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

Sommersemester 2004

Übungen zur Kryptologie 2

3. Übung

Aufgabe 1

Zeigen Sie, dass die in der Vorlesung hergeleitete Entropieschranke für die Impersonationswahrscheinlichkeit α „scharf“ ist. Hinweis: Betrachten Sie einen beliebigen stark universalen MAC.

Aufgabe 2

Zeigen Sie, dass für eine Zufallsvariable X mit endlichem Wertebereich $W(X) \subseteq \mathcal{R}^+$ immer $E(\log X) \leq \log E(X)$ gilt. Hinweis: Ungleichung von Jensen.

Aufgabe 3

Berechnen Sie für den Authentikationscode aus Aufgabe 1 der 1. Übung die Entropiewerte $H(K)$ und $H(K|X, Y)$ und bestimmen Sie die in der Vorlesung hergeleitete Entropieschranke für α. Vergleichen Sie diese Entropieschranke mit dem tatsächlichen Wert von α.

Aufgabe 4

Für eine Hashfunktion $h : X \to Y$ mit $\|X\| = n$ und $\|Y\| = m$ sowie 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.