Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 20.11.2015

Einführung in Kryptographie

WS 2015/2016

Präsenzübungszettel 3

AUFGABE 1:
Betrachten Sie ein Kryptosystem mit $\mathcal{P} = \{x, y, z\}$, $\mathcal{C} = \{1, 2, 3\}$ und $\mathcal{K} = \{k_1, k_2, k_3\}$. Die Verschlüsselungsfunktionen in $\mathcal{E}$ seien durch folgende Tabelle gegeben:

$m =$	x	y	z
$E_{k_1}(m) =$	1	2	3
$E_{k_2}(m) =$	2	3	1
$E_{k_3}(m) =$	3	2	1

Angenommen, der Schlüssel $k \in \mathcal{K}$ wird unabhängig vom Klartext und zufällig gleichverteilt gewählt. Ausserdem sei folgende Verteilung auf dem Klartextraum $\mathcal{P}$ gegeben:

$$\Pr(x) = \frac{1}{4}, \qquad \Pr(y) = \frac{1}{4}, \qquad \Pr(z) = \frac{1}{2}.$$

Bestimmen Sie $\Pr(m \,|\, c)$ für alle $m \in \mathcal{P}$ und alle $c \in \mathcal{C}$. Ist das Kryptosystem perfekt geheim?

AUFGABE 2:
Zeigen Sie: wenn ein Kryptosystem mit $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| < \infty$ und $\Pr(p) > 0$ für alle $p \in \mathcal{P}$ perfekt geheim ist, dann gilt für alle Chiffretexte $c \in \mathcal{C}$:

$$\Pr(c) = \frac{1}{|\mathcal{C}|}.$$

AUFGABE 3:
Sei im Folgenden $\Pr(p) > 0$ für alle $p \in \mathcal{P}$. Zeigen Sie:

a) Ein Kryptosystem ist genau dann perfekt geheim, wenn für alle Klartext $p \in \mathcal{P}$ und alle Chiffretexte $c \in \mathcal{C}$ gilt:
$$\Pr(c \,|\, p) = \Pr(c).$$

b) Ein Kryptosystem ist genau dann perfekt geheim, wenn für alle Klartexte $p, p' \in \mathcal{P}$ und alle Chiffretexte $c \in \mathcal{C}$ gilt:
$$\Pr(c \,|\, p) = \Pr(c \,|\, p').$$