# TP 12 : cryptographie

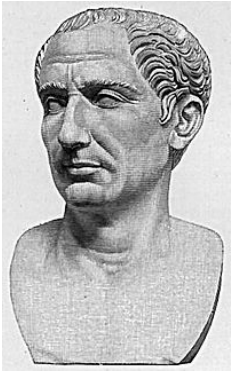
La cryptographie est un domaine de l'informatique très développé de nos jours. Afin d'assurer la confidentialité et l'intégrité des données échangées, il est très commun de crypter ces données en utilisant un code et une clef de chiffrement. Les domaines d'application sont très larges : informations militaires, données bancaires, respect de la vie privée… Dans de TP, vous allez découvrir les bases de la cryptographie. Nous nous contenterons de chiffrer des messages sous la forme de chaines de caractères. Ainsi, il paraît nécessaire dans un premier temps de se familiariser avec ce type d'objet : `str`.

Les chaines de caractères sont de type `str` en Python : ce sont des **séquences itérables non modifiables**. Voici les opérations de base que nous pouvons réaliser sur les chaines de caractère :

- itération : on peut écrire `for c in string` pour parcourir la chaine;
- accès à un élément (caractère) par son indice dans la chaine `s[2]` **en commençant par 0** ;
- le nombre de caractère est obtenu avec la methode `len(s)` ;
- concaténation avec l'opérateur + ;
- transformation d'une chaine en liste et inversement : `l=list(s)` et `s="".join(l)` ;
- mise en majuscule avec `s.upper()` ;
- utilisation de chaines de plusieurs lignes en les encadrant de 3 guillemets simples ou doubles ;
- remplacement d'une sous-chaine avec `string.replace()` ;
- présence d'une sous-chaine dans une chaine : l'expression `"salut" in "salut tout le monde"` est un booléen `True`.

Dans toutes les activités, nous chiffrerons et déchiffrerons **uniquement les lettres en majuscules** présentes dans les messages.

## Le chiffrement de César



Le principe de ce système de chiffrement est simple. Chaque lettre du message subi un décalage dans l'alphabet. Le décalage, positif ou négatif, peut être considéré comme la clef de chiffrement. Par exemple, le message suivant est crypté avec un décalage de +3 :

`I WAS BORN IN A CROSSFIRE HURICANE` devient

`L ZDV ERUQ LQ D FURVVILUH KXULFDQH`

Evidemment, si l'on re-chiffre avec un décalage de -3, le message revient comme à l'origine. Nous considérerons que l'alphabet est cyclique et il est d'usage de ne chiffrer que les lettres majuscules. Les autres caractères devront rester inchangés dans le message.

1. Ecrire une fonction `creer` qui à partir d'une chaine de caractère renvoie une liste contenant tous les éléments ordonnés de la chaine. Tester cette fonction pour obtenir une liste de toutes les lettres de l'alphabet en majuscule.

```
creer('ABCDEFGHIJKLMNOPQRSTUVWXYZ')
```

doit renvoyer

```
['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']
```

2. Ecrire une fonction `trouver` qui à partir d'une lettre et d'une chaine de caractère renvoie l'indice de la lettre dans la chaine ou -1 si la lettre n'est pas présente dans la chaine.

```
trouver('A','SAlut')
```

doit renvoyer

```
1
```

3. Ecrire une fonction `decaler` qui à partir d'une chaine et d'une valeur de décalage renvoie une liste décalée des caractères de la chaine. Tester votre fonction avec un décalage de +3 puis de -3 pour obtenir une liste décalée des lettres de l'alphabet.

```
decaler('ABCDEFGHIJKLMNOPQRSTUVWXYZ',3)
```

doit renvoyer

```
['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']
```

*Indice : le problème ici est qu'en décalant l'indice de parcours de la chaine, on « sort » de la chaine. Il faut donc utiliser la fonction modulo : %.*

4. Ecrire une fonction `cesar` qui à partir d'une chaine de caractère et d'un décalage renvoie la chaine cryptée à l'aide du chiffrement de César.

```
cesar('I WAS BORN IN A CROSSFIRE HURICANE',3)
```

doit renvoyer

```
L ZDV ERUQ LQ D FURVVILUH KXULFDQH
```

*Séquence à suivre :*

- *créer l'alphabet ;*
- *décaler l'alphabet ;*
- *en parcourant la chaine de caractère, trouver la lettre dans l'alphabet non décalé ;*
- *ajouter à une liste la lettre de l'alphabet décalé ;*
- *convertir la liste en chaine de caractère.*

5. Pour valider vos fonctions, faire les tests suivants :

`cesar('ALEA JACTA est',2)` doit renvoyer `CNGC LCEVC est`

`cesar("BONJOUR",2)` doit renvoyer `DQPLQWT`

6. Pour terminer, écrire un programme qui décrypte le message suivant en essayant de trouver le décalage (*indice : il est compris entre 15 et 20*):

```
XBHUK WHUAYHNYBLS MBA UL XBP MBA IPLU LIHOP LA WLYWSLEL JL MBA NHYNHUABH
ZVU WLYL JHY CVFHUA K BU JVAL ZH MLTTL IHKLILJ TVYAL LA KL S HBAYL ZVU
MPSZ WHUAHNYBLS UL AHUA ILHB LA AHUA NYHUK UL ZHCHPA XBL KPYL UP XBL MHPYL
LA SL KVBAL XBP AYVBISHPA ZVU LUALUKLTLUA LAHPA H ZHCVPY Z PS KLCHPA
WSLBYLY WVBY SL KLBPS KL ZH MLTTL VB YPYL WVBY SH QVPL KL ZVU MPSZ
```

Qui en est l'auteur ? Vous pouvez utiliser internet et garder la réponse pour vous.

## Le chiffre de Vigenère

Le chiffre de Vigenère (cryptographe du 16ème siècle) est une méthode de chiffrement permettant de crypter un texte à partir d'une clef de chiffrement (mot de passe). Le texte ne pourra être lisible que par la personne possédant la bonne clef. Le chiffre de Vigenère est basé sur le carré de Trithème :

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

Version moderne du carré de Vigenère

Chaque ligne du tableau représente un alphabet décalé. Le résultat du cryptage de N par le caractère S donne F. Ainsi, si l'on définit un mot de passe, par exemple EIFFEL, et si l'on souhaite crypter une phrase simple : on obtient le message codé suivant : `BONJOUR A TOUS` devient `MOXJBUC L TYUF`. Pour coder, on procède de la manière suivante :

- le cryptage de B par E (1ère lettre du mot de passe) est F ;
- le cryptage de O par I (2ème lettre du mot de passe) est M ;
- ...
- le cryptage d'un espace est un espace ;
- le cryptage de A par F (on considère que le mot de passe se répète) est F ;
- .....
- on obtient finalement `FWSOSFV F XZYA`.

Pour décoder, on procède à l'envers à partir du texte crypté.

1. Ecrire une fonction `tritheme` qui à partir d'une lettre renvoie une liste ordonnée contenant toutes les lettres de la ligne du carré de Trithème.

```
tritheme('O')
```

doit renvoyer

```
['O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', 'A', 'B', 'C',
'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N']
```

*Indice : utiliser les fonctions trouver et décaler créées plus haut.*

2. Ecrire une fonction decrypter qui à partir d'un mot de passe et d'une phrase renvoie le message décrypté.

```
decrypter("FWSOSFV F XZYA", "EIFFEL")
```

doit renvoyer

```
BONJOUR A TOUS
```

*Séquence à suivre :*

- *créer la liste cyclique du mot de passe ;*
- *en parcourant la chaine de caractère :*
  - *créer la ligne du tableau de trithème correspondant à la lettre du mot de passe ;*
  - *trouver la lettre à décoder dans cette ligne ;*
  - *ajouter à une liste la lettre de l'alphabet correspondante ;*
- *convertir la liste en chaine de caractère.*

3. Tester vos fonctions avec le texte codé suivant avec la clef `LIEVRE`:

```
AZIIVD LSIT OC QZR LMO PP PDVZCM
```

4. Quel est le titre de ce texte ? Qui en est l'auteur ?