Übungsblatt 5

Aufgabe 23 ***mündlich***

(a) Seien $p_1, \dots, p_n$ und $q_1, \dots, q_n$ Wahrscheinlichkeitsverteilungen mit $p_1 \le \dots \le p_n$. Zeigen Sie, dass $\alpha(\pi) = \sum_{i=1}^n p_i q_{\pi(i)}$ im Fall $q_{\pi(1)} \le \dots \le q_{\pi(n)}$ einen maximalen Wert annimmt.

(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. Erklären Sie, warum

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

wahrscheinlich für $k = k_i$ maximal wird.

Aufgabe 24 Zeigen Sie: ***mündlich***

(a) In einem absolut sicheren Kryptosystem hängt die Kryptotextverteilung nicht von der Verteilung der Klartexte ab.

(b) Ein Kryptosystem ist absolut sicher, wenn $\sum_{k:E(k,x)=y} p(k) = 1/\|M\|$ für alle $x \in M$ und $y \in C$ gilt. Im Fall $\|C\| = \|M\|$ ist dies auch notwendig.

(c) Ein Kryptosystem mit $\|K\| < \|M\|$ kann nicht absolut sicher sein.

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

Aufgabe 25 ***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) $\mathcal{H}(X,Y) \le \mathcal{H}(X) + \mathcal{H}(Y)$, mit Gleichheit genau dann, wenn X und Y unabhängig sind.

Aufgabe 26 ***mündlich***

(a) Bestimmen Sie in Abhängigkeit von der Redundanz R_L der Klartextsprache und der Größe m des Alphabets A näherungsweise die Eindeutigkeitsdistanz

- einer einfachen Substitutionschiffre,
- einer Hill-Chiffre mit Blocklänge l,
- einer Blocktransposition mit Blocklänge l und
- einer Blockchiffre, in der jede Bijektion auf $M = A^l$ durch (genau) einen Schlüssel $k \in K$ realisiert wird.

Hinweis: Benützen Sie zur Abschätzung von $n!$ die Stirling-Formel $n! \approx \sqrt{2\pi n}(n/e)^n$.

(b) Geben Sie für jede dieser Chiffren einen möglichst langen Kryptotext y mit $\|K(y)\| > 1$ an, falls Deutsch als Klartextsprache benutzt wird. (Die Blocklänge l kann beliebig zwischen 2 und 5 gewählt werden).

Aufgabe 27 ***mündlich***

Sei (M, C, E, D, K) ein Kryptosystem und bezeichne $\alpha_{\max}$ den maximalen Vorteil, den ein Gegner (mit unbeschränkten Rechenressourcen) erzielen kann. Zeigen Sie:

(a) Wenn $\|K\| < \|M\|$ ist, dann ist $\alpha_{\max} > 0$.

(b) Wenn $\|K\| (\|K\| - 1) < \|M\| - 1$ ist, dann ist $\alpha_{\max} = 1/2$.

(c) Über welche Rechenressourcen muss ein optimaler Gegner in Teilaufgabe (b) höchstens verfügen, wenn die Verschlüsselungsfunktion E effizient berechenbar ist?

Aufgabe 28 Zeigen Sie: ***mündlich***

(a) Ein Kryptosystem ist genau dann absolut sicher, wenn es unter jeder Klartextverteilung $p(x)$ mit $p(x) \in \{0, 1/2\}$ für alle $x \in M$ absolut sicher ist.

(b) Ein Kryptosystem ist absolut sicher, falls kein Gegner mit einem Vorteil $\alpha(G,V) > 0$ existiert.

Aufgabe 29 Zeigen oder widerlegen Sie folgende Aussagen: ***10 Punkte***

(a) Ist ein Kryptosystem absolut sicher, so gilt $p(y_1) = p(y_2)$ für alle $y_1, y_2 \in C$.

(b) In jedem Kryptosystem gilt $\mathcal{H}(S|Y) \ge \mathcal{H}(X|Y)$.

(c) In einem absolut sicheren Kryptosystem gilt $\mathcal{H}(X) \le \mathcal{H}(S)$.