Gregor Leander
9.06.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 8

Aufgabe 1 *Rechnen auf Elliptischen Kurven III* 16 Punkte Punkte

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)

Aufgabe 2 *DSA* 10 Punkte Punkte

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) !

Der DSA:
Für DSA wird eine Hashfunktion $h : \{0,1\}^* \to \mathbb{Z}_q$ benötigt.

1. Schlüsselerzeugung
   (a) Wähle eine Primzahl q.
   (b) Wähle eine Primzahl p mit $p = tq + 1$.
      i. Wähle zufällig ein Element $g \in \mathbb{Z}_p^*$.
      ii. Berechne $\alpha = g^{(p-1)/q}$.
      iii. Wenn $\alpha = 1$ gehe zu 1(b)i.
   (c) Wähle zufällig a mit $1 \leq a \leq q - 1$.
   (d) Berechne $y = \alpha^a \bmod p$.
   (e) Der öffentliche Schlüssel ist (p, q, α, y). Der private Schlüssel ist a.
2. Signaturerstellung
   (a) Wähle zufällig k mit $0 < k < q$.
   (b) Berechne $r = (\alpha^k \bmod p) \bmod q$.
   (c) Berechne $s = k^{-1}(h(m) + ar) \bmod q$.
   (d) Die Signatur ist (r, s).

Abgabe: Freitag, 13.06.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 14.06.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.