Brandon Soledad

TCSS 487

CRYPTOGRAPHY PROJECT REPORT

Program instructions:

1) Run the java program after you have opened it in your IDE.
2) You will be prompted to choose a service from the program the options are numbered from 1-10.
3) Choose your service.

Services:

1) Cryptographic Hash from a file: We take in the file then read the bytes, then we compute the hash using symmetric cryptography and KMACXOF256.
2) Cryptographic Hash from input: Same as above except we take a user given input instead of reading from a file.
3) Encrypt file under a given password: We encrypt the file using KMACOF256 based on the password given by the user
4) Decrypt cryptogram under given password: Similar to above except we are decrypting the file we originally encrypted with KMACOF256 as long as the given password is correct.
5) Compute Authentication tag (MAC): Computed using hash function KMACXOF256 converting bytes to hex.
6) Generate elliptic key pair from given password and write to a file: Uses the KMACXOF256 algorithm with Elliptic Curve Cryptography utilizing a curve defined by a pair of constants and a field.
7) Encrypt file under given elliptic public key file: Encrypts the file after giving the password using KMACXOF256 to create a new cryptogram.

8) Decrypt elliptic-encrypted key file under a given password: Like above, once given the password the file will be decrypted using KMACXOF256.
9) Sign a given file from a given password to a file: Signature is written to file using ECC and KMACXOF256.
10) Verify given file and its signature file under a given public key file: Verifies using KMACXOF256 and under ECHDIES public key.

BUGS:

Not sure why but sometimes when a service is using JFileChooser the window that pops up to choose a file does not show up. I tried running the program in Eclipse and this did not happen. It happens when I run it under my usual workspace in Visual Studio Code. I am not sure why.