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

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 3 / 11. und 13. Mai 2011

AUFGABE 1. Gegenangriff.
Betrachten Sie den in der Vorlesung vorgestellten Chosen-Ciphertext Angriff auf das ElGamal-Verfahren. Ein Angreifer beobachtet dabei einen Chiffretext $c = \langle c_1, c_2 \rangle = \langle g^y, h^y \cdot m \rangle$ und sendet anschließend den Chiffretext $c' = \langle c_1, c_2 \cdot m' \rangle$, der eine gültige Verschlüsselung der Nachricht $m \cdot m'$ ist.
Angenommen der Empfänger findet es verdächtig, wenn zwei Verschlüsselungen mit der gleichen ersten Komponente an ihn gesendet werden und verwirft den zweiten Chiffretext. Zeigen Sie, wie ein Angreifer dieses Problem beseitigen kann!

AUFGABE 2. Konstruktives.
Sei $\mathcal{G}$ ein Algorithmus der bei Eingabe 1^n eine n-bit Primzahl p und einen Generator g für die multiplikative Gruppe $\mathbb{Z}_p^*$ ausgibt. Zeigen Sie, dass die Schwierigkeit des *diskreten Logarithmus Problems* bezüglich einer von $\mathcal{G}$ ausgegebenen Gruppe die Existenz einer Familie von Einwegpermutationen impliziert, d.h. konstruieren Sie ein Tupel $\Pi = (\mathsf{Gen}, \mathsf{Samp}, f)$ gemäß Folie 60 und zeigen Sie die Einwegeigenschaft.

AUFGABE 3. Einbahnstraße.
Wir beschäftigen uns mit einigen Details zum Thema Einwefunktionen und -permutationen:

a) Diskutieren Sie, warum es notwendig ist, dem Invertierer $\mathcal{A}$ aus dem Spiel $\mathsf{Invert}_{\mathcal{A},f}(n)$ (siehe Folie 53) zusätzlich zur Eingabe y auch die Eingabe 1^n zu übergeben!

b) Sei $\{0,1\}^n \to \{0,1\}^n$ eine Funktion und sei $y = f(0^n)$. Sei $|f^{-1}(y)|/2^n > \mathsf{negl}(n)$, d.h. das Urbild von $f(0^n)$ enthalte mehr als vernachlässigbare viele Elemente. Zeigen Sie, dass f dann keine Einwegfunktion sein kann, indem Sie einen effizienten Invertierer $\mathcal{A}$ für f angeben!

AUFGABE 4. Harte Kerne.
Sei $\mathsf{hc} : \{0,1\}^* \to \{0,1\}$ ein Hardcore-Prädikat für eine beliebige Funktion $f : \{0,1\}^* \to \{0,1\}^*$. Zeigen Sie, dass hc *erwartungstreu (auch unbiased)* ist, d.h.

$$\left|\mathbf{Pr}_{x \in_R \{0,1\}^n}[\mathsf{hc}(x) = 0] - \mathbf{Pr}_{x \in_R \{0,1\}^n}[\mathsf{hc}(x) = 1]\right| \leq \mathsf{negl}(n)$$