RWTH AACHEN UNIVERSITY

Lehrstuhl für Theoretische Informationstechnik

Homework 14 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Georg Böcherer

01.02.2011

Exercise 43. Describe how the DSA signature scheme can be carried out in a group of $\mathbb{F}_p$-rational points on an elliptic curve $E/\mathbb{F}_p$.

Exercise 44. Consider the elliptic curve

$$E : Y^2 = X^3 + 3X + 5.$$

The curve is defined over $\mathbb{F}_{11}$.

(a) Calculate all points of the curve. How many points are in $E(\mathbb{F}_{11})$?

(b) Identify the inverses $-P$ for all points $P \in E(\mathbb{F}_{11})$.

Now the Diffie-Hellman key exchange is performed on $E(\mathbb{F}_{11})$ with the generator $P = (0, 7)$. Alice chooses the secret $x = 5$ and Bob chooses $y = 3$.

(c) Calculate Bob's message to Alice.

For the given curve, the cardinality is easily found by counting the points. When using secure curves, this does not hold. However, an estimation of the number of points is necessary for rating the security of the curve.

(d) Give a sensible upper and lower bound for the cardinality of the curve $E(\mathbb{F}_{11^4})$.