Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 4

Friday, November 20, 2015

Problem 1. *(Goldwasser-Micali)* Using the Goldwasser-Micali cryptosystem, decrypt a ciphertext. Start by finding the cryptosystem's parameters.

a) Find a pseudo-square modulo $n = p \cdot q = 31 \cdot 79$ by using the algorithm from the lecture notes. Start with $a = 10$ and increase a by 1 until you find a quadratic non-residue modulo p. For b, start with $b = 17$ and proceed analoguously.

b) Decrypt the ciphertext $c = (1418, 2150, 2153)$.

Problem 2. *(decpiher Blum-Goldwasser)* Bob receives the following cryptogram from Alice:

$$c = (1010101110000110100010111001011111001101110 00, x_{t+1} = 1306)$$

The message m has been encrypted using the Blum-Goldwasser cryptosystem with public key $n = 1333 = 31 \cdot 43$. The letters of the Latin alphabet $A, \ldots, Z$ are represented by the following 5 bit scheme: $A = 00000,\ B = 00001, \ldots,\ Z = 11001$. 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.

Problem 3. *(chosen-ciphertext attack on Blum-Goldwasser)* Assume that an attacker has 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.

Further 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.

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

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