

Übungsblatt 6

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.

- Beschreiben Sie, wie sich hieraus z im Fall $\text{ggT}(\delta_1 - \delta_2, p - 1) = 1$ effizient berechnen lässt, und wie sogar der geheime Exponent a bestimmt werden kann.
- 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 $x \in \mathbb{Z}_p$ wird unter $\hat{k} = (p, \alpha, a)$ mit $\text{sig}(\hat{k}, x, z) = (\gamma, \delta)$ 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 .

- Beschreiben Sie, wie sich die Unterschrift (γ, δ) eines Dokuments x bei Kenntnis des Verifikationsschlüssels $k = (p, \alpha, \beta)$ verifizieren lässt.
- 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 $z_i \equiv_{p-1} z_{i-1} + 2$.)

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

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

Aufgabe 48

mündlich

- Falls sich bei der Berechnung einer ElGamal-Signatur der Wert $\delta = 0$ ergibt, muss eine neue Zufallszahl z gewählt werden. Überlegen Sie, wie sich aus einer ElGamal-Signatur (γ, δ) mit $\delta = 0$ und dem öffentlichen Verifikationsschlüssel der geheime Signaturschlüssel berechnen lässt.
- Beim DSA muss auch im Fall $\gamma = 0$ eine neue Zufallszahl z gewählt werden. Überlegen Sie, wie aus einer DSA-»Signatur« (γ, δ) mit $\gamma = 0$ die benutzte Zufallszahl z bestimmt werden kann, und wie sich daraus für ein beliebiges Dokument x eine gefälschte »Signatur« (γ, δ) mit $\gamma = 0$ erhalten lässt.

Aufgabe 49

mündlich

Wir haben gesehen, dass das ElGamal-Signaturverfahren gebrochen werden kann, wenn die gleiche Zufallszahl k mehrmals verwendet wird. Zeigen Sie, wie ähnliche Angriffe auf das Schnorr-Signaturverfahren, DSA und ECDSA möglich sind.

Aufgabe 50

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 $\text{ggT}(j, p - 1) = 1$ die Fälschung (x, γ, δ) mittels

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

- 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 $j = 179$.)
- 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 $\text{ggT}(h\gamma - j\delta, p - 1) = 1$

$$\gamma' := \gamma^h g^i b^j \bmod p,$$

$$\delta' := \delta \gamma' (h\gamma - j\delta)^{-1} \bmod p - 1 \text{ und}$$

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

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

- 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.

