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

Sommersemester 2006

Übungen zur Kryptologie 2

5. Aufgabenblatt

Aufgabe 1

Sei $h\colon \{0,1\}^{m+t} \to \{0,1\}^m$ eine kollisionsresistente Kompressionsfunktion. Wie in der Vorlesung gezeigt, kann h zu einer kollisionsresistenten Hashfunktion $\hat{h}\colon \{0,1\}^* \to \{0,1\}^m$ 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 $y(x) = x\, pad(x)$ verwendet, wobei $pad\colon \{0,1\}^* \to \{0,1\}^*$ 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 2

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 3

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

Aufgabe 4

Für zwei Dokumente x_1 und x_2 seien die ElGamal-Signaturen (γ, δ_1) bzw. (γ, δ_2) bekannt, d.h. es wurde beidesmal dasselbe r verwendet.

a) Beschreiben Sie, wie sich hieraus r im Fall $\mathrm{ggT}(\delta_1 - \delta_2, p-1) = 1$ effizient berechnen lässt, und wie sogar der geheime Exponent a bestimmt werden kann.

b) Seien $p = 31847$, $g = 5$ und $b = 25703$. Berechnen Sie r und a anhand der Dokumente $x_1 = 8990$, $x_2 = 31415$ sowie der Unterschriften $(23972, 31396)$ und $(23972, 20481)$.

Aufgabe 5

Betrachten Sie die folgende Variante des ElGamal-Signaturverfahrens. Die Schlüssel werden ähnlich wie beim ElGamal-Signaturverfahren generiert: p ist prim, g ist ein Erzeuger von $\mathbb{Z}_p^*$, a ist der geheime Exponent und $b = g^a \bmod p$. Allerdings wird a jetzt aus $\mathbb{Z}_{p-1}^*$ (anstelle von $\mathbb{Z}_{p-1}$) gewählt. Ein Dokument $x \in \mathbb{Z}_p$ wird unter $\bar{k} = (p, g, a)$ mit $sig(x, \bar{k}, r) = (\gamma, \delta)$ signiert, wobei gilt:

$$\gamma = g^r \bmod p \text{ und } \delta = (x - r\gamma)a^{-1} \bmod (p-1).$$

Dieses Verfahren unterscheidet sich also auch in der Berechnung von δ.

a) Beschreiben Sie, wie sich die Unterschrift (γ, δ) eines Dokuments x bei Kenntnis des Verifikationsschlüssels $k = (p, g, b)$ verifizieren lässt.

b) Welchen Vorteil bei der Berechnung der Signatur besitzt diese Variante gegenüber dem ursprünglichen Verfahren.

Aufgabe 6 (10 Punkte)

In der Vorlesung wurde ein Angriff gegen das ElGamal-Signaturverfahren vorgestellt, mit dem sich eine gültige Signatur (γ, δ) für ein zufälliges Dokument x berechnen lässt (nichtselektive Fälschung bei bekanntem Verifikationsschlüssel). Hierbei berechnet der Gegner für beliebige Paramater i, j mit $0 \leq i, j \leq p-2$ und $ggt(j, p-1) = 1$ die Fälschung (x, γ, δ) mittels

$$\begin{aligned} \gamma &:= g^i b^j \bmod p, \\ \delta &:= -\gamma j^{-1} \bmod p-1 \text{ und} \\ x &:= -\gamma i j^{-1} \bmod p-1. \end{aligned}$$

a) Berechnen Sie eine Fälschung (x, γ, δ) für den Verifikationsschlüssel $k = (b, g, p)$ mit $p = 467$, $g = 2$ und $b = 132$. (Wählen Sie $i = 99$ und $j = 179$.)

b) Ähnlich wie oben lässt sich auch eine nichtselektive Fälschung (x', γ', δ') bei bekannter Signatur (x, γ, δ) vornehmen, indem für beliebige Paramater h, i, j mit $0 \leq h, i, j \leq p-2$ und $ggt(h\gamma - j\delta, p-1) = 1$

$$\begin{aligned} \gamma' &:= \gamma^h g^i b^j \bmod p, \\ \delta' &:= \delta\gamma'(h\gamma - j\delta)^{-1} \bmod p-1 \text{ und} \\ x' &:= \gamma'(hx + i\delta)(h\gamma - j\delta)^{-1} \bmod p-1 \end{aligned}$$

gewählt wird. Zeigen Sie, dass die Signatur (x', γ', δ') als echt anerkannt wird.

c) Das Dokument $x = 100$ hat unter ElGamal (mit $p = 461$, $g = 2$ und $b = 132$) die Signatur $(\gamma, \delta) = (29, 51)$ erhalten. Berechnen Sie hieraus ein signiertes Dokument, das Oskar bei Verwendung der Werte $h = 102$, $i = 45$ und $j = 293$ erzeugen kann. Überprüfen Sie die Verifikationsbedingung.