**TP - Chiffrement – Principes**

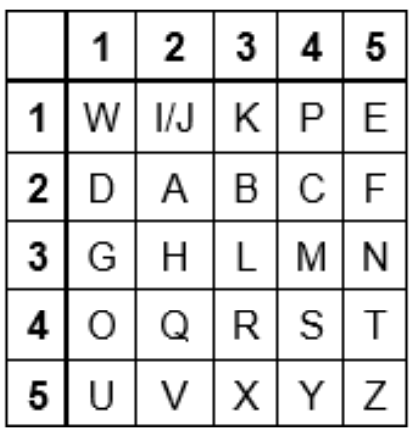
**Exo. 1 : Le carré de Polybe**

technique de chiffrement par substitution, décrite pour la première fois vers 150 av. J.-C par l’historien grec Polybe

Ce chiffrement consiste à remplacer une lettre du message clair par une autre

| clair | chiffré |
| --- | --- |
| FACILE | 21 11 13 24 31 15 |

| chiffré | clair |
| --- | --- |
| 22 11 22 33 15 | gagne |



Exemple d'ajout d’une clé, WIKIPEDIA dans cet exemple

| chiffré | clair |
| --- | --- |
| 14 41 33 54 23 15 | POLYBE |

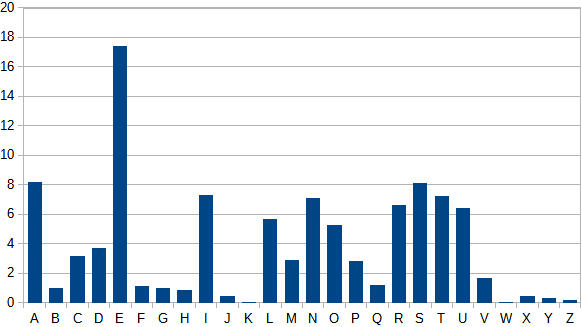
**Exo. 2 : Code César**

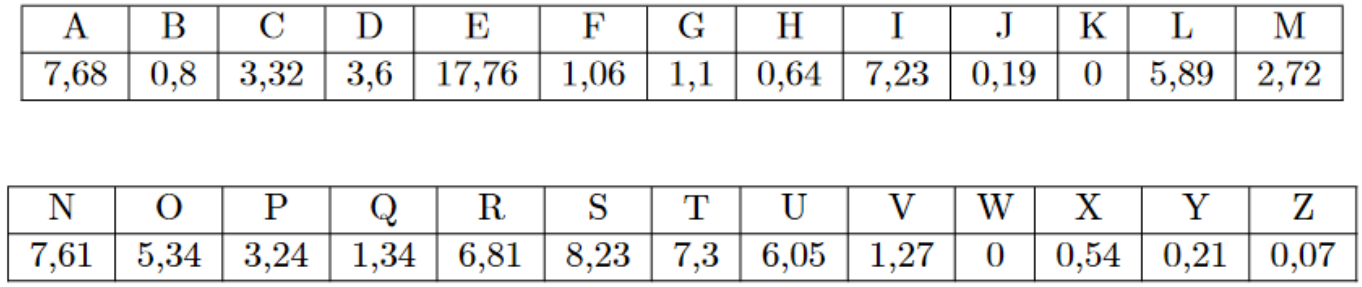
chiffrement par décalage, méthode utilisée par Jules César. Chaque lettre de l’alphabet est remplacée par une autre obtenue par un décalage de l’alphabet

| Clair (clé 5) | chiffré |
| --- | --- |
| Hello world | Mlqqt btwqi |

**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.

****

****

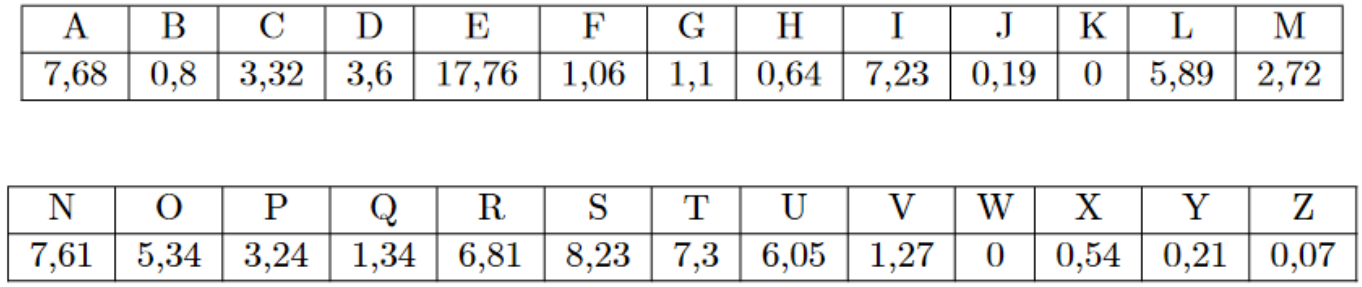
La lettre E est la plus fréquente

La lettre J apparaît le plus dans cette phrase, on peut conclure que la clé peut etre 5 afin de superposer la lettre E avec J dans l’ordre alphabétique.

| chiffré | clair |
| --- | --- |
| Q J J J X Y Y W J X K W J V Z J S Y | Le e est tres frequent |

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

Lien référence: [Chiffre de César (apprendre-en-ligne.net)](https://www.apprendre-en-ligne.net/crypto/cesar/index.html)

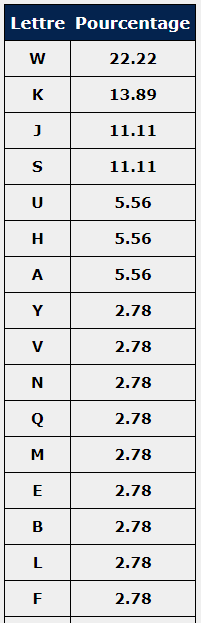
****

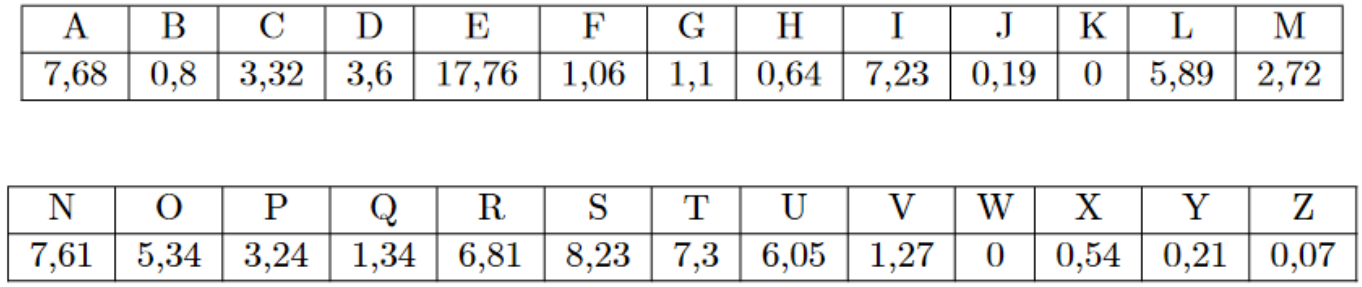
| Chiffré (clé 6) | clair |
| --- | --- |
| rg bok kyz hkrrk | LA VIE EST BELLE |

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

Lien référence: [Outil : analyse des fréquences (cryptage.org)](https://www.cryptage.org/outil-crypto-frequences.html)

| Chiffré (clé 6) | clair |
| --- | --- |
| Bwfwkmakhsksjjanwsvwujqhlwjuwewkksyw | JE NE SUIS PAS ARRIVÉ À DÉCRYPTER CE MESSAGE |

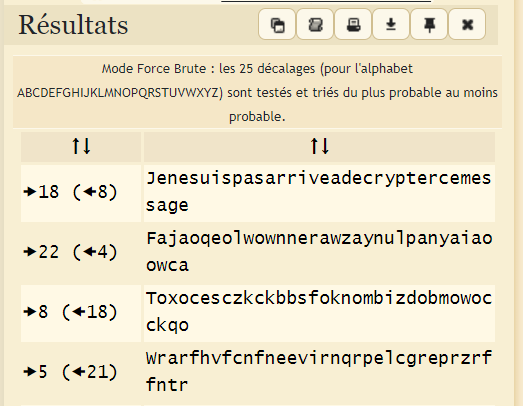
****

****

On conclut que la lettre w est la plus fréquente, on va donc la superposer avec la lettre E. les 3 lettres les plus fréquentes sont: w, k, j

La clé de chiffrement est: 18

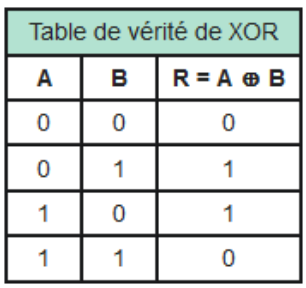
Lien référence 2: [Code Cesar - Chiffre de César - Déchiffrer, Coder, Décoder en Ligne (dcode.fr)](https://www.dcode.fr/chiffre-cesar)

****

Affiche les possibilités

**Exo. 6 : Chiffrement avec OU Exclusif**

Le OU Exclusif (XOR) est un opérateur logique



Utilisé dans les algorithmes de chiffrement modernes

Le text qu’on veut chiffré “IN”

Clé 01010110

| **Chiffrement** | I | | | | | | | | N | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Texte clair | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| clé | **0** | **1** | **0** | **1** | **0** | **1** | **1** | **0** | **0** | **1** | **0** | **1** | **0** | **1** | **1** | **0** |
| Texte chiffré | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |

Le texte chiffré ne correspond pas forcément à des lettres

| Texte chiffré | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| clé | **0** | **1** | **0** | **1** | **0** | **1** | **1** | **0** | **0** | **1** | **0** | **1** | **0** | **1** | **1** | **0** |
| Texte clair | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| **Déchiffrement** | I | | | | | | | | N | | | | | | | |