CS557 Password Wallet Project Goals

1. The adversary capabilities expected.
    a. The adversary cannot edit/delete the “CipherPass.txt” file, or change the location where the file is stored in. (It should be in root directory of the project.)
    b. The adversary cannot in some way monitor or keep track of the user’s keyboard input when the user is using the software.
    c. The adversary cannot capture screen when the user is using the software.
2. The goals of the adversary.
    a. The primer goal for adversary is to retrieve the password stored in the password wallet.
    b. The adversary is expecting to get some relevant information concerned about the password. For example, the length or type of characters of the original password.
    c. The adversary are looking for some ways to crack the software, so that the software cannot be launched normally or there will be some run-time errors which is not supposed to be happen.
3. System goals.
    a. The security goal is to prevent unauthorized user from getting the plaintext of the password that doesn't belong to him.
    b. Anyone uses the software can create their own record. (A record contains an URL, an username and a password)
    c. User can delete the record that belongs to him after the user is authorized.

4. User profile.

a. The user cannot create a record which has a same URL and password as an existing record. Because in real world it is not possible that there are two different passwords correspond to exact same URL and username.

5. Security mechanism.

a. The process of generate cipher text of password is:

Ciphertext = AES_ENC(MD5(Userinput), password)

b. The process of decrypting cipher text of password is:

password = AES_DEC(MD5(Userinput), Ciphertext)

c. The password input textfield on GUI is implemented in a way that the user input is not shown in plaintext, but in ciphertext.

d. The decrypted plaintext cannot be copy/cut to clipboard so that it is not possible for the password to being leak.