

Mini-Projet Python (DS)

Problème :

1) Écrivez une application Console « **Application Multi Taches** » qui permet de réaliser un ensemble des opérations (**A, B (B1 & B2), C**) regrouper dans le Menu principal (**MenuPr**) ci-dessous. L'utilisateur doit choisir l'une des opérations de ce Menu pour accéder au différents Menus secondaires de cette Application (**MenuA , MenuB, MenuB1 et MenuB2**). Pour le dernier choix « **C** » du Menu principal, vous allez quitter simplement cette application.

Le Menu « **MenuPr** » est représenté comme suit :

```
|   Application Multi Taches   |
-----|   Menu Principal   |-----
      A- Enregistrement
      B- Authentification
          B1- Hachage
          B2- Chiffrement
      C- Quitter
```

Le contrôle de notre application et l'accès aux différentes tâches (**A, B (B1 & B2), C**) de ce Menu se fait par la variable « **choixP** » qui contient la **lettre** de la commande à appliquer.

Remarques : Vous allez créer des fonctions pour gérer le choix de ces tâches pour le Menu Principal et les Menus secondaires dans la bibliothèque personnelle « **MaBiB.py** » et faire appel à cette bibliothèque dans le script principal du projet appelé « **MainApp.py** ».

2) La représentation du Menu secondaire « **MenuA** » est la suivante :

```
-----|   Menu A : Enregistrement   |-----
      A1- Sauvegarder Données utilisateur
      A2- Lire Données utilisateur
      A3- Revenir au menu principal
```

L'option « **A1** » de ce Menu consiste à sauvegarder dans un fichier « **Authentification.txt** » les données personnelles au moins de deux personnes. Le fichier « **Authentification.txt** » est structuré comme suit :

```
""""

Id_user : 21810

Login&pwd: Ahmed&Ahmed123

Classe : CII-2-SIIR-A

Email : Ahmed@gmail.com


Id_user: 21950

Login&pwd: Sarra&sarra123

Classe : CII-2-SIIR-B

Email : Sarra@gmail.com

""""
```

Remarques : Ces données sont entrées par l'utilisateur et sauvegardés ligne par ligne de chaque étudiant. Il faut remplir ce fichier avant de passer aux autres menus de notre Application Console.

Id_user : Entrer le N° d'inscription d'un étudiant

Login : Introduire le login en **clair**

pwd : Introduire le mot de passe en mode **invisible** en utilisant soit le module « **getpass()** » ou le module « **maskpass()** ». Puis relié les deux champs par & (concaténé **Login&pwd**)

email : Introduire l'email avec une expression régulière pour la validité. Voir ce lien :

(<https://stackabuse.com/python-validate-email-address-with-regular-expressions-regex/>)

Classe : Introduire votre classe CII-2-SIIR-A / B / C / D

L'option « **A2** » consiste à lire et afficher les données déjà enregistrées par l'utilisateur sur l'écran.

L'option « **A3** » est utilisée pour revenir directement au menu principal.

3) La représentation du Menu secondaire « **MenuB** » est la suivante :

```
-----|   Menu B : Authentification   |-----  
      B1- Hachage  
      B2- Chiffrement  
      B3- Revenir au menu principal
```

Remarques : Avant d'accéder au menu secondaire « **MenuB** », il faut Vérifier la présence du fichier « **Authentification.txt** » avant de lancer les différents menus « **MenuB1** » et « **MenuB2** », si le fichier existe, on aura sur écran :

Login :

pwd :

Si le couple (**Login,pwd**) est présent dans le fichier « **Authentification.txt** » (sous la forme **Login&pwd**) l'utilisateur s'authentifie sinon Il ne va pas continuer avec les différents menus, en lui affichant il faut s'enregistrer avant de s'authentifier.

Il faut donc béliser le fichier texte et sauvegarder dans un dictionnaire **AuthDic** comme suit :

```
AuthDic={'Login1': "pwd1", 'Login2': "pwd2"}
```

Ensuite taper le login et mot de passe en mode **invisible**

L'option « **B1** » de ce Menu permet l'accès au Menu « **MenuB1** » du Hachage.

L'option « **B2** » de ce Menu permet l'accès au Menu « **MenuB2** » du chiffrement.

L'option « **B3** » est utilisée pour revenir directement au menu principal.

4) La représentation du Menu secondaire « **MenuB1** » est la suivante :

```
-----|   Menu B1 : Hachage   |-----  
      B1-a Hacher un message par MD5  
      B1-b Hacher un message par SHA256  
      B1-c Hacher un message par Blake2b  
      B1-d Cracker un message Haché  
      B1-e Revenir au menu MenuB
```

Pour les trois options « **B1-a** », « **B1-b** » et « **B1-c** », vous allez utiliser la liste des mots suivant `ListeM = ["Password", "azerty", "shadow", "hunter"]` pour appliquer l'un de ces algorithmes de hachage de la bibliothèque python « **Hashlib** ».

L'option « **B1-a** » de ce Menu consiste à hacher les quatre mots de la liste « **ListeM** » avec l'algorithme de hachage « **MD5** » et sauvegarder les résultats dans la liste « **ListeMD5** ».

L'option « **B1-b** » de ce Menu consiste à hacher les quatre mots de la liste « **ListeM** » avec l'algorithme de hachage « **SHA256** » et sauvegarder les résultats dans la liste « **ListeSHA256** ».

L'option « **B1-c** » de ce Menu consiste à hacher les quatre mots de la liste « **ListeM** » avec l'algorithme de hachage « **Blake2b** » et sauvegarder les résultats dans la liste « **ListeBlake2b** ».

L'option « **B1-d** » de ce Menu consiste à déduire l'indice du mot de la liste « **ListeM** » parmi la liste hachée « **ListeMH** ». La liste « **ListeMH** » contient les résultats de hachage des trois algorithmes (MD5, SHA256 et Blake2b) de l'un des mots de la liste « **ListeM** ».

```
ListeMH = ["3bf1114a986ba87ed28fc1b5884fc2f8",  
"0bb09d80600eec3eb9d7793a6f859bedde2a2d83899b70bd78e961ed674b32f4",  
"84cbb818cfade90c0630a1ee3145fdda66c1b1fb4862cc854c312c98c388dd84cb1f03d2ef971  
26071e9529943bf3da4abe0dacd2a5a85028381a65afe1e3623"]
```

L'option « **B1-e** » est utilisée pour revenir directement au menu « **MenuB** ».

5) La représentation du Menu secondaire « **MenuB2** » est la suivante :

```
-----|   Menu B2 : Chiffrement   |-----  
      B2-a Cesar  
          B2-a1 Chiffrement message  
          B2-a2 Déchiffrement message  
          B1-a3 Revenir au menu MenuB2  
      B2-b Affine  
          B2-b1 Chiffrement message  
          B2-b2 Déchiffrement message  
          B1-b3 Revenir au menu MenuB2  
      B2-c RSA  
          B2-c1 Chiffrement message  
          B2-c2 Déchiffrement message.  
          B2-c3 Signature  
          B3-c4 Vérification Signature  
          B1-c5 Revenir au menu MenuB2  
      B1-d Revenir au menu MenuB
```

L'option « **B2-a** » de ce Menu permet l'accès au Menu « **MenuB2a** » chiffrement de César.

L'option « **B2-a1** » de ce Menu consiste à appliquer l'algorithme de chiffrement de César sur une chaîne de caractère en respectant cette formule :

$$C(x) = (x + k) \text{ Mod}(26)$$

Avec Alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

L'option « **B2-a2** » de ce Menu consiste à appliquer l'algorithme de déchiffrement de César sur une chaîne de caractère en respectant cette formule :

$$D(x) = (x - k) \text{ Mod}(26)$$

Avec Alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

L'option « **B2-a3** » est utilisée pour revenir directement au menu **MenuB2**.

L'option « **B2-b** » de ce Menu permet l'accès au Menu « **MenuB2b** » chiffrement Affine.

L'option « **B2-b1** » de ce Menu consiste à appliquer l'algorithme de chiffrement Affine (il faut implémenter les deux clés « **Ka** » & « **kb** ») sur une chaîne de caractère en respectant cette formule :

$$Ca(x) = (Ka * x + kb) \text{ Mod}(26)$$

Avec Alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

L'option « **B2-b2** » de ce Menu consiste à appliquer l'algorithme de déchiffrement Affine sur une chaîne de caractère en respectant cette formule :

$$D(x) = (Ka^{-1} * (x - Kb)) \text{ Mod}(26)$$

Avec Alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

L'option « **B2-b3** » est utilisée pour revenir directement au menu **MenuB2**.

L'option « **B2-c** » de ce Menu permet l'accès au Menu « **MenuB2c** » chiffrement RSA.

L'option « **B2-c1** » de ce Menu consiste à appliquer l'algorithme de chiffrement RSA.

L'option « **B2-c2** » de ce Menu consiste à appliquer l'algorithme de déchiffrement RSA sur un **Mot** (chaîne de caractères).

L'option « **B2-c3** » de ce Menu consiste à créer une signature numérique du **Mot** par la clé privée.

L'option « **B2-c4** » de ce Menu consiste à vérifier la signature du mot signé.

Remarques : Pour le chiffrement RSA, il faut sauvegarder les clés générées (**pub**, **priv**) dans un fichier : il chiffre un **mot** introduit par l'utilisateur par la **clé publique**, il le déchiffre avec la **clé privée**. Il signe un mot par la clé privée de l'utilisateur, il vérifie la signature du mot.

L'option « **B2-d** » est utilisée pour revenir directement au menu **MenuB**.

6) Pour quitter la totalité de l'application Console et sortir du Menu Principal ; Tapez la commande « **C** ».

Dernier délai : Vendredi 20/10/2023