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

Sommersemester 2006

Übungen zur Kryptologie 2

2. Aufgabenblatt

Aufgabe 1 Sei $h : X \to Y$ eine beliebige, aber feste (n, m)-Hashfunktion.

a) Bestimmen Sie die Erfolgswahrscheinlichkeit $\varepsilon(h, x, q)$ von FindSecondPreimage(h, x, q), falls für X_0 eine zufällige Teilmenge von $X \setminus \{x\}$ der Größe $q - 1$ gewählt wird.

b) Bestimmen Sie die durchschnittliche Erfolgswahrscheinlichkeit $\varepsilon(h, q)$ von FindSecondPreimage(h, x, q), falls X_0 wie in a) und x zufällig aus X gewählt wird. Berechnen Sie $\varepsilon(h, 2)$.

Aufgabe 2

Berechnen Sie α und β für den MAC mit nebenstehender Authentikationsmatrix. 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

	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

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

Geben Sie auch die optimalen Impersonations- und Substitutionsstrategien an.

Aufgabe 3

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 4 (4 Punkte)

Konstruieren Sie eine stark universale $(6, 5)$-Hashfamilie und eine stark universale $(13, 3)$-Hashfamilie.

Aufgabe 5

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

b) Zeigen Sie, dass für jede (n, m)-Hashfamilie $\mathcal{H}$ gilt: $\beta = 1/m$ impliziert $\alpha = 1/m$.

Aufgabe 6

Sei eine Textmenge X und eine Menge Y von Hashwerten mit $\|Y\| = m$ vorgegeben. Charakterisieren Sie die MACs mit dem optimalen Wert $\alpha = 1/m$ und minimaler Schlüsselmenge K (bei geeigneter Wahl der Wahrscheinlichkeitsverteilung auf K).

Aufgabe 7

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 8

Zeigen Sie, dass die in der Vorlesung hergeleitete Entropieschranke für die Impersonationswahrscheinlichkeit α „scharf“ ist. Hinweis: Betrachten Sie eine beliebige stark universale Hashfamilie.

Aufgabe 9

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 10

Zeigen Sie, dass für eine Zufallsvariable X mit endlichem Wertebereich $W(X) \subseteq \mathcal{R}^+$ immer $E(\log X) \leq \log E(X)$ gilt. Hinweis: Ungleichung von Jensen.

Aufgabe 11 (6 Punkte)

Schreiben Sie ein Programm, das für den MAC aus Aufgabe 2 die Entropiewerte $H(K)$ und $H(K|X)$ und daraus die in der Vorlesung hergeleitete Entropieschranke für α berechnet. Vergleichen Sie diese Entropieschranke mit dem tatsächlichen Wert von α.