



## Projet scripting Vigenère :

### Introduction et description :

Dans le cadre du module 122, il vous est demandé de réaliser un projet de Scripting sur le chiffre de Vigenère.

Blaise de Vigenère (1523 – 1596) apporta une amélioration décisive au chiffre de César en utilisant 26 alphabets différents, tous réunis dans un tableau.

Le chiffrement de Vigenère est un chiffrement symétrique par substitution. À la différence que dans cette méthode, il va y introduire la notion de clé. La substitution se fera donc par rapport à la clé.

Pour faire simple :

$\text{TexteChiffré}[i] = (\text{TexteClaire}[i] + \text{Clés}[i]) \text{ modulo } 26$

$\text{TexteClaire}[i] = (\text{TexteChiffré}[i] - \text{Clés}[i]) \text{ modulo } 26$

	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

## Exemple de chiffrement :

Texte : We love crypto

Clé : Yes

TEXT	W	E	L	O	V	E	C	R	Y	P	T	O
Key	Y	E	S	Y	E	S	Y	E	S	Y	E	S
CIPHER	U	I	D	M	Z	W	A	V	Q	N	X	G

## Objectifs :

Les objectifs de ce projet sont les suivants :

- Comprendre et analyser le fonctionnement du chiffre de Vigenère
- Appuyer et décrire les éléments théoriques vus pendant ce module
- Réaliser un script et le faire fonctionner selon les indications
- Réaliser une documentation (max 3 pages) de test afin de prouver le bon fonctionnement de votre script

## Spécifications techniques :

1. Le langage du script doit être en Python
2. Le script doit pouvoir se lancer sans installation particulière
3. La gestion des paramètres s'effectue avec la librairie argparse
4. Le code doit être structuré selon les directives vues en classe
5. Votre chiffrement et déchiffrement doivent prendre en compte les minuscules et les majuscules
6. La gestion des erreurs de saisie doit être prise en compte
7. Directives minimales du script :
  - a. L'utilisateur peut choisir s'il souhaite effectuer un chiffrement ou un déchiffrement.
  - b. L'utilisateur doit spécifier le contenu du fichier à chiffrer, la clé de dé/chiffrement qui sera utilisée et le fichier de sortie où le résultat sera stocké. Ce contenu doit directement être envoyé en argument au script.

```
D:\drive\Epsic\Scripting\python\TP_Vigenere>python main.py --help
usage: main.py [-h] (-c | -d) fichierEntree Clé fichierSortie

positional arguments:
  fichierEntree      Définit le fichier d'entrée qui sera chiffré ou déchiffré
  Clé                Définit la clé qui sera utilisée pour chiffrer ou déchiffrer
  fichierSortie      Définit le fichier de sortie ou le résultat sera stocké

optional arguments:
  -h, --help          show this help message and exit
  -c, --chiffrement    Permet de spécifier l'action de chiffrement
  -d, --déchiffrement  Permet de spécifier l'action de déchiffrement
```

## Travail à effectuer :

### Documentation (max 3 pages) :

1. Explications des fonctions utilisées
2. Documentation sur la lib Argparse
3. Documentation sur la fonction chiffrement + tests
4. Documentation sur la fonction déchiffrement + tests
5. Mini conclusion

### Réalisation :

1. Réaliser le script selon les spécifications techniques
2. Ajouter des commentaires

## Informations sur le rendu :

**Quand** : samedi 16 avril 2022 à 23h55

**Combien** : par binôme

**Quoi** : Me faire parvenir en zippant votre (script + documentation pdf) sur Moodle