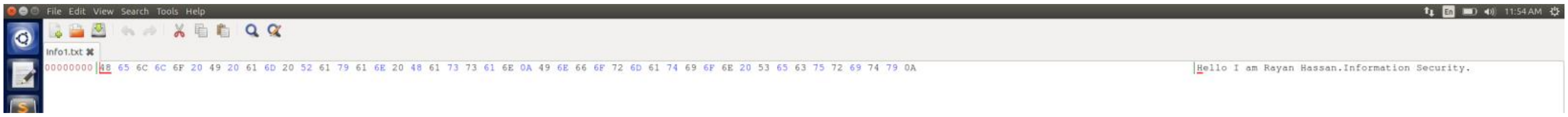
Lab1 – ECE 1155 – Rayan Hassan 4511021

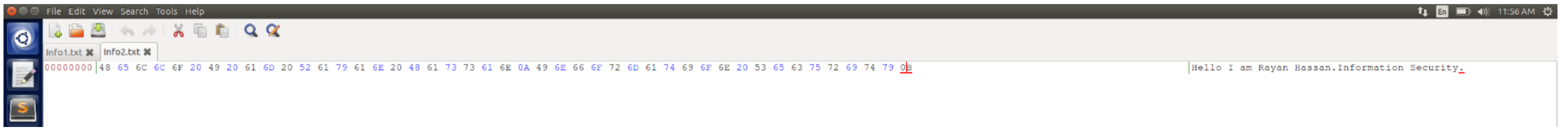
To communicate a file and make sure attackers don't get access to it, encryption is needed. A plaintext is encrypted using a key forming a ciphertext, which will later be decrypted to form the original plaintext intended for the receiver to read. Many methods and algorithms are applied today to encrypt files, DES and AES are examples of that. These are block ciphers that take inputs in and change them in a series of permutations and substitutions in multiple rounds with multiple sub-keys generated to finally give the ciphertext. Many encryption modes are used in both AES and DES, mainly ECB, CBC, CFB, OFB and CTR. In this assignment we don't use the latter, so we will only focus on the other four.

Task 1



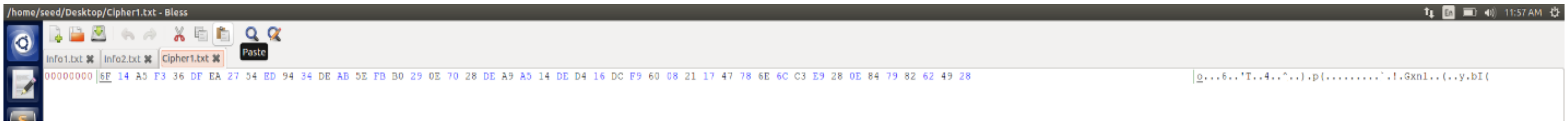
```
00000000 48 65 6C 6C 6F 20 49 20 61 6D 20 52 61 79 61 6E 20 48 61 73 73 61 6E 0A 49 6E 66 6F 72 6D 61 74 69 6F 6E 20 53 65 63 75 72 69 74 79 0A     Hello I am Rayan Hassan.Information Security.
```

The screenshot above shows my Info1.txt document in Hex editor. My Info2.txt file with the minor change is below. The change is 0B instead of 0A (last byte), so only one bit was changed (0000 1010 → 0000 1011)



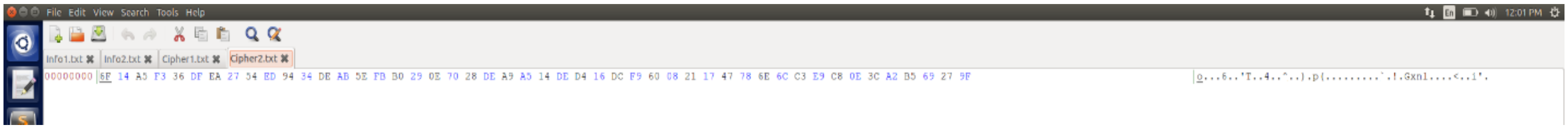
```
00000000 48 65 6C 6C 6F 20 49 20 61 6D 20 52 61 79 61 6E 20 48 61 73 73 61 6E 0A 49 6E 66 6F 72 6D 61 74 69 6F 6E 20 53 65 63 75 72 69 74 79 0B     Hello I am Rayan Hassan.Information Security.
```

Encrypting Info1.txt using DES (ECB mode) gives the following Cipher1.txt



```
00000000 6F 14 A5 F3 36 DF EA 27 54 ED 94 34 DE AB 5E FB B0 29 0E 70 28 DE A9 A5 14 DE D4 16 DC F9 60 08 21 17 47 78 6E 6C C3 E9 28 0E 84 79 82 62 49 28     o...6..'T..4..^..).p(.........`.!.Gxnl..(..y.bI(
```

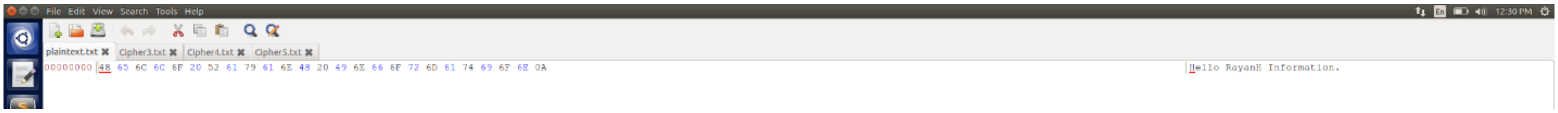
Encrypting Info2.txt using DES (ECB modes) gives the following Cipher2.txt



```
00000000 6F 14 A5 F3 36 DF EA 27 54 ED 94 34 DE AB 5E FB B0 29 0E 70 28 DE A9 A5 14 DE D4 16 DC F9 60 08 21 17 47 78 6E 6C C3 E9 C8 0E 3C A2 B5 69 27 9F     o...6..'T..4..^..).p(.........`.!.Gxnl....<..i'.
```

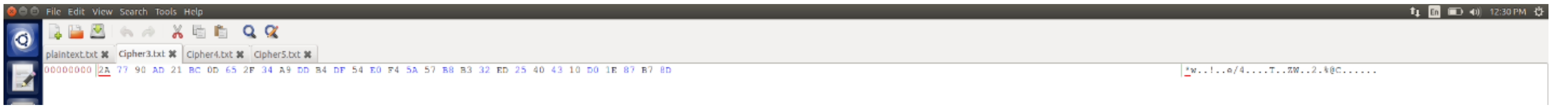
We can tell that multiple bits were changed. So this one slight modification in the plaintext actually resulted in a larger change in the ciphertext, which is what the avalanche effect is all about.

2) The plaintext.txt file I created is the following

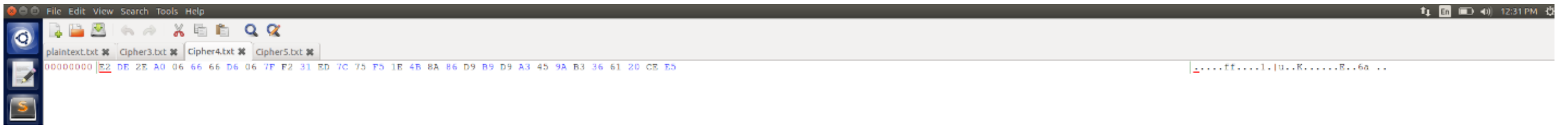


```
00000000 48 65 6C 6C 6F 20 52 61 79 61 6E 48 20 49 6E 66 6F 72 6D 61 74 69 6F 6E 0A     Hello RayanH Information.
```

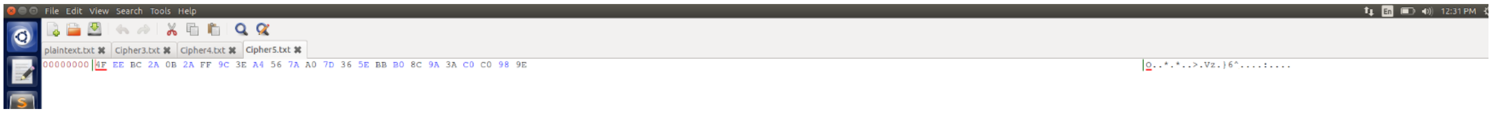
The encrypted files using AES are shown below, with ECB, CBC and CFB respectively



```
00000000 2A 77 90 AD 21 BC 0D 65 2F 34 A9 DD B4 DF 54 E0 F4 5A 57 B8 B3 32 ED 25 40 43 10 D0 1E 87 B7 8D     *w..!..e/4....T..ZW..2.%@C......
```

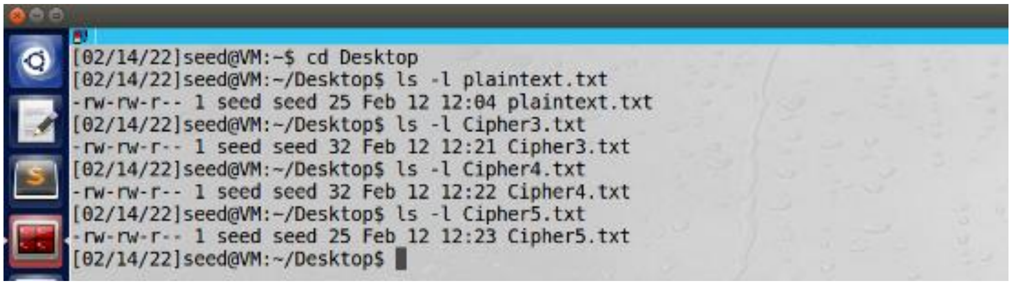


```
00000000 E2 DE 2E A0 06 66 66 D6 06 7F F2 31 ED 7C 75 F5 1E 4B 8A 86 D9 B9 D9 A3 45 9A B3 36 61 20 CE E5     .....ff....1.|u..K......E..6a ..
```



```
00000000 4F EE BC 2A 0B 2A FF 9C 3E A4 56 7A A0 7D 36 5E BB B0 8C 9A 3A C0 C0 98 9E     O..*.*..>.Vz.}6^....:....
```

The length of each file is given in this command window:

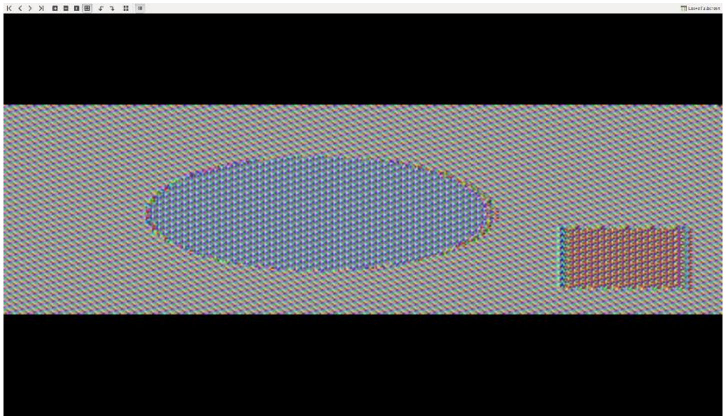


```
[02/14/22]seed@VM:~$ cd Desktop
[02/14/22]seed@VM:~/Desktop$ ls -l plaintext.txt
-rw-rw-r-- 1 seed seed 25 Feb 12 12:04 plaintext.txt
[02/14/22]seed@VM:~/Desktop$ ls -l Cipher3.txt
-rw-rw-r-- 1 seed seed 32 Feb 12 12:21 Cipher3.txt
[02/14/22]seed@VM:~/Desktop$ ls -l Cipher4.txt
-rw-rw-r-- 1 seed seed 32 Feb 12 12:22 Cipher4.txt
[02/14/22]seed@VM:~/Desktop$ ls -l Cipher5.txt
-rw-rw-r-- 1 seed seed 25 Feb 12 12:23 Cipher5.txt
[02/14/22]seed@VM:~/Desktop$ 
```

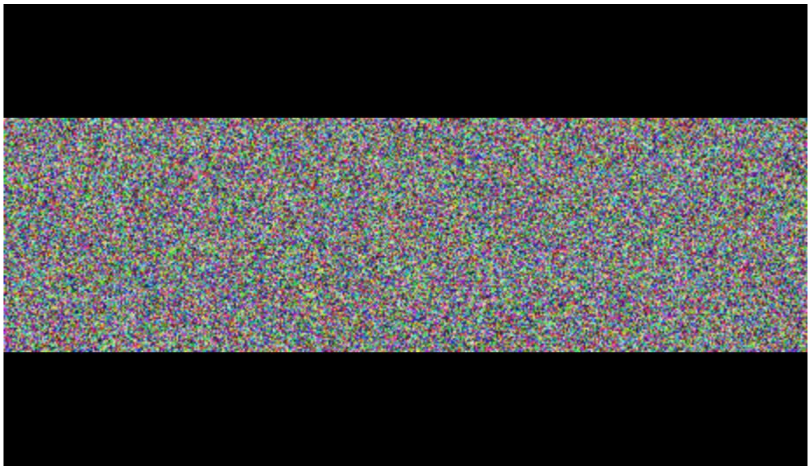
More clearly, the lengths of plaintext.txt, Cipher_aes_ebc.txt, Cipher_aes_cbc.txt and Cipher_aes_cfb.txt are 25 bytes, 32 bytes, 32 bytes and 25 bytes respectively. We can see that the number of bytes in ciphertext using ECB and CBC is different than the plaintext. The one using OFB is same.

Task 2

Using AES with ECB, encrypting the picture would give us the following picture



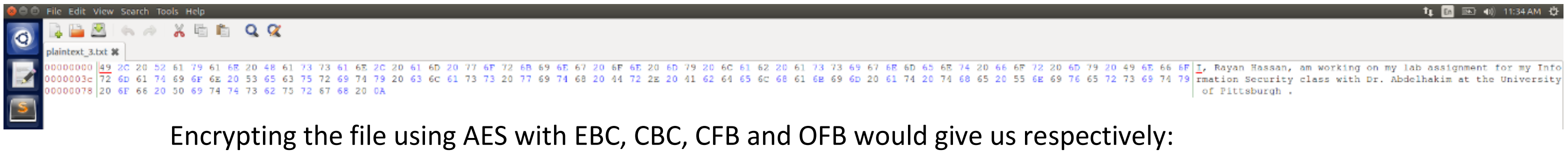
Whereas if we use AES with CBC we get:



This makes sense because in ECB, we only use a key, whereas in CBC we also use an initial vector, pass it to the first encryption block and then the output is the vector for the second cipher encryption block. The process is more complicated since every encryption block depends on the previous one, so encryption is much better. This is what we see in its corresponding picture where the plaintext can't be seen, unlike the first one where it is still visible.

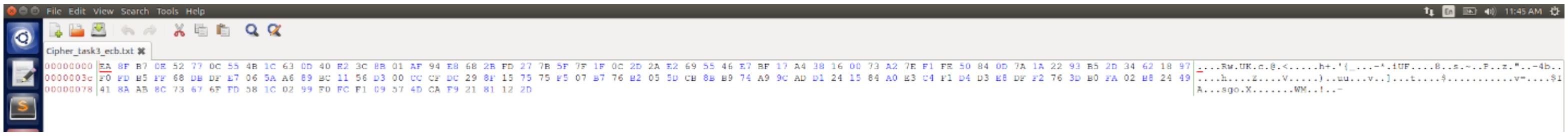
Task 3

The file created of a minimum of 64 bytes is:

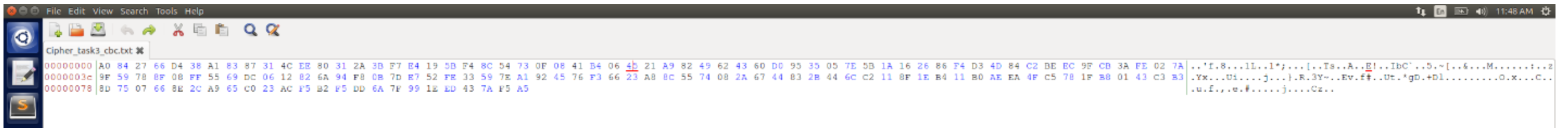


```
00000000 49 2C 20 52 61 79 61 6E 20 48 61 73 73 61 6E 2C 20 61 6D 20 77 6F 72 6B 69 6E 67 20 6F 6E 20 6D 79 20 6C 61 62 20 61 73 73 69 67 6E 6D 65 6E 74 20 66 6F 72 20 6D 79 20 49 6E 66 6F I, Rayan Hassan, am working on my lab assignment for my Info
0000003c 72 6D 61 74 69 6F 6E 20 53 65 63 75 72 69 74 79 20 63 6C 61 73 73 20 77 69 74 68 20 44 72 2E 20 41 62 64 65 6C 68 61 6B 69 6D 20 61 74 20 74 68 65 20 55 6E 69 76 65 72 73 69 74 79 rmation Security class with Dr. Abdelhakim at the University
00000078 20 6F 66 20 50 69 74 74 73 62 75 72 67 68 20 0A                                                                                                                                                                  of Pittsburgh .
```

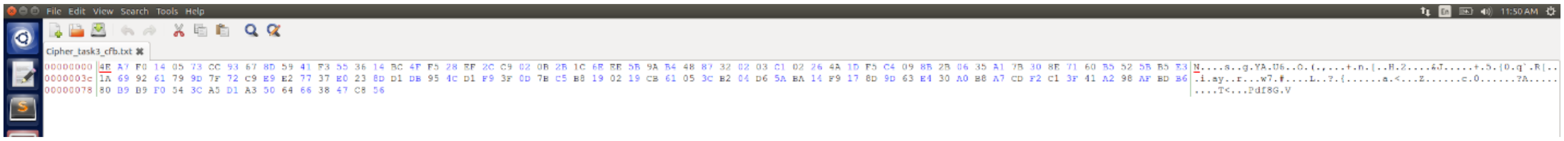
Encrypting the file using AES with EBC, CBC, CFB and OFB would give us respectively:



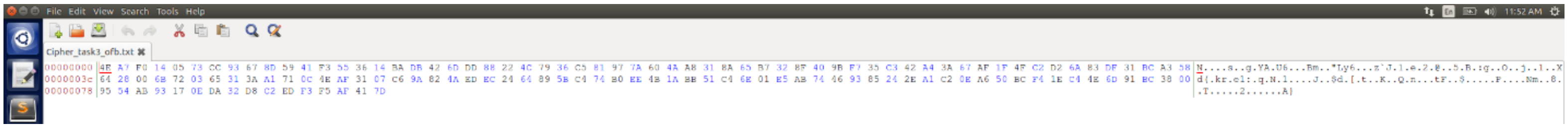
```
00000000 EA 8F B7 0E 52 77 0C 55 4B 1C 63 0D 40 E2 3C 8B 01 AF 94 E8 68 2B FD 27 7B 5F 7F 1F 0C 2D 2A E2 69 55 46 E7 BF 17 A4 38 16 00 73 A2 7E F1 FE 50 84 0D 7A 1A 22 93 B5 2D 34 62 18 97 ....Rw.UK.c.@.<.....h+.'{_...-*.iUF....8..s.~..P..z."..-4b..
0000003c F0 FD B5 FF 68 DB DF E7 06 5A A6 89 BC 11 56 D3 00 CC CF DC 29 8F 15 75 75 F5 07 B7 76 B2 05 5D CB 8B B9 74 A9 9C AD D1 24 15 84 A0 E3 C4 F1 D4 D3 E8 DF F2 76 3D B0 FA 02 B8 24 49 ....h....Z....V.....)..uu...v..]...t.....$...........v=....$I
00000078 41 8A AB 8C 73 67 6F FD 58 1C 02 99 F0 FC F1 09 57 4D CA F9 21 81 12 2D                                                                                                                   A...sgo.X.......WM..!..-
```



```
00000000 A0 84 27 66 D4 38 A1 83 87 31 4C EE 80 31 2A 3B F7 E4 19 5B F4 8C 54 73 0F 08 41 B4 06 40 21 A9 82 49 62 43 60 D0 95 35 05 7E 5B 1A 16 26 86 F4 D3 4D 84 C2 BE EC 9F CB 3A FE 02 7A ..'f.8...1L..1*;...[..Ts..A..@!..IbC`..5.~[..&...M......:..z
0000003c 9F 59 78 8F 08 FF 55 69 DC 06 12 82 6A 94 F8 0B 7D E7 52 FE 33 59 7E A1 92 45 76 F3 66 23 A8 8C 55 74 08 2A 67 44 83 2B 44 6C C2 11 8F 1E B4 11 B0 AE EA 4F C5 78 1F B8 01 43 C3 B3 .Yx...Ui....j...}.R.3Y~..Ev.f#..Ut.*gD.+Dl.........O.x...C..
00000078 8D 75 07 66 8E 2C A9 65 C0 23 AC F5 B2 F5 DD 6A 7F 99 1E ED 43 7A F5 A5                                                                                                                   .u.f.,.e.#.....j....Cz..
```

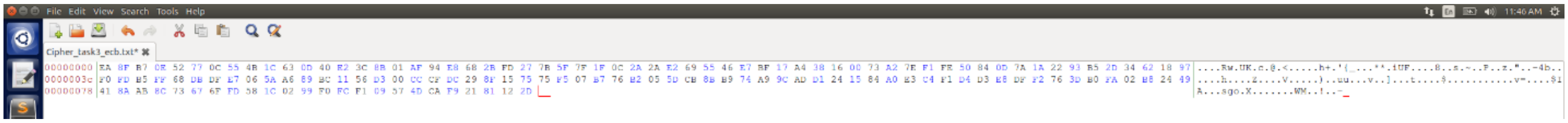


```
00000000 4E A7 F0 14 05 73 CC 93 67 8D 59 41 F3 55 36 14 BC 4F F5 28 EF 2C C9 02 0B 2B 1C 6E EE 5B 9A B4 48 87 32 02 03 C1 02 26 4A 1D F5 C4 09 8B 2B 06 35 A1 7B 30 8E 71 60 B5 52 5B B5 E3 N....s..g.YA.U6..O.(.,...+.n.[..H.2....&J.....+.5.{0.q`.R[..
0000003c 1A 69 92 61 79 9D 7F 72 C9 E9 E2 77 37 E0 23 8D D1 DB 95 4C D1 F9 3F 0D 7B C5 B8 19 02 19 CB 61 05 3C B2 04 D6 5A BA 14 F9 17 8D 9D 63 E4 30 A0 B8 A7 CD F2 C1 3F 41 A2 98 AF BD B6 .i.ay..r...w7.#....L..?.{......a.<...Z......c.0......?A.....
00000078 80 B9 B9 F0 54 3C A5 D1 A3 50 64 66 38 47 C8 56                                                                                                                                           ....T<...Pdf8G.V
```

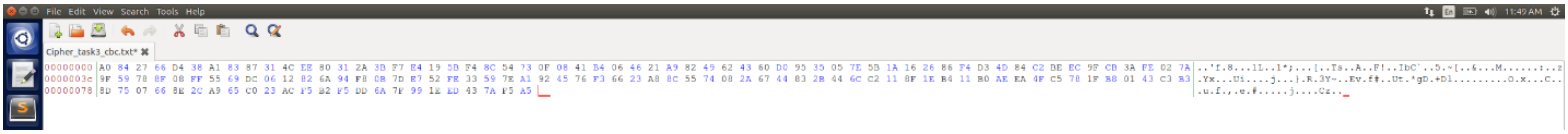


```
00000000 4E A7 F0 14 05 73 CC 93 67 8D 59 41 F3 55 36 14 BA DB 42 6D DD 88 22 4C 79 36 C5 81 97 7A 60 4A AB 31 8A 65 B7 32 BF 40 9B F7 35 C3 42 A4 3A 67 AF 1F 4F C2 D2 6A 83 DF 31 BC A3 58 N....s..g.YA.U6...Bm.."Ly6...z`J.1.e.2.@..5.B.:g..O..j..1..X
0000003c 64 28 00 6B 72 03 65 31 3A A1 71 0C 4E AF 31 07 C6 9A 82 4A ED EC 24 64 89 5B C4 74 B0 EE 4B 1A BB 51 C4 6E 01 E5 AB 74 46 93 85 24 2E A1 C2 0E A6 50 BC F4 1E C4 4E 6D 91 BC 38 00 d(.kr.e1:.q.N.1....J..$d.[.t..K..Q.n...tF..$.....P....Nm..8.
00000078 95 54 AB 93 17 0E DA 32 D8 C2 ED F3 F5 AF 41 7D                                                                                                                                           .T.....2......A}
```

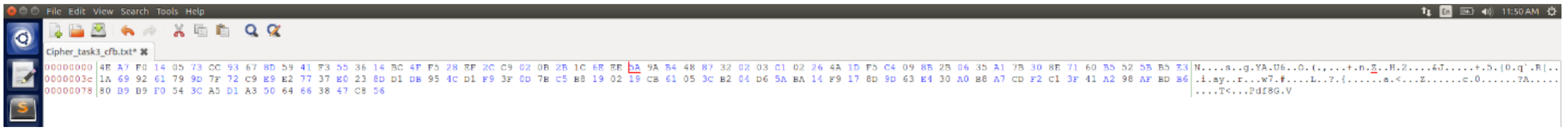
The corrupted AES encrypted files are given below (ECB, CBC, CFB and OFB respectively). I changed the 30th byte for each one of them (2D →2A ; 40 → 46 ; 5B →5A ; 7A → 7B for ECB, CBC, CFB and OFB respectively)



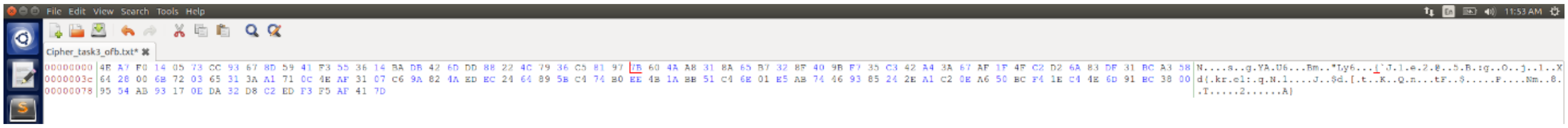
```
00000000 EA 8F B7 0E 52 77 0C 55 4B 1C 63 0D 40 E2 3C 8B 01 AF 94 E8 68 2B FD 27 7B 5F 7F 1F 0C 2A 2A E2 69 55 46 E7 BF 17 A4 38 16 00 73 A2 7E F1 FE 50 84 0D 7A 1A 22 93 B5 2D 34 62 18 97 ....Rw.UK.c.@.<.....h+.'{_...**.iUF....8..s.~..P..z."..-4b..
0000003c F0 FD B5 FF 68 DB DF E7 06 5A A6 89 BC 11 56 D3 00 CC CF DC 29 8F 15 75 75 F5 07 B7 76 B2 05 5D CB 8B B9 74 A9 9C AD D1 24 15 84 A0 E3 C4 F1 D4 D3 E8 DF F2 76 3D B0 FA 02 B8 24 49 ....h....Z....V.....)..uu...v..]...t.....$...........v=....$I
00000078 41 8A AB 8C 73 67 6F FD 58 1C 02 99 F0 FC F1 09 57 4D CA F9 21 81 12 2D                                                                                                                   A...sgo.X.......WM..!..-
```



```
00000000 A0 84 27 66 D4 38 A1 83 87 31 4C EE 80 31 2A 3B F7 E4 19 5B F4 8C 54 73 0F 08 41 B4 06 46 21 A9 82 49 62 43 60 D0 95 35 05 7E 5B 1A 16 26 86 F4 D3 4D 84 C2 BE EC 9F CB 3A FE 02 7A ..'f.8...1L..1*;...[..Ts..A..F!..IbC`..5.~[..&...M......:..z
0000003c 9F 59 78 8F 08 FF 55 69 DC 06 12 82 6A 94 F8 0B 7D E7 52 FE 33 59 7E A1 92 45 76 F3 66 23 A8 8C 55 74 08 2A 67 44 83 2B 44 6C C2 11 8F 1E B4 11 B0 AE EA 4F C5 78 1F B8 01 43 C3 B3 .Yx...Ui....j...}.R.3Y~..Ev.f#..Ut.*gD.+Dl.........O.x...C..
00000078 8D 75 07 66 8E 2C A9 65 C0 23 AC F5 B2 F5 DD 6A 7F 99 1E ED 43 7A F5 A5                                                                                                                   .u.f.,.e.#.....j....Cz..
```

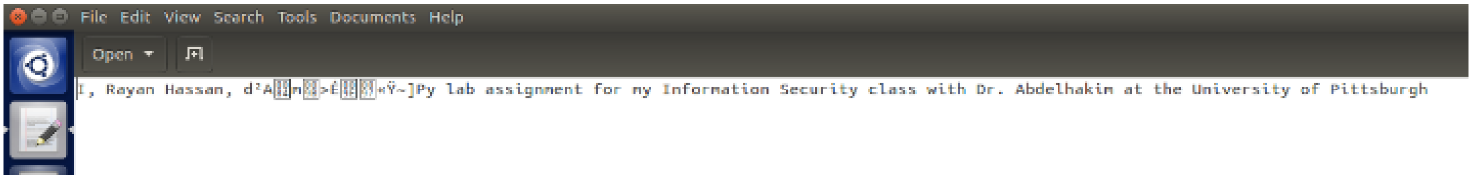


```
00000000 4E A7 F0 14 05 73 CC 93 67 8D 59 41 F3 55 36 14 BC 4F F5 28 EF 2C C9 02 0B 2B 1C 6E EE 5A 9A B4 48 87 32 02 03 C1 02 26 4A 1D F5 C4 09 8B 2B 06 35 A1 7B 30 8E 71 60 B5 52 5B B5 E3 N....s..g.YA.U6..O.(.,...+.n.Z..H.2....&J.....+.5.{0.q`.R[..
0000003c 1A 69 92 61 79 9D 7F 72 C9 E9 E2 77 37 E0 23 8D D1 DB 95 4C D1 F9 3F 0D 7B C5 B8 19 02 19 CB 61 05 3C B2 04 D6 5A BA 14 F9 17 8D 9D 63 E4 30 A0 B8 A7 CD F2 C1 3F 41 A2 98 AF BD B6 .i.ay..r...w7.#....L..?.{......a.<...Z......c.0......?A.....
00000078 80 B9 B9 F0 54 3C A5 D1 A3 50 64 66 38 47 C8 56                                                                                                                                           ....T<...Pdf8G.V
```

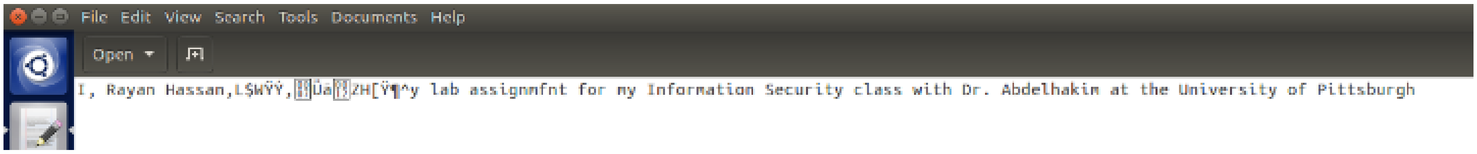


```
00000000 4E A7 F0 14 05 73 CC 93 67 8D 59 41 F3 55 36 14 BA DB 42 6D DD 88 22 4C 79 36 C5 81 97 7B 60 4A AB 31 8A 65 B7 32 BF 40 9B F7 35 C3 42 A4 3A 67 AF 1F 4F C2 D2 6A 83 DF 31 BC A3 58 N....s..g.YA.U6...Bm.."Ly6...{`J.1.e.2.@..5.B.:g..O..j..1..X
0000003c 64 28 00 6B 72 03 65 31 3A A1 71 0C 4E AF 31 07 C6 9A 82 4A ED EC 24 64 89 5B C4 74 B0 EE 4B 1A BB 51 C4 6E 01 E5 AB 74 46 93 85 24 2E A1 C2 0E A6 50 BC F4 1E C4 4E 6D 91 BC 38 00 d(.kr.e1:.q.N.1....J..$d.[.t..K..Q.n...tF..$.....P....Nm..8.
00000078 95 54 AB 93 17 0E DA 32 D8 C2 ED F3 F5 AF 41 7D                                                                                                                                           .T.....2......A}
```

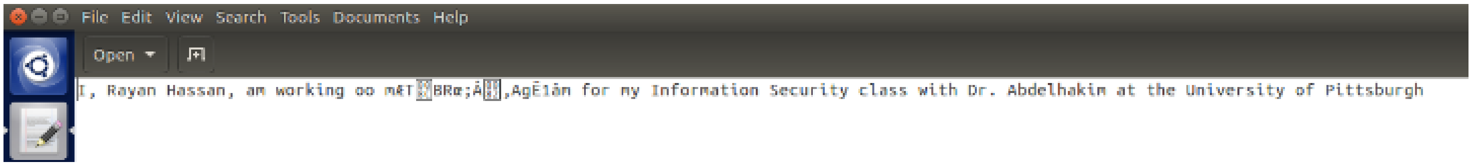
Now the decrypted files corresponding to each of them are the following (ECB, CBC, CFB, OFB respectively)



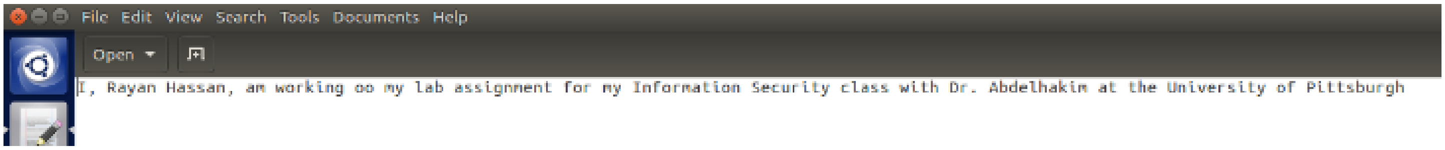
```
I, Rayan Hassan, d²A▯n▯>É▯▯«Ÿ~]Py lab assignment for my Information Security class with Dr. Abdelhakim at the University of Pittsburgh
```



```
I, Rayan Hassan,L$WŸÝ,▯Üa▯ZH[Ÿ¶^y lab assignmfnt for my Information Security class with Dr. Abdelhakim at the University of Pittsburgh
```



```
I, Rayan Hassan, am working oo m&T▯BRø;Å▯,AgÊ1ân for my Information Security class with Dr. Abdelhakim at the University of Pittsburgh
```



```
I, Rayan Hassan, am working oo my lab assignment for my Information Security class with Dr. Abdelhakim at the University of Pittsburgh
```

We notice that for just a slight change in the encrypted files, the decryption drastically change for ECB, CBC and CFB. This is not the case however for OFB because unlike the other modes, it uses the sub-key before it is XORed with the plaintext. Since the sub-key is not affected by encryption errors, these errors do not propagate.

Task 4

First of all, the keys and initial vectors are the same for both plaintexts and they are too easy, which is not very secure. Secondly, they used OFB mode to encrypt the plaintexts, which means a simple XOR would reverse the process and give the attacker access to them. The attacker knows the Ciphertexts and plaintext 1. So P1 XOR C1 gives him the key (the output they were referring too). This key XORed with C1 gives P2. So the attacker

In conclusion, encryption is a process that should be taken seriously in order to secure our files. In fact, we saw that one mistake or corruption in the encrypted file (ciphertext) can lead to a big difference in the resulting plaintext after decryption. This is called the avalanche effect. Also, the different modes studied in this lab have distinct effects and effectiveness. For instance, an encrypted picture using ECB would still be clearly visible, whereas using CBC it wouldn't, which mean it is more secure. The avalanche effect is also dependant on those modes. For instance, using OFB, a corrupted ciphertext doesn't affect the recovered plaintext as much as the other modes. All these differences are related to the inner-workings of these modes, which are different.