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

Sommersemester 2004

Übungen zur Kryptologie 2

1. Übung

Aufgabe 1

Berechnen Sie α und β für den MAC mit der Authentikationsmatrix

	a	b	c	d
k_1	1	1	2	3
k_2	1	2	3	1
k_3	2	1	3	1
k_4	2	3	1	2
k_5	3	2	1	3
k_6	3	3	2	1

Die Wahrscheinlichkeitsverteilung auf der Textmenge $X = \{a, b, c, d\}$ sei

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

und die Wahrscheinlichkeitsverteilung auf der Schlüsselmenge K sei

$$p(k_1) = p(k_6) = 1/4, \quad p(k_2) = p(k_3) = p(k_4) = p(k_5) = 1/8.$$

Geben Sie auch die optimalen Impersonations- und Substitutionsstrategien an.

Aufgabe 2

Angenommen, Sie wollen Nachrichten über dem 26-stelligen Alphabet $\{A, \ldots, Z\}$ der Länge 1000 authentisieren. Wie könnte ein entsprechender MAC aussehen, falls die Erfolgswahrscheinlichkeit eines Gegners bei Durchführung eines Impersonations- oder Substitutionsangriffs nicht größer als 10^{-4} sein soll?

Aufgabe 3

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

Aufgabe 4

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