Übungen zur Kryptologie 1 Wintersemester 07/08

*Johannes Köbler/Sebastian Kuhnert*

# Übungsblatt 6

**Aufgabe 24** (mündlich)

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

**Aufgabe 25** (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 26** (mündlich)

Sei $S = (M, C, E, D, K)$ 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 $\|K\|(\|K\| - 1) < \|M\|$ 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 27** (schriftlich, 10 Punkte)

Zeigen oder widerlegen Sie folgende Aussagen:

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

b) In einem absolut sicheren Kryptosystem gilt $\mathcal{H}(X) \leq \mathcal{H}(K)$.

c) In jedem Kryptosystem gilt $\mathcal{H}(K|Y) \geq \mathcal{H}(X|Y)$.