

Übungsblatt 2

**Aufgabe 9** Sei  $h : X \rightarrow Y$  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.
- c) Berechnen Sie  $\varepsilon(h, 2)$ .

**Aufgabe 10**

Sei  $h : X \rightarrow Y$  eine *balancierte*  $(n, m)$ -Kompressionsfunktion (d.h.  $\|h^{-1}(y)\| = n/m$  für alle Hashwerte  $y$  und es gilt  $m \leq n/2$ ). Sei  $A$  ein probabilistischer Invertierungsalgorithmus für  $h$ , der mit Wahrscheinlichkeit  $\varepsilon$  für einen zufällig gewählten Hashwert  $y$  ein Urbild  $x$  mit  $h(x) = y$  berechnet.

- a) Konstruieren Sie einen Las-Vegas Algorithmus  $B$ , der mit Wahrscheinlichkeit mindestens  $\varepsilon/2$  eine Kollision für  $h$  aufspürt.
- b) Wieviele Hashwertberechnungen führt  $B$  höchstens aus, falls  $A$  nicht mehr als  $q$  Hashwertberechnungen benötigt?

**Aufgabe 11** (10 Punkte)

- a) Schreiben Sie ein Programm, das bei Eingabe von  $m$  und  $q$  die exakte Erfolgswahrscheinlichkeit  $\varepsilon$  von COLLISION( $h, q$ ) im ZOM berechnet.
- b) Vergleichen Sie die exakten Werte für  $m = 365$  und  $q \in \{15, \dots, 30\}$  mit den approximativen Werten  $q^2/2m$ .
- c) Schreiben Sie ein Programm, das bei Eingabe von  $m$  und  $\varepsilon$  die Anzahl  $q$  von Hashwertberechnungen berechnet, die COLLISION( $h, q$ ) im ZOM benötigt, um eine Erfolgswahrscheinlichkeit von mindestens  $\varepsilon$  zu erreichen.
- d) Vergleichen Sie für  $\varepsilon = 1/2$  und  $m \in \{10, 50, 100, 200, 365, 1000\}$  die exakten Werte von  $q$  mit den approximativen Werten  $\sqrt{m}$ .

**Aufgabe 12**

Berechnen Sie  $\alpha$  und  $\beta$  für den MAC mit nebenstehender Authentifikationsmatrix. Die Wahrscheinlichkeitsverteilung auf der Textmenge  $X = \{a, b, c, d\}$  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

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

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 13**

Sei  $h : \{0, 1\}^{m+t} \rightarrow \{0, 1\}^m$  eine kollisionsresistente Kompressionsfunktion. Wie in der Vorlesung gezeigt, kann  $h$  zu einer kollisionsresistenten Hashfunktion  $\hat{h} : \{0, 1\}^* \rightarrow \{0, 1\}^m$  erweitert werden, sofern hierzu ein öffentlich bekannter Initialisierungsvektor  $IV \in \{0, 1\}^m$  und eine suffixfreie Preprocessing-Funktion  $y$  verwendet werden (wobei wir auf die optionale Ausgabetransformation verzichten).

Für die Preprocessing-Funktion wird meist eine Funktion der Bauart  $y(x) = xpad(x)$  verwendet, wobei  $pad : \{0, 1\}^* \rightarrow \{0, 1\}^*$  eine so genannte Paddingfunktion mit  $|x| + |pad(x)| \equiv_t 0$  ist. Um nun einen MAC zu konstruieren, könnte man  $K = \{0, 1\}^m$  als Schlüsselraum wählen und bei der Berechnung von  $\hat{h}(x)$  anstelle von  $IV$  den geheimen Schlüssel  $k$  benutzen, um  $h_k(x)$  zu erhalten. Zeigen Sie, dass der so konstruierte MAC nicht berechnungsresistent ist.

**Aufgabe 14**

Sei  $X$  eine Zufallsvariable mit endlichem Wertebereich  $W$  und für  $x \in W$  sei  $p(x) = \Pr[X = x]$ . Dann ist die **Entropie** von  $X$  definiert als  $H(X) = \sum_x p(x) \text{Inf}_X(x)$ , wobei

$$\text{Inf}_X(x) = \begin{cases} \log_2(1/p(x)), & p(x) > 0 \\ 0, & \text{sonst} \end{cases}$$

der **Informationsgehalt** von  $x$  ist. Für zwei Zufallsvariablen  $X$  und  $Y$  sei  $H(X, Y) = \sum_{x,y} p(x, y) \cdot \log(1/p(x, y))$  die (gemeinsame) Entropie von  $X$  und  $Y$ . Zeigen Sie:

- a)  $H(X) \leq \log_2(n)$ , wobei  $n = \|W\|$  ist und Gleichheit genau im Fall  $p(x) = 1/n$  für alle  $x \in W$  eintritt.
- b)  $H(X, Y) = H(Y) + H(X|Y) = H(X) + H(Y|X)$ .
- c)  $H(X, Y) \leq H(X) + H(Y)$ , mit Gleichheit genau dann, wenn  $X$  und  $Y$  unabhängig sind.