Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

WS 2002/3

Übungen zur Kryptologie II

2. Übung

Aufgabe 1

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 2

Sei $f : \{0,1\}^m \to \{0,1\}^m$ eine Einwegpermutation. Zeigen Sie, dass die Funktion $h : \{0,1\}^{2m} \to \{0,1\}^m$, definiert durch

$$h(x_1x_2) = f(x_1 \oplus x_2),\ x_1, x_2 \in \{0,1\}^m$$

nicht schwach kollisionsresistent ist.

Aufgabe 3

Sei $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ eine kollisionsresistente Hashfunktion.

a) Zeigen Sie, dass die Funktion $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$, definiert durch

$$h_2(x_1x_2) = h_1(h_1(x_1)h_1(x_2)),\ x_1, x_2 \in \{0,1\}^{2m}$$

dann auch kollisionsresistent ist.

b) Zeigen Sie, dass die rekursiv durch

$$h_i(x_1x_2) = h_1(h_{i-1}(x_1)h_{i-1}(x_2)),\ x_1, x_2 \in \{0,1\}^{2^{i-1}m}$$

definierten Funktionen $h_i : \{0,1\}^{2^i m} \to \{0,1\}^m$, ebenfalls kollisionsresistent sind.

Aufgabe 4

Seien $h_i : X \to Y_i$, $i = 1, 2$, zwei (N, M_i)-Hashfunktionen. Zeigen Sie, dass

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

kollisionsresistent ist, wenn mindestens eine der beiden Hashfunktionen h_1 und h_2 kollisionsresistent ist.

Aufgabe 5 (4 Punkte)

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

a) Bestimmen Sie die Erfolgswahrscheinlichkeit $\varepsilon(h, x, q)$ von FindSecondPreimage(h, x, q), falls für X_0 eine zufällige Teilmenge von $X \setminus \{x\}$ der Größe $q - 1$ gewählt wird.

b) Bestimmen Sie die durchschnittliche Erfolgswahrscheinlichkeit $\varepsilon(h, q)$ von FindPreimage(h, y, q), falls X_0 wie in a) und x zufällig aus X gewählt wird.

c) Bestimmen Sie $\varepsilon(h, 2)$.