Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 1 (18.10.2024)

Bemerkungen:

(1) Zur Lösung einer Kryptographie-Aufgabe gehört auch eine (kurze) Darstellung des Lösungswegs.
(2) Mit **P** werden Präsenzaufgaben, mit **H** Hausaufgaben bezeichnet.
(3) Abgabe der Hausaufgaben bis Freitag, 25.10.2024 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P1: Entschlüssle folgenden CAESAR-chiffrierten Text.
`ERIEDDUDISXUYDERIJUHDWUVKDAUBYCJKDDUBRBUYRJUIYCCUHTKDAUB`

Aufgabe P2: Maximilian schreibt an Johannes eine E-Mail mit folgendem Inhalt:

```
NOVVY QYNOXXED,
ED IOC DTNYEX, BODD BG GXDECE NYTNMEPF WPF GXD REPECX UYXXFEDF. CETNF
YCPSPXEVV ROXBEX IPC OGTN, BODD BG GXD EPXEX UVEPXEX BGBEVDOTU OVD
HYCKECEPFGXS GXDECEC DTNYFFVOXBCEPDE SEDTNEXUF NODF. FOFDOETNVPTN UOXX
WOX OGR PNW OGTN DZPEVEX. NECMVPTNEX BOXU BORGEC!
HPEVE SCGEDDE, WOJPWPVPOX
```

Entschlüssle den Text. (Hinweis: ZNFP)

Aufgabe P3: Entschlüssle folgenden TRANSMAT-verschlüsselten Text:
`IURREHRMATEBERENERINTHWJEHHDNIOUECRUNNTDIJDCEAHDERHRNIDANECDIATEEENHNFRTDTREAICMKKEAE`
(Hinweis: `FPUYHRFFRYQERVZNYIVRE`)

Aufgabe P4: Entschlüssle folgenden TRANSSPA-verschlüsselten Text:
`TUELECAEBAZHEATSETODDFTTITKFGHRINNOGETNSECUNT`
(Hinweis: `FPUYHRFFRYJBEGBXGBORE`)

Datei: ki_u1.tex. Version vom 17.10.2024

Hausaufgaben

Aufgabe H1: Entschlüssle folgenden CAESAR-chiffrierten Text. Wer ist der Autor? Wo steht der Text?

```
zp ubtlybz h ubtlyvybt i, j kpmmlyluapht tlapaby, i la j zljbukbt h jvunybp kpjbuaby,
zpu tpubz, pujvunybp; pwzbt h tvkbsbt hwwlsshtbz.
```

(Hinweis: `YNGRVAVFPUREGRKG`)

Aufgabe H2: Entschlüssle folgenden MASC-chiffrierten Text und bestimme ein Schlüsselwort:

```
AOH TINZC AHB IHVHIB OBC HOVH JOZQSOFNH OZZTINZC OU EHEHVBICM MD AHZ OZZTINZC AHB
WALBBHDB. AHB WALBBHDB OZZTINZC UDBB UIV ZHSICOGOHZHV: MHNV PINZH JIZ HZ DVCHZ
JHEB, NHOBBC HB. GWV AOHBHV MHNV PINZHV GHZRZIFNCH HZ ISSHOV BOHRHV PINZH RHO AHZ
NDHRBFNHV VLUXNH QISLXBW DVA MJHO JHOCHZH PINZH RHO AHZ OVCHZHBBIVCHV NHKH QOZQH,
ISBW AIDHZCH AOH OZZTINZC HOV PINZ. IDBBHZAHU JDBBCH WALBBHDB BHOV MOHS, HZ
JDBBCH VOFNC, WR HZ HB HZZHOFNHV JDHZAH, IRHZ OUUHZNOV NICCH HZ HOV MOHS, HOV
QWVQZHCHB MOHS - OCNIQI. AOH OZZTINZC AHB IHVHIB JIZ HOVH TSDFNC, HZ JDBBCH VOFNC,
 JW AIB HVAH BHOV JOZA. AIB MOHS JIZ VOFNCB JHOCHZ ISB HOVH GHZNHOBBDVE. AOH EIVMH
JHSC JIZ XWCHVCOHSSH NHOUIC TDHZ ONV, IHVHIB NICCH QHOVH NHOUIC UHNZ.
```

(Hinweis: `QNFJBEGTRTRAFNGMXBZZGVZXYNEGRKGIBE`)

Aufgabe H3: Sei $\mathcal{A} = \{\mathrm{A}, \ldots, \mathrm{Z}\}$ die Menge der Großbuchstaben. Bei der MASC-Verschlüsselung liefert jedes (aus Großbuchstaben bestehende) Wort w eine Permutation f_w von $\mathcal{A}$, d.h. eine bijektive Abbildung $f_w : \mathcal{A} \to \mathcal{A}$. Ein Fixpunkt von f_w ist ein Buchstabe a mit $f_w(a) = a$.

(1) Beschreibe f_{AG}, f_{BG}, f_{GA}, f_{GB}, f_{NO} und f_{ON} durch Tabellen und bestimme die Fixpunkte.
(2) Bestimme Wörter w_1, w_2 mit $f_{w_1} = f_{\mathrm{NO}} \circ f_{\mathrm{ON}}$ und $f_{w_2} = f_{\mathrm{ON}} \circ f_{\mathrm{NO}}$.
(3) Bestimme alle Wörter w der Länge 2, sodass f_w genau 3 Fixpunkte besitzt.

Aufgabe H4: Entschlüssle folgenden TRANSSPA-verschlüsselten Text:

```
HISEBDRDRLRNDEIDEGGLSUNIHRSSTDNSSGBCHHIKTWSTSCAGEBASIESNEICCRNFNETUENCEOHTTEDTET
UHTWGUIEBEZHSNSRLAWIAAIDASEENEDAARE
```

(Hinweis: `NYYRFCNYGRAFVAQTYRVPUYNAT`)