Homework 8 in Advanced Methods of Cryptography

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

13.12.2011

Exercise 23. The parameters for the cryptosystem used in an ElGamal signature scheme are

$$p = 4793,\ x = 9177, a = 4792, \text{ and a random secret } k = 2811.$$

(a) Check if these parameters fulfill the requirements of the signature scheme.

If the requirements are not fulfilled take the alternative values

$$x = 257 \text{ and } a = 1400.$$

(b) Sign the message $m = 231$ using the ElGamal signature scheme.

Exercise 24. The message $m = 65$ was signed using the ElGamal signature scheme with public parameters $y = 399$, $p = 859$, and $a = 206$.

(a) Verify the signature $< r, s >=< 373, 15 >$.

Exercise 25. An attacker has intercepted one valid signature (r, s) of the ElGamal signature scheme and a hashed message $h(m)$ which is invertible modulo $p - 1$.

(a) Show that the attacker can generate a signature $< r', s' >$ for any hashed message $h(m')$, if $1 \leq r < p$ is not verified.