**Rapport de projet**

**Orthos**

**SOMMAIRE**

1. **Introduction**
2. **Description du projet**
3. **Planification**
4. **Gestion des ressources**
5. **Gestion des risques**
6. **Suivi et contrôle**
7. **Résultats et réalisations**
8. **Axes d’amélioration**
9. **Conclusion**

**Introduction**

Le présent rapport décrit le développement d'un outil de chiffrement, conçu pour sécuriser les fichiers sensibles en utilisant l'algorithme AES (Advanced Encryption Standard). L'outil permet de chiffrer et déchiffrer des fichiers en utilisant une clé AES générée de manière aléatoire.

L'objectif principal de ce projet était de fournir aux utilisateurs un moyen simple et efficace de protéger leurs données confidentielles. Le chiffrement AES est largement reconnu pour sa sécurité et sa fiabilité, en faisant un choix approprié pour notre outil de chiffrement.

**Description du projet**

L'outil de chiffrement permet aux utilisateurs de sélectionner un ou plusieurs fichiers à chiffrer. Une fois les fichiers sélectionnés, l'outil génère une clé AES de 256 bits, qui est utilisée pour chiffrer les données. Le chiffrement est effectué en utilisant le mode CBC (Cipher Block Chaining)\* qui ajoute un niveau supplémentaire de sécurité en utilisant un vecteur d'initialisation aléatoire pour chaque fichier.

CBC : Consiste à diviser chaque mot en blocs de lettres. Par exemple, "bonjour" peut être divisé en deux blocs : "bon" et "jour". On utilise le premier bloc de lettres du message, par exemple "bon". On le “mélange” à l’aide de la clé AES. Ce qui nous donne un message chiffré.

**Planification**

**Semaine 1 :**

1. Analyse des exigences : Comprendre en détail les fonctionnalités attendues de l'outil de chiffrement.
2. Conception initiale : Élaborer une conception l'architecture logicielle et de l’interface utilisateur.

**Semaine 2 :**

1. Mise en place de l'interface utilisateur : Créer l'interface utilisateur en utilisant la bibliothèque Tkinter.
2. Implémentation des fonctionnalités de base : Ajouter la fonctionnalité de sélection de fichiers, de génération de clé AES, et d'affichage de la clé générée.

**Semaine 3 :**

1. Implémentation du chiffrement AES : Intégrer l'algorithme AES pour chiffrer les fichiers sélectionnés.
2. Ajout de la fonctionnalité de sauvegarde de la clé AES : Permettre aux utilisateurs de sauvegarder la clé générée pour une utilisation ultérieure.

**Semaine 4 :**

1. Implémentation du déchiffrement AES : Ajouter la fonctionnalité de déchiffrement des fichiers chiffrés en utilisant la clé AES.
2. Tests et débogage : Effectuer des tests approfondis pour vérifier le bon fonctionnement de l'outil de chiffrement/déchiffrement, et résoudre les éventuels problèmes identifiés.

**Derniers jours** :

1. Documentation et préparation de la livraison : Rédiger la documentation du projet et préparer les livrables finaux.

**Gestion des ressources**

**Ressources humaines :**

Développeurs : L'équipe de développement comprendra deux développeurs.

Chef de projet : Une personne responsable de la coordination du projet, de la planification, du suivi des tâches et de la communication avec l'équipe de développement.

**Ressources matérielles :**

Ordinateurs : L'équipe de développement utilisera ses ordinateurs portables pour effectuer le développement et les tests.

Stockage : Un espace de stockage (git) a été utilisé pour enregistrer les fichiers de développement, les fichiers de test et les fichiers de sauvegarde.

Équipements de communication : Les moyens de communication tels que des messageries instantanées (discord) ou des outils de gestion de projets ont été nécessaires pour faciliter la collaboration et la coordination au sein de l'équipe.

**Environnement de développement :**

L'équipe a utilisé un environnement de développement intégré (IDE) tel que PyCharm ou Visual Studio Code pour faciliter le développement et le débogage.

Bibliothèques et modules :

Des bibliothèques Python standard nécessaires pour le projet, telles que **os**, **base64**, **tkinter**, **Crypto** (pour AES), ont été utilisées.

**Outils de gestion de versions :**

Un système de contrôle de versions tel que Git nous a facilité la collaboration et le suivi des modifications du code source.

**Logiciels de test :**

Des outils de test automatisés et des frameworks de test Python tels que PyTest ou UnitTest ont été utilisés pour effectuer les tests.

**Gestion des risques**

**Compréhension insuffisante des exigences**

Mesure de gestion :

Réaliser une analyse approfondie des exigences dès le début du projet.

**Compétences techniques insuffisantes de l'équipe**

Mesure de gestion :

S'assurer que l'équipe dispose des compétences techniques nécessaires avant le début du projet. Identifier les lacunes éventuelles. Encourager le partage des connaissances et la collaboration au sein de l'équipe ainsi que la formation.

**Problèmes de planification et de gestion du temps**

Mesure de gestion :

Établir une planification réaliste en tenant compte des dépendances, des ressources disponibles et des contraintes. Suivre et mettre à jour régulièrement le planning du projet.

**Problèmes de sécurité des données**

Mesure de gestion :

Mettre en place des mesures de sécurité appropriées pour protéger les données sensibles, comme le stockage sécurisé des clés de chiffrement et la gestion des accès

**Dépendance des ressources clés**

Mesure de gestion :

Identifier les ressources clés du projet et mettre en place des mesures de contingence en cas d'indisponibilité. Assurer une documentation adéquate et un partage des connaissances pour minimiser l'impact des absences ou des départs inattendus.

**Suivi et contrôle**

**Création du tableau de bord** : Utilisation de l'application Monday pour créer un tableau de bord dédié au projet.

**Assignation des tâches** : À chaque phase du projet, les tâches étaient attribuées aux membres de l'équipe de développement.

**Suivi des tâches** : Changement du statut des tâches dans le tableau de bord Monday "À faire", "En cours" ou "Terminé". Cela a permis à tous les membres de l'équipe de voir rapidement où en est chaque tâche et d'identifier les éventuels retards ou problèmes.

**Communication et collaboration** : Commentaires et notifications via l’application Monday pour encourager la communication et la collaboration au sein de l'équipe. Les membres de l'équipe pouvaient laisser des commentaires sur les tâches, poser des questions ou partager des mises à jour.

**Résultats et réalisations**

Les résultats et réalisations du projet de développement de l'outil de chiffrement incluent :

**Outil de chiffrement fonctionnel :** L'équipe a réussi à développer un outil de chiffrement complet et fonctionnel.

**Interface utilisateur :** L'interface utilisateur de l'outil de chiffrement a été conçue de manière simple, permettant aux utilisateurs d'effectuer les actions nécessaires de manière intuitive.

**Génération de clé AES sécurisée :** L'outil est capable de générer une clé AES sécurisée de 256 bits de manière aléatoire, fournissant ainsi un niveau élevé de sécurité pour le chiffrement des fichiers. La clé générée est sauvegardée dans un fichier pour une utilisation ultérieure ou dans une base de données.

**Chiffrement et déchiffrement des fichiers :** L'outil utilise l'algorithme AES (Advanced Encryption Standard) en mode CBC (Cipher Block Chaining) pour chiffrer et déchiffrer les fichiers sélectionnés. Les données des fichiers sont divisées en blocs, chiffrées avec la clé AES et sauvegardées dans de nouveaux fichiers chiffrés. Le processus de déchiffrement restaure les fichiers à leur état d'origine.

**Sauvegarde des fichiers chiffrés et déchiffrés** : L'outil crée des répertoires dédiés pour stocker les fichiers chiffrés et déchiffrés, permettant aux utilisateurs de retrouver facilement leurs fichiers dans les différentes étapes du processus.

**Barre de progression et notifications :** L'outil utilise une barre de progression pour indiquer visuellement l'avancement du chiffrement ou du déchiffrement des fichiers. Des notifications sont également affichées pour informer les utilisateurs du succès des opérations ou des erreurs éventuelles.

**Gestion des erreurs :** L'outil est conçu pour gérer les erreurs de manière appropriée. Des messages d'erreur sont affichés en cas de problème lors du chiffrement ou du déchiffrement des fichiers, aidant ainsi les utilisateurs à comprendre et à résoudre les problèmes éventuels.

**Axes d’amélioration**

I**nterface utilisateur conviviale améliorée :**

L'interface utilisateur pourrait être repensée pour offrir une expérience plus intuitive et conviviale aux utilisateurs. Cela pourrait inclure l'amélioration de la disposition des éléments.

**Options de personnalisation :**

L'outil pourrait proposer des options de personnalisation pour permettre aux utilisateurs de choisir des préférences telles que le thème de l'interface ou la langue. Cela offrirait une plus grande flexibilité et une expérience plus adaptée à chaque utilisateur.

**Conclusion**

En conclusion, le projet de développement a été une réussite. L'équipe a créé un outil fonctionnel, permettant le chiffrement et le déchiffrement des fichiers en utilisant l'algorithme AES en mode CBC. L'outil offre aux utilisateurs la possibilité de rendre confidentielles leurs données sensibles de manière efficace.

L'outil génère une clé AES sécurisée, chiffre tout type de fichiers (pdf, xlms, word, txt etc). Sauvegarde les clés générées.

L’interface utilisateur permet de naviguer facilement à travers les différentes fonctionnalités de l'outil et de visualiser les fichiers sélectionnés.

Cependant, il reste des opportunités d'amélioration. L'équipe peut se concentrer sur l'amélioration de l'interface utilisateur pour la rendre plus agréable.

Dans l'ensemble, le projet a permis à l'équipe de développer ses compétences en matière de programmation, de sécurité des données et de gestion de projet. La collaboration et la communication au sein de l'équipe ont été essentielles pour mener à bien le projet dans les délais impartis.

L'outil de chiffrement développé constitue une contribution précieuse dans le domaine de la sécurité des données, offrant une solution pratique pour protéger les fichiers sensibles. Il peut être utilisé par les utilisateurs qui souhaitent renforcer la confidentialité de leurs données et maintenir leur intégrité lorsqu'ils les partagent ou les stockent.