Spezielle Aspekte: Kryptographie *SoSe 2011*
PD Dr. Barbara Baumeister
Tutoren: Patrick Wegener, Philipp Neumann, Patrick Odenbach

5. Übungsblatt

Abgabe: Mittwoch, 11.5.11

Aufgabe 1 *Sei $|\mathcal{C}| = |\mathcal{K}| = |\mathcal{P}| < \infty$ und sei $P(x) > 0$ für jeden Klartext $x \in \mathcal{P}$. Wir nehmen an, dass das Kryptosystem $\mathbb{K}$ perfekt sicher ist. Zeigen Sie:*

(a) Sei $x \in \mathcal{P}$ und $y \in \mathcal{C}$. Dann gibt es einen Schlüssel $k \in \mathcal{K}$ so, dass $e_k(x) = y$ gilt.

(b) Der Schlüssel aus (a) ist eindeutig: Gilt $e_l(x) = y$ für ein $l \in \mathcal{K}$, dann folgt $l = k$.

Aufgabe 2 *Die Voraussetzungen seien wie in Aufgabe 1. Zeigen Sie, dass die Wahrscheinlichkeitsverteilung auf der Menge der Schüssel $\mathcal{K}$ die Gleichverteilung ist.*

Aufgabe 3 *Seien M und N endliche Mengen derselben Mächtigkeit, d.h. $|M| = |N|$, und sei $f : M \to N$ eine Abbildung, die surjektiv ist. Zeigen Sie:*

(a) Ist $|M| = |N| < \infty$, dann ist f bijektiv.

(b) Gilt die Aussage auch, falls $|M| = |N| = \infty$? Beweisen Sie die Aussage oder geben Sie ein Gegenbeispiel an.

Aufgabe 4 *Überprüfen Sie, ob die Abbildung $g : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ definiert durch*

$$x \mapsto Mx$$

$$\text{mit} \quad M := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

eine bijektive Abbildung ist.