

## Übungsblatt 5

### Aufgabe 21

Gegeben sei ein Kryptosystem mit Klartextrraum  $M = \{a, b\}$ , 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 Kryptotextrraum  $C = \{1, 2, 3, 4\}$ , sowie nebenstehender Verschlüsselungsfunktion.

*mündlich*

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

- Berechnen Sie die (bedingten) Wahrscheinlichkeiten  $p(y)$  und  $p(x | y)$  für alle Klartexte  $x \in M$  und Kryptotexte  $y \in C$ .
- 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:

- 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.
- Ein Kryptosystem mit  $\|K\| < \|M\|$  und  $p(x) > 0$  für alle  $x \in M$  ist nicht absolut sicher.
- Ein Kryptosystem ist genau dann absolut sicher, wenn  $\mathcal{H}(X | Y) = \mathcal{H}(X)$  ist.
- 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:

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

### Aufgabe 24

**10 Punkte**

Zeigen oder widerlegen Sie folgende Aussagen:

- Ist ein Kryptosystem absolut sicher, so gilt  $p(y_1) = p(y_2)$  für alle  $y_1, y_2 \in C$ .
- In einem absolut sicheren Kryptosystem gilt  $\mathcal{H}(X) \leq \mathcal{H}(K)$ .
- In jedem Kryptosystem gilt  $\mathcal{H}(K | Y) \geq \mathcal{H}(X | Y)$ .