

Übungsblatt 3

Aufgabe 15

Berechnen Sie α und β für den MAC mit nebenstehender Authentifikationsmatrix. 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 dem Schlüsselraum 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 16

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

(b) Zeigen Sie, dass für jede (n, m, l) -Hashfamilie gilt: $\beta = 1/m \Rightarrow \alpha = 1/m$.

Aufgabe 17

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 18

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 Gleichungssystem für alle $y \in K^m$ lösbar ist.

Aufgabe 19

Zeigen Sie, dass die in der Vorlesung hergeleitete Entropieschranke für die Impersonationswahrscheinlichkeit α »scharf« ist.

Hinweis: Betrachten Sie eine beliebige 2-universale Hashfamilie.

	<i>mündlich</i>			
	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>
<i>k</i> ₁	1	1	2	3
<i>k</i> ₂	1	2	3	1
<i>k</i> ₃	2	1	3	1
<i>k</i> ₄	2	3	1	2
<i>k</i> ₅	3	2	1	3
<i>k</i> ₆	3	3	2	1

Aufgabe 20

mündlich

- (a) Konstruieren Sie für jede Primzahl p und jede natürliche Zahl $d \geq 2$ eine 2-universale (n, m, l) -Hashfamilie mit $n = (p^d - 1)/(p - 1)$, $m = p$ und $l = p^d$.
- (b) Sei H eine 2-universale (n, m, l) -Hashfamilie. Konstruieren Sie auf der Basis von H eine 2-universale (n, m^d, l^d) -Hashfamilie H' .

Aufgabe 21

mündlich

Angenommen, Sie wollen Nachrichten über dem 26-stelligen Alphabet $\{A, \dots, Z\}$ 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 22

mündlich

Eine (n, m, l) -Hashfamilie heißt (**stark**) ***j*-universal**, falls für alle $x_1, \dots, x_j \in X$ mit $x_i \neq x_{i'}$ für $i \neq i'$ und alle $y_1, \dots, y_j \in Y$ gilt:

$$\left\| \left\{ k \in K \mid h_k(x_i) = y_i \text{ für } i = 1, \dots, j \right\} \right\| = \frac{\|K\|}{m^j}.$$

- (a) Zeigen Sie, dass jede j -universale Hashfamilie auch j' -universal ist, falls $1 \leq j' \leq j$ gilt.
- (b) Konstruieren Sie für jede Primzahl p und jedes $j \geq 1$ eine j -universale (p, p, p^j) -Hashfamilie.

Hinweis: Betrachten Sie die Menge aller Polynome vom Grad höchstens $j - 1$ über dem Körper \mathbb{F}_p .

Aufgabe 23

mündlich

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

Hinweis: Benutzen Sie die Ungleichung von Jensen.

Aufgabe 24

6 Punkte

Konstruieren Sie eine 2-universale $(6, 5, l)$ -Hashfamilie und eine 2-universale $(13, 3, l')$ -Hashfamilie für geeignete l, l' .

Aufgabe 25

4 Punkte

Schreiben Sie ein Programm, das für den MAC aus Aufgabe 15 die Entropiewerte $H(\mathcal{K})$ und $H(\mathcal{K}|\mathcal{X}, \mathcal{Y})$ und daraus die in der Vorlesung hergeleitete Entropieschranke für α berechnet. Vergleichen Sie diese Schranke mit dem tatsächlichen Wert von α .