Übungsblatt 4

Aufgabe 26 ***mündlich***

Sei H eine 2-universale (n, m, l)-Hashfamilie und sei $\lambda = l/m^2$.

(a) Wieviele Text-Hashwert-Paare $(x_i, h_k(x_i))$ $(i = 1, \ldots, j)$ benötigt der Gegner im Fall $\lambda = 1$ höchstens, um mit Erfolgswahrscheinlichkeit 1 ein gültiges Paar $(x, h_k(x))$ für den unbekannten Schlüssel k mit $x \notin \{x_1, \ldots, x_j\}$ generieren zu können?

(b) Mit welcher Erfolgswahrscheinlichkeit kann ein Gegner bei Kenntnis von 2 Text-Hashwert-Paaren $(x_i, h_k(x_i))$ ein gültiges Paar $(x, h_k(x))$ für den unbekannten Schlüssel k mit $x \notin \{x_1, x_2\}$ generieren?

Aufgabe 27 ***mündlich***

Sei H eine (n, m, l)-Hashfamilie mit $\alpha, \beta \leq j^{-1}$. Wie groß muss dann der Schlüsselraum K von H mindestens sein, wenn der Schlüssel unter Gleichverteilung gewählt wird?

Aufgabe 28 ***mündlich***

Für eine Primzahl $p > 2$ und ein Paar $(a, b) \in K = \mathbb{Z}_p \times \mathbb{Z}_p$ sei die Funktion $h_{(a,b)} : \mathbb{Z}_p \to \mathbb{Z}_p$ definiert durch $h_{(a,b)}(x) = (x + a)^2 + b \bmod p$. Zeigen Sie, dass (X, Y, K, H) mit $X = Y = \mathbb{Z}_p$ und $H = \{h_k \mid k \in K\}$ eine 2-universale Hashfamilie ist.

Aufgabe 29 ***mündlich***

Überlegen Sie, wie der mittels einer Verschlüsselungsfunktion E_k konstruierte CBC-MAC auch durch eine einfache Modifikation einer CFB-Verschlüsselung unter E_k berechnet werden kann.

Aufgabe 30 ***mündlich***

Welche Angriffe sind möglich, wenn ein Schlüssel k sowohl für CBC-Verschlüsselung als auch für einen CBC-MAC einer Nachricht m verwendet wird?

Aufgabe 31 ***mündlich***

Sei $E_k \colon \{0,1\}^l \to \{0,1\}^l$, $k \in K$, eine Familie von Verschlüsselungsfunktionen. Betrachten Sie für eine Konstante $d \geq 2$ die Hashfamilie (X, Y, K, H) mit $X = \{0,1\}^{dl}$, $Y = \{0,1\}^l$ und $H = \{h_k \mid k \in K\}$, wobei $h_k \colon X \to Y$ durch

$$h_k(x_1 \cdots x_d) = E_k(x_1) \oplus \cdots \oplus E_k(x_d), |x_1| = \cdots = |x_d| = l$$

definiert ist.

(a) Geben Sie im Fall d gerade einen existentiellen $(1, 0)$-Fälscher für diese Hashfamilie an.

(b) Geben Sie einen selektiven $(1, 1)$-Fälscher für diese Hashfamilie an.

Aufgabe 32 ***mündlich***

Ein Dokument x soll mit dem RSA-Verfahren sowohl verschlüsselt als auch signiert werden. Beschreiben Sie, worauf hierbei zu achten ist, damit die Nachricht nicht abgefangen und unbemerkt mit der Signatur eines Angreifers versehen werden kann.

Aufgabe 33 ***mündlich***

Sei g ein Erzeuger von $\mathbb{Z}_p^*$, p prim. Bestimmen Sie die Ordnung von g^i in $\mathbb{Z}_p^*$.

Aufgabe 34 ***mündlich***

Sei $n = pq$ ein RSA-Modul (d.h. p und q sind verschiedene ungerade Primzahlen) und sei $\alpha \in \mathbb{Z}_n^*$.

(a) Zeigen Sie, dass $\mathrm{ord}_n(\alpha) = \mathrm{kgV}(\mathrm{ord}_p(\alpha), \mathrm{ord}_q(\alpha))$ ist.

(b) Zeigen Sie, dass $\mathrm{ord}_n(\alpha)$ ein Teiler von $\mathrm{kgV}(p-1, q-1) = \varphi(n)/\,\mathrm{ggT}(p-1, q-1)$ ist.

(c) Bestimmen Sie für den Fall $\mathrm{ggT}(p-1, q-1) = 2$ die Anzahl der Elemente $\beta \in \mathbb{Z}_n^*$ mit $\mathrm{ord}_n(\beta) = \mathrm{kgV}(p-1, q-1)$.

(d) Überlegen Sie, wie im Fall $\mathrm{ggT}(p-1, q-1) = 2$ mit $p, q > 3$ der Wert von $\varphi(n)$ bei Kenntnis von $a = \log_\alpha \alpha^n$ berechnet werden kann, wenn $\mathrm{ord}_n(\alpha) = \varphi(n)/2$ ist.

(e) Geben Sie einen effizienten probabilistischen Algorithmus an, der einen RSA-Modul $n = pq$ im Fall $\mathrm{ggT}(p-1, q-1) = 2$ unter Verwendung eines Orakels für den diskreten Logarithmus faktorisiert.

Aufgabe 35 ***10 Punkte***

Sei $E_k \colon \{0,1\}^l \to \{0,1\}^l$, $k \in K$, eine Familie von Verschlüsselungsfunktionen. Betrachten Sie für eine Konstante $d \geq 2$ die Hashfamilie (X, Y, K, H) mit $X = \{0,1\}^{dl}$, $Y = \{0,1\}^l$ und $H = \{h_k \mid k \in K\}$, wobei $h_k \colon X \to Y$ durch

$$h_k(x_1 \cdots x_d) = E_k(x_1) + 3E_k(x_2) + \cdots + (2d-1)E_k(x_d) \bmod 2^l, |x_1| = \cdots = |x_d| = l$$

definiert ist.

(a) Geben Sie einen existentiellen $(1, 2)$-Fälscher für diese Hashfamilie an.

(b) Geben Sie einen selektiven $(1, 3)$-Fälscher für diese Hashfamilie an.