Exercise 12 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2015-01-30

Problem 37. *(working with elliptic curves I)* Consider the equation

$$Y^2 = X^3 + X + 1.$$

a) Show that this equation describes an elliptic curve E over the field $\mathbb{F}_7$.

b) Determine all points in $E(\mathbb{F}_7)$ and compute the trace t of E.

c) Show that $E(\mathbb{F}_7)$ is cyclic and give a generator.

Problem 38. *(working with elliptic curves II)* Consider the following function in the field $\mathbb{F}_7$

$$E_{a,b} : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_7$.

a) Determine the parameters a, b for which $P_1 = (1, 1)$ and $P_2 = (6, 2)$ are points on the curve. Do these parameters describe an elliptic curve in the field $\mathbb{F}_7$? Give a reason.

Consider the curve $E_{6,1}$ for the remainder of this exercise.

b) Show that $E_{6,1}$ is an elliptic curve in the field $\mathbb{F}_7$. Determine all points P and their inverses $-P$ in the $\mathbb{F}_7$-rational group.

c) What are possible group orders for any group which is generated by an arbitrary point P of the curve?

d) Show that $Q = (1, 1)$ is a generator of $E_{6,1}(\mathbb{F}_7)$. You know that $4 \cdot (1, 1) = (3, 2)$.

Problem 39. *(babystep-gaintstep-algorithm on elliptic curves)*

(a) Show that $E_\alpha : Y^2 = X^3 + \alpha X + 1$ is an elliptic curve over the finite field $\mathbb{F}_{13}$ for $\alpha = 2$.

(b) Compute the points iP for $P = (0, 1)$ on E_2 with $i = 0, \ldots, 4$.

(c) The group order of E_2 is $\#E_2(\mathbb{F}_q) = 8$. Show that P is a cyclic generator for E_2.

Consider the following algorithm to compute the discrete logarithm on elliptic curves:

Algorithm 1 The Babystep-Giantstep-Algorithm on Elliptic Curves

---

Input: An elliptic curve $E_\alpha(\mathbb{F}_q)$ and two points $P, Q \in E_\alpha(\mathbb{F}_q)$
Output: $a \in \mathbb{F}_q$, i.e., the discrete logarithm of $Q = aP$ on E_α
(1) Fix $m \leftarrow \lceil \sqrt{q} \rceil$.
(2) Compute a table of *babysteps* $b_i = iP$ for indices $i \in \mathbb{Z}$ in $0 \leq i < m$.
(3) Compute a table of *giantsteps* $g_j = Q - j(mP)$ for all indices $j \in \mathbb{Z}$ in $0 \leq j < m$ until you find a pair (i, j) such that $b_i = g_j$ holds.
return $a = i + mj \bmod q$.

(d) Show that the given algorithm calculates the discrete logarithm on elliptic curves.

(e) Compute the discrete logarithm of $Q = aP$ with points $P = (0, 1)$ and $Q = (8, 3)$ on the elliptic curve E_2 using this algorithm.