# Kryptologie

**Übung, LVA 405.321**
**C. Fuchs**

## 3. Übungsblatt, SS 2022

**23.03.2022**

1. Ein Angreifer fängt die Nachricht "WKNCCHSSJH" ab. Weiters weiß er, dass das erste Wort "GIVE" ist. Gesucht ist die Verschlüsselungsmatrix (eine $2\times 2$-Matrix) $A$ über $\mathbb{Z}_{26}$. Dabei sei $\Sigma = \{A, B, \ldots, Z\}$ mit der Identifikation $A = 0, B = 1, \ldots, Z = 25$.
   (Hinweis: Die Matrix $A$ gibt es! Man reduziere das Problem zuerst auf $\mathbb{Z}_{13}$ und hebe dann die Lösung auf $\mathbb{Z}_{26}$. Der verschlüsselte Text ist englisch und sinnvoll!)

2. Zur Verschlüsselung des Textes im File `krypto_S3A2.txt` wurde eine affin lineare Blockchiffre benutzt, das Alphabet ist $\{A, B, C, \ldots, Z\}$ und wird mit den Zahlenwerten $\{0, 1, \ldots, 25\}$ identifiziert, d. h.

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \longmapsto A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

   mit $A \in \mathrm{GL}_2(\mathbb{Z}_{26})$ und $b_1, b_2 \in \mathbb{Z}_{26}$. Bestimme $A, b_1, b_2$. Verwende dabei die folgende Häufigkeitstabelle:

| EN | ER | CH | TE | DE | ND | EI | IE | IN | ES |
|---|---|---|---|---|---|---|---|---|---|
| 3.88 | 3.75 | 2.75 | 2.26 | 2.00 | 1.99 | 1.88 | 1.79 | 1.67 | 1.52 |

   (natürlich halten sich nicht alle Texte an diese Prozentangaben!).

3. Sei $b \in \mathbb{Z}_N^n$ und $\pi$ eine Permutation vom Grad $n$. Warum ist die *Permutationschiffre*, welche mit der Abbildung $x \mapsto \pi(x)$ arbeitet, wahrscheinlich sicherer als die affine Cäsar-Chiffre, welche $x \mapsto x + b$ verwendet? Zeige ausserdem, dass durch $c(x) = \pi(x) + b \bmod N$ ein Kryptosystem gegeben ist.

4. Man betrachte das folgende Chiffriersystem, bei dem Nachrichten $m$ Elemente $\neq 0$ von $\mathbb{F}_q$ sind: A wählt zufällig ein $h \in \mathbb{N}$ mit $1 \leq h \leq q-1$ und $\mathrm{ggT}(h, q-1) = 1$ und sendet $x = m^h$ an B. B wählt ein zufälliges $k \in \mathbb{N}$ mit $\mathrm{ggT}(k, q-1) = 1$ und sendet $y = x^k$ an A zurück. Nun bildet A die Nachricht $z = y^{h'}$ mit $hh' \equiv 1 \pmod{q-1}$ und sendet $z$ an B. Man zeige, daß bei diesem "No-Key Algorithm" B die geheime Nachricht $m$ entschlüsseln kann und das Verfahren unter geeigneten Annahmen über $q$ sicher gegenüber kryptographischen Angriffen ist.