CHALMERS — GÖTEBORGS UNIVERSITET

CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

12 Jan. 2017, 14:00 - 18:00

No extra material is allowed during the exam except for pens and a simple calculator (not smartphones). *No other electronic devices allowed.* Your answers in the exam must be written in *English.* Your language skills will not be graded (but of course we cannot grade your answer if we do not understand it), so try to give *clear answers.* Your thoughts and ways of reasoning must be clearly understood!

Teacher: Elena Pagnin
Examiner: Aikaterini Mitrokotsa
Questions during the exam: Elena Pagnin (phone 072 9681552)
Inspection of exam: See web page for announcement.

The exam has 4 *topics* and *some bonus questions* to gain extra points.
The total number of points is 100 points *(+ 8 bonus points).*
Grades are :

CTH Grades:	50-64 → 3,	65-89 → 4,	90 or above → 5
GU Grades:	50-89 → G,	90 or above → VG	

Good luck!

Symmetric Ciphers (20p)

1. Consider the message $m =$ `HKPUFCMHY BHDDXZH`, and let $(\mathbf{E}, \mathbf{D})$ be a substitution cipher.

   (a) Decrypt m using the following (secret) substitution key: **(2p)**

plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O

   (b) Can this cipher be broken by someone who has access to m but not to the secret key? Why? **(3p)**

2. Let ($\mathbf{E}$, $\mathbf{D}$) be a (one-time) semantically secure cipher, where the messages, ciphertexts and keys are binary strings, e.g., you can think $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n$, with $n \geq 2$. Are the following encryption schemes, derived from ($\mathbf{E}$, $\mathbf{D}$), semantically secure or not? Explain why (no need for formal proofs, but your motivations should be well-justified).
   Why do we require $n \geq 2$? Would $n = 1$ provide different answers? (1 bonus point)

   (a) $\mathbf{E}'(k, m) = \mathbf{E}(k, m) \oplus \mathbf{1}$, where $\mathbf{1}$ denotes the string with all ones. **(2p)**

   (b) $\mathbf{E}'(k, m) = \mathbf{E}(k, m)||RB(m)$, where $RB(m)$ gives back a random bit of the input m. **(2p)**

   (c) $\mathbf{E}'(k, m) = \mathbf{E}(k, m)||RB(k)$, where $RB(k)$ gives back a random bit of the input k. **(2p)**

3. Does the OTP (One Time Pad) cipher achieve perfect secrecy? Prove it. **(9p)**
   (Hint: you can start by quickly describing how the OTP cipher works and how perfect secrecy is defined).

Public Key Encryption (30p)

4. Describe the ElGamal encryption scheme. **(6p)**
   (Hint: write down input, output and behaviour of the algorithms).

5. Define the IND-CCA security game (indistinguishability chosen ciphertext attack) and show that the ElGamal encryption scheme is not secure under IND-CCA. **(11p)**

6. Consider the cyclic group $\mathbb{Z}_{37}^*$. *If you explain in details the functions / theorems / theory involved in this exercise you can gain a maximum of (3 bonus points)*

   (a) How many elements are in $\mathbb{Z}_{37}^*$, i.e., what is the order of the group? **(2p)**

   (b) Is $\mathbb{Z}_{37}^*$ a cyclic group? How many generators does it have? **(4p)**

   (c) Is 4 a generator of $\mathbb{Z}_{37}^*$? Prove it. **(7p)**

Data Integrity (20p)

7. Describe the RSA digital signature scheme. **(10p)**
   (Hint: write down input, output and behaviour of the algorithms).

8. Let $N > 2$ be a positive integer. Consider the function $h : \mathbb{Z} \longrightarrow \mathbb{Z}_N$, defined as $h(m) = m \mod N$. To check if h is a cryptographic hash function we need to assure that h satisfies (at least) the following three properties:

   (2a) Given a message m, the message digest $y = h(m)$ can be computed in an efficient way.

   (2b) Given a message digest y, it is computationally infeasible to find an m with $h(m) = y$ (in other words, h is a one-way, or pre-image resistant function).

   (2c) It is computationally infeasible to find two dinstint messages $m_1, m_2 \in \mathbb{Z}$ such that $h(m_1) = h(m_2)$ (in this case, the function h is said to be collision-free).

   Check if h is a cryptographic hash function, i.e., for each of the properties ((8a), (8b) and (8c)) show if h satisfies it or not. **(10p)**

Advanced Topics in Cryptography (30p)

9. Describe in your own words (or give the definition of):

   (a) Unconditional and provable security. Also, give at least one example of a cryptosystem in each category. **(6p)**

   (b) The three main properties of the Fiat-Shamir identification protocol (Completeness, Soundness and Zero-Knowledge). **(8p)**

10. Consider the Secure Multiparty Computation (SMPC) protocol for addition, based on the Shamir Secret Sharing Scheme, seen in class. Assume that there are $n = 4$ parties (P_1, P_2, P_3, P_4), that the system tolerates $t = 3$ corrupted parties, and that all computations are done in $\mathbb{Z}_{13}$.

    (a) Imagine you are P_1, and your secret input to the computation is $a = 5$. Explain how you would share your secret value a with the other parties and what you expect to receive from each other party (note that no explicit computation is required for this step, just a formal description of how the scheme works). **(4p)**

    (b) Now, imagine you are P_1 and hold the table below (which corresponds to your view of the protocol). Compute the value $S = a+b+c+d$ using the information contained in the table. **(12p)**

	P_1	P_2	P_3	P_4
$a = 5$	$a_1 = 5$	$a_2 = 12$	$a_3 = 7$	$a_4 = 10$
$b =?$	$b_1 = 4$	?	?	?
$c =?$	$c_1 = 12$	?	?	?
$d =?$	$d_1 = 9$	?	?	?
S	$s_1 = 4$	$s_2 = 6$	$s_3 = 1$	$s_4 = 7$

    (c) *Bonus question: Looking at the table in point (10b), are you able to determine what was the polynomial f chosen by P_1 to share a? Why? Compute the polynomial f, if possible.* *(4 bonus points)*