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

WS 2002/3

Übungen zur Kryptologie II

1. Übung

Aufgabe 1 (4 Punkte)

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

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

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

b) Zeigen Sie:

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

wobei S die Zufallsvariable $S = \|\{\{x, x'\} \subseteq X \mid h(x) = h(x'), x \neq x'\}\|$ ist.

c) Zeigen Sie für S die untere Schranke

$$S \geq \frac{1}{2}\left(\frac{N^2}{M} - N\right),$$

wobei Gleichheit nur im Fall $S_y = N/M$ für alle $y \in Y$ eintritt.

Aufgabe 2

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

a) Zeigen Sie:

$$Prob[h(x_1) = h(x_2)] \geq 1/M,$$

falls x_1, x_2 zufällig unter Gleichverteilung aus X gewählt werden.

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