Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 1

Lösungsvorschläge

Kryptokomplexität 1

Bearbeitungszeit: 10. Oktober bis 18-20. Oktober
Verantwortlich: Roman Zorn

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?

Lösungsvorschlag: ▶ Es handelt sich um die Verschiebungschiffre.

(b) ▶ Verschlüsseln Sie mit dem Schlüssel $k = 3$ den Klartext $m =$ `ZEHN`.

Lösungsvorschlag: ▶ `ZEHN` $\widehat{=}$ (25 4 7 13) mit $k = 3$ verschlüsselt ergibt

$$\begin{aligned}(25+3) \bmod 26 &= 28 \bmod 26 \equiv 2\\ (4+3) \bmod 26 &= 7 \bmod 26 \equiv 7\\ (7+3) \bmod 26 &= 10 \bmod 26 \equiv 10\\ (13+3) \bmod 26 &= 16 \bmod 26 \equiv 16\end{aligned}$$

also (2 7 10 16) $\widehat{=}$ `CHKQ`.

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

Lösungsvorschlag: ▶ Da die Verschiebungschiffre symmetrisch ist, ist der Entschlüsselungsschlüssel gleich dem Verschlüsselungsschlüssel, also 3.
▶ Es gilt $c =$ `FKLIIUH` $\widehat{=}$ (5 10 11 8 8 20 7), also ist der entschlüsselte Klartext

$$
\begin{aligned}
(5-3) \bmod 26 &= 2 \bmod 26 \equiv 2 \\
(10-3) \bmod 26 &= 7 \bmod 26 \equiv 7 \\
(11-3) \bmod 26 &= 8 \bmod 26 \equiv 8 \\
(8-3) \bmod 26 &= 5 \bmod 26 \equiv 5 \\
(8-3) \bmod 26 &= 5 \bmod 26 \equiv 5 \\
(20-3) \bmod 26 &= 17 \bmod 26 \equiv 17 \\
(7-3) \bmod 26 &= 4 \bmod 26 \equiv 4
\end{aligned}
$$

und damit (2 7 8 5 5 17 4) $\widehat{=}$ `CHIFFRE`.

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.

Lösungsvorschlag: Wir benutzen die Definition, dass $x \equiv y \mod m$ genau dann gilt, wenn m die Differenz $x - y$ teilt.

(a) ▶ **Reflexivität:** Zu zeigen: $x \equiv x \mod m$.
Dies gilt, wenn m die Differenz $x - x = 0$ teilt, was offenbar gilt.

(b) ▶ **Symmetrie:** Zu zeigen: $x \equiv y \mod m \Longrightarrow y \equiv x \mod m$.
Wir wissen also, dass m die Differenz $x - y$ teilt. Da $x - y = -(-x + y) = -(y - x)$ gilt, können wir folgern, dass m die Differenz $-(y - x)$ teilt, und da das Vorzeichen keinen Einfluss hat, teilt m also auch $y - x$.

(c) ▶ **Transitivität:** Zu zeigen: wenn $x \equiv y \mod m$ und $y \equiv z \mod m$, dann $x \equiv z \mod m$.
Wir wissen also, dass m die Differenzen $x - y$ und $y - z$ teilt. Das bedeutet, es existieren zwei ganze Zahlen α und β, sodass $x - y = \alpha \cdot m$ und $y - z = \beta \cdot m$. Für die Differenz $x - z$ können wir obige Gleichungen einfach addieren und es ergibt sich

$$
\begin{aligned}
x - y + (y - z) &= \alpha m + \beta m \\
\Longleftrightarrow \; x - z &= (\alpha + \beta) m.
\end{aligned}
$$

Da α und β beide ganzzahlig waren, ist auch ihre Summe ganzzahlig, folglich teilt m die Differenz $x - z$ und damit ist Transitivität gezeigt.

Aufgabe 3 : Permutationschiffre

Betrachten Sie die Permutationschiffre aus der Vorlesung.

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

Lösungsvorschlag: ▶ Es gibt $n! = 6! = 720$ mögliche Schlüssel.

(b) Gegeben sei der Klartext $m = \texttt{FINDEDENGEHEIMTEXT}$ 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.

Lösungsvorschlag: ▶ Wir zerteilen den Klartext in Blöcke der Länge 6, also FINDED, ENGEHE und IMTEXT. Es gilt

$$E_\pi(\texttt{FINDED}) = \texttt{DFNEDI},\ E_\pi(\texttt{ENGEHE}) = \texttt{EEGHEN} \text{ und } E_\pi(\texttt{IMTEXT}) = \texttt{TITXEM}.$$

Also lautet der Ciphertext $c = \texttt{DFNEDIEEGHENTITXEM}$.

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

Lösungsvorschlag: ▶ Das Inverse zu π lässt sich durch "Rückwärtslesen" direkt ablesen und lautet

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

▶ Es gilt $E_{\pi^{-1}}(\texttt{DFNEDI}) = \texttt{FINDED}$, $E_{\pi^{-1}}(\texttt{EEGHEN}) = \texttt{ENGEHE}$ und $E_{\pi^{-1}}(\texttt{TITXEM}) = \texttt{IMTEXT}$. Zusammensetzen ergibt den erwarteten Klartext $m = \texttt{FINDEDENGEHEIMTEXT}$.

(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.

Lösungsvorschlag: ▶ Diese Schreibweise ist nicht eindeutig. Die Reihenfolge, in der man die Zyklen angibt und die Zahl mit der man einen Zyklus beginnt sind beliebig. So ist auch $\pi = (621)(45)(3)$ eine korrekte Schreibweise.