INSTITUT FÜR INFORMATIK
KOMPLEXITÄT UND KRYPTOGRAFIE
PROF. DR. JOHANNES KÖBLER

SOMMERSEMESTER 2004

Übungen zur Kryptologie 2

2. Übung

Aufgabe 1

a) Konstruieren Sie für jede Primzahl p und jede natürliche Zahl $l \geq 2$ einen stark universalen MAC $(M, T, K, \mathcal{A})$ mit $\|M\| = (p^l - 1)/(p - 1)$, $\|T\| = p$ und $\|K\| = p^l$.

b) Sei $(M, T, K, \mathcal{A})$ ein stark universaler MAC. Konstruieren Sie auf der Basis von $(M, T, K, \mathcal{A})$ einen stark universalen MAC $(M, T', K', \mathcal{A}')$ mit $\|T'\| = \|T\|^l$ und $\|K'\| = \|K\|^l$.

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 dafür an, dass das Gleichungssystems für alle $y \in K^m$ lösbar ist.

Aufgabe 3

Zeigen Sie, dass für jeden MAC $(M, T, K, \mathcal{A})$ gilt: $\beta = 1/\|T\|$ impliziert $\alpha = 1/\|T\|$.

Aufgabe 4

Konstruieren Sie stark universale MACs mit $\|M\| = 6$ und $\|T\| = 5$ sowie $\|M\| = 13$ und $\|T\| = 3$.