

SIVANATHAN  
NARTHTHANAN

TS1



# CRYPTOGRAPHIE

PROJET INFORMATIQUE ET SCIENCES DU NUMÉRIQUE

RAPPORT

Année Scolaire :

2016-2017

# SOMMAIRE

## I. Présentation

1. Introduction
2. Cahier des charges

## II. Le programme

1. Rapport technique
2. Manuel d'utilisation
3. Les étapes de la démarche

## III. Conclusion

1. Problèmes rencontrés
2. Après le projet

# I. Présentation

## 1. Introduction

La cryptographie est une méthode qui permet de transférer des textes à le destinataire sans que les autres personnes comprennent le vrai sens du texte. Pour que le destinataire comprenne la vraie sens du texte il doit savoir la clé avec laquelle l'expéditeur a crypté le texte. Il y a plusieurs types de cryptage ou décryptage, par exemple César, Vigenère, Affine, RSA, etc. Dans le cas de notre projet on a décidé de programmer trois types de cryptage ou décryptage. Pour faciliter les tâches chacun d'entre nous a décidé de programmer un des trois types de cryptage. ASLAN Serhat occupé du César, MORAUX Brice occupé d'Affine et moi je me suis occupé de Vigenère.

César : Le cryptage avec César c'est le plus facile des cryptages car c'est juste du décalage.

Par exemple : Texte = ABCDE ; Clé = 1 ; Texte décrypté = BCDEF

Vigenère : Le cryptage avec Vigenère c'est une combinaison entre le texte et la clé

Affine : Le cryptage avec affine c'est par des calculs comme  $ax+b$  il faut définir  $a$  et  $b$  pour la clé.

Pendant la seconde guerre mondiale il y a des pays qui ont utilisé la cryptographie pour faire passer les messages à leur allié sans que leur ennemi comprenne leur message.

## 2. Cahier des charges

Cryptage en commun on doit utiliser un dictionnaire, dans notre cas on va utiliser un dictionnaire avec l'alphabet (26 lettres), 0 à 9 chiffres (10 chiffres) et l'espace. Les autres symboles ne sont pas définis dans notre dictionnaire. Donc dans notre dictionnaire on a 37 valeurs qui vont de 0 à 36. Dans le cas de ma partie le cryptage Vigenère on doit associer le texte et la clé.

Par exemple : Texte = BONJOUR ; Clé = MOT

<b>Texte</b>	B	O	N	J	O	U	R
<b>Clé</b>	M	O	T	M	O	T	M
<b>Valeur Texte + Valeur Clé</b>	B+M	O+O	N+T	J+M	O+O	U+T	R+T

Puis il faut prendre la valeur combinée entre le texte et la clé puis on va l'affecte a l'inverse dictionnaire. Pour crypte le message et pour décrypte il faut faire l'inverse de cryptage. Sans oublier il faut le modulo le modulo c'est une boucle qui permette de trouve toujours un caractère dans le dictionnaire.

Par exemple : Si on  $21+19 = 40$  et la valeur 40 n'existe pas dans notre dictionnaire donc la valeur du texte décrypte doit toujours trouve un caractère.

Au début l'utilisateur doit définir es qu'il veut crypte ou décrypte puis il doit choisir le type de cryptographie entre César, Vigenère et affine après il doit entrer la clé. Dans cette méthode l'utilisateur a tous sa liberté de choisir son cryptage ou décryptage et leur type.

## II. Le programme

### 1. Rapport technique

Dans ce rapport technique on va séparer la Programme en deux parties. La première partie est celle du programme en commun et l'autre partie est celle du programme qui concerne Vigenère.

Partie n°1 :

Programme dictionnaire :

```

dico = {}
for i in range (65,91):
    dico[chr(i)]= i-65
dico[" "] =26
for i in range(10):
    dico[str(i)]=i+27

return dico

```

Il y a 37 valeur dans ce dictionnaire les alphabet, espace et les chiffres de 0 à 9. Chaque caractère a sa valeur dans le dico. Pour mieux comprendre la fonction de dico on va le représente sous la forme d'un tableau.

TABLEAU DICTIONNAIRE										
Caractère	'A'	'B'	'C'	'D'	'E'	'F'	'G'	'H'	'I'	'J'
Valeur Cara	0	1	2	3	4	5	6	7	8	9
Caractère	'K'	'L'	'M'	'N'	'O'	'P'	'Q'	'R'	'S'	'T'
Valeur Cara	10	11	12	13	14	15	16	17	18	19
Caractère	'U'	'V'	'W'	'X'	'Y'	'Z'	'espace'	'o'	'1'	'2'
Valeur Cara	20	21	22	23	24	25	26	27	28	29
Caractère	'3'	'4'	'5'	'6'	'7'	'8'	'9'			
Valeur Cara	30	31	32	33	34	35	36			

Programme inverse dictionnaire :

```

inversDico = dict((dico[i],i)for i in dico)

return inversDico

```

Dans le cette fonction on va faire l'inverse de dictionnaire donc les caractères vont transforme en valeur du caractère et les valeurs du caractère vont transforme en caractères. Pour comprendre je vais ajouter un tableau comme celui de dictionnaire.

TABLEAU INVERSE DICTIONNAIRE										
Caractère	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'	'8'	'9'
Valeur Cara	A	B	C	D	E	F	G	H	I	J
Caractère	'10'	'11'	'12'	'13'	'14'	'15'	'16'	'17'	'18'	'19'
Valeur Cara	K	L	M	N	O	P	Q	R	S	T
Caractère	'20'	'21'	'22'	'23'	'24'	'25'	'26'	'27'	'28'	'29'
Valeur Cara	U	V	W	X	Y	Z	espace	o	1	2
Caractère	'30'	'31'	'32'	'33'	'34'	'35'	'36'			
Valeur Cara	3	4	5	6	7	8	9			

Programme majuscule :

```
texte = texte.upper()

return texte
```

Cette fonction permet de transformer le texte entré en minuscule en majuscule et le texte entré en majuscule reste majuscule car dans notre dico on a que les valeurs de l'alphabet en majuscule.

Programme texte valeur :

```
liste_nb_correspondante=[]
for caractere in texte:
    liste_nb_correspondante.append(dico[caractere])

return liste_nb_correspondante
```

Cette fonction permet de affecte le caractère du dico sa valeur qui se trouve dans le dictionnaire.

Programme valeur texte inverse :

```

texte_final = []
for number in liste:
    texte_final.append(inversDico[number])

return texte_final

```

Cette fonction permet de affecte le caractère du dico sa valeur qui se trouve dans le l'inverse dictionnaire donc il fait l'inverse le programme que j'aborde précédemment.

Partie n°2 :

Programme boucle clé et sa valeur dico :

```

cle = input("entrez la cle de cryptage")
cle = cle.upper()

longueurPhrase = len(texte)
longueurCle = len(cle)
longueurCleBoucle = list(cle)

Entier=longueurPhrase // longueurCle
Reste=longueurPhrase % longueurCle

p1_Boucle = longueurCleBoucle*Entier
p2_Boucle = longueurCleBoucle[0:Reste]

Boucle = p1_Boucle + p2_Boucle
ValeurCleBoucle = []
for valeur in Boucle:
    ValeurCleBoucle.append(dico[valeur])

return ValeurCleBoucle

```

Cette fonction permet de répète les caractères de la clé au nombre de fois de caractères du texte. Puis pour ce liste on affecte les valeurs du dico.

Programme associé les valeur texte et valeur boucle clé :

```

ValeurCrypte = []
for i in range(len(liste_nb_correspondante)):
    ValeurCrypte.append(liste_nb_correspondante[i]+ValeurCleBoucle[i])

```

Cette fonction associe les valeurs du clé boucle avec les valeurs du texte. Donc on une liste avec ces valeurs combinées. Ceci est la liste des valeurs du texte crypte.

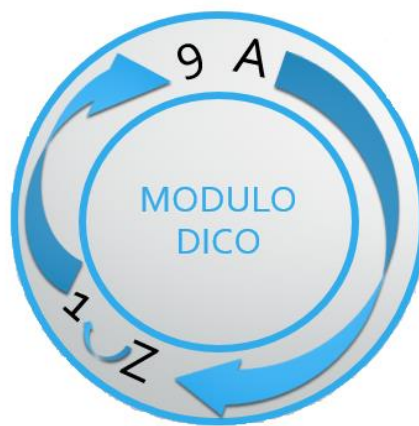


Programme modulo :

```
liste_vigenere = []
for number in range(len(liste_nb_correspondante)):
    liste_vigenere.append(ValeurCrypte[number]%37)

return liste_vigenere
```

Dès que les valeurs de dico dépassent la valeur 36 donc quand la valeur vaut 37 il doit prendre la valeur 0 comme une boucle voire ce schéma :



Programme inverse combination valeur texte et valeur boucle clé / inverse modulo :

```
liste_anti_vigenere = []
for i in range(len(liste_nb_correspondante)):
    nvx_num = liste_nb_correspondante[i] - ValeurCleBoucle[i]
    if nvx_num < 0:
        nvx_num = 37 + nvx_num
    liste_anti_vigenere.append(nvx_num)

return liste_anti_vigenere
```





Cette fonction associe les valeurs du clé boucle avec les valeurs du texte. Donc on a une liste avec ces valeurs combinées. Ceci est la liste des valeurs du texte décrypté. Dès que les valeurs de dico dépassent la valeur 36 donc quand la valeur vaut -1 il doit prendre la valeur 36 comme une boucle voire ce schéma :

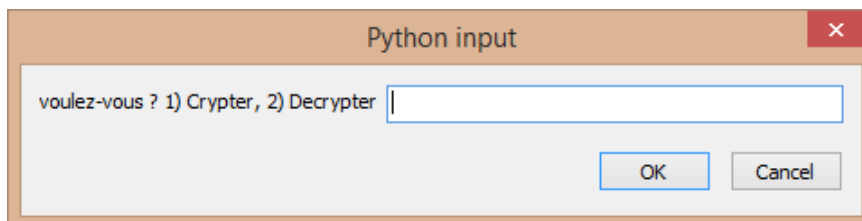




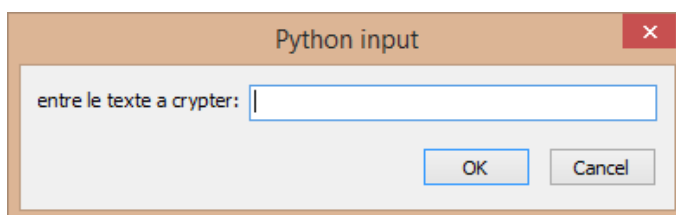
## 2. Manuel d'utilisation

Pour utiliser notre programme :

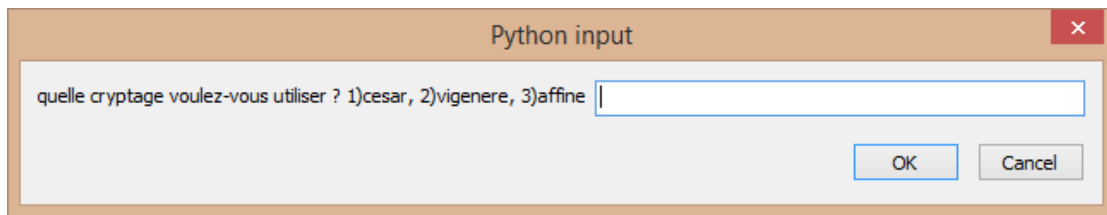
- ✚ Il faut ouvrir le logiciel Edupython 
- ✚ Puis cliquer sur ouvrir 
- ✚ Puis sélectionner   
Cryptographie.py
- ✚ Puis cliquer sur 
- ✚ Puis notre programme va proposer 2 choix (Crypter et Décrypter).



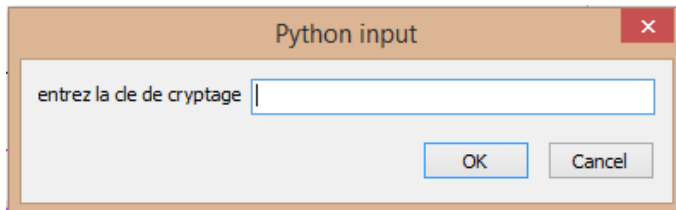
- ✚ Puis il faut entrer le texte à crypter ou décrypter



- ✚ Puis il faut sélectionner le type de cryptage ou décryptage



- ✚ Puis il faut entre la clé



- ✚ Voir le texte crypte ou décrypte

```
*** Console de processus distant Réinitialisée ***
>>>
['N', 'A', 'R', 'T', 'H', 'T', 'H', 'A', 'N', 'A', 'N']
>>>
```

### 3. Les étapes de la démarche

Au début on a décidé repartir le travail. Donc on sait que chaqu'un entre nous aurons une partie équitable. Puis on fait de recherche sur internet pour comprendre le vrai sens du cryptage et décryptage. Puis on fait des recherches sur les différents types de cryptage et décryptage que le professeur nous a conseillé qui sont César, Vigenère et Affine et au même temps il nous a conseillé de crée un dictionnaire au début en commun on crée ce dictionnaire a trois. Puis on a essayé plusieurs fois le cryptage sur des feuilles et trouvé des méthodes ça nous a permis de trouvé des solutions avec de programme sur Edupython.

## III. Conclusion

## 1. Problèmes rencontrés

Au début pour notre projet on voulait crée le jeu othello mais il y'a un autre groupe qui voulait aussi donc on a abandonné le projet mais la fini l'autre groupe aussi a abandonné le projet sur othello. Après avoir abandonné le projet d'othello on voulait faire de la bataille navale mais à la fin ont pensée on aura pas le temps de finir donc à la fin le professeur a proposé des projets au groupes qui n'ont pas idée et ce projet c'est notre professeur qui nous a donné l'idée. Pendant le projet je perdu beaucoup de temps sur les recherche sur internet, et à cause du temps perdu pour choisir notre projet on n'a pas eu le temps de faire l'interface graphique.

## 2. Après le projet

Après le projet je beaucoup de connaissance sue python et ça peut-être utile dans les étude supérieur que je vais faire sue la domaine informatique. Grace à ce projet et celle su Science de l'ingénieur je sais comment présente un projet.

