TP Sécurisation des données : Stockage des mots de passe

Pour chaque question, il est demandé de fournir un code python (`.py`) du programme et un rapport démontrant son fonctionnement.

1. Stockage en clair des mots de passe et des logins d'utilisateurs. Faire une interface textuelle basique en mode console python qui permet :
   — (2 point) d'entrer un login et un mot de passe en entrant deux fois le mot de passe
   — (2 point) d'afficher toutes les données stockées dans la base de données.
   — (2 point) de vérifier si un login et un mot de passe sont corrects pour permettre l'authentification d'un utilisateur.
2. (2 points) En partant du programme précédent modifier votre stockage des mots de passe en les hachant avec SHA-256.
3. (2 points) En partant du programme précédent modifier votre stockage des mots de passe en les hachant avec SHA-256 et en ajoutant un sel global que vous avez choix et mis dans votre code.
4. (3 points) En partant du programme précédent modifier votre stockage des mots de passe en les hachant avec SHA-256 et en ajoutant du sel par utilisateur que vous stoker dans une autre base de données.
5. (2 points) En partant du programme précédent modifier votre stockage pour utiliser le hachage `bcrypt`.
6. (3 points) Enfin chiffrer en plus avec une clef symmetrique AES-256 les mots de passe.

(2 points) Pour chaque questions évaluer les temps de vérification sur 10000 de mots de passe tiré au hasard, donner les résultats sous forme de tableau comparatif dans votre rapport.

Quelques commandes utiles

Il est recommandé d'utiliser `redis` pour la base de données.

```
from Crypto.Hash import SHA256
import bcrypt
from Crypto.Cipher import AES
```