Homework 12 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

07.02.2014

Exercise 33. The parameters for the cryptosystem used in an ElGamal signature scheme are

$$p = 4793, \ x = 9177, a = 4792, \text{ and a random secret } k = 2811.$$

(a) Check if these parameters fulfill the requirements of the signature scheme. You do not need to proof that 4793 and 599 are prime.

If the requirements are not fulfilled take the alternative values

$$x = 257 \text{ and } a = 1400.$$

(b) Sign the message $m = 231$ using the ElGamal signature scheme.

Exercise 34. The message $m = 65$ was signed using the ElGamal signature scheme with public parameters $y = 399$, $p = 859$, and $a = 206$.

(a) Verify the signature $(r, s) = (373, 15)$.

Exercise 35. 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 $4 \cdot (1, 1) = (3, 2)$.