Homework 8 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

02.07.2009

Exercise 23. Sign the message $m = 231$ using the ElGamal signature scheme. The parameters for the crypto system are

$$p = 4793,\ x_A = 9177 \text{ and } a = 4792.$$

Before signing, check if these parameters fulfill the requirements of the signature scheme. Alternative values (in case the requirements are not fulfilled) are

$$p = 8501,\ x_A = 257 \text{ and } a = 1400.$$

The random secret shall be chosen as $k = 2811$.

Exercise 24. Verify the ElGamal signature $< r, s > = < 373, 15 >$ for the message $m = 65$. The message was signed using the public parameters $y_A = 399$, $p = 859$ and $a = 206$.

Exercise 25. The complete subtree method within a broadcast encryption scenario with $N \in \mathbb{N}$, $N = 2^l$, $l \in \mathbb{N}$, users is modelled by a binary tree, where the leaves represent the users. Each node of the tree has an encryption key known by all of the descendant users. There shall be $r \in \mathbb{N}$, $r \leq N$ users revoked, i.e. none of the keys of their ancestor nodes must be used.

(a) Show that a maximum of $r \log_2 \left(\frac{N}{r}\right)$ encrypted keys with their respective identifiers must be sent.

(b) For which r is the maximum number of pairs necessary? How do the revoked users need to be positioned at the leaves of the tree such that the maximum is attained?

(c) How many messages must be sent at minimum if $r = 2^k$, $0 \leq k \leq l$ users are revoked?