Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

12. Übungsblatt

Abgabe: Donnerstag, 28.1.2016

Aufgabe 1 Sei p eine Primzahl mit $p \equiv 3 \pmod 4$ und sei

$$E_p = E(\mathbb{F}_p) : y^2 = x^3 + x.$$

Zeigen Sie, dass $|E_p| = p + 1$.

Aufgabe 2 Für $\pi \in S_3$ sei e_π die Permutation der Bits für Wörter der Länge 3. Weiter sei $\oplus$ die Addition in $\mathbb{Z}_2^3$. Bestimmen Sie für jedes $\pi \in S_3$ die Anzahl der Kollisionen der Kompressionsfunktion $h_\pi(x) = e_\pi(x) \oplus x$.

Aufgabe 3 Sei $h : \mathbb{Z}_2^\infty \to \mathbb{Z}_2^\infty$ die Hashfunktion

$$k \mapsto \lfloor 10000(k(1+\sqrt{5})/2 \pmod 1)) \rfloor,$$

wobei k mit der durch es dargestellten natürlichen Zahl identifiziert wird und r mod $1 := r - \lfloor r \rfloor$ für eine positive reelle Zahl r.

(a) Bestimmen Sie die maximale Länge der Bilder.

(b) Geben Sie eine Kollision dieser Hashfunktion an.

Aufgabe 4 Seien $x \neq x'$ binäre Folgen endlicher Länge und seien $x_1 \dots x_t$ bzw. $x'_1 \dots x'_{t'}$ die zugehörigen Bitfolgen mittels derer nach der Konstruktion aus der Vorlesung die Hash-Werte von x und x' bestimmt werden. Zeige: Ist $t \leq t'$, so existiert ein $0 \leq i < t$ mit $x_{t-i} \neq x'_{t'-i}$.