

(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)

- Define *stream cipher* and *block cipher* (with formulas), and explain how they differ in practice, from an application point of view. (2p)
- Explain how a MAC can be constructed using a) a hash function, b) a block cipher. (2p)
- What is meant by resistance against *existential forgery* in the context of MAC functions? (2p)

2. Block cipher modes of operation (6p)

- Which block cipher mode of operation (of those covered in the course) would you choose for encrypting a hard disk? (1p)
- 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)
- Describe the mode you chose in (a) using a figure, for both encryption and decryption. (2p)

3. Symmetric cryptography (6p)

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

4. Asymmetric cryptography (6p)

- Describe the Diffie-Hellman protocol using a figure (include the formulas). (2p)
- 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)
- 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)

- How does a cryptographic pseudo-random number generator (PRNG) differ from an ordinary (statistically good) PRNG? (3p)
- What is *wooping*? Describe the basic solution principle (you don't need to give exact formulas), and explain what possible threat(s) wooping may protect against. (3p)

6. Side and covert channels (6p)

- Define the term side channel briefly. Give two examples of a side channel in cryptographic computations. (3p)
- Explain the difference between a side channel and a covert channel. (3p)