Rapport sur le projet: gestionnaire de mot de passe



Yosef Nademo – CID2B

Rue de Sébeillon 12, 1004 Lausanne

24 périodes

Table des matières

[1. Introduction 3](#_Toc185342799)

[Contexte 3](#_Toc185342800)

[Description 3](#_Toc185342801)

[2. Objectifs principaux 3](#_Toc185342802)

[3. Planification 3](#_Toc185342803)

[Chronologie du projet 3](#_Toc185342804)

[La planification-journal de travail de Excel 3](#_Toc185342805)

[4. Gestion des risques 4](#_Toc185342806)

[5. Analyse Fonctionnelle du Gestionnaire de Mots de Passe 4](#_Toc185342807)

[Objectifs du programme 4](#_Toc185342808)

[Objectifs et Fonctionnalités Principales 4](#_Toc185342809)

[Mécanique de programme 7](#_Toc185342810)

[6. Conclusion 8](#_Toc185342811)

[7. Webographie 9](#_Toc185342812)

**Gestionnaire de mots de passe**

# Introduction

## 

## 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 du Gestionnaire de Mots de Passe

## ****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.
* Interface Utilisateur : Fournir une interface intuitive pour naviguer facilement à travers les différentes fonctions.
* Sécurité : Chiffrer les mots de passe avec le Vigenère cipher et gérer les erreurs efficacement.

## Objectifs et Fonctionnalités Principales

1. **Gestion des Utilisateurs** :
   * **Création de compte** : Permet aux utilisateurs de créer un compte sécurisé en fournissant des informations minimales telles que le nom d'utilisateur et le mot de passe. Cette étape est cruciale pour sécuriser l'accès et garantir que chaque utilisateur dispose d'un identifiant unique.
   * **Connexion** : Les utilisateurs peuvent se connecter à leur compte à l'aide de leurs informations d'identification, assurant ainsi un contrôle d'accès strict. Cette fonctionnalité est renforcée par des pratiques de sécurité telles que la vérification en deux étapes.
   * **Mot de passe oublié** : Permet aux utilisateurs de réinitialiser leur mot de passe en utilisant des méthodes comme le courrier électronique ou une question secrète. Cela aide à récupérer un compte oublié ou piraté.
2. **Gestion des Mots de Passe** :
   * **Affichage des mots de passe** : Les utilisateurs peuvent visualiser leurs mots de passe enregistrés, ce qui facilite la gestion de leurs informations confidentielles. L'affichage peut inclure des détails tels que le nom du service, le nom d'utilisateur associé, et le mot de passe chiffré.
   * **Ajout de mots de passe** : Permet aux utilisateurs d'ajouter de nouveaux mots de passe de différentes manières, telles que la génération aléatoire, le chiffrement Vigenère, ou la saisie manuelle. Cette souplesse aide à répondre aux besoins divers des utilisateurs.
   * **Modification de mots de passe** : Les utilisateurs peuvent modifier un mot de passe existant pour renforcer la sécurité ou ajuster l'accès en cas de changement des informations.
   * **Suppression de mots de passe** : Permet une gestion stricte des mots de passe en permettant leur suppression définitive, ce qui est essentiel pour maintenir la sécurité du système.
3. **Sécurité et Confidentialité** :
   * **Cryptage des mots de passe** : Les mots de passe sont stockés de manière sécurisée à l'aide de l'algorithme de chiffrement Vigenère. Ce processus garantit que les données sensibles ne sont accessibles qu'aux utilisateurs autorisés.
   * **Authentification à deux facteurs (2FA)** : Optionnellement, la 2FA peut être activée pour ajouter une couche de sécurité supplémentaire au processus de connexion. Cela inclut des méthodes comme la vérification par email ou SMS.
   * **Gestion des erreurs et notifications** : Le système alerte les utilisateurs en cas de tentative de connexion infructueuse ou d'activités suspectes. Cela aide à identifier rapidement les violations potentielles de sécurité et à y répondre immédiatement.
   * **Protection contre les attaques courantes** : Met en œuvre des mesures de sécurité telles que le verrouillage automatique du compte après un certain nombre de tentatives infructueuses pour se connecter. Cela réduit le risque d'attaques par force brute.
4. **Navigation et Interface Utilisateur** :
   * **Interface utilisateur simple et intuitive** : Offrir une interface conviviale qui permet aux utilisateurs d'interagir facilement avec le logiciel. La navigation est conçue pour minimiser la confusion et permettre un accès rapide aux fonctionnalités principales.
   * **Navigation claire** : Les utilisateurs peuvent se déplacer aisément entre les différentes sections du logiciel (Accueil, Consultation, Ajout, Suppression) grâce à un menu intuitif.
   * **Confirmation des actions critiques** : Exiger une confirmation explicite pour des actions comme la suppression de mots de passe ou la modification de données sensibles. Cela renforce la sécurité en s'assurant que les utilisateurs prennent des décisions conscientes et avisées.
5. **Stockage et Sauvegarde** :
   * **Sauvegarde régulière des données** : Sauvegarder automatiquement les mots de passe pour éviter toute perte de données en cas de panne système ou d'erreur humaine. Cette fonctionnalité garantit que les informations restent accessibles même en cas de défaillance matérielle.
   * **Restaurer des données** : Permet aux utilisateurs de restaurer facilement leur accès aux mots de passe en cas de perte ou de corruption. Cela est crucial pour maintenir la continuité des opérations et éviter les interruptions dues à des incidents techniques.

## ****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. Ce mot de passe est essentiel pour sécuriser l'accès au gestionnaire de mots de passe.
  + Si un fichier config.txt existe déjà, le programme vérifie si la clé maître saisie correspond à celle stockée dans ce fichier pour garantir que l'utilisateur est autorisé à accéder au système.

#### 2. Gestion des Mots de Passe

* **Ajout d'un Mot de Passe** :
  + L'utilisateur saisit les informations nécessaires : nom du site, identifiant, et mot de passe.
  + Ces données sont ensuite **chiffrées** à l'aide de l'algorithme de **cryptage Vigenère**, utilisant la clé maître comme clé de chiffrement.
  + Les informations chiffrées sont **stockées dans un fichier** dédié dans un répertoire nommé password. Chaque fichier contient les détails du mot de passe chiffré pour une gestion sécurisée.
* **Consultation** :
  + Pour consulter les informations d'un mot de passe, l'utilisateur doit vérifier son identité en entrant le mot de passe maître.
  + Le programme affiche les informations demandées après la vérification.
* **Mise à Jour** :
  + Permet à l'utilisateur de modifier les informations existantes (nom du site, identifiant, mot de passe).
  + Les modifications apportées seront **chiffrées** de la même manière que les informations initiales et stockées dans le fichier concerné.

#### 3. Structure de Stockage

* Chaque mot de passe est **stocké dans un fichier séparé** au format chiffré dans le répertoire password. Cette méthode permet une organisation claire et sécurisée des informations.
* Le format des fichiers garantit que les mots de passe sont protégés contre l'accès non autorisé, même si des tentatives de visualisation directe des fichiers sont faites.

#### Algorithmes Utilisés

* **Cryptage de Vigenère** :
  + Transforme les mots de passe en utilisant la clé maître comme clé de chiffrement. Ce chiffrement est **symétrique**, ce qui signifie que la même clé est utilisée pour chiffrer et déchiffrer les données.
  + Permet de garantir la confidentialité des mots de passe en les rendant illisibles sans la clé correcte.
* **Décryptage** :
  + Permet de convertir les données chiffrées en informations lisibles après vérification de la clé maître.
  + Utilise également l'algorithme de **cryptage Vigenère** inversé pour rendre les données compréhensibles uniquement pour les utilisateurs ayant la clé correcte.

# Conclusion

Ce programme propose une solution robuste pour la gestion des mots de passe. Il intègre un chiffrement sécurisé, utilise un mot de passe maître pour protéger l'accès, et stocke les informations de manière structurée et sécurisée. Les utilisateurs bénéficient d'une interface simple pour ajouter, consulter, et mettre à jour leurs mots de passe, tout en bénéficiant de la sécurité accrue offerte par le chiffrement de Vigenère. L'intégration de la vérification par le mot de passe maître ajoute une couche supplémentaire de sécurité, protégeant les utilisateurs contre le vol de données. L'organisation en fichiers séparés et le chiffrement adéquat garantissent que les mots de passe restent confidentiels et sécurisés, même en cas de violation potentielle du système.

# Webographie

P\_Sec-Gestionnaire de mots de passe.pdf

<https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher>

https://www.dcode.fr/vigenere-cipher