COMP3800

Lab1

Notes

Part 1

The cleartext.txt file is 4 bytes the encrypt file DESciphertext is 8 bytes, but the DEScleartext.txt is back to the original size of 4 bytes.

The same goes to the TDES files.

The cipher files that are encrypted have a bunch of random characters in place of the plan text I added in the cleartext file

The encrypted photo is the same size but the

Part 2

It worked the same way as if it was encrypted once but the file that is encrypted twice is larger at 16 bytes but it has the same outcome.

Part 3

This does not work as it gives an error because the final block is not properly padded.

Part 4

You can’t encrypt with AES than decrypt with 3DES as it damages the file and will make it so the file can’t open

Serializable- is the process of translating data structures or objects state into a format that can be stored and reconstructed later

Sealed Object- This class enables a programmer to create an object and protect its confidentiality with a cryptographic algorithm