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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2016-2017).

# Full examination. September 4, 2017.

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

## Part I:

### Exercise 1:

Decrypt the following ciphertext c by assuming that it has been obtained by using an Output feedback (OFB) cipher with the specified IV, by supposing that each block is of 8 bits and that the block cipher encryption is a Feistel cipher with 2 rounds, with keys $k_0$=0011, $k_1$=1010, and by supposing that the function F is the logical disjunction (OR). Notice that c and IV are already given in the binary code and just return the binary code of the plaintext.

c = 0101110001010011 IV = 10011001

### Exercise 2:

Describe how encryption and decryption work in the Data Encryption Standard (DES) round. (Notice that you do NOT need to describe the generating round keys, that is suppose you already have the keys. Moreover, concerning the Mangler function, it is enough to say that it takes as input 32 bits of the data plus 48 bits of the key to produce a 32-bit output).

### Exercise 3:

Compute the Diffie-Hellman secret between Alice and Bob by using the following parameters:

p = 61 g = 21 $S_{Alice}$=5 $S_{Bob}$=7

## Part II:

### Exercise 1:

Return an optimal schedule for the following instance of the Scheduling identical Job SUM (minimization) problem with 4 machines and 10 jobs with the following processing times:

Processing times: $p_1$=2; $p_2$=4; $p_3$=6; $p_4$=3; $p_5$=5; $p_6$=2; $p_7$=9; $p_8$=13; $p_9$=15; $p_{10}$=1.

### Exercise 2:

Describe the Online Scheduling Identical Machine MAKESPAN (minimization) problem. Show the algorithm LIST that computes an approximated schedule and formally prove the performance of such an algorithm.

(It continues)

➡

**Exercise 3:**

Given the following instance of the 3-Envy-free Scheduling Identical Machine MAKESPAN (minimization) problem with 4 machines and 10 jobs (processing times are given below). Consider the following schedule S. Is S a 3-envy-free scheduling? Justify your answer.

*Jobs processing times:* $p_1=5$; $p_2=5$; $p_3=2$; $p_4=2$; $p_5=1$; $p_6=1$; $p_7=1$; $p_8=2$; $p_9=3$; $p_{10}=3$.

*The schedule S is:* $S_1=\{j_1; j_2\}$ $S_2=\{j_3; j_4\}$ $S_3=\{j_5; j_6; j_7\}$ $S_4=\{j_8; j_9; j_{10}\}$.

If S is not 3-envy-free then return a 3-envy-free scheduling S' whose MAKESPAN is at most 4/3 times the MAKESPAN of the scheduling S, by using the algorithm of theorem 9 (Recall *Theorem 9*: The *Price of k-envy-freeness for identical machines is at most* $1+1/k$, *for any* $k\geq2$).

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2016-2017).

# Full examination. June 20, 2017.

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

## Part I:

### Exercise 1:

Decrypt the following ciphertext c obtained by using a double irregular transposition ciphers with keys $k_1$: width=6 and permutation=235614; $k_2$: width=5 and permutation=23451;

c = IESTONUTGXIPOSY

### Exercise 2:

Encrypt the following plaintext m by using an Output feedback (OFB) cipher with the specified IV (already given in the binary code) by supposing that each block is of 8 bits and that the block cipher encryption is a Feistel ciphers with 2 rounds, with keys $k_0$=1010; $k_1$=0101, and by supposing that the function F is the logical conjunction (AND).

`m = AQ` IV= 10011001

### Exercise 3:

Describe strong authentication and show how it is possible with cryptography by using a secret key.

## Part II:

### Exercise 4:

Describe the Scheduling Unrelated Job SUM (minimization) problem with weights and one machine (m=1). Show a polynomial time algorithm that finds a schedule that minimizes the Job (weighted) SUM for the case where there is only one machine, and formally prove the performance (i.e., optimality) of such an algorithm.

Return an optimal schedule for the following instance with 10 jobs:

Processing times: $p_1$=2; $p_2$=3; $p_3$=4; $p_4$=6; $p_5$=1; $p_6$=7; $p_7$=1; $p_8$=8; $p_9$=5; $p_{10}$=5.

Weights: $w_1$=5; $w_2$=6; $w_3$=3; $w_4$=6; $w_5$=3; $w_6$=8; $w_7$=9; $w_8$=2; $w_9$=2; $w_{10}$=1.

### Exercise 5:

Formally prove that the *Price of k-envy-freeness for identical machines is at most 1+1/k, for any k≥2.*

First name:________________ Last name:_______________ ID student number:___________

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2018-2019).

# Full examination. June 17, 2019.

## Part I:

### Exercise 1:

Apply the Keystream generation (Pseudo-random generation algorithm - PRGA) of the RC4 cipher, by using 3 bits instead of 8 (8 instead of 256 symbols), to the following permutation S (that we suppose we have obtained by applying the Initialization (Key-scheduling algorithm - KSA) algorithm), by supposing that we want to encrypt the following message m:

S = [7 0 3 6 1 5 2 4]     m = [2 4 1]

### Exercise 2:

Encrypt the following plaintext m (given in the binary code) by using a Cipher-block chaining (CBC) cipher with the specified IV (given in the binary code) by supposing that each block is of 7 bits and that the block cipher encryption is a double irregular columnar transposition cipher with the following keys: $k_1$: width=4, permutation=3412 and $k_2$: width=3, permutation=213. Just return the binary code.

m = 11001011110100     IV = 0101110

### Exercise 3:

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.

**(Part II)**

➡

## Part II:

### Exercise 4:

Formally prove that *The Price of k-envy-freeness for unrelated machines is at most* $(1+1/k)^{min\{n,m\}-1}$ , *for any* $k \geq 1$.

### Exercise 5:

Consider the following instance of the Item Pricing problem with 7 items and 5 buyers

| \\<br>**Items**<br>**Buyers\** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|
| **1** | 3 | 8 | 10 | 11 | 16 | 17 | 20 |
| **2** | 2 | 8 | 8 | 12 | 14 | 15 | 19 |
| **3** | 6 | 7 | 8 | 11 | 14 | 15 | 15 |
| **4** | 4 | 7 | 9 | 10 | 11 | 12 | 13 |
| **5** | 1 | 6 | 7 | 8 | 9 | 10 | 10 |

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

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2016-2017).

# Full examination. July 18, 2017.

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

## 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 Feistel cipher with 2 rounds, with keys $k_0$=1011, $k_1$=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 = 1101110100110011 IV = 10110110

### Exercise 2:

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.

## Part II:

### Exercise 3:

Return an optimal schedule for the following instance of the Scheduling identical Job SUM (minimization) problem with 3 machines and 10 jobs with the following processing times:

Processing times: $p_1$=1; $p_2$=3; $p_3$=2; $p_4$=5; $p_5$=4; $p_6$=9; $p_7$=10; $p_8$=3; $p_9$=8; $p_{10}$=2.

### Exercise 4:

Formally prove that *The Price of k-envy-freeness for unrelated machines is at most* $(1+1/k)^{min\{n,m\}-1}$, *for any* $k\geq 1$.

(It continues)

➡

**Exercise 5:**

Consider an instance of the Item Pricing problem with 5 items and 5 buyers with the following buyers' valuations.

| \ Items<br>Buyers\ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1** | 2 | 6 | 8 | 10 | 12 |
| **2** | 4 | 7 | 8 | 10 | 13 |
| **3** | 3 | 6 | 8 | 11 | 14 |
| **4** | 4 | 7 | 8 | 11 | 14 |
| **5** | 5 | 5 | 8 | 10 | 11 |

Consider the following outcome $(X,p)$ : $X=<x_1,x_2,x_3,x_4,x_5> = <0,1,2,2,1>;$ $p=3$.

Is $(X,p)$ a nearly-feasible and envy-free outcome? Motivate your answer.

If $(X,p)$ is indeed a nearly-feasible and envy-free outcome then Apply Lemma A to it and return the corresponding outcome.

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2017-2018).

# Full examination. January 29, 2018.

## Part I:

### Exercise 1:

Apply the Initialization algorithm (Key-scheduling algorithm - KSA) of the RC4 cipher, by using 3 bits instead of 8 (8 instead of 256 symbols), and thus obtaining the permutation S[0] S[1]…..S[7], to the following Key = [4 1 5 1].

### 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 an irregular columnar transposition cipher with key: width=3 and permutation=231. Notice that c and IV are already given in the binary code and just return the binary code of the plaintext.

c = 1100001100111100 IV = 10100011

### Exercise 3:

Describe how encryption and decryption work in the Data Encryption Standard (DES) round. (Notice that you do NOT need to describe the generating round keys, that is suppose you already have the keys. Moreover, concerning the Mangler function, it is enough to say that it takes as input 32 bits of the data plus 48 bits of the key to produce a 32-bit output).

(Part II)

➡

## Part II:

### Exercise 1:

Consider the following schedule *S* for the Scheduling Unrelated Machine setting with 5 machines and 8 jobs with the following processing times:

| **M\J** | **$J_1$** | **$J_2$** | **$J_3$** | **$J_4$** | **$J_5$** | **$J_6$** | **$J_7$** | **$J_8$** |
|---|---|---|---|---|---|---|---|---|
| **$M_1$** | 2 | 1 | 2 | 1 | 2 | 1 | 1 | 2 |
| **$M_2$** | 2 | 2 | 8 | 1 | 3 | 3 | 1 | 4 |
| **$M_3$** | 2 | 1 | 2 | 2 | 3 | 1 | 2 | 2 |
| **$M_4$** | 1 | 2 | 2 | 3 | 4 | 3 | 4 | 3 |
| **$M_5$** | 2 | 1 | 2 | 1 | 2 | 1 | 4 | 4 |

The schedule is: $S_1=\{j_1;j_2\}$ $S_2=\{j_3\}$ $S_3=\{j_4;j_5\}$ $S_4=\{j_6;j_7\}$ $S_5=\{j_8\}$

- Is *S* a 2-envy free schedule? Justify your answer.
- Is *S* a 3-envy free schedule? Justify your answer.
- If S is not 2-envy-free then return a 2-envy-free scheduling S' whose MAKESPAN is at most $(3/2)^4$ times the MAKESPAN of scheduling S, by using Theorem 11.

### Exercise 2:

Show ALGORITHM1 in the setting of the pricing problem and formally prove that it has approximation ratio $min\{1/2;1/H_n\}$ (i.e., Theorem 13).

First name:__________________ Last name:__________________ ID number:__________________

# Laurea Magistrale in Informatica
# Information Systems and Network Security (2016-2017).
# Second Mid-term + full examination. January 25, 2017.

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

## Part I:

### Exercise 1:

Decrypt the following ciphertext c obtained by using a double irregular transposition ciphers with keys $k_1$: width=5 and permutation=35241; $k_2$: width=9 and permutation=987612345;

c = TIANLTNYSEUAADOMRXIASETOENX

### Exercise 2:

Compute the CBC residue of the following message m with the specified key k and IV (already given in the ascii code), by supposing that each block is of 8 bits and that the block cipher encryption just XOR the input with k.

m = MAN  k = 10010010  IV= 00100101

### Exercise 3:

Describe the Output feedback (OFB) block cipher (encryption and decryption) and also highlight pros and cons (advantages and disadvantages) of such cipher.

### Exercise 4:

Describe the Man-in-the-Middle attack in the Diffie-Hellman cipher setting.

## Part II:

### Exercise 1:

Describe the Scheduling Unrelated Job SUM (minimization) problem without weights with one machine (m=1). Show a polynomial time algorithm that finds a schedule that minimizes the Job SUM and formally prove the performance (i.e., optimality) of such an algorithm.
Return an optimal schedule for the following instance with 7 jobs:

Processing times: $p_1=6$; $p_2=2$; $p_3=4$; $p_4=3$; $p_5=1$; $p_6=1$; $p_7=5$.

### Exercise 2:

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 3:

Consider the following instance of the Item Pricing problem with 4 items and 3 buyers and the following buyers' valuations:

| \ Items<br>Buyers\ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| **1** | 2 | 3 | 4 | 5 |
| **2** | 2 | 2 | 3 | 4 |
| **3** | 1 | 2 | 3 | 6 |

In the following questions if at least one property is not satisfied then just answer "no" by showing which property is not satisfied.

a) Is the following output a feasible and envy-free outcome? $X=<x_1,x_2, x_3>= <1,1,1>;$ $p$=2.

b) Is the following output a feasible and envy-free outcome? $X=<x_1,x_2, x_3>= <2,1,1>;$ $p$=1.

c) Is the following output a feasible and envy-free outcome? $X=<x_1,x_2, x_3>= <3,0,1>;$ $p$=1.

## Exercise 4:

Consider the following instance of the Item Pricing problem with 4 items and 4 buyers and the following buyers' valuations.

| \ Items<br>Buyers\ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| **1** | 4 | 6 | 6 | 8 |
| **2** | 2 | 4 | 6 | 6 |
| **3** | 3 | 5 | 7 | 7 |
| **4** | 2 | 4 | 6 | 6 |

Consider the following outcome ($X$,$p$) : $X=<x_1,x_2,x_3,x_4>= <1,2,2,0>;$ $p$=2.

Is ($X$,$p$) a nearly-feasible and envy-free outcome? Motivate your answer.

If ($X$,$p$) is indeed a nearly-feasible and envy-free outcome then Apply Lemma A to it and return the corresponding outcome.

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2019-2020).

# Full examination. January 20, 2020.

## Part I:

### Exercise 1:

Apply the Keystream generation (Pseudo-random generation algorithm - PRGA) of the RC4 cipher, by using 3 bits instead of 8 (8 instead of 256 symbols), to the following permutation S (that we suppose we have obtained by applying the Initialization (Key-scheduling algorithm - KSA) algorithm), by supposing that we want to encrypt the following message m:

S = [6 2 0 1 4 7 5 3] m = [1 2 3]

### 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 7 bits and that the block cipher encryption is a double irregular columnar transposition cipher with the following keys: $k_1$: width=5, permutation=52143, and $k_2$: width=3, permutation=231. Notice that c and IV are already given in the binary code and just return the binary code of the plaintext.

c = 10110110110110 IV = 1100110

### Exercise 3:

Describe how encryption and decryption work in the Data Encryption Standard (DES) round. (Notice that you do NOT need to describe the generating round keys, that is suppose you already have the keys).

**(Part II)**

➡

## Part II:

### Exercise 4:

Return an optimal schedule for the following instance of the Scheduling identical Job SUM (minimization) problem with 3 machines and 10 jobs with the following processing times:

Processing times: $p_1=4$; $p_2=2$; $p_3=3$; $p_4=3$; $p_5=1$; $p_6=9$; $p_7=5$; $p_8=4$; $p_9=10$; $p_{10}=2$.

### Exercise 5:

Formally prove that *The Price of k-envy-freeness for identical machines is at least 1 + 1/k - ε, for any (small) ε>0, and for any k≥2.*

### Exercise 6:

Consider the following instance of the Item Pricing problem with 7 items and 5 buyers

| **\ Items**<br>**Buyers\** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|
| **1** | 6 | 8 | 13 | 16 | 20 | 24 | 28 |
| **2** | 8 | 9 | 12 | 14 | 17 | 22 | 25 |
| **3** | 6 | 9 | 14 | 15 | 16 | 17 | 18 |
| **4** | 4 | 10 | 15 | 18 | 18 | 25 | 25 |
| **5** | 5 | 9 | 12 | 14 | 19 | 19 | 26 |

and show the execution of ALGORITHM1 just for the price *p=4.*

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2017-2018).

# Full examination. January 15, 2018.

## Part I:

### Exercise 1:

Describe how to get *authentication* by using public key and secret key.

### Exercise 2:

Decrypt the following ciphertext c by assuming that it has been obtained by using an Output feedback (OFB) cipher with the specified IV, by supposing that each block is of 4 bits and that the block cipher encryption is a Feistel cipher with 2 rounds, with keys $k_0$=01, $k_1$=10, 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 = 101101001100 IV = 1001

### Exercise 3:

Encode the message `m = 19` by using RSA and the following parameters:

`p = 17` `q = 7` `e = 37`

## Part II:

### Exercise 1:

Describe the Scheduling Unrelated Job SUM (minimization) problem with weights and one machine (m=1). Show a polynomial time algorithm that finds a schedule that minimizes the Job (weighted) SUM for the case where there is only one machine, and formally prove the performance (i.e., optimality) of such an algorithm.

### Exercise 2:

Given the following instance of the 2-Envy-free Scheduling Identical Machine MAKESPAN (minimization) problem with 6 machines and 11 jobs. Consider the following schedule S.
Is S a 2-envy-free scheduling? Justify your answer.

*Jobs processing times:* $p_1=2; p_2=2; p_3=2; p_4=2; p_5=2; p_6=3; p_7=3; p_8=4; p_9=4; p_{10}=4; p_{11}=5$

*The schedule S is:* $S_1=\{j_1; j_2\}$ $S_2=\{j_3; j_4\}$ $S_3=\{j_5; j_6; j_7\}$ $S_4=\{j_8\}$ $S_5=\{j_9\}$ $S_6=\{j_{10}; j_{11}\}$

If S is not 2-envy-free then return a 2-envy-free scheduling S' whose MAKESPAN is at most 3/2 times the MAKESPAN of the scheduling S, by using the algorithm of theorem 9 (Recall *Theorem 9*: The *Price of k-envy-freeness for identical machines is at most $1+1/k$, for any $k \geq 2$*).

(It continues)

➡

### Exercise 3:

Consider the following instance of the Item Pricing problem with 5 items and 5 buyers

| \ Items<br>Buyers\ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1** | 5 | 6 | 9 | 10 | 14 |
| **2** | 5 | 6 | 8 | 11 | 11 |
| **3** | 10 | 10 | 10 | 14 | 15 |
| **4** | 3 | 7 | 9 | 11 | 12 |
| **5** | 2 | 5 | 8 | 11 | 12 |

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

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2018-2019).

# Full examination. January 14, 2019.

## Part I:

### Exercise 1:

Apply the Keystream generation (Pseudo-random generation algorithm - PRGA) of the RC4 cipher, by using 3 bits instead of 8 (8 instead of 256 symbols), to the following permutation S (that we suppose we have obtained by applying the Initialization (Key-scheduling algorithm - KSA) algorithm), by supposing that we want to encrypt the following message m:

S = [2 0 6 3 4 5 7 1]  m = [3 2 5]

### Exercise 2:

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 7 bits and that the block cipher encryption is a double irregular columnar transposition cipher with keys: $k_1$: width=4, permutation=3421 and $k_2$: width=3, permutation=231. Just return the binary code.

m = 11001100011001  IV= 1000111

### Exercise 3:

Describe how encryption and decryption work in the Data Encryption Standard (DES) round. (Notice that you do NOT need to describe the generating round keys, that is suppose you already have the keys).

**(Part II)**

➡

**Part II:**

**Exercise 4:**

Formally prove that *The Price of k-envy-freeness for identical machines is at most 1+1/k, for any k≥2.*

**Exercise 5:**

Consider an instance of the Item Pricing problem with 7 items and 5 buyers with the following buyers' valuations.

| \ Items<br>Buyers\ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| **1** | 2 | 4 | 6 | 8 | 9 | 12 | 15 |
| **2** | 3 | 5 | 7 | 8 | 10 | 11 | 14 |
| **3** | 3 | 5 | 7 | 10 | 11 | 12 | 13 |
| **4** | 3 | 7 | 8 | 10 | 12 | 12 | 12 |
| **5** | 3 | 5 | 7 | 9 | 9 | 10 | 10 |

a) Consider the following outcome $(X,p)$ : $X=<x_1,x_2,x_3,x_4,x_5> = <0,1,2,3,4>;$ $p=2$.

- Is $(X,p)$ a nearly-feasible and envy-free outcome? Motivate your answer.
- If $(X,p)$ is indeed a nearly-feasible and envy-free outcome then Apply Lemma A to it and return the corresponding outcome.

b) Consider the following outcome $(X,p)$ : $X=<x_1,x_2,x_3,x_4,x_5> = <1,1,1,2,3>;$ $p=2$.

- Is $(X,p)$ a nearly-feasible and envy-free outcome? Motivate your answer.
- If $(X,p)$ is indeed a nearly-feasible and envy-free outcome then Apply Lemma A to it and return the corresponding outcome.

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2016-2017).

# Second Mid-term + full examination.  January 11, 2017.

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

## Part I:

### Exercise 1:

Apply the Initialization algorithm (Key-scheduling algorithm - KSA) of the RC4 cipher, by using 3 bits instead of 8 (8 instead of 256 symbols), and thus obtaining the permutation S[0] S[1]…..S[7], to the following   Key = [3 4 2 5].

### Exercise 2:

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 =101101110111.     $k_0$=111010;   $k_1$=010111;   $k_2$=111001.

### Exercise 3:

Describe strong authentication and show how it is possible with cryptography by using a secret key.

### Exercise 4:

Describe how to get authentication by using message digests (hash functions).

## Part II:

### Exercise 1:

Describe the Scheduling Unrelated Job SUM (minimization) problem with weights and one machine (m=1). Show a polynomial time algorithm that finds a schedule that minimizes the Job (weighted) SUM for the case where there is only one machine, and formally prove the performance (i.e., optimality) of such an algorithm.

Return an optimal schedule for the following instance with 10 jobs:

Processing times: $p_1$=5;  $p_2$=3;  $p_3$=6;  $p_4$=7;  $p_5$=1;  $p_6$=2;  $p_7$=3;  $p_8$=7;  $p_9$=7; $p_{10}$=2.

Weights: $w_1$=2; $w_2$=6; $w_3$=2; $w_4$=4; $w_5$=3; $w_6$=8; $w_7$=9; $w_8$=2; $w_9$=6; $w_{10}$=7.

**Exercise 2:**

Formally prove that The *Price of k-envy-freeness* for identical machines is at most *min {n,m}*, *for any k≥1.*

**Exercise 3:**

Given the following instance of the k-Envy-free Scheduling Identical Machine MAKESPAN (minimization) problem with 6 machines and 11 jobs (processing times are given below). Consider the following schedule S. Is S a 2-envy-free scheduling? Justify your answer.

*Jobs processing times:* $p_1=1; p_2=1; p_3=1; p_4=1; p_5=1; p_6=2; p_7=4; p_8=5; p_9=6; p_{10}=7; p_{11}=8.$

*The schedule S is:* $S_1= \{j_1\}$ $S_2=\{ j_2; j_3\}$ $S_3=\{ j_4; j_5; j_6\}$ $S_4=\{ j_7; j_8\}$ $S_5=\{ j_9\}$ $S_6=\{ j_{10}; j_{11}\}$.

If S is not 2-envy-free then return a 2-envy-free scheduling S' whose MAKESPAN is at most 3/2 times the MAKESPAN of the scheduling S, by using the algorithm of theorem 9 (Recall *Theorem 9*: The *Price of k-envy-freeness for identical machines is at most 1+1/k, for any k≥2.*).

**Exercise 4:**

Consider the following instance of the Item Pricing problem with 4 items and 3 buyers and the following buyers' valuations:

| **\ Items**<br>**Buyers\** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| **1** | 2 | 2 | 2 | 3 |
| **2** | 3 | 5 | 5 | 5 |
| **3** | 1 | 3 | 5 | 5 |

In the following questions if at least one property is not satisfied then just answer "no" by showing which property is not satisfied.

a) Is the following output a feasible and envy-free outcome? $X=<x_1,x_2, x_3>= <0,2,2>;$ $p=2$.

b) Is the following output a feasible and envy-free outcome? $X=<x_1,x_2, x_3>= <1,2,1>;$ $p=1$.

c) Is the following output a feasible and envy-free outcome? $X=<x_1,x_2, x_3>= <1,2,2>;$ $p=1$.

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

## Laurea Magistrale in Informatica

## Information Systems and Network Security (2017-2018).

## Full examination. February 12, 2018.

### Part I:

### Exercise 1:

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 5 bits and that the block cipher encryption is an irregular columnar transposition cipher with key: width=2 and permutation=21. Just return the binary code.

m = 001101100100011 IV= 10101

### Exercise 2:

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 disjunction (OR).

m =010010001101. $k_0$=101010; $k_1$=010010; $k_2$=110101.

### Exercise 3:

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.

(Part II)

➡

## Part II:

### Exercise 1:

Describe the Online Scheduling Identical Machine MAKESPAN (minimization) problem. Show the algorithm LIST that computes an approximated schedule and formally prove the performance of such an algorithm.

### Exercise 2:

Formally prove that *The Price of k-envy-freeness for identical machines is at most min{n,m}, for any* $k\geq 1$.

### Exercise 3:

Consider an instance of the Item Pricing problem with 7 items and 6 buyers with the following buyers' valuations.

| \Items<br>Buyers\ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| **1** | 4 | 8 | 9 | 10 | 12 | 13 | 14 |
| **2** | 3 | 8 | 9 | 10 | 12 | 12 | 12 |
| **3** | 2 | 9 | 12 | 11 | 13 | 15 | 19 |
| **4** | 5 | 8 | 9 | 11 | 11 | 11 | 11 |
| **5** | 3 | 6 | 9 | 10 | 10 | 12 | 14 |
| **6** | 1 | 7 | 10 | 11 | 15 | 16 | 16 |

Consider the following outcome $(X,p)$ : $X=<x_1,x_2,x_3,x_4,x_5,x_6> = <2,2,3,1,0,2>;$ $p$=3.

Is $(X,p)$ a nearly-feasible and envy-free outcome? Motivate your answer.

If $(X,p)$ is indeed a nearly-feasible and envy-free outcome then Apply Lemma A to it and return the corresponding outcome.

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2016-2017).

# Second Mid-term + full examination. February 8, 2017.

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

## Part I:

### Exercise 1:

Apply the Keystream generation (Pseudo-random generation algorithm - PRGA) of the RC4 cipher, by using 3 bits instead of 8 (8 instead of 256 symbols), to the following permutation S (that we suppose we have obtained by applying the Initialization (Key-scheduling algorithm - KSA) algorithm), by supposing that we want to encrypt the following message m:

S = [6 3 2 0 1 7 5 4]  m = [6 3 2]

.

### Exercise 2:

Encrypt the following message m by using the Output feedback (OFB) cipher with the specified key k and IV (already given in the binary ASCII code), by supposing that each block is of 8 bits and that the block cipher encryption just XOR the input with k.

m = HI  k = 00100101  IV= 01100110

### Exercise 3:

Describe how encryption and decryption work in the Data Encryption Standard (DES) round. (Notice that you do NOT need to describe the generating round keys, that is suppose you already have the keys).

## Part II:

### Exercise 1:

Return an optimal schedule for the following instance of the Scheduling identical Job SUM (minimization) problem with 4 machines and 11 jobs with the following processing times:

Processing times: $p_1$=1; $p_2$=3; $p_3$=2; $p_4$=5; $p_5$=7; $p_6$=6; $p_7$=9; $p_8$=8; $p_9$=10; $p_{10}$=11; $p_{11}$=4.

### Exercise 2:

Describe the Online Scheduling Identical Machine MAKESPAN (minimization) problem. Show the algorithm LIST that computes an approximated schedule and formally prove the performance of such an algorithm.

## Exercise 3:

Define the k-Envy-free Scheduling Unrelated Machine MAKESPAN (minimization) problem.

Consider the following schedule *S* for the Scheduling Unrelated Machine setting with 3 machines and 5 jobs with the following processing times:

| **M\J** | **$J_1$** | **$J_2$** | **$J_3$** | **$J_4$** | **$J_5$** |
|---|---|---|---|---|---|
| **$M_1$** | 3 | 5 | 5 | 3 | 1 |
| **$M_2$** | 2 | 4 | 8 | 4 | 2 |
| **$M_3$** | 2 | 4 | 5 | 5 | 6 |

The schedule is: $S_1=\{j_1; j_2\}$ $S_2=\{ j_3\}$ $S_3=\{j_4; j_5\}$

Is *S* a 2-envy free schedule? Justify your answer.

Is *S* a 3-envy free schedule? Justify your answer.

## Exercise 4:

Consider an instance of the Item Pricing problem with 5 items and 6 buyers with the following buyers' valuations.

| **\ Items**<br>**Buyers** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|
| **1** | 2 | 4 | 4 | 6 | 7 |
| **2** | 3 | 5 | 5 | 6 | 8 |
| **3** | 3 | 5 | 5 | 6 | 6 |
| **4** | 2 | 2 | 3 | 6 | 7 |
| **5** | 2 | 4 | 4 | 6 | 7 |
| **6** | 2 | 4 | 5 | 6 | 8 |

Consider the following outcome $(X,p)$ : $X=<x_1,x_2,x_3,x_4,x_5,x_6> = <0,1,1,0,2,2>;$ $p$=2.

Is $(X,p)$ a nearly-feasible and envy-free outcome? Motivate your answer.

If $(X,p)$ is indeed a nearly-feasible and envy-free outcome then Apply Lemma A to it and return the corresponding outcome.

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

# Laurea Magistrale in Informatica

# Information Systems and Network Security (2019-2020).

# Full examination. February 3, 2020.

## Part I:

### Exercise 1:

Apply the Initialization algorithm (Key-scheduling algorithm - KSA) of the RC4 cipher, by using 3 bits instead of 8 (8 instead of 256 symbols), and thus obtaining the permutation S[0] S[1]…..S[7], to the following Key = [3 1 5 2 6].

### Exercise 2:

Encrypt the following plaintext m by using an Output feedback (OFB) 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 Feistel cipher with 2 rounds, with keys $k_0$=0101, $k_1$=1000, and by supposing that the function F is the logical disjunction (OR). Just return the binary code of the ciphertext.

m = 0010011010010011 IV = 01001110

### Exercise 3:

Describe how to get *authentication* by using public key and secret key.

**(Part II)**

➡

## Part II:

### Exercise 4:

Describe the Online Scheduling Identical Machine MAKESPAN (minimization) problem. Show the algorithm LIST that computes an approximated schedule and formally prove the performance of such an algorithm.

### Exercise 5:

Given the following instance of the 4-Envy-free Scheduling Identical Machine MAKESPAN (minimization) problem with 7 machines and 13 jobs (processing times are given below). Consider the following schedule S. Is S a 4-envy-free scheduling? Justify your answer.

*Jobs processing times:* $p_1=1;\ p_2=2;\ p_3=1;\ p_4=1;\ p_5=1;\ p_6=2;\ p_7=4;\ p_8=4;\ p_9=6;\ p_{10}=7;\ p_{11}=5;\ p_{12}=1;\ p_{13}=3.$

*The schedule S is:* $S_1=\{j_1\}\ \ S_2=\{j_2; j_3\}\ \ S_3=\{j_4; j_5; j_6\}\ \ S_4=\{j_7; j_8\}\ \ S_5=\{j_9\}\ \ S_6=\{j_{10}; j_{11}\}\ \ S_7=\{j_{12}; j_{13}\}.$

If S is not 4-envy-free then return a 4-envy-free scheduling S' whose MAKESPAN is at most 5/4 times the MAKESPAN of the scheduling S, by using the algorithm of Theorem 9 (Recall *Theorem 9*: The *Price of k-envy-freeness for identical machines is at most* $1+1/k$, *for any* $k\geq 2$.).

### Exercise 6:

Consider an instance of the Item Pricing problem with 7 items and 5 buyers with the following buyers' valuations.

| **\ Items**<br>**Buyers\** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|
| **1** | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| **2** | 5 | 7 | 8 | 9 | 10 | 10 | 10 |
| **3** | 3 | 7 | 10 | 12 | 15 | 15 | 15 |
| **4** | 3 | 5 | 7 | 11 | 11 | 13 | 13 |
| **5** | 3 | 3 | 7 | 8 | 10 | 10 | 11 |

Consider the following outcome $(X,p)$ : $X=<x_1,x_2,x_3,x_4,x_5> = <1,2,3,4,1>;$ $p$=2.

Is $(X,p)$ a nearly-feasible and envy-free outcome? Motivate your answer.

If $(X,p)$ is indeed a nearly-feasible and envy-free outcome then Apply Lemma A to it and return the corresponding outcome.