Cryptologie et code de César

La cryptologie est la "science du secret", et regroupe deux branches : d'une part, la cryptographie, qui permet de coder les messages, et d'autre part, la cryptanalyse, qui permet de les décoder.

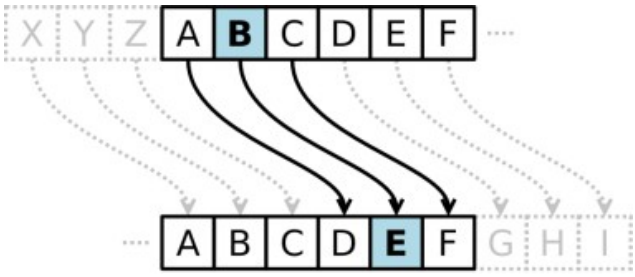
La cryptographie est un mot désignant l'ensemble des techniques permettant de chiffrer (coder) des messages. Le but est de rendre illisible un message codé pour une personne qui n'a pas la clé.

On utilise la cryptographie dans la vie de tous les jours, par exemple pour l'achat sur Internet (ton navigateur affiche un cadenas dans la barre d'adresse) ou via l'utilisation de cartes de crédit, cartes sans contact, ou de téléphones.

De l'Antiquité, Jules César, transmettait des messages secrets en utilisant un système de codage appelé le chiffre de César.

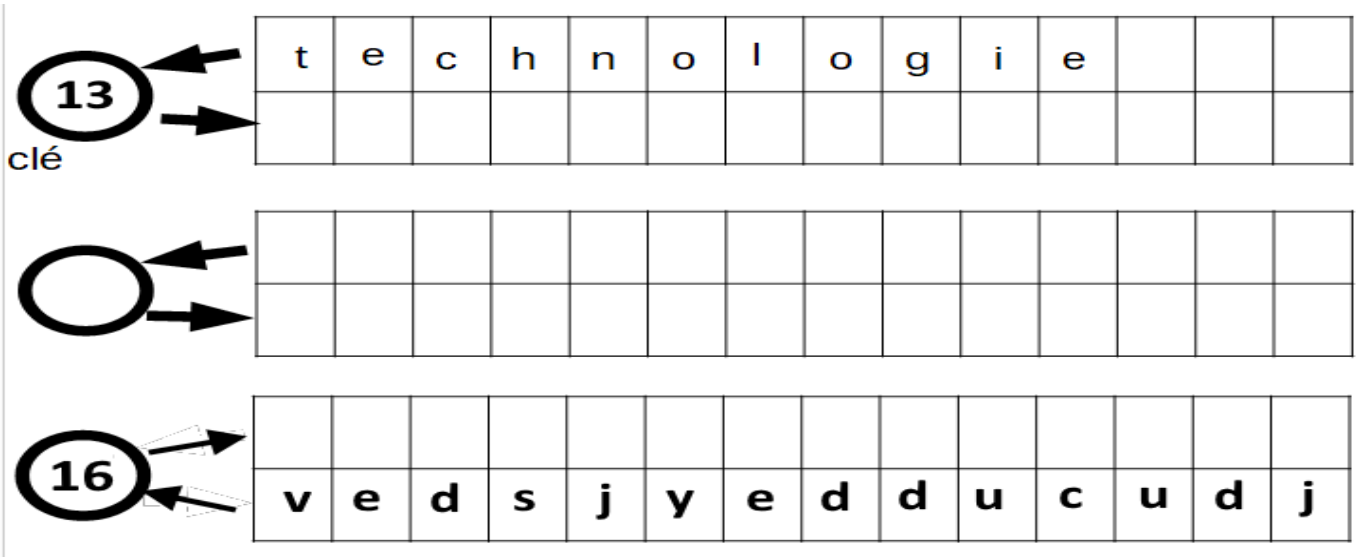
Le chiffre de César fonctionne par décalage des lettres de l'alphabet.
Ce codage consistait à décaler chaque lettre de l'alphabet de plusieurs rangs vers la droite (ou la gauche pour décoder).

La longueur du décalage, 3 dans l'exemple, constitue la clé du chiffrement qu'il suffit de transmettre au destinataire . Il y a une distance de 3 caractères, donc B devient E dans le texte codé.



Le texte chiffré s'obtient en remplaçant chaque lettre du texte 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.

Source wikipédia, article Chiffrement par décalage
https://fr.wikipedia.org/wiki/Chiffrement_par_décalage

Source Tice Education, article Comprendre les principes de base de la cryptographie
https://www.tice-education.fr/

Exercices : à l'aide des tableaux ci-dessous, encoder le mot technologie avec une clé de 13, ensuite votre Nom avec la clé de votre choix. Pour terminer, décoder le mystérieux message