University of M'sila
Faculty of MI
Department of Computer Science

TD No. 01

Level: 3rd year Bachelor's degree

Course: Computer Security

Exercise 01: QCM

1. Which of the following best describes the CIA triad?
   a. Confidentiality, Integrity, Availability
   b. Control, Isolation, Authentication
   c. Confidentiality, Identification, Authorization
   d. Consistency, Integrity, Accountability
2. Authentication is the process of :
   a. Determining the actions of the user
   b. Verifying the identity of a user
   c. Encrypting data before transmission
   d. Monitoring system activity
3. Which of the following attacks target availability?
   a. Identity theft
   b. Denial of service
   c. Journal modification
   d. Bombardment and saturation of the network
4. Which statement is correct?
   a. Security failures are always accidental
   b. Safety considers malicious behavior
   c. Security focuses on intentional attacks
   d. Safety and security are identical concepts
5. Which statement is correct?:
   a. A threat is the same as a risk
   b. Risk exists only if an attack has occurred
   c. A threat exploits a vulnerability to create risk
   d. Risk depends only on system vulnerabilities
6. The primary goal of physical security is to:
   a. Protect data confidentiality
   b. Prevent unauthorized physical access and damage
   c. Detect malware infections
   d. Ensure software correctness
7. Information integrity means that data:
   a. Is encrypted
   b. Is always available
   c. Has not been altered without authorization
   d. Is stored securely
8. Which of the following best defines an active attack?
   a. Monitoring network traffic
   b. Reading sensitive files
   c. Altering data or system behavior
   d. Collecting metadata
9. Which is an example of an operational security control?
   a. Firewalls
   b. Encryption algorithms
   c. Change management procedures
   d. Secure boot
10. Which is an example of a passive attack?
    a. A. Denial-of-service attack
    b. Man-in-the-middle altering messages
    c. Eavesdropping on network traffic
    d. SQL injection
11. Which of the following is an example of a logical security failure?
    a. Server room fire
    b. Hard disk theft
    c. Weak password policy
    d. Power outage
12. Which dimension is not part of the IT security architecture?
    a. Technical dimension
    b. Monetary dimension
    c. Organizational dimension
    d. Legal dimension

Exercise 02:

ISIL

1. Explain the difference between identification and authentication.
2. What is the relationship between: authentication, integrity, and non-repudiation?
3. Give examples of attackers in the real world.
4. Why are hackers interested in corporate information systems?
5. What is the difference between computer security and cybersecurity?

SI

Correction

Exercise 1:

13. Which of the following best describes the CIA triad?
    a. Confidentiality, Integrity, Availability
    b. Control, Isolation, Authentication
    c. Confidentiality, Identification, Authorization
    d. Consistency, Integrity, Accountability
14. Authentication is the process of :
    a. Determining the actions of the user
    b. Verifying the identity of a user
    c. Encrypting data before transmission
    d. Monitoring system activity
15. Which of the following attacks target availability?
    a. Identity theft
    b. Denial of service
    c. Journal modification
    d. Bombardment and saturation of the network
16. Which statement is correct?
    a. Security failures are always accidental
    b. Safety considers malicious behavior
    c. Security focuses on intentional attacks
    d. Safety and security are identical concepts
17. Which statement is correct?
    a. A threat is the same as a risk
    b. Risk exists only if an attack has occurred
    c. A threat exploits a vulnerability to create risk
    d. Risk depends only on system vulnerabilities
18. The primary goal of physical security is to:
    a. Protect data confidentiality
    b. Prevent unauthorized physical access and damage
    c. Detect malware infections
    d. Ensure software correctness
19. Information integrity means that data:
    a. Is encrypted
    b. Is always available
    c. Has not been altered without authorization
    d. Is stored securely
20. Which of the following best defines an active attack?
    a. Monitoring network traffic
    b. Reading sensitive files
    c. Altering data or system behavior
    d. Collecting metadata
21. Which is an example of an operational security control?
    a. Firewalls
    b. Encryption algorithms
    c. Change management procedures
    d. Secure boot
22. Which is an example of a passive attack?
    a. A. Denial-of-service attack
    b. Man-in-the-middle altering messages
    c. Eavesdropping on network traffic
    d. SQL injection
23. Which of the following is an example of a logical security failure?
    a. Server room fire
    b. Hard disk theft
    c. Weak password policy
    d. Power outage
24. Which dimension is not part of the IT security architecture?
    e. Technical dimension
    f. Monetary dimension
    g. Organizational dimension
    h. Legal dimension

Exercise 2:

1. ***Explain the difference between identification and authentication.***
   Identification = knowing the identity of an entity (who I am).
   Authentication = proving the identity of an entity

2. ***What is the relationship between: authentication, integrity, and non-repudiation?***
   The relationship is one of inclusion: integrity ⊂ authentication ⊂ non-repudiation.

3. ***Give examples of attackers in the real world.***
    - A government
    - A criminal or a terrorist
    - Industrial or commercial spy (competitor) Howawi Samsung
    - Internal employee

4. ***Why are hackers interested in corporate information systems?***
    - Financial gains: access to information, then monetization and resale (customer files, user files, emails, passwords, etc.)
    - Resource usage: bandwidth and storage space, Zombies (botnets).
    - Blackmail: preventing access to resources
    - Gathering information on the system: industrial/competitive, state espionage.

5. ***What is the difference between computer security and cybersecurity?***
    - Computer security concerns all computer systems, whether or not they are connected to the internet or networks.
    - Cybersecurity concerns computer systems connected to the internet or networks.

University of M'sila
Faculty of MI
Computer Science Department
Level: 3rd year Bachelor's degree **Course:** ***Computer Security***

TD N°02

Classical Cryptography

Exercise No. 01:

1. Find the coefficients *u* , *v* and the *GCD* of the following integers:
   - (a, b) = (60, 19)

     60 = 19 * 3 + 3 ➔3 = 60 - 19 * 3

     19 = 3*6 + 1 ➔1 = 19 - 3*6 = 19 - (60 - 19*3)*6

     1 = 19*19 – 60*6

     u=-6, v=19, GCD=1
   - (a, b) = (280, 11)

     u=-2, v=51, GCD=1
   - (a, b) = (38, 26)

   u=-2, v=3, GCD=2
2. Calculate the inverse of:
   - $41^{-1} \bmod 53$.

   To calculate the modular inverse of 41 mod 53, we use the extended Eclude algorithm to find the GCD(53,41) and the coefficient v. The condition is GCD=1

$$\underbrace{(53)}_{A} \times \underbrace{-17}_{u} + \underbrace{(41)}_{B} \times \underbrace{22}_{v} = \underbrace{1}_{\text{PGCD}(A,B)}$$

   v=22, then $41^{-1} \bmod 53 = 22$

   - $317^{-1} \bmod 521$

$$\underbrace{(521)}_{A} \times \underbrace{-101}_{u} + \underbrace{(317)}_{B} \times \underbrace{166}_{v} = \underbrace{1}_{\text{PGCD}(A,B)}$$

   v=166, then $317^{-1} \bmod 521=166$
   - $24\text{-}1^{\text{mod}}512$

$$\underbrace{(512)}_{A} \times \underbrace{1}_{u} + \underbrace{(24)}_{B} \times \underbrace{-21}_{v} = \underbrace{8}_{\text{PGCD}(A,B)}$$

GCD(512,24)=8 ≠ 1. Therefore, there is no

Exercise No. 2: (*Shift cipher*)

1. Write a pseudo-code for encrypting/decrypting a text using Caesar.

Encryption:

```
char indtolettre (int ind)
int j=0;
while j<26
{ if j == ind
return alpha[j] j
else j++
}

int lettretoind (char lettre)
int j=0;
while j<26
{ if t[j] == letter
return j
   else j++
}

%Encryption
char p[], c[], k
char alph[] = {'A','B','C', …., 'Z'} % alphabet array
int l, I, k1
l = length(p);
k1 = lettertoind (k)
for (i:=0; i< l; i=i+1 )
c[i]= indtoletter ( lettertoind (p[i]) + k1 % 26)

% Decryption:
l = length(p);
k1 = lettertoind (k)
for (i:=0; i< l; i=i+1 )
p[i]= indtoletter ( lettertoind (p[i]) – k1 + 26 % 26)
```

2. Prove that $D_k(E_k(m))=m$.

   Let $c=E_k(m)= m + k \bmod 26$ and $m=D_k(c)= c – k \bmod 26$

   $D_k(E_k(m))= D_k(m + k \bmod 26)= (m + k \bmod 26) – k \bmod 26$

   $= m$

3. Encrypt the text "CRYPTOGRAPHY" with the key **K.**

   We apply the encryption function $E_k(m)= m + k \bmod 26$ where k= 10

Plain text	C	R	Y	P	T	O
Clue. Clear	2	17	24	15	19	14
Key	K	K	K	K	K	K
Clue. Key	10	10	10	10	10	10
Ind. Chiff	12	1	8	25	3	24
Encrypted text	M	B	I	Z	D	Y

E_k(CRYPTOGRAPHY)= MBIZDYQBKZRSO

4. Decrypt the text "JSHZZPXBL" using the key **H.**

We apply the decryption function $D_k(c)= c – k \bmod 26$ where k= 7
(In the table, encrypt only the word "ENCRYPT")
D_k(JSHZZPXBL)= CLASSIC

Exercise No. 4: (*Vigenère cipher*)

1. Write a pseudo-code for encrypting/decrypting a text using Vigenère.

```
Input: char p[], chair k[]
Output: chair c[]

l = length(cle)
For i=0 to length(p)-1
    c[i]= indtoletter(lettertoind(p[i]) + lettertoind(k[i%lc]) % 26)
```

2. Encrypt the text "CRYPTOGRAPHY" with the key "SECRET".
   The encryption function is applied. $E_k(x_1, x_2, \ldots, x_n) = (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n)$
   E_k(CRYPTOGRAPHY)= UVAGXHYVCGLBW
3. Decipher the text "ORABCNDIBDIVD" using the key "KEY":
   The decryption function is applied. $D_k(y_1, y_2, \ldots, y_n) = (y_1 – k_1, y_2 – k_2, \ldots, y_n – k_n)$
   D_k(ORABCNDIBDIVD)=ENCRYPTEDTEXT

Exercise No. 5: (*Affine Cipher*)

Let K = (5,11)

1. Prove that $D_k(E_k(m))=m$

- $E_k(x) = ax + b \bmod 26$
- $D_k(y) = a^{-1}. (yb) \bmod 26$

$D_k(y) = a^{-1}. (yb) \bmod 26 = a^{-1}. (ax + b -b) \bmod 26$
$= a^{-1}. ax \bmod 26$
$= x$

2. Calculate the encryption and decryption functions,

Let K=(5,11)

$E_k(x) = 5x + 11 \bmod 26$
We calculate $5^{-1} \bmod 26$
$26 = 5 * 5 + 1 \Rightarrow 1 = 26 – 5*5$
$5^{-1} \bmod 26 = -5 = -5 + 26 = 21$
Then $D_k(y) = 21(y-11) \bmod 26 = 21y – 21*11 \bmod 26 = 21y – 23 \bmod 26 = (21y + 3 \bmod 26)$

3. Encrypt the following word: "AFFINE"

Use a table like in exercise 2 and apply the function $E_k(x) = 5x + 11 \bmod 26$

The encrypted text is: LKKZYF

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exercise No. 5: (*Transposition Cipher*)

The password is "SAMI"

1. Encrypt the text " COMPUTER SCIENCE "
2. Decipher the text "YEMSRQITEXXU"

1. Encryption:

S	A	M	I
4	1	3	2
I	N	F	O
R	M	A	T
I	Q	U	E

A	I	M	S
1	2	3	4
N	O	F	I
M	T	A	R
Q	E	U	I

Encrypted text: NOFIMTARQEUI

2. Decrpting

A	I	M	S
1	2	3	4
Y	E	M	S
R	Q	I	T
E	X	X	U

S	A	M	I
4	1	3	2
S	Y	M	E
T	R	I	Q
U	E	X	X

Plain text: Symmetrique

Exercise 6:

Without knowing the key, decrypt the first 9 letters of the following message using the shift algorithm.

ATKGIZOUTSGRBKORRGTZKWAOIUSVXUSKZRGYKIAXOZKJKYJUTTKKYUAYEYZKSKYJOTLUXSGZOWAK

We use frequency analysis, the most frequent letter in the ciphertext is K(10), and the most frequent letter in the French text is E(4).

c= m + K mod 26 ➔k = c – m mode 26 ➔k = 10 – 4 =6

The decryption function is: m = c – 6 mod 26

So, the first 9 letters of the plain text are: **AN ACTION**

University of M'sila
Faculty of MI
Department of Computer Science

TD N° 03

Level: 3rd year Bachelor's degree

Course: Computer Security

Exercise N° 01: *diagram of Feistel*

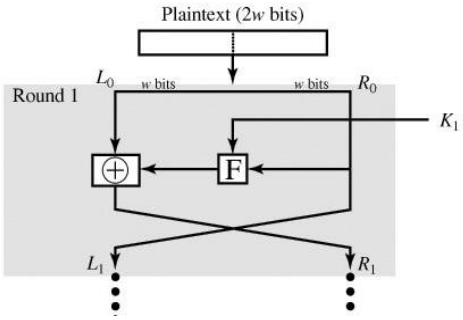
1. Write the encryption formulas with the Feistel scheme according to iteration *i*,

   $L_i = R_{i-1}$,
   $Ri = Li\text{-}1_F (Ri\text{-}1, Ki)$

2. Write the decryption formulas with this scheme according to iteration *i*,

   $R_{i-1} = L_i$
   $L_{i-1} = R_{iF(R \oplus i, K_i)}$

3. Draw this scheme for encryption



4. Apply this scheme on:
   - The block: 11010110
   - The key (K_0): 1010
   - F(x,k)= x or k
   - $K_i = k_{i-1}$ xor 1011
   - Number of iterations: 3.

i	1	2	3
Ki	0001	1010	0001
Li	0110	1010	1100
Ri	1010	1100	0111

The encrypted block is: 11010110

Exercise N° 02: *AES*

1. Define the four transformations of the AES

SubByte: substitution of bytes in the state table

ShiftRow: shift of rows in the status table

MixColumn: moving columns in the status table (except last round)

AddRoundKey: addition of a "round key" that varies with each round.

2. Apply SubBytes to byte (01001001).

0100 1001

4 9➔ we use the S-box matrix to find the value of line 4 and column 9

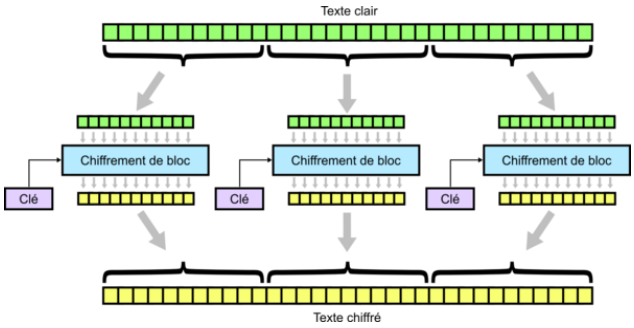
The result is **3b**, so the new byte is: **00111011**

3. Apply ShiftRow to the table:

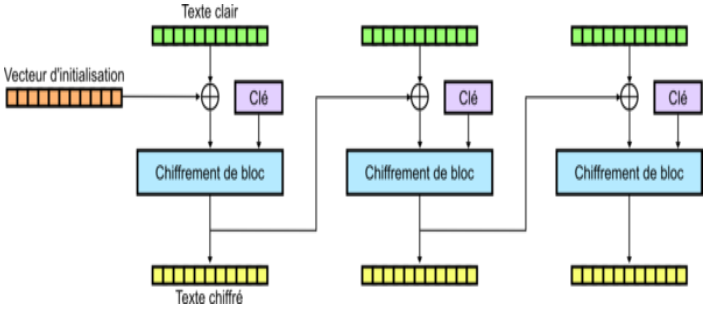
34	9a	aa	01
00	0e	67	f4
fb	5th	89	ff
c5	00	e4	cc

Exercise N° 03: *Modes of operation*

Be the schemas of symmetric encryption operation modes:



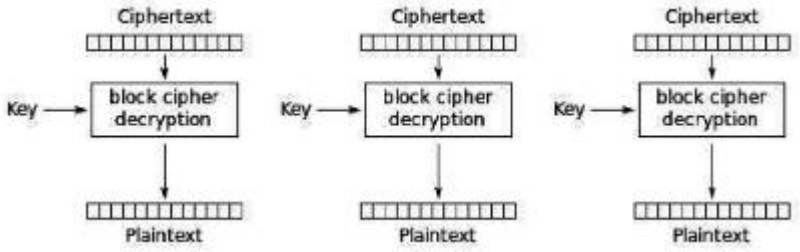
(1) ECB



(2) CBC

1. The ECB mode**:**

- Draw the decryption diagram.



- Deduce the encryption/decryption functions.

Encryption: Ci = EK(Pi)

Decryption: Pi = DK(Ci)

- What is the problem with this mode?

The repetitions of clear message fragments are not masqued and are found in the form of repeated fragments in the encrypted message.

- Calculate the ciphertext:

M = 101100011011101

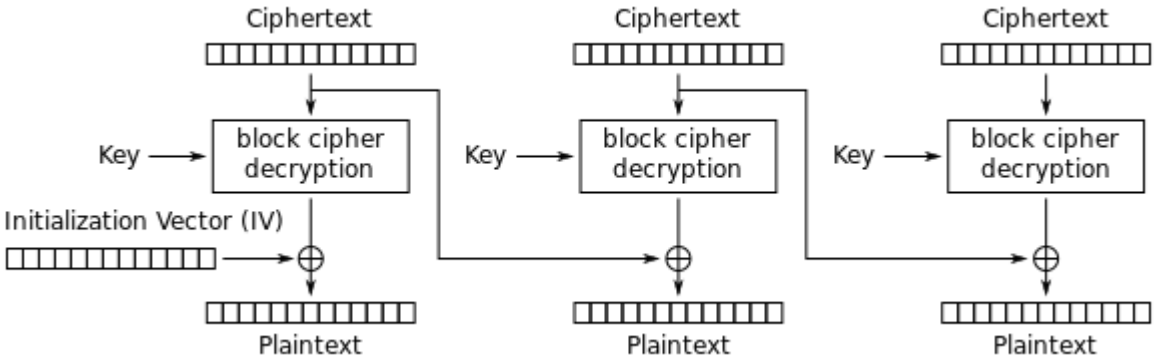
We have a 4-bit size key, so the block size is 4 bits.

B1=1011, B2=0001, B3=1011, B4=101 **0** (add a bit in the least significant bit (LSB) of value 0)

The cipher text is: 0111001001110101

2. The **CBC** mode:

- Draw the decryption diagram.



- Deduce the encryption/decryption functions.

  Encryption: C0VI = Ci = EK(Pi⊕ Ci-1)

  Decryption: C0VI =Pi = DK(Ci)⊕ Ci-1

- Calculate the ciphertext:

  We apply the encryption function after splitting the message into blocks.

  0010011010110010

Exercise No. 01: *(Mathematical concepts)*

Apply Fermat's test on p=11, with a=2 and a=3.

- 2^{10} mod 11=1, 11 is pseudo(-Fermat)-prime base 2.
- 3^{10} mod 11=1, 11 is pseudo(-Fermat)-prime base 3.

Calculate Φ (19), Φ (15), Φ (8)

- Φ (19)=19-1 = 18
- Φ (15)= 5 *3 = (5-1)(3-1)= 8
- Φ (8)= Φ (23)=22(2-1)=4

Calculate 5^{13} mod 71 using the fast exponentiation algorithm.

a=5, n=71

e=13= (1101)2 m=4

i	-	2	1	0
ei	1	1	0	1
r	5	25	5	25
R=r*a		54		54

Exercise No. 2: *(RSA encryption)*

Let p = 7 and q = 19

1. Describe the key generation scheme, encryption scheme, and decryption scheme.

   See the course

2. Show that D(E(m)) = m.

   D(E(m))= D(me mod n)= (me)d mod n= med mod n

   knowing that ed = 1 mod Φ(n) = k Φ(n)+1

   then D(E(m)) = $mk^{\Phi(n)+1}$ mod n = m

3. Calculate N and Φ (n).

   N = pq = 133 and Φ(n) = (p-1)(q-1) = 108

4. We propose e = 5. Calculate the private key d.

   ed = 1 mod Φ(n) $d = e^{-1}$ mod Φ(n)

   $d = 5^{-1}$ mod 108 = 65

5. Encrypt the plaintext m = 6.

   $C = m^e$ mod n = 6^5 mod 133 = 62

6. Decrypt the ciphertext c= 62.

$M = c^d \bmod n = 62^{65} \bmod 133 = 6$

Exercise No. 2: (Diffie-Hellman Protocol)

1. What is the purpose of the Diffie-Hellman protocol?

   Key exchange

2. Determine the Diffie-Hellman session key if Alice communicates the numbers g = 3 and p = 23 to Bob, given that Alice selects the random number a = 5 and Bob selects the number b = 7.

   The session key calculated in the Diffie-Hellman protocol is $K = g^{xy} \bmod p$

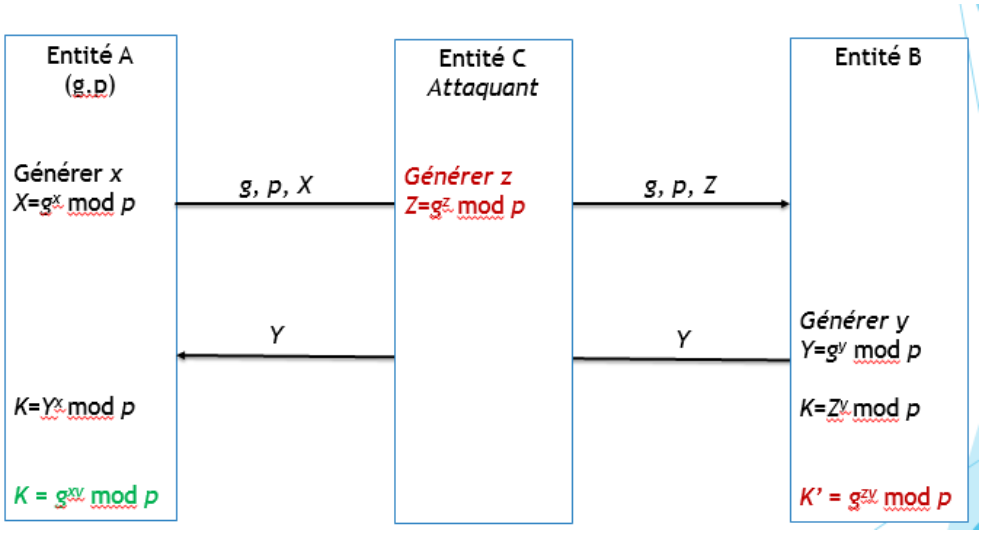
   It's necessary to calculate X and Y.

   $K = 3^{5*7} \bmod 23 = 9$

3. Explain the weaknesses of the Diffie-Hellman protocol.

The Diffie-Hellman protocol is vulnerable to man-in-the-middle attacks.

4. Propose a MITM type attack scenario.



Exercise No. 4: (Hash Functions)

- What properties must hash functions check?

  Pre-image resistance, Second pre-image resistance, Collision resistance

- Give examples of applications of hash functions.
  - Password protection,
  - Pseudo-random number generator,
  - Message authentication code (MAC),
  - Deriving session keys.
  - Blockchain.
  - Compress messages during digital signature generation and verification.

- What is the difference between MDC and HMAC type functions?

MDC	HMAC

▶ A hash function H that can be computed without knowledge of a secret. ▶ Ensures integrity. ▶ The function is defined as follows: H(m)	▶ Ensures integrity and authentication ▶ is a type of message authentication code (MAC), calculated using a hash function in combination with a secret key. ▶ HMAC security is dependent on the hash function used.

- Which of these hash functions are secure: MD-5, SHA-3, SHA-1, SHA-512?

  SHA-3, SHA-512.

- Why is a hash function a better way to verify integrity than a checksum such as the Internet checksum?

  The properties of the hash function are not applied for Internet checksum.