Présentation du projet

Nom : GDM-001

Début du projet : le 07/03/2022 18h35

Fin du projet : le 22/03/2022 15h23

Lien vers la vidéo peertub (video_GDM-001) :
https://peertube.iriseden.eu/w/mkQqhgjyHpRav4VnotU8GN

Description : GDM-001 est un gestionnaire de mot de passe, il permet de stocker et de chiffrer les mots de passe et les associant aux comptes correspondants et à d'autres informations. Les mots de passe sont donc stockés dans une base de données au quelle personne ne peut avoir accès sauf l'utilisateur à l'aide du seul mot de passe qu'il devra retenir ce mot de passer et hasher (transformer en une chaînes incompréhensible, et indéchiffrable car la fonction de hashage n'est pas réversible) et servira pour chiffrer la master key, la clé qui nous servira à chiffré les mots de passe lors du stockage pour que si par mal chance un individué ait accès à la base de données il ne puisse lire les mots de passe. La clé servira aussi pour le déchiffrement des mots de passe lors de l'affichage.

Pour le chiffrement des mots de passe nous avons développé un système de chiffrement symétrique (qui utilise la même clé pour le chiffrement et le déchiffrement), nous l'avons appelé le codage Mawa
La fonction de chiffrement du codage Mawa se présente comme ceci. Premièrement on chiffre le mot de passe avec une fonction définie par f(x) = -x + le nombre de caractère disponible. Ensuite on chiffre f(mot de passe) soit l'image du mot de passe par la fonction f avec la clé de chiffrement en faisant f(mot de passe) + K, K étant la clé de chiffrement.

Schéma de l'algorithme de chiffrement du codage Mawa:

Naturellement le codage Mawa dispose en plus d'un algorithme de chiffrement, d'un algorithme de déchiffrement qui se présente de la façon suivante. Premièrement le chiffré est déchiffré par la clé de chiffrement en faisant chiffré - K, K étant la clé de chiffrement ce qui renvois une nouvelle suite de caractère qu'on appellera M_K . Ensuite on déchiffre M_K par la fonction g qui est la réciproque de la fonction f, elle est définie par g(x) = |x -nombre de caractère disponible|, g(mot de passe) correspond au mot de passe en clair.

Schéma de l'algorithme de déchiffrement du codage Mawa:

Le GDM-001 dispose de plusieurs fonctionnalités :

- Sauvegarder un mot de passe : permet de sauvegarder un mot de passe dans une base de données SQLite.
- Afficher tout : permet d'afficher tout le contenue de la base de données SQLite correspondant à l'utilisateur (les données ayant comme id l'id de l'utilisateur).
- Trouver un mot de passe : permet de rechercher un mot de passe dans la base de données SQLite correspondant à l'utilisateur (les données ayant comme id l'id de l'utilisateur).
- Importation : permet d'importer des données d'un fichier csv de l'utilisateur vers la base de données.

- Tout supprimer permet de supprimer toutes les données de la base de données (les données ayant comme id l'id de l'utilisateur)
- Supprimer : permet de supprimer un mot de passe de L'utilisateur .
- Modifier: permet de modifier un mot de passe de l'utilisateur.
- Exporter : permet d'exporter les données de l'utilisateur vers un fichier csv.

Présentation des développeurs

Nous sommes deux élèves du lycée de Sada de l'académie de Mayotte en régions d'outre-mer, nous somme en classe de 1er spécialité NSI. L'idée du gestionnaire de mot de passe viens de la faite que ikraam oublie tout le temps ses mot de passe et que Anrezki est passionné de cybersécurité.

Le développeur n°1 est : Ayouba Anrezki -> développeur

Le développeur n°2 est : Anli Ikraam -> designer

Comme le projet a été monté durant les vacances une grande partie du travail a été réaliser en distanciel, pour se faire nous avons utilisé plusieurs outils :

- GitHub : pour les dépôts du projet après chaque modification pour éviter de refaire la même chose à chaque fois.

- L'éditeur de texte Atom avec le plug-in teletype : pour coder en simultané.

- Discord : pour les vocaux et visio.

Jour 1 à 4 : Anrezki coder le système de chiffrement Codage Mawa et Ikraam faisait la première version de la GUI.

Pour coder le système de chiffrement Anrezki a dû suivre un cours sur la cryptographie. Les premières versions du système de chiffrement étaient non fonctionnelle, quelle que problème avec la différence de longueur entre mot de passe et clé de chiffrement. Qu'on a résolue avec un système Si la longueur du password est inférieur à la longueur de la master key on incrémente le password avec des lettres pseudo aléatoires préfixé de 'Σ' pour pouvoir les repérer lors du déchiffrement. 'Σ' marque la fin du mot de passe et le début de la chaine aléatoire. Si au contraire c'est la master key

qui a une longueur inférieure à la longueur du password alors on incrémente la master key avec ses (longueur password – longueur master key) premières valeurs, (longueur password – longueur master key) fois pour avoir longueur password = longueur master key.

```
if len(master_key) > len(password):
    password += 'Σ'+''.join([self.elements[random.SystemRandom().randint(0, sys.maxsize)%len(self.elements)] for i in range((len(master_key) - len(password))-1)])
elif len(password) > len(master_key):
    for i in range(len(password) - len(master_key)):
        master_key += master_key[:(len(password) - len(master_key))]
```

. Nous avons aussi rencontré quelque difficulté avec l'ouverture et la fermeture des fenêtres qu'on n'a résolu après consultation de la documentation officiel du module PyQt5, il suffisait d'instancier toutes les fenêtres avant la fermeture de notre app :

```
app = QApplication(sys.argv)
Les fenêtre ...
app.exec_()
```

Jour 4 à 7 : Anrezki crée les fonctions permettant de gérer l'utilisateur et les données, en même temps Ikraam faisait les associations de ces fonctions avec le bouton de la GUI. Difficulté rencontrée : requête SQL, résolue avec l'aide du professeur.

Enfin rédaction de la documentation au CDI du lycée.

Idée d'amélioration

- Fonction générateur de mots de passe : permet de proposer à l'utilisateur des mots de passe s'sécuriser mais pas compliqué.

- Amélioration du système de chiffrement Codage Mawa: peut-être faire du chiffrement symétrique en bloc type **CBC (Cipher Block Chaining)**

- Améliorer la GUI