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

SS 2001

Übungen zur Kryptologie II

1. Übung

Aufgabe 1 (4 Punkte)

Berechnen Sie die Parameter α und β für den Authentikationscode mit der Matrix:

	a	b	c	d
1	1	1	2	3
2	1	2	3	1
3	2	1	3	1
4	2	3	1	2
5	3	2	1	3
6	3	3	2	1

Die Wahrscheinlichkeitsverteilung auf der Nachrichtenmenge M ist

$$p(a) = p(d) = 1/6, \quad p(b) = p(c) = 1/3$$

und die Wahrscheinlichkeitsverteilung auf der Schlüsselmenge K ist

$$p(1) = p(6) = 1/4, \quad p(2) = p(3) = p(4) = p(5) = 1/8.$$

Geben Sie auch die optimalen Impersonations- und Substitutionsstrategien an.

Aufgabe 2

Sei eine Nachrichtenmenge M und eine Menge von Tags T mit $\|T\| = l$ vorgegeben. Charakterisieren Sie die Authentikationscodes mit $\alpha = 1/l$ und minimaler Schlüsselmenge K (bei geeigneter Wahl der Wahrscheinlichkeitsverteilung auf K).

Aufgabe 3

Geben Sie einen Authentikationscode an, bei dem $\alpha > \beta$ gilt.