1. Système Cryptographique

Un **système cryptographique** est un ensemble d'éléments définis comme suit :

- **P** : un ensemble fini de **textes clairs** (c'est-à-dire le texte original que l'on souhaite protéger).
- **C** : un ensemble fini de **textes chiffrés** (c'est-à-dire le texte après avoir été chiffré).
- **K** : un ensemble fini de **clés** utilisées pour chiffrer et déchiffrer les messages.
- **E** : un ensemble de règles de **chiffrement**, qui permet de transformer un texte clair en texte chiffré à l'aide d'une clé.
- **D** : un ensemble de règles de **déchiffrement**, permettant de récupérer le texte clair à partir du texte chiffré en utilisant une clé.

2. Protocole de chiffrement/déchiffrement

Voici un protocole de base pour le chiffrement et le déchiffrement des messages entre deux personnes, Alice et Bob :

1. **Accord préalable** : Alice et Bob conviennent du système cryptographique à utiliser (c'est-à-dire des ensembles P, C, K, E, D).
2. **Choix des clés** : Ils choisissent la clé qu'ils utiliseront pour chiffrer et déchiffrer le message.
3. **Chiffrement par Alice** :
    - Alice prend le texte clair, par exemple, "x = x_1 x_2 ... xn", et l'envoie à Bob après l'avoir chiffré avec une clé choisie.
    - Elle applique la règle de chiffrement **Ek** (en fonction de la clé k), ce qui donne le texte chiffré **y = y_1 y_2 ... yn**, où chaque lettre **Yi = Ek(x_i)**.
4. **Déchiffrement par Bob** :
    - Bob reçoit le texte chiffré et applique la règle de déchiffrement **D**, ce qui lui permet de retrouver le texte clair **x** : **Xi = D(Yi)**.

3. Exemple de Chiffrement par Transposition

Le chiffrement par **transposition** consiste à mélanger l'ordre des lettres dans un texte. Cela peut être fait en divisant le texte en blocs et en lisant les lettres dans un ordre spécifique.

Exemple :

Texte : **"DIEU EST LE POINT TANGENT ENTRE ZERO ET L INFINI"**

Diviser le texte en blocs de taille fixe (par exemple 3 lettres) :
mathematica
Copier le code

```
DIE
U E
ST
LE
```

```
POI
NT
TAN
GEN
TE
NTR
E Z
ERO
ET
LI
NFI
NI
```

1.
2. **Lire par colonne** : Une fois le texte divisé en blocs, on lit par colonne pour obtenir le texte chiffré.
    - Colonne 1 : D, U, S, L, T, A, N, G, E, N, E, E, T
    - Colonne 2 : I, E, T, E, P, G, E, E, I, Z, O, N, F
    - Colonne 3 : E, S, N, I, O, T, N, T, R, O, T, T, I
3. Texte chiffré : **"DUST TEE LPNEOT I TETAF NNENEET RRZO NELETTIN T"**

4. Chiffrement avec une Clé Simple ("FAUSTROLL")

Dans ce type de chiffrement, une clé est utilisée pour déterminer l'ordre des colonnes lors de la lecture du texte.

Exemple :

Clé : **"FAUSTROLL"**

Texte : **"DIEU EST LE POINT TANGENT TANGENT"**

Diviser le texte en blocs de 9 lettres (puisque la clé a 9 lettres) :
mathematica
Copier le code
```
DIEU EST
LE POINT
TANGENT E
NTRE ZERO
ET LINFI
NI
```

1.
2. **Attribuer un numéro à chaque lettre de la clé**, selon l'ordre alphabétique :
    - F → 2, A → 1, U → 9, S → 8, T → 7, R → 6, O → 5, L → 4

3. **Lire les colonnes dans l'ordre des lettres de la clé** : L'ordre des colonnes est déterminé par la clé.

5. Chiffrement de Vigenère

Le chiffrement de **Vigenère** est une méthode de chiffrement **polyalphabétique**. Cela signifie qu'une clé est utilisée pour déterminer un décalage différent pour chaque lettre du texte clair.

Exemple :

Texte : **"CETEXTEESTCHIFFREPARVIGENERE"** Clé : **"CHIFFRE"**

Répéter la clé pour couvrir tout le texte :
arduino
Copier le code
```
Clé : "CHIFFRECHIFFRECHIFFRECHIFFRECHIFFRE"
```

1.
2. **Appliquer le chiffrement de Vigenère** : Chaque lettre du texte clair est décalée selon la position de la lettre correspondante de la clé. Par exemple :
    - **C** (3) et **C** (3) donnent un décalage de 6, donc la lettre **C** devient **I**.
    - **E** (4) et **H** (8) donnent un décalage de 12, donc la lettre **E** devient **Q**, et ainsi de suite.
3. Texte chiffré : **"EMCKDLJHACINAKIZNVGJALONTKJJ"**

6. Chiffrement de César

Le **chiffrement de César** est un exemple simple de **substitution monoalphabétique** où chaque lettre du texte est décalée d'un nombre fixe de positions dans l'alphabet.

Exemple avec un décalage de 3 :

Texte : **"CE TEXTE EST CHIFFRE PAR CÉSAR"**

1. Chaque lettre est décalée de 3 positions dans l'alphabet :
    - **C** devient **F**
    - **E** devient **H**
    - **T** devient **W**
    - Et ainsi de suite...
2. Texte chiffré : **"FH WHAWV HVW FKIIHUH SDU FÉVDU"**

7. Substitution Affine

Le **chiffrement affine** est une combinaison de multiplication et d'addition dans un alphabet numéroté. La clé consiste en un couple de nombres **(a, b)**, où **a** doit être inversible modulo 26 pour que le chiffrement soit valide.

Exemple avec la clé (3, 12) :

1. Le texte clair est transformé selon la formule **E(x) = ax + b**, et le texte chiffré est obtenu avec cette règle.

Le chiffrement affine est une méthode de chiffrement où chaque lettre du texte est transformée par une fonction affine de la forme $Ek(x)=ax+bEk(x)=ax+b$, où aa et bb sont des clés, et xx est l'index de la lettre dans l'alphabet. Pour déchiffrer, on utilise la fonction inverse $Dk(y)=a−1(y−b)Dk(y)=a−1(y−b)$, où $a−1a−1$ est l'inverse de aa modulo 26.

Exemple de chiffrement affine avec $K=(3,12)K=(3,12)$

1. **Lettre et indices** :
   - L'alphabet est $\{A=0,B=1,C=2,...,Z=25\}\{A=0,B=1,C=2,...,Z=25\}$.
   - Soit le message clair : "HELLO".
2. **Application du chiffrement affine** :
   - La clé $K=(3,12)K=(3,12)$ signifie que :
     - $a=3a=3$
     - $b=12b=12$
   - La formule de chiffrement est : $Ek(x)=ax+b\mod 26Ek(x)=ax+bmod26$.
3. **Chiffrement de chaque lettre** :
   - $H→x=7H→x=7$, donc $Ek(7)=(3×7+12)\mod 26=(21+12)\mod 26=33\mod 26=7Ek(7)=(3×7+12)mod26=(21+12)mod26=33mod26=7$, soit HH reste HH.
   - $E→x=4E→x=4$, donc $Ek(4)=(3×4+12)\mod 26=(12+12)\mod 26=24\mod 26=24Ek(4)=(3×4+12)mod26=(12+12)mod26=24mod26=24$, soit EE devient YY.
   - $L→x=11L→x=11$, donc $Ek(11)=(3×11+12)\mod 26=(33+12)\mod 26=45\mod 26=19Ek(11)=(3×11+12)mod26=(33+12)mod26=45mod26=19$, soit LL devient TT.
   - $L→x=11L→x=11$ (identique au précédent), donc LL devient encore TT.

- O→x=14O→x=14, donc Ek(14)=(3×14+12)mod 26=(42+12)mod 26=54mod 26=2Ek(14)=(3×14+12)mod26=(42+12)mod26=54mod26=2, soit OO devient CC.

4. **Message chiffré** : "HYTTC"

Transposition des caractères :

Le terme "transposition des caractères" fait référence à une méthode où l'on réorganise l'ordre des caractères dans le texte plutôt que de les transformer selon une règle mathématique.

Par exemple, après avoir obtenu un texte chiffré avec la méthode affine, on pourrait ensuite appliquer une **transposition**pour réarranger l'ordre des lettres, selon une certaine clé (comme dans les exemples précédents avec les transpositions par blocs ou par clés spécifiques).

Dans l'exemple donné, les caractères du texte chiffré ne sont pas transposés après le chiffrement affine. Cependant, s'il y avait une règle de transposition, comme celle avec une clé (par exemple, "FAUSTROLL"), on pourrait organiser les lettres du message chiffré dans un tableau et les lire selon l'ordre des colonnes, déterminé par la clé.

En résumé, **la transposition des caractères dans le chiffrement affine** se réfère à l'application d'une méthode où les caractères du texte chiffré sont réorganisés en fonction d'une clé spécifique. Mais dans le cas d’un chiffrement affine simple, les lettres sont directement modifiées selon la fonction affine, et il n'y a pas de transposition impliquée