CEG-4750 Information Security

Brandon Walker

Meilin Liu

03/16/2024

Project 2

I opened up the encryption and decryption code in vscode and modified the files by changing ECB to CTR, setkey to setkeywithiv, added a byte iv[] field to the encryption/decryption method, and to the method call in main, added an iv field to main right after the key is declared and hardcoded it. I then connected to fry and compiled the programs. I encrypted every file and saved to a '.e' file. I then decrypted all the files and saved them to a '.d' file. I ran diff on every files original and '.d' version, and finally ran od -b on every file to compare the bytes of the files. There were no differences between the originals and the decrypted versions. There were only 2 bytes of difference between MSG1.e and MSG2.e, and 1 byte of difference between MSG1.e and MSG3.e. I suspect this is why I saw info about not using the same IV repeatedly, as I used the same IV for every file, I am sure a different IV each time would give a bigger difference, and a new key every time would increase that difference. All images will be included in this folder with names describing what part of the process they document.