André Bajorat Rasmus Diederichsen Lisa Goerke

## 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:

$$[km]_{n} = [km']$$

$$k \odot_{n} m = k \odot_{n} m'$$

$$[k]_{n} \odot_{n} [m]_{n} = [k]_{n} \odot_{n} [m']_{n}$$

$$k \odot_{n} m = k \odot_{n} m'$$

$$m = m'$$

Gibs aber nicht. Also habe ich einen ganzen Tag ohne Fortschritt mit der Suche nach einer anderen Begründung verbracht. Jetzt ist es 9 Uhr. #fuckmylife

b)

Für die Injektivität ist Folgendes zu zeigen.

$$E_k(\mathfrak{m}_1) = E_k(\mathfrak{m}_2) \Rightarrow \mathfrak{m}_1 = \mathfrak{m}_2$$

$$\begin{split} [\mathfrak{m}_1 k + \mathfrak{l}]_{\mathfrak{n}} &= [\mathfrak{m}_2 k + \mathfrak{l}]_{\mathfrak{n}} \\ [\mathfrak{m}_1 k]_{\mathfrak{n}} \oplus_{\mathfrak{n}} [\mathfrak{l}]_{\mathfrak{n}} &= [\mathfrak{m}_2 k]_{\mathfrak{n}} \oplus_{\mathfrak{n}} [\mathfrak{l}]_{\mathfrak{n}} \\ [\mathfrak{m}_1 k]_{\mathfrak{n}} \oplus_{\mathfrak{n}} \mathfrak{l} \oplus_{\mathfrak{n}} (\mathfrak{n} - \mathfrak{l}) &= [\mathfrak{m}_2 k]_{\mathfrak{n}} \oplus_{\mathfrak{n}} \mathfrak{l} \oplus_{\mathfrak{n}} (\mathfrak{n} - \mathfrak{l}) \\ [\mathfrak{m}_1 k]_{\mathfrak{n}} &= [\mathfrak{m}_2 k]_{\mathfrak{n}} \end{split}$$

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