**Année Universitaire** :2024 – 2025

**Département** : Informatique

**Module** : Cryptographie Appliquée

**Master** : 2I2S

**Semestre**: 3

Université Mohammed V
Faculté des Sciences
Rabat

**Travaux Dirigés de Cryptographie Appliquée**

**TD1** : Cryptographie Classique

## Exercice 1 : Chiffrement de César

1. Chiffrez le texte clair suivant en utilisant le chiffrement de César avec un décalage de k = 5.

Texte clair : BIENVENUE DANS LE COURS DE CRYPTOGRAPHIE APLLIQUEE

2. Déchiffrez le texte chiffré suivant, sachant qu'il a été chiffré avec un décalage de k = 7.

Texte chiffré : SLZKVUULLZZVUAJVUMPKLUAPLSSLZ

3. Proposez une méthode pour casser un chiffrement de César sans connaître le décalage utilisé.

Texte chiffré : ZHOFRPH DXFRXUV GH FUBSWRJUDSKLH

a) Appliquez une attaque par force brute : testez les 25 décalages possibles pour retrouver le texte clair.
b) Identifiez le décalage correct et écrivez le texte clair obtenu.
c) Si vous disposez de la fréquence moyenne des lettres en français (E, A, S, T, etc.), comment pourriez-vous accélérer la recherche de la clé ?

## Exercice 2 : Chiffrement de Vigenère

1. Chiffrez le texte clair suivant avec le mot-clé CLE.

Texte clair : MISSION SECRETE

2. Déchiffrez le texte suivant avec le mot-clé CODE.

Texte chiffré : ~~PQVTVX RXHWGRX~~

~~3. Expliquez pourquoi le chiffrement de Vigenère~~ résiste mieux à l'analyse de fréquence que le chiffrement de César.

## Exercice 3 : Chiffrement de Vernam

1. Chiffrez le texte clair suivant en binaire, en utilisant la clé donnée :

Texte clair (ASCII) : MESSAGE, clé (ASCII) : CLESCRT

Utilisez le code binaire ASCII de chaque caractère et appliquez l'opération XOR.

2. Déchiffrez le texte suivant, sachant que la clé utilisée est :

Clé : 10101101, texte chiffré : 11010010

## Exercice 4 : Chiffrement ROT13

1. Chiffrez le texte suivant en appliquant ROT13.

Texte clair : HELLO WORLD

2. Déchiffrez le texte suivant en appliquant à nouveau ROT13.

Texte chiffré : URYYB JBEYQ

**Formule :**

$$E(x) = (x + 13) \bmod 26$$

## Exercice 5 : Chiffrement Affine

1. Chiffrez le texte clair suivant en utilisant la fonction affine : $E(x) = (5x+8) \bmod 26$.

Texte clair : AFFINE

2. Déchiffrez le texte chiffré suivant avec la fonction affine inverse : $D(x) = 21(x - 8) \bmod 26$.

Texte chiffré : IHHWVCSWFRCP

3. Montrez comment calculer l'inverse multiplicatif de a = 5 modulo 26 (utile pour le déchiffrement).

**Formule :**

$$E(x) = (ax + b) \bmod 26,\ D(x) = a^{-1}(x - b) \bmod 26$$

## Exercice 6 : Carré de Polybe

Carré de Polybe standard : Le carré de Polybe associe chaque lettre de l'alphabet à une paire de coordonnées dans une grille 5 × 5. Les lettres I et J partagent la même case. Voici le tableau de correspondance :

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | A | B | C | D | E |
| 2 | F | G | H | I/J | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

1. Chiffrez le texte clair suivant en utilisant le carré de Polybe :

Texte clair : BIENVENUE DANS CE COURS

Indiquez les coordonnées de chaque lettre et écrivez le texte chiffré.

2. Déchiffrez le texte suivant en utilisant le carré de Polybe :

Texte chiffré : 32 15 43 11 22 15 43 15 13 42 15 44

écrivez le texte clair correspondant.

## Exercice 7 : Chiffrement Scytale

Le chiffrement Scytale est une méthode de transposition ancienne où un message est écrit sur un support rectangulaire selon un nombre fixe de colonnes (clé). Le message chiffré est obtenu en lisant les caractères colonne par colonne.

1. Chiffrez le texte clair suivant en utilisant le chiffrement Scytale avec la clé 6

   Texte clair : BIENVENUE DANS LE COURS DE CRYPTOGRAPHIE APPLIQUEE.

   Clé (nombre de colonnes) : 6.

2. Déchiffrez le texte chiffré suivant en utilisant la clé (nombre de colonnes) :4

   Texte chiffré : MAETEGCZSERZSSEZ