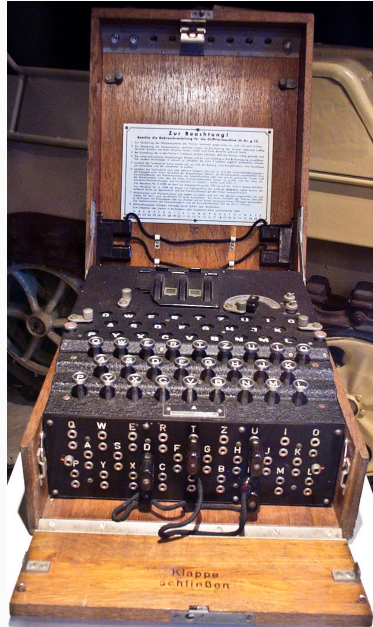


Die Enigma

Grundlagen

- Maschinell durchgeführtes Verschlüsselungsverfahren
- Erfunden von Arthur Scherbius (1918)
- Zunächst zur zivilen Nutzung gedacht
- Militärisches Interesse ab Mitte der 1920er



- Verdrahtete, drehbaren Walzen mit 26 Kontakten auf jeder Seite
 - Weitschaltung vergleichbar mit einem analogen Kilometerzähler
 - Reihenfolge der Walzen veränderbar
- Steckerbrett für Buchstabenvertauschungen
- Tastatur und Leuchtfeld
 - Eingabe und Ausgabe der Botschaft

Video :-)

- Bastle (yeah!) die Papier-Enigma
- Entschlüssele die auf dem Blatt angegebene Beispielnachricht

- Anzahl möglicher Walzenlagen: $3! = 6$
- Anzahl möglicher Anfangsstellungen: $26^3 = 17576$
- Anzahl möglicher Steckerverbindungen (bei 6 Steckern):
$$100.391.791.500 = \frac{(26 \cdot 25) \cdot (24 \cdot 23) \cdot (22 \cdot 21) \cdot (20 \cdot 19) \cdot (18 \cdot 17) \cdot (16 \cdot 15)}{2^6 \cdot 6!}$$
- Insgesamt rund 10^{16} mögliche Schlüssel
- Weiterentwicklungen der Enigma erhöhten die Zahl der Walzen und der Steckerverbindungen

- Bestimmte Regeln zur Benutzung schränkten die Sicherheit ein:
 - Eine Walze durfte nicht zwei Tage in Folge an der selben Position sein
 - Bestimmte Steckerverbindungen waren unzulässig
- Der Reflektor schwächte die Verschlüsselung
 - Buchstaben konnten nicht auf sich selbst abgebildet werden

- Erster erfolgreicher Angriff durch Marian Rejewski (polnischer Mathematiker)
 - Ausnutzung bekannter Textwiederholungen
 - Maschinelle Suche nach richtiger Walzenlage (Bomba)
- Britische Kryptoanalytiker unter Alan Turing
 - “wahrscheinliche Wörter” (cribs) als Anhaltspunkte
 - maschinelle Suche nach richtiger Walzenlage (Turing-Bombe)
 - Erbeutete Codebücher (insbesondere für die Marine-Enigma)

Noch ein Video :-)

Navajo-Codesprecher

- Maschinelle Verschlüsselung (Enigma etc.) kryptografisch stark
 - Aufwand zum Entziffern war hoch
- Aber: In der Praxis nicht immer einsetzbar
 - Gerät ist eher unhandlich
 - Ver- und Entschlüsseln ist zeitaufwändig

- US-amerikanischer Funkverkehr im Pazifikkrieg sollte geheim bleiben
 - Viele japanische Soldaten verstanden Englisch
 - Für maschinelle Verfahren fehlte Platz und Zeit
- Idee (Philip Johnston)
 - Rückgriff auf eine möglichst wenig gesprochene Sprache
 - Wahl fiel auf Mitglieder der Navajo

- Ausbildung zahlreicher Navajo-Codesprecher
- Verwendung alternativer Wörter für militärische Fachbegriffe:
 - Schlachtschiff ↔ Wal
 - Offizier ↔ Kriegshäuptling
- Zusätzlich: Alphabetcode zum Buchstabieren von Ortsnamen etc.
- Das Vorgehen war außerordentlich erfolgreich
 - Bis zum Kriegsende nicht geknackt