First name:________________ Last name:________________ ID number:________________

Laurea Magistrale in Informatica

Information Systems and Network Security (2017-2018).

Mid-term examination. November 8, 2017.

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

Exercise 1:

Decrypt the following ciphertext c obtained by using a triple irregular transposition cipher with keys k_1: width=4 and permutation=2413; k_2: width=9 and permutation=123987654; k_3: width=2 and permutation=21.

c = SDTIOIUAHMLWLEESOXTPKAE

Exercise 2:

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

m = B2 3C D1 k = 53 CB F4

Exercise 3:

Compute the CBC residue of the following message m with the specified IV (already given in binary code), by supposing that each block is of 8 bits and that the block cipher encryption is a Feistel cipher with 2 rounds, with keys k_0=0110, k_1=1100, and by supposing that the function F is the logical conjunction (AND). Just return the binary code.

m = 0111001111101100 IV= 11101110

Exercise 4:

Describe how to encrypt by using message digest (hash function).

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.