DATA SECURITY/
TIETOTURVA (TUR)

TEST 1

30.11.2005, 10–12

Use of a **calculator** and a **dictionary** is allowed.

Each question is worth 4 points. The number of points for each subquestion is given in brackets (Xp means X points) *after* it. Answer in English or vastaa suomeksi.

GOOD LUCK!

1. Answer shortly the following questions (1p for each):

   (a) What is Kerckhoffs' principle?

   (b) What is the main benefit of the one-time-pad? What is the main drawback of it?

   (c) What does Miller-Rabin test tell about a number?

   (d) What computationally difficult mathematical problem ElGamal is based on?

2. Draw a scheme depicting one phase of DES. (1p) What is the purpose of the f-function? (1p) What is the purpose of the S-boxes in the f-function? (1p) Show how to perform *de*cryption in DES: how to compute blocks L_{i-1} and R_{i-1} if you know L_i, R_i, and subkey K_i? (1p)

3. Apply the column mix transformation (in Rijndael) to the word `53 D4 02 23`. Here is a reminder:

$$\begin{pmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix}$$

   It is enough to calculate s'_0 only. (3p)

   Is the column mix transformation fast in implementations of Rijndael? Explain your answer. (1p)

4. Perform encryption of the message $x = 9$ and decryption of the resulting ciphertext c with the RSA algorithm. Use the following parameters: $p = 5$, $q = 11$, $e = 7$ (where p and q are two prime numbers, and e is the public exponent). What is the secret decryption key in this scheme?