**CPSC 526 Assignment 3: Network data-transfer w/ Symmetric encryption**

How to compile/run

To run server:

"python3 server.py [port] [key]"

[port] = port number where server will be listening

[key] = password used for encryption if client decides to use; if not provided, server will generate a random 32-character password

Note: server is assumed to be running in localhost

To run client:

"python3 client.py [cmd] [filename] [ip]:[port] [cipher] [key]"

[cmd] = determines if client will be uploading/downloading data to/from server

can either be read/write

[filename] = if cmd is read, server will send contents of filename

else, server will upload contents of stdout to filename

[ip] = ip address of server

[port] = port server is listening to

[cipher] = specifies what encryption algorithm is used for communication

can be none/aes128/aes256

[key] = key to be used for encryption. not necessary if cipher=none

Communication Protocol

1) Client connects to server

2) Client sends [Cipher, IV] to server in the clear

3) If encryption requested, password authentication:

a) Client sends encrypted IV to server and vice versa

b) Both parties compare received encrypted IV to locally encrypted IV

c) If the same, password checks out. Else, connection is terminated.

4) Client sends [cmd, filename] to server. If cipher is specified, this is encrypted.

5) If cmd=write

a) client sends data size and then data in 4096 chunks to server

b) server receives and processes data

c) once client has sent all data, server sends response to client and client displays this to console

6) If cmd=read

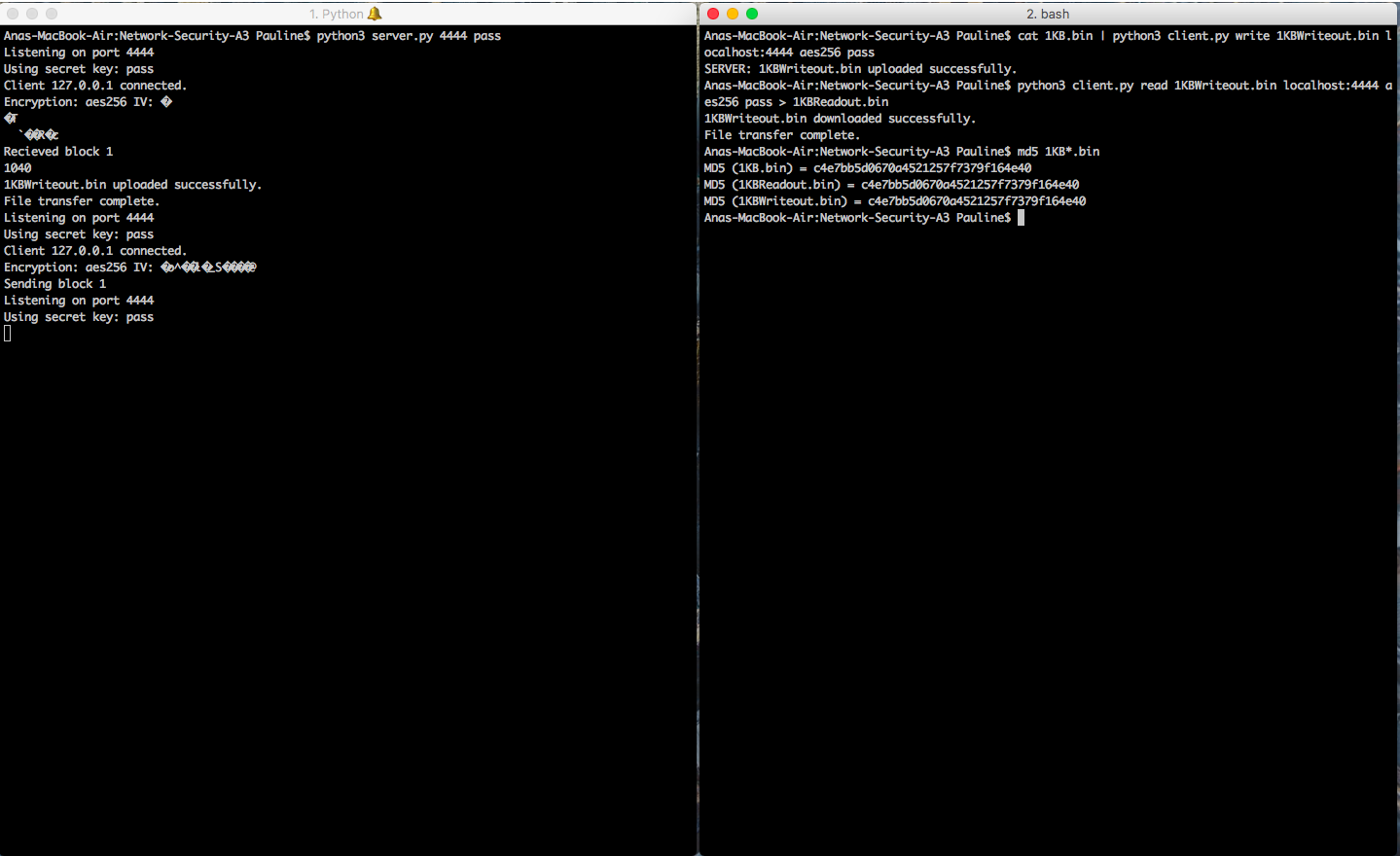
a) server sends data size and then data in 4096 chunks to client

b) client receives and processes data

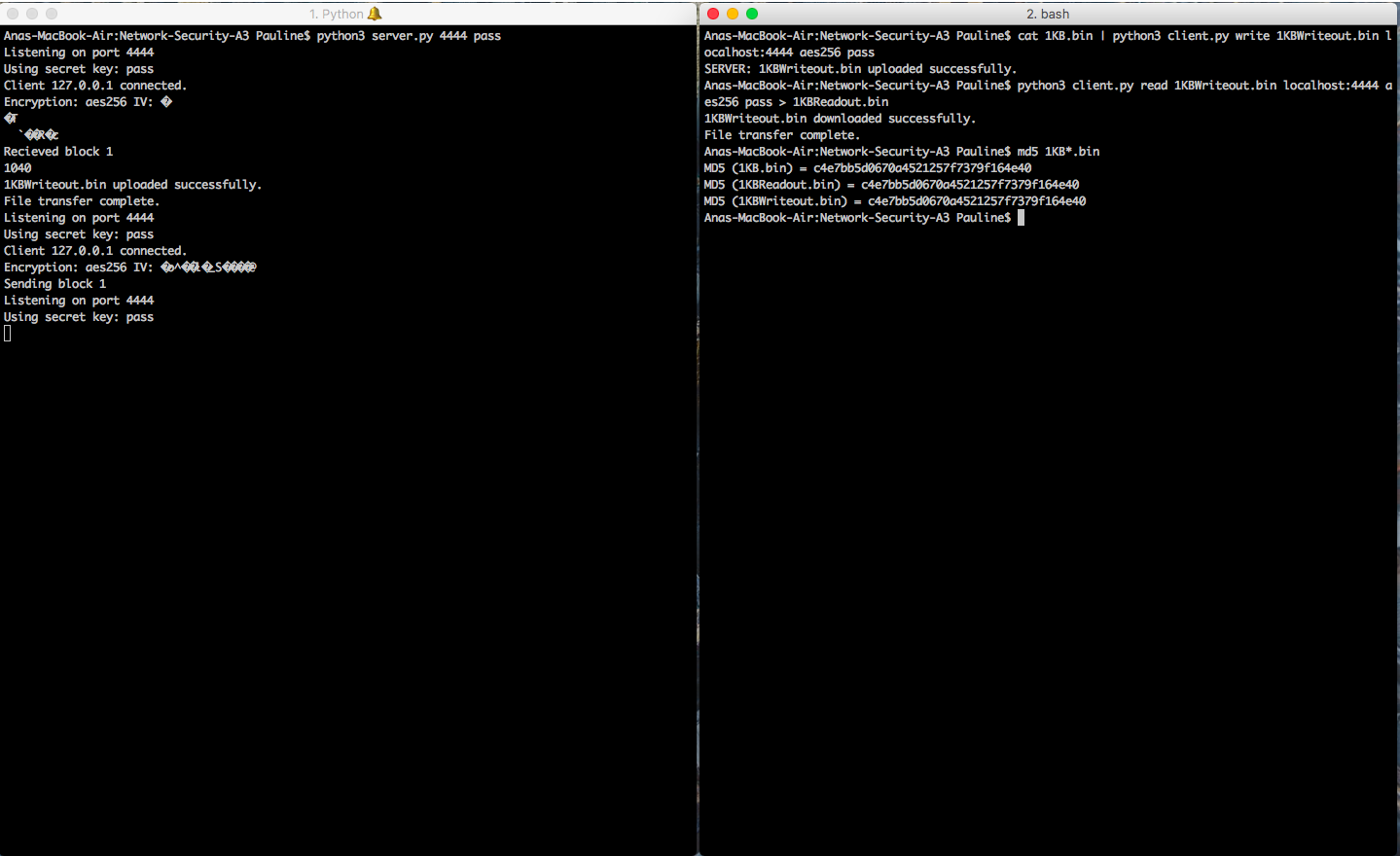
7) Connection is closed

Testing AES256 on 1KB bin file using MD5 hash

Server:



Client:



Timing tests

*Note: a full list of raw values can be found in timedata.txt*

Write

|  |  |  |  |
| --- | --- | --- | --- |
| **File size** | **None** | **AES128** | **AES256** |
| 1KB | 0.687s | 1.101s | 1.115s |
| 1MB | 1.975s | 1.872s | 1.534s |
| 1GB | 55m20.356s | 1h1m08.678s | 1h2m10.434s |

Read

|  |  |  |  |
| --- | --- | --- | --- |
| **File size** | **None** | **AES128** | **AES256** |
| 1KB |  |  |  |
| 1MB |  |  |  |
| 1GB |  |  |  |

<explanation here>