Homework 12 in Advanced Methods of Cryptography

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

15.01.2013

Exercise 35.

Alice and Bob are using the Rabin cryptosystem. Bob's public key is $n = 4757$. All integers in the set $\{1, \dots, n-1\}$ are represented by sequences of 13 bits. In order to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Suppose Alice sends the cryptogram $c = 1935$.

(a) Find the private key by factoring the public key $n = pq$.

(b) Decipher the cryptogram c and identify the correct message m.

Exercise 36.

Consider the following hash-function:

$$h: \mathbb{N} \to \mathbb{N}_0, \; k \mapsto \lfloor 10000(k(1+\sqrt{5})/2 - \lfloor k(1+\sqrt{5})/2 \rfloor) \rfloor.$$

(a) Determine the upper and lower bounds of the codomain of h.

(b) Find a collision for h.

Exercise 37.

(a) Assume that p, q are prime and $p = 2q + 1$.
What values can $\gcd(a, p-1)$ attain for $a \in \mathbb{N}$?

Complete the proof of Example 10.2 from the lecture notes.

(b) Show that from
$$k(x_1 - x_1') \equiv x_0' - x_0 \pmod{p-1}$$
the discrete logarithm $k = \log_a b$ can be efficiently computed.