Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Kryptologie - SoSe 2018
7. Juni 2018

Übungsblatt 7

Aufgabe 44 Sei $(G, \circ, e)$ eine endliche Gruppe der Ordnung n. ***mündlich***

(a) Zeigen Sie, dass G genau dann zyklisch ist, wenn G isomorph zu $(\mathbb{Z}_n, +, 0)$ ist.

(b) Zeigen Sie, dass das Produkt zweier zyklischer Gruppen der Ordnungen n_1 und n_2 genau dann zyklisch ist, wenn $\mathrm{ggT}(n_1, n_2) = 1$ ist.

(c) Folgern Sie, dass $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ im Fall $n_1 | n_2$ genau dann zyklisch ist, wenn $n_1 = 1$ ist.

(d) Bestimmen Sie die Ordnung $\mathrm{ord}(a) = \min\{k \geq 1 \mid ka \equiv_m 0\}$ von a in $\mathbb{Z}_m$.

(e) Sei $a \in \mathbb{Z}_m^*$ ein Element der Ordnung $\mathrm{ord}(a) = k$. Welche Ordnung hat dann die Potenz a^i in $\mathbb{Z}_m^*$?

Aufgabe 45 ***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 46 ***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 $\mathrm{ggT}(\delta_1 - \delta_2, p-1) = 1$ effizient berechnen lässt, und wie sogar der geheime Exponent a bestimmt werden kann.

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

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 $u \in \mathbb{Z}_{p-1}$ und $v \in \mathbb{Z}_{p-1}^*$ die Fälschung (x, γ, δ) mittels

$$\gamma := \alpha^u \beta^v \bmod p, \qquad \delta := -\gamma v^{-1} \bmod p-1 \qquad \text{und} \qquad x := u\delta \bmod p-1.$$

(a) Berechnen Sie eine Fälschung (x, γ, δ) für den Verifikationsschlüssel $k = (p, \alpha, \beta)$ mit $p = 467$, $\alpha = 2$ und $\beta = 132$. (Wählen Sie $u = 99$ und $v = 179$.)

(b) Ähnlich wie oben lässt sich auch eine nichtselektive Fälschung (x', γ', δ') bei bekannter Signatur (x, γ, δ) vornehmen, indem für beliebige Parameter $u, v, w \in \mathbb{Z}_{p-1}$ mit $\mathrm{ggT}(w\gamma - v\delta, p-1) = 1$

$$\begin{aligned} \gamma' &:= \gamma^w \alpha^u \beta^v \bmod p, \\ \delta' &:= \delta\gamma'(w\gamma - v\delta)^{-1} \bmod p-1 \text{ und} \\ x' &:= \gamma'(wx + u\delta)(w\gamma - v\delta)^{-1} \bmod p-1 \end{aligned}$$

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

(c) Das Dokument $x = 100$ hat unter ElGamal (mit $p = 467$, $\alpha = 2$ und $\beta = 132$) die Signatur $(\gamma, \delta) = (29, 51)$ erhalten. Berechnen Sie hieraus ein signiertes Dokument, das ein Angreifer bei Verwendung der Werte $w = 102$, $u = 45$ und $v = 293$ erzeugen kann. Überprüfen Sie die Verifikationsbedingung.