Brandon Lokey

CIS 3319

Lab 2

**Implementation and Application of HMAC**

How It Works: Similar to the DES application, this application utilizes client/server socket programming to create a chat program utilizing HMAC. The server starts a connection and waits for a client. The client then connects, generating HMAC and DES keys and storing them into two different files that the client and server can access. After that, the client and the server exchange messages that are encrypted with both DES encryption + HMAC authentication. The plaintext, ciphertext, keys, HMAC, and HMAC verification are displayed on each side, showing what is being sent and how it is being encrypted/decrypted.

How It Was Made: This program used much of the same code as the previous project, only introducing the HMAC aspect. I utilized Java’s socket library and various input/output streams to handle communications and file reading/writing. In addition to that, I also used Java’s crypto libraries to generate keys and handle encryption, decryption, etc.

Testing: When testing, I was making sure that the right messages were being sent back and forth. This was done by not only observing the encrypted and decrypted messages, but also what each side displayed for the keys, HMAC, and more. I sent multiple messages and tried running the program several times to make sure that the program was working consistently. I also performed HMAC verification to make sure the right HMAC was being sent and received.

Github: <https://github.com/gourmetpez/CIS-3319-Lab-2>



