**University Djilali Bounaâma of Khemis-Miliana**

**Department of Computer Science**

**3rd year Bachelor's Degree – Computer Systems (S6) - 2023/2024**

**Subject: IT Security and Cryptography**

## Series of exercises N° 01

**Exercise 01:** Match each of the following concepts with the appropriate definition.

1)

| | | | |
|---|---|---|---|
| A | Integrity | A | Ensures that the content of a communication or file is not accessible to third parties |
| B | Confidentiality | B | Guarantees the identity of a given entity or the origin of a communication or file |
| C | Authenticity | C | Ensures that the content of a communication or file has not been modified |

2)

| | | | |
|---|---|---|---|
| A | Cryptosystem | A | Encryption algorithm |
| B | Cipher program | B | Encrypted text |
| C | Cryptogram | C | Ciphergram |

3)

| | | | |
|---|---|---|---|
| A | Cryptanalysis | A | To transform plaintext messages into unreadable text |
| B | Ciphering | B | To analyze the encrypted messages in order to decrypt them |
| C | Decryption | C | To decode the encoded messages |

4)

| | | | |
|---|---|---|---|
| A | To encode | A | Letter-level substitution |
| B | To cipher | B | Word-level substitution |
| C | To Transpose | C | Sentence-level substitution |

5)

| | | | |
|---|---|---|---|
| A | Symmetric cryptography | A | It uses the same key to encrypt/decrypt |
| B | Secret-key cryptography | B | It uses two different keys to encrypt/decrypt |
| C | Asymmetric cryptography | C | It does not use secret conventions before exchanging secret messages |

6)

| | | | |
|---|---|---|---|
| A | Worm | A | Self-Replicate by inserting into hosts |
| B | Virus | B | Spread through the network |
| C | Trojan horse | C | Activity that appears legitimate but is malicious |

7)

| | | | |
|---|---|---|---|
| A | Detection | A | Create virtual disks |
| B | Prevention | B | Create a restore point |
| C | Recovery | C | Block/Delete suspicious connections/files |
| D | Filtering | D | Restore the last known good configuration |

8)

| | | | |
|---|---|---|---|
| A | Confidentiality breach | A | Log in with someone else's username and password |
| B | Integrity breach | B | Intercepting a secret communication |
| C | Authenticity breach | C | Modify the amount of a monetary transaction |
| D | Repudiation | D | Bombarding a server with TCP-SYN requests |
| E | Availability breach | E | Deny sending or receiving a message |

**Exercise n° 02:** Use Polybius square to decrypt the following:

3532444413443532444413441341151225522134345212133214151225424425151532251415133115122535213434

Key = "GHOST"

**Exercise n° 03:** The following message was encrypted with **CAESAR** Cipher: "NYRN WNPGN RFG"

- Decrypt mathematically this message knowing that the 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° 04:** Encrypt the message "SHOW ME THE MONEY" using Playfair cipher.

Key = "SMART"

- What type of encryption system does this cipher belong to?

**Exercise n° 05:**

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

**Exercise n° 06:** Encrypt mathematically the following message using Vigenère:

"**SHOW ME THE MONEY"**

Key = **SMART**

- Decrypt with the same key the message: **CQEGVSXMRGVETRRHASZMAHE**

**Exercise n° 07 :**

| **Encrypt:** «Beat around the bush» | **Decrypt:** |
|---|---|
| 1. Simple Transposition: Key = 3.1.2 | «NIOGNRCASEBISLSI» Key = 3.1.4.2 |
| 2. ZigZag of three levels | «SMEEHWEHMNYOTO» ZigZag = 3 |
| 3. Matrix-Based Transposition : Key = (4*4) | «HEBEVOLEDLRYOY!» Key = (3*5) |
| 4. ADFGVX : Key = DEMAIN<br>Fill the encryption matrix in the following order:<br>0..9,A..Z | FFAGFXGDADGADGFXGADDAXFXD_ _ F_ _<br>Key = CIPHER<br>Fill the encryption matrix in the following order:<br>Z..A,9..0 |
| 5. Bazeries Cipher : Key = 22 | |
| 6. Nihilists Cipher :<br>Key 1 = DIFFICULT Key 2 = EASY | |