Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 1

Übung zur Vorlesung
Kryptokomplexität 1

Ausgabe:	10. Oktober
Besprechung:	18-20. Oktober
Verantwortlich:	Roman Zorn

Begründen Sie Ihre Antworten und bereiten Sie sie so vor, dass Sie sie in der Übung präsentieren können.

Aufgabe 1 : Kryptosysteme

Gegeben ist das folgende Kryptosystem $S = (M, C, K, \mathscr{E}, \mathscr{D})$ mit

$$M = C = K = \mathbb{Z}_{26}$$
$$\mathscr{E} = \{E_k : M \to C \mid k \in K\} \text{ mit } E_k(m) = (m + k) \bmod 26$$
$$\mathscr{D} = \{D_k : C \to M \mid k \in K\} \text{ mit } D_k(c) = (c - k) \bmod 26$$

(a) ▶ Um welches Ihnen bekannte Kryptosystem handelt es sich?

(b) ▶ Verschlüsseln Sie mit dem Schlüssel $k = 3$ den Klartext $m = \texttt{ZEHN}$.

(c) Der Ciphertext $c = \texttt{FKLIIUH}$ wurde mit dem Schlüssel $k = 3$ verschlüsselt.
- ▶ Welches ist der zugehörige Schlüssel für die Entschlüsselung? Warum?
- ▶ Entschlüsseln Sie c.

Aufgabe 2 : Kongruenzrelation

Zeigen Sie, dass die Kongruenzrelation modulo m eine Äquivalenzrelation ist, d.h., zeigen Sie die in der Vorlesung angegebenen Eigenschaften:

(a) ▶ Reflexivität,

(b) ▶ Symmetrie und

(c) ▶ Transitivität.

Aufgabe 3 : Permutationschiffre

Betrachten Sie die Permutationschiffre aus der Vorlesung.

(a) ▶ Wie viele mögliche Schlüssel gibt es bei einer Blocklänge von $n = 6$?

(b) Gegeben sei der Klartext $m =$ `FINDEDENGEHEIMTEXT` und die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{pmatrix}$$

(also $\pi(1) = 6$, $\pi(2) = 1$, ...) bei einer Blocklänge von $n = 6$.
▶ Verschlüsseln Sie den Klartext m mit dem Schlüssel π.

(c) ▶ Bestimmen Sie die zu π inverse Permutation π^{-1}.
▶ Überprüfen Sie Ihr Ergebnis, indem Sie den in Aufgabenteil (b) erhaltenen Ciphertext entschlüsseln.

(d) Der Schlüssel π kann in der sogenannten *Zyklenschreibweise* als $\pi = (162)(3)(45)$ geschrieben werden – überlegen Sie sich, wie man diese liest.
▶ Ist diese Schreibweise eindeutig? Begründen Sie Ihre Antwort.