**CHALMERS | GÖTEBORGS UNIVERSITET**

# Cryptography

**TDA352 (Chalmers) - DIT250 (GU)**

**24 August 2017, 8:30 - 12:30**

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 plaintext *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.* You can draw diagrams to explain concepts like security games, cryptographic protocols or simple ciphers modes of operation. In any case, 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. Let $(\mathbf{E}, \mathbf{D})$ be a secure block cipher. Describe the CBC mode of operation (encryption and decryption). **(8p)**

2. Show that the One Time Pad (OTP) cipher is malleable, i.e., that and adversary can change the ciphertexts so that it decrypts to a different message. **(7p)**

3. Let (**E**,**D**) be a correct cipher. Write the formula for correct decryption in the encryption schemes below.
(Hint: your solution should look like $\mathbf{D}'((k_1, k_2), c) = \mathbf{D}(k_1, c \oplus k_1) \oplus k_2$ ).
   (a) $\mathbf{E}'((k_1, k_2), m) = \mathbf{E}(k_1, m) \oplus k_2 \oplus k_1$. **(2p)**
   (b) $\mathbf{E}'((k_1, k_2, k_3), m) = \mathbf{E}(k_3, \mathbf{E}(k_2, \mathbf{E}(k_1, m)))$. **(3p)**

## Public Key Encryption (30p)

4. This exercise is about RSA encryption. You are given two prime numbers $p = 11$ and $q = 17$, an RSA modulus $N = p \cdot q = 187$, and an encryption exponent $e = 3$.
   (a) Compute the RSA decryption exponent $d$. **(7p)**
   (b) Encrypt the message $m = 100$ using RSA with the values given above. **(7p)**

5. Give a pseudocode for Fermát primality test. **(8p)**
(Hint: Fermát's primality test is based on Fermát little theorem that states: $a^p = a \mod p$ if $p$ is a prime number (and $a \in \mathbb{Z}_p \setminus \{0\}$))

6. Use the Chinese Remainder Theorem (CRT) to solve the following system of linear congruences. **(8p)**

$$\begin{cases} x = 1 \mod 7 \\ x = 3 \mod 11 \end{cases}$$

7. *Bonus question: describe the IND-CCA security game (indistinguishability chosen ciphertext attack)* *(4 bonus points)*

## Data Integrity (20p)

8. Consider the following signature scheme. The setting is a cyclic group $\mathbb{Z}_q^*$, for a large prime $q$. Let $g$ be a generator for $\mathbb{Z}_q^*$.
The **KeyGen** algorithm picks a random value $\mathbf{sk} = x \in \mathbb{Z}_q^*$, computes the corresponding public key $\mathbf{pk} = X = g^x \in \mathbb{Z}_q^*$, and outputs $(\mathbf{pk}, \mathbf{sk})$.
The **Sign** algorithm takes as input **sk** and a message $m \in \{0,1\}^n$, and proceed as follows. First it computes $h = H(m) \in \mathbb{Z}_q^*$ for some hash function $H : \{0,1\}^n \longrightarrow \mathbb{Z}_q^*$. Secondly, it computes $z = xh^{-1}$ in $\mathbb{Z}_q^*$. Finally, it outputs the signature $\sigma = g^z$.
   (a) Define the correctness property of a signature scheme. **(2p)**
   (b) What computations should the **Verify** algorithm perform for the above signature scheme to be correct? **(3p)**
   (c) Is it computationally infeasible for an attacker to produce a valid signature for an arbitrary message $m^*$, without knowing the secret key $x$? **(5p)**

9. Let $2 < N < 100$ be a positive integer such that $GCD(N, 3) = 1$. Consider the function $h : \mathbb{Z} \longrightarrow \mathbb{Z}_N$, defined as $h(m) = 3m + 1 \mod N$.

   (a) Is $h$ such that, given a message digest $y$, it is computationally infeasible to find an $m$ with $h(m) = y$? Why? (i.e., is $h$ one-way / pre-image resistant?). **(5p)**

   (b) Is $h$ such that it is computationally infeasible to find two distinct messages $m_1, m_2 \in \mathbb{Z}$ such that $h(m_1) = h(m_2)$? Why? (i.e., is $h$ collision-free?). **(5p)**

## Advanced Topics in Cryptography (30p)

10. Consider the following identification protocol based on the discrete logarithm problem. $G =< g >$ is a cyclic group of prime order $q$, the prover (called Peggy) has a private key $x \in \{1, 2, \ldots, q-1\}$ and publishes the corresponding public key $h = g^x \in G$. The purpose of the protocol is to convince the verifier (called Victor) that Peggy knows the secret value $x$:

    -1- Peggy chooses a random $r \in \{1, 2, \ldots, q-1\}$, computes $R = g^r$ and $S = g^{x-r}$. She sends $R$ and $S$ to Victor.

    -2- Victor chooses a random challenge bit $c \in \{0, 1\}$, and sends $c$ to Peggy.

    -3- Peggy replies to Victor with the value $z = cx - r$.

    (a) What computations should Victor do in order to check Peggy's values? **(4p)**

    (b) Show that if Eve, who does not know Peggy's secret key $x$, can predict Victor's challenge, than she has probability 1 to pass the identification protocol (i.e., be accepted by Victor). **(6p)**
    (Hint: for the case $c = 1$, you can try to swap the role of $R$ and $S$)

    (c) Show that if an honest Peggy chooses the same randomness $r$ twice, an honest-but-curious Victor can retrieve Peggy's secret $x$. **(6p)**

11. Consider Shamir Secret Sharing Scheme. 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 the Dealer. Explain how you would share your secret value $a$ among the four parties (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 your share is $a_1 = 5$. Suppose you also learn the other parties' shares: $a_2 = 12, a_3 = 7, a_4 = 10$. Can you recover the secret value $a$ shared among the four parties? Show how or explain why not. **(10p)**

12. *Bonus question: describe textbook Diffie-Hellman key exchange. (4 bonus points)*