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:

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

Gibs aber nicht. $\mathbb{Z}_n$ mit $\odot_n$ ist keine Gruppe, weil 0 schonmal 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:

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

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 $m_1 = m_2$.