**CHALMERS — GÖTEBORGS UNIVERSITET**

# Cryptography

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

**11 April 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:** Carlo Brunetta (phone 072 3515913)
(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.

   (a) Describe the ECB mode of operation (encryption and decryption). **(5p)**

   (b) Show that ECB is not semantically secure if the length of the message is more than two blocks. **(9p)**
   (Hint: start by describing the semantic security game and show a successful attack strategy in the case $M = (m_0, m_1)$ is a two-block message).

   (c) *Bonus question: Give the definition of a secure Pseudo-Random Generator.* *(3 bonus points)*

2. 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) $\mathbf{E}'((k_1, k_2), m) = \mathbf{E}(k_1, m \oplus k_2)$. **(2p)**

   (b) $\mathbf{E}'((k_1, k_2), m) = \mathbf{E}(k_1, m) \oplus k_2$. **(2p)**

   (c) $\mathbf{E}'((k_1, k_2), m) = \mathbf{E}(k_2, \mathbf{E}(k_1, m)) \oplus k_1$. **(2p)**

## Public Key Encryption (30p)

3. Describe the RSA encryption scheme. **(7p)**

4. This exercise is about the Extended Euclidean Algorithm (and modular inversion).

   (a) Use the Extended Euclidean Algorithm to show that 25 and 28 are relatively prime and to find $x, y \in \mathbb{Z}$ such that $25x + 28y = 1$. **(6p)**

   (b) Are there many integer solutions $x$, $y$ to the equation $25x + 28y = 1$? Write them explicitly. **(5p)**

   (c) Compute the inverse of 25 in $\mathbb{Z}_{28}^*$ and the inverse of 28 in $\mathbb{Z}_{25}^*$ . **(2p)**

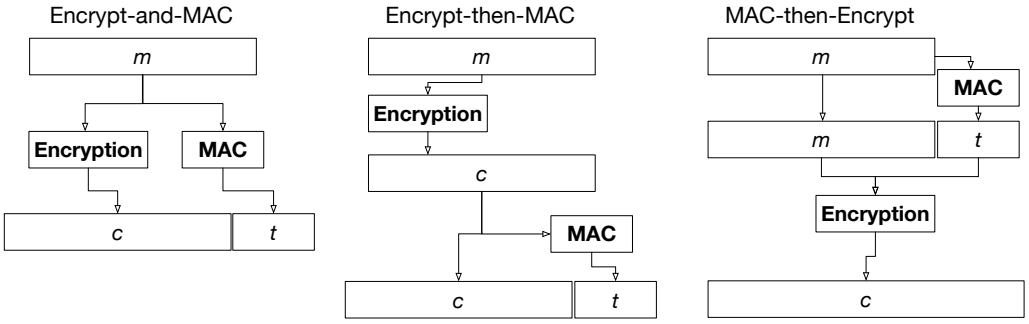
   (d) How many elements are in $\mathbb{Z}_{28}^*$? **(2p)**

   (e) *Bonus question: Write down all the elements in $\mathbb{Z}_{28}^*$.* *(3 bonus points)*

5. Describe the Man-in-the-Middle attack against the Diffie-Hellman key-exchange protocol. **(8p)**

## Data Integrity (20p)

6. In order to achieve authenticated encryption, i.e., authenticity (and integrity) of ciphertexts one can combine a MAC (Message Authentication Code) with an Encryption scheme in the following three ways:




   (a) Using the functions $\mathbf{Enc}(\mathbf{pk}, \cdot)$ and $\mathbf{MAC}(\mathbf{sk}', \cdot)$, write the output of the three schemes above. **(6p)**
   *(Hint: your answer is a composition of the above functions. It shall look like:* $\mathbf{Enc}\big(\mathbf{pk}, \mathbf{MAC}(\mathbf{sk}', m)\big)$*. You can denote the concatenation of two strings with the symbol* $||$*.)*

   (b) Write an Authenticated-Decryption algorithm for the Encrypt-and-MAC scheme. Note that the output of $\mathbf{ADec}\big((\mathbf{sk}, \mathbf{sk}'), c \,||\, t\big)$ is $\perp$ if we cannot guarantee the integrity of the message, otherwise the output is the correct plaintext. **(4p)**

7. One fundamental property of hash functions is *collision resistance*.

   (a) Give the definition of a collision resistant hash function. **(3p)**

   (b) What security class do collision resistant hash function belong to? (e.g. unconditional security, computational security...) **(2p)**

   (c) Prove the birthday paradox: for large enough $N$ (where $N$ is the size of the output of the hash function) after $k^2 = 2N\log(2)$ trials the probability of finding a collision is at least $1/2$. **(5p)**
   *(Hints: start by computing the probability of the complementary event, i.e., that after k trials one has found no collision. Towards the end, you can do the substitution* $k^2 \sim k(k-1)$*, to simplify computations. Additional useful bounds and formulas:* $\log(1-x) < -x$*,* $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$*.)*

## Advanced Topics in Cryptography (30p)

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

   (a) The structure of a $\Sigma$ (sigma) protocol. **(6p)**

   (b) The three main properties of a Secret Sharing Scheme, with threshold $t$. **(6p)**

9. Consider the Mignotte's Secret Sharing Scheme with the values $m_1 = 5, m_2 = 6, m_3 = 7, m_4 = 11, m_5 = 13$.

   (a) Imagine you are the Dealer and you want to share the value $s = 150$. Explain how you would compute the shares for each of the 5 parties, and compute the values $s_i$, for $i = 1, 2, 3, 4, 5$. **(6p)**

   (b) Now assume you hold the three shares $s_1 = 0$, $s_2 = 4$, $s_5 = 5$. You know that the shares have been generated using Mignotte's Secret Sharing Scheme with $m_1 = 5, m_2 = 6, m_3 = 7, m_4 = 11, m_5 = 13$. Can you reconstruct the secret value $s$? If so, compute it, otherwise explain why not. **(12p)**

   (c) *Bonus question: For what values of the threshold t, the given* $m_i$ *can be used? (2 bonus points)*