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

SS 2001

Übungen zur Kryptologie II

3. Übung

Aufgabe 1

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

Aufgabe 2 (4 Punkte)

Zeigen Sie, dass die in der Vorlesung hergeleitete Entropieschranke für die Impersonationswahrscheinlichkeit α „scharf“ ist. Hinweis: Betrachten Sie einen Authentikationscode, der auf der Basis einer beliebigen (m, n, l, λ)-Orthogonalmatrix entworfen wurde.

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.