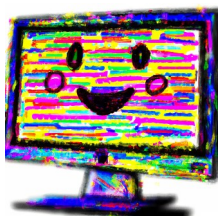
Des énigmes… pour découvrir l'informatique !

LA SEMAINE </>NSI



Énigme 02 (première partie)

Cybersécurité et chiffrement

Les **objets du numérique**, qu'ils soient matériels (ordinateurs, smartphones, objets connectés, réseaux informatiques) ou immatériels (logiciels, données, systèmes d'information), sont de plus en plus souvent la **cible d'attaques**.
Le domaine de la **cybersécurité** développe des méthodes en amont pour éviter ou détecter de tels actes malveillants.
Les défis qu'il soulève représentent un **enjeu majeur** aussi bien au niveau scientifique et technologique qu'au niveau sociétal, économique, politique et militaire.

Chiffrement des données

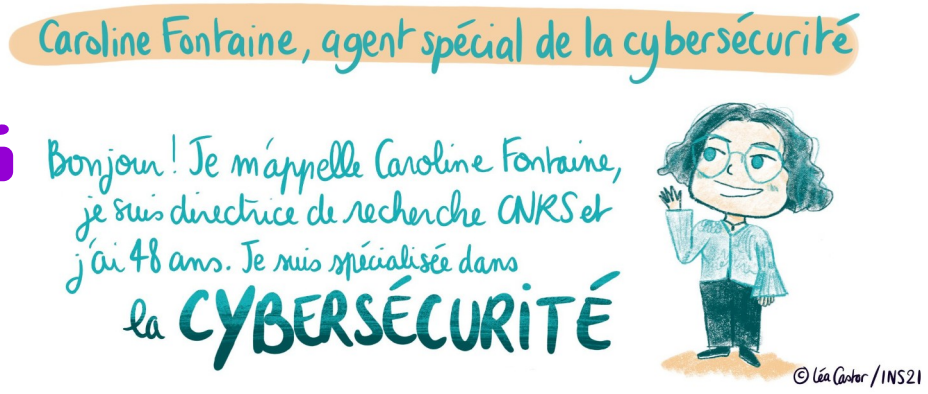
Pour protéger la confidentialité de nos données, il est nécessaire de les **chiffrer**, c'est-à-dire de les transformer en une suite de caractères incompréhensibles par celui qui s'en emparerait.
Des méthodes de chiffrement sont utilisées depuis l'antiquité, et l'une des utilisations les plus célèbres pour cette époque est le chiffre de César, nommé en référence à Jules César qui l'utilisait pour ses communications secrètes (voir encadré ci-contre).

🔍 Code à trouver 🔍

Le code de la première partie de cette énigme est le nom de la seconde option choisie par Caroline Fontaine lors de ses études en maths-info à l'université de Saclay, suivi de la phrase à décrypter ci-dessous qui a été chiffrée avec la méthode du chiffre de César :

WSBZ KL TPEPAL LU ZJPLUJLZ

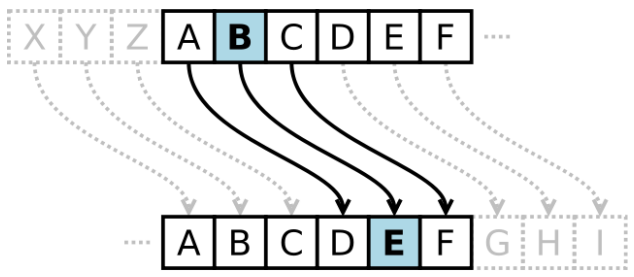
Attention, on supprimera les espaces dans le code attendu. Exemple de réponse : *bioinformatiqueUNEPHRASEMYSTERE*



Voir son portrait en BD ci-contre

Chiffre de César

Il s'agit d'un chiffrement par décalage. On définit un nombre correspondant au décalage à effectuer dans l'alphabet pour remplacer chaque lettre. Ce nombre s'appelle la clé du codage.
Par exemple, avec un décalage de 3 vers la droite, A est remplacé par D, B par E,…, Z par C.



Avec cette clé de codage égale à 3, le mot INFORMATIQUE devient LQIRUPDWLTXH.
On peut bien sûr déchiffrer le message codé facilement si on connaît la clé : ici, un décalage de 3 mais vers la gauche et le tour est joué !

La méthode du chiffre de César **n'est pas infaillible** ! En effet, il n'y a au pire que 26 clés à tester pour décrypter un message codé. Et mieux : il peut très facilement être « cassé » par analyse de fréquences. Par exemple, pour un message écrit en français, il y a de fortes chances que la lettre qui apparaît le plus souvent corresponde à la lettre E...

Les méthodes de chiffrement actuelles sont bien plus sophistiquées que le chiffre de César, en particulier elles assurent qu'une personne qui n'a pas la clé de chiffrement ne puisse pas comprendre le message.

Crédits images : haut droite : Léa Castor/INS2I, milieu : Cepheus, domaine public, icônes : https://uxwing.com/