# Kryptologie

**Übung, LVA 405.321**
**C. Fuchs**

## 2. Übungsblatt, SS 2022

**16.03.2022**

1. Es sei $\Sigma$ ein Alphabet mit $|\Sigma| = N$ und dieses werde mit dem Ring $\mathbb{Z}_N$ identifiziert. Eine Nachricht $m$ werde verschlüsselt indem man jedes Symbol $s$ durch $as + b \pmod N$ ersetzt, wobei $a, b$ ganze Zahlen sind. Ein Schlüssel $k = (a, b)$ ist nur dann gültig, wenn die Abbildung $\mathbb{Z}_N \to \mathbb{Z}_N$ injektiv ist.
   a) Zeige, dass es sich um ein Kryptosystem (nämlich das *affine Cäsar-System*) handelt.
   b) Erkläre, warum injektiv eine sinnvolle Forderung ist.
   c) Wie entschlüsselt man einen Ciphertext $c$?
   d) Beschreibe alle gültigen Schlüssel.
   e) Wieviele gültige Schlüssel gibt es?

2. Die folgende Nachricht sei mit einem affinen Cäsar-System mit $N = 26$ Buchstaben verschlüsselt. Man entschlüssele "VBEDXSXIXKPXS".

3. *Hill-Chiffre:* Es sei $A$ eine $n \times n$-Matrix über $\mathbb{Z}_N$.
   a) Man zeige: $A$ ist genau dann invertierbar, wenn $\det A$ invertierbar in $\mathbb{Z}_N$ ist.
   b) Man verschlüssele einen Text $m$, indem man $m$ in Blöcke der Länge $n$ zerlegt und jeden Block $b_m \in \mathbb{Z}_N^n$ durch $c_m = Ab_m$ ersetzt. Wie erhält man den ursprünglichen Text zurück? Wann ist dies möglich? Beispiel?
   c) Wieviele invertierbare $n \times n$-Matrizen über $\mathbb{Z}_p$ gibt es, wenn $p$ eine Primzahl ist.
   d) Es sei $N$ eine Primzahl. Wie hoch ist die Sicherheit der Hill-Chiffre im Vergleich zu einem Vignère-Schlüssel der Länge $n$?

4. Gesucht ist die $2 \times 2$-Matrix $A$ über $\mathbb{Z}_{37}$ die "BLEI" in "GOLD" verwandelt. Dabei sei $\Sigma = \{A, B, \ldots, Z, \_, 0', 1', \ldots, 9'\}$ mit der Identifikation $A = 0, B = 1, \ldots, Z = 25, \_ = 26, 0' = 27, \ldots, 9' = 36$.