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

Laurea Magistrale in Informatica

Information Systems and Network Security (2019-2020).

Mid-term examination. November 6, 2019.

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

Exercise 1:

Encrypt the following plaintext m (that is a block of 12 bits) into the ciphertext (still in binary code) by using a Feistel Cipher with 3 rounds with the following keys and by supposing that the function F is the logical conjunction (AND).

m =101000111100 k_0=110110; k_1=111001; k_2=100100.

Exercise 2:

2.1) Decrypt the following ciphertext c (given in the binary code) by supposing that it has been obtained by using a Cipher-block chaining (CBC) cipher with the specified IV (given in the binary code), by supposing that each block is of 8 bits and that the block cipher encryption is a double irregular columnar transposition cipher with the following keys: k_1: width=5, permutation=53142 and k_2: width=3, permutation=231. Just return the binary code.

c = 0101010111001010 IV = 00110011

2.2) Encrypt the obtained plaintext (show the execution).

Exercise 3:

Consider the following parameters in the RSA cipher: p=5, q=17, e=5 (where e is the public key). Is d=13 a proper private key? Is d=19 a proper private key? Motivate your answers.

Exercise 4:

- Describe how to get authentication by using message digest (hash function).
- Describe how to encrypt and decrypt 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 the security of this cipher and finally show the man-in-the-middle attack.