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

WS 2002/3

Übungen zur Kryptologie II

4. Übung

Aufgabe 1 (4 Punkte)

a) Konstruieren Sie für jede Primzahl p und jede natürliche Zahl $l \geq 2$ eine stark universale (N, M)-Hashfamilie mit $N = (p^l - 1)/(p-1)$, $M = p$ und $\|K\| = p^l$.

b) Sei $\mathcal{H}$ eine stark universale (N, M)-Hashfamilie. Konstruieren Sie auf der Basis von $\mathcal{H}$ eine stark universale (N, M^l)-Hashfamilie $\mathcal{H}'$ mit $\|K'\| = \|K\|^l$.

Aufgabe 2

Sei A eine $m \times l$-Matrix über einem endlichen Körper K und sei $y \in K^m$. Zeigen Sie, dass das Gleichungssystem

$$Ax = y$$

im Falle der Lösbarkeit genau $\|K\|^{l-r}$ Lösungen besitzt, falls r der Rang von A ist. Geben Sie eine notwendige und hinreichende Bedingung für die Lösbarkeit des Gleichungssystems an.

Aufgabe 3

Zeigen Sie, dass für jede (N, M)-Hashfamilie $\mathcal{H}$ gilt: $p_{sub} = 1/M$ impliziert $p_{imp} = 1/M$.