T-110.5210 Cryptosystems **Exam 14.5.2007**

(Questions are in English only, but you can answer in English, Finnish or Swedish.
Keep your answers short and to the point.)

1. Basic primitives (6p)

a) Define *stream cipher* and *block cipher* (with formulas), and explain how they differ in practice, from an application point of view. **(2p)**
a) Explain (at a high level) some common method of designing a stream cipher. **(2p)**
b) What is meant by resistance against *existential forgery* in the context of MAC functions? **(2p)**

2. Block cipher modes of operation (6p)

a) Which block cipher mode of operation (of those covered in the course) would you choose for encrypting a hard disk? **(1p)**
b) Justify your choice in (a). Compare the mode you chose to other modes of operation from the point of view of hard disk encryption. **(3p)**
c) Which modes of operation (of those covered in the course) have the property that a single bit change in ciphertext changes exactly one bit in the corresponding plaintext (when decrypting)? Justify. **(2p)**

3. Symmetric cryptography (6p)

a) What does the term *effective key length* mean (as in: "X has an effective key length of 80 bits")? **(2p)**
b) What is the effective key length (in bits) of 3DES? Why? **(2p)**
c) Draw a figure and explain how 3DES-EDE-CBC encryption works, with DES as a black box primitive. **(2p)**

4. Asymmetric cryptography (6p)

a) Explain the man-in-the-middle attack against the Diffie-Hellman protocol. Draw a message sequence chart and show also the mathematical computations done by the participants. **(2p)**
b) How could the man-in-the-middle attack be avoided? What is needed in practice? **(2p)**
a) Describe how a public key encryption primitive (such as RSA) can be used to implement *digital signatures*. How is a message **m** signed in such a system (one example)? **(2p)**

5. Protocols and practical issues (6p)

a) What is *wooping*? What possible threats does it help prevent, and what is the basic solution principle? (You don't need to give exact mathematical formulas.) **(4p)**
b) What do cryptographic protocols need random numbers for? **(1p)**
c) Give two examples for sources of true randomness. **(1p)**

6. Side channels (6p)

a) Describe what a *side channel* is, and give an example of how a side channel could be used against Diffie-Hellman. **(6p)**