CHALMERS — GÖTEBORGS UNIVERSITET

EXAM IN CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

18 January 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 (plus 6 *bonus points*).
The grades are:

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

Good luck!

3 Data Integrity (15 p)

(a) *Bonus points: How do we define a secure MAC (message authentication code)? (3 p).*

Hint: Give the security game and formal definition.

(b) Describe how raw CBC-MAC works. (2 p).

(c) Show that raw CBC-MAC is insecure. (5 p).

Hint: Describe an existential forgery. Use a security game and a successful strategy of the attacker. Consider that in the challenge phase, a message with length two blocks is used.

(d) How may we avoid the security problem in raw CBC-MAC? Describe a solution. (2 p).

(e) Give three advantages of digital signatures in comparison to MACs. (3 p)

4 Cryptographic Protocols (13 p)

1. 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	$\xleftarrow{\;z\;}$	$z = rs^c \pmod N$
$z^2 = wv^c \pmod N$		

(a) What is the probability that a fake Peggy (not having the secret s) to be identified correctly. Justify your answer and explain how we may decrease the success probability of a fake Peggy. (1 p).

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

(c) Consider that an attacker (who does not have access to the secret key) can always predict Victor's challenge. Describe how the attacker may always successfully pass the protocol. (3 p).

2. Consider that we have three parties P_1, P_2, P_3 and each of them has a secret value $a = 1, b = 2$ and $c = 3$ 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 $t = 1$.

(a) 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. (4 p)

Hint: Describe how P_1, P_2 and P_3 create their shares and distribute them and how finally the sum is computed.

(b) Consider that P_3 decides not to collaborate with P_1 and P_2. Can P_1 and P_2 still compute the sum σ? If yes, justify why and show how. (3 p)