

# TP - Chiffrement – Principes

## SIO 1 – BLOC 3 –Cybersécurité

### Exo. 1 : Le carré de Polybe

C'est une **technique de chiffrement par substitution** ancienne, décrite pour la première fois vers 150 av. J.-C. par l'historien grec Polybe. Celle-ci a été utilisée par plusieurs civilisations de différentes manières tout au long de l'histoire. (source : [https://fr.wikipedia.org/wiki/Carr%C3%A9\\_de\\_Polybe](https://fr.wikipedia.org/wiki/Carr%C3%A9_de_Polybe) )

Un **chiffrement par substitution** consiste à remplacer une lettre du message clair par une autre.

**Principe** : les lettres de l'alphabet sont placées en ordre alphabétique dans un tableau dont chaque ligne et chaque colonne sont numérotées.

Ensuite, pour chiffrer un mot, il faut trouver la paire de numéros correspondant à chaque lettre. Le premier chiffre est le numéro de la ligne et le second celui de la colonne.

Exemple : A => 11      B => 12      F => 21

**Q.1.1 - Travail à faire** : chiffrer le message suivant :

F          A          C          I          L          E

**Q.1.2 - Travail à faire** : déchiffrer le message suivant :

22          11          22          33          15

#### Ajout d'une clé

Le moyen le plus simple pour renforcer cette méthode de chiffrement est d'ajouter une clé.

Par exemple, le carré de Polybe avec la clé WIKIPEDIA est représenté par l'image ci-contre.

**Q.1.3 - Travail à faire** : déchiffrer le message suivant avec la clé WIKIPEDIA :

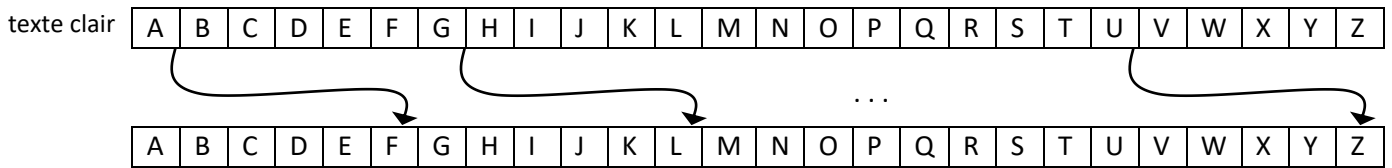
14          41          33          54          23          15

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

## Exo. 2 : Code César

Pour rappel : le code César (ou chiffrement par décalage) est une méthode de chiffrement très simple utilisée par Jules César. Chaque lettre de l'alphabet est remplacée par une autre obtenue par un décalage de l'alphabet, par exemple de 5 lettres :



Chiffrer le message "hello world" à l'aide du chiffrement César (par décalage) et de la clé **C = 5**.

Texte clair : . . .

Texte chiffré : . . .

## Exo. 3 : Casser le code César par analyse fréquentielle

La **cryptanalyse** est la branche de la cryptographie qui étudie la manière de casser des codes.

Dans la cryptanalyse, l'**analyse fréquentielle** se base sur la fréquence d'apparition des lettres dans le message chiffré.

Le tableau suivant présente la fréquence moyenne d'apparition des lettres dans un texte en Français (en %) :

| A    | B   | C    | D   | E     | F    | G   | H    | I    | J    | K | L    | M    |
|------|-----|------|-----|-------|------|-----|------|------|------|---|------|------|
| 7,68 | 0,8 | 3,32 | 3,6 | 17,76 | 1,06 | 1,1 | 0,64 | 7,23 | 0,19 | 0 | 5,89 | 2,72 |

| N    | O    | P    | Q    | R    | S    | T   | U    | V    | W | X    | Y    | Z    |
|------|------|------|------|------|------|-----|------|------|---|------|------|------|
| 7,61 | 5,34 | 3,24 | 1,34 | 6,81 | 8,23 | 7,3 | 6,05 | 1,27 | 0 | 0,54 | 0,21 | 0,07 |

**Q.3.1** – d'après ce tableau, quelle est la lettre la plus fréquente en Français ? . . .

On vous donne le texte suivant, chiffré par la méthode César :

Q J J J X Y Y W J X K W J V Z J S Y

**Q.3.2** – Quelle lettre apparaît le plus dans cette phrase chiffrée ? . . .

**Q.3.3** – En supposant que cette lettre corresponde au E, pouvez-vous en déduire la clé ? (= le nombre de lettres de décalage)

. . .

**Q.3.4** – Déchiffrer le texte chiffré (reproduit ci-dessous) :

Q J J J X Y Y W J X K W J V Z J S Y

. . .

## Exo. 4 sur PC : Déchiffrer le code César avec un outil

Travail à faire :

1) Aller sur le site :

<https://www.apprendre-en-ligne.net/crypto/cesar/index.html>

2) Déchiffrer le texte de l'exercice 3, afin de vérifier qu'on ne s'est pas trompé :

QJJJXYYWJXKWJVZJSY

3) Sur le même site, déchiffrer le message « *rg bok kyz hkr rk* » sachant qu'il est chiffré par décalage.  
Indice : la clé est comprise entre 1 et 9.

Qu.4.1 – Quelle est la clé ? . . .

Qu.4.2 – Quel est le message clair ? . . .

## Exo. 5 sur PC : Casser un code César par analyse fréquentielle

Travail à faire :

Qu.5.1 - Ouvrir l'outil : <http://www.cryptage.org/outil-crypto-frequences.html>

Qu.5.2 - déchiffrer le message suivant (qui a été chiffré par substitution César)

bwfwmakhsksjjanwsvwujqhlwj uwewkksyw

Qu.5.3 – D'après le site, dans ce message chiffré, quelles sont les 3 lettres les plus fréquentes et leurs fréquences ?

. . .

Qu.5.4 - Quelle lettre correspond à la lettre 'E' (qui est la plus fréquente en Français) : . . .

Qu.5.5 - En déduire la clé de chiffrement : . . .

Qu.5.6 – Aller sur le site : <https://www.apprendre-en-ligne.net/crypto/cesar/index.html>

afin de déchiffrer le message chiffré ( bwfwmakhsksjjanwsvwujqhlwj uwewkksyw ).

Qu.5.7 – Quel était le message en clair ? . . .

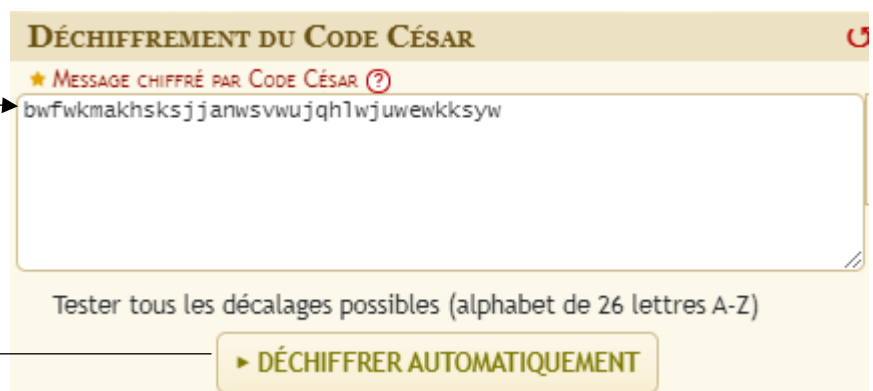
Qu.5.8 – Aller sur le site : <https://www.dcode.fr/chiffre-cesar>

et casser directement le message chiffré.

saisir le texte chiffré

Cliquer. Le résultat apparaît à gauche.

Qu.5.9 – Est-ce que vous retrouvez le texte clair ? . . .



## Exo. 6 : Chiffrement avec OU Exclusif

Le **OU Exclusif (XOR)** est un opérateur logique dont voici la table :

| Table de vérité de XOR |   |                  |
|------------------------|---|------------------|
| A                      | B | $R = A \oplus B$ |
| 0                      | 0 | 0                |
| 0                      | 1 | 1                |
| 1                      | 0 | 1                |
| 1                      | 1 | 0                |

Le résultat vaut 1 si **l'une et une seule** des propositions A OU B vaut 1.

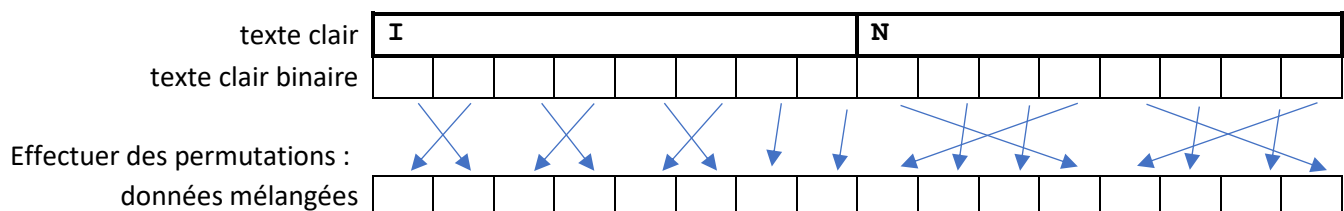
Il est utilisé dans les algorithmes de chiffrement modernes comme AES.

**But :** on veut chiffrer le texte **IN**

- le code ASCII du I est 73 et celui du N est 78

- la clé est 01010110

**Travail à faire :**



XOR avec la clé :

clé 

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

texte chiffré 

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

**Déchiffrement :**

XOR avec la clé :

clé 

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

données mélangées 

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

Faire permutations inverses :

texte clair binaire 

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

texte clair 

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|