Exercise 5 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2014-11-21

Problem 14. *(Blum-Blum-Shub generator)* The security of the Blum-Blum-Shub generator is based on the difficulty to compute square roots modulo $n = pq$ for two distinct primes p and q with $p, q \equiv 3 \mod 4$.

Design a generator for pseudo-random bits which is based on the hardness of the RSA-problem.

Problem 15. *(proof of Example 10.2)* Complete the proof of Example 10.2 from the lecture notes. Show that from

$$k(x_1 - x_1') \equiv x_0' - x_0 \mod (p-1)$$

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

Problem 16. *(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.