RWTH AACHEN UNIVERSITY

Lehrstuhl für Theoretische Informationstechnik

Homework 9 in Cryptography II

Prof. Dr. Rudolf Mathar, Peter Schwabe

04.07.2007

Exercise 25.

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 26.

Implementation cost of elliptic curve arithmetic is often expressed in terms of the number of multiplictions, squarings and inversions in the underlying field K. Determine how many of each of these operations are needed for a point addition and for a point doubling, respectively.