Name: Mohammad Fakhruddin Babar

ID: M564K763

Task 1: Encryption using Different Ciphers and Modes

Cipher mode that I chose in this task:

1. -aes-128-cbc
2. -aes-128-ecb
3. -des-cbc
4. -des-ecb

Reason of Choosing:

Those cipher modes are discussed in class, and I wanted to familiarize myself with them by using the OpenSSL library.

Task 2: Encryption Mode – ECB vs. CBC

1(a)Encrypted picture using ECB mode for both picture:

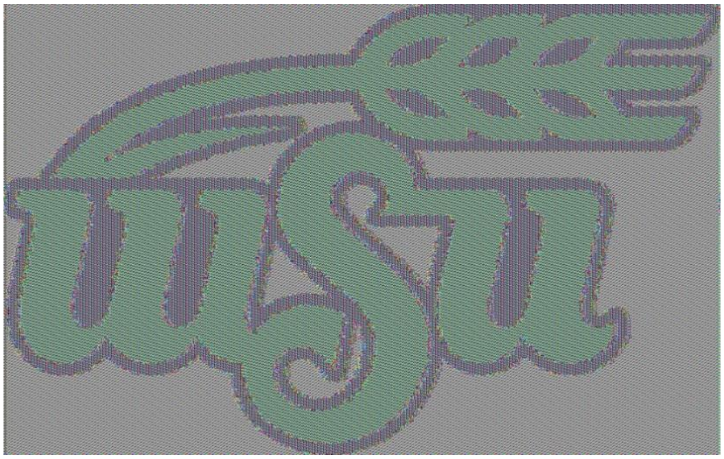


Fig: Encrypted picture for given image 1 in ECB mode

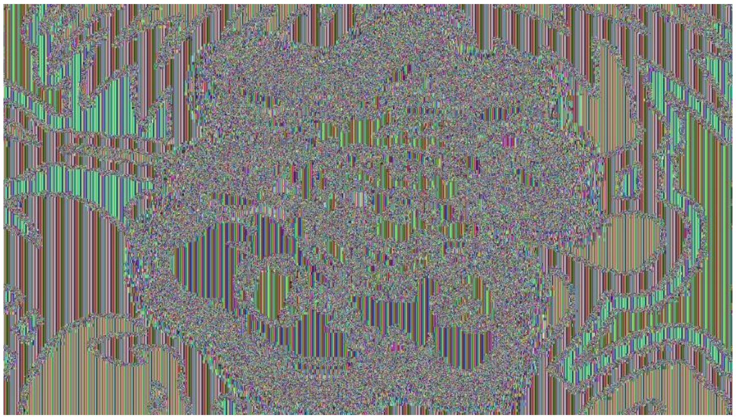


Fig: Encrypted picture for given image 2 in ECB mode

1(b): We can get a rough idea of the original picture's shape from the encrypted image, but not the color. Using ECB mode, however, an attacker can extract significant information from those encrypted images. As a result, this can't possibly be a good encryption mode.

2(a): Encrypted picture using CBC mode for both picture:

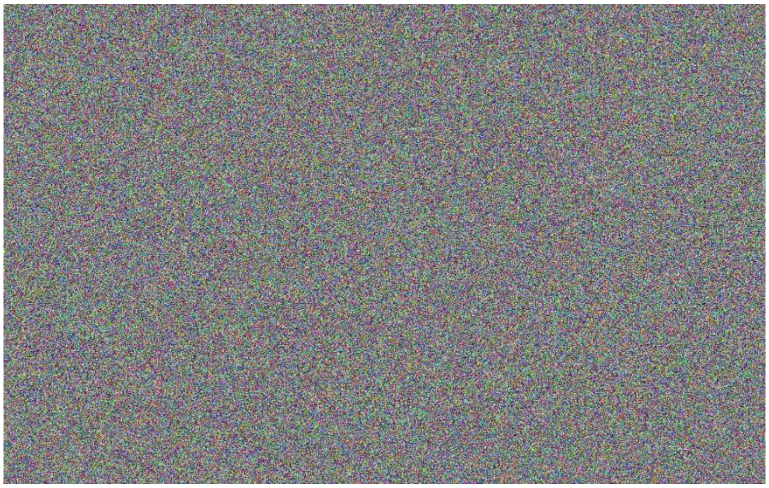


Fig: Encrypted picture for given image 1 in CBC mode

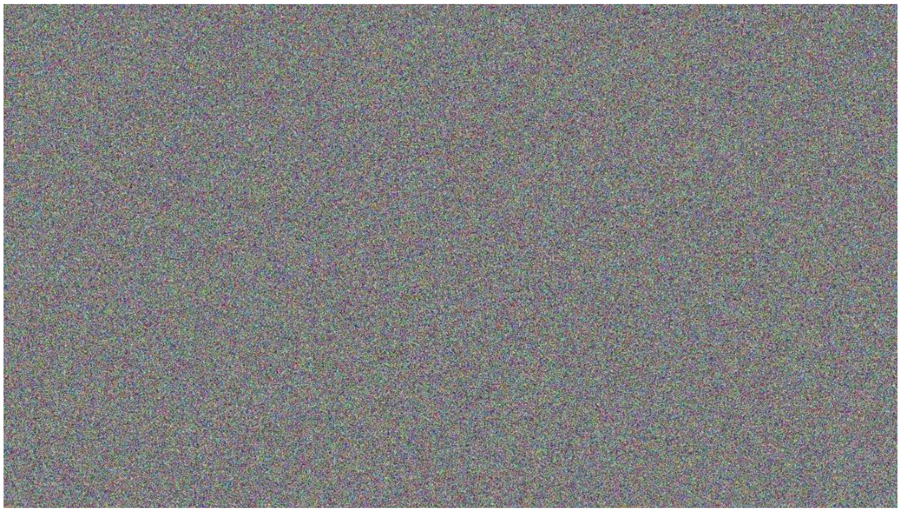
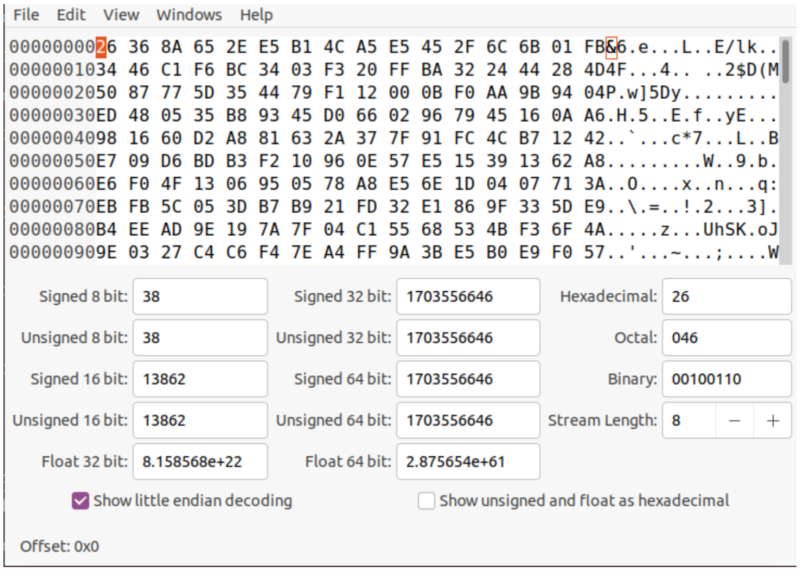


Fig: Encrypted picture for given image 2 in CBC mode

2(b) We can't tell what the original picture looked like or what color it was from the encrypted image. We have no idea what the photograph is about. As a result, an attacker won't be able to extract any useful information from the CBC-encrypted images. As a result, this could be a useful encryption mode.

Task 3: Error Propagation – Corrupted Cipher Text

ECB Mode:



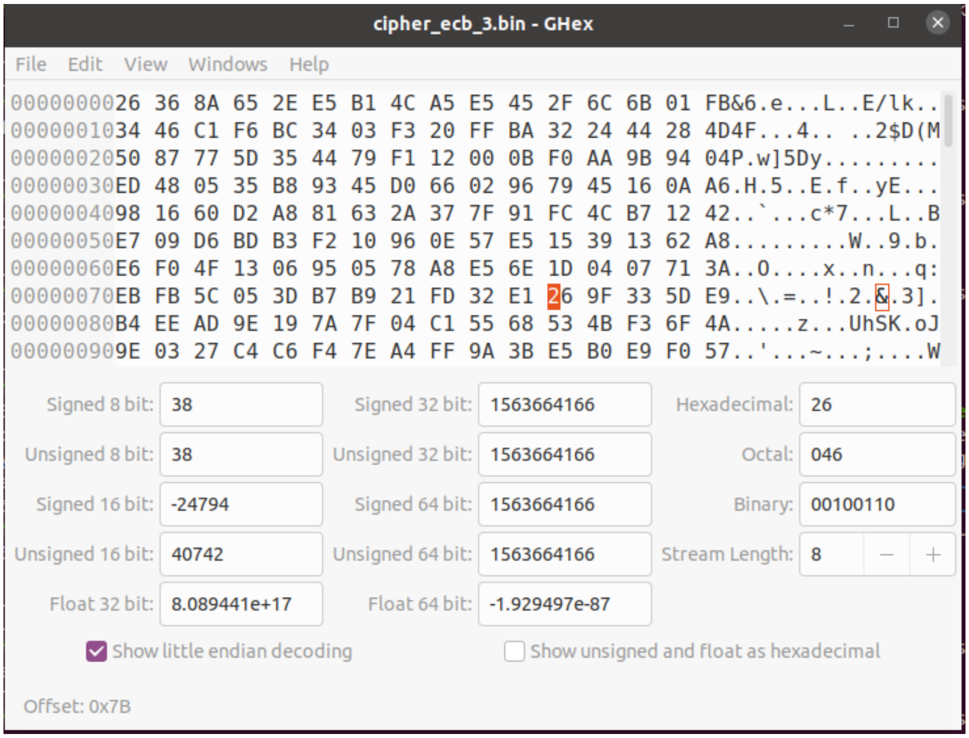
```
0000000026 36 8A 65 2E E5 B1 4C A5 E5 45 2F 6C 6B 01 FB&6.e...L..E/lk..
0000001034 46 C1 F6 BC 34 03 F3 20 FF BA 32 24 44 28 4D4F...4.. ..2$D(M
0000002050 87 77 5D 35 44 79 F1 12 00 0B F0 AA 9B 94 04P.w]5Dy.........
00000030ED 48 05 35 B8 93 45 D0 66 02 96 79 45 16 0A A6.H.5..E.f..yE...
0000004098 16 60 D2 A8 81 63 2A 37 7F 91 FC 4C B7 12 42..`...c*7...L..B
00000050E7 09 D6 BD B3 F2 10 96 0E 57 E5 15 39 13 62 A8.........W..9.b.
00000060E6 F0 4F 13 06 95 05 78 A8 E5 6E 1D 04 07 71 3A..O....x..n...q:
00000070EB FB 5C 05 3D B7 B9 21 FD 32 E1 86 9F 33 5D E9..\.=..!.2...3].
00000080B4 EE AD 9E 19 7A 7F 04 C1 55 68 53 4B F3 6F 4A.....z...UhSK.oJ
000000909E 03 27 C4 C6 F4 7E A4 FF 9A 3B E5 B0 E9 F0 57..'...~...;....W
```

Signed 8 bit: 38
Signed 32 bit: 1703556646
Hexadecimal: 26
Unsigned 8 bit: 38
Unsigned 32 bit: 1703556646
Octal: 046
Signed 16 bit: 13862
Signed 64 bit: 1703556646
Binary: 00100110
Unsigned 16 bit: 13862
Unsigned 64 bit: 1703556646
Stream Length: 8 − +
Float 32 bit: 8.158568e+22
Float 64 bit: 2.875654e+61

☑ Show little endian decoding
□ Show unsigned and float as hexadecimal

Offset: 0x0

Fig: Original encrypted picture in ECB mode



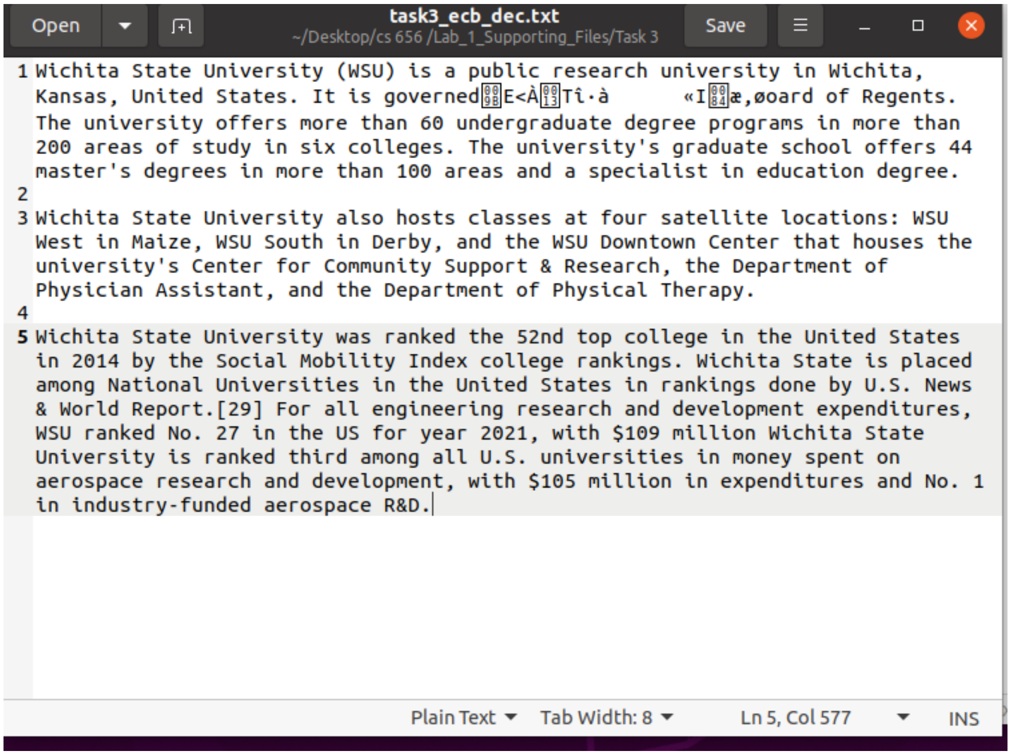
```
0000000026 36 8A 65 2E E5 B1 4C A5 E5 45 2F 6C 6B 01 FB&6.e...L..E/lk..
0000001034 46 C1 F6 BC 34 03 F3 20 FF BA 32 24 44 28 4D4F...4.. ..2$D(M
0000002050 87 77 5D 35 44 79 F1 12 00 0B F0 AA 9B 94 04P.w]5Dy........
00000030ED 48 05 35 B8 93 45 D0 66 02 96 79 45 16 0A A6.H.5..E.f..yE...
0000004098 16 60 D2 A8 81 63 2A 37 7F 91 FC 4C B7 12 42..`...c*7...L..B
00000050E7 09 D6 BD B3 F2 10 96 0E 57 E5 15 39 13 62 A8.........W..9.b.
00000060E6 F0 4F 13 06 95 05 78 A8 E5 6E 1D 04 07 71 3A..O....x..n...q:
00000070EB FB 5C 05 3D B7 B9 21 FD 32 E1 26 9F 33 5D E9..\.=..!.2.&.3].
00000080B4 EE AD 9E 19 7A 7F 04 C1 55 68 53 4B F3 6F 4A.....z...UhSK.oJ
000000909E 03 27 C4 C6 F4 7E A4 FF 9A 3B E5 B0 E9 F0 57..'...~...;....W
```

Signed 8 bit: 38
Signed 32 bit: 1563664166
Hexadecimal: 26
Unsigned 8 bit: 38
Unsigned 32 bit: 1563664166
Octal: 046
Signed 16 bit: -24794
Signed 64 bit: 1563664166
Binary: 00100110
Unsigned 16 bit: 40742
Unsigned 64 bit: 1563664166
Stream Length: 8
Float 32 bit: 8.089441e+17
Float 64 bit: -1.929497e-87

☑ Show little endian decoding
□ Show unsigned and float as hexadecimal

Offset: 0x7B

Fig: Corrupted file in ECB mode



task3_ecb_dec.txt
~/Desktop/cs 656 /Lab_1_Supporting_Files/Task 3

Wichita State University (WSU) is a public research university in Wichita, Kansas, United States. It is governedE<ÀTî·à   «Iæ,øoard of Regents. The university offers more than 60 undergraduate degree programs in more than 200 areas of study in six colleges. The university's graduate school offers 44 master's degrees in more than 100 areas and a specialist in education degree.

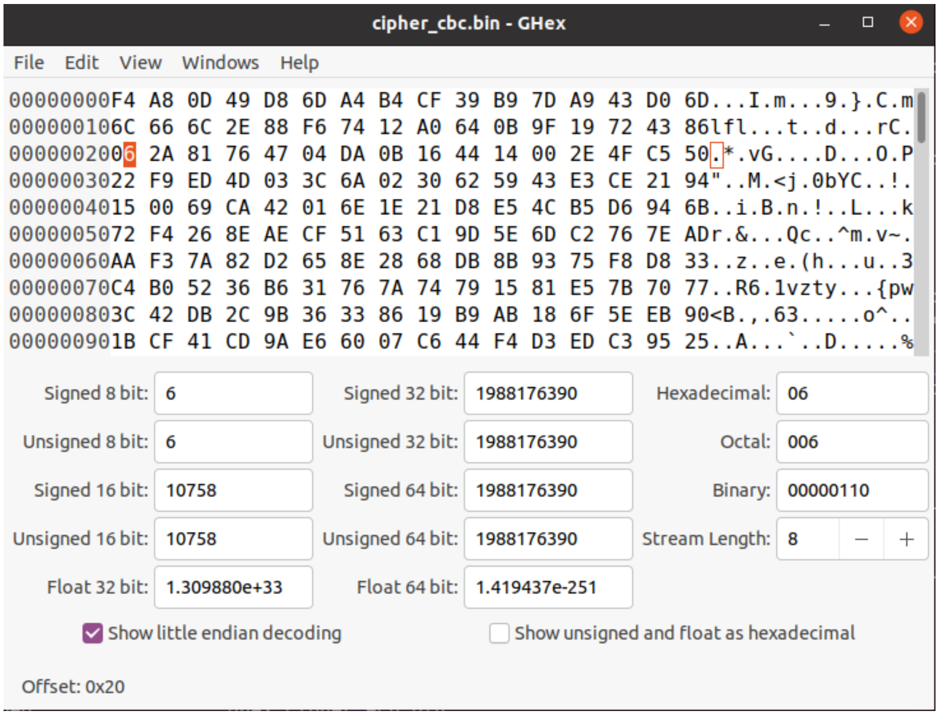
Wichita State University also hosts classes at four satellite locations: WSU West in Maize, WSU South in Derby, and the WSU Downtown Center that houses the university's Center for Community Support & Research, the Department of Physician Assistant, and the Department of Physical Therapy.

Wichita State University was ranked the 52nd top college in the United States in 2014 by the Social Mobility Index college rankings. Wichita State is placed among National Universities in the United States in rankings done by U.S. News & World Report.[29] For all engineering research and development expenditures, WSU ranked No. 27 in the US for year 2021, with $109 million Wichita State University is ranked third among all U.S. universities in money spent on aerospace research and development, with $105 million in expenditures and No. 1 in industry-funded aerospace R&D.

Ln 5, Col 577

Fig: Decrypted file of corrupted encrypted file in ECB mode

CBC Mode:



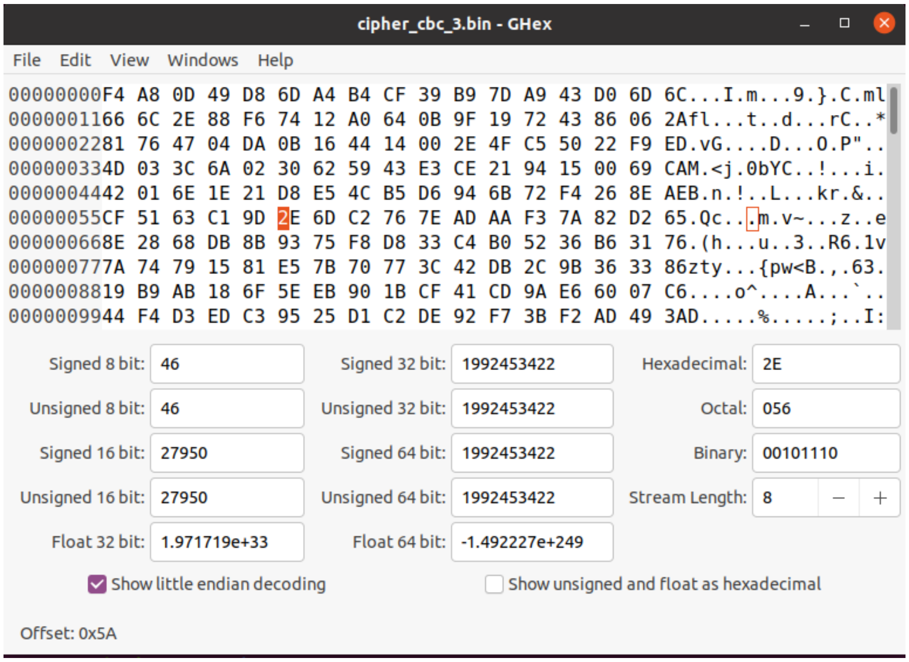
```
00000000F4 A8 0D 49 D8 6D A4 B4 CF 39 B9 7D A9 43 D0 6D...I.m...9.}.C.m
000000106C 66 6C 2E 88 F6 74 12 A0 64 0B 9F 19 72 43 86lfl...t..d...rC.
0000002006 2A 81 76 47 04 DA 0B 16 44 14 00 2E 4F C5 50.*.vG....D...O.P
0000003022 F9 ED 4D 03 3C 6A 02 30 62 59 43 E3 CE 21 94"..M.<j.0bYC..!.
0000004015 00 69 CA 42 01 6E 1E 21 D8 E5 4C B5 D6 94 6B..i.B.n.!..L...k
0000005072 F4 26 8E AE CF 51 63 C1 9D 5E 6D C2 76 7E ADr.&...Qc..^m.v~.
00000060AA F3 7A 82 D2 65 8E 28 68 DB 8B 93 75 F8 D8 33..z..e.(h...u..3
00000070C4 B0 52 36 B6 31 76 7A 74 79 15 81 E5 7B 70 77..R6.1vzty...{pw
000000803C 42 DB 2C 9B 36 33 86 19 B9 AB 18 6F 5E EB 90<B.,.63.....o^..
000000901B CF 41 CD 9A E6 60 07 C6 44 F4 D3 ED C3 95 25..A...`..D.....%
```

Signed 8 bit: 6
Signed 32 bit: 1988176390
Hexadecimal: 06
Unsigned 8 bit: 6
Unsigned 32 bit: 1988176390
Octal: 006
Signed 16 bit: 10758
Signed 64 bit: 1988176390
Binary: 00000110
Unsigned 16 bit: 10758
Unsigned 64 bit: 1988176390
Stream Length: 8 – +
Float 32 bit: 1.309880e+33
Float 64 bit: 1.419437e-251

☑ Show little endian decoding
□ Show unsigned and float as hexadecimal

Offset: 0x20

Fig: Original encrypted picture in CBC mode



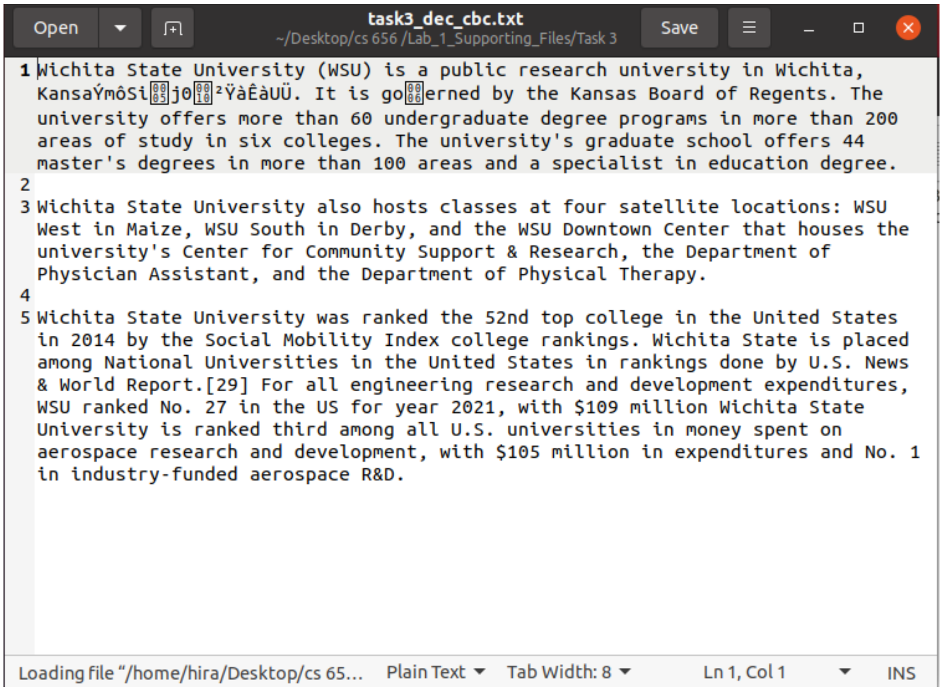
```
00000000F4 A8 0D 49 D8 6D A4 B4 CF 39 B9 7D A9 43 D0 6D 6C...I.m...9.}.C.ml
0000001166 6C 2E 88 F6 74 12 A0 64 0B 9F 19 72 43 86 06 2Afl...t..d...rC..*
0000002281 76 47 04 DA 0B 16 44 14 00 2E 4F C5 50 22 F9 ED.vG....D...O.P"..
000000334D 03 3C 6A 02 30 62 59 43 E3 CE 21 94 15 00 69 CAM.<j.0bYC..!...i.
0000004442 01 6E 1E 21 D8 E5 4C B5 D6 94 6B 72 F4 26 8E AEB.n.!..L...kr.&..
00000055CF 51 63 C1 9D 2E 6D C2 76 7E AD AA F3 7A 82 D2 65.Qc...m.v~...z..e
000000668E 28 68 DB 8B 93 75 F8 D8 33 C4 B0 52 36 B6 31 76.(h...u..3..R6.1v
000000777A 74 79 15 81 E5 7B 70 77 3C 42 DB 2C 9B 36 33 86zty...{pw<B.,.63.
0000008819 B9 AB 18 6F 5E EB 90 1B CF 41 CD 9A E6 60 07 C6....o^....A...`..
0000009944 F4 D3 ED C3 95 25 D1 C2 DE 92 F7 3B F2 AD 49 3AD.....%.....;..I:
```

Signed 8 bit: 46
Signed 32 bit: 1992453422
Hexadecimal: 2E
Unsigned 8 bit: 46
Unsigned 32 bit: 1992453422
Octal: 056
Signed 16 bit: 27950
Signed 64 bit: 1992453422
Binary: 00101110
Unsigned 16 bit: 27950
Unsigned 64 bit: 1992453422
Stream Length: 8 – +
Float 32 bit: 1.971719e+33
Float 64 bit: -1.492227e+249

☑ Show little endian decoding
□ Show unsigned and float as hexadecimal

Offset: 0x5A

Fig: Corrupted file in CBC mode


Open
task3_dec_cbc.txt
~/Desktop/cs 656 /Lab_1_Supporting_Files/Task 3
Save
Loading file "/home/hira/Desktop/cs 65...
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

```
Wichita State University (WSU) is a public research university in Wichita,
KansaÝmôSi▯jO▯²ŸàÊàUÜ. It is go▯erned by the Kansas Board of Regents. The
university offers more than 60 undergraduate degree programs in more than 200
areas of study in six colleges. The university's graduate school offers 44
master's degrees in more than 100 areas and a specialist in education degree.

Wichita State University also hosts classes at four satellite locations: WSU
West in Maize, WSU South in Derby, and the WSU Downtown Center that houses the
university's Center for Community Support & Research, the Department of
Physician Assistant, and the Department of Physical Therapy.

Wichita State University was ranked the 52nd top college in the United States
in 2014 by the Social Mobility Index college rankings. Wichita State is placed
among National Universities in the United States in rankings done by U.S. News
& World Report.[29] For all engineering research and development expenditures,
WSU ranked No. 27 in the US for year 2021, with $109 million Wichita State
University is ranked third among all U.S. universities in money spent on
aerospace research and development, with $105 million in expenditures and No. 1
in industry-funded aerospace R&D.
```

Fig: Decrypted file of corrupted encrypted file in CBC mode

CBC and ECB's are block ciphers, and if we change a single bit in CBC or ECB, it will only affect the next one or two blocks. Before beginning this task, I reasoned that changing a single bit in the encrypted file would result in a minor data loss. And after completing this task, I've concluded that changing a single bit does not affect a lot and it changes the information a little bit. Which is matched with my previous assumption. I'm able to extract almost all of the data from the original file.

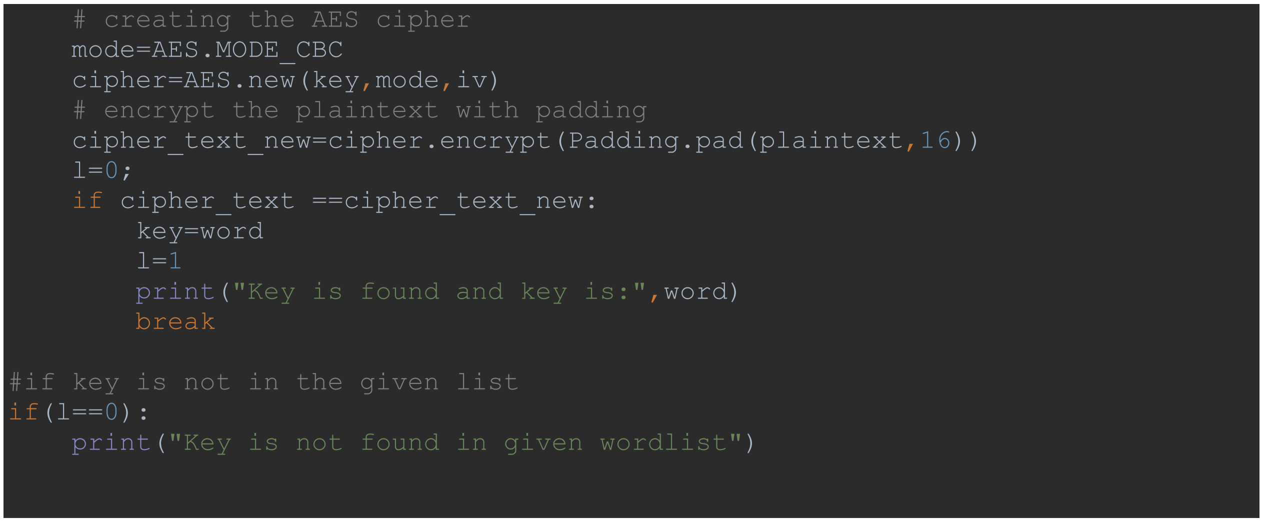
Task 4: Brute-force Attack using the Crypto Library

For this task I have used python crypto library to get the keys from the given English word list. And key is **Kansas**.

Plaintext, ciphertext, IV, and a wordlist are all provided. To get the key, I used the Python crypto library. To recover the key, I used AES-128-CBC. I padded each key in the given worldlist with '#' until it was 16 bytes(128 bits) long. Then I used that key to encrypt the given text, and then compared the new cipher text to the given cipher text. We stop checking and get the key if both the new cipher and the given cipher match.

Here is the code:

```
#Mohammad Fakhruddin Babar
#M564K763
#dictionary Attack with common word
#CS656, Lab-1, Task-4

from Crypto.Cipher import AES
from Crypto.Util import Padding

#given plaintext cipher text and iv
plaintext=b"I will crack the key."
#print(plaintext)
cipher_text="673ff1376c5b9a2e7cdbd7daf1faeb180bfa2b7ab150e25b7915525500a045fa
"
iv='0f0e0d0c0b0a00908070605040302010'

#converting iv and ciphertext
iv=bytes.fromhex(iv)
cipher_text=bytes.fromhex(cipher_text)

# Reading the wordlist file
fp=open("task4_wordlist.txt","r")
#accessing the word line-wise
wordlist_linewise=fp.readlines()
fp.close()

for word in wordlist_linewise:
    #print(len(word))
    #replacing new line with space ; then padding with #
    word=word.replace("\n","")
    if len(word) <= 16:
        n=16-len(word)
        key=word+'#'*n
       # print(key)
        key=key.encode("ascii")
        #print(key)
```



```
    # creating the AES cipher
    mode=AES.MODE_CBC
    cipher=AES.new(key,mode,iv)
    # encrypt the plaintext with padding
    cipher_text_new=cipher.encrypt(Padding.pad(plaintext,16))
    l=0;
    if cipher_text ==cipher_text_new:
        key=word
        l=1
        print("Key is found and key is:",word)
        break

#if key is not in the given list
if(l==0):
    print("Key is not found in given wordlist")
```