Kryptographie Anwesenheitsblatt 0 hhu Düsseldorf WiSe 2023/24

Keine Abgabe! Nur zur Besprechung in den Übungen am 11.10.2023

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Permutationen in S_{26}

Wieviele $\sigma \in S_{26}$ gibt es, die

(a) die Ordnung 2 haben (d. h. $\sigma(\sigma(n)) = n$ für alle $1 \leq n \leq 26$),

(b) höchstens k viele Fixpunkte ($1 \leq n \leq 26$ mit $\sigma(n) = n$) haben,

(c) keinen Zykel der Länge > 13 enthalten?

Aufgabe 2: Papier-Enigma

Basteln Sie die Papier-Enigma von der Webseite
`https://mckoss.com/posts/paper-enigma/paper-enigma-german.pdf`

(a) Verschlüsseln Sie damit (bei der angegebenen Walzenauswahl I-II-III: MCK) den Text "INVOLUTION"

(b) Welche der drei Klartexte können nicht am Anfang des von der Enigma in (a) erzeugten Geheimtextes GBDQQBHNWZTA... stehen, und warum nicht? WETTERBERICHT, OBERKOMMANDO, KEINEBESONDERENVORKOMMNISSE

Aufgabe 3: Mini-Enigma

Gegeben ist eine Enigma mit dem Alphabet $\sigma = \{A, E, H, N\}$ und mit zwei Walzen und einer Umkehrwalze. Bekannt ist der Klartext "AHNEHANNAHNAHEANNE", der damit zu "HAENAHEEHAEHANHEEN" verschlüsselt wurde.

(a) Geben Sie den Geheimtext an, den die Enigma (in derselben Anfangsstellung) zum Klartext "NAEHEANNA" ausgibt.

(b) Geben Sie eine "innere Verdrahtung" der Walzen an, mit der diese Art der Verschlüsselung erreicht werden kann.