Homework 13 in Advanced Methods of Cryptography

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

22.01.2013

Exercise 38. Consider two hash functions, one with an output length of 64 bits and another one with an output length of 128 bits.

For each of these functions, do the following:

(a) Determine the number of messages that have to be created to find a collision with a probability larger than 0.86 by means of the birthday paradox.

(b) Determine the hardware ressources required for this attack in terms of memory size, number of comparisons, and number of hash function executions.

Exercise 39. 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 40. 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 $< r, s >=< 373, 15 >$.