Kryptographie **Blatt 2**

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 23.10.2023, vor der Vorlesung

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

Aufgabe 1: Affinlineare Verschlüsselung

Gegeben sei die affinlineare Verschlüsselung $E : \mathbb{Z}_n^4 \to \mathbb{Z}_n^4$, $x \mapsto Ax + b$, mit $n = 26$, $b \in \mathbb{Z}_n^4$ und der Matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Für das Alphabet `A,...,Z` wird die Kodierung `A` $\mapsto 1$, `B` $\mapsto 2$, ..., `Z` $\mapsto 0$ gewählt.

(a) Beschreiben Sie die Funktionsweise der Verschlüsselung, wenn $b = 0$.

(b) Geben Sie die Entschlüsselungsfunktion D an, für die $E \circ D = D \circ E = \mathrm{id}_{\mathbb{Z}_n^4}$ gilt, wenn b der Vektor zum Schlüsselwort "`FLAU`" ist.

(c) Verschlüsseln Sie mit diesem b einen kurzen Text aus etwa 10 Wörtern.

(d) Wie viele invertierbare Matrizen $A \in \mathbb{Z}_4^{2\times 2}$ gibt es?

(e) Wie viele invertierbare Matrizen $A \in \mathbb{Z}_p^{2\times 2}$ gibt es, wenn p eine beliebige Primzahl ist?

Aufgabe 2: Kartenmischung

Bei einer Mischung von 2^n vielen Karten werden zunächst die erste und letzte Karte des Stapels auf den Tisch platziert, danach die erste und letzte Karte des verbliebenen Stapels aufgelegt und so fortgefahren, bis ein neuer gemischter Kartenstapel entstanden ist. Ausgehend von einem Kartenstapel mit z. B. 8 Karten $1, 2, \ldots, 8$ hat der entstandene Stapel die neue Kartenreihenfolge $4, 5, 3, 6, 2, 7, 1, 8$.
Nach wievielen solcher Mischvorgänge wird der Kartenstapel wieder in die Originalreihenfolge zurückkehren?

Aufgabe 3: Verschlüsselung mit Schablonen-Drehung

Gegeben ist ein Quadrat aus $n \times n$ Feldern, von denen manche zu Löchern gestanzt wurden. Diese Schablone wird auf einen Geheimtext aus $n \times n$ Buchstaben gelegt und der Klartext der Reihe nach aus den Löchern ausgelesen. Dann wird die Schablone um 90° gedreht aufgelegt, die Löcher zeigen dann neue Buchstaben an, die den Klartext fortsetzen. Sie wird noch zweimal gedreht und aufgelegt, bis der komplette Text so ausgelesen ist.

(a) Wie muss eine solche Schablone beschaffen sein? Wieviele dieser Schablonen gibt es?

(b) Geben Sie ein Beispiel für eine solche Schablone mit $n = 8$ an, sowie einen Geheimtext, der damit verschlüsselt wurde, samt Klartext.

(c) Welche schwachen Schlüssel gibt es, d. h. welche Schablonen erlauben einen einfachen kryptoanalytischen Angriff?