Übungsblatt 5

Abgabe der schriftlichen Lösungen bis 02.06.2022, 24 Uhr

Aufgabe 25 — *mündlich, 10 Punkte*

Gegeben sei das Kryptosystem (M, C, E, D, K) mit Klartextraum $M = \{a, b\}$, Schlüsselraum $K = \{k_1, k_2, k_3, k_4\}$, Kryptotextraum $C = \{1, 2, 3, 4\}$ und der nebenstehenden Verschlüsselungsfunktion E. Zudem betrachten wir die Klartextverteilung $p(a) = 1/4$, $p(b) = 3/4$ sowie die Schlüsselverteilung $p(k_1) = 1/2$, $p(k_2) = p(k_3) = p(k_4) = 1/6$.

E	a	b
k_1	1	2
k_2	2	3
k_3	3	4
k_4	4	1

E'	a	b
k_1	1	2
k_2	3	4
k_3	4	3
k_4	2	1

(a) Berechnen Sie die (bedingten) Wahrscheinlichkeiten $p(y)$ und $p(x|y)$ für alle Klartexte $x \in M$ und Kryptotexte $y \in C$. Welche Kryptotexte geben dem Gegner Informationen über den Klartext und welche über den Schlüssel? ***mündlich***

(b) Berechnen Sie die Entropien $\mathcal{H}(\mathcal{X})$, $\mathcal{H}(S)$, $\mathcal{H}(\mathcal{Y})$, $\mathcal{H}(\mathcal{X}|\mathcal{Y})$ und $\mathcal{H}(S|\mathcal{Y})$ für die Klartext-, Kryptotext- und Schlüssel-Verteilungen $\mathcal{X}$, $\mathcal{Y}$ und S. ***mündlich***

(c) Bei welchen Schlüsselgeneratoren S' ist das System absolut sicher? ***mündlich***

(d) Lösen Sie (a) bis (c) für die Verschlüsselungsfunktion E'. ***10 Punkte***

Aufgabe 26 — *mündlich*

Für zwei Zufallsvariablen $\mathcal{X}$ und $\mathcal{Y}$ sei $\mathcal{H}(\mathcal{X}, \mathcal{Y}) = \sum_{x,y} p(x, y) \cdot \log(1/p(x, y))$ die (gemeinsame) Entropie von $\mathcal{X}$ und $\mathcal{Y}$. Zeigen Sie:

(a) $\mathcal{H}(\mathcal{X}, \mathcal{Y}) = \mathcal{H}(\mathcal{Y}) + \mathcal{H}(\mathcal{X}|\mathcal{Y}) = \mathcal{H}(\mathcal{X}) + \mathcal{H}(\mathcal{Y}|\mathcal{X})$.

(b) $\mathcal{H}(\mathcal{X}, \mathcal{Y}) \le \mathcal{H}(\mathcal{X}) + \mathcal{H}(\mathcal{Y})$ mit Gleichheit genau dann wenn $\mathcal{X}, \mathcal{Y}$ unabhängig sind.

Aufgabe 27 — *mündlich*

(a) Zeigen Sie, dass die Eindeutigkeitsdistanz bei der Häufigkeitsanalyse von Blocktranspositionen auf der Basis von Einzelzeichen für jede Blocklänge $\ell > 1$ den Wert $n_0 = \infty$ hat (bei gleichverteilter Schlüsselverteilung).

Hinweis: Überprüfen Sie die Abschätzungen bei der Herleitung der unteren Schranke $n_0 \ge \log_2(|K|)/\mathcal{R}(\mathcal{L}_1) \log_2 m$ für den Fall einer Blocktransposition unter einer Klartextverteilung, bei der $p(x)$ nicht von der Reihenfolge der Zeichen in x abhängt, und finden Sie die Stelle wo die Abschätzung zu grob ist.

(b) Lässt sich daraus ableiten, dass Blocktranspositionen mit Blocklänge $\ell > 1$ bei jeder Klartextverteilung absolut sicher sind, bei der $p(x)$ nicht von der Reihenfolge der Zeichen in x abhängt?

Aufgabe 28 — *mündlich*

(a) Sei $p_1 \le \cdots \le p_n$ eine Wahrscheinlichkeitsverteilung und seien $q_1, \ldots, q_n \in \mathbb{R}$. Zeigen Sie, dass $\alpha(\pi) = \sum_{i=1}^{n} p_i q_{\pi(i)}$ genau dann einen maximalen Wert auf S_n annimmt, wenn $p_i < p_j \Rightarrow q_{\pi(i)} \le q_{\pi(j)}$ für alle $i, j \in [n]$ gilt.

(b) Gegeben sei ein Kryptotext, der mit der Vigenère-Chiffre unter einem Schlüssel $k_1 \ldots k_d$ erstellt wurde. Sei $p(a)$ die bekannte Wahrscheinlichkeitsverteilung der Klartextzeichen $a \in A$ und $h_i(b)$ sei die relative Häufigkeit von b unter allen Kryptotextzeichen, die mit dem Schlüsselbuchstaben k_i verschlüsselt wurden. Überlegen Sie, unter welchen Voraussetzungen die Funktion

$$\alpha_i(k) = \sum_{a \in A} p(a) h_i(a + k)$$

wahrscheinlich für $k = k_i$ einen maximalen Wert annimmt.

Aufgabe 29 — *mündlich*

Sei $KS = (M, C, E, D, K, \mathcal{S})$ ein Kryptosystem. Zeigen Sie:

(a) KS ist absolut sicher, falls $\sum_{k, E(k,x)=y} p(k) = 1/|M|$ für alle $(x, y) \in M \times C$ gilt. Im Fall $|C| = |M|$ ist dies auch notwendig (dies impliziert die Rückrichtung von Satz 65 im Skript).

(b) Im Fall $|K| < |M|$ kann KS nicht absolut sicher sein.

(c) KS ist genau dann absolut sicher, wenn es eine Klartextverteilung mit $p(x) > 0$ für alle $x \in M$ gibt, unter der es absolut sicher ist.

(d) KS ist genau dann absolut sicher, wenn es unter allen Klartextverteilungen mit $p(x) \in \{0, 1/2\}$ für alle $x \in M$ absolut sicher ist.

Aufgabe 30 — *mündlich*

(a) Bestimmen Sie in Abhängigkeit von der Redundanz der Klartextsprache und der Größe m des Klartextalphabets eine untere Schranke für die Eindeutigkeitsdistanz

- einer einfachen Substitutionschiffre ($|K| = m!$),
- einer Hill-Chiffre mit Blocklänge ℓ (nur für quadratfreies m), sowie
- einer Blocktransposition ($|K| = \ell!$) und einer Blockchiffre ($|K| = (m^l)!$).

Welche Schranke ergibt sich jeweils für deutschen Klartext über dem lateinischen Alphabet? (*Hinweis:* Benutzen Sie die Stirling-Formel $n! \approx \sqrt{2\pi n}(n/e)^n$.)

(b) Finden Sie für jede dieser Chiffren einen möglichst langen Kryptotext y mit $|K(y)| \ge 2$ (falls Deutsch oder Englisch als Klartextsprache benutzt wird; die Blocklänge ℓ kann beliebig zwischen 2 und 5 gewählt werden).