**Université Des Sciences et de la Technologie d'Oran Mohamed Boudiaf USTO-MB**
**Faculté des Mathématiques et Informatique**
**Département d'informatique**

**Sécurité Informatique** **2025-2026**
**Dr F.Khalifa**

# TD3

## Cryptographique Classique

### Exercice 1

**Question 1.** Le code de César est une méthode de chiffrement par rotation de l'alphabet. Dans la version utilisée par Jules César, un décalage de trois lettres vers la droite était effectué pour coder.

1. Chiffrer le message "la rencontre est prévue à la cafétéria" à l'aide du chiffrement par décalage et de la clé K = 5.
2. Décrypter le message "RGNEIDVGPEWXTRAPHHXFJT" sachant qu'il a été crée par un chiffrement par décalage.
3. Dans un texte en français les lettres les plus fréquentes sont le A (8.4%) et le E (17.26%). Sachant que le message est en français, chiffré en utilisant le chiffrement par décalage sur les 26 lettres de l'alphabet, déterminer la clef et décrypter le début du message : SVOXFYIKNKXCVKVSQEBSOKMRODOBNOCCYVNKDC

**Question 2.** Soit le message suivant: la rencontre est prévue à la cafeteria

1. Crypter le message précédent à l'aide de la méthode de Vigenére et du mot clé poule
2. Est-il possible de décoder le message « DSJWPHYRSSUHPAJXVQV » codé par un chiffrement de Vigenère sans connaître la clé. Décoder ce message sachant qu'il a été créé à l'aide du mot clé BORDEAUX.

**Question 3 (Chiffrement Affine)**

Le chiffrement affine est un chiffrement par substitution mono-alphabétique. La clé consiste en un coupe d'entier (a, b) ∈ (Z/26Z) ∗ x (Z/26Z). L'idée est d'utiliser comme fonction de chiffrement la fonction affine y = ax + b mod 26. Il faut remplacer une lettre par son rang :

| 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 |

1) Chiffrer le mot CODE avec la clé (F,T).
2) Déchiffrer KZXI avec la clé (H,V)..

**Question 4 (chiffrement de Hill )**

Chiffrer le message SUPINFO avec la clé $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$