P\_Secu 114



Figure - Logo de l'application

Segalen Alban – mid2b

Sébeillon

24p

Helder Costa Lopes

Table des matières

[1 introduction 3](#_Toc187253517)

[1.1 Titre 3](#_Toc187253518)

[1.2 Description 3](#_Toc187253519)

[1.2.1 Objectifs et portée du projet (objectifs SMART) 3](#_Toc187253520)

[1.2.2 Fonctionnalités requises (du point de vue de l’utilisateur) 3](#_Toc187253521)

[1.3 Les points suivants seront évalués 3](#_Toc187253522)

[1.4 Validation et conditions de réussite 3](#_Toc187253523)

[2 Description générale 3](#_Toc187253524)

[2.1 Présentation de l’application 3](#_Toc187253525)

[2.2 Fonctionnalités principales 3](#_Toc187253526)

[3 algorithme et conception 3](#_Toc187253527)

[3.1 Chiffrement de Vigenère 3](#_Toc187253528)

[3.2 Schémas des algorithmes 5](#_Toc187253529)

[4 implémentation 5](#_Toc187253530)

[4.1 Structure du code 5](#_Toc187253531)

[4.2 Modules et fonctions principales 6](#_Toc187253532)

[4.2.1 Fonction de chiffrement 6](#_Toc187253533)

[4.2.2 Fonction de déchiffrement 7](#_Toc187253534)

[4.2.3 Fonction de sauvegarde 8](#_Toc187253535)

[4.2.4 Fonction de récupération 9](#_Toc187253536)

[5 sécurité 10](#_Toc187253537)

[6 tests et validation 10](#_Toc187253538)

[7 journal de travail 10](#_Toc187253539)

[8 Analyse 10](#_Toc187253540)

[8.1 Document d’analyse et conception 10](#_Toc187253541)

[9 Conclusion 11](#_Toc187253542)

[9.1 Bilan des fonctionnalités demandées 11](#_Toc187253543)

[9.2 Bilan personnel 11](#_Toc187253544)

[10 Divers 11](#_Toc187253545)

[10.1 Bibliographie 11](#_Toc187253546)

[10.2 Webographie 11](#_Toc187253547)

[11 Annexes 11](#_Toc187253548)

# introduction

## Titre

P\_Secu 114 : Gestionnaire de mot de passe

## Description

Réaliser un gestionnaire de mot de passeCahier des charges

### Objectifs et portée du projet (objectifs SMART)

Réaliser une application qui permet de gérer ses mots de passes.

### Fonctionnalités requises (du point de vue de l’utilisateur)

L’utilisateur utilise un Master Password pour accéder aux mots de passes. Le Master Password est utilisé comme clé de Vigenère.

On peut ajouter, modifier, supprimer un mot de passe.

Un mot de passe contient : un titre, l’URL du site, le nom d’utilisateur et le mot de passe.

## Les points suivants seront évalués

* Le rapport
* Les planifications (initiale et détaillée)
* Le journal de travail
* Le code et les commentaires
* Les documentations de mise en œuvre et d’utilisation

## Validation et conditions de réussite

* Compréhension du travail
* Possibilité de transmettre le travail à une personne extérieure pour le terminer, le corriger ou le compléter
* Etat de fonctionnement du produit livré

# Description générale

## Présentation de l’application

## Fonctionnalités principales

Ajouter, supprimer, modifier et sauvegarder des mots de passes de manières sécurisé.

# algorithme et conception

## Chiffrement de Vigenère

Récupérer la valeur du premier caractère du message. Y ajouter la valeur du premier caractère de la clé. Y soustraire le nombre de possibilité (fait automatiquement avec c#). Répéter l’opération avec la deuxième lettre du message et de la clé. Si on arrive au bout de la clé, on prendre la première lettre de la clé.

[https://eduvaud.sharepoint.com/sites/msteams\_3cc8eb/Supports%20de%20cours/Forms/AllItems.aspx?id=%2Fsites%2Fmsteams%5F3cc8eb%2FSupports%20de%20cours%2FICT%2F114%2DCodificationChiffrement%2Fb%2DUnitesEnseignement%2FS%2D114%2DCompendio%2Epdf&parent=%2Fsites%2Fmsteams%5F3cc8eb%2FSupports%20de%20cours%2FICT%2F114%2DCodificationChiffrement%2Fb%2DUnitesEnseignement](https://eduvaud.sharepoint.com/sites/msteams_3cc8eb/Supports%20de%20cours/Forms/AllItems.aspx?id=%2Fsites%2Fmsteams_3cc8eb%2FSupports%20de%20cours%2FICT%2F114-CodificationChiffrement%2Fb-UnitesEnseignement%2FS-114-Compendio.pdf&parent=%2Fsites%2Fmsteams_3cc8eb%2FSupports%20de%20cours%2FICT%2F114-CodificationChiffrement%2Fb-UnitesEnseignement)

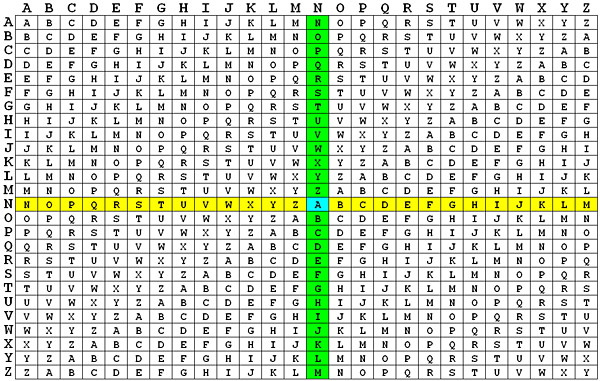


Figure - Table de Vigenère - ictteachersug.net

## Schémas des algorithmes

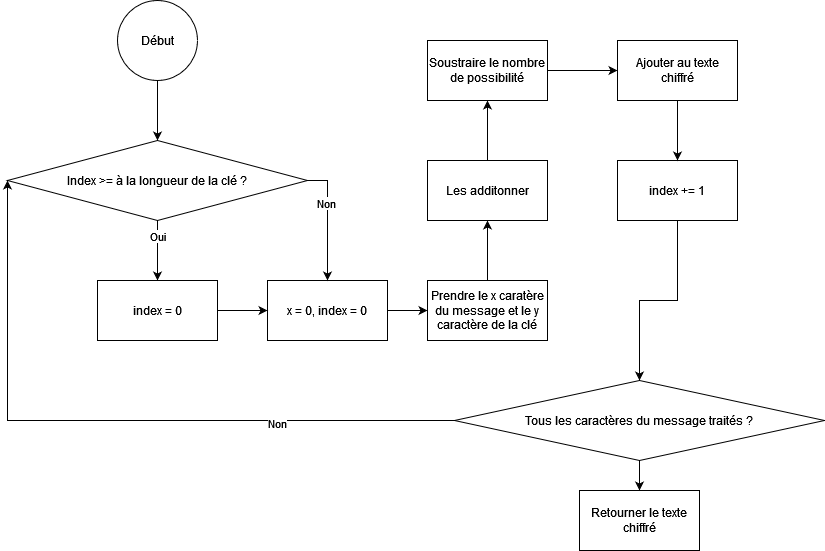


Figure - Schéma du chiffrement avec Vigenère

# implémentation

## Structure du code

Le code est structuré sous la forme d’une application WindowsForms, ce qui implique l’utilisation de la programmation orienté objet.

## Modules et fonctions principales

### Fonction de chiffrement

/// <summary>

/// Chiffre un texte

/// </summary>

/// <param name="text">Le texte à chiffrer</param>

/// <returns>Un texte chiffré</returns>

public static string Encrypt(string text)

{

string encryptedText = ""; //Le texte chiffré

int keyIndex = 0; //L'index de la clé

//Pour chaque charactère du texte

foreach (char c in text)

{

//Si l'index de la clé est plus grand que la longueur de la clé, on revient au début de la clé

if (keyIndex >= MasterPassword.Key.Length)

{

keyIndex = 0;

}

int characterValue = (int)c; //Le code du caractère à chiffrer

characterValue += (int)MasterPassword.Key[keyIndex]; //On ajoute le code du caractère de la clé au code du caratère à chiffrer

encryptedText += (char)characterValue; //On ajoute le caractère chiffré au texte chiffré

keyIndex++; //On incremente l'index de la clé

}

return encryptedText; //On retourne le texte chiffré

}

Figure - Fonction de chiffrement

Implémentation de cet algorithme :

* D’abord penser à une boucle foreach pour parcourir le message
* Ensuite un index pour parcourir la clé
* Il faut remettre l’index à 0 quand on à atteint le bout de la clé

### Fonction de déchiffrement

/// <summary>

/// Déchiffre un text

/// </summary>

/// <param name="text">Le texte à déchiffrer</param>

/// <returns>Un texte déchiffré</returns>

public static string Decrypt(string text)

{

string decryptedText = ""; //Le texte déchiffré

int keyIndex = 0; //L'index de la clé

//Pour chaque charactère du texte

foreach (char c in text)

{

//Si l'index de la clé est plus grand que la longueur de la clé, on revient au début de la clé

if (keyIndex >= MasterPassword.Key.Length)

{

keyIndex = 0;

}

int characterValue = (int)c; //Le code du caractère à déchiffrer

characterValue -= (int)MasterPassword.Key[keyIndex]; //On soustrait le code du caractère de la clé au code du caratère à déchiffrer

decryptedText += (char)characterValue; //On ajoute le caractère déchiffré au texte déchiffré

keyIndex++; //On incremente l'index de la clé

}

return decryptedText; //On retourne le texte déchiffré

}

Figure - Fonction de déchiffrement

Pareil que le chiffrement, sauf qu’on soustrait.

### Fonction de sauvegarde

/// <summary>

/// Sauvegarde les entrées

/// </summary>

public static void SaveEntries()

{

//Crée le dossier password si nécessaire

if (!Directory.Exists(savePath))

{

Directory.CreateDirectory(savePath);

}

//Crée le fichier de configuration si nécessaire et y écrit le Master password chiffré

if (!File.Exists(configFile))

{

File.WriteAllText(configFile, EncryptionManager.Encrypt(MasterPassword.Key));

}

//Rempli la liste de mots de passes

foreach (Entry entry in PasswordManager.PasswordList)

{

File.WriteAllText(Path.Combine(savePath, entry.Title + fileExtension), JsonSerializer.Serialize(entry));

}

}

Figure - Fonction de déchiffrement

Implémentation :

* D’abord : écrire la liste de mots de passes avec un foreach
* Ensuite : Créer le dossier et le fichier de config si ils n’existent pas

### Fonction de récupération

/// <summary>

/// Récupère les mots de passes du fichier de sauvegardes

/// </summary>

/// <param name="inputMasterPassword">Le mot de passe que l'utilisateur a rentrer</param>

/// <exception cref="WrongPasswordException">Lance une exception si le mot de passe n'est pas correct</exception>

public static void ReadEntries(string inputMasterPassword)

{

try

{

MasterPassword.Key = inputMasterPassword;

//Si le fichier de configuration n'est pas présent, on le crée

if (!File.Exists(configFile))

{

SaveEntries();

}

//Si le mot de passe est correct

if (EncryptionManager.Encrypt(inputMasterPassword) == File.ReadAllText(configFile)) ;

{

string[] files = Directory.GetFiles(savePath); //Récupère les noms des fichiers

//Rempli la liste de mots de passes

foreach (string file in files)

{

PasswordManager.PasswordList.Add(JsonSerializer.Deserialize<Entry>(File.ReadAllText(file)));

}

return;

}

throw new WrongPasswordException("Mauvais mot de passe");

}

catch (Exception ex)

{

//Si le mot de passe n'est pas correct

if (ex.GetType() == typeof(WrongPasswordException))

{

//On affiche un pop-up

string message = "Vous vous êtes trompés de mot de passe : l'application va s'éteindre";

string caption = "Erreur dans le mot de passe";

MessageBoxButtons buttons = MessageBoxButtons.OK;

MessageBox.Show(message, caption, buttons);

//On quitte l'application

Application.Exit();

}

}

}

Figure - Fonction de récupération / Lecture des entrées

Cette méthode est beaucoup plus grande que la sauvegarde, car elle arrête l’application en cas de mot de passe erroné.

Implémentation :

* On récupère la liste des fichiers
* On lit et déchiffre leur contenu et on rempli la liste de mots de passe
* Si le fichier de config n’est pas présent, on le crée
* Si le mot de passe n’est pas correct, on affiche un pop-up et on quitte l’application

# sécurité

Les entrées sont toujours chiffrées sur le disque. Les mots de passes sont cachés à la saisie et à la consultation, avec un bouton pour les copier.

# tests et validation

|  |  |  |
| --- | --- | --- |
| Tests | Résultats | Validé |
| Entrer un master password erroné | L’application s’arrête | Oui |
| Ajouter une entrée | L’entrée est ajoutées | Oui |
| Quittez l’application et se connecter | Les mots de passes sont toujours disponibles | Oui |
| Supprimer une entrée | L’entrée est supprimée | Oui |
| Modifier le champ titre d’une entrée | Le titre est mis à jour | Oui |
| Quittez l’application et se connecter après avoir mis à jour le titre | Le titre est bien à jour | Oui |
| Modifier une le champ url d’une entrée et quitter l’application avec alt + f4 et se connecter | L’url de l’entrée à bien été modifiée. | Oui |

# journal de travail

# Analyse

## Document d’analyse et conception

Chaque entrée est déjà chiffrée sur le disque.

Le stockage des mots de mot de passe ce fait en Json, car c’est un format largement utilisé et standardisé.

Encodage

Pour stocker la liste de mot de passe, la méthodes est la suivante :

On sérialise la liste de mot de passe en Json (l’entrée est déjà chiffrée).

On crée ensuite une liste de string qui contient le MasterPassword chiffré avec lui-même et le Json chiffré.

On sérialise cette liste en Json.

On écrit le Json ainsi obtenu dans le fichier de sauvegarde.

Ce paragraphe décrit le fonctionnement de manière détaillée.

Autant que possible de manière graphique, imagée, tableaux, etc.

Tous les cas particuliers devraient y être spécifiés…

Il s’agit d’y présenter les fonctionnalités à développer :

Découpage en étapes, en modules, en fonctionnalités, etc.

Formulaires, interfaces graphiques, pages web, etc.

Schémas de navigation, schémas événementiels, structogramme, pseudocode, etc.

Si le projet inclut une base de données :

Dictionnaire des données

Modèle conceptuel des données, modèles logique des données.

# Conclusion

## Bilan des fonctionnalités demandées

Il s’agit de reprendre point par point les fonctionnalités décrites dans les spécifications de départ et de définir si elles sont atteintes ou pas, et pourquoi.

Si ce n’est pas le cas, estimer en « % » ou en « temps supplémentaire » le travail qu’il reste à accomplir pour terminer le tout.

## Bilan personnel

Comme la sécurité des données est primordiale de nos jours, c’est un projet nécessaire.

J’ai bien aimé ce projet car il m’a permis de réaliser une application que je pourrais utiliser pour le restant de ma formation.

Ce projet m’a également permis de perfectionner mes compétences en C#.

Si c’était à refaire:

Qu’est-ce qu’il faudrait garder ? Les plus et les moins ?

Qu’est-ce qu’il faudrait gérer, réaliser ou traiter différemment ?

Qu’est que ce projet m’a appris ?

Suite à donner, améliorations souhaitables, …

Remerciements, signature, etc.

# Divers

## Bibliographie

Références des livres, revues et publications utilisés durant le projet.

## Webographie

[Figure 1 - Logo de l'application 1](#_Toc187253552)

[Figure 2 - Table de Vigenère - ictteachersug.net 4](#_Toc187253553)

[Figure 3 - Schéma du chiffrement avec Vigenère 5](#_Toc187253554)

[Figure 4 - Fonction de chiffrement 6](#_Toc187253555)

[Figure 5 - Fonction de déchiffrement 7](#_Toc187253556)

[Figure 6 - Fonction de déchiffrement 8](#_Toc187253557)

[Figure 7 - Fonction de récupération / Lecture des mots de passes 9](#_Toc187253558)

Références des sites Internet consultés durant le projet.

# Annexes

Listing du code source (partiel ou, plus rarement complet)

Guide(s) d’utilisation et/ou guide de l’administrateur

Etat ou « dump » de la configuration des équipements (routeur, switch, robot, etc.).

Extraits de catalogue, documentation de fabricant, etc.