Dr. Michael Reyer

Tutorial 4

Friday, November 16, 2018

Problem 1. *(Hash function)*

a) Explain the four requirements for a cryptographic hash function.

Let $h : \{0,1\}^* \to \{0,1\}^n$ be a hash function and $h^{'} : \{0,1\}^* \to \{0,1\}^{n+1}$ given as

$$h'(m) = \begin{cases} 0 \,\|\, m & m \in \{0,1\}^n, \\ 1 \,\|\, h(m) & \text{otherwise}, \end{cases}$$

where the symbol $\|$ denotes concatenation.

b) Show that h' is not preimage resistant, but still second-preimage resistant.

Problem 2. *(Proof of Example 10.2)* Complete the proof of Example 10.2 from the lecture notes. Show that from

$$k(x_1 - x_1') \equiv x_0' - x_0 \pmod{p-1}$$

the discrete logarithm $k = \log_a(b) \mod p$ can be efficiently computed.

Problem 3. *(Number of messages and hardware resources of two hash functions)* 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.