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

WS 2002/3

Übungen zur Kryptologie II

5. Übung

Aufgabe 1 (4 Punkte)

Konstruieren Sie eine stark universale $(6, 5)$-Hashfamilie und eine stark universale $(13, 3)$-Hashfamilie.

Aufgabe 2

Zeigen Sie, dass die in der Vorlesung hergeleitete Entropieschranke für die Impersonationswahrscheinlichkeit p_{imp} „scharf“ ist. Hinweis: Betrachten Sie eine beliebige stark universale Hashfamilie.

Aufgabe 3

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 4

Schreiben Sie ein Programm, das für den Authentikationscode aus Aufgabe 1 der 3. Übung die Entropiewerte $H(K)$ und $H(K|X)$ und daraus die in der Vorlesung hergeleitete Entropieschranke für p_{imp} berechnet. Vergleichen Sie diese Entropieschranke mit dem tatsächlichen Wert von p_{imp}.