Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 7

Besprechung der mündlichen Aufgaben am 8. 1. 2021
Abgabe der schriftlichen Lösungen bis 12. 1. 2021, 23:59 Uhr

Aufgabe 42 Sei E_q die elliptische Kurve $y^2+y=x^3$ über $\mathbb{F}_q$ $(q=2^n)$. ***mündlich***

(a) Sei $P=(x,y)\in E_q$. Bestimmen Sie die Koordinaten von $-P$ und von $2P$.

(b) Bestimmen Sie die Ordnung aller Punkte P von E_{16}. (*Hinweis:* Berechnen Sie die Koordinaten von $4P$.)

(c) Bestimmen Sie die Anzahl der Punkte von E_4 und von E_{16}. (*Hinweis:* Zeigen Sie $\#E_{16}=\#E_4$ und benutzen Sie den Satz von Hasse.)

Aufgabe 43 Sei E die elliptische Kurve $y^2=x^3+x+26$ über $\mathbb{Z}_{127}$. ***mündlich***

(a) Bestimmen Sie die NAF-Darstellung der Zahl 87.

(b) Bestimmen Sie mit Hilfe des Algorithmus DoubleAddSub das Vielfache $87P$ des Punktes $P=(2,6)$ auf der elliptischen Kurve E.

Aufgabe 44 ***mündlich***
Bestimmen Sie die Anzahl l_i aller natürlichen Zahlen, die eine NAF-Darstellung der Form $(c_{i-1},\ldots,c_0)$ mit $c_{i-1}=1$ haben. Zeigen Sie hierzu folgende Rekursion und finden Sie eine explizite Formel für l_i.

$$l_i=\begin{cases}1, & i\le 2,\\ 2(l_1+\cdots+l_{i-2})+1, & i\ge 3.\end{cases}$$

Aufgabe 45 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 $\mathrm{ord}(a)=\min\{k\ge 1\mid ka\equiv_m 0\}$ 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 46 ***mündlich***

Ein Text 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 47 ***mündlich***

Für zwei Texte 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 Texte $x_1 = 8990$, $x_2 = 31415$ sowie der Unterschriften $(23972, 31396)$ und $(23972, 20481)$.

Aufgabe 48 ***10 Punkte***

In der Vorlesung wurde ein Angriff gegen das ElGamal-Signaturverfahren vorgestellt, mit dem sich eine gültige Signatur (γ, δ) für einen zufälligen Text 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) Der Text $x = 100$ hat unter ElGamal (mit $p = 467$, $\alpha = 2$ und $\beta = 132$) die Signatur $y = (\gamma, \delta) = (29, 51)$ erhalten. Berechnen Sie hieraus eine Fälschung (x', y') unter Verwendung der Werte $w = 102$, $u = 45$ und $v = 293$. Überprüfen Sie die Verifikationsbedingung.