CPSC 526 Assignment #4

Steven Leong 10129668 T01

Marco Quines 10138118 T03

----------------------------------------------------------HOW TO RUN---------------------------------------------------------

To run this program you will need to open two terminals

1. Server terminal

python3 server.py <PORT> <KEY>

1. Client terminal

python3 client.py <\*COMMAND> <FILENAME> <HOSTNAME:PORT> <\*CIPHER> <KEY>

Options:

\*COMMAND : read or write

\*CIPHER : null or aes128 or aes256

Note: <KEY> and <PORT> must be the same

---------------------------------------------------TEST FOR CORRECTNESS------------------------------------------------

------------------------------------------------COMMUNICATION PROTOCOL------------------------------------------------

|  |  |  |
| --- | --- | --- |
| Client |  | Server |
|  | Server starts and initializes |  |
|  | Server binds to PORT and waits for a Client |  |
|  | Client initializes arguments, creates random nonce and connects |  |
| ----- > | Client sends first message (cipher,nonce) in the clear | ----- > |
| < ----- | Server sends back acknowledgement that the message was received | <----- |
| <----- | Server sends key challenge to Client | <----- |
| -----> | Client computes and sends back reply that can only be computed using the secret key | -----> |
| <----- | Server verifies the reply and sends back success/failure message | <----- |
| -----> | If success,  Client sends (operation;filename) request | -----> |
| <----- | Server responses indicating whether the operation is valid or not.  If valid,  Proceed to Data transfer | <----- |
| <----- | If operation is **read**:  Server checks if the file exists. If it does the Server continues, if not the Server sends the Client an error message | <----- |
| <----- | Server reads the file, encrypts it, and sends it to the Client | <----- |
|  | Client receives the contents, decrypts it, removes padding, and writes to <FILENAME> |  |
| -----> | If operation is **write**:  Server tries to open file to write, If failed Server sends error msg to Client | -----> |
| -----> | Client reads the file, encrypts it, and sends it to the Server | -----> |
|  | Server receives the contents, decrypts it, removes padding, and writes to <FILENAME> |  |

------------------------------------------------------TIMING TESTS------------------------------------------------------------