T-110.5211 Cryptosystems   Exam 17.12.2008

(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 a *hash function* (with formulas), and explain what it is used for. **(2p)**
b) Explain (at a high level) some common method of designing a block cipher. **(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? Justify. Compare the mode you chose to other modes of operation from the point of view of hard disk encryption. **(4p)**
b) Which modes of operation (of those covered in the course) have the property that a single bit change in ciphertext changes (with high probability) more than 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) Explain, using formulas, what a *ciphertext collision* means in the context of the CBC mode of operation. What can an attacker deduce about the plaintext as a result? **(4p)**

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. **(3p)**
b) Compute the Diffie-Hellman shared secret in the following scenario. Alice selects n=11 (modulus), g=2 (generator), x=4 (Alice's exponent). Bob selects y=3 (Bob's exponent). Complete the Diffie-Hellman computations on both sides, compute the Diffie-Hellman shared secret, and show that both parties will arrive at the same Diffie-Hellman secret. **(3p)**

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? Give two examples for sources of true randomness. **(2p)**

6. Miscellaneous (6p)

a) Describe what a *side channel* is, and give an example of how a side channel could be used against Diffie-Hellman. **(3p)**
b) Explain Kerckhoffs' principle. **(3p)**