
	Projet 2 Le code de César et de Vigenère Présentation	1 / 1 
---	--	---

1 Présentation

1.1 Objectifs

- Voir projet 1

1.2 Les outils à utiliser

- Programmation : Spyder
- Diaporama de présentation : à l'aide de la suite bureautique de l'ENT et son application powerpoint.

1.3 L'organisation

- Le projet se fait à deux.
- Vous aurez à rendre une certains nombres de fichiers (voir les jalons posés dans les énoncés) ainsi qu'un diaporama commun au groupe

2 Quelques consignes

2.1 Organisation dans le groupe

- Chaque membre du groupe (élève 1 et élève 2) devra traiter ses propres questions. Vous disposez chacun d'un fichier de questionnement,
- Pour les questions communes, vous devrez vous les répartir au sein du groupe,

2.2 Le code python

- Le code doit être structuré en utilisant des fonctions,
- Normalement le nom des variables est donnée mais vous serez peut être amené à en créer,
- Tester les fonctions au fur et à mesure de l'avancée du projet,
- Commenter le code informatique,

2.3 Sauvegardes

- Pensez à faire des sauvegardes régulières et en plusieurs exemplaires de votre travail,

2.4 Tests des programmes ou des portions de programme

Vous pouvez utiliser le site Dcode pour vérifier si le texte codé par votre programme est correct. Voici le lien : <https://www.dcode.fr/chiffre-cesar>

2.5 Diaporama (compte rendu)

- Voir document spécifique.

3 Descriptif

3.1 Code de César

Lors de ses batailles, l'empereur romain JULES CÉSAR cryptait les messages qu'il envoyait à ses généraux. Sa méthode de codage consistait à décaler les lettres de 3 rangs, vers la droite, dans l'alphabet. Cette méthode de cryptage est appelée chiffrement de César, ou Code César. Le nombre de rangs de décalage des lettres est appelé la clé. (JULES CÉSAR employait donc une clé égale à 3).

3.2 Chiffre de Vigenère

Le chiffre de Vigenère est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

3.3 Notion de clé

Une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature). ... La protection apportée par un algorithme de chiffrement est liée à la longueur de la clé, qui peut s'exprimer en bits.