**T-110.5210 Cryptosystems** **Exam 21.12.2006**

(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)**
b) What is meant by *preimage resistance* and *collision resistance* in the context of hash functions? **(2p)**
c) 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 both encryption and decryption can be parallelized (i.e., there are no dependencies that prevent parallel computation)? 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) Describe the Diffie-Hellman protocol using a figure (include the formulas). **(2p)**
b) Explain the *man-in-the-middle attack* against the Diffie-Hellman protocol. Draw a message sequence chart and also show the mathematical computations done by the participants. **(2p)**
c) 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) How does a cryptographic pseudo-random number generator (PRNG) differ from an ordinary (statistically good) PRNG? **(3p)**
b) What is *secret sharing*? Describe the properties of *Shamir's scheme* for secret sharing. **(3p)**

**6. Side channels (6p)**

a) D. Bernstein has described a timing attack against software AES implementations. What weakness in software implementations of AES enables the attack? How could the attack be prevented? **(3p)**
b) Give an example of how a side channel could be used to attack a Diffie-Hellman computation. **(3p)**