CSE 5381,4381   Information Security II (Cryptography)
Spring 2022, © DL, UTA, 2022

Programming Assignment 2
Cipher Machine
Due: On Canvas March, 2022

Description (you will implement):

1. You are creating a file vault, a repository where a (single) user can store encrypted and/or file hashes.
That is: a user can submit a plaintext file (any type, such as photos, text, spreadsheets, movies) and you will present a menu (doesn’t need to be pretty) that allows that user to encrypt the supplied file (DES, AES, and your choice of another) then stores (saves) only the encrypted file in your vault.
Additionally, you will have an option to create a (secure) file hash (such as SHA-1 or SHA-2). You will also have an option for a user to download (copy) a file in the vault or hash to her local computer.
You should allow a file in the vault to be removed.

2. Of course, a user must authenticate herself with a password of sufficient “strength”. Absolutely no plaintext passwords should be stored.

3. Users will need help generating and storing keys remotely. Each file in the vault will have it’s own key. The keys should (of course) not be stored as plaintext.

4. You should use a “reasonable” block mode encryption, and IV if necessary. (Why?)

5. Users should also be able to decrypt a file or check a hash.

6. Bonus:
Allow multiple users, add additional encryption methods, discuss other options with instructor.

General:
Python:
(These are all the same software, different views, information)

https://pypi.org/project/cryptography/
https://github.com/pyca/cryptography
https://cryptography.io/en/latest/

C/C++:
https://www.cryptopp.com/

Comparison:
https://en.wikipedia.org/wiki/Comparison_of_cryptography_libraries

(You are free to use any of this code, texts, or anything you find on the Web/Internet,
as long as you clearly identify, in your code, where and what parts.)

Please, Submit ONLY to Canvas.
All work must be your own (you may use “external” modules or libraries),
you may reference web sites, books, etc, but
You MUST site the references.