

Cryptographie

La cryptographie consiste à protéger les informations en les transformant avec des algorithmes pour qu'elles deviennent illisibles sans la clé appropriée (assurant confidentialité, authenticité et intégrité). Elle est utilisée pour sécuriser les messages, les transactions ou les données personnelles sur Internet. Les méthodes peuvent être symétriques (même clé pour chiffrer et déchiffrer) ou asymétriques (clé publique pour chiffrer, clé privée pour déchiffrer).

Pour ce petit résumé je parle chiffrement de César. Technique de cryptographie classique consistant à décaler chaque lettre d'un texte d'un certain nombre de positions dans l'alphabet.

Illustration visuelle du décalage

Texte clair : H E L L O

Décalage +3 : K H O O R

Alphabet : 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
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Exemple de code en python :

```
def chiffrer_cesar(texte, decalage):  
    resultat = ""  
    for lettre in texte:  
        if lettre.isalpha():  
            valeur = (ord(lettre.lower()) - ord('a') + decalage) % 26  
            resultat += chr(ord('a') + valeur)  
    return resultat
```

```
def dechiffrer_cesar(texte_chiffre, decalage):  
    return chiffrer_cesar(texte_chiffre, -decalage)
```

```
texte_clair = "hello"  
decalage = 3
```

```
texte_chiffre = chiffrer_cesar(texte_clair, decalage)  
texte_dechiffre = dechiffrer_cesar(texte_chiffre, decalage)
```

```
print("Texte clair :", texte_clair)  
print("Texte chiffré (+3) :", texte_chiffre)  
print("Texte déchiffré :", texte_dechiffre)
```

Sur la condition FOR on Boucle sur chaque caractère du texte a traiter chaque lettre individuellement.

On vérifie si le caractère est une lettre.

Conversion de la lettre en nombre :

- `ord(lettre.lower())` → donne la valeur Unicode de la lettre.
- `ord('a')` → valeur Unicode de a pour calculer l'index 0-25.
- + décalage → applique le décalage pour chiffrer.
- `% 26` → modulo pour revenir au début de l'alphabet si on dépasse Z.

Reconstruit la lettre chiffrée à partir de la valeur numérique.

Ajoute cette lettre (minuscule) à la chaîne résultat.

Le déchiffrement utilise le décalage inverse (-décalage) pour retrouver le texte original soit disant de chiffrer avec +3 → déchiffrer avec -3.