Spezielle Aspekte: Kryptographie *SoSe 2011*
PD Dr. Barbara Baumeister
Tutoren: Patrick Wegener, Philipp Neumann, Patrick Odenbach

6. Übungsblatt

Abgabe: Mittwoch, 18.5.11

Aufgabe 1 *(a) Probieren Sie AES auf Cryptool-online aus (es ist dort unter Highlights aufgeführt).*

(b) Finden Sie den Unterschied zwischen CBC und ECB heraus.

Aufgabe 2 *Zeigen Sie, dass $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ irreduzibel ist, d.h. ist $f = f_1 \cdot f_2$ mit $f_1, f_2 \in \mathbb{Z}_2[x]$, dann folgt $f_1 = f$ und $f_2 = 1$ oder umgekehrt.*

Aufgabe 3 *Sei L ein Körper, der $\mathbb{Z}_2$ enthält und der ein α mit $f(\alpha) = 0$ enthält (f das Polynom aus Aufgabe 2). Setze*

$$\mathbb{K} := \{a_1\alpha + a_0 \mid a_i \in \mathbb{Z}_2\}.$$

(a) Zeigen Sie: Es gilt $(a_1\alpha + a_0) + (b_1\alpha + b_0) = (a_1 + b_1)\alpha + (a_0 + b_0)$ für alle $a_0, a_1, b_0, b_1 \in \mathbb{Z}_2$.

(b) Schreiben Sie die Verknüpfungstabelle von $(\mathbb{K}, +)$ auf.

(c) Zeigen Sie: Es gilt $-k = k$ für alle $k \in \mathbb{K}$.

Aufgabe 4 *Leiten Sie aus $f(\alpha) = 0$ die Verknüpfungstabelle von $(\mathbb{K}, \cdot)$ her.*