**Aufgabe 4.1** (1+2+2 Pkt.)

Seien $X$, $Y$ zwei Zufallsvariablen, die endlich viele Werte $x_1, \ldots, x_m$ bzw. $y_1, \ldots, y_n$ annehmen können. Beweisen Sie ausgehend von den Definitionen aus der Vorlesung:

a) $H(X|Y) = H(X,Y) - H(Y)$

b) $H(X) \leq H(X,Y)$

c) $I(X,Y) \geq 0$

*Tipp:* Die Logarithmusfunktion ist konkav, für jede Wahrscheinlichkeitsverteilung $(p_1, \ldots, p_k)$ sowie positive Zahlen $z_1, \ldots, z_k$ gilt also $p_1 \log z_1 + \ldots + p_k \log z_k \leq \log(p_1 z_1 + \ldots p_k z_k)$.

**Aufgabe 4.2** (3 Pkt.)

Wie in der Vorlesung verwenden wir die Variablen $M$, $K$ und $C$ zur Bezeichnung der Zufallsvariablen, die Klartext, Schlüssel und Chiffre eines Verschlüsselungsverfahrens repräsentieren. Zeigen Sie: Für jedes absolut sichere Verschlüsselungsverfahren (mit deterministischer Verschlüsselungsfunktion und deterministischer Entschlüsselungsfunktion) gilt

$$H(M) \leq H(C) \leq H(K)\,.$$

**Aufgabe 4.3** (3 Pkt.)

Betrachten Sie ein Kryptosystem mit

- möglichen Klartexten $\mathcal{M} = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$,
- möglichen Schlüsseln $\mathcal{K} = \{\mathtt{k}_1, \mathtt{k}_2, \mathtt{k}_3\}$,
- möglichen Chiffretexten $\mathcal{C} = \{\mathtt{1}, \mathtt{2}, \mathtt{3}, \mathtt{4}\}$.

Die Verschüsselung erfolgt nach folgender Matrix:

| | a | b | c |
|---|---|---|---|
| $\mathtt{k}_1$ | 1 | 2 | 3 |
| $\mathtt{k}_2$ | 2 | 3 | 4 |
| $\mathtt{k}_3$ | 3 | 4 | 1 |

Angenommen, die Schlüssel werden unabhängig vom Klartext und gleichverteilt ausgesucht und für die Klartexte gilt $\Pr[M = \mathtt{a}] = 1/2$, $\Pr[M = \mathtt{b}] = 1/3$, $\Pr[M = \mathtt{c}] = 1/6$. Berechnen Sie $H(M)$, $H(C)$, $H(K)$, $H(K|C)$ und $H(M|C)$ ($M, K, C$ wie in Aufgabe 4.2). Ist die Verschlüsselung absolut sicher?

**Aufgabe 4.4** (1 Pkt.)

Moderne Kryptosysteme verwenden einen kleinen Schlüssel, um lange Nachrichten zu verschlüsseln. Sind diese Systeme absolut sicher? Begründen Sie Ihre Antwort.

**Aufgabe 4.5** (4 Pkt.)

Lösen Sie die SPOX-Aufgabe Lineare Komplexität.