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

Sommersemester 2006

Übungen zur Kryptologie 2

4. Aufgabenblatt

Aufgabe 1

Zeigen Sie, dass für beliebige reelle Zahlen $a_1, \ldots, a_m$ folgende Ungleichung gilt:

$$\left(\sum_{i=1}^{m} a_i\right)^2 \leq m \sum_{i=1}^{m} a_i^2.$$

Aufgabe 2

Sei H eine (n,m)-Hashfamilie mit $\alpha, \beta \leq M^{-1}$. Wie groß muss dann der Schlüsselraum K von H mindestens sein, wenn der Schlüssel unter Gleichverteilung gewählt wird?

Aufgabe 3 (10 Punkte)

Sei X eine Zufallsvariable mit endlichem Wertebereich W und für $x \in W$ sei $p(x) = Pr[X = x]$. Dann ist die **Entropie** von X definiert als $H(X) = \sum_x p(x) Inf_X(x)$, wobei

$$Inf_X(x) = \begin{cases} \log_2(1/p(x)), & p(x) > 0 \\ 0, & \text{sonst} \end{cases}$$

der **Informationsgehalt** von x ist. Für zwei Zufallsvariablen X und Y sei $H(X,Y) = \sum_{x,y} p(x,y) \cdot \log(1/p(x,y))$ die (gemeinsame) Entropie von X und Y. Zeigen Sie:

a) $H(X) \leq \log_2(n)$, wobei $n = \|W\|$ ist und Gleichheit genau im Fall $p(x) = 1/n$ für alle $x \in W$ eintritt.

b) $H(X,Y) = H(Y) + H(X|Y) = H(X) + H(Y|X)$.

c) $H(X,Y) \leq H(X) + H(Y)$, mit Gleichheit genau dann, wenn X und Y unabhängig sind.