Homework 6 in Advanced Methods of Cryptography

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

29.11.2011

Exercise 17. Complete the proof of Example 10.2 from the lecture notes.

(a) 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.

Exercise 18. 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 19. Using a block cipher $E_K(x)$ with block length k and key K a hash function $h(m)$ is provided in the following way:

Append m with zero bits until it is a multiple of k, divide m into n blocks of k bits each.
$c \leftarrow E_{m_0}(m_0)$
for i **in** $1..(n-1)$ **do**
  $d \leftarrow E_{m_0}(m_i)$
  $c \leftarrow c \oplus d$
end for
$h(m) \leftarrow c$

(a) Does this function fulfill the basic requirements for a cryptographic hash function?

(b) Can these requirements be fulfilled by replacing the operation XOR ($\oplus$) by AND?