Kryptography Presence sheet 0

hhu Düsseldorf
Winter term 23/24

Not to hand in! For oral discussion in the exercise class on 11.10.2023

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

Exercise 1: Permutations in S_{26}

How many $\sigma \in S_{26}$ are there which

(a) have order 2 (i. e. $\sigma(\sigma(n)) = n$ for all $1 \leq n \leq 26$),

(b) have at most k many fix points ($1 \leq n \leq 26$ with $\sigma(n) = n$),

(c) contain no cycle of length > 13?

Exercise 2: Paper-Enigma

Construct the paper-Enigma from the website
`https://mckoss.com/posts/paper-enigma/paper-enigma.pdf`

(a) Encrypt with it (choosing the given adjustment I-II-III: MCK of the rotors) the plain text "INVOLUTION"

(b) Which of the three plain texts can not be the beginning of the generated secret text GBDQQBHNWZTA... (from the Enigma in (a)), and why not? WETTERBERICHT, OBERKOMMANDO, KEINEBESONDERENVORKOMMNISSE

Exercise 3: Mini-Enigma

Given an Enigma with alphabet $\sigma = \{A, E, H, N\}$, two rotors and one Reflector. A plain text is known to be "AHNEHANNAHNAHEANNE", which has been encrypted to "HAENAHEE-HAEHANHEEN".

(a) Give the secret text which is generated by the Enigma (in the same adjustment) for the plain text "NAEHEANNA".

(b) Give a possible "inner wiring" of the rotors, such that this encryption can be reached by the Enigma.