VL 17.6.15 12^{30}-14^{00}
M4

DIE ENIGMA

Aufbau und Prinzip

Idee: Die Maschine verwendet drei bewegliche Walzen und eine feste Umkehrwalze, die Permutationen aus S_{26} entsprechen und während der Verschlüsselung bewegt werden.

$\rightsquigarrow$ erhalte so für jeden Buchstaben ein neues Verschlüsselungsalphabet.

Def./Fakt: Bijektive Abb $\sigma: \{1, \dots, n\} \to \{1, \dots, n\}$ heißen Permutationen, man bezeichnet mit

$$S_n := \{\sigma \mid \sigma: \{1, \dots, n\} \to \{1, \dots, n\} \text{ bij.}\}$$

die Menge der Definitionen von n Elementen.

Mit der Verknüpfung

$$\circ: S_n \times S_n \to S_n$$
$$(\sigma, \tau) \mapsto \sigma \circ \tau \quad \text{wobei } \sigma \circ \tau(i) = \sigma(\tau(i))$$

wird $(S_n, \circ)$ zu einer (nichtabelschen) endl. Gruppe, der symmetrischen Gruppe von n Elementen

Konvention: Wir lassen $\circ$ weg, schreiben $\sigma\tau$ für $\sigma \circ \tau$. D.h. wir schreiben $(S_n, \circ)$ multiplikativ, lese $\sigma\tau\eta$ von "rechts nach links" (erst wird η angewendet).

Beachte: $(\sigma\tau\eta)^{-1} = \eta^{-1}\tau^{-1}\sigma^{-1}$

Bemerkung: Identifiziere $\{A, B, C, \dots, Z\}$ mit $\mathbb{Z}_{26} = \{\underline{0}, \underline{1}, \dots, \underline{25}\}$.

Vertauschen von Buchstaben $\hat{=}$ Permutation aus S_{26}.

Eine Walze der Enigma ist ca. 10cm im Durchmesser und hat auf beiden Seiten das Alphabet A, ..., Z stehen, wobei die Buchstaben rechts und links miteinander verkabelt sind. Diese innere Verdrahtung entspricht also einer festen Permutation $\sigma \in S_{26}$.
Es werden drei austauschbare Walzen (mit Perm. $\sigma_1, \sigma_2, \sigma_3 \in S_{26}$) verwendet.
Strom kann von rechts nach links durch diese Drähte fließen, kehrt an der Umkehrwalze um (entspricht Permutation $\tau \in S_{26}$), und fließt zurück von links nach rechts.
Die Maschine hat Tastenfeld mit Buchstaben A-Z.
Bei Druck einer Taste:

- die Walzen bewegen sich um einen Schritt weiter (wie ein Kilometerzähler!
  Nachdem die rechte Walze 26 Schritte gemacht hat, dreht sich die mittlere Walze etc)
- es fließt Strom durch den Walzenweg des gedrückten Buchstabens
- es leuchtet eine Anzeigelampe, die den kodierten Buchstaben anzeigt.

Beispiel: Papierenigma.

Schlüssel:
- Auswahl der Walzen (3 aus 4 oder 5 möglichen)
- Anfangsstellung der Walzen (Bsp: FMJ)
- zusätzliches Steckbrett
  (= stationäre Walze mit frei wählbarer Verdrahtung ↝ "Eingangspermutation")
- durch Verdrehen eines Ringes konnte auch i zu i+I ersetzt werden, für ein festes I.

Die Enigmagleichung (aufgestellt von Rejewski) für einen Klartextbuchstaben B mit Geheimbuchst. C lautet nun:

$$C = \upsilon^{-1} \circ S_z^{-1} \circ \tau \circ S_z \circ \upsilon\,(B)$$

τ: Permutation durch Umkehrwalze

S_z: Permutation durch die 3 Walzen nacheinander, $S_z = \upsilon_3 \circ \upsilon_2 \circ \upsilon_1$ (S_z hängt davon ab, die wievielte Taste wir drücken!)

υ: "innere Verdrahtung" durch zus. Steckbrett

Beachte: Eine Enigma kann keinen Buchstaben als sich selbst verschlüsseln
(Strom kann nicht "zu sich selbst" zurückfließen zur Quelle)

"Fixpunktfrei"

$\Rightarrow \tau(i) \neq i$ f.a. $i \in \{0, \dots, 25\}$

denn $\tau(i) = i \Rightarrow \upsilon^{-1} \circ S_z^{-1} \circ \tau \circ S_z \circ \upsilon(j) = j$ für $j = \upsilon^{-1} \circ S_z^{-1}(i)$

↝ Enigma verschlüsselt den Buchstaben als sich selbst.

Zur einfacheren Handhabung: τ wird als Involution gewählt, d.h. $\tau^2 = id$.

↝ Entschlüsseln = Verschlüsseln

"involutorisch"

Nun: von den $26! \approx 4 \cdot 10^{26}$ Permutation aus S_{26} bleiben nur $25!! = 25 \cdot 23 \cdot \ldots \cdot 3 \cdot 1 \approx 8 \cdot 10^{12}$ viele übrig, die fixpunktfrei & involutorisch sind

("echte involutorische Permutationen")

Beispiel $\Sigma = \{A, B, C, D\}$ Mögliche verschl. von ABCD

ABCD	ACBD	ADBC	CABD	CDBA	DBAC
BACD	ACDB	BDCA	CBAD	CBDA	DBCA
BCAD	ABDC	BDAC	CDAB	DABC	DCAB
BCDA	ADBC	BADC	CADB	DACB	DCBA

BCDA	CDAB	CBDA
BDAC	CADB	DCAB
BADC	CDBA	DCBA

Fixpunktfrei

echt involutorisch bleiben

BADC CDAB DCBA

Beispiel

BHEINKSQRVCXSKOEBIIAWFBTZGCYEHQQ

WETTERVORHERSAGE

WE

WETTERVORHERSAGE

WETTER

WETTERVORHERSAGE

WETTERVORHE

WETTERVORHERSAGE

WETTERVO

WETTERVORHERSAGE

WETTERVORHERSAGE

W

W

WETTERVORHERSAGE

etc