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------------------------------------------------------------

|  |  |  |  |
| --- | --- | --- | --- |
| WRITE | NULL | AES128 | AES256 |
| 1KB Test: 1 | 0.325 | 0.213 | 0.2 |
| 1KB Test: 2 | 0.224 | 0.205 | 0.205 |
| 1KB Test: 3 | 0.209 | 0.211 | 0.207 |
| 1KB Test: 4 | 0.213 | 0.202 | 0.203 |
| 1KB Test: 5 | 0.204 | 0.21 | 0.25 |
| 1KB Test: 6 | 0.204 | 0.201 | 0.205 |
| 1KB Test: 7 | 0.217 | 0.207 | 0.211 |
| 1KB Test: 8 | 0.208 | 0.211 | 0.211 |
| 1KB Test: 9 | 0.208 | 0.204 | 0.201 |
| 1KB Test: 10 | 0.212 | 0.197 | 0.203 |
|  |  |  |  |
| 1MB Test: 1 | 0.337 | 0.21 | 0.527 |
| 1MB Test: 2 | 0.332 | 0.212 | 0.542 |
| 1MB Test: 3 | 0.328 | 0.192 | 0.546 |
| 1MB Test: 4 | 0.329 | 0.203 | 0.535 |
| 1MB Test: 5 | 0.328 | 0.204 | 0.545 |
| 1MB Test: 6 | 0.332 | 0.2 | 0.502 |
| 1MB Test: 7 | 0.337 | 0.198 | 0.536 |
| 1MB Test: 8 | 0.321 | 0.197 | 0.54 |
| 1MB Test: 9 | 0.331 | 0.213 | 0.536 |
| 1MB Test: 10 | 0.338 | 0.214 | 0.533 |
|  |  |  |  |
| 1GB Test: 1 | 2m1.496 | 0.36 | 14.311 |
| 1GB Test: 2 | 2m9.000 | 0.212 | 14.079 |
| 1GB Test: 3 | 2m6.64 | 0.212 | 12.735 |
| 1GB Test: 4 | 2m7.583 | 0.222 | 12.796 |
| 1GB Test: 5 | 2m10.339 | 0.217 | 13.168 |
| 1GB Test: 6 | 2m0.700 | 0.202 | 12.379 |
| 1GB Test: 7 | 1m57.476 | 0.216 | 12.838 |
| 1GB Test: 8 | 2m12.105 | 0.212 | 13.29 |
| 1GB Test: 9 | 2m3.401 | 0.218 | 13.133 |
| 1GB Test: 10 | 2m3.401 | 0.234 | 12.9 |
|  |  |  |  |
| READ |  |  |  |
| 1KB Test: 1 | 0.193 | 0.197 | 0.3 |
| 1KB Test: 2 | 0.19 | 0.199 | 0.3 |
| 1KB Test: 3 | 0.201 | 0.198 | 0.503 |
| 1KB Test: 4 | 0.208 | 0.195 | 0.255 |
| 1KB Test: 5 | 0.201 | 0.195 | 0.258 |
| 1KB Test: 6 | 0.195 | 0.201 | 0.21 |
| 1KB Test: 7 | 0.192 | 0.198 | 0.204 |
| 1KB Test: 8 | 0.199 | 0.203 | 0.228 |
| 1KB Test: 9 | 0.194 | 0.198 | 0.243 |
| 1KB Test: 10 | 0.205 | 0.202 | 0.234 |
|  | 0 |  |  |
| 1MB Test: 1 | 0.377 | 0.195 | 0.105 |
| 1MB Test: 2 | 0.268 | 0.097 | 0.128 |
| 1MB Test: 3 | 0.277 | 0.092 | 0.232 |
| 1MB Test: 4 | 0.341 | 0.084 | 0.129 |
| 1MB Test: 5 | 0.249 | 0.098 | 0.086 |
| 1MB Test: 6 | 0.261 | 0.091 | 0.085 |
| 1MB Test: 7 | 0.267 | 0.082 | 0.108 |
| 1MB Test: 8 | 0.262 | 0.087 | 0.14 |
| 1MB Test: 9 | 0.265 | 0.198 | 0.095 |
| 1MB Test: 10 | 0.27 | 0.109 | 0.097 |
|  |  |  |  |
| 1GB Test: 1 | 1.551 | 0.2 | 0.091 |
| 1GB Test: 2 | 1.493 | 0.112 | 0.103 |
| 1GB Test: 3 | 1.521 | 0.08 | 0.09 |
| 1GB Test: 4 | 1.49 | 0.088 | 0.089 |
| 1GB Test: 5 | 1.516 | 0.08 | 0.084 |
| 1GB Test: 6 | 1.646 | 0.083 | 0.085 |
| 1GB Test: 7 | 1.516 | 0.085 | 0.086 |
| 1GB Test: 8 | 1.489 | 0.084 | 0.086 |
| 1GB Test: 9 | 1.474 | 0.081 | 0.083 |
| 1GB Test: 10 | 1.502 | 0.093 | 0.086 |