**Chiffre de César (ou chiffrement par décalage)**

Définition (source Wikipédia) :

*En cryptographie, le chiffrement par décalage, aussi connu comme le chiffre de César (ou le code de César) est une méthode de chiffrement très simple utilisée par Jules César dans ses correspondances secrètes.*
*Le texte chiffré s'obtient en remplaçant chaque lettre du texte en clair original par une lettre à distance fixe, toujours du même côté, dans l'ordre de l'alphabet.*
*Pour les dernières lettres (dans le cas d'un décalage à droite), on reprend au début.*

*Par exemple avec un décalage de 3 vers la droite, A est remplacé par D, B devient E, et ainsi jusqu'à W qui devient Z, puis X devient A etc. Il s'agit d'une permutation circulaire de l'alphabet.*

*La longueur du décalage, 3 dans l'exemple évoqué, constitue la clé du chiffrement qu'il suffit de transmettre au destinataire — s'il sait déjà qu'il s'agit d'un chiffrement de César — pour que celui-ci puisse déchiffrer le message.*

*Dans le cas de l'alphabet latin, le chiffre de César n'a que 26 clés possibles (y compris la clé nulle, qui ne modifie pas le texte).*

Exercice à réaliser

- Faire saisir un message
- Demander s'il s'agit d'un message en clair ou s'il est chiffré
- Faire saisir le décalage souhaité (nombre de caractères de décalage)
- Faire saisir le sens du décalage (ordre alphabétique ou ordre alphabétique inverse)
- Vous pouvez également choisir de faire saisir un décalage négatif à la question précédente et donc ne pas faire saisir de sens
- Faire le décalage et afficher le message après décalage