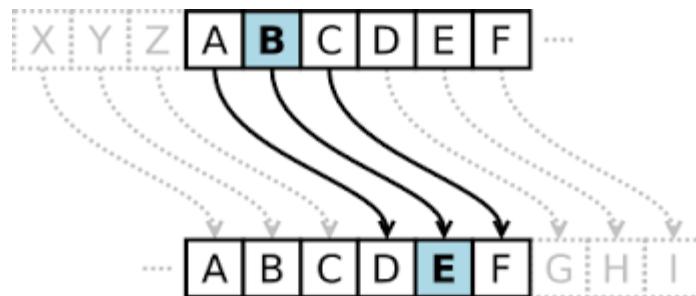


Le chiffrement de CEASAR (ou chiffrement de César) est l'une des méthodes de chiffrement les plus simples et connues. Il s'agit d'un chiffrement par substitution où chaque lettre dans le texte en clair est décalée d'un certain nombre de places dans l'alphabet.



Principe du chiffrement de César :

1. **Clé** : Un entier positif n , qui représente le nombre de décalages.
2. **Chiffrement** : Pour chaque lettre du texte, remplacez-la par la lettre située n positions plus loin dans l'alphabet. Si on atteint la fin de l'alphabet, on revient au début.

Exemple :

- **Texte en clair** : BONJOUR
- **Clé** : 3
- **Texte chiffré** : ERQMRAU (chaque lettre a été décalée de 3 positions vers la droite)

Formule mathématique :

Si on utilise l'alphabet de 26 lettres, la formule pour chiffrer une lettre x est :
 $E(x) = (x + n) \bmod 26$ où x est la position de la lettre (0 pour A, 1 pour B, etc.) et n est la clé de décalage.

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

Déchiffrement :

Le déchiffrement se fait en décalant chaque lettre de n positions vers la gauche : $D(x) = (x - n + 26) \bmod 26$

Exemple de code en Python :

Cliquer sur le fichier [chiffrement de César.py](#)

