CHALMERS — GÖTEBORGS UNIVERSITET

EXAM IN CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

26 August 2020, 14:00 – 18.00

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

Teacher/Examiner: Katerina Mitrokotsa
Questions during exam: Katerina Mitrokotsa phone: 031 772 1040 or
Carlo Brunetta, phone: 031 772 1619

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

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

Good luck!

1 Symmetric Ciphers (16 p)

(a) Describe in simple words what *perfect secrecy* means. (2 p)

(b) Does *perfect secrecy* imply integrity? Does One Time Pad (OTP) provide integrity? (2 p)

(c) Describe in simple words how we may perform encryption and decryption using *stream ciphers*. (2 p)

(d) Consider that the PRG used to construct a stream cipher is *predictable*. Describe how an attack can be performed against the stream cipher. (2 p)

(e) 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.,* $B(c) = MSB(m)$ for any key k. Show that this is not semantically secure and compute the advantage of compromising the cipher using B. (4 p)

Hint: use the standard game between a challenger and an adversary.

(f) Consider a variant of DES block cipher defined as: $DESX'_{k_1,k_2}(m) = Enc_{DES}(k_1,m) \oplus k_2$ Is $DESX'$ secure? Is it possible to perform a better attack than a simple brute force? If yes explain the attack in detail and give an estimation of the complexity required. (4 p)

2 Public Key Encryption (10 p)

(a) Let us assume that in order to encrypt a message m we use the following encryption algorithm $Enc(m,k) = (m^{e_1}(\mod N))^{e_2} \pmod N$, where $k = e_1||e_2$. Explain why this encryption algorithm is not more secure than textbook RSA. (4 p)

(b) In a *chosen ciphertext* attack the adversary wants to decrypt a message c and is allowed to ask for and get the decryption of any message except of c. Show that textbook RSA is not secure against such an attack. (4 p)

Hint: use the standard game between a challenger and an adversary.

(c) You are working in a company and you are responsible for the confidentiality of some data. You plan to use an encryption algorithm to encrypt the data. Would you use a symmetric key encryption or a public key encryption algorithm? Discuss the advantages and disadvantages of each choice. (2 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 an homomorphic signature scheme. Show that Bob can perform an existential forgery attack against the underlying signature scheme, *i.e.,* given messages, m_1, m_2, and the corresponding signatures, σ_1 and σ_2. (4 p)

Hint: Show this by describing an attacker and his strategy to win the existential forgery game against signatures that satisfy the homomorphic property.

(b) How can we change the way we produce signature schemes that satisfy the homomorphic property to protect against the above existential forgery attack? Give the construction for the modified textbook RSA signature scheme and show that the attack no longer works. (3 p)

(c) Describe the two main properties that a cryptographic hash function should have. (2 p)

(d) Consider that H_1 and H_2 denote two collision resistant hash functions mapping inputs in a set $\mathcal{M}$ to $\{0,1\}^{256}$. Is the function $H_2(H_1(m))$ for $m \in \mathcal{M}$ collision resistant? Explain your answer. (3 p)

(e) You are working as a security consultant and you are asked to prove the *authenticity* and *integrity* of an important document m generated by you and sent to five more entities. How can you prove this? Would you use a primitive from public key cryptography (*i.e.,* signature) or secret key cryptography (*i.e.* MAC)? Explain your choice and the reasons for this. (2 p)

4 Cryptographic Protocols (10 p)

(a) Let p, q two large prime numbers such that $N = p \cdot q$. Let $s \in \mathbb{Z}_N$ such that $gcd(s,N) = 1$ and it holds $v = s^2 \pmod N$.

Peggy (the prover) and Victor (the verifier) run the following zero-knowledge protocol:

Verifier (Victor) $\mathcal{V}$		**Prover** (Peggy) $\mathcal{P}$
(N, v)		(N, s, v)
		s secret key
		pick a random
		$r \in \{1, 2, \ldots, N-1\}$
pick a random	$\xleftarrow{w}$	$w = r^2 \pmod N$
$c \in \{0,1\}$	$\xrightarrow{c}$	compute
check	$\xleftarrow{z}$	$z = rs^c \pmod N$
$z^2 = wv^c \pmod N$		

i. Can Victor persuade his friend Charlie, that indeed Peggy has the secret x? Explain why. (2 p)

ii. Consider that an adversary is able to always predict the challenge correctly. What is the probability of successfully passing the protocol without knowing the secret key x. Explain in detail. (2 p)

(b) Consider that we have three parties P_1, P_2 , P_3 and each of them has a secret value $a = 2$, $b = 3$ and $c = 4$ correspondingly. Consider that we are in $\mathbb{Z}_{11}$.

i. Show how P_1, P_2 and P_3 using the secure multi party computation protocol for addition (that we have seen in the lectures) based on Shamir's Secret Sharing Scheme with $t = 2$ can compute the sum σ; i.e., fill in the following table. (3 p)

	P_1	P_2	P_3
$a = 4$	a_1	a_2	a_3
$b = 3$	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_2 decides not to collaborate with P_1 and P_3. Can P_1 and P_3 still compute the sum s? If yes, justify why and show how. (3 p)