ECE 1150: Intro to Computer Networks – Lab 2

XOR Cipher Encryption Server/Client

Zachary Mattis – 4020473

For my lab 2 project, I designed a server/client pair that is used to encode and decode an input file by passing it through an XOR cipher encryption algorithm on the server side. The program works by parsing an input file on the client side into a raw byte stream that is read into a buffer. This data is passed onto the server after a TCP connection has been established. On the server side, the data is sent through an XOR cipher algorithm that XOR’s each byte of data with a designated encryption character, in this case ‘Z’. After being passed through this function, the data is sent back to the client, where it is received. This processed data is then written back to the original file that it came from, creating an encrypted file. This process can be repeated once again, with the encrypted file to decrypt the file back into the original message.

Input file: **secret.txt**

My secret message...

Decrypted message:

Encrypted message:

\_#z)?9(?.z7?));=?ttt

Client

Server

Input Input

./server

./client unixs.cis.pitt.edu secret.txt

Encrypting message…

file: "secret.txt"

client: connecting to 136.142.4.246

client: sending data to the server...

Sending: "My secret message..."

client: receiving data from the server

Received: "\_#z)?9(?.z7?));=?ttt"

client: writing server data back to file

server: waiting for connections...

server: got connection from 136.142.4.246

Received: "My secret message..."

server: running XOR cipher...

Sending: "\_#z)?9(?.z7?));=?ttt"

Decrypting message…

file: "secret.txt"

client: connecting to 136.142.4.246

client: sending data to the server...

Sending: "\_#z)?9(?.z7?));=?ttt"

client: receiving data from the server

Received: "My secret message..."

client: writing server data back to file

server: waiting for connections...

server: got connection from 136.142.4.246

Received: "\_#z)?9(?.z7?));=?ttt"

server: running XOR cipher...

Sending: "My secret message..."

Note: IP addresses for the client and server are the same because I was using the Pitt unixs.cis.pitt.edu machine to run both the client and the server.