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

Laurea Magistrale in Informatica

Information Systems and Network Security (2020-2021).

Mid-term examination. November 19, 2020.

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

Exercise 1:

Decrypt the following ciphertext c by supposing that it has been obtained by using a Vigenère cipher with the specified key.

c = RCXEGWOJPMWXRC k = TODBY

Exercise 2:

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 11 bits and that the block cipher encryption is a double irregular columnar transposition cipher with the following keys: k_1: width=3, permutation=312 and k_2: width=4, permutation=3241. Just return the binary code.

c = 01010101111000010101 IV = 00000111110

Exercise 3:

Consider the following parameters in the RSA cipher: p=7, q=13, e=7 (where e is the public key). Is d=27 a proper private key? Is d=31 a proper private key? Motivate your answers.