CEG-4750 Information Security

Brandon Walker

Meilin Liu

03/06/2024

Project 1

I downloaded PuTTy, and connected to fry, and am already familiar with its use, so I used the third compiling method because that is the method I have been using to run other containers and programs on fry. I then encrypted all of the test files using the compiled program.

1. I ran OD on all of the files
2. There are 8 bytes difference between MSG1.e and MSG2.e and 8 bytes difference between MSG1.e and MSG3.e
3. There was no difference between any of the decrypted files and the originals.

I used vscode on my computer to edit the programs, and I just changed where each said “ECB” to say “CBC”, changed the “SetKey” to “SetKeyWithIV”, added a `byte iv[]` field to the encryption function, then in main right after the key is coded I made an iv variable and I just made it a flip of the key, and then changed the function call to pass the iv. I then encrypted all the files but with a capital E for the end of the file, and decrypted to a file ending with a capital D to separate them from the original encryption and decryption files.

All images are in this folder named clearly as what the image contains, ex: “ECB-encryption” shows me encrypting the files with the ECB encryptions method.