Institut für Informatik
Komplexität und Kryptografie
Prof. Dr. Johannes Köbler

Sommersemester 2006

Übungen zur Kryptologie 2

1. Aufgabenblatt

Aufgabe 1

Sei $f : \{0,1\}^k \to \{0,1\}^k$ wie folgt definiert (dabei identifizieren wir $\{0,1\}^k$ mit $\mathbb{Z}_{2^k}$)

$$f(x) = x^2 + ax + b \bmod 2^k.$$

Zeigen Sie, dass f nicht schwach kollisionsresistent ist.

Aufgabe 2

Sei $k > l$ und seien $a_i \in \mathbb{Z}_{2^l}$ für $i = 0, \ldots, d$ mit $a_d \neq 0$. Zeigen Sie, dass die durch

$$f(x) = \sum_{i=0}^{d} a_i x^i \bmod 2^l$$

definierte Funktion $f : \{0,1\}^k \to \{0,1\}^l$ nicht schwach kollisionsresistent ist.

Aufgabe 3

Sei $f : \{0,1\}^m \to \{0,1\}^m$ eine Einwegpermutation. Zeigen Sie, dass die durch

$$h(x_1 x_2) = f(x_1 \oplus x_2),\ x_1, x_2 \in \{0,1\}^m$$

definierte Funktion $h : \{0,1\}^{2m} \to \{0,1\}^m$ nicht schwach kollisionsresistent ist.

Aufgabe 4

Seien $h_i : X \to Y_i$ (n, m_i)-Hashfunktionen (für $i = 1, 2$), von denen mindestens eine kollisionsresistent ist. Zeigen Sie, dass dann die Funktion

$$h(x) = h_1(x) h_2(x)$$

kollisionsresistent ist.

Aufgabe 5

Sei $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ kollisionsresistent. Zeigen Sie, dass dann die durch

$$h_i(x_1 x_2) = h_1(h_{i-1}(x_1) h_{i-1}(x_2)),\ x_1, x_2 \in \{0,1\}^{2^{i-1} m}$$

induktiv definierte Hashfunktion h_i $(i \geq 2)$ kollisionsresistent auf $X_i = \{0,1\}^{2^i m}$ ist.

Aufgabe 6

Sei $n = pq$ für zwei Primzahlen $p > q$. Betrachten Sie die Funktion

$$h(x) = x^2 \bmod n, \ x \in \mathbb{Z}_n^*.$$

Welche Eigenschaften (Einweg-Hashfunktion, (schwache) Kollisionsresistenz) hat h, falls n nur mit sehr hohem Aufwand faktorisiert werden kann?

Aufgabe 7

Für eine (n, m)-Hashfunktion $h : X \to Y$ und für $y \in Y$ sei

$$h^{-1}(y) = \{x \in X \mid h(x) = y\}$$

die Menge aller Texte mit Hashwert y.

a) Bestimmen Sie die Verteilung und den Erwartungswert $\overline{s}$ der Zufallsvariablen $S_y = \|h^{-1}(y)\|$ im ZOM.

b) Zeigen Sie:

$$\sum_{y \in Y} (S_y - \overline{s})^2 = 2S + n - n^2/m,$$

wobei die Zufallsvariable S die Anzahl $\|\{\{x, x'\} \in \binom{X}{2} \mid h(x) = h(x')\}\|$ aller Kollisionspaare von h bestimmt.

c) Zeigen Sie, dass

$$S \geq \frac{1}{2} \left(\frac{n^2}{m} - n \right)$$

ist, wobei Gleichheit nur im Fall $S_y = n/m$ für alle $y \in Y$ eintritt.

Aufgabe 8 (10 Punkte)

Sei $h : X \to Y$ eine beliebige, aber feste (n, m)-Hashfunktion.

a) Zeigen Sie, dass für zufällig unter Gleichverteilung aus X gewählte Texte x_1, x_2

$$Pr[h(x_1) = h(x_2)] \geq 1/m$$

ist, wobei Gleichheit nur im Fall $\|h^{-1}(y)\| = n/m$ für alle $y \in Y$ eintritt.

b) Bestimmen Sie die Erfolgswahrscheinlichkeit $\varepsilon(h, y)$ von FindPreimage(h, y, q), falls für X_0 eine zufällige Teilmenge von X der Größe q gewählt wird.

c) Berechnen Sie die durchschnittliche Erfolgswahrscheinlichkeit $\varepsilon(h, q)$ von FindPreimage(h, y, q), falls X_0 wie in b) und y zufällig aus Y gewählt werden.

d) Bestimmen Sie $\varepsilon(h, 1)$.