First name:_________________ Last name:_________________ ID number:_________________

Laurea Magistrale in Informatica

Information Systems and Network Security (2020-2021).

Full examination. January 25, 2021.

Part I:

Exercise 1:

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 a Feistel Cipher with one round with the following key k_0=0101, and by supposing that the function F is the logical conjunction (AND). Notice that c and IV are already given in the binary code and just return the binary code of the plaintext.

c = 1101101101101100 IV = 11001100

Exercise 2:

Describe how to get authentication by using public key and hash functions.

Part II:

Exercise 3:

Formally prove that *The Price of 1-envy-freeness for identical machines is at least min {n,m}-ε, for any (small) ε>0.*

Exercise 4:

Consider the following instance of the Item Pricing problem with 6 items and 4 buyers

\ Items **Buyers**	**1**	**2**	**3**	**4**	**5**	**6**
1	6	12	13	14	15	20
2	2	9	9	9	9	17
3	7	7	8	10	10	15
4	4	8	8	8	8	15

and show the execution of ALGORITHM1 just for the price *p=3*.