Übungen zur Kryptologie 1 — Wintersemester 2003-2004

Johannes Köbler/Lorenz Weizsäcker

Übungsblatt 6

Aufgabe 21

Es liege ein symmetrisches Kryptosystem vor mit $\|K\| < \|M\|$, d. h. der Schlüsselraum K ist kleiner als der Nachrichtenraum M. Zeigen Sie, dass das Kryptosystem nicht informationstheoretisch sicher sein kann.

Aufgabe 22

Gegeben sei ein Kryptosystem mit Klartextraum $M = \{a, b\}$, wobei $p(a) = 1/4$ und $p(b) = 3/4$, Schlüsselraum $K = \{k_1, k_2, k_3\}$, wobei $p(k_1) = 1/2$ und $p(k_2) = p(k_3) = 1/4$ und dem Kryptotextraum $C = \{1, 2, 3, 4\}$. Die Verschlüsselungsfunktion ist definiert durch

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

a) Berechnen Sie die (bedingten) Wahrscheinlichkeiten $p(y)$ und $p(x|y)$ für alle Klartextnachrichten $x \in M$ und Kryptotextnachrichten $y \in C$.

b) Berechnen Sie die Entropie $\mathcal{H}(X)$ der Klartexte, sowie die Entropie $\mathcal{H}(K)$ des Schlüssels und die Entropie $\mathcal{H}(Y)$ der Kryptotexte.

c) Berechnen Sie die bedingte Entropie $\mathcal{H}(K|Y)$.

Aufgabe 23 (schriftlich, 10 Punkte)

Zeigen Sie, dass ein Kryptosystem mit $\|K\| = \|C\| = \|M\|$ genau dann absolut sicher ist, wenn jeder Schlüssel mit gleicher Wahrscheinlichkeit $1/\|K\|$ verwendet wird, und es für jedes $x \in M$ und jedes $y \in C$ genau einen Schlüssel k mit $E(k, x) = y$ gibt.

Aufgabe 24

Seien X und Y Zufallsvariablen. Dann ist $\mathcal{H}(X, Y) = \sum_{x,y} p(x, y) \cdot \log(1/p(x,y))$ 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) $\mathcal{H}(X, Y) \leq \mathcal{H}(X) + \mathcal{H}(Y)$, wobei Gleichheit genau dann eintritt, wenn X und Y unabhängig sind.