

(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) Explain (at a high level) some common method of designing a stream 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? (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)
- 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)**

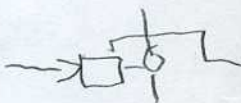
- a) What is *wooping*? What possible threats does it help prevent, and what is the basic solution principle? (You don't need to give exact mathematical formulas.) (4p)
- b) What do cryptographic protocols need random numbers for? (1p)
- c) Give two examples for sources of true randomness. (1p)

**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)

ECB  
CBC  
CTR  
CFB  
KFC

}  
}





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 *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) Describe the mode of operation you chose in (b) using a figure and a short explanation. (2p)

**3. Symmetric cryptography (6p)**

- a) What is the effective key length (in bits) of 3DES? Why? (2p)
- b) Explain the connection between a typical stream cipher and the "one time pad" cipher. (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)
- c) Describe (any) two advantages of Diffie-Hellman when compared to symmetric key distribution (such as the Kerberos protocol). (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) How does a cryptographic PRNG differ from a statistically good but non-cryptographic PRNG? (2p)

**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. (4p)
- b) Explain briefly, at a high level, what enables the Bernstein software AES attack described in lectures. (You don't need to describe formulas or attack details.) (2p)



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) Explain the connection between a *one-time pad cipher* and a typical *stream 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? (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 operation)? 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)
- 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) 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) How does a cryptographic PRNG differ from a statistically good but non-cryptographic PRNG? (2p)

### 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. (4p)
- b) Explain briefly, at a high level, what enables the Bernstein software AES attack described in lectures. (You don't need to describe formulas or attack details.) (2p)



1. (6 pts) The ciphertext

DLVRE BIBCC SWBKW OXYQN ZVFEO OHJDI KRRNI JMEID RIJGC SQGNO CYSUD SXLVS  
YRTTI ZXFIB KQJWC SRXHB OULGX MCRPK VCJKC KRUVR OSKJO BWKCX NEIFD OGYPS  
AYVUK FEIKK XXFHD RMJOO DLFFZ BSGQC OHSAD RIWTO XGYEB ITKQQ BEGJO BOVTM  
ULFHP SWSCC OHFPN SWTQF OVZPQ DLVMO IAFN SXJGV PEEFD RIEWC SRXKD DSUGM  
STYGB DLVEB ITKQQ BED

was generated using the *Vigenere Shift cipher*. Use Kasiski's method to determine the keylength (period).

2. Describe by drawing a picture, or using formulas, or both

- (a) (2 pts) the encryption function of the CBC mode of operation;
- (b) (2 pts) the decryption function of the CBC mode of operation; and
- (c) (2 pts) the CBC MAC.

3. Consider the RSA cryptosystem with modulus  $n = 101 \cdot 131 = 13231$ .

- (a) (3 pts) A random number generator produces three random numbers: 1313, 313 and 1030. Show that only 313 is a suitable value for the public encryption exponent  $e$ .
- (b) (3 pts) Compute the private decryption exponent  $d$  using  $e = 313$ .

4. (6 pts) Determine the modulus  $m$ , multiplier  $a$  and increment  $c$  of a linear congruential generator given four consecutive outputs  $x_2 = 13$ ,  $x_3 = 7$ ,  $x_4 = 14$  and  $x_5 = 9$ . Determine the initial value  $x_0$ .

5. (6 pts) Assume that we have two number generators as black boxes. Both generators output 64-bit numbers. One box contains a Counter Mode PRNG using Triple-DES encryption as  $E_K$  and with a counter of length 64 bits. The second box contains a true random number generator. The boxes look exactly the same, and the task is to determine which one is the true RNG just by examining the output of the generators. After both generators have produced about  $2^{32}$  numbers, one has about 50% chance of being able to distinguish the generators. Explain why.