

Assignment 4  
CPSC 526 Fall 2017  
November 12, 2017

Mason Lieu	Shane Sims
ID: 10110089	ID: 00300601
Tutorial 04	Tutorial 04
mliu@ucalgary.ca	shane.sims@ucalgary.ca

## How to run Server and Client

### Running the server

---

```
1 python FTserver.py <port number> <key>
```

---

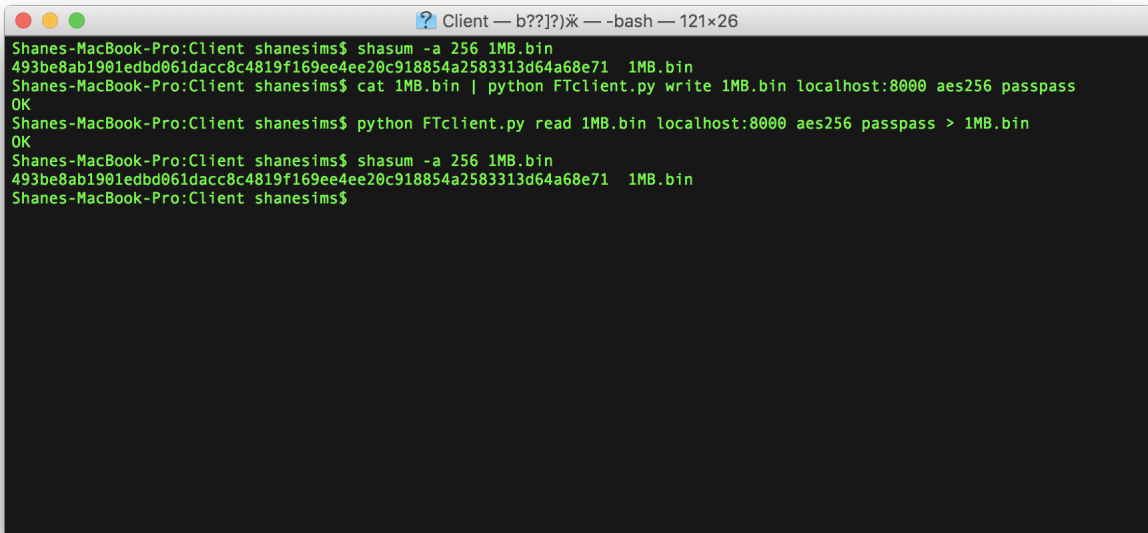
### Running the client

---

```
1 python FTclient.py <command> <file name> <host>:<port> <cipher> <key>
```

---

## AES256 upload/download/checksum test

A terminal window titled "Client — b??[?]\* — -bash — 121x26" showing a series of commands and their outputs. The commands are: 1. shasum -a 256 1MB.bin, which outputs a long hexadecimal string. 2. cat 1MB.bin | python FTclient.py write 1MB.bin localhost:8000 aes256 passpass, which outputs "OK". 3. python FTclient.py read 1MB.bin localhost:8000 aes256 passpass > 1MB.bin, which outputs "OK". 4. shasum -a 256 1MB.bin, which outputs the same long hexadecimal string as the first command. The terminal background is black with green text.

```
Shanes-MacBook-Pro:Client shanesims$ shasum -a 256 1MB.bin
493be8ab1901edbd061dacc8c4819f169ee4ee20c918854a2583313d64a68e71 1MB.bin
Shanes-MacBook-Pro:Client shanesims$ cat 1MB.bin | python FTclient.py write 1MB.bin localhost:8000 aes256 passpass
OK
Shanes-MacBook-Pro:Client shanesims$ python FTclient.py read 1MB.bin localhost:8000 aes256 passpass > 1MB.bin
OK
Shanes-MacBook-Pro:Client shanesims$ shasum -a 256 1MB.bin
493be8ab1901edbd061dacc8c4819f169ee4ee20c918854a2583313d64a68e71 1MB.bin
Shanes-MacBook-Pro:Client shanesims$
```

Figure 1: Test for correctness

## Communication Protocol

### **write** command

	Client	Server
1.	send write	
2.		send ACK
3.	send fileName	
4.		echo fileName
5.	encrypt 1024 byte blocks and send	
6.		receive and decrypt blocks
7.	send EOF	
8.		send status/result flag
9.	print status	

### **read** command

	Client	Server
1.	send read	
2.		send ACK
3.	send file name	
4.		send file size
5.		encrypt 1024 byte blocks and send
6.	receive and decrypt blocks	
8.	send status/result flag	
9.	print status	

## Timing Tests