CHALMERS — GÖTEBORGS UNIVERSITET

EXAM IN CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

12 January 2018, 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 (plus 6 *bonus points*).
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 (9 p)

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

(b) Describe how we may get a pseudorandom generator (PRG) from a pseudorandom function (PRF). (2 p)

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

(d) 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).

2 Public Key Encryption (11 p)

(a) Describe how the El Gamal encryption scheme works. (2 p)

Hint: Describe the algorithms with their corresponding input and output.

(b) What does the discrete log problem state? (2 p)

(c) *Bonus points: Give the definition of chosen-chiphertext attacks (IND-CCA) for public key encryption using a security game. (3 p)*

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

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

3 Data Integrity (18 p)

(a) Describe the textbook RSA signature scheme. (2 p)

Hint: Describe the algorithms with their corresponding input and output.

(b) Show that textbook RSA signatures have the homomorphic property. (2 p)

(c) *Bonus points: How do we define an existential forgery in digital signatures? (3 p)*

Hint: Give the security game and formal definition.

(d) Describe an existential forgery against RSA signatures. (5 p)

Hint: Describe an existential forgery that relies on their homomorphic property. Use a security game and a successful strategy of the attacker.

(e) How may we avoid this forgery? Describe a solution and explain why in this case the forgery is not possible. (3 p)

(f) Give three advantages of digital signatures in comparison to MACs (message authentication codes). (3 p)

4 Cryptographic Protocols (18 p)

(a) Let $\langle g \rangle$ be a group of order n, where n is a large prime. Let selected uniformly at random from $\mathbb{Z}_q$ be a 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		$X = g^x$
		$r \in \{1,2,\ldots,q-1\}$
	$\xleftarrow{R}$	$R = g^r$
$c \in \{1,2,\ldots,q-1\}$	$\xrightarrow{c}$	
$R \stackrel{?}{=} g^s \cdot X^{-c}$	$\xleftarrow{s}$	$s = (r + c \cdot x) \bmod q$

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

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

iii. Peggy (the prover) happens to use the same R in two different executions of the protocol. Can Victor (the verifier) learn anything about x? If yes show how. (3 p)

(b) Consider that we have three parties P_1, P_2, P_3 and each of them has a secret value $a = 3$, $b = 5$ and $c = 2$ correspondingly. We are using the secure multi party computation (SMPC) protocol for addition (that we have seen in the lectures) based on Shamir's Secret Sharing Scheme with $t = 1$.

i. Show how P_1, P_2 and P_3 can distribute shares of their secrets a, b, c to each other and compute the shares of the sum $\sigma = a + b + c$ *i.e.,* fill in the following table. (3 p)

	P_1	P_2	P_3
$a = 3$	a_1	a_2	a_3
$b = 5$	b_1	b_2	b_3
$c = 2$	c_1	c_2	c_3
$\sigma = a + b + c$	σ_1	σ_2	σ_3

ii. Show how P_1, P_2, P_3 using the shares σ_1, σ_2 and σ_3, can compute the sum σ. (4 p)

iii. Consider that P_3 decides not to announce his share σ_3 and thus P_1 and P_2 collaborate announcing σ_1 and σ_2. Is it still possible to compute the sum σ? If yes, justify why and show how. (4 p)