Homework 6 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

15.06.2010

Exercise 16.

The security of the Blum-Blum-Shub-generator is based on the difficulty to compute square roots modulo n, where $n = p\,q$ for two distinct primes p and q with $p, q \equiv 3 \pmod 4$.

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

Exercise 17.

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.
$c \leftarrow E_{m_0}(m_0)$
for i **in** $1 \ldots (n-1)$
  $d \leftarrow E_{m_0}(m_i)$
  $c \leftarrow c \oplus d$
end for
$h(m) \leftarrow c$

Does this function fulfill the basic requirements for a cryptographic hash function? Can these requirements be fulfilled by replacing the XOR-operation by a logical AND?

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 resources required for this attack in terms of memory size, number of comparisons and number of hash function executions.