Homework 4 in Cryptography II

Prof. Dr. Rudolf Mathar, Peter Schwabe

10.05.2007

Exercise 9.
Bob receives the following cryptogram from Alice:

$$(10101011100001101000101110010111110011011100 0, 1306)$$

The corresponding message has been encrypted using the Blum-Goldwasser cryptosystem with public key $n = 1333$. The number 1306 corresponds to the value x_{10} (cf. lecture notes). Decipher the cryptogram.
Hint: The letters of the latin alphabet $A, \ldots, Z$ have been represented using the following 5 bit representation: $A = 00000,\ B = 00001, \ldots,\ Z = 11001$.

Exercise 10.
Show that the Blum-Goldwasser cryptosystem is not secure against chosen-ciphertext-attacks.

Assume that the attacker has access to the decoding-hardware that computes the message when fed with a cryptogram. The output of the machine is not the value x_0 but only the message m. Further assume that it is possible to compute a square root modulo n when knowing the last h bits of this square root.

Exercise 11.
The security of the Blum-Blum-Shub-generator is based on the difficulty to compute square roots modulo n, where $n = pq$ 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.