André Bajorat
Rasmus Diederichsen
Lisa Goerke

Sebastian Höffner
Kristin Schmidt

Lösungen zu Übungsblatt 2
Kryptographische Verfahren

Besprechung 30. Oktober 2015

Aufgabe 2.1. Multiplikation von Resten

a)

Gäbe es ein inverses Element bezüglich $\odot_n$, so könnte man Folgendes rechnen:

$$\begin{aligned} [km]_n &= \left[km'\right] \\ k \odot_n m &= k \odot_n m' \\ m &= m' \end{aligned}$$

Gibs aber nicht. $\mathbb{Z}_n$ mit $\odot_n$ ist keine Gruppe, weil 0 kein Inverses haben kann $(0 \cdot ? = 1)$. Also habe ich einen ganzen Tag ohne Fortschritt mit der Suche nach einer anderen Begründung verbracht. Jetzt ist es 9 Uhr. #fuckmylife

Noch ne Idee:

$$\begin{aligned} [km]_n - \left[km'\right] &= 0 \\ k \odot_n m - k \odot_n m' &= 0 \\ \left[km - km'\right]_n &= 0 \\ \left[k \cdot (m - m')\right]_n &= 0 \\ k \odot_n (m - m') &= 0 \end{aligned}$$

Das bedutet, dass n $k \odot_n (m - m')$ teilt. Nach Vorraussetzung sind n und k teilerfremd, sodass n stattdessen $(m - m')$ teilen muss. Da $m, m' \in \mathbb{Z}_n$, kann $[m - m'] = 0$ nur gelten, falls $m = m'$.

b)

Für die Injektivität ist Folgendes zu zeigen.

$$E_k(m_1) = E_k(m_2) \Rightarrow m_1 = m_2$$

$$\begin{aligned} [m_1 k + l]_n &= [m_2 k + l]_n \\ [m_1 k]_n \oplus_n [l]_n &= [m_2 k]_n \oplus_n [l]_n \\ [m_1 k]_n \oplus_n l \oplus_n (n - l) &= [m_2 k]_n \oplus_n l \oplus_n (n - l) \\ [m_1 k]_n &= [m_2 k]_n \end{aligned}$$

Nach Teilaufgabe a) folgt hieraus $m_1 = m_2$. $\square$

Aufgabe 2.2. Die Wahrscheinlichkeit von Kryptotexten in perfekt sicheren Kryptosystemen

Sei Y die Zufallsvariable über den möglichen Kryptotexten $y \in \mathcal{C}$. Sei mit $\mathcal{C}(k) = \{c \in \mathcal{C} \mid \exists x \in \mathcal{M} : E_k(x) = c\}$ die Menge der durch einen Schlüssel k in Abhängigkeit des Klartextes erzeugbaren Kryptotexte bezeichnet. Für die Wahrscheinlichkeit, einen bestimmten Kryptotext zu erhalten, gilt

$$
\begin{aligned}
P(Y = y) &= \sum_{\{k|y \in \mathcal{C}(k)\}} P(K = k, E_k(x) = y) \\
P(Y = y) &= \sum_{\{k|y \in \mathcal{C}(k)\}} P(K = k, X = E_k^{-1}(y)) \\
&= \sum_{\{k|y \in \mathcal{C}(k)\}} P(K = k)\ P(X = E_k^{-1}(y)) && \text{Schlüssel und Klartext unabhängig} \\
&= \frac{1}{|\mathcal{K}|} \sum_{\{k|y \in \mathcal{C}(k)\}} P(X = E_k^{-1}(y)) && \text{Schlüssel gleichverteilt}
\end{aligned}
$$

Da das System perfekt sicher ist, E_k injektiv sowie $|\mathcal{C}| = |\mathcal{M}|$, gibt es für jedes $(x, y) \in \mathcal{M} \times \mathcal{C}$ genau ein k mit $E_k(x) = y$.

$$
= \frac{1}{|\mathcal{K}|} \sum_{\{k|y \in \mathcal{C}(k)\}} \frac{1}{|\mathcal{K}|}
$$

Da E_k injektiv ist, muss jedes k auf $|\mathcal{M}| = |\mathcal{C}|$ verschiedene Kryptotexte abbilden. Dies bedeutet aber auch, dass jeder Kryptotext $c \in \mathcal{C}$ durch jedes $k \in \mathcal{K}$ generiert werden kann. Die obige Summe iteriert folglich über komplett $\mathcal{K}$, somit

$$
P(Y = y) = \frac{1}{|\mathcal{K}|} \cdot 1
$$

$\square$