Rumen Kasabov  
ID: 10128754  
Tutorial Section: T02

Group partner: Michael Radke

~~~

To run the code you need to start the server first on terminal as follows:

$python3.6 server.py port key

Where:

* port is the port number the server will be listening on
* key is the secret key of the server

Then you need to start the client as follows:

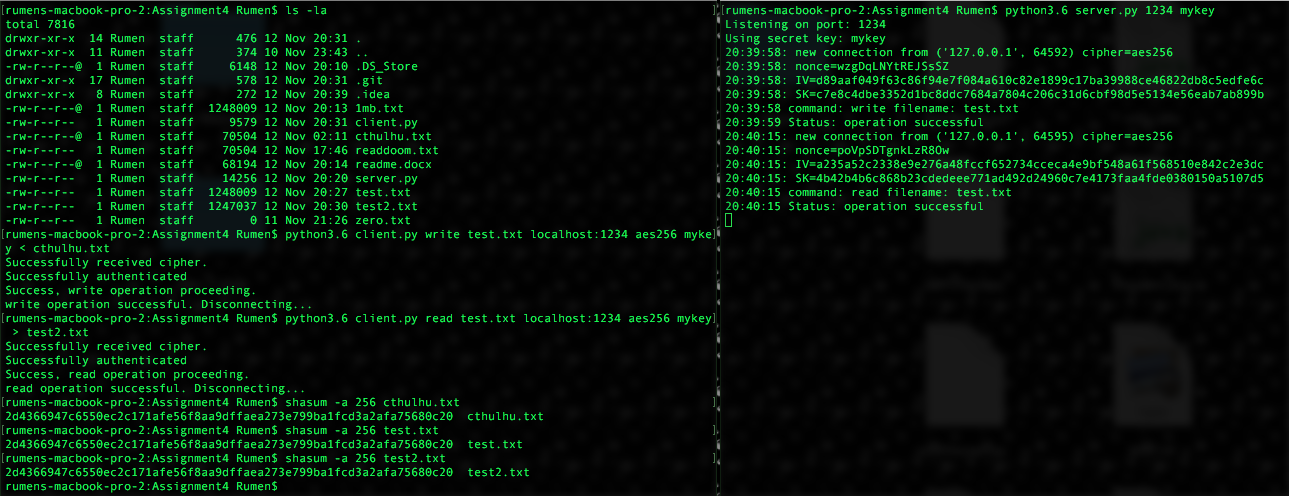
$python3.6 client.py command filename hostname:port cipher key

Where:

* command is the file operation the client will be performing (either ‘read’ or ‘write’)
* filename is the file that the server will read from to the client or write to on the server side
* hostname:port is the server address of the server the client is connecting to and port is the port number of that server. A colon separates them.
* cipher is the cipher being used (either aes128, aes256 or the null cipher)
* key is the secret key of the client

Test for correctness:

We upload (write) a 71KB text file to the server from the client. Then download (read) the uploaded file to a different file. This yields the same checksums for all three files.



Note: Left terminal is the client.py program and right terminal is the server.py.

As seen in the image above, cthulhu.txt is a ~71KB file:

:::Screen Shot 2017-11-12 at 8.49.34 PM.png

We connect to the server and read cthulhu.txt standard input and write it to a file called test.txt. Afterwards we connect to the server again, reading it test.txt into another file called test2.txt through standard output.

Then we compute the checksums using sha256 which as seen in the left terminal in the image yields the same three checksums:

