

Projet scripting Vigenère:

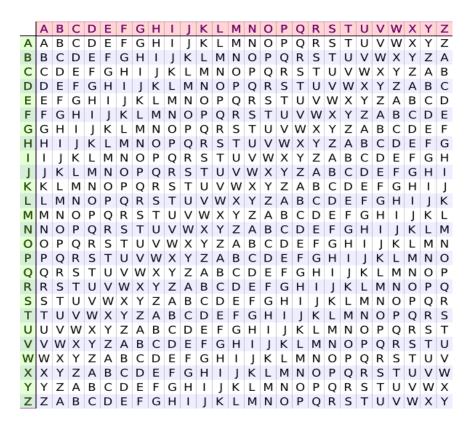
Introduction et description :

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 :

TexteChiffré[i] = (TexteClaire[i] + Clés[i]) modulo 26 TexteClaire[i] = (TexteChiffré[i] - Clés[i]) modulo 26



Yannick Widmer 04.04.2022

Exemple de chiffrement :

Texte: We love crypto

Clé : Yes

TEXT	W	Е	L	0	V	Е	С	R	Υ	Р	Т	0
Key	Υ	Е	S	Υ	Е	S	Υ	Е	S	Υ	E	S
CIPHER	U	1	D	M	Z	W	Α	V	Q	N	Х	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 libraire 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.

Yannick Widmer 04.04.2022

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

Yannick Widmer 04.04.2022