CPSC 526 Assignment 3: Readme

Albert Luu (10129499) , Ana Pauline Telan (10124075)

# Compiling and running

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]

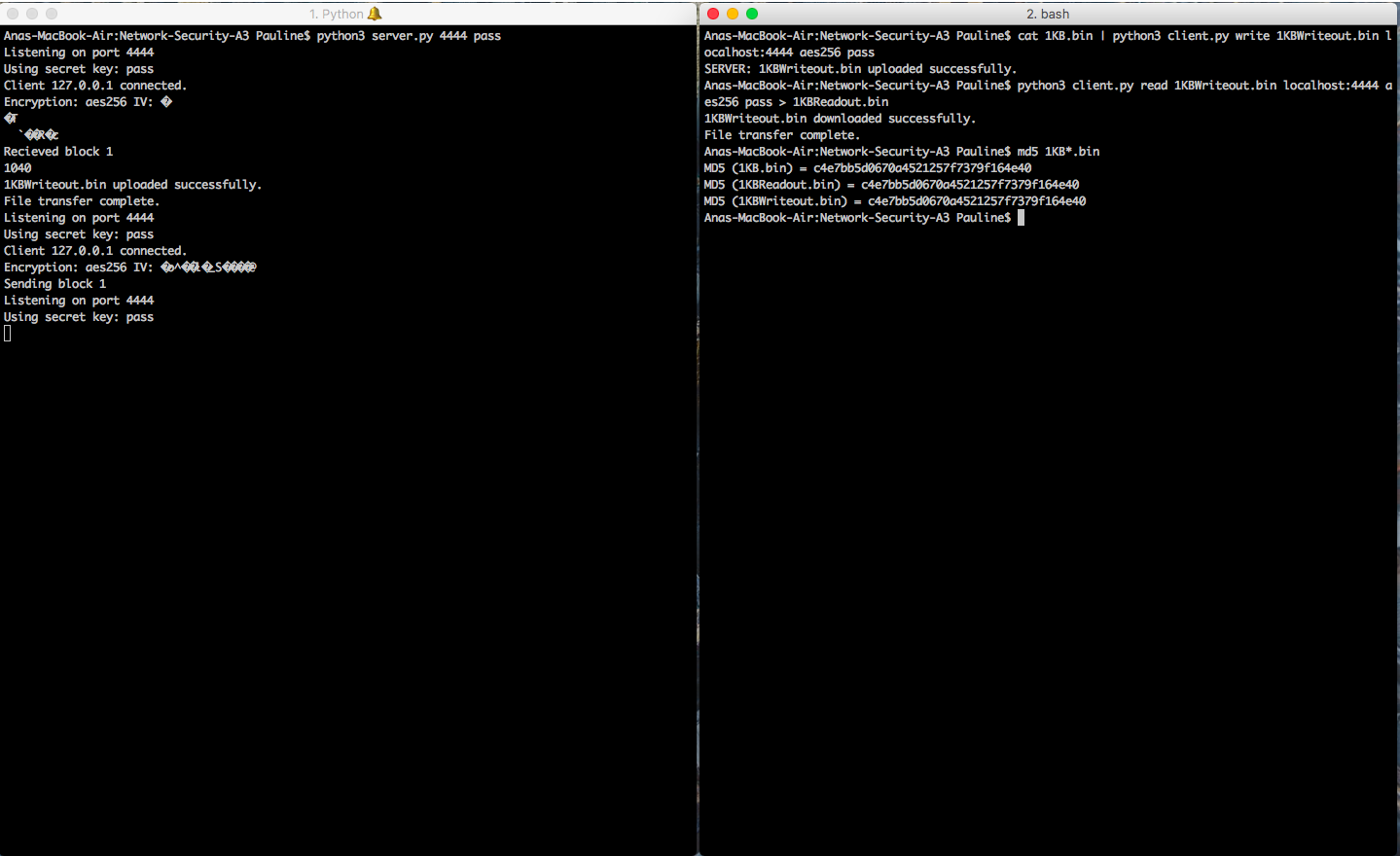
|  |  |
| --- | --- |
| cmd | Determines if client will be uploading/downloading data to/from server either be read/write |
| filename | If cmd is read, server will send contents of filename, else the server will upload contents of stdout to filename |
| ip | IP address of server |
| port | The port the server is listening on |
| cipher | specifies what encryption algorithm is used for communication, can be none, aes128 or aes256 |
| key | Key to be used for encryption. Not applicable when cipher is none. |

# Communication Protocol

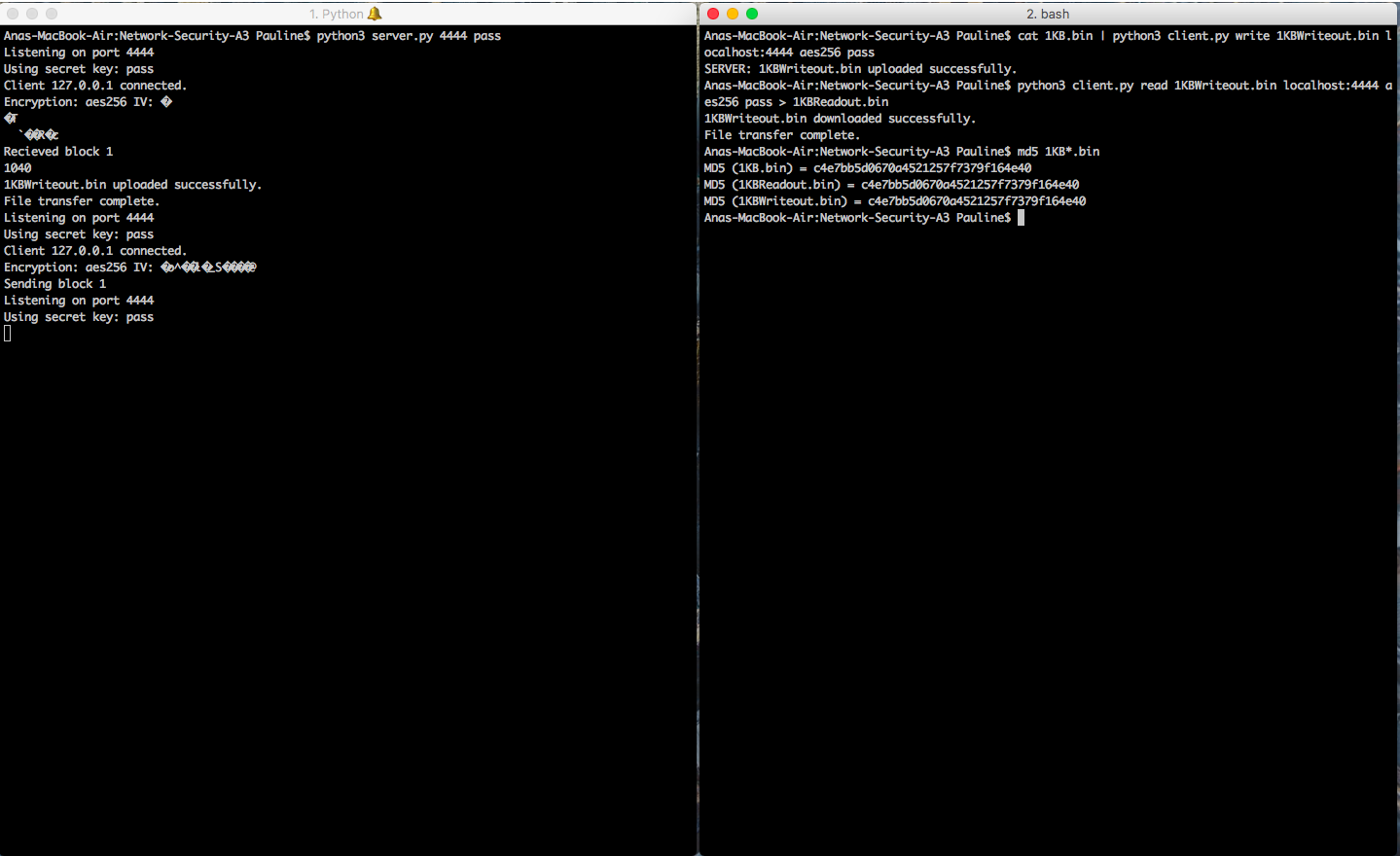
1. Client connects to server
2. Client sends [Cipher, IV] to server in the clear
3. If encryption requested, password authentication:
   1. Client sends encrypted IV to server and vice versa
   2. Both parties compare received encrypted IV to locally encrypted IV
   3. If the same, password checks out. Else, connection is terminated.
4. Client sends [cmd, filename] to server. If cipher is specified, this is encrypted.
5. If cmd=write
   1. client sends data size and then data in 4MB chunks to server
   2. server receives and processes data
   3. once client has sent all data, server sends response to client and client displays this to console
6. If cmd=read
   1. server sends data size and then data in 4MB chunks to client
   2. 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 | 0.684s | 1.100s | 1.108s |
| 1MB | 1.962s | 1.696s | 1.505s |
| 1GB | 13.825s | 56.565s | 58.740s |

Read

|  |  |  |  |
| --- | --- | --- | --- |
| **File size** | **None** | **AES128** | **AES256** |
| 1KB | 0.681s | 0.957s | 0.945s |
| 1MB | 1.116s | 1.449s | 1.582s |
| 1GB | 13.006s | 54.350s | 57.884s |

<explanation here>