**CPSC 526**

**Assignment 4**

**Tutorial: T01**

**Name: Artin Rezaee-Anzabee**

**ID: 10121269**

**Partner: Sam Ao**

**Running the program:**

**Running the server:**

Run the server by: python3 server.py <Port> <Key>

**Running the client:**

To upload a file to the server run: cat <fileToUpload> | python3 client.py <command> <fileName> <address>:<Port> <cipher> <Key>

To download from the server run: python3 client.py <command> <fileName> <address>:<Port> <cipher> <Key> > <fileToWriteTo>

Command can be read and write

Cipher can be null, aes128, and aes256

Key is the key used by server and client for authentication. The key used by server and client must be the same for the communication to progress

**Connecting to server and handshake details:**

The server will be bound to a source port and will accept clients. Upon client’s connection, server received an unencrypted message from the client including the nonce and cipher specified by the client. The server will then use this information to create the initialization vector and session key for this particular session. Server will then use the specified cipher (or null) to encrypt further communication between the client. The server will then challenge the client about its knowledge of the key. To do so, the server generates a random authentication token and sends it to the client. The client then has to add their key to the authentication token and send the hash of the auth token and key over to the server. The server then does the same and if the two strings match, the server allows the client to execute its command (read/write). Each client is only able to execute one command before they are terminated. If the client is uploading a file, the server will receive data from client, give a response to client that it has received it, and write the receiving data to a file specified by the user. If the command is read, then the server will read from the file specified by the user and send each line to the client, wait for the client to give a response on whether they have received the data chunk, and then continue reading the next line. The server will send a feedback regarding the success or failure of the operation to the client. When the operation is over, the server will the terminate the client.

**Client Server operation**

**Uploading a 1MB file using AES256**

**Downloading a 1MB file using AES256**

**Timing**