CHALMERS — GÖTEBORGS UNIVERSITET

EXAM IN CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

15 January 2021, 08:30 – 12.30

Answers must be given in *English* and should be clearly justified.

Teacher/Examiner: Katerina Mitrokotsa
Questions during exam: Katerina Mitrokotsa, phone 031 772 1040

The exam is divided in four main topics and the total number of points is 50).
The grades are:

CTH Grades:	22-30 → 3	31-39 → 4	40-50→5
GU Grades:	22-39 → G	40-50 → VG	

Good luck!

1 Symmetric Ciphers (15 p)

(a) Let us consider the following symmetric cipher:

$$E(k, m_0) = E(k, m_{00}||m_{01}) = E(k \oplus m_{00})||m_{01}$$

where m_{00} and m_{01} denote the first and second bit of a message m_0. Prove that this symmetric cipher is not semantically secure. (4 p)

Hint: Use a security game and describe a successful strategy of the attacker.

(b) Does the One Time Pad (OTP) provide integrity? Describe with an example why integrity cannot be guaranteed when using OTP to encrypt and decrypt messages. (2 p)

(c) You are using the CTR mode of operation to encrypt a message and the IV has length 256 bits while the nonce has length 128 bits. How many blocks can you encrypt with one nonce to guarantee security (*i.e.,* a message will not be encrypted using the same IV)? (2 p)

Hint: We consider that the IV is composed of two parts a nonce (random number used only once) that has length 128 bits and a counter that has length 128 bits.

(d) Bob is using a block cipher E where both the block size and the key size are 64 bits. Since he considers the key size to be short, he uses a variant of this block cipher by incorporating two keys in the cipher. More precisely, to encrypt a message m two keys (k_0, k_1) are used as follows:

$$c = E_{k_0}(m) \oplus k_1$$

Suppose that an adversary gets access to two plaintext/ciphertext pairs (i.e., (m, c) and (m', c')) and is able to perform a brute-force attack on the original block cipher E and recover the key in a known plaintext attack.

   (a) Show that the adversary can also break Bob's "improved" cipher and recover his extended key. (2 p)

   (b) Does the attack against the "improved" cipher require much more effort than an attack against the block cipher E? Explain why. (2 p)

(e) n different entities (*i.e.,* persons) need to communicate with each other using *secret key cryptography*. How many keys are needed to guarantee *confidentiality* among all parties? Would it be possible to achieve *non-repudiation* in this setting? (3 p)

2 Public Key Encryption (10 p)

(a) Alice is using textbook RSA to encrypt and decrypt messages and send them to Bob. Eve realises that textbook RSA is used and performs a successful IND-CCA attack. Show what is the strategy that Eve will follow to win the security game for an IND-CCA attack. (4 p)

(b) We consider double RSA encryption using a common modulus N and two public keys e_1 and e_2 with corresponding private keys. Thus, a message m is encrypted first using RSA encryption with the key e_1; the result is encrypted again using key e_2. Explain why this approach does not increase security. (3 p)

(c) You are working in a company and you are responsible for the *confidentiality* of some files that need to be shared with different clients (one file for each client) *i.e.,* only one client should be able to decrypt the corresponding file. You plan to use an encryption algorithm to encrypt the files. Would you use a *symmetric key encryption* or a *public key encryption* algorithm? Discuss the advantages and disadvantages of each choice. (3 p)

3 Data Integrity (14 p)

(a) Bob has received from Alice two signed documents (m_1, σ_1) and (m_2, σ_2) computed via the textbook RSA signature scheme. Show that Bob can compute a valid signature for a new message using the messages m_1, m_2 and the corresponding signatures σ_1 and σ_2.

Hint: Describe a successful existential forgery. Use a security game and a successful strategy of the attacker. (4 p)

(b) Describe how the above existential forgery can be avoided and give a complete definition of the signature scheme (*i.e.,* the key generation, the signing and the verification algorithm) that avoids this forgery. (4 p)

(c) Explain in simple words what does the birthday paradox state and how it affects the security of a hash function, i.e., what is the security level provided for a hash function with output n bits. (2 p)

(d) You are given a MAC that is produced using a hash function that follows the Merkle-Damgard construction such that $MAC(m) = H(k||m||p)$ where k denotes the secret key shared between the sender and the recipient and p padding. Is this MAC construction secure against existential forgeries? Prove it using a security game. (4 p)

4 Cryptographic Protocols (11 p)

(a) Suppose that Alice has a secret value $a = 2$ and Bob has a secret value $b = 4$. Describe how Alice and Bob may establish a secret key using the Diffie-Hellman protocol using the group $G = \mathbb{Z}_{13}$ and the generator $g = 6$. (2 p)

(b) Describe how Eve may perform a man-in-the-middle attack against the Diffie-Hellman exchange protocol used above. (2 p)

(c) Assume that we have three parties P_1, P_2 and P_3 and that we tolerate $t = 1$ corrupted parties. Assume that we work in $\mathbb{Z}_{11}$ and each of the parties have a secret value $a = 4$, $b = 3$ and $c = 2$ correspondingly. The three parties want to compute the sum $\sigma = a + b + c$ while keeping their corresponding value secret.

Using Shamir's secret sharing show how to calculate the sharing of a, b, c and of their sum σ. More precisely if we denote by a_1, a_2, a_3 the shares of the secret value a and we denote similarly the shares of b, c and σ. Then:

(i) Show how P_1, P_2 and P_3 can compute the sum $\sigma = a + b + c$, without disclosing the values a, b and c. (3 p)

Hint: Fill in the following table:

	P_1	P_2	P_3
$a = 2$	a_1	a_2	a_3
$b = 4$	b_1	b_2	b_3
$c = 1$	c_1	c_2	c_3
$\sigma = a + b + c$	σ_1	σ_2	σ_3

(ii) Consider that P_3 decides not to collaborate with P_1 and P_2. Can P1 and P2 ~~Can P_1 and P_3~~ still compute the sum σ? If yes, justify why and show how. (4 p)