CSE 478

Lab 6: Programming Symmetric & Asymmetric Crypto Report

Abdullah Aziz Sharfuddin | Nazmul Islam
2014331011 | 2014331034

To run the program use $ python main.py

AES(ECB and CBC)

When the program is running it will show 5 options. By pressing 1 one can enter into AES encryption and decryption system. Then the program will ask for whether it is ECB or CBC. For ECB press 1 and for CBC press 2. After entering any of these it will again ask for key length. Press 1 for 128 bit key length and 2 for 256 bit key length. Now entering the message and pressing enter it will show the encrypted message and also decrypted message.

RSA encryption and decryption

Press 2 for RSA encryption. Then it ask for a message to encrypt. After entering your message hit enter. Then it will show the encrypted text along with the decrypted message. And all the keys and messages(encrypted and decrypted) are stored.

RSA signature

By pressing option 3 one can enter into RSA signature. Input is taken from input.txt file. Signature is generated and add to signature.txt file. Signature and input is send for verification. If the signature is verified a message “Verification successful” will be shown.

SHA- 256

Pressing 4 one can do hashing. It uses sha-256 hashing mechanism to hash a file. After pressing 4 it will ask for a file name. The file has to be in the same directory. We have kept a file named ”fileToHash”. After entering the file the name hit enter. And the hashed file will be saved in a filename “hashout.txt” in the same directory.

We have also implemented timing. It will show time taken after every operation.

Resources we used.

1. https://techtutorialsx.com/2018/04/09/python-pycrypto-using-aes-128-in-ecb-mode
2. https://stackoverflow.com/questions/46904355/aes-128-cbc-decryption-in-python
3. https://stackoverflow.com/questions/30056762/rsa-encryption-and-decryption-in-python
4. https://gist.github.com/ErbaAitbayev/8f491c04af5fc1874e2b0744965a732b#file-rsa-py-L126
5. https://stackoverflow.com/questions/22058048/hashing-a-file-in-python

All the respective resource links are commented in the source files.