Projet SSI (GL4 2021-2022)

Phase 1 : Enregistrement :

a- Saisie des emails (email bien écrit)
b- Saisie des pwds (inserer doublement pwd)
c- Les données seront enregistrées dans une table user (Nom, Prenom, Email, pwd (haché)) de votre Base de données.

Phase 2 : Authentification :

a- Authentification pourrait être double factor (vérification avec BD)
A- Donner votre email :
B- Donner votre password (ind. Votre mot de passe ne sera pas afficher)

Phase 3 : Menu ()

1- Codage et décodage d'un message
a- Codage
b- Décodage

2- Hachage d'un message
a- Md5
b- SHA1
c- SHA256

3 - Craquage d'un message haché
a- Md5
b- SHA1
c- SHA256

4 - Chiffrement et déchiffrement symétrique d'un message
a- DES
b- AES256

5 - Chiffrement et déchiffrement asymétrique d'un message
a- RSA
b- Elgamal

6 - Communication sécurisé entre deux clients (ChatRoom)

7 - Quitter

- Le langage Python est recommandé.
- Supposons que les mots de passe des utilisateurs se présentent comme suit : Nom.Prenom@insat.ucar.tn, avec par exemple Nom sur 6 caractères et prénom sur 5 caractères, et une partie fixe '@insat.ucar.tn'. Générez un dictionnaire de données insat.dic avec la commande crunch afin de répondre à ces contraintes.
  Vous êtes amenés dans l'étape 2 de votre menu à insérer un email à hacher pour que vous puissiez craquer le hash de cet email à l'étape 3 en s'appuyant sur le dictionnaire insat.dic.
- Pour la communication sécurisée, elle s'appuie sur des sockets entre deux terminaux pour simuler un chat room sécurisé entre eux. Le choix de la méthode de chiffrement des messages échangés est libre.

Deadline : Validation dans mon bureau le mercredi après les examens.