Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 4

Übung zur Vorlesung

Kryptokomplexität 1

Ausgabe:	31. Oktober
Besprechung:	8-10. November
Verantwortlich:	Roman Zorn

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

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.

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.

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 $0 \leq j \leq n-1$,
- $C = \{c_0, c_1, \ldots, c_{n-1}\}$,
- $\mathcal{E} = \{E_{k_i}(m_j) = c_s \mid s \equiv j + 2i \mod n,\ 0 \leq i, j \leq n-1\}$.

(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 $0 \leq j \leq n-1$,
- $C = \{c_0, c_1, \ldots, c_{n-1}\}$,
- $\mathcal{E} = \{E_{k_i}(m_j) = c_s \mid s \equiv j + 2i \mod n,\ 0 \leq i, j \leq n-1\}$.

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.

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