Rapport sur le projet :gestionnaire de mot de passe



Yosef Nademo – CID2B

Vennes

24 périodes

Table des matières

[1 Introduction 3](#_Toc182986846)

[1.1 Titre 3](#_Toc182986847)

[1.2 Description 3](#_Toc182986848)

[2 Planification 3](#_Toc182986849)

[2.1 Chronologie du projet 3](#_Toc182986850)

[2.2 La planification-journal de travail de Excel 3](#_Toc182986851)

[2.3 Gestion des risques 3](#_Toc182986852)

[3 Analyse fonctionnelle 4](#_Toc182986853)

[3.1 1. Objectifs du programme 4](#_Toc182986854)

[3.2 2. Mécanique de programme 4](#_Toc182986855)

[4 Webographie 4](#_Toc182986856)

# Introduction

## Titre

**Gestionnaire de mot de passe**

## Contexte

Dans un monde numérique où la sécurité des comptes en ligne est essentielle, la gestion des mots de passe est devenue un défi majeur. Les utilisateurs doivent souvent jongler avec de multiples mots de passe pour leurs divers comptes, ce qui engendre des risques liés à l'utilisation de mots de passe faibles ou réutilisés.

## Description

Ce projet consiste à concevoir et développer un gestionnaire de mots de passe local. Cette application permet de sauvegarder de manière sécurisée des informations sensibles, telles que le site Internet, le nom d'utilisateur et le mot de passe, tout en garantissant la confidentialité grâce à un cryptage basé sur la méthode de Vigenère.

# Objectifs principaux

Permettre à l'utilisateur de :

* Saisir un mot de passe maître pour accéder au gestionnaire.
* Ajouter, consulter et mettre à jour des informations de connexion (site, identifiant, mot de passe).
* Stocker les mots de passe de manière chiffrée sur le disque.

# Planification

## Chronologie du projet

Le projet se déroulera sur le premier trimestre et comprendra un total de 24 périodes, réparties comme suit :

* P\_Secu : Gestionnaire de mot de passe : 24 périodes

## La planification-journal de travail de Excel

La planification complète sera faite dans le fichier qui s’appelle « JDT\_Yosef-Nademo ».

## Gestion des risques

**Perte de données** : Sauvegardes régulières et utilisation de systèmes de versionnement GIT.

**Retard dans le développement** : Revue hebdomadaire de l'avancement et ajustement du planning si nécessaire.

**Problèmes techniques** : Consultation des clients et demande d'aide externe si nécessaire, avec documentation des solutions apportées.

# Analyse fonctionnelle

## ****Objectifs du programme****

* Offrir une solution sécurisée pour la gestion des mots de passe sans dépendance à une connexion Internet.
* Garantir une interface simple et intuitive pour les utilisateurs.

## ****Mécanique de programme****

1. **Saisie du mot de passe maître** :
   * Au démarrage, le programme demande à l'utilisateur de saisir un mot de passe maître.
   * Si un fichier config.txt existe, le programme vérifie la validité de la clé maître en la comparant à la clé stockée.
2. **Gestion des mots de passe** :
   * Ajout d'un mot de passe : L'utilisateur entre un site, un identifiant, et un mot de passe. Ces données sont chiffrées et stockées dans un fichier.
   * Consultation : Le programme affiche les informations demandées après avoir vérifié l'identité de l'utilisateur.
   * Mise à jour : Permet de modifier les informations existantes.
3. **Structure de stockage** :
   * Chaque mot de passe est stocké dans un fichier séparé au format chiffré dans un répertoire nommé password.

## Algorithmes utilisés

* Cryptage de Vigenère : Transforme les mots de passe en utilisant une clé (le mot de passe maître) et permet de garantir leur confidentialité.
* Décryptage : Permet de convertir les données chiffrées en informations lisibles après vérification de la clé maître.

# Conclusion

Le gestionnaire de mots de passe proposé répond aux exigences modernes de sécurité et de gestion des données confidentielles. Sa conception locale offre une maîtrise complète des informations, tandis que l'usage d'un algorithme de cryptage garantit leur confidentialité. Ce projet fournit une base solide pour une gestion robuste et évolutive des mots de passe.

# Webographie