Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 6 / 17./19. Januar 2011

AUFGABE 1. Doppelte Hashfunktion.
Sei (Gen, H) eine kollisionsresistente Hashfunktion. Betrachten Sie nun die Hashfunktion $\mathsf{Gen}, \hat{H}$ mit

$$\hat{H}_s(x) := H_s(H_s(x)) \ .$$

Ist die neue Hashfunktion kollisionsresistent?

AUFGABE 2. Kollisionsresistente Kandidaten?
Untersuchen Sie, ob die folgenden Kompressionsfunktionen (Gen, H) mit $H : \{0,1\}^{2n} \to \{0,1\}^n$ kollisionsresistent sind.

a) $\mathsf{Gen}(1^n) \to s \in_R \{0,1\}^n$ gibt zufälligen Bitstring s aus. s definiert eine Kompressionsfunktion $f_s : \{0,1\}^{2n} \to \{0,1\}^n$ durch

$$x = (x_1, \ldots, x_{2n}) \mapsto (x_1, \ldots, x_n) \oplus (s_1, \ldots, s_n) \ .$$

b) $\mathsf{Gen}(1^n) \to \mathbf{S} \in_R \mathbb{Z}_2^{n \times 2n}$ gibt zufällige $(n \times 2n)$-Matrix mit vollem Rang $\mathrm{rank}(\mathbf{S}) = n$ über $\mathbb{Z}_2$ aus. Die Matrix $\mathbf{S}$ definiert eine Kompressionsfunktion $H_{\mathbf{S}} : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2^n$ durch

$$\mathbf{x} \mapsto \mathbf{Sx} \ .$$

AUFGABE 3. Merkle-Damgard verallgemeinert.
Verallgemeinern Sie die Merkle-Damgard Tranformation aus der Vorlesung (siehe Folie 126) für beliebige Kompressionsfunktionen $h : \{0,1\}^\ell \to \{0,1\}^{\ell'}$ mit $\ell > \ell'$.