RWTH AACHEN UNIVERSITY

Lehrstuhl für Theoretische Informationstechnik

Homework 4 in Cryptography II

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

01.06.2010

Exercise 11.

(a) Describe the coin flipping protocol over the telephone. Explain the functionalities of each step of the protocol.

(b) Consider the following protocol:

   a) A chooses $p, q : p, q \pmod 4 \equiv 1$ or $p, q \pmod 4 \equiv 3$. $N = p \cdot q$ and transmits N to B.

   b) B guesses if $p, q \pmod 4 \equiv 1$ or $p, q \pmod 4 \equiv 3$.

   c) A transmits p, q to B.

   If B has guessed correctly then B wins, otherwise A wins. Explain the functionalities of each step of the protocol. On which problem is this protocol based?

(c) How can you realize a coin flipping protocol over the telephone using a hash function $y = h(x)$?

(d) Finally we use the block cipher $y = E_k(x)$. Consider the following protocol:

   a) A and B agree upon a key k.

   b) A chooses x, calculates $y = E_k(x)$ and transmits y to B.

   c) B guesses if x is even or odd.

   d) A transmits x to B.

   If B has guessed correctly then B wins, otherwise A wins. How fair is this protocol? How can you improve this protocol?

Exercise 12.

Establish a message decryption with the Goldwasser-Micali cryptosystem. Start by finding the cryptosystem's parameters.

(a) Find a pseudo-square modulo $n = p \cdot q = 31 \cdot 79$ 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 $c = (1418, 2150, 2153)$.