Homework 2 in Advanced Methods of Cryptography

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

25.10.2011

Exercise 5. Let G be an additive group with $n \in \mathbb{N}$ elements, i.e., there is no multiplication, but addition only. Furthermore, this group is generated by a point P, i.e.,

$$G = \{\mathcal{O}, P, 2P, 3P, \ldots, (n-1)P\},$$

where $2P = P + P$, $3P = 2P + P$, and so forth holds, and $\mathcal{O}$ is the neutral element of G. The element P has order n, i.e., $nP = \mathcal{O}$.

This group G is appropriate for the generalized ElGamal encryption.

(a) Describe the generalized ElGamal encryption for this group G.

(b) What properties should the group G have such that the cryptosystem is secure and efficient?

(c) Obviously, multiples of P must be calculated. Give an effcient algorithm to calculate kP, $k \in \mathbb{N}$.

Exercise 6. Consider the finite field $\mathbb{F}_{2^3}$ with 8 elements. This field can be constructed as the residue ring of the polynomial ring $\mathbb{F}_2[u]$ modulo an irreducible polynomial of degree 3.

(a) Determine all irreducible polynomials of degree 3 in $\mathbb{F}_2[u]$.

Consider the cyclic group $G = \mathbb{F}_{2^3}^*$, where the multiplication is taken modulo the polynomial $f(u) = u^3 + u + 1$.

(b) Show that u is a generator for G.

Exercise 7. Consider the group $G = \mathbb{F}_{2^3}^*$ of the last exercise for the generalized ElGamal encryption with public key $y = (110)$, which is the binary representation of the polynomial $u^2 + u$, message $m = (111)$, and $k = 3$.

(a) What is the private key x of Alice?