**Université Djilali Bounaâma - Khemis-Miliana**
**Département : Mathématiques et Informatique**
**3ème Année Licence - informatique**
**Matière : Sécurité informatique et Cryptographie**

# Série d'exercice N° 01

**Exercice n° 01 : Choisir les bonnes réponses**

| | |
|---|---|
| 1. Un bon cryptosystème est celui qui garantit l'intégrité des données échangées, cela veut dire qu'il : | |
| a | Garantit que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers |
| b | Garantit l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier |
| c | Garantit que le contenu d'une communication ou d'un fichier n'a pas été modifié |
| 2. Un cryptogramme est un terme qui désigne : | |
| a | L'algorithme de cryptage |
| b | Le message crypté |
| c | Le programme de cryptage |
| 3. Le cryptanalyste est la personne qui : | |
| a | Analyse les messages en clairs en vue de les crypter |
| b | Analyse les messages chiffrés en vue de les décrypter |
| c | Aucune des deux |
| 4. La différence entre les termes « chiffrer » et « coder » est que: | |
| a | Le deuxième utilise la substitution au niveau des lettres et le premier l'utilise au niveau des mots |
| b | Le deuxième utilise la substitution au niveau des mots et le premier l'utilise au niveau des lettres |
| c | Il n y a pas de différence entre les deux |
| 5. La cryptographie est dite symétrique si : | |
| a | Elle utilise la même clé pour chiffrer / déchiffrer |
| b | Elle utilise deux clés différentes pour chiffrer / déchiffrer |
| c | Elle n'utilise pas des conventions secrètes avant d'échanger des messages |

**Exercice n° 02 :**

Chiffrer avec Polybe (Alphabet français) le message suivant :

RENDEZ VOUS DEMAIN MATIN

Clé de chiffrement : CLE

**Exercice n° 03 :**

Soit le message chiffré avec CESAR : NYRN WNPGN RFG

- Déchiffrer ce message sachant que le décalage est : A → N
- Le chiffrement avec le décalage précédent est associé à un type particulier de CESAR, donner son nom.
- Déchiffrer mathématiquement le message précédent.
- Si nous ne connaissons pas le nombre de décalage, Combien de fois on doit essayer pour pouvoir déchiffrer un message chiffré avec CESAR (Prendre en considération la première lecture du message chiffré).

**Exercice n° 4**

Chiffrer par Playfair, le message : SHOW ME THE MONEY Clé : SMART

- A quel type de chiffrement appartient ce système ?
- Expliquer le mécanisme de chiffrement de ce système.

**Exercice n° 5**

- Chiffrer le mot **ALGERIEN** par le système de Hill (chiffrement par bigramme) en expliquant les différentes étapes de chiffrement.

  Clé $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$

**Exercice n° 6 :**

- Chiffrer avec Vigenère le message en clair : **SHOW ME THE MONEY**

avec la clé **SMART**.

- Déchiffrer mathématiquement le message chiffré.

**Exercice n° 7 :**

1. Chiffrer avec transposition simple le message : ATTAQUER CE SOIR

Clé = 3.1.2

2. Chiffrer le même message avec un zig zag de deux puis de trois niveaux.
3. Chiffrer le même message avec une transposition à base matricielle
Clé = (4*4)
4. Chiffrer le même message avec ADFGVX, Clé = DEMAIN
(ranger le contenu de la matrice selon l'ordre 0..9,A..Z).
5. Surchiffrer le même message avec le chiffre de Bazeries
Clé = 22
6. Surchiffrer le même message avec le chiffre des Nihilistes
Clé 1 = DIFFICULT
Clé 2 = EASY