

Übungsblatt 5

Abgabe für die mündlichen Aufgaben bis 25. 05. 2020 und für die schriftliche Aufgabe bis 02. 06. 2020

Aufgabe 26

mündlich

- (a) Sei p_1, \dots, p_n eine Wahrscheinlichkeitsverteilung mit $p_1 \leq \dots \leq p_n$ und seien $q_1, \dots, q_n \in \mathbb{R}$. Zeigen Sie, dass $\alpha(\pi) = \sum_{i=1}^n p_i q_{\pi(i)}$ genau dann einen maximalen Wert auf S_n annimmt, wenn $p_i < p_j \Rightarrow q_{\pi(i)} \leq q_{\pi(j)}$ für alle $i, j \in [n]$ gilt.
- (b) Gegeben sei ein Kryptotext, der mit der Vigenère-Chiffre unter einem Schlüssel $k_1 \dots k_d$ 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 27

mündlich

Sei $KS = (M, C, E, D, K, S)$ 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 X 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 X mit $p(x) \in \{0, 1/2\}$ für alle $x \in M$ absolut sicher ist.

Aufgabe 28

mündlich

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

- (a) $\mathcal{H}(X, Y) = \mathcal{H}(Y) + \mathcal{H}(X|Y) = \mathcal{H}(X) + \mathcal{H}(Y|X)$.
- (b) $\mathcal{H}(X, Y) \leq \mathcal{H}(X) + \mathcal{H}(Y)$, mit Gleichheit genau dann, wenn X und Y unabhängig sind.

Aufgabe 29

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 $n_0 \geq \log_2(\|K\|)/\mathcal{R}_{abs}(L)$ 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 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 ($\|K\| = (m')!$).

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 $\|K(y)\| > 1$ (falls Deutsch oder Englisch als Klartextsprache benutzt wird; die Blocklänge ℓ kann beliebig zwischen 2 und 5 gewählt werden).

Aufgabe 31

mündlich, 10 Punkte

Gegeben sei das Kryptosystem (M, C, E, D, K) mit Klartextrraum $M = \{a, b\}$, Schlüsselraum $K = \{k_1, k_2, k_3, k_4\}$, Kryptotextrraum $C = \{1, 2, 3, 4\}$ 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	E'	a	b
k_1	1	2	k_1	1	2
k_2	2	3	k_2	3	4
k_3	3	4	k_3	4	3
k_4	4	1	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 $\mathcal{H}(X)$, $\mathcal{H}(S)$, $\mathcal{H}(Y)$, $\mathcal{H}(X|Y)$ und $\mathcal{H}(S|Y)$ für die Klartext-, Kryptotext- und Schlüssel-Verteilungen X , 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**