Homework 5 in Cryptography II

Prof. Dr. Rudolf Mathar, Peter Schwabe

24.05.2007

Exercise 14.
Complete the proof of example 9.2 from the lecture (example 11.2 in the lecture notes): Show that from

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

the discrete logarithm $k = \log_a b$ can be efficiently computed.

Exercise 13.
Consider the following function:

$$h:\ \{0,1\}^* \to \{0,1\}^*,\ k \mapsto (\lfloor 10000((k)_{10}(1+\sqrt{5})/2 - \lfloor (k)_{10}(1+\sqrt{5})/2)\rfloor)\rfloor)_2.$$

Here, $\lfloor x \rfloor$ is the floor function of x (round down to the next integer smaller than x).
For computing $h(k)$, the bitstring k is identified with the positive integer it represents. The result is then converted to binary representation.
(example: $k = 10011$, $(k)_{10} = 19$, $h(k) = (7426)_2 = 1110100000010$)

a) Determine the maximal length of the output of h.

b) Give a collision for h.

Exercise 14.
Let $G = (V, E)$ be an undirected, connected, 3-regular graph with n vertices (each of the vertices has exactly 3 adjacent edges).
Describe a hash function

$$h:\ \{0,1\}^* \to \{0,1\}^l,$$

based on this graph, where $l := \lfloor \log_2 n \rfloor$. Rephrase the terms “preimage resistant” and “strongly collision resistant” for your function.

Hint: Use a starting vertex and consider walks through the graph.