CHALMERS — GÖTEBORGS UNIVERSITET

EXAM IN CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

25 April 2019, 08:30 – 12.30

Tillåtna hjälpmedel: Typgodkänd räknare. Annan minnestömd räknare får användas efter godkännande av kursansvarig vid dennes besök i skrivsalen.
No extra material is allowed during the exam except of pens and a simple calculator (with cleared memory). No smartphones or other electronic devices are allowed.
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 (14 p)

(a) Let (Enc, Dec) be a cipher such that there exists an algorithm B that given the ciphertext $c \leftarrow Enc(k,m)$ retrieves the least significant bit of the plaintext, i.e. $B(c) = LSB(m)$ for any k. Show that this not semantically secure and compute the advantage of compromising the cipher using B. (4 p)

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

(b) Describe how encryption and decryption works in ECB (Electronic Codebook Block) mode for block ciphers. (1 p)

(c) Show that ECB (Electronic Codebook Block) mode for block ciphers works is not semantically secure when a message is longer than one block. (4 p)

Hint: Use in your description a security game and a successful strategy of the attacker in the case the messages used in the security game have length two blocks).

(d) We consider Triple DES encryption, in the common form

$$E3_{(K_1,K_2)}(B) = E_{K_1}(D_{K_2}(E_{K_1}(B)))$$

where E_K and D_K denote the standard (single) DES encryption and decryption functions, respectively and $E3_{(K_1,K_2)}$ denotes Triple DES encryption with key (K_1,K_2). This form of 3DES uses two keys and three operations and achieves 112 bits of security.

A similar construction is 2DES:

$$2DES_{k_1,k_2}(m) = E_{k_1}(E_{k_2}(m))$$

However 2DES does not achieve 112 bits of security, due to the *meet-in-the-middle* attack.

1 Describe the steps of the meet-in-the-middle attack in detail, if necessary use also a figure. (4 p)

2 What level of security does 2DES achieve (i.e., how many steps of computation the adversary has to do for the attack) (1 p)?

2 Public Key Encryption (12 p)

(a) Let $G = \mathbb{Z}_{13}^*$ and $g \in G$. Show that g=6 is a generator of the group G. (2 p)

(b) Suppose that Alice has a secret value $a = 3$ and Bob has a secret value $b = 6$. 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)

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

(d) We consider Elgamal encryption using a generator g for p^* for some large prime p. Remainder: Every user chooses a random private key $x < p$ and computes the public key $X = g^x$. To encrypt message m for a user with public key X, the sender chooses a random $y < p$ and computes the encryption $(g^y, m \cdot X^y)$.

Describe how decryption is done. (2 p)

(e) Show that El Gamal encryption is not secure against chosen chiphertext attacks (IND-CCA) (4 p)

3 Data Integrity (12 p)

(a) Explain what a cryptographic hash function is and the notion of collision resistance. (2 p)

(b) Describe the birthday paradox and its impact on the security of hash functions. (3 p)

(c) Suppose H_1 and H_2 are collision resistant hash functions mapping inputs in a set $\mathcal{M}$ to $\{0,1\}^{256}$. Show that the function $H_2(H_1(m))$ for $m \in \mathcal{M}$ is also collision resistant. (3 p)

Hint: Prove the contra-positive.

(d) MACs are employed in symmetric key cryptography to guarantee the integrity of a message. Consider the case of designing a MAC scheme that employs a hash function with iterative structure (e.g. uses the Merkle-Damgard iterated construction) and works as follows:

$$MAC(m) = h(K||m||p),$$

where m is the message for which we need to guarantee integrity, K is the symmetric key shared between two communicating parties (e.g. Alice and Bob) and p is padding.

Show that this MAC scheme is not secure against existential forgery (i.e. possible to create a valid MAC for an unknown message). (4 p)

4 Cryptographic Protocols (12 p)

1. Let $\langle g \rangle$ be a group of order n, where n is a large prime. Let x selected uniformly at random from $\mathbb{Z}_q$ be the prover's private key, and let $X = g^x$ bet the prover's public key (the verifier has the prover's public key). Peggy (the prover) and Victor (the verifier) run the following zero-knowledge protocol:

Verifier $\mathcal{V}$		**Prover $\mathcal{P}$**
		x secret key
X		$X = g^x$
		$r \in \{1,2,\ldots,q-1\}$
	$\xleftarrow{R}$	$R = g^r$
$c \in \{1,2,\ldots,q-1\}$	$\xrightarrow{c}$	
$R \stackrel{?}{=} g^s \cdot X^{-c}$	$\xleftarrow{s}$	$s = (r + c \cdot x) \bmod q$

   (a) Show that a true Peggy, following the protocol will be identified correctly by Victor. (2 p)

   (b) Can an adversary impersonate Peggy successfully? If yes, what is the corresponding success rate? (2 p)

   (c) Can Victor transfer his knowledge, that indeed Peggy has the secret x, to someone else? Explain why. (2 p)

2. Assume that we have five parties $P_1, \cdots, P_5$ and that we tolerate $t = 2$ corrupted parties in a Shamir threshold secret sharing scheme.
   Assume that we work in $\mathbb{Z}_{11}$ and want to share the secret value $s = 8$.

   - Show how we can distribute s among five parties, *i.e.*, compute the shares $s_1, \cdots, s_5$. Each of the shares s_i is sent to the party P_i ($i \in \{1, \cdots, 5\}$) (2 p)
   - Assume that someone is given the shares s_3, s_4, s_5, while someone else is given the shares s_1, s_2. Which of the two is able to compute the secret s on its own? Show how? (4 p)