**Task 2:**

**Text

Description automatically generated**

^three different types of encryption for plain.txt the first file was encrypted with the aes-128-cbc method, the second file was encrypted with -bf-cbc method and the third file was encrypted with the aes-128-cfb method

Text

Description automatically generated

^contents of plain.txt before encryption

**Task 3:**

Icon

Description automatically generated

^contents of downloading pic\_original.bmp, this image was downloaded with a simple wget in the terminal

Text

Description automatically generated

^creating a header and body file as described in the lab, the header consists of the first 54 bytes while the tail consists of the last 55 bytes of the file

Opening header individually and body individually yields only a black screen which I thought was interesting, I though perhaps the header and body would perhaps yield two smaller dimension pictures

Background pattern

Description automatically generated

^contents of new.bmp, we can get an appreciation for the encryption here as there is no way to tell just from this image what the actual image actually is, it is a true scrambling

**Task 4**

**Text

Description automatically generated**

Here 3 files were created f1, f2, and f3 all with a .txt suffix

The content of f1 were 12345

The content of f2 was 1234567890

The content of f3 was 1234567876543210

This is demonstrated above with the use of the cat function for each file

Text

Description automatically generated

^hexdump results after encrypting each of the 3 files with the -nopad option

I am a little confused by this result because I would have thought that f3 being size 16 would not have had any padding but it seems that it does (unless I am reading this wrong)

**Task 5**

**Text

Description automatically generated**

^ partial view of the contents of my rand.txt 1000+ byte file as well as a view of the size of rand.txt below, with ls -l function which shows the length of the file we see that we have 1333 digits in the file

Text

Description automatically generated

^ View of what happens after corrupting the 55th bit of the hex using bless hex editor

**IV Task**

**Text

Description automatically generated**

^creating a file with my name, encrypting it with the given IV value and key, generating the md5sum of the resulting predictable IV

Text

Description automatically generated

^making a guess on P1, it was a little interesting here that the last few values repeated with 2e constitently

Graphical user interface, text, application, email

Description automatically generated

^calculated XOR of the guess compared to the actual, I was not able to get the python file working (something wrong with my python environment I believe) but I was able to use this XOR calculator to help me get a hex value of the XOR between the guess and the actual IV