Projet intra - Chiffrement /20

# Durée du projet

Les 3 périodes en classe, 7 heures, de la semaine 11 (7, 8 et 10 novembre) seront allouées pour la réalisation du projet. De plus, vous avez la possibilité de poursuivre le projet en dehors des heures du cours.

# Remise

Votre **projet compressé (.zip)** doit être déposé sur LÉA **à la fin de chaque cours.**

# But du projet

* Faire un plan / pseudo code / organigramme
* Utiliser les conditions
* Utiliser les boucles
* Utiliser les collections
* Utiliser les fonctions
* Utiliser les modules (*import*)

# Chiffrer et déchiffrer une chaîne de caractères

Nicolas veut parler avec son être cher en toute intimité, mais chaque fois qu’il envoie un message sa mère l’intercepte et le lit. Vous, en tant que romantique, voulez l’aider.

Créez pour Nicolas une application qui permet de chiffrer et de déchiffrer des messages.

Votre projet devra contenir 3 fichiers.

* **main.py** : Lance l’exécution du code
* **fn\_chiffrement.py** : Contient vos fonctions de chiffrement et déchiffrement. Ce fichier sera importé comme un module dans main.py
* **projet Intra – Chiffrement.docx** : Fichier d’instructions ici présent, dans lequel vous aurez copié le code Python de vos 2 fichiers au bas.

## Menu

Vous devrez afficher un menu qui permettra à l’utilisateur de choisir s’il veut chiffrer ou déchiffrer son texte ainsi que le type de chiffrement à utiliser. Il faut ensuite demander d’entrer le texte et la clé de chiffrement puis appeler la fonction correspondante.

## Chiffrements

Les types de chiffrement que nous allons utiliser.

* **Substitution** : Nous allons utiliser la méthode par [décalage](https://www.dcode.fr/chiffre-decalages) (ou [rotation](https://www.dcode.fr/chiffre-rot)), pour recréer des chiffrements célèbres comme celui de [César](https://www.dcode.fr/chiffre-cesar) et de [Vigénère](https://www.dcode.fr/chiffre-vigenere).
* **BONUS**- **Transposition** : La méthode par [transposition](https://www.dcode.fr/chiffre-transposition) sera aussi utilisée, par elle-même, et pour créer un chiffrement supérieur en la combinant à la substitution.

**Tuple à utiliser pour la substitution**

\_tp\_decalage = (  
 ' ', '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', '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', '0', '1', '2', '3', '4', '5', '6',  
 '7', '8', '9', '!', 'é', 'É', 'À', 'à', 'ù', 'Ù',  
 'è', 'È', 'ô', 'Ô', 'Î', 'î', 'ï', 'Ï', "'", '/',  
 '$', '%', '?', '&', '\*', '(', ')', '\_', '+', '=',  
 '.', ',', '-', '"', "@")

## Important

* **Avant de commencer le codage**, écrivez un pseudo-code ou réalisez organigramme de programmation.
  + La séquence générale des opérations devrait être établie, ainsi que les fonctions que vous allez créer et le rôle de chacune.
* Valider
  + Le nombre pour le décalage de César doit toujours être un entier positif.
  + La clé du chiffrement Vigénère doit être alphabétique uniquement.
  + Si vous utilisez une fonction ou module qui pourrait donner une erreur. Valider les valeurs avant de les envoyer à ces fonctions. Ex. : (int(bob) : ValueError, string.index() : IndexError)
  + Il devrait être **impossible de faire *crash*** votre application. Dans le pire des cas, vous affichez un message d’erreur significatif et vous terminez vous-même l’exécution avec un sys.exit().
* Si le caractère à chiffrer n’existe pas dans le tuple\_decalage (Ex. ~), laissez-le tel quel.
* Si le décalage génère un index en dehors de la liste, disons un décalage de 150, il faut recommencer à compter à partir du début. (*wrap around*)
* En plus de ***\_tp\_decalage***, vous pouvez utiliser d’autres dictionnaires ou liste à votre convenance, mais le résultat pour une phrase entrée **doit reproduire exactement la même chose que dans mon exemple**.

#### Bonus

* Il pourrait être bénéfique d’investiguer la **fonction zip()**, qui joint deux listes en une seule liste de deux niveaux.
* Lorsque votre transposition fonctionne bien, créer une fonction qui va enchaîner la substitution et la transposition. Cela rend le déchiffrement beaucoup plus difficile pour les pirates.

## Conseils

* N’oubliez pas de faire un petit morceau à la fois et testez-le, beaucoup.
* Essayez seulement le chiffrement d’un seul mot, comparez votre résultat en faisait le chiffrement à la main.
* Faites ensuite le déchiffrement de la même façon.
* Profiter de votre temps en classe pour poser des questions à l’enseignant pour éviter de passer trop de temps sur un bug.

#### Exemple d’une phrase chiffrée (plus d’exemples à la fin du document)

"This is major Tom to ground control." # Phrase originale.

"YmnxenxerfotweYtreytelwtzsiehtsywtq " # César, rotation 5

"îqw9CrGQPjx5Ui75PiH5CpF5XwrQFxB!UxzL" # Vigénère, clé CinQ

"isTih oasm j orT mogt oro udnc.onrtl" # Transposition, clé Un1Qu3

"nnxYmertfxeoYetweretlytwitezshw tsyq" # Combo(César:5,Transpo:Un1Qu3)

# Votre code

### Pseudo-code ou organigramme

Pseudo-code ou organigramme

### main.py

Code Python main.py

### fn\_chiffrement.py

Code Python fn\_chiffrement.py

# Critères de correction /20

|  |  |
| --- | --- |
| **Critères** | **Points** |
| **Pseudo code et/ou organigramme de programmation (draw.io)** | / 2 points |
| **Respect des normes et documentation des fonctions (noms significatifs, commentaires, lecture facile du code, docstring)** | / 3 points |
| **Modules et fonctions (Utilisation de *import*, plusieurs fonctions, passer des paramètres, retourner une valeur)** | / 3 points |
| **Validation (Est-ce que je peux le faire planter ?, testez abondamment)** | / 4 points |
| **Affichage et mise en page (Espacement, alignement, etc.)** | / 2 points |
| **Fonctionnement (Menu, chiffrer, déchiffrer)** | / 6 points |
| **Bonus (transposition, combinaison de chiffrement)** | \*Considérations futures\* |
| **Total** | **/ 20** |

# Exemples

## Chiffrement César

Bienvenu à "Meilleur Chiffrement" !

1- Chiffrer

2- Déchiffrer

Quelle opération désirez-vous effectuer ? 1

1- César

2- Vigénère

Quel chiffrement désirez-vous utiliser ? 1

Entrez la chaîne à manipuler : Les chemises de l'archiduchesses sont-elles sèches?

Quelle est la rotation à utiliser ? 132

Après les manipulations demandés, voici la chaîne :

îP3KNSPXT3P3KOPKWtL2NSTO5NSP33P3K3ZY4HPWWP3K3lNSP3x

## Déchiffrement César

Bienvenu à "Meilleur Chiffrement" !

1- Chiffrer

2- Déchiffrer

Quelle opération désirez-vous effectuer ? 2

1- César

2- Vigénère

Quel chiffrement désirez-vous utiliser ? 1

Entrez la chaîne à manipuler : îP3KNSPXT3P3KOPKWtL2NSTO5NSP33P3K3ZY4HPWWP3K3lNSP3x

Quelle est la rotation à utiliser ? 132

Après les manipulations demandés, voici la chaîne :

Les chemises de l'archiduchesses sont-elles sèches?

## Chiffrement Vigénère

Bienvenu à "Meilleur Chiffrement" !

1- Chiffrer

2- Déchiffrer

Quelle opération désirez-vous effectuer ? 1

1- César

2- Vigénère

Quel chiffrement désirez-vous utiliser ? 2

Entrez la chaîne à manipuler : Les chemises de l'archiduchesses sont-elles sèches?

Quelle est la clé de chiffrement alphabétique à utiliser ? alphaBET

Après les manipulations demandés, voici la chaîne :

MqIhdJJ6jEuAaFJTm.qzdJNXvoxmtUJÉaEEvuyJ5mqIhtcH1fEc

## Déchiffrement Vigénère

Bienvenu à "Meilleur Chiffrement" !

1- Chiffrer

2- Déchiffrer

Quelle opération désirez-vous effectuer ? 2

1- César

2- Vigénère

Quel chiffrement désirez-vous utiliser ? 2

Entrez la chaîne à manipuler : MqIhdJJ6jEuAaFJTm.qzdJNXvoxmtUJÉaEEvuyJ5mqIhtcH1fEc

Quelle est la clé de chiffrement alphabétique à utiliser ? alphaBET

Après les manipulations demandés, voici la chaîne :

Les chemises de l'archiduchesses sont-elles sèches?

## Chiffrement Transposition

Bienvenu à "Meilleur Chiffrement" !

1- Chiffrer

2- Déchiffrer

Quelle opération désirez-vous effectuer ? 1

1- César

2- Vigénère

3- Transposition

4- Combo (César, Transposition)

Quel chiffrement désirez-vous utiliser ? 3

Entrez la chaîne à manipuler : Les chemises de l'archiduchesses sont-elles sèches?

Quelle est la clé de chiffrement à utiliser (caractères uniques) ? faible

Après les manipulations demandés, voici la chaîne :

e hLscmsseied ' elrhdacicesuhsssne o-letel èhsscse?

## Déchiffrement Transposition

Bienvenu à "Meilleur Chiffrement" !

1- Chiffrer

2- Déchiffrer

Quelle opération désirez-vous effectuer ? 2

1- César

2- Vigénère

3- Transposition

4- Combo (César, Transposition)

Quel chiffrement désirez-vous utiliser ? 3

Entrez la chaîne à manipuler : e hLscmsseied ' elrhdacicesuhsssne o-letel èhsscse?

Quelle est la clé de chiffrement à utiliser (caractères uniques) ? faible

Après les manipulations demandés, voici la chaîne :

Les chemises de l'archiduchesses sont-elles sèches?

## Chiffrement Combo (César, Transposition)

Bienvenu à "Meilleur Chiffrement" !

1- Chiffrer

2- Déchiffrer

Quelle opération désirez-vous effectuer ? 1

1- César

2- Vigénère

3- Transposition

4- Combo (César, Transposition)

Quel chiffrement désirez-vous utiliser ? 4

Entrez la chaîne à manipuler : Les chemises de l'archiduchesses sont-elles sèches?

Quelle est la rotation à utiliser ? 132

Quelle est la clé de chiffrement à utiliser (caractères uniques) ? faible

Après les manipulations demandés, voici la chaîne :

PKSî3NX33PTPOKtKPW2SOLNTNP35S333YPKZHWP4PWKlS33N3Px

## Déchiffrement Combo (César, Transposition)

Bienvenu à "Meilleur Chiffrement" !

1- Chiffrer

2- Déchiffrer

Quelle opération désirez-vous effectuer ? 2

1- César

2- Vigénère

3- Transposition

4- Combo (César, Transposition)

Quel chiffrement désirez-vous utiliser ? 4

Entrez la chaîne à manipuler : PKSî3NX33PTPOKtKPW2SOLNTNP35S333YPKZHWP4PWKlS33N3Px

Quelle est la rotation à utiliser ? 132

Quelle est la clé de chiffrement à utiliser (caractères uniques) ? faible

Après les manipulations demandés, voici la chaîne :

Les chemises de l'archiduchesses sont-elles sèches?