LES TROPHÉES NSI

Édition 2023

DOSSIER DE CANDIDATURE

PRÉSENTATION DU PROJET

NOM DU PROJET : Agent Césarus

Application de cryptage/décryptage et d'échange d'emails entre agents secrets en utilisant l'algorithme de cryptage de César

> PRÉSENTATION GÉNÉRALE :

L'idée de ce projet est de mettre à la disposition d'un groupe d'agents secrets un outil permettant de crypter et de décrypter des messages secrets pour les faire véhiculer entre eux, par messagerie électronique, d'une manière sécurisée.
Cette idée de projet nous est parvenue suite à notre intérêt aux films d'espionnage tels que ceux de James Bond 😊
Pour pouvoir mener ce projet, on s'est intéressé aux algorithmes de cryptage et surtout ceux que nous avons la capacité d'implémenter en tant que élèves en 1ere. Nous avons donc utilisé l'algorithme de César, pour le cryptage et décryptage des messages.
Nous avons développé notre projet avec le langage Python dans sa version 3.8

Qu'est ce que l'algorithme de César ?

L'algorithme de César (ou Chiffrement par décalage) est l'algorithme de cryptographie connu le plus ancien. Il est rendu célèbre par Jules César pour l'usage qu'il en fait pendant ses échanges avec ses généraux.
Son principe est très simple : On remplace chaque lettre du message en clair par la lettre qui la suit d'exactement **n places** dans l'alphabet (le nombre n est appelé clé de décalage) ; et si ça déborde après la lettre 'Z', on continue depuis le début de l'alphabet.
Exemple : Supposons qu'on va crypter un message en utilisant une clé de décalage de 3 positions. Si on prend le mot 'BONJOUR' son cryptage nous donne le mot 'ERQMRXU'.
Si jamais après le décodage d'une lettre on arrive à la fin de l'alphabet, on continue le décalage à partir du début de l'alphabet.

Par ailleurs lors du déchiffrement du message une lettre est remplacée **par une autre précédente** par décalage de n positions.

> ORGANISATION DU TRAVAIL :

Equipe projet :

Notre équipe est composée de 2 personnes : Rayane AYARI et Youssef BOUCHEHIOUA
On a réparti le travail sur 2 volets importants :

- Rayane s'est occupée du développement des scripts Python sous forme de fonctions (les def) qu'on utilisera pour implémenter les fonctionnalités offertes par notre application.
- Par ailleurs Youssef s'est consacré au développement des interfaces utilisateurs (User Interface) en utilisant la bibliothèque Tkinter de Python.

Par ailleurs, la rédaction de la documentation et la préparation de la capsule vidéo on l'a faite conjointement.
Pour la phase de test de l'application, on a préféré faire appel à d'autres personnes pour avoir un regard externe sur notre travail.

Méthodologie de travail :

Suite à la constitution de notre équipe, nous avons commencé par une première réunion pour se mettre d'accord sur :

- Le principe de fonctionnement de l'application
- Les fonctionnalités qu'elle doit offrir
- Le calendrier de déroulement de notre projet
- Les outils techniques à utiliser (Editeur Python, espace de partage des différents fichiers Python via la plateforme CodePen ….)

- La fréquence de nos réunions : Une réunion par semaine soit au sein de notre lycée au via Discord
- Un tableau Excel a été proposé pour suivre conjointement notre état d'avancement sur les différents développements à faire.

LES ÉTAPES DU PROJET :

• Présenter les différentes étapes du projet (de l'idée jusqu'à la finalisation du projet)

Etape	**Tâches**	**Ce qu'on a produit**
Comprendre le principe de l'algorithme de César	Utilité de l'algorithme Principe de cryptage Principe de décryptage Cas particuliers d'utilisations	Une note courte sur le fonctionnement de cet algorithme et les cas particuliers de son utilisation.
Réflexion sur les fonctionnalités à intégrer dans notre application	5 fonctionnalités majeures à savoir : • Une fonctionnalité d'authentification permettant à chaque agent d'accéder à l'application en saisissant son login et son mot de passe. • Une fonctionnalité accessible uniquement à l'administrateur permettant de créer, modifier ou supprimer un agent secret. • Une fonctionnalité permettant de crypter un nouveau message, de l'envoyer par email et d'afficher la liste des tous les messages cryptés par l'agent. • Une fonctionnalité permettant de décrypter un message reçu et d'avoir accès à la liste de tous les messages reçus par un agent. • Une fonction d'aide permettant d'avoir accès à l'aide d'utilisation de notre application.	Un tableau décrivant pour chaque fonction les interfaces Tkinter à préparer et les champs à y intégrer.
Développement de l'application	Le développement de chaque fonctionnalité se fait sur 3 étapes clés : • Développer les codes de l'interface • Développer les codes de traitement • Intégrer les deux codes pour préparer la phase de test	Liste des bibliothèques à utiliser dans Python (Par exemple : CSV, Tkinter, SMTPLIB, DateTime) Créer les bibliothèques en favorisant le plus possible la programmation sous forme de fonctions (def).

Test de l'application	La phase de test de l'application est faite sur 3 étapes : • Validation par l'équipe projet • Validation par des personnes externes au projet (nos parents). • Apporter les corrections nécessaires	Un tableau recensant les différents bugs permettant de cocher chaque ligne lorsque le bug est corrigé.

> FONCTIONNEMENT ET OPÉRATIONNALITÉ :

On a essayé, dans un temps record, de finaliser l'application et d'assurer le bon fonctionnement des fonctionnalités développées. Avec plus de temps on pouvait enrichir notre application avec d'autres fonctionnalités.
Nous avons essayé de prioriser la facilité d'utilisation de l'application chose qui a nous a été bien confirmé par les utilisateurs qui ont pu la tester.
D'ailleurs les personnes ayant testés l'application avaient comme objectif de nous donner leurs avis sur sa facilité d'utilisation mais aussi à nous faire remonter les bugs dans un fichier pour que nous à notre tour on puisse les corriger.

Des différentes difficultés sont apparues tout au long du projet :

- Ce n'est pas facile de se retrouver avec le paramétrage des bibliothèques qu'on a utilisé notamment celles de CSV, Tkinter et SMTPLib. Beaucoup de temps a été consacré pour lire leurs documentations respectives.
- Difficulté d'envoi des emails via notre solution mais on a réussi à débloquer la situation via des forums de discussion qui nous ont fourni des pistes de solutions pour résoudre notre problème. Pour résoudre ce problème on a réussi à avoir accès à un serveur SMTP pour l'envoi de nos emails.
- La communication entre les différentes fenêtres Tkinter nous a posé des problèmes notamment pour partager des variables. Cela nous a amené à mettre des variables comme étant globaux (instruction 'global' en langage Python) pour pouvoir y accéder facilement et les traiter.

> OUVERTURE :

Nous proposons des nouvelles améliorations à savoir :

- Le développement d'une version Web en ligne pourra être intéressante vu le caractère sécuritaire des fonctionnalités de l'application.
- De même, l'algorithme de César n'est pas le plus performant en termes de sécurité, avec plus de compétences en programmation, on pourrait développer des algorithmes plus performants.
- La gestion des données des utilisateurs via des fichiers CSV, n'est pas la plus adaptée donc, on pourra la remplacer par des bases de données chose qui sera faite en terminale lorsqu'on abordera cette technique.

> Lancement de l'application :

Pour lancer l'application il faut aller dans le répertoire **sources** et lancer le fichier **menu.py**