Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
9. Jan. 2019

Übungen zur Vorlesung Kryptographie

Blatt 11

Aufgabe 41

Sei E eine elliptische Kurve über einem Körper K der Charakteristik $\neq 2, 3$ mit der affinen Gleichung

$$y^2 = x^3 + ax + b.$$

Seien $\alpha, \beta \in K^*$ mit $\beta^2 = \alpha^3$. Man zeige: Die Abbildung $(x, y) \mapsto (\alpha x, \beta y)$ bildet E bijektiv auf eine elliptische Kurve $\tilde{E}$ mit affiner Gleichung $y^2 = x^3 + \tilde{a}x + \tilde{b}$ ab. Die Abbildung ist ein Gruppen-Isomorphismus. Wie lauten die Koeffizienten $\tilde{a}, \tilde{b}$?

Aufgabe 42

Sei E eine elliptische Kurve über dem Körper $\mathbb{F}_p = \mathbb{Z}/p$ mit einer Primzahl $p > 3$. Man beweise:

a) Falls $p \equiv 3 \bmod 4$, ist E isomorph zu einer Kurve folgender Gestalt:

$$y^2 = x^3 + ax + b \quad \text{mit} \quad a \in \{0, 1, -1\}.$$

b) Sei $p \equiv 1 \bmod 4$ und g eine Primitivwurzel modulo p. Dann ist E isomorph zu einer Kurve folgender Gestalt:

$$y^2 = x^3 + b \qquad \text{oder} \qquad y^2 = x^3 + g^k x + b \quad \text{mit} \quad k \in \{0, 1, 2, 3\}.$$

Aufgabe 43

Man beschreibe und implementiere das Analogon des Pollardschen Rho-Algorithmus zur Berechnung des Diskreten Logarithmus auf elliptischen Kurven über dem Körper $\mathbb{F}_p = \mathbb{Z}/p$, wobei p eine ungerade Primzahl ist.

Der Algorithmus soll Folgendes leisten: Gegeben sei eine elliptische Kurve E über $\mathbb{F}_p$ mit affiner Gleichung

$$y^2 = x^3 + ax + b,$$

sowie ein Punkt $P_0 = (x_0, y_0) \in E_{\text{aff}}(\mathbb{F}_p)$, der die (bekannte) Primzahlordnung q besitze. Der Algorithmus berechnet dann für einen Punkt $P \in E_{\text{aff}}(\mathbb{F}_p)$, der in der von P_0 erzeugten zyklischen Untergruppe liegt, d.h. $P = \lambda \cdot P_0$ mit einem (unbekannten) $\lambda \in \mathbb{Z}/q$, diesen Multipliator λ.

---

b.w.

Aufgabe 44

Alice benutzt eine EC-Variante des ElGamal Public Key Kryptosystems. Die zugrunde liegende elliptische Kurve über dem Körper $\mathbb{F}_p$ mit $p = 1\,00000\,00033$ sei gegeben durch

$$E: \quad Y^2 = X^3 + X + 7.$$

Außerdem sind Punkte

$$P_0 = (1, 3), \quad P = (8811\,81254, 79153\,22138) \in E_{\text{aff}}(\mathbb{F}_p)$$

gegeben, wobei P_0 Primzahl-Ordnung $q = 99998\,70619$ hat und $P = \omega \cdot P_0$ mit einem geheimen $\omega \in \mathbb{Z}/q$. Alice's Public Key ist nun (E, p, q, P_0, P).

Wenn Bob eine verschlüsselte Nachricht an Alice senden will, teilt er die Nachricht in Blöcke von 4 Bytes. Ein Block (b_0, b_1, b_2, b_3), $(0 < b_\nu < 2^8)$, wird als 32-Bit-Zahl $x = \sum_{\nu=0}^{3} b_\nu \cdot 2^{8\nu}$ interpretiert. Ein solcher Block wird wie folgt verschlüsselt: Bob wählt eine (vom Block abhängige) geheim zu haltende Zufallszahl $\alpha \in (\mathbb{Z}/q)^*$ und berechnet die Punkte

$$A_0 := \alpha \cdot P_0 = (\xi_0, \eta_0), \quad A := \alpha \cdot P = (\xi, \eta) \in E.$$

Die Verschlüsselung von x ist dann

$$y = (\xi_0,\ \xi x \bmod p) \in (\mathbb{Z}/p) \times (\mathbb{Z}/p).$$

Man entschlüssele den folgenden, aus einem 24 Bytes langen ASCII-Klartext entstandenen Geheimtext

(48232 29261, 30940 83924), (58925 20813, 85064 90069), (87494 50710, 31630 56932),
(7993 91596, 90722 09260), (62730 01856, 48413 82856), (64360 06616, 50246 18680)

indem man das DL-Problem $P = \omega \cdot P_0$ auf der Kurve E für das unbekannte ω löse.