

How to run– To run the client first need to compile server and client and first need to run server then client.

Language and Library– C++, OpenSSL.

Description– At first 3 keys have been generated from using Diffiehellman Key exchange. Those 3 keys have been used for encryption and decryption using 3DES. First client connect to server. Then using diffiehellman key exchange 3 keys are generated for encryption decryption. If client wants any file to download it send a request to the server asking for that file. Server responds with proper message if file is not present. If file is present server starts transferring file in chunk size of 1024 bytes by encrypting the chunks using 3DES and sends it to the client. Client receives those chunks one by one and decrypts those chunks by those 3 keys using 3DES and writes the decrypted chunk to appropriate file position. Multiple clients can connect to the server at anytime. To disconnect the client send the server disconnect message and the server disconnects the clients with proper message.