Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 4

Lösungsvorschläge

Kryptokomplexität 1

Bearbeitungszeit: 31. Oktober bis 8-10. November
Verantwortlich: Roman Zorn

Aufgabe 1 : Known-Plaintext-Angriff

► Führen Sie einen Known-Plaintext-Angriff auf die affin-lineare Blockchiffre aus. Ihnen sind dabei $m = \texttt{ENIGMA}$, $c = \texttt{LGXÖJÄ}$, $n = 2$ und $\Sigma = \{\texttt{A}, \texttt{B}, \texttt{C}, \ldots, \texttt{Z}, \texttt{Ä}, \texttt{Ö}, \texttt{Ü}\}$ über $\mathbb{Z}_{29}$ bekannt.

Lösungsvorschlag: ► Wir bestimmen X^{-1} aus m.
Es gilt $m = \texttt{ENIGMA} \mathrel{\widehat{=}} (4\ 13\ 8\ 6\ 12\ 0)$ und damit:

$$x_0 = \begin{pmatrix} 4 \\ 13 \end{pmatrix},\ x_1 = \begin{pmatrix} 8 \\ 6 \end{pmatrix},\ x_2 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$$

$$\Rightarrow\ X = \begin{pmatrix} x_1 - x_0 & x_2 - x_0 \end{pmatrix} \equiv \begin{pmatrix} 4 & 8 \\ 22 & 16 \end{pmatrix} \mod 29$$

$$\Rightarrow\ X^{-1} = 4^{-1} \begin{pmatrix} 16 & 21 \\ 7 & 4 \end{pmatrix} \equiv 22 \begin{pmatrix} 16 & 21 \\ 7 & 4 \end{pmatrix} \equiv \begin{pmatrix} 4 & 27 \\ 9 & 1 \end{pmatrix} \mod 29$$

► Nun bestimmen wir den Schlüssel (A, b) aus X^{-1} und c.
Es gilt $c = \texttt{LGXÖJÄ} \mathrel{\widehat{=}} (11\ 6\ 23\ 27\ 9\ 26)$ und damit:

$$y_0 = \begin{pmatrix} 11 \\ 6 \end{pmatrix},\ y_1 = \begin{pmatrix} 23 \\ 27 \end{pmatrix},\ y_2 = \begin{pmatrix} 9 \\ 26 \end{pmatrix}$$

$$\Rightarrow\ Y = \begin{pmatrix} y_1 - y_0 & y_2 - y_0 \end{pmatrix} \equiv \begin{pmatrix} 12 & 27 \\ 21 & 20 \end{pmatrix} \mod 29$$

$$\Rightarrow\ A = Y \cdot X^{-1} = \begin{pmatrix} 12 & 27 \\ 21 & 20 \end{pmatrix} \begin{pmatrix} 4 & 27 \\ 9 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 3 \\ 3 & 7 \end{pmatrix} \mod 29$$

$$\Rightarrow\ b = y_0 - A \cdot x_0 = \begin{pmatrix} 11 \\ 6 \end{pmatrix} - \begin{pmatrix} 1 & 3 \\ 3 & 7 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 26 \\ 19 \end{pmatrix} \mod 29$$

Wir haben also den geheimen Schlüssel (A, b) ermittelt mit

$$A = \begin{pmatrix} 1 & 3 \\ 3 & 7 \end{pmatrix}, \quad b = \begin{pmatrix} 26 \\ 19 \end{pmatrix}.$$

Aufgabe 2 : Perfekte Geheimhaltung

Sei $S = (M, C, K, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit den folgenden Eigenschaften:

- $M = \{m_0, m_1, \ldots, m_{n-1}\}$, und wir setzen $\alpha_j := \Pr(m_j)$ für alle j, $0 \leq j \leq n-1$, wobei $0 < \alpha_j < 1$ sowie $\sum_{j=0}^{n-1} \alpha_j = 1$ gilt,
- $K = \{k_0, k_1, \ldots, k_{n-1}\}$ mit $\Pr(k_i) = 1/n$, für alle i, $0 \leq i \leq n-1$,
- $C = \{c_0, c_1, \ldots, c_{n-1}\}$,
- $\mathcal{E} = \{E_{k_i}(m_j) = c_s \mid s \equiv i - j \mod n,\ 0 \leq i, j \leq n-1\}$.

► Bestimmen und begründen Sie (OHNE Nutzung des Satzes von Shannon) für das angegebene Kryptosystem, ob es perfekte Geheimhaltung (*perfect secrecy*) garantiert.

Lösungsvorschlag: ► Berechne zuerst $\Pr(m_j, k_i)$ für alle Paare i, j mit $0 \leq i, j < n$:

$$\Pr(m_j, k_i) \;=\; \Pr(m_j) \cdot \Pr(k_i) = \alpha_j/n.$$

Berechne dann die Wahrscheinlichkeit dafür, dass $c_s \in C$ erhalten wird. Wir verwenden dabei, dass $E_{k_{(j+s \mod n)}}(m_j) = c_s$ (aus der Definition von $\mathcal{E}$ durch Umformen).

$$\Pr(c_s) \;=\; \sum_{j=0}^{n-1} \Pr(m_j) \cdot \Pr\left(k_{(j+s \mod n)}\right) = \sum_{j=0}^{n-1} \alpha_j \cdot 1/n = 1/n$$

da $\sum_{j=0}^{n-1} \alpha_j = 1$.
Für jedes Paar $(m_j, c_s) \in M \times C$, $0 \leq j, s < n$, berechnet sich $\Pr(m_j | c_s)$ durch

$$\Pr(m_j | c_s) \;=\; \frac{\Pr(m_j \cap c_s)}{\Pr(c_s)} = \frac{\Pr\left(m_j, k_{(j+s \mod n)}\right)}{\Pr(c_s)} = \frac{\frac{\alpha_j}{n}}{\frac{1}{n}} = \alpha_j = \Pr(m_j).$$

Also garantiert S für jede gültige Wahl der α_j perfekte Geheimhaltung.

Aufgabe 3 : Perfekte Geheimhaltung, Shannons Theorem

Bestimmen und begründen Sie (gegebenenfalls unter Nutzung des Satzes von Shannon) für die folgenden Kryptosysteme, ob sie perfekte Geheimhaltung garantieren:

(a) ▶ Sei n ungerade und $S = (M, C, K, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit den folgenden Eigenschaften:

- $M = \{m_0, m_1, \ldots, m_{n-1}\}$ mit $0 < \Pr(m_j) = \alpha_j < 1$ für $0 \leq j \leq n-1$, und $\sum_{j=0}^{n-1} \alpha_j = 1$,
- $K = \{k_0, k_1, \ldots, k_{n-1}\}$ mit $\Pr(k_j) = 1/n$, für $0 \leq j \leq n-1$,
- $C = \{c_0, c_1, \ldots, c_{n-1}\}$,
- $\mathcal{E} = \{E_{k_i}(m_j) = c_s \mid s \equiv j + 2i \mod n,\ 0 \leq i, j \leq n-1\}$.

Lösungsvorschlag: ▶ S erfüllt die Voraussetzungen des Satzes von Shannon, somit garantiert S perfekte Geheimhaltung genau dann, wenn Eigenschaften (1) und (2) aus der Vorlesung gelten:

(1) Die Verschlüsselung einer Nachricht m_j mit einem Schlüssel k_i ergibt das $j + 2i$-te Element aus dem Ciphertextraum, modulo n. Diese Operation ($j + 2i \mod n$) erreicht alle Zahlen von 0 bis $n-1$, wenn man entweder i oder j fixiert, da n ungerade ist. Somit existiert für jedes $m \in M$ und $c \in C$ ein eindeutiger Schlüssel $k \in K$ mit $E_k(m) = c$.

(2) Es gilt $\Pr(k_j) = 1/n$, für $0 \leq j \leq n-1$, und somit sind die Schlüssel in K gleichverteilt.

Somit garantiert S perfekte Geheimhaltung.

(b) ▶ Sei n gerade und $S = (M, C, K, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit den folgenden Eigenschaften:

- $M = \{m_0, m_1, \ldots, m_{n-1}\}$ mit $0 < \Pr(m_j) = \alpha_j < 1$ für $0 \leq j \leq n-1$, und $\sum_{j=0}^{n-1} \alpha_j = 1$,
- $K = \{k_0, k_1, \ldots, k_{n-1}\}$ mit $\Pr(k_j) = 1/n$, für $0 \leq j \leq n-1$,
- $C = \{c_0, c_1, \ldots, c_{n-1}\}$,
- $\mathcal{E} = \{E_{k_i}(m_j) = c_s \mid s \equiv j + 2i \mod n,\ 0 \leq i, j \leq n-1\}$.

Lösungsvorschlag: ▶ Wieder erfüllt S die Voraussetzungen des Satzes von Shannon. Allerdings gilt, dass $E_{k_0}(m_0) = c_0$ und $E_{k_{n/2}}(m_0) = c_0$. Somit existiert nicht für jede Kombination aus Nachricht und Ciphertext ein eindeutiger Schlüssel und Bedingung (1) ist verletzt. Aus dem Satz von Shannon folgt, dass S keine perfekte Geheimhaltung garantiert.

Aufgabe 4 : Wahrscheinlichkeit und Entropie

Gegeben sei ein Kryptosystem $S = (M,\ C,\ K,\ \mathcal{E},\ \mathcal{D})$ mit den folgenden Eigenschaften:

- $M = \{a, b, c\}$, $C = \{A, B, C\}$, $K = \{0, 1, 2\}$,
- $\Pr(a) = 1/7$, $\Pr(b) = 2/7$, $\Pr(c) = 4/7$,
- $\Pr(0) = 2/7$, $\Pr(1) = 2/7$, $\Pr(2) = 3/7$,
- $E_0(a) = A$, $E_0(b) = B$, $E_0(c) = C$,
  $E_1(a) = B$, $E_1(b) = C$, $E_1(c) = A$,
  $E_2(a) = C$, $E_2(b) = A$, $E_2(c) = B$.

(a) ▶ Bestimmen Sie die Wahrscheinlichkeitsverteilung auf dem Schlüsseltextraum C, die durch die Verteilungen auf M und K induziert wird.

Lösungsvorschlag: ▶ Bestimme zunächst die Wahrscheinlichkeiten dafür, dass bestimmte Elemente in M und in K gleichzeitig "auftreten":

$$\begin{aligned}
\Pr(a,0) &= \Pr(a)\cdot\Pr(0) = \frac{1}{7}\cdot\frac{2}{7} = \frac{2}{49}\\
\Pr(a,1) &= \Pr(a)\cdot\Pr(1) = \frac{1}{7}\cdot\frac{2}{7} = \frac{2}{49}\\
\Pr(a,2) &= \Pr(a)\cdot\Pr(2) = \frac{1}{7}\cdot\frac{3}{7} = \frac{3}{49}\\
\Pr(b,0) &= \Pr(b)\cdot\Pr(0) = \frac{2}{7}\cdot\frac{2}{7} = \frac{4}{49}\\
\Pr(b,1) &= \Pr(b)\cdot\Pr(1) = \frac{2}{7}\cdot\frac{2}{7} = \frac{4}{49}\\
\Pr(b,2) &= \Pr(b)\cdot\Pr(2) = \frac{2}{7}\cdot\frac{3}{7} = \frac{6}{49}\\
\Pr(c,0) &= \Pr(c)\cdot\Pr(0) = \frac{4}{7}\cdot\frac{2}{7} = \frac{8}{49}\\
\Pr(c,1) &= \Pr(c)\cdot\Pr(1) = \frac{4}{7}\cdot\frac{2}{7} = \frac{8}{49}\\
\Pr(c,2) &= \Pr(c)\cdot\Pr(2) = \frac{4}{7}\cdot\frac{3}{7} = \frac{12}{49}
\end{aligned}$$

Das Ereignis A umfasst die Ereignisse $a \cap 0$ (wegen $E_0(a) = A$), $b \cap 2$ (wegen $E_2(b) = A$) und $c \cap 1$ (wegen $E_1(c) = A$). Da diese Ereignisse disjunkt sind, können wir einfach deren Wahrscheinlichkeiten aufaddieren um die Wahrscheinlichkeit von A zu erhalten (für B und C analog).

$$\begin{aligned}
\Pr(A) &= \Pr(a,0) + \Pr(b,2) + \Pr(c,1) = \frac{16}{49}\\
\Pr(B) &= \Pr(a,1) + \Pr(b,0) + \Pr(c,2) = \frac{18}{49}\\
\Pr(C) &= \Pr(a,2) + \Pr(b,1) + \Pr(c,0) = \frac{15}{49}
\end{aligned}$$

(b) ▶ Fassen Sie M, K und C als Zufallsvariablen auf und bestimmen Sie ihre Entropien.

Lösungsvorschlag: ▶ Es gilt

$$\begin{aligned}
\mathcal{H}(M) &= -\left(\frac{1}{7}\log\frac{1}{7} + \frac{2}{7}\log\frac{2}{7} + \frac{4}{7}\log\frac{4}{7}\right) \\
&= -\left(\frac{1}{7}(0-\log 7) + \frac{2}{7}(1-\log 7) + \frac{4}{7}(2-\log 7)\right) \\
&= \frac{\log 7}{7} - \frac{2}{7} + \frac{2\log 7}{7} - \frac{8}{7} + \frac{4\log 7}{7} \\
&= \log 7 - \frac{10}{7} \approx 1,379
\end{aligned}$$

Analog ergibt sich

$$\begin{aligned}
\mathcal{H}(K) &= -\left(\frac{2}{7}\log\frac{2}{7} + \frac{2}{7}\log\frac{2}{7} + \frac{3}{7}\log\frac{3}{7}\right) \\
&= \log 7 - \frac{3}{7}\log 3 - \frac{4}{7} \approx 1,557
\end{aligned}$$

und

$$\begin{aligned}
\mathcal{H}(C) &= -\left(\frac{16}{49}\log\frac{16}{49} + \frac{18}{49}\log\frac{18}{49} + \frac{15}{49}\log\frac{15}{49}\right) \\
&= \log 49 - \frac{18}{49}\log 18 - \frac{15}{49}\log 15 - \frac{64}{49} \approx 1,581
\end{aligned}$$

Hinweis: Die maximale Entropie wäre hier jeweils

$$\mathcal{H}(X) = \log n = \log 3 \approx 1,585.$$