Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 3

Lösungsvorschläge

Kryptokomplexität 1

Bearbeitungszeit: 24. Oktober bis 2-3. November
Verantwortlich: Roman Zorn

Aufgabe 1 : Affin-lineare Blockchiffre

Betrachten Sie die affin-lineare Blockchiffre aus der Vorlesung mit der Matrix

$$A = \begin{pmatrix} 4 & 28 & 2 \\ 0 & 7 & 6 \\ 0 & 0 & 9 \end{pmatrix}$$

und

$$\vec{b} = \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix}.$$

Das verwendete Alphabet ist $\Sigma = \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{Z}, \mathtt{Ä}, \mathtt{Ö}, \mathtt{Ü}\}$ über $\mathbb{Z}_{29}$.

(a) ▶ Verschlüsseln Sie den Klartext $m = \mathtt{AMEISE}$ mit A und $\vec{b}$.

Lösungsvorschlag: ▶ Da $\vec{b}$ dreielementig ist, bilden wir Dreier-Blöcke und es gilt $m = \mathtt{AME\ ISE} \mathrel{\widehat{=}} (0\ 12\ 4)(8\ 18\ 4)$. Daher gilt:

$$\vec{x}_1 = \begin{pmatrix} 0 \\ 12 \\ 4 \end{pmatrix}, \vec{x}_2 = \begin{pmatrix} 8 \\ 18 \\ 4 \end{pmatrix}.$$

$$\begin{aligned} E_{(A,\vec{b})}(\vec{x}_1) &= \begin{pmatrix} 4 & 28 & 2 \\ 0 & 7 & 6 \\ 0 & 0 & 9 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 12 \\ 4 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix} \\ &= \begin{pmatrix} 344 \\ 108 \\ 36 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 28 \\ 22 \\ 11 \end{pmatrix} \mod 29 \end{aligned}$$

und

$$E_{(A,\vec{b})}(\vec{x}_2) = \begin{pmatrix} 4 & 28 & 2 \\ 0 & 7 & 6 \\ 0 & 0 & 9 \end{pmatrix} \cdot \begin{pmatrix} 8 \\ 18 \\ 4 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix}$$
$$= \begin{pmatrix} 544 \\ 150 \\ 36 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 25 \\ 6 \\ 11 \end{pmatrix} \mod 29$$

Der Schlüsseltext ist also $\vec{y} = (28\ 22\ 11)(25\ 6\ 11) \mathrel{\widehat{=}} \texttt{ÜWLZGL} = c$.

(b) ▶ Entschlüsseln Sie den Schlüsseltext $c = \texttt{SUV}$. (Sie haben die Inverse von A auf Blatt 2 in Aufgabe 4 berechnet.)

Lösungsvorschlag: ▶ $\texttt{SUV} \mathrel{\widehat{=}} (18\ 20\ 21)$, daher gilt:

$$\vec{y} = \begin{pmatrix} 18 \\ 20 \\ 21 \end{pmatrix}.$$

$$D_{(A^{-1},\vec{b})}(\vec{y}) = A^{-1} \cdot (\vec{y} - \vec{b})$$
$$= \begin{pmatrix} 22 & 28 & 28 \\ 0 & 25 & 22 \\ 0 & 0 & 13 \end{pmatrix} \cdot \left(\begin{pmatrix} 18 \\ 20 \\ 21 \end{pmatrix} - \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix} \right) = \begin{pmatrix} 1338 \\ 849 \\ 221 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 8 \\ 18 \end{pmatrix} \mod 29.$$

Der Klartext ist also $(4\ 8\ 18) \mathrel{\widehat{=}} \texttt{EIS}$.

Aufgabe 2 : Hill- und Stromchiffre

Betrachten Sie die Hill-Chiffre aus der Vorlesung.

(a) Betrachten Sie die Matrix

$$A = \begin{pmatrix} 8 & 2 \\ 6 & 9 \end{pmatrix}.$$

▶ Ist A bei einem Alphabet mit 26 Zeichen ein gültiger Schlüssel? Begründen Sie Ihre Antwort.

Lösungsvorschlag: ▶ Damit A ein gültiger Schlüssel ist, muss die Matrix in $\mathbb{Z}_{26}^{2\times 2}$ invertierbar sein, es muss also $\mathrm{ggT}(\det(A), 26) = 1$ gelten. Um das zu prüfen, berechnen wir die Determinante:

$$\det(A) = 8 \cdot 9 - 2 \cdot 6 = 60 \equiv 8 \mod 26.$$
$$\text{ggT}(8, 26) = 2 > 1 \Rightarrow A \text{ ist nicht invertierbar.}$$

Also ist A über $\mathbb{Z}_{26}$ *kein* gültiger Schlüssel für die Hill-Chiffre.

(b) Nach der Vorlesung ist die Permutationschiffre ein Spezialfall der Hill-Chiffre.
► Geben Sie für die folgende Permutation π die entsprechende Verschlüsselungsmatrix M_π an:

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

Lösungsvorschlag: ► Laut Vorlesung erhalten wir die Verschlüsselungsmatrix M_π aus der Einheitsmatrix, indem wir in der i-ten Zeile von M_π die $\pi(i)$-te Zeile der Einheitsmatrix eintragen. Das ergibt:

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

(c) Betrachten Sie die Stromchiffre basierend auf einem linear rückgekoppelten Schieberegister mit Alphabet $\Sigma = \{0, 1\}$, $n = 6$, Koeffizienten $a_1 = a_3 = a_5 = a_6 = 1, a_2 = a_4 = 0$ und Schlüssel $\vec{k} = (1, 0, 1, 1, 0, 1)$.
► Verschlüsseln Sie den Klartext

$$\vec{m} = (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1).$$

Lösungsvorschlag: ► Der Schlüsselstrom $\vec{s}$ wird durch die Rekursion

$$s_{i+6} = s_{i+5} + s_{i+3} + s_{i+1} + s_i$$

erzeugt. Da $|m| = 13$ gilt, erhält man mit $\vec{k}$

$$\vec{s} = (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, \ldots).$$

Insgesamt ergibt dies den Schlüsseltext

$$\vec{c} = (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0).$$

Aufgabe 3 : Cipherblock Chaining Mode

Wenden Sie den CBC (Cipherblock Chaining Mode) auf die Hill-Chiffre an, mit dem Alphabet $\Sigma = \{0, 1\}$ sowie

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \text{ und } c_0 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

(a) ▶ Verschlüsseln Sie $m = \texttt{101001010}$.

Lösungsvorschlag:

▶ Hier gilt

$$b_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, b_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, b_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

und damit:

$$\begin{aligned} c_1 &= A \cdot (c_0 \oplus b_1) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right) \\ &= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mod 2 \\ c_2 &= A \cdot (c_1 \oplus b_2) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right) \\ &= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \mod 2 \\ c_3 &= A \cdot (c_2 \oplus b_3) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \left(\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right) \\ &= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \mod 2 \end{aligned}$$

Damit ist der Schlüsseltext $\texttt{001000110}$.

(b) ▶ Entschlüsseln Sie $c = \texttt{101001010}$.

Lösungsvorschlag:
▶ Hier gilt

$$A^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, c_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, c_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, c_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

und damit:

$$\begin{aligned} b_1 &= c_0 \oplus A^{-1} \cdot c_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \\ &\equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \mod 2 \\ b_2 &= c_1 \oplus A^{-1} \cdot c_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \\ &\equiv \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \mod 2 \\ b_3 &= c_2 \oplus A^{-1} \cdot c_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \\ &\equiv \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \mod 2 \end{aligned}$$

Damit ist der entschlüsselte Klartext $\texttt{000110110}$.

Aufgabe 4 : Output Feedback Mode

Betrachten Sie den OFB (Output Feedback Mode) in Kombination mit der affin-linearen Blockchiffre auf dem Alphabet $\Sigma = \{0, 1\}$. Zum Verschlüsseln wurde $k = 2$ und

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \quad z_0 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

verwendet.
▶ Entschlüsseln Sie den Schlüsseltext $c = \texttt{10100111}$.

Lösungsvorschlag:

▶ Hier gilt $c_1 = \begin{pmatrix}1\\0\end{pmatrix}$, $c_2 = \begin{pmatrix}1\\0\end{pmatrix}$, $c_3 = \begin{pmatrix}0\\1\end{pmatrix}$ und $c_4 = \begin{pmatrix}1\\1\end{pmatrix}$.

$$x_1 = A \cdot z_0 + b = \begin{pmatrix}0&0&1&0\\0&0&0&0\\1&0&1&0\\0&1&1&0\end{pmatrix} \cdot \begin{pmatrix}1\\1\\0\\0\end{pmatrix} + \begin{pmatrix}1\\1\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\1\end{pmatrix} + \begin{pmatrix}1\\1\\1\\0\end{pmatrix} \equiv \begin{pmatrix}1\\1\\0\\1\end{pmatrix} \mod 2$$

$$y_1 = \begin{pmatrix}1\\1\end{pmatrix}$$

$$b_1 = c_1 \oplus y_1 = \begin{pmatrix}1\\0\end{pmatrix} \oplus \begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$$

$$z_1 = x_1 = \begin{pmatrix}1\\1\\0\\1\end{pmatrix}$$

$$x_2 = A \cdot z_1 + b = \begin{pmatrix}0&0&1&0\\0&0&0&0\\1&0&1&0\\0&1&1&0\end{pmatrix} \cdot \begin{pmatrix}1\\1\\0\\1\end{pmatrix} + \begin{pmatrix}1\\1\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\1\end{pmatrix} + \begin{pmatrix}1\\1\\1\\0\end{pmatrix} \equiv \begin{pmatrix}1\\1\\0\\1\end{pmatrix} \mod 2$$

$$y_2 = \begin{pmatrix}1\\1\end{pmatrix}$$

$$b_2 = c_2 \oplus y_2 = \begin{pmatrix}1\\0\end{pmatrix} \oplus \begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$$

$$z_2 = x_2 = \begin{pmatrix}1\\1\\0\\1\end{pmatrix}$$

$$
\begin{aligned}
x_3 &= A \cdot z_2 + b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \mod 2 \\
y_3 &= \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\
b_3 &= c_3 \oplus y_3 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
z_3 &= x_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
x_4 &= A \cdot z_3 + b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \mod 2 \\
y_4 &= \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\
b_4 &= c_4 \oplus y_4 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}
\end{aligned}
$$

Aus den b_i ergibt sich der entschlüsselte Klartext `01011000`.