Gregor Leander
9.06.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Lösungsvorschläge für Übungsblatt 8

Aufgabe 1 *Rechnen auf Elliptischen Kurven III*

Sei $\mathbb{F}_5$ der Körper mit 5 Elementen. Verifiziere, dass 2 kein Quadrat in $\mathbb{F}_5$ ist, und somit konstruiere den Körper $\mathbb{F}_{25}$ mit 25 Elementen als die durch das Polynom $z^2 - 2$ definierte Körpererweiterung von $\mathbb{F}_5$.
Betrachte die über $\mathbb{F}_5$ durch folgende Gleichung definierte Kurve

$$E : y^2 = x^3 + 1 \ .$$

1. Zeige, dass E eine elliptische Kurve ist. (2 Punkte)
2. Bestimme alle Punkte auf E über $\mathbb{F}_5$. (2 Punkte)
3. Bestimme alle Punkte auf E über $\mathbb{F}_{5^2}$, die nicht über $\mathbb{F}_5$ definiert sind. (4 Punkte)
4. Zeige die Punkte der Ordnung 2 auf $E(\mathbb{F}_5)$. (2 Punkte)
5. Zeige die Punkte der Ordnung 2 auf $E(\mathbb{F}_{5^2})$. (2 Punkte)
6. Finde einen Punkt P in $E(\mathbb{F}_{5^2}) \setminus E(\mathbb{F}_5)$ derart, dass $2 \cdot P \in E(\mathbb{F}_5)$ aber $2 \cdot P \neq 0$. (4 Punkte)

Lösung

1. Hier berechnet man am einfachsten die Diskriminante. Es gilt

   $$\Delta = 4a^3 + 27b^2$$

   und hier ist $a = 0$ und $b = 1$ und damit

   $$\Delta = 27 \neq 0 \bmod 5.$$

2. Hier die Liste der Punkte

   $$E(\mathbb{F}_5) = \{(0,1), (0,4), (2,2), (2,3), (4,0), \mathcal{O}\}$$

3. Hier die Liste der Punkte als Polynome in z mit $z^2 = 2$.

$$\begin{aligned} E(\mathbb{F}_{25}) \setminus E(\mathbb{F}_5) \quad = \quad & \{(1, z), (1, 4z), (4z + 3, z + 3), (4z + 3, 4z + 2), (4z + 1, 2z), \\ & (4z + 1, 3z), (3z + 3, 0), (z + 3, 4z + 3), (z + 3, z + 2), (3z + 2, z), \\ & (3z + 2, 4z), (2z, z + 3), (2z, 4z + 2), (z + 1, 2z), (z + 1, 3z), (z + 2, 4z + 3), \\ & (z + 2, z + 2), (z + 4, 2), (z + 4, 3), (2z + 2, z), (2z + 2, 4z), (4z + 2, z + 3), \\ & (4z + 2, 4z + 2), (3, 2z), (3, 3z), (2z + 3, 0), (3z, 4z + 3), (3z, z + 2), (4z + 4, 2) \\ & (4z + 4, 3)\}. \end{aligned}$$

4. Punkte $P = (x, y)$ der Ordnung zwei erfüllen immer $y = 0$. Damit ist

$$P = (4, 0)$$

der einzige Punkt in $E(\mathbb{F}_5)$ mit Ordnung 2.

5. Punkte $P = (x, y)$ der Ordnung zwei erfüllen immer $y = 0$. Damit sind

$$P = (3z + 3, 0) \text{ und } P = (2z + 3, 0)$$

die einzigen Punkte in $E(\mathbb{F}_{25}) \setminus E(\mathbb{F}_5)$ mit Ordnung 2.

6. Solch ein Punkt ist zum Beispiel

$$P = (z + 4, 2)$$

hier gilt nämlich $2P = (0, 4)$.

□

Aufgabe 2 *DSA*

Eine Chipkarte kann Signaturen mit Hilfe des DSA erzeugen. Hier sind die Ein- und Ausgabewerte der Karte angegeben: Der öffentliche Schlüssel:

$$(p, q, \alpha, y) = (10267, 59, 4504, 8893)$$

Erste Signatur:

$$(r_1, s_1) = (54, 12) \text{ mit } h(m_1) = 47$$

Zweite Signatur:

$$(r_2, s_2) = (54, 7) \text{ mit } h(m_2) = 34$$

Berechne den privaten Schlüssel a. Brute Force gibt keine Punkte!

Hinweis: Die Chipkarte muß Zufallszahlen erzeugen und dabei unterlief ihr ein Fehler (vergleiche r_1 und r_2) !

Lösung
Da $r_1 = r_2 = r$ gilt muss auch der Zufallswert k bei beiden Signaturen gleich sein. Damit gilt

$$\begin{aligned} s_1 &= k^{-1}(h(m_1) + ar) \bmod q \\ s_2 &= k^{-1}(h(m_2) + ar) \bmod q \end{aligned}$$

Mit k multiplizieren und durch s_1 bzw. s_2 dividieren und gleichsetzen liefert

$$s_1^{-1}(h(m_1) + ar) = s_2^{-1}(h(m_2) + ar) \bmod q.$$

Auflösen nach a liefert

$$a = \frac{h(m_2)s_1 - h(m_1)s_2}{r(s_2 - s_1)} \bmod q.$$

Einsetzen der Werte für s_1, s_2 und h_1, h_2 sowie r liefert

$$a = 48 \bmod q.$$

Probe:

$$\alpha^{48} = y \bmod p$$

□