Homework 5 in Advanced Methods of Cryptography

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

22.11.2011

Exercise 14.

Bob receives the following cryptogram from Alice:

$$(c = 1010101110000011010001011100101111100110111000, x_{t+1} = 1306)$$

The message m has been encrypted using the Blum-Goldwasser cryptosystem with a public key $n = 1333$. The letters of the Latin alphabet $A, \ldots, Z$ are represented by the following 5 bit representation: $A = 00000,\ B = 00001, \ldots,\ Z = 11001$.

(a) Factorize n and decipher the cryptogram c.

Remark: The security requirement to use at most $h = \lfloor \log_2 \lfloor \log_2 n \rfloor \rfloor$ bits of the Blum-Blum-Shub generator is violated in this example. Instead, 5 bits of the output are used.

Exercise 15.

We assume that the attacker has secret access to the decoding-hardware of the Blum-Goldwasser cryptosystem computing the message m when fed with a cryptogram c. The decoded output is not the value x_0 but only the message m.

Furthermore assume that it is possible to compute[1] a quadratic residue modulo n when knowing the last $h = \lfloor \log_2 \lfloor \log_2 n \rfloor \rfloor$ bits of the given quadratic residue.

(a) Show that the given cryptosystem is not secure against chosen-ciphertext attacks.

Exercise 16.

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

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

[1] Assume that a function $f : \{0,1\}^h \to \mathbb{Z}_n$ with $f(b_i) = x_i$, $1 \le i \le t$, exists.