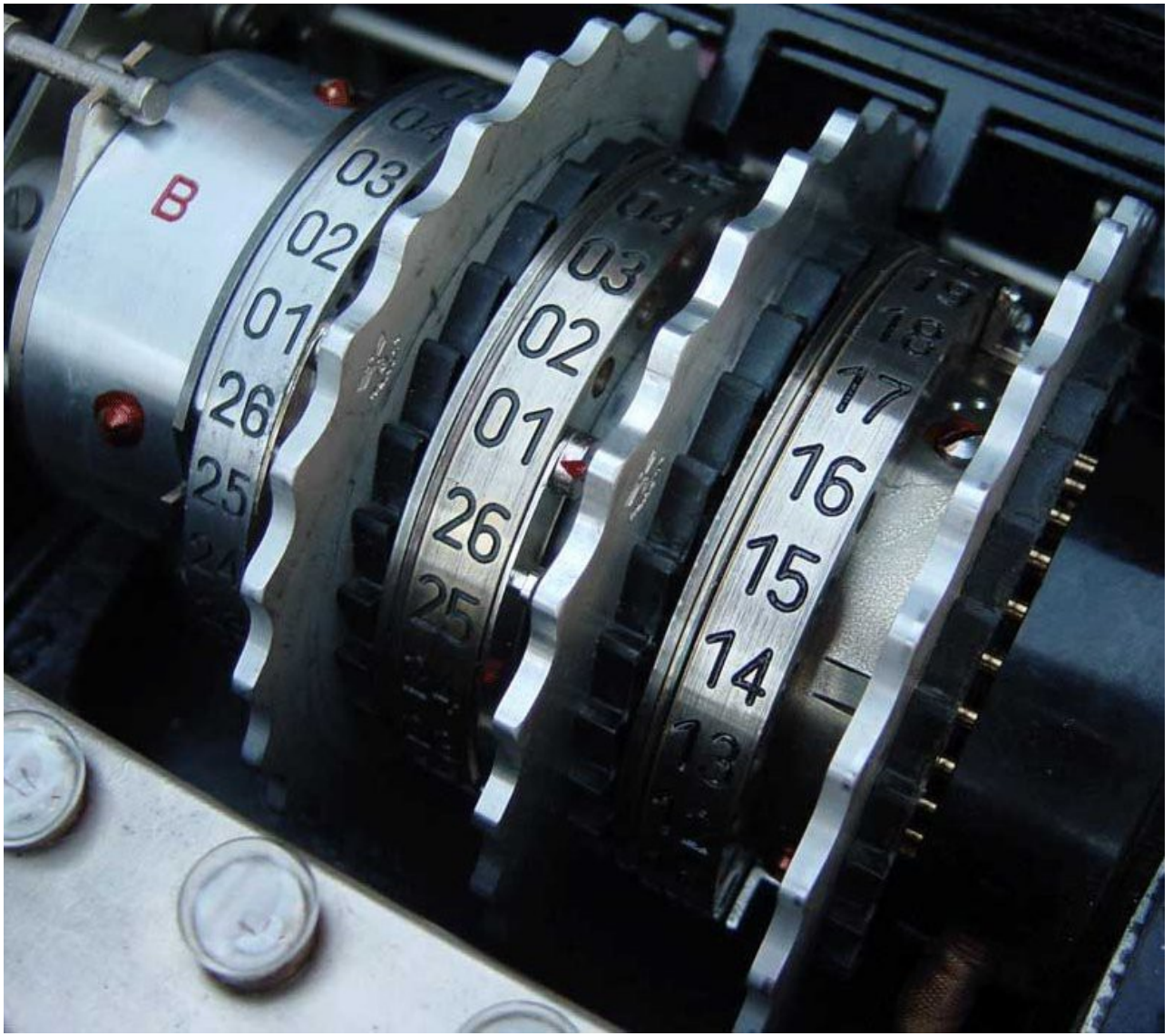
Bilder und Zeichnungen sind dem deutschen Wikipediaartikel über „Enigma (Maschine)“ entnommen, sie unterliegen den jeweiligen dort beschriebenen Lizenzen

Allgemeines

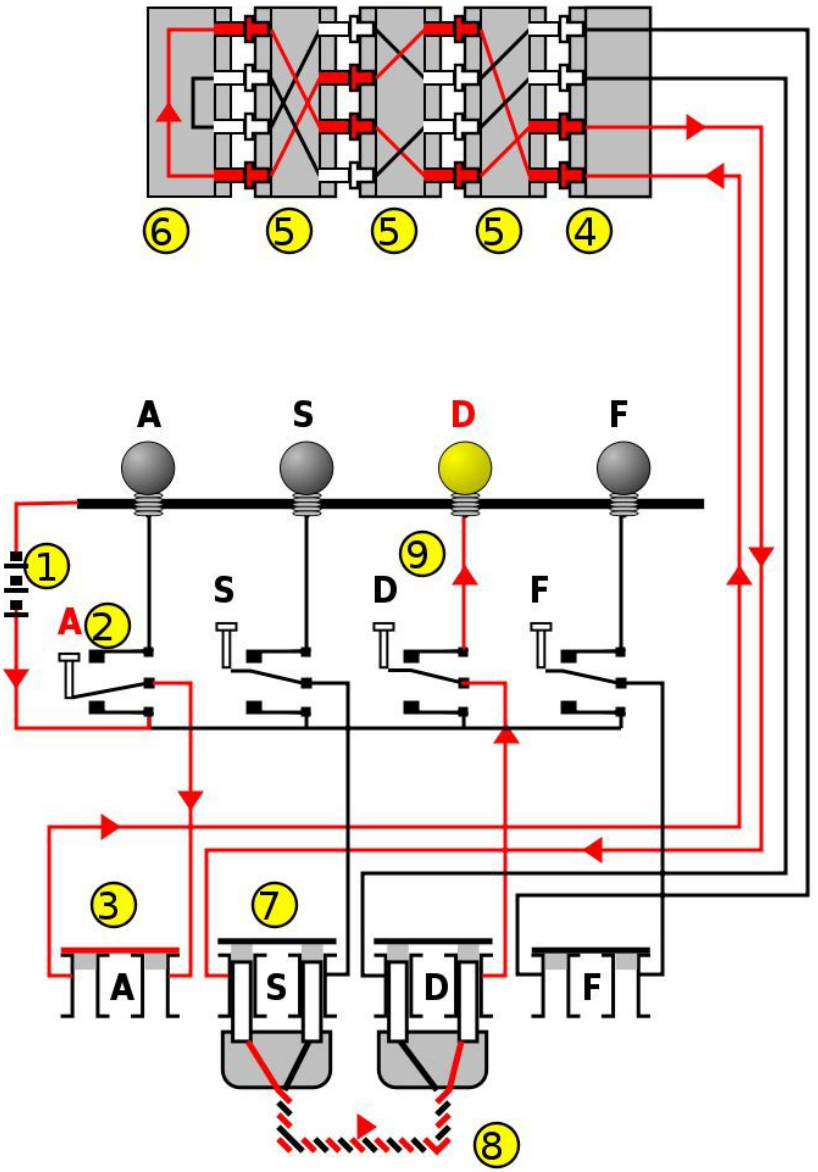
- Elektromechanische Rotor-Chiffriermaschine
- Rotor-Prinzip erfunden etwa gleichzeitig erfunden von Edward H. Hebern (USA), Arthur Scherbius (D), Hugo Koch (NL), Arvid G. Damm (S) 1917-1919
- galt als unknackbar
- ab 1926 bei der dt. Wehrmacht im Einsatz
- erste Entschlüsselungen durch Polen (Rejewski) , später durch Briten (Bletchley Park)
- Maße ca 12 kg, LxBxH: 340mmx280mmx150mm
- Verschieden Varianten
  - 26 Zeichen: A-Z
  - 3 oder 4 aus 5 bis 8 Rotoren, 2 Umkehrwalzen, bis zu 13 Steckerverbindungen

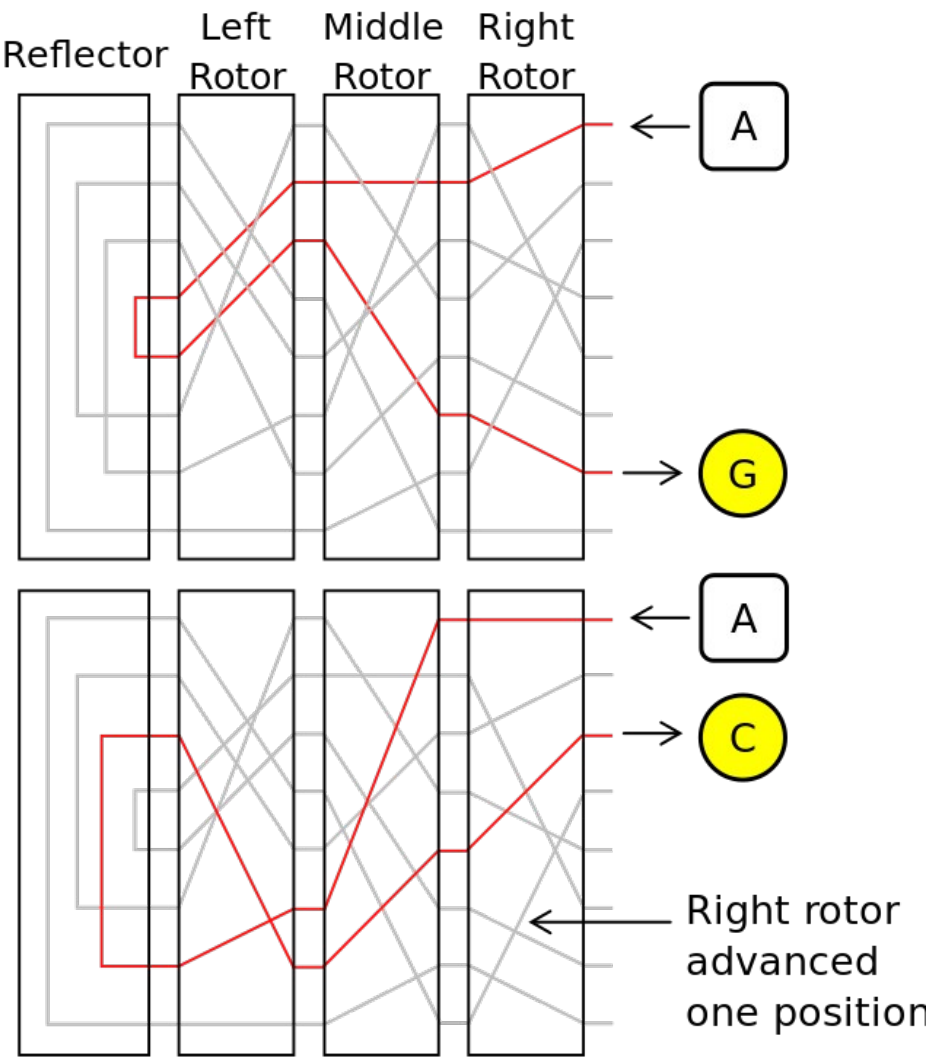
Vollständiges Gerät

Walzen



Vereinfachtes Schema (4 Buchstaben)





Nutzung der Enigma (Beispiel)

Schlüsseltafel – Abgaben pro Tag:

- Umkehrwalze (B oder C)
- Liste der 3 gewählten Walzen (I, II, III, IV, V)
- 3 Ringstellungen, die bestimmen bei welchem Buchstaben der Übertrag erfolgt
- Steckerverbindungen (z.B 10 Stück)

Pro Spruch

- 3 zufällige Walzenstellungen (sichtbare Nummer neben Walze)
- zufälliger dreistelliger Spruchschlüssel
- Spruchkopf: Zeit – Textlänge – Walzenstellung verschlüsselter Spruchschlüssel –
  - z.B 2230 – 214 – QWE EGW –
  - Spruchkopf wird in Klartext der Meldung vorangestellt

Kenngruppentabelle: pro Tag 3 Kenngruppenbuchstaben

- wurden beliebig permutiert und um 2 Füllbuchstaben ergänzt und folgten unverschlüsselt dem Spruchkopf
- Aufgabe: Integritätscheck

Maximale Spruchlänge: 250 Zeichen

Theoretischer Schlüsselraum

- Walzenwahl
  - 2 UKWs, 3 aus 5 Walzen: 2•5•4•3= 120
- Ringstellungen
  - 2 Überträge, da UKW fest: 26^2=676
  - 3. Übertrag effektlos, da UKW fest
- Walzenstellungen
  - 3 Walzen: 26^3=17576 (-26^2 wegen einer Anomalie des Fortschaltmechanismus: 16900)
- Steckerverbindungen
  - mit bis zu 13 Steckern: ca 150 • 10^{12}
- insgesamt: ca 2 • 10^{23} das entspricht etwa 77 bit

Analyse I

- fixe Steckerverbindungen entsprechen monoalphabetischer Chiffre
  - kann bei gegebenem Restschlüssel mit statistischer Analyse geknackt werden
- Ringstellung
  - 1. Übertrag alle 26 Zeichen
    - monoalphabetische Chiffre über Passagen von bis zu 26 Zeichen
  - 2. Übertag alle 25 • 26 Zeichen:
    - Periodenlänge 650
    - findet wegen max Spruchlänge 250 selten statt

Analyse II

- Umkehrwalze (elektrische Eigenschaften)
  - Strom wird durch Walzen zurückgeleitet
    - erhoffte Steigerung der Sicherheit: jede Walze wird 2 Mal genutzt
    - sei enc_w die Verschlüsselung durch die Walzen
    - involutorische Permutation: $enc_w(enc_w(a)) = a$ für alle a B∑
      - $enc_w = dec_w$
    - fixpunktfreie Permutation: $enc_w(a) \neq a$ für alle a B∑
      - kein Buchstabe kann auf sich selbst abgebildet werden
    - nur 25!! = 1•3•...•23•25 (ca $8 \cdot 10^{12}$) erlaubte Permutationen
    - anstatt 26! (ca $4 \cdot 10^{26}$)
    - es gilt: $((|\sum|-1)!!)^2 < |\sum|!$
- Stecker
  - vertauschen je zwei Buchstaben
    - involutorische Permutation (nicht fixpunktfrei)
      - sei enc_s die Verschlüsselung durch die Stecker
      - $enc_s(enc_s(a)) = a$ für alle a B∑
- Enigma-Verschlüsselung: $enc_E = enc_s$ Yenc_w Yenc_s
  - ist involutorisch
    - $enc_s(enc_w(enc_s(enc_s(enc_w(enc_s(a)))))) = enc_s(enc_w(enc_w(enc_s(a)))) = enc_s(enc_s(a)) = a$
  - es gilt $enc_E(a) \neq a$ für alle a B∑
    - Fall 1 $enc_s(a) = a$: dann $enc_E(a) = enc_w(a)$ ist fixpunktfrei - Widerspruch
    - Fall 2 $enc_s(a) \neq a$, dann müsste gelten $enc_w(enc_s(a)) = enc_s^{-1}(a) = enc_s(a)$, das wäre auch ein Widerspruch zu enc_w fixpunktfrei

Entzifferung

- Erste Erfolge 1932 den Polen Marian Rejwski mit einer einfachen Version der Enigma

- im Krieg in Bletchtley Park
  - „Bomben“ simulierten parallel viele Enigmazustände
    - entwickelt von Alan Turing
    - bei 26 Zuständen / Umdrehung und 64 U/min: <11h für vollständige Suche
    - bei Kriegsende: 210 „Bomben“
  - Suche nach erwarteten Wörtern („cribs“)
  - sich wiederholenden Standardtexten