Übungsblatt 6

Aufgabe 43 ***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 44 ***mündlich***

Sei g ein Erzeuger von $\mathbb{Z}_p^*$, p prim (d.h. $\mathbb{Z}_p^* = \{1,\dots,p-1\} = \{g^i \bmod p \mid i = 1,\dots,p-1\}$). Bestimmen Sie die Ordnung $\operatorname{ord}(g^i) = \min\{j \geq 1 \mid (g^i)^j \equiv_p 1\}$ von g^i in $\mathbb{Z}_p^*$.

Aufgabe 45 ***mündlich***

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 z verwendet.

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

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

Aufgabe 46 ***mündlich***

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

$$\gamma = \alpha^z \bmod p \text{ und } \delta = (x - z\gamma)a^{-1} \bmod (p-1) \;.$$

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 $k = (p, \alpha, \beta)$ verifizieren lässt.

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

Aufgabe 47 ***mündlich***

Angenommen, Alice verwendet das ElGamal-Signaturverfahren und möchte bei der Berechnung der beim Signieren verwendeten Zufallszahlen Zeit sparen, indem sie ein z_0 wählt und die i-te Nachricht unter Verwendung von $z_i \equiv_{p-1} z_0 + 2i$ signiert. (Es gilt also $z_i \equiv_{p-1} z_{i-1} + 2$.)

(a) Zeigen Sie, wie Bob bei Kenntnis von zwei aufeinander folgenden signierten Nachrichten $(x_i, sig(x_i, z_i))$ und $(x_{i+1}, sig(x_{i+1}, z_{i+1}))$ den privaten Schlüssel a berechnen kann, ohne einen diskreten Logarithmus zu berechnen.
Bemerkung: Für diesen Angriff muss der Wert von i nicht bekannt sein.

(b) Führen sie den Angriff durch, wenn Bob die Werte $p = 28703$, $\alpha = 5$, $\beta = 11339$, $x_i = 12000$, $sig(x_i, z_i) = (26530, 19862)$, $x_{i+1} = 24567$ und $sig(x_{i+1}, z_{i+1}) = (3081, 7604)$ kennt.

Aufgabe 48 ***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 Parameter i, j mit $0 \leq i, j \leq p-2$ und $\operatorname{ggT}(j, p-1) = 1$ die Fälschung (x, γ, δ) mittels

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

(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 Parameter h, i, j mit $0 \leq h, i, j \leq p-2$ und $\operatorname{ggT}(h\gamma - j\delta, p-1) = 1$

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

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

(c) Das Dokument $x = 100$ hat unter ElGamal (mit $p = 467$, $g = 2$ 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.