First name:_____ Last name:_____ ID number:_____

# Laurea Base and Laurea Magistrale in Informatica
# Information Systems and Network Security (2016-2017).
# Mid-term examination. November 9, 2016.

**In the following exercises on cryptography ignore punctuation marks and white spaces**

**Exercise 1:**

Encrypt the following message m by using a One-time pad with the specified key k (message and key are given in hexadecimal code).

m = F1 29 D1 k = A5 6B C4

**Exercise 2:**

Decrypt the following ciphertext c by assuming that it has been obtained by using a Cipher-block chaining (CBC) cipher with the specified IV, by supposing that each block is of 8 bits and that the block cipher encryption is a regular columnar transposition cipher with key: width=4 and permutation=4231. Notice that c and IV are already given in the binary code and just return the binary code of the plaintext.

c = 0011110011000011 IV = 10101010

**Exercise 3:**

Encrypt the message m = 75 by using RSA and the following parameters:

p = 11 q = 13 e = 19

**Exercise 4:**

Describe the encryption and decryption algorithms of the Feistel ciphers.

**Exercise 5:**

Describe the Diffie-Hellman cipher and how Diffie-Hellman allows two individuals to agree on a shared key, by using a public communication channel. Discuss about security of this cipher and also about the man-in-the-middle attack.