Cahier des charges du projet SSI (premier semestre).
L'étudiant est amené à développer une application qui ressemble à celle de Pentbox (https://github.com/technicaldada/pentbox).


Dans 1, il y aura un sous menu :

a- Pour la saisie d'un texte et son codage.
b- Pour le décodage du message codé.

Dans 2 : Pour la saisie d'un texte, le choix de la fonction de hachage, puis le calcul du hash.
Dans 3 : Pour la saisie du hash, choix du dictionnaire de données, craquage du hash.
Dans 4 :

a- Saisie du message à chiffrer
    a. Choisir l'algorithme de chiffrement symétrique
    b. Générer le mot de passe (clé symétrique) en mode illisible.
    c. Afficher le message chiffré.
b- Saisie du message chiffré
    a. Afficher l'algorithme utilisé dans le chiffrement symétrique
    b. Saisir son pwd
    c. Afficher le message en clair

Dans 5 :

a- Saisie du message à chiffrer
    a. Choisir l'algorithme de chiffrement Asymétrique
    b. Générer les paires de clés.
        i. Protéger sa clé privée par un PWD

c. Choisir soit chiffrer soit signer le message
d. Afficher le message chiffré ou bien signé.

b- Saisie du message chiffré
a. Afficher l'algorithme utilisé dans le chiffrement Asymétrique
b. Saisir son pwd de protection de sa clé privée
c. Choisir soit déchiffrer soit vérifier le message
d. Afficher le message en clair

Dans 6, Quitter.