# II. CHIFFREMENT CLASSIQUE

- Cryptographie **?**, Histoire
- Méthodes de chiffrement
  - Substitution
  - Transposition

# CRYPTOGRAPHIE ?

La **cryptographie** est une des disciplines s'attachant à protéger des messages.

en assurant leur :
Confidentialité, Authenticité  et Intégrité

en s'aidant souvent de *secrets* ou *clés* .

Le mot cryptographie vient des mots en grec ancien :
*kruptos* : « caché ou secret» et *graphein* : « écrire »

« Ecriture secrète »

# HISTOIRE

- Âge artisanal (Les origines)

❑ *Substitution et Permutation*

*Chiffre de César : décalage des lettres*

*Codes à répertoire : dictionnaire à double entrée*

- Âge technique (Les machines)

❑ *Substitution et Permutation à l'aide de machine électromécaniques*

*Hagelin.*

*Enigma.*

- Âge paradoxal (Les algorithmes)

❑ *Cryptographie asymétrique (utilisation des clés publiques).*

*sans avoir établi au préalable des conventions secrètes*

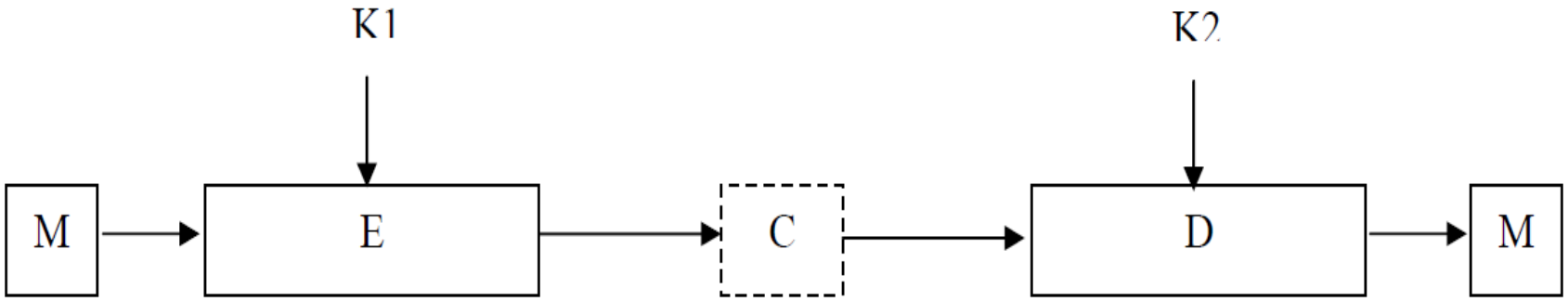
# CONCEPTS

- **Chiffrement :** transformation à l'aide d'une clé d'un message en clair

(dit texte clair) en un message incompréhensible (dit texte chiffré).

- **Chiffre :** utilisation de la substitution au niveau des lettres pour chiffrer ;
- **Code :** utilisation de la substitution au niveau des mots ou des phrases pour coder;
- **Coder :** on remplace un mot ou une phrase par un autre mot, un nombre ou un symbole ;
- **Cryptogramme :** message chiffré ;
- **Cryptosystème :** algorithme de chiffrement;
- **Décrypter :** retrouver le message clair correspondant à un message chiffré *sans posséder la clé de déchiffrement* ;
- **Cryptographie :** La science visant à créer des cryptogrammes ;
- **Cryptanalyse :** science analysant les cryptogrammes en vue de les décrypter ;
- **Cryptologie :** science regroupant la cryptographie et la cryptanalyse.

# FORMALISATION




M : message en clair,
C : message chiffré,
E : fonction de chiffrement (Encryption),
D : fonction inverse de déchiffrement (Decryption),
K1 : clé de chiffrement,
K2 : clé de déchiffrement,

E(M)=C (E transforme M en C)
D(C)=M (D transforme C en M)
D(E(M))=M

# CRYPTOGRAPHIE CLASSQIUE

- La cryptographie classique manipule des caractères :

- Substitution : Remplacer des caractères

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Mot : | C | H | I | F | F | R | E |
| Position dans l'alphabet : | 03 | 08 | 09 | 06 | 06 | 18 | 05 |

- Transposition : Permuter des caractères

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Clé : | 5 | 7 | 2 | 3 | 6 | 1 | 4 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Mot : | C | H | I | F | F | R | E | = | R | I | F | E | C | F | H |

# SUBSTITUTION

Consiste à substituer dans un message chacune des lettres de l'alphabet par une autre (du même alphabet ou éventuellement d'un autre alphabet)

TYPES :

- substitution simple
- substitution homophonique
- substitution par polygrammes
- substitution polyalphabétique
- substitution tomogrammique

# SUBSTITUTION SIMPLE

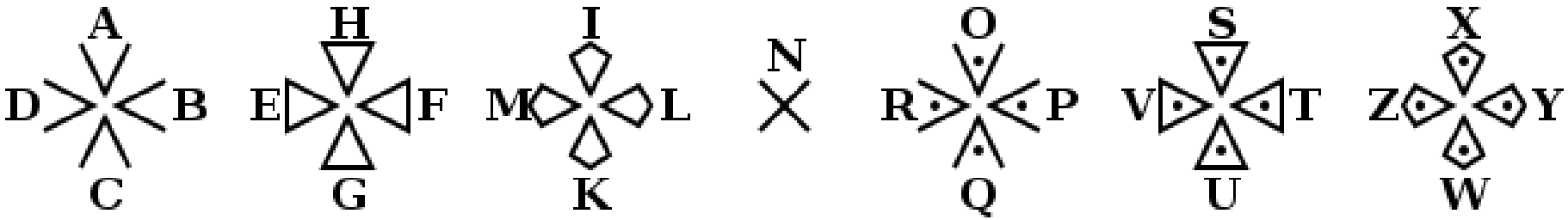
Consiste à remplacer chacune des lettres de l'alphabet du clair par un signe conventionnel : lettre, groupe de lettres ou nombre, une même lettre du clair étant ***toujours représentée*** par le même signe conventionnel.

| | | | | | | |
|---|---|---|---|---|---|---|
| d | i | n | o | s | v | du clair par, |
| **o** | **y** | **v** | **m** | **d** | **b** | ou par, |
| 12 | 23 | 04 | 18 | 08 | 16, | |

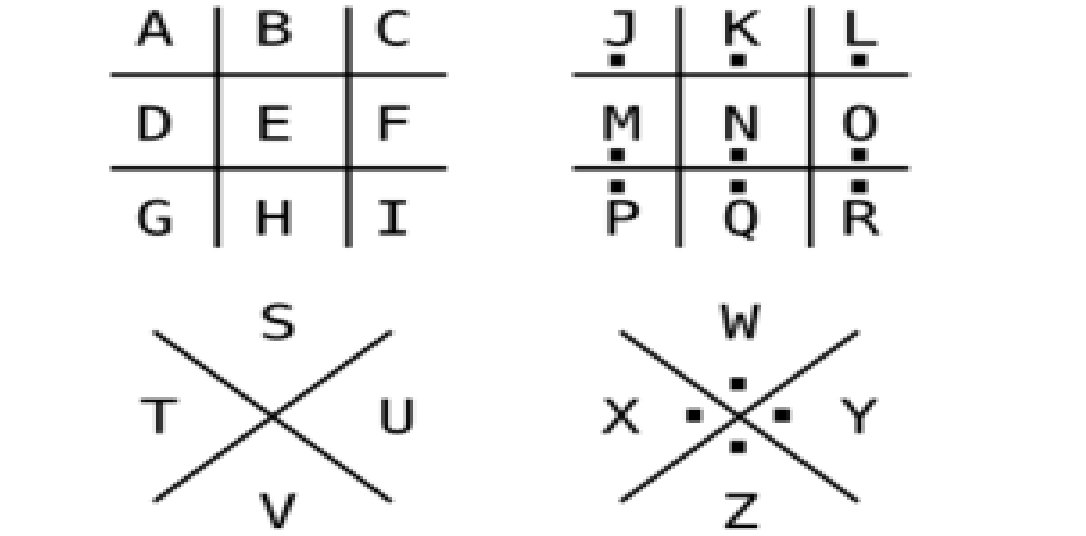
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| le mot en clair : | d | i | v | i | s | i | o | n |
| se chiffrera par : | **o** | **y** | **b** | **y** | **d** | **y** | **m** | **v** |
| ou par : | 12 | **23** | 16 | **23** | 08 | **23** | 18 | 04 |

Exemples : templiers, francs-maçons, ATBASH, polybe, César

- TEMPLIERS



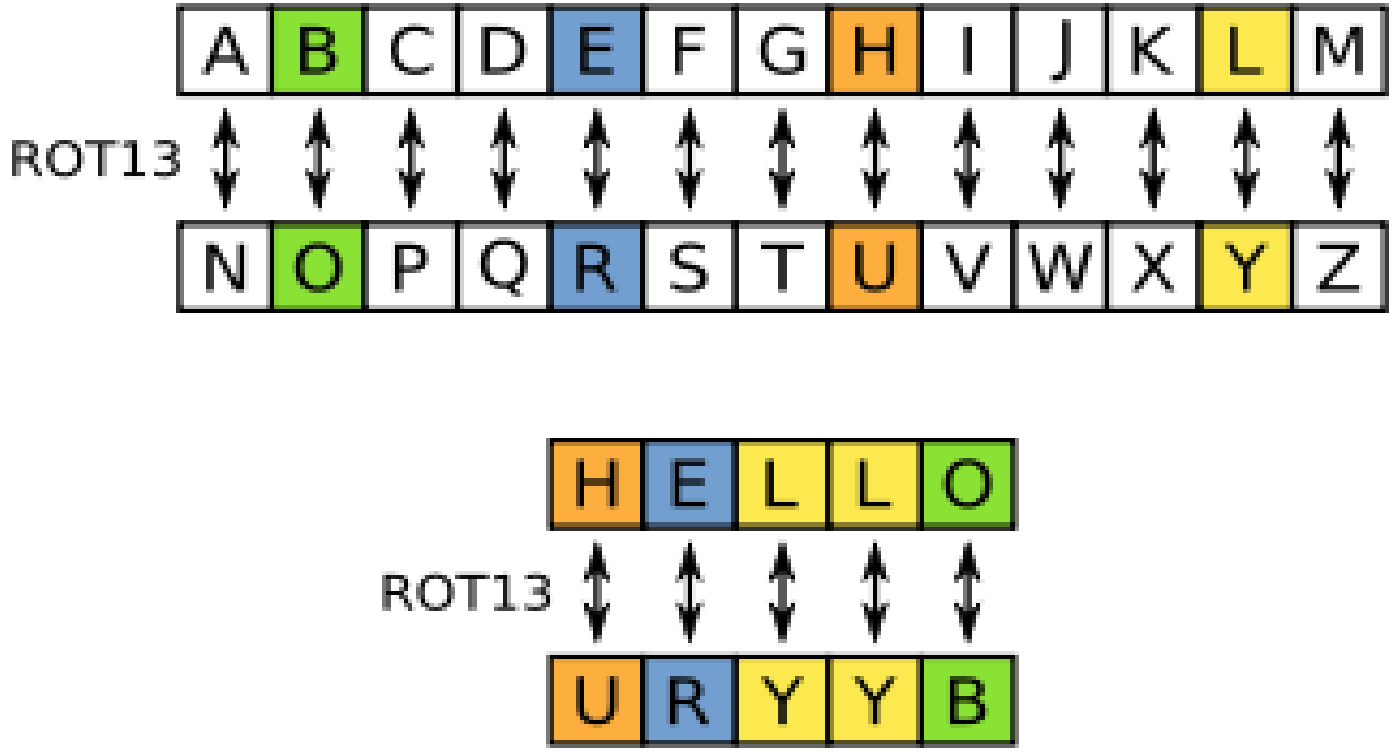

- Parc à couchons (Pigpen)



- ATBASH

| Clair | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Chiffré | Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

- ROT 13



- CARRÉ DE POLYBE

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i | j |
| 3 | k | l | m | n | o |
| 4 | p | q | r | s | t |
| 5 | u | v/w | x | y | z |

Exemples : "e"=15, "u"=51, "n"=34

n.b : Français (v/w), Anglais (i/j)

Il est possible de remplir le tableau de plusieurs façons différentes, par exemple en commençant par remplir avec un mot-clé, puis par ordre alphabétique.

# CHIFFRE DE CÉSAR

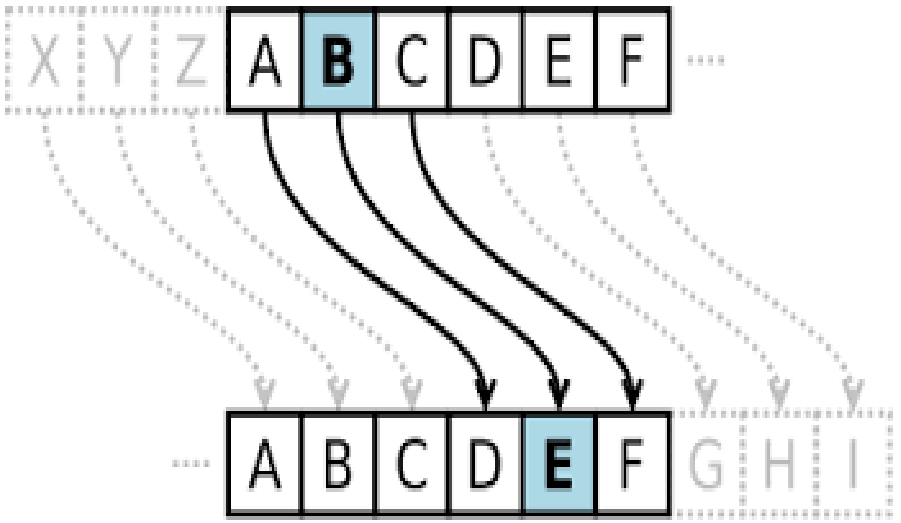
Le chiffre de césar est l'un des premiers protocoles cryptographiques, En effet, pour crypter les messages envoyés à son armée, César procédé comme suit :

- Chaque caractère du texte en clair est remplacé par celui qui se trouve **trois positions** plus loin dans l'alphabet.
  Le A est chiffré en D, le B en E, ..
- Pour le déchiffrement on décale dans l'autre sens. D en A, E en B

Exemple :
César envoya à son armée le message :
DOHD MDFWD HVW

Le message est donc déchiffré en :
ALEA JACTA EST

Qui veut dire en français : Les dés sont jetés



# ▪ CHIFFRE DE CÉSAR (FORMALISATION)

## ➢ Chiffrement :

- Le principe est de numéroter les lettres de l'alphabet de 0 à 25 (A=0,B=1,…, Z=25). Chaque lettre de l'alphabet est chiffrée par la fonction de chiffrement **E** qui utilise un décalage **k**. la fonction **E** est définit comme suite :

$$E_K : \{0,1,\ldots,25\} \rightarrow \{0,1,\ldots,25\}$$
$$i \rightarrow (i+K) \bmod 26$$

**$E_k(i)=(i+k) \bmod 26$ / $i \in \{0,1,\ldots,25\}$**

Si on prend par exemple, k=3 :
$E_3(0)=(0+3) \bmod 26 = 3 = D$
$E_3(1)=(1+3) \bmod 26 = 4 = E$

**Exemple1 :** soit à chiffrer le mot ATTAQUE avec k =3

- CHIFFRE DE CÉSAR (FORMALISATION)

## ➢ Déchiffrement :

Le déchiffrement est définit par la fonction **D** qui utilise un décalage inverse avec les **k** positions définies par la fonction de chiffrement, la fonction **D** est définit comme suite :

$$D_k : \{0,1,\ldots,25\} \rightarrow \{0,1,\ldots,25\}$$
$$i \rightarrow (i-k) \bmod 26$$

$$\mathbf{D_k(i)=(i-k) \bmod 26 \ / \ i \in \{0,1,\ldots,25\}}$$

si 1 a été chiffré en 4 alors $\mathbf{D_3(4) = 4 - 3 = 1}$

Mathématiquement, nous disons que $\mathbf{D_k}$ est une ***bijection réciproque*** de $\mathbf{E_k}$ :
Pout tout $\mathbf{i \in \{0,1,\ldots,25\} : D_k(E_k(i)) = i}$

# SUBSTITUTION HOMOPHONIQUE

Elle est comme un chiffrement à substitution simple, sauf qu'à un caractère du texte en clair on fait correspondre plusieurs caractères dans le texte chiffré.
**Par exemple**, le caractère '**a**' lui correspond les caractères suivants : 2, 13, 45 ou 22.

# SUBSTITUTION PAR POLYGRAMME

La substitution par polygrammes est un chiffre pour lequel les caractères sont chiffrés par blocs.
**Par exemple,** «aba» peut être chiffré par «rtq» tandis que «abb » est chiffré par « sll ».

# SUBSTITUTION PAR POLYGRAMME

***Exemple : Substitution par bi-grammes*** (groupes de 2 caractères)
Procède du même principe que la substitution simple. Mais au lieu de chiffrer isolément chaque lettre du texte clair, on découpe celui-ci en groupes de deux lettres ou bi-grammes.

Par exemple le clair "**Colonne ennemie**" se traduit par :

| Co | lo | nn | ee | nn | em | ie |
|---|---|---|---|---|---|---|
| OP | LN | VK | ST | VK | LI | RE |

# SUBSTITUTION PAR BIGRAMME

***a)- Utilisation d'une table – Système de Plyfair***

Introduit en 1854 par les savants anglais L.Playfair et C.Wheatstone, illustre la notion de chiffrement par polygrammes.

- On utilise le carré alphabétique de playfair qui comporte cinq lettres en largeur et cinq lettres en hauteurs.

- Le mot clé est inscrit horizontalement sans répéter aucune lettre puis les lettres restantes sont écrites en respectant leur ordre alphabétique

- On traite le **I** et le **J** comme unique lettre.

## *Système de Plyfair (Exemple)*

Si on prend le mot clé : **SPART**, le carré alphabétique est le suivant :

| | | | | |
|---|---|---|---|---|
| **S** | **P** | **A** | **R** | **T** |
| B | C | D | E | F |
| G | H | IJ | K | L |
| M | N | O | Q | U |
| V | W | X | Y | Z |

Les lettres de chaque paire ne peuvent avoir que trois états. Elles occupent

**1/ La ligne :**
Chacune des lettres est remplacée par celle situé à sa droite.
**Exemple : E D** est remplacé par **F E** ou **T R** par **S T**.

**2/ La colonne :**
Chaque lettre est remplacée par celle qui se trouve au-dessous.
**Exemple : R Q** est remplacé par **E Y** ou **Q Y** par **Y R**.

**3/ Aucune des deux :**
Chaque lettre est remplacée par la lettre qui se trouve à l'intersection de sa ligne et de la colonne de l'autre lettre en respectant l'ordre des paires.
**Exemple : A H** devient **P IJ** ou **S Z** par **T V**.

**4/ Etant donné** que **I** et **J** sont considérés comme la même lettre, une transformation en **IJ** peut être transcrite par **I** ou par **J**, au gré du chiffreur.

## *Système de Plyfair (Exemple)*

**Exemple :** On veut chiffrer le texte "**RENDEZ VOUS A PARIS**" avec la clé **SPART**

| | | | | |
|---|---|---|---|---|
| **S** | **P** | **A** | **R** | **T** |
| B | C | D | E | F |
| G | H | IJ | K | L |
| M | N | O | Q | U |
| V | W | X | Y | Z |

***b)- Utilisation d'une transformation mathématique - Système de Hill***

**Chiffrement :**
(1) : remplacer chaque lettre par son ordre dans l'alphabet : A devient 0, B devient 1,..., Z devient 25.
(2) : grouper les nombres ainsi obtenus par **m** (prenons par exemple **m=2**).
(3) : pour chaque bloc de **m** nombres à coder (**x1x2...xm)**, on calcule le texte codé en effectuant des combinaisons linéaires en utilisant une clé de chiffrement (ici **m=2**).
(4) : pour obtenir les lettres chiffrées **(y1y2…ym)** nous calculons les restes modulo 26 des combinaisons linéaires avec la formule suivante :

$$\begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} \quad mod\ 26$$

Par exemple pour les deux premières lettres **x1x2** Nous aurons :
**Y1=(ax1+bx2) mod 26**
**Y2=(cx1+dx2) mod 26**

**Remarque :** le choix de la clé correspond au choix d'un nombre **m**, et au choix des combinaisons linéaires à effectuer.

***Exemple :*** crypter le mot **ELECTION** avec le **chiffre de Hill**, pour **m=2, a=3, b=5, c=1 et d=2**.

**Etape 1 :** On partage en blocs de 2 lettres : EL EC TI ON.
**Etape 2 :** On remplace les lettres par leur ordre associé : 4-11 | 4-2 | 19-8 | 14-13.
**Etape 3 :** On effectue les combinaisons linéaires pour chaque bloc. Par exemple, pour le premier bloc, où x1=4 et x2=11, on a :

$$\begin{pmatrix} y1 \\ y2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x1 \\ x2 \end{pmatrix} \ \boldsymbol{mod\ 26} = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 4 \\ 11 \end{pmatrix} \boldsymbol{mod\ 26} \rightarrow \begin{pmatrix} y1=3\times4+5\times11=67 \\ y2=1\times4+2\times11=26 \end{pmatrix} \boldsymbol{mod\ 26} \rightarrow \begin{pmatrix} y1 \\ y2 \end{pmatrix}$$
$$= \begin{pmatrix} 67 \\ 26 \end{pmatrix} \boldsymbol{mod\ 26} \rightarrow \begin{pmatrix} y1=15 \\ y2=0 \end{pmatrix} \rightarrow \begin{pmatrix} y1=P \\ y2=A \end{pmatrix}$$

De même, y3=22, y4=8, y5=97, y6=35, y7=107, y8=40.
Les modulos sont respectivement (15, 0, 22, 8, 19, 9, 3, 14).

**Etape 4 :** On reconvertit en lettres, pour trouver PAWITJDO.

| Lettres | E | L | E | C | T | I | O | N |
|---|---|---|---|---|---|---|---|---|
| Rangs (Xi) | 4 | 11 | 4 | 2 | 19 | 8 | 14 | 13 |
| Rangs chiffrés (Yi) | 15 | 0 | 22 | 8 | 19 | 9 | 3 | 14 |
| Lettres chiffrées | P | A | W | I | T | J | D | O |

**Déchiffrement**

Pour déchiffrer, le principe est le même que pour le chiffrement: on prend les lettres deux par deux, puis on les multiplie par ***l'inverse de la matrice de chiffrement.***

$$\begin{pmatrix} x_i \\ x_i \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} \quad mod\ 26$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

**Exemple :** Déchiffrer le mot précédemment chiffré PAWITDJO.

**Etape 1 :** On partage en blocs de 2 lettres : PA WI TJ DO.

**Etape 2 :** On remplace les lettres par leur ordre associé : 15-0 | 22-8 | 19-9 | 3-14.

**Etape 3 :** On calcule la matrice de déchiffrement (mod 26)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} mod\ 26 = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}^{-1} mod\ 26 = \frac{1}{3.2 - 5.1}\begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix} mod\ 26 = \frac{1}{1}\begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix} mod\ 26$$

**Alors :**

$$\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}^{-1} mod\ 26 = \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix} mod\ 26 = \begin{pmatrix} 2 & 21 \\ 25 & 3 \end{pmatrix}$$

**Etape 4 :** On effectue les combinaisons linéaires pour chaque bloc. Par exemple, pour le premier bloc, où y1=15 et y2=0, on a :

$$x_1 = (2 \times 15 + 21 \times 0) \bmod 26 = 30 \bmod 26 = 4$$
$$x_2 = (25 \times 15 + 3 \times 0) \bmod 26 = 375 \bmod 26 = 11$$

$$x_3 = (2 \times 22 + 21 \times 8) \bmod 26 = 212 \bmod 26 = 4$$
$$x_4 = (25 \times 22 + 3 \times 8) \bmod 26 = 574 \bmod 26 = 2$$

$$x_5 = (2 \times 19 + 21 \times 9) \bmod 26 = 227 \bmod 26 = 19$$
$$x_6 = (25 \times 19 + 3 \times 9) \bmod 26 = 502 \bmod 26 = 8$$

$$x_7 = (2 \times 3 + 21 \times 14) \bmod 26 = 300 \bmod 26 = 14$$
$$x_8 = (25 \times 3 + 3 \times 14) \bmod 26 = 117 \bmod 26 = 13$$

**4 11 4 2 19 8 14 13 = ELECTION**