Brandon Lokey

Wireless Networks and Security

Lab 1

**Implementation and Application of DES**

How It Works: This application utilizes client/server socket programming to create a chat program that utilizes DES encryption. The server starts a connection and then waits for a client. When a client connects, the client generates a key and then puts it in a file that both the client and server can access. After that, the client and server take turns sending user input and then decrypting it using DES encryption. The program shows plaintext, the key, and then the encrypted/decrypted data.

How It Was Made: I utilized Java’s socket library and input/output stream libraries to handle the server/client communications. For the encryption, I used Java’s various security and crypto libraries to generate keys and to encrypt/decrypt data when being sent/received.

Testing: When writing the program, I tested the application by sending many different inputs to make sure everything is being encrypted and decrypted properly. I compared the printed outputs on each side to make sure everything is matching and working properly.

Github: https://github.com/gourmetpez/CIS-3319-Lab-1

