Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 0 / Vorübung / 12. April 2013

Definition (Hashfunktion): Eine Hashfunktion ist ein Paar $\Pi = (\mathsf{Gen}, H)$ von pt Algorithmen mit

Gen: Wähle ein (öffentlich bekanntes) $s \leftarrow \mathsf{Gen}(1^n)$, das eine konkrete Hashfunktion beschreibt. Gen ist probabilistisch.

H: H_s berechnet eine Funktion $\{0,1\}^* \rightarrow \{0,1\}^{\ell(n)}$. H_s ist deterministisch.

Definition (Kollisionsresistenz): Eine Hashfunktion $\Pi = (\mathsf{Gen}, H)$ heißt kollisionsresistent, falls <u>für alle</u> ppt-Algorithmen $\mathcal{A}$ gilt, dass $\mathsf{Ws}[\mathsf{HashColl}_{\mathcal{A},\Pi}(n) = 1] \leq \mathsf{negl}(n)$.

AUFGABE 1:

(a) Sei $\Pi = (\mathsf{Gen}, H)$ eine kollisionsresistente Hashfunktion. Zeigen Sie, dass dann aber $\hat{\Pi} = (\mathsf{Gen}, \hat{H})$ mit $\hat{H}_s(x) := H_s(x) \oplus H_s(\bar{x})$ <u>keine</u> kollisionsresistente Hashfunktion ist. Wir bezeichnen mit $\bar{x}$ das Komplement von x, z.B. $\overline{110} = 001$.

(b) Sei $\Pi = (\mathsf{Gen}, H)$ eine kollisionsresistente Hashfunktion. Zeigen Sie, dass dann auch $\hat{\Pi} = (\mathsf{Gen}, \hat{H})$ mit $\hat{H}_s(x) := (H_s(x), H_s(\bar{x}))$ eine kollisionsresistente Hashfunktion ist.

AUFGABE 2:

- Berechnen Sie $17^{8000039}$ mod 55 ohne Taschenrechner.
- Berechnen Sie 21^{144} mod 91 ohne Taschenrechner.

Definition (Gruppe): Eine abelsche Gruppe $(G, \cdot)$ ist abgeschlossen, kommutativ, assoziativ und besitzt ein neutrales Element. Zudem besitzt *jedes* Element in G ein Inverses Element.

AUFGABE 3:

Sei $N \in \mathbb{N}$. Zeigen Sie, dass $\mathcal{QR}_N := \{x \in \mathbb{Z}_N^* \mid \text{es existiert ein } y \in \mathbb{Z}_N^* \text{ mit } y^2 = x \bmod N\}$ (zusammen mit der Multiplikation modulo N) eine multiplikative, abelsche Gruppe ist.

AUFGABE 4:

Bestimmen Sie $\left(\frac{2}{7}\right)$, $\left(\frac{3}{11}\right)$ und, falls existent, alle Wurzeln von 58 modulo 77.