Kryptographie *WS 2012/13*
Barbara Baumeister

1. Übungsblatt

Abgabe: Donnerstag, 18.11,2013

Aufgabe 1 (a) Betrachten Sie auf $\mathbb{Z}_m$ die Multiplikation:

$$\overline{a} \odot \overline{b} := \overline{ab} \text{ for } \overline{a}, \overline{b} \in \mathbb{Z}_m.$$

Zeigen Sie an einem Beispiel, dass aus $\overline{a} \odot \overline{b} = \overline{a} \odot \overline{c}$ nicht $\overline{b} = \overline{c}$ folgen muss.

(b) Berechnen Sie ohne Taschenrechner 2^{19} mod 7.

Aufgabe 2 Sei $\mathcal{A} := \mathbb{Z}_2$, $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$ für ein $n \in \mathbb{N}$ und $\mathcal{K} = S_n$. Setzte für $\pi \in \mathcal{K}$ und $(a_1, \ldots, a_n) \in \mathcal{P}$

$$e_\pi((a_1, \ldots, a_n)) = (a_{\pi(1)}, \ldots, a_{\pi(n)}) \text{ und } d_\pi((a_1, \ldots, a_n)) = (a_{\pi^{-1}(1)}, \ldots, a_{\pi^{-1}(n)}).$$

Zeigen Sie, dass die Chiffre $\mathbb{K} := (\mathcal{P}, \mathcal{C}, \mathcal{K}, e, d)$ linear ist, d.h. dass e eine lineare Abbildung von dem $\mathbb{Z}_2$-Vektorraum $\mathbb{Z}_2^n$ in sich ist.

Aufgabe 3 Seien $n, r \in \mathbb{N}$. Zeigen Sie:
$A \in \mathbb{Z}_n^{r \times r}$ ist genau dann invertierbar über $\mathbb{Z}_n$, wenn $\det(A)$ invertierbar ist in $(\mathbb{Z}_n \setminus \{0\}, \cdot)$.

Aufgabe 4 Entschlüsseln Sie:
ihurnlolptupz