Homework 11 in Advanced Methods of Cryptography

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

08.01.2013

Exercise 32. 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., $nP = \mathcal{O}$ and $mP \neq \mathcal{O}$, $1 \leq m < n$.

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 33. Prove Euler's criterion: Let $p > 2$ be prime, then

$$c \in \mathbb{Z}_p^* \text{ is a quadratic residue modulo } p \Leftrightarrow c^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Exercise 34. Santa Claus still has to deliver a lot af presents. He cannot take all presents at once, but wants to divide the presents in heaps with same quantity. Unfortunately, he has failed so far. While dividing the presents on 5, 7, 8, 9, and 11 heaps, there are 3, 2, 1, 2, and 5 presents left over. Please help Santa Claus and tell him, how many presents he has and which heap sizes are possible. Santa Claus knows that he has less than 50,000 presents.

Merry Christmas and a Happy New Year