Übungen zur Kryptologie 2 Sommersemester 2008

Johannes Köbler/Sebastian Kuhnert

Übungsblatt 4

Aufgabe 28

Sei $h : \{0,1\}^{m+t} \to \{0,1\}^m$ eine kollisionsresistente Kompressionsfunktion. Welche zusätzliche Eigenschaft sollte h besitzen, damit folgende Konstruktion eine kollisionsresistente Hashfunktion $\hat{h}\colon \bigcup_{r\geq 1}\{0,1\}^{rt} \to \{0,1\}^m$ liefert?

> Sei $IV = 0^m$ und sei $x = x_1 \cdots x_r$ mit $|x_i| = t$ für $i = 1, \ldots, r$. Berechne eine Folge $y_0, \ldots, y_r$ von Strings $y_i \in \{0,1\}^m$ mit
>
> $$y_i = \begin{cases} IV, & i = 0, \\ h(y_{i-1}x_i), & i = 1, \ldots, r, \end{cases}$$
>
> und definiere $\hat{h}(x) = y_r$.

Aufgabe 29

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 stark universale Hashfamilie ist.

Aufgabe 30

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 31

Sei $E_k : \{0,1\}^l \to \{0,1\}^l$, $k \in K$, 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 $h_k : X \to Y$ 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 (10 Punkte)

Sei $E_k : \{0,1\}^l \to \{0,1\}^l$, $k \in K$, 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 $h_k : X \to Y$ 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.

Aufgabe 33

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 34

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

Aufgabe 35

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 $ord_n(\alpha) = \mathrm{kgV}(ord_p(\alpha), ord_q(\alpha))$ ist.

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

c) Zeigen Sie, dass ein Elemente $\alpha \in \mathbb{Z}_n^*$ mit $ord_n(\alpha) = \mathrm{kgV}(p-1, q-1)$ existiert.

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 $ord_n(\alpha) = \varphi(n)/2$ 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.