DATA SECURITY/
TIETOTURVA (TUR)

FINAL EXAM

18.1.2006, 12–16

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

Each question is worth 5 points. Answer in English or vastaa suomeksi.

GOOD LUCK!

1. What is the Cipher-Block Chaining (CBC) mode of a block cipher? Draw a scheme for encryption in this mode. What is the initialization vector? Compare CBC to the Electronic-Codebook (ECB) mode.

2. Encryption in the block cipher Rijndael consists of 10-14 rounds. In each of the rounds data blocks are processed step by step:

   (a) Byte substitution
   (b) Shift row
   (c) Mix columns
   (d) Add round key

   Explain what happens in each of these steps.

3. Consider a Diffie-Hellman key exchange with a common prime $p = 19$ and a primitive root $g = 3$. Suppose Alice's *public* key is 4, and Bob's *private* key is 6. What is their common secret key, Alice's private key, and Bob's public key?

4. Give 1–2 lines long answers to the following questions (each worth 1 point):

   (a) According to Shannon, what two basic operations a good secret key encryption is based on?
   (b) How does increase of the block size affect properties of a block cipher?
   (c) What is the main innovation in the Secure Electronic Transaction (SET) protocol?
   (d) What is the difference between a hash function and a message authentication code?
   (e) What computationally difficult mathematical problem RSA is based on?

5. List the properties that a digital signature should have. What techniques can be used for implementation of a good digital signature? Why timestamps, nonces, and other kinds of serial numbers are needed in digital signatures? Explain the difference between direct and arbitrated digital signature.