Encrypted File Storage
Scott Gordon, Than Lim, Christa Davis

For our project, we started by creating a simple client server program. We adjusted this client server model to be able to send and receive files. From there we found an implementation of AES 128-bit encryption and custom fit that implementation to our program by getting it to work with text files and increasing the length of text it was able to handle. We include a reference to the source material in our submission. From there we wanted to implement RSA to allow for secure communication between client and server but failed to get an implementation working with our project in time for the submission. We did however get a simple version of RSA working on its own that we believe is worth adding to our submission because of the substantial work it took to develop, even though it does not work specifically with our project.

Aside from the RSA implementation, the most challenging parts of this project were two things primarily. The first being getting the AES implementation to work with longer text, and specifically text files rather than just command line input. The second thing was getting the ciphertext to properly send over the sockets in our client server implementation.

Our project submission includes work relevant to this class in the form of AES and RSA. We directly use AES encryption as the primary security method in our application. We have a working sample of RSA as a part of our submission that works on it's own, just not with our project. In continuing this project, we plan to develop our implementation of RSA so that it can work with our project, this would include changing some things about our RSA implementation as well as our project.

To develop and run our project, we are using macOS as our operating system. We developed the codebase for our project entirely within Visual Studio Code. Further compilation and running instructions are given separately within the README.txt for our project.

Here I will include running samples for our project:

Encrypting a file:

```
[scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./aes/encrypt
Enter file name to encrypt: myFile.txt
Working on: myFile.txt
Message Length in encrypt.cpp :230
number of encrypted characters: 240

Encrypted message in hex:
b9 29 95 bf 47 8f fd df c8 b5 f1 b7 a5 15 ad 42 2c 5e b8 43 43 3b a0 6a cf c1 c9
 ad fd f8 9a 66 95 26 32 3 c8 21 4a 11 f0 92 e6 14 24 5 67 b1 18 d8 46 4d 67 9d
85 c7 d6 8a 76 7b 4b c3 e3 e8 59 6a 62 2f 82 b 1f 3 1a 4a f1 4e 44 d2 ad 7f d6 1
5 46 dc af 17 4d 55 ef 17 a6 77 48 26 70 42 6d 11 95 59 1e e1 4 31 5d 89 e3 6c 6
5 e3 fb 9d ec a8 c9 a 8d aa fd a 60 c3 88 1d e3 8c 88 d9 cb 14 62 e3 fe 15 93 78
 3f a f7 7d 82 50 dc 4c 49 d6 db 85 13 9d a5 18 f1 e6 df f0 b1 78 64 2c 55 a8 62
 da 57 e4 f6 49 35 83 30 9e d 3e 27 82 cb 14 62 e3 fe 15 93 78 3f a f7 7d 82 50
dc 4c 40 47 e1 ae 81 0 4d 3e aa 1e a0 aa de bc c0 1a 7 ee e6 7c df 74 9 22 b8 55
 14 c3 22 8d b1 cf 12 76 9b 25 4a e5 21 46 22 23 c6 18 e8 ad b4 c1

Encrypted message stored in: ./data/client/ENCmyFile.txt
[scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./aes/encrypt
```

Client uploading a file:

```
[scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./client
Socket successfully created..
connected to the server..
1 : Upload
2 : Download
Please select an option : 1
Please enter the name of the file : ENCmyFile.txt
[LOG] : File is ready to Transmit.
[LOG] : Transmission Data Size 240 Bytes.
[LOG] : Sending...
[LOG] : Transmitted Data Size 240 Bytes.
[LOG] : File Transfer Complete.
[scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./client
```

Client downloading a file:

```
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./client
Socket successfully created..
connected to the server..
1 : Upload
2 : Download
Please select an option : 2
Please enter the name of the file : ENCmyFile.txt
[LOG] : File Created.
[LOG] : Data received 240 bytes
[LOG] : Saving data to file.
[LOG] : File Saved.
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 %
```

Client decrypting a file:

```
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./aes/decrypt
Enter file name to decrypt: ENCmyFile.txt
Working on: ENCmyFile.txt


Decrypted message in hex:
48 65 72 65 20 69 73 20 6d 79 20 74 65 78 74 20 66 69 6c 65 20 6c 69 6e 65 20 6f
 6e 65 2e a 54 68 69 73 20 69 73 20 6c 69 6e 65 20 74 77 6f 20 6f 66 20 6d 79 20
 74 65 78 74 20 66 69 6c 65 2e a 74 68 69 73 20 66 69 6c 65 20 68 61 73 20 61 20
 6c 6f 74 20 6f 66 20 6c 69 6e 65 73 20 3a 29 a 54 68 69 73 20 69 73 20 74 68 65
 20 73 65 63 6f 6e 64 20 74 6f 20 6c 61 73 74 20 6c 69 6e 65 20 6f 66 20 6d 79 2
0 74 65 78 74 20 66 69 6c 65 20 28 6c 69 6e 65 20 34 29 2e a 54 68 69 73 20 69 7
3 20 74 68 65 20 6c 61 73 74 20 6c 69 6e 65 20 6f 66 20 6d 79 20 74 65 78 74 20
66 69 6c 65 2e a 4a 75 73 74 20 6b 69 64 64 69 6e 67 2c 20 74 68 69 73 20 69 73
20 74 68 65 20 6c 61 73 74 20 6c 69 6e 65 2e 0 0 0 0 0 0 0 0 0 0
Decrypted message stored in: ./data/client/myFile.txt
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./client
```

Server running and receiving a file:

```
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./server
[LOG] : Socket successfully created..
[LOG] : Socket successfully binded..
[LOG] : Server listening..
[LOG] : server accept the client...
[LOG] : Option 1 selected...
[LOG] : Waiting for file selection...
[LOG] : File Created.
[LOG] : Data received 240 bytes
[LOG] : Saving data to file.
[LOG] : File Saved.
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./server
```

Server running and sending a file:

```
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./server
[LOG] : Socket successfully created..
[LOG] : Socket successfully binded..
[LOG] : Server listening..
[LOG] : server accept the client...
[LOG] : Option 2 selected...
[LOG] : Requesting file name...
[LOG] : File is ready to Transmit.
[LOG] : Transmission Data Size 240 Bytes.
[LOG] : Sending...
[LOG] : Transmitted Data Size 240 Bytes.
[LOG] : File Transfer Complete.
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./server
```

RSA demo:

```
scottgordon@Scotts-MacBook-Pro-2 NSfinal2 % ./rsaDemo/rsaDemo

INPUT
N: 1.58087e+09
pubKey: 7
priKey: 0.142857

Original message: Net
Encrypted Message: 9.44993e+46
Decrypted Message: Net

scottgordon@Scotts-MacBook-Pro-2 NSfinal2 %
```