Security

Assignment 5, Wednesday October 15, 2008

Goals: After successfully completing this exercise you should be able to work with simple encrypting/decrypting in public key cryptography like RSA.

Deadline: Friday October 24, during the lecture or earlier in Flavio's or Olha's post box (in the white cabinet near the printer at the station-side-end of the corridor on the second floor of the Huygens building).

1. (3 points) In exercise 4 of assignment 4 we noticed that a deterministic symmetric- (secret-) key algorithm is not secure if used more than once. This time we want to use a deterministic public key algorithm (for instance RSA) in the same situation, i.e. without using nonces to randomize the message.

   Discuss why Eve's attack from exercise C(a) of assignment 4, in which Alice asked Bob out on a date and Bob answered with either encrypted "yes" or encrypted "no", cannot be used even one time if RSA is used.

2. (4 points) The El Gamal public key cryptosystem is based on a mathematical problem that seems hard to solve, see `http://en.wikipedia.org/wiki/ElGamal_encryption`. Explain this problem briefly, and discuss a brute-force algorithm to solve it.

3. (3 points) Consider the RSA cryptosystem, see e.g.
   `http://nl.wikipedia.org/wiki/RSA_(cryptografie)`.
   Suppose $p = 5, q = 11$ and $e = 29$.

   (a) Determine the corresponding d.

   (b) Explain what the public key is in terms of p, q, e, d.

   (c) Explain what the private key is in terms of p, q, e, d.

   (d) We are going to encrypt the message "rabarber" with the public key in Electronic code book (ECB) mode, that is block-by-block. This is explained in 8.2.3 of Tanenbaum. Take blocks of length 1 letter, so that we have 8 blocks: "r", "a", ..., "r".

   (e) Translate each letter-block into a number: "a" $\mapsto$ 1, "b" $\mapsto$ 2, ..., "A" $\mapsto$ 27, "B" $\mapsto$ 28, ... Write a table.

   (f) Encrypt each integer-block with the public key. Which sequence of numbers do you have?

   (g) Decrypt it with the private key. What do we have (after translating the numbers back into the letters)?

   Explain your answers briefly.