Übungen zur Kryptologie 1 — Wintersemester 05/06

Johannes Köbler/Olaf Beyersdorff

Übungsblatt 6

Aufgabe 21 (mündlich)

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 $C = \{1, 2, 3, 4\}$, sowie nebenstehender Verschlüsselungsfunktion.

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 Klartexte $x \in M$ und Kryptotexte $y \in C$.

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

Aufgabe 22 (mündlich)

Zeigen Sie:

a) 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 $\|C\| = \|M\|$ und $p(x) > 0$ für alle $x \in M$ ist dies auch notwendig.

b) Ein Kryptosystem mit $\|K\| < \|M\|$ und $p(x) > 0$ für alle $x \in M$ ist nicht absolut sicher.

c) Ein Kryptosystem ist genau dann absolut sicher, wenn $\mathcal{H}(X|Y) = \mathcal{H}(X)$ ist.

d) Ist ein Kryptosystem mit $p(x) > 0$ für alle $x \in M$ absolut sicher, dann ist es unter allen Klartextverteilungen absolut sicher.

Aufgabe 23 (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 24 (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 $\mathcal{H}(K|Y) \geq \mathcal{H}(X|Y)$.