Ein alter Hut im Wandel der Zeit

Geschichtlicher Abriss der Kryptographie

Linus Lüssing

Cryptoparty, 24. Jan. 2015, Chaotikum e.V. / Lübeck

Steganographie: Vorläufer der Kryptographie

steganós gráphein = ”bedeckt schreiben”
vs.
kryptós graphein = ”geheim schreiben”

- Beispiel Steganographie:
  Nachricht auf Kopfhaut von Sklaven tätowiert
- Soll den Griechen einen Sieg gegen die Perser beschert haben
  $\Rightarrow$ ca. 500 BC, laut Herodotus

Cäsar-Chiffre (I)

Bildquelle: Wikipedia, CC-BY-SA

- ca. 100 BC
- Wurde von Cäsar für seine militärischen Aktionen genutzt
- Substitutions-Chiffre
- Jeder Buchstabe wird durch genau ein anderes ersetzt

Cäsar-Chiffre (II)

Bildquelle: Wikipedia, CC-BY-SA

Beispiel:

- CAESAR, 13 Stellen rotiert $\Rightarrow$ LNJVNW
- ”Passwort”: 13 Stellen rotiert (ROT13)

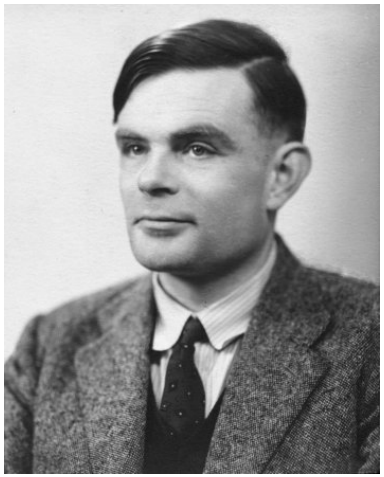
- Buchdruck, 15. Jh.
  $\Rightarrow$ Die Zensur durch politische+religöse Obrigkeit
- Wenig(er) Neuerungen in Kryptographie
- Mehr Steganographie
  $\Rightarrow$ Subtile/versteckte Nachrichten in Bild/Text

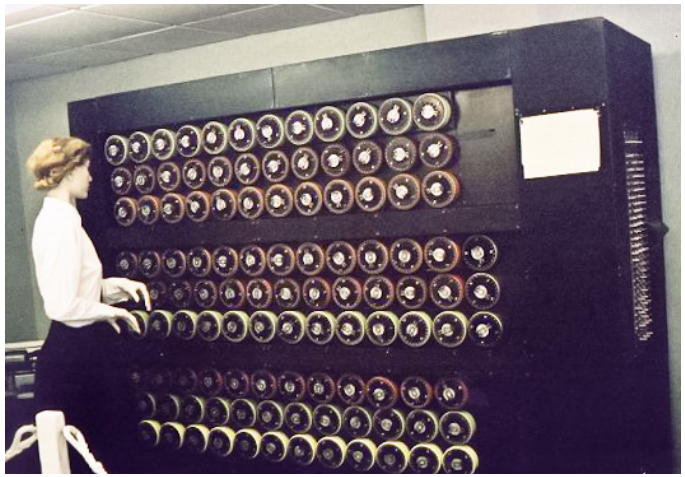
Enigma - Kryptographie

Bildquelle: Wikipedia, CC-BY-SA

- Zweiter Weltkrieg, deutsches Militär
- Anfang 20. Jahrhundert: Maschinen zur Verschlüsselung ”in Mode”
- viel mehr Möglichkeiten $\Rightarrow$ händisches Durchprobieren nicht möglich

Enigma - Kryptoanalyse





Bildquelle: Wikipedia, CC-BY-SA

- Große Fortschritte in der Verschlüsselungstheorie
  $\Rightarrow$ mathematische Anforderungen und Schwachstellen
- Aber auch:
  Elektromechanische Maschinen zum Entschlüsseln
  Turing-Bombe, Bletchley Park
  $\Rightarrow$ Vorläufer des Computers (Stichwort ”Turing-Maschine”)

Zusammenfassung

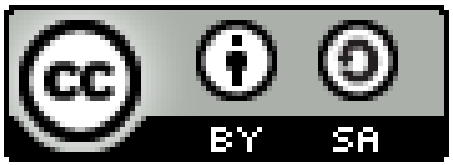
- ”Nichts neues:”
  $\Rightarrow$ Bedürfnis seit mehreren Jahrtausenden
  $\Rightarrow$ Zum eigenen Schutz gegen Verfolgung
- Großer Sprung im 20. Jh.
  $\Rightarrow$ Fernmeldeschreiber
  $\Rightarrow$ Robuste(re) Verfahren

Herausforderungen heute - Internet, anderes, Grenzen?

Lizenz

Bilderverzeichnis:

- https://en.wikipedia.org/wiki/File:Bust_of_Gaius_Iulius_Caesar_in_Naples.jpg
- https://en.wikipedia.org/wiki/File:Alan_Turing_photo.jpg
- https://de.wikipedia.org/wiki/Datei:TuringBombeBletchleyPark.jpg
- https://de.wikipedia.org/wiki/Datei:CipherDisk2000.jpg
- https://de.wikipedia.org/wiki/Datei:Enigma_Verkehrshaus_Luzern_cropped.jpg



Creative Commons, Attribution-ShareAlike

https://creativecommons.org/licenses/by-sa/4.0/