CSE 4381,5381 Information Security II (Cryptography)
Spring 2023, © DL, UTA, 2023
Programming Assignment 5, 6
Cryptography Site
Due: On Canvas, Implementation

Description:
Create a web "site" (interface, service) that allows a user to submit a files, such as a picture, or text, and request services: encrypt, decrypt, securely hash or create and share keys.

These methods should be used:
Encryption:
  3-DES (discussed in class)
  AES (at least two different sizes)
  (At least two different block modes should be used, as well as selection of IV, and similar issues)
  Public/Private (RSA, EC, or other)
Secure Hashing
  SHA-2 or SHA-3
Key Generation and sharing
  Variation of DH or your choice

More Details:
There are several common activities that users will use in cryptographic utilities (or systems.)
Many (most?) users would like a simple web interface to common methods, but of course, it should be "secure".
The basic flow/requirements/needs are:
Users must be authenticated (user names and passwords, or other methods such as names and personal questions, or certificates.)
There must be a method to add new users, or remove them, as well for them to manage their authentication.

Then for an (any) individual user:
  Generate a password
  Generate a key (or keys)
  Encrypt a file (symmetric, one key, AES or equivalent)
  Decrypt a file
  Encrypt a file (two key, public/private key, RSA or equivalent)
  Decrypt (two key, similar to previous)
  Save keys, documents, on the system
  Hash a file
  Compare file hashes
  Upload/download files

Some hints: 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

All work must be your own, you may reference web sites, books, etc, but you must give a citation to any used.