University Djilali Bounaâma of Khemis-Miliana
Department of Computer Science
L3 – Computer Systems (S6) - 2025/2026
Subject: Computer Security and Cryptography

Series of exercises N° 01

Exercise n° 01: (Polybius)

Use Polybius square to decrypt the following:

3532444413443532444413441341151225522134345212133214151225424425151532251415133115122535213434

Key = "GHOST"

Exercise n° 02: (CAESAR)

The following message was encrypted with CAESAR Cipher: "NYRN WNPGN RFG"

- Decrypt mathematically this message knowing that the used shift is: A → N
- The encryption with the previous shift is associated with a particular type of CAESAR, give its name.
- If we do not know the number of shifts, how many times must we try to be able to decrypt a message encrypted with CAESAR?

Exercise n° 03: (Playfair)

Encrypt the message "SHOW ME THE MONEY" using Playfair cipher. Key = "SMART"

Exercise n° 04: (Hill)

1) Encrypt the word **ALGERIAN** using Hill cryptosystem Key = $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$
2) Decrypt with Hill the ciphertext C = MWHEFHWXMA Key = $\begin{pmatrix} 3 & 6 \\ 2 & 5 \end{pmatrix}$

Exercise n° 05: (Hill – Arabic version) – Right-to-Left

Decrypt with Hill the ciphertext C = **"ي،ل،ص،ش،ح،ن،ص،ش"** Key = $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$

Exercise n° 06: (Bellaso/Porta – Arabic version) – Right-to-Left

Deccrypt with Bellaso/Porta the ciphertext: **ك، ش، ق، ر، غ، ر، ب، ب، س، ف، غ، ش**

Key = طروادة

Exercise n° 07: (Vigenère)

Encrypt mathematically the following ciphertext using Vigenère: "SHOW ME THE MONEY"

Key = SMART

Decrypt with the same key the ciphertext: "CQEGVSXMRGVETRRHASZMAHE"

Exercise n° 08: (ZigZag – Rail Fence)

Encrypt the plaintext: "Beat around the bush" using a ZigZag of three levels.

Decrypt the ciphertext: "SMEEHWEHMNYOTO"

Exercise n° 09: (ADFGVX)

Encrypt the plaintext: "Beat around the bush" using ADFGVX Key = DEMAIN

Fill the encryption matrix in the following order: 0..9,A..Z

Decrypt the ciphertext: FFAGFXGDADGADGFXGADDAXFXD_ _ F_ _ Key = CIPHER

Fill the encryption matrix in the following order: Z..A,9..0

Exercise n° 10: (Bazeries)

Encrypt the plaintext: "Beat around the bush" using Bazeries. Key = 22

Exercise n° 11: (Nihilists)

Encrypt the plaintext: "Beat around the bush" using Nihilists. Key 1 = DIFFICULT Key 2 = EASY

Exercise n° 12: (Over-Encryption)

A plaintext M was over-encrypted three times using three different algorithms to get a ciphertext X = 336564432374432375334454534464542375546554533336746_237543

Encryption keys:

Bazeries (Key = 38)

ADFGVX (Key = AGENCY)

Nihilists (Key 1 = VIRUS, Key 2 = BIN)

- Decrypt the ciphertext X.

	A	D	F	G	V	X
A	Q	Y	A	L	S	E
D	Z	C	R	X	H	0
F	F	O	4	M	8	7
G	3	I	T	G	U	K
V	P	D	6	2	N	V
X	1	5	J	9	W	B

Exercise n° 13: (Brute force)

A system is protected by a **password**. After an unsuccessful attempt, the system waits for a while before asking for the password again (the total time for one attempt is 3 seconds). How long (in seconds) will it take to penetrate the system knowing that the password consists of:

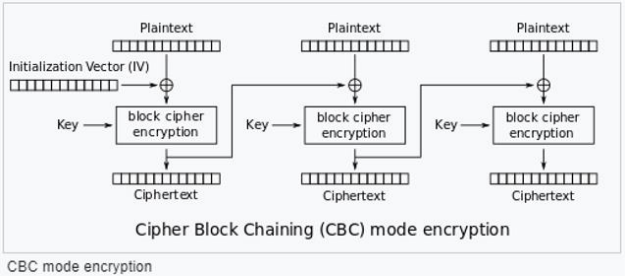
- 4 digits?
- 4 letters?
- 4 alphanumerics (digits/letters)?

Exercise n° 14: (Xoring)

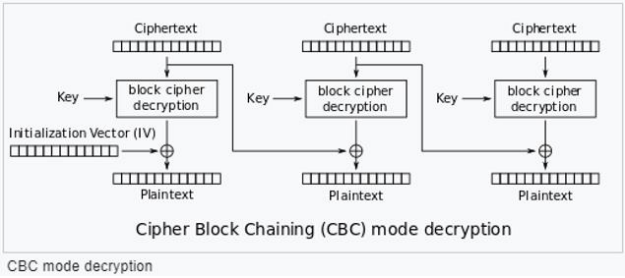
We want to encrypt the plaintext word '**EYE**' with the key '**S**' using a **XORing** encryption: Knowing that the decimal values of the plaintext letters in the ASCII table are: E=69, Y=89, S=83. Provide the encrypted word in decimal?

Exercise n° 15: (CBC mode encryption)

We want to encrypt the binary sequence "**1100110101110111010111011**" using CBC mode with **8-bit** blocks, knowing that: The initialization vector **IV** = **"10010101"**. The key **K** = **"11101101"**. The encryption function is used to invert the block to be encrypted after XORing with K. Write down the encrypted binary sequence? Decrypt the encrypted sequence in order to get the initial binary sequence?



CBC mode encryption



CBC mode decryption