Homework 11 in Advanced Methods of Cryptography

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

31.01.2014

Exercise 31. Alice and Bob are using the Rabin cryptosystem. Bob's public key is $n = 4757$. All integers in the set $\{1, \ldots, n-1\}$ are represented as bit sequences with 13 bits. In order to be able to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Alice sends the cryptogram $c = 1935$. Decipher this cryptogram.

Exercise 32. Consider the following hash function based on the discrete logarithm:

$$h(m) = a^{x_0} b^{x_1} \mod p$$

with q prime such that $p = 2q + 1$ is also prime, two primitive elements a, b modulo p, and message $m = x_0 + x_1 q, 0 \leq x_0, x_1 \leq q - 1$.

(a) What values can $\gcd(c, p-1)$ attain for $c \in \mathbb{N}$?

(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.

(c) Show that $h(m)$ is a collision-free hash function.

Exercise 33. Alice wants to send a letter to the manager Bob concerning some important money transfer. She has no time to write the letter by herself and instructs her assistant Oscar to write a corresponding letter m. However, Oscar intends to generate a fraudulent letter m' where the money is transferred to his account. As long as the letter m is meaningful and includes the correct transfer, Alice will sign the hash value $h(m)$.

Oscar takes advantage of the birthday paradox to generate his fraudulent message.

(a) How many alternative text elements k from m, with only a dual choice per element, must he vary in both the original message m and the fraudulent message m' so that the probability of a hash collision is above 60%.
Hint: Use $k = \sqrt{\lambda n}$ in the generalized birthday paradox for simplicity.

(b) What can Alice do to complicate this attack?