EXPERIMENT : 3

NAME : Aartee chimate
BRANCH : IT
UID : 2018140012
BATCH : E
COURSE : CSS LAB

AIM :

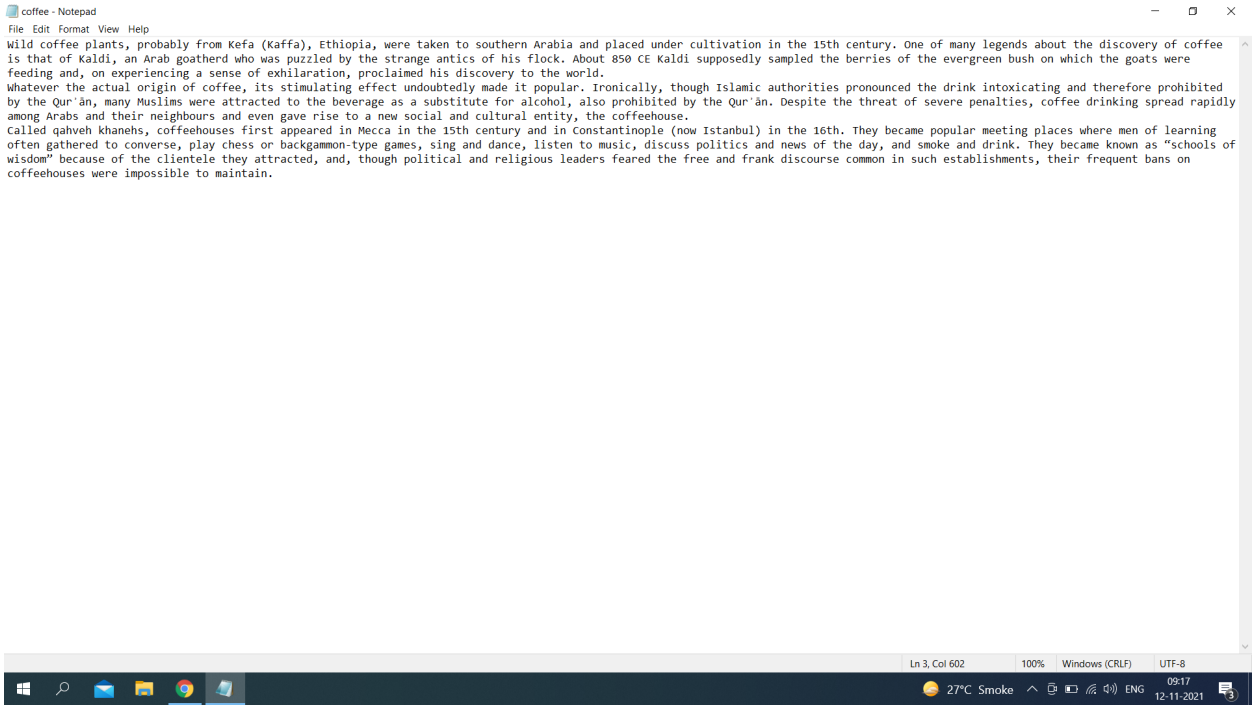
To get familiar with the concepts in secret-key encryption also gain first-hand experience on encryption algorithms, encryption modes, paddings, and initial vector (IV). After this lab should be able to use tools and write programs to encrypt/decrypt messages.

PROBLEM STATEMENT :

Task 1: Encryption using different ciphers and modes.
Task 2: Encryption Mode – ECB vs. CBC (Image)
Task 3: Encryption Mode – Corrupted Cipher Text
Task4 : Padding
Task 5: Programming using the Crypto Library

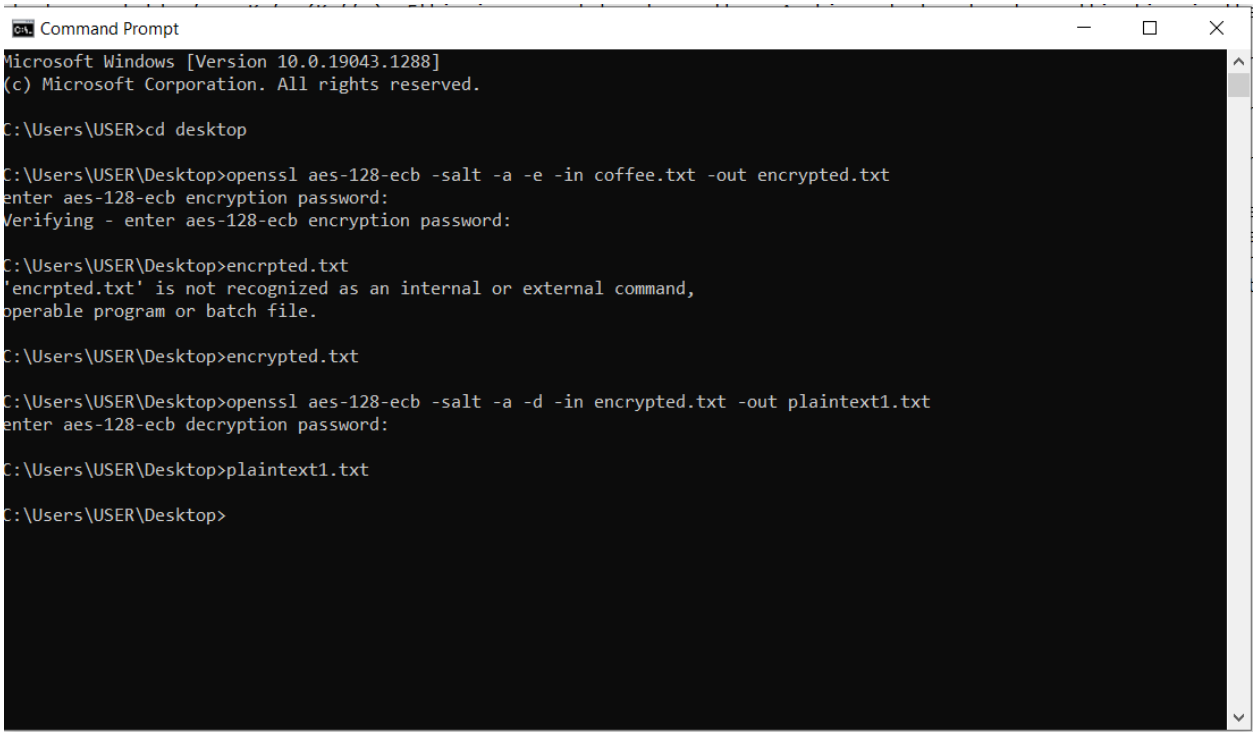
TASK-1:

Plain text:



Using the cipher type -aes

1] Encryption using aes-128-ecb



After Encryption the text is:

encrypted - Notepad

File Edit Format View Help

```
U2FsdGVkX18BrtJ182odLojcOpLo4e1ESLhk8vvRXwkycqoYn/SEwgC8xAbTuy8A
yZt1ro95HNfS714sYstwWUAP2fiRLD3oM/3D6YFLy6U0lZqK6/C+5KcZiaVKuWQo
SRzs1AVD/Zzr24ijfYNs9R9KyJhCL7MqCPJgRRD1PdG/zxbnq1q1/aoxFv1i2dKz
YQMBU7iz3Ofh+eAOiA9iNacWLiaxhKOJjhZIca6mVBI76t88b20eny8YQf+9u/FI
P/pLLswJwI/728UqvGPwYBFhc0xRbe9yQCTd9YX3zinTSv5gvzxDcpav/d6CbxiX
yizOr4GL65QBAmI+qd9vjyZVBECSVKN+xWg1c7JLIvVlPc/7U+Mm36A1nmoxnlLv
+iz9BMovJbTM7wLciwv3ilOjYwBtgeMdplA8lZbwARiXUOiqWBiMfM+kkz1UySFi
Voh20zIO97G/dv2ezm8T4zuqNFijZ8dlAylMqcpG75QwPY57QvTuT8DinItc1heO
ZNcA1+p59jrMS00f9OjZpiSE2gQ5ve/ZFq7PYrUhSczr6yiQiEuizqI1DwWaCj5b
YxsgoKLS/Looik7nVAEMVHwZ9zbE6RBwGwdelwF40KxDGTOXFy9oTcZrqxarpFS/
PPmiXnlxVwKDZKRfy4chOm/zkTATxUMirKZiee4QxYm/FwD1ReeDMIQUUcDpZkk8
0jj5wqo1KLc5MdJUyh9Gtx/jGviQhIfcH6Qw6ppfnbg7ySFt3bUiMi9BjqcEL5nu
hRtMDxbs/oXaxeHt236qHnqnud4PnEg+vY9LpPWBt65ogCn4G+VSzNjVmL8rqQXJ
QRFMWA2Vbt68z0reCf9xUIQ0MD9zugKv7exs8wxcS+7qYl12ZXpQfjt9P56ZzXHU
+ovSuZUYc188rmU9PB9KNs57LSXmkyzUaZYKCJvQS/L4m3deKBbPS8jYu/D+ZQax
Lx+KZy2zNSWOwS1V45ThbAmVOPEzVFiEAkQqzisdUe8zIrbO9NSc2sCahn7spZCc
K5QRUoZc0Gdp6LVpVb73QrXozHV5QTW4evplRiELQbmRsaMrrCQc9ESjeNnmRhiV
TSWy7U/zqj6PLHtOXuEDF0WGZY75zzXP6COELq0syjfEHUdEdAlP1m+10rpOnTua
XF9bjsiEXBsxWo8AAuK1xRQ+GknqV0WWBsn3jXeJ2fDoylVJS6PDSyGl38eA0FHK
RSwF1TxV6pBvNyzLuj9DZrmJZWViAmrLUWxqoV+aK9e/yEMWmaSNVdYrx3bBTrcy
cjFd8/cU0fuA7pjr86OaYYqJvllgg3O0sjy/pg5wfswr1OMpLEZ/nA0HwKVcMXzx
Vb1xgPlmJvVWwCh293TuZvfev1ZPTT5HtORock/Y2UPRegRzPQfcc2bTnkKG9wAA
z20KdQdv/18a6Wv8vEIOJWzvr0e+2WuRKGZDdDYay5nzcSL0HfQU1PSL6EgR/Gce
YsJxJwte0bVSQbXcjW20bk3Iv9pMaeISBvRL9ZEmO5VGpCMPrgSqk5IdTMpnQ6M0
kqsdEpVY5sTf7c1EaflD/EeIf6HOu+lyz71hce6JJemqUwsX7aIIvx50DQpTp2+7
6+3b65i00Yp5Sx0bb3Z/GVZDwJYekQDnAfZNJtz6xKcboB0QD7wrpK9EaxXxPBqC
Q+TFK5a3qj7J4B+fS2jsLtwWY+GDnj6fi0bBvoryQT74go5qepsBRKyDgAysww76
ULZpdVAclO6h7Lqa/DM4rx+ZpDNLPetA+EgiyLRoC0u4wEtaBnQ4cXyN+d5vwo9w
c5vNUD7nLgsbKdvuOzTlZP0UfmCSkhlCfQDc71BK26M8OFOK7Gz/86epPIFg/j3j
```

After decryption the text is:

plaintext1 - Notepad

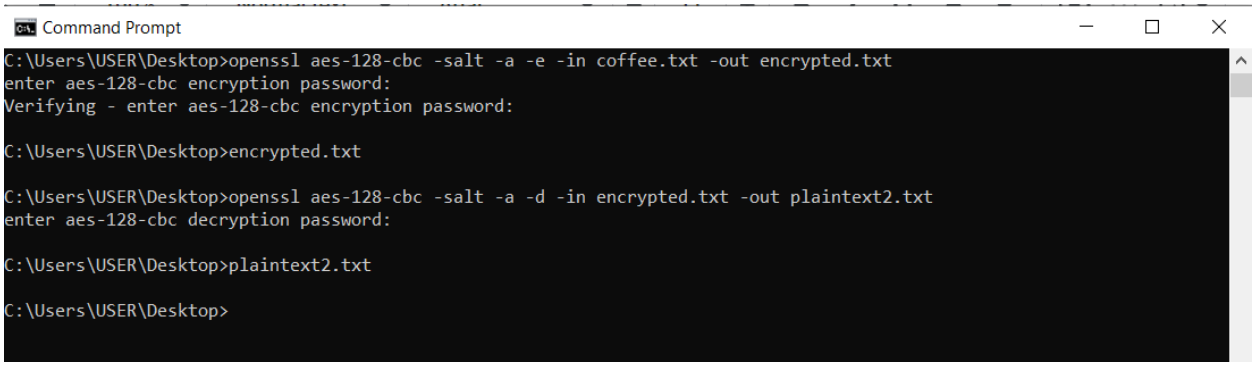
File Edit Format View Help

Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century. One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock. About 850 CE Kaldi supposedly sampled the berries of the evergreen bush on which the goats were feeding and, on experiencing a sense of exhilaration, proclaimed his discovery to the world.

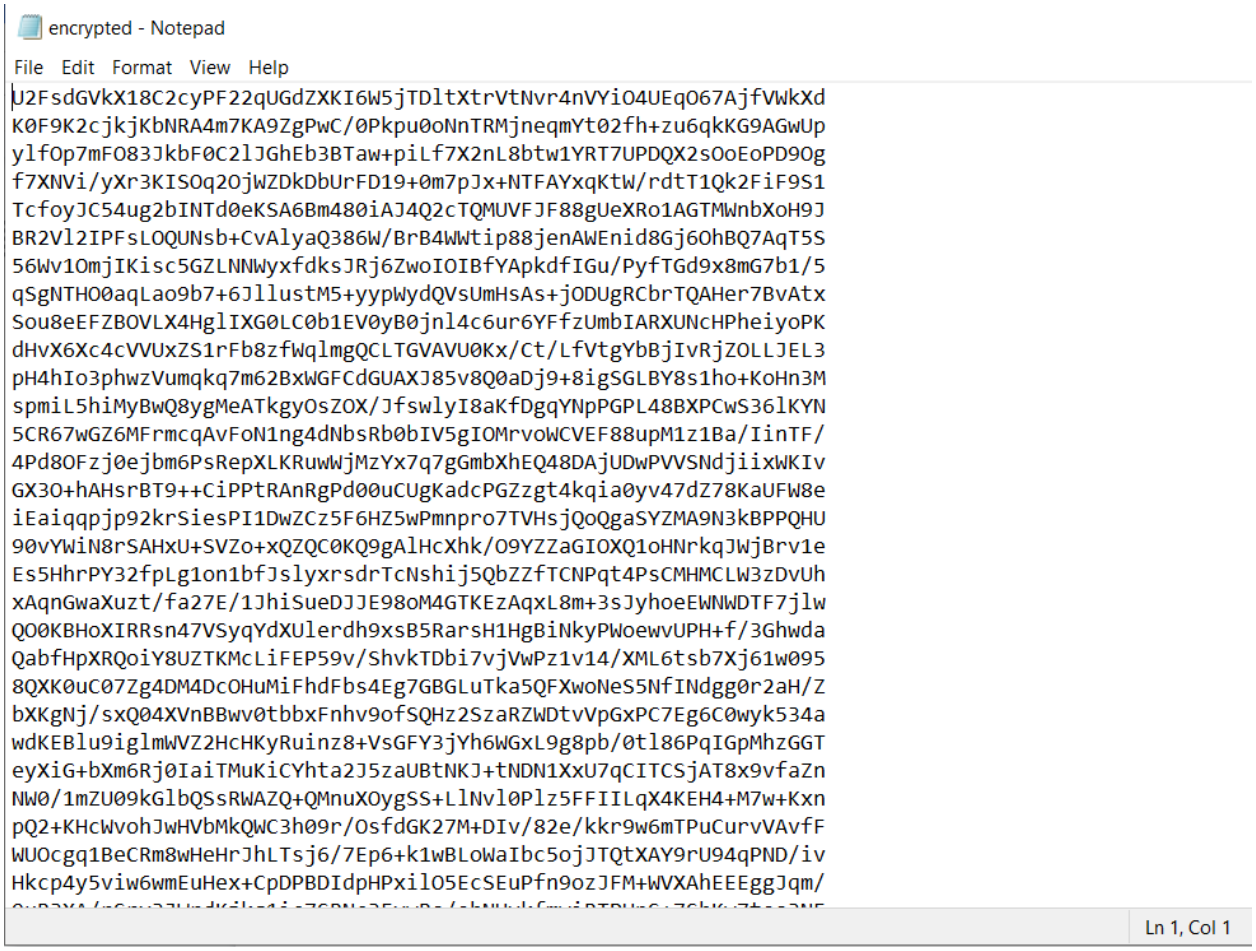
Whatever the actual origin of coffee, its stimulating effect undoubtedly made it popular. Ironically, though Islamic authorities pronounced the drink intoxicating and therefore prohibited by the Qurʾān, many Muslims were attracted to the beverage as a substitute for alcohol, also prohibited by the Qurʾān. Despite the threat of severe penalties, coffee drinking spread rapidly among Arabs and their neighbours and even gave rise to a new social and cultural entity, the coffeehouse.

Called qahveh khanehs, coffeehouses first appeared in Mecca in the 15th century and in Constantinople (now Istanbul) in the 16th. They became popular meeting places where men of learning often gathered to converse, play chess or backgammon-type games, sing and dance, listen to music, discuss politics and news of the day, and smoke and drink. They became known as “schools of wisdom” because of the clientele they attracted, and, though political and religious leaders feared the free and frank discourse common in such establishments, their frequent bans on coffeehouses were impossible to maintain.

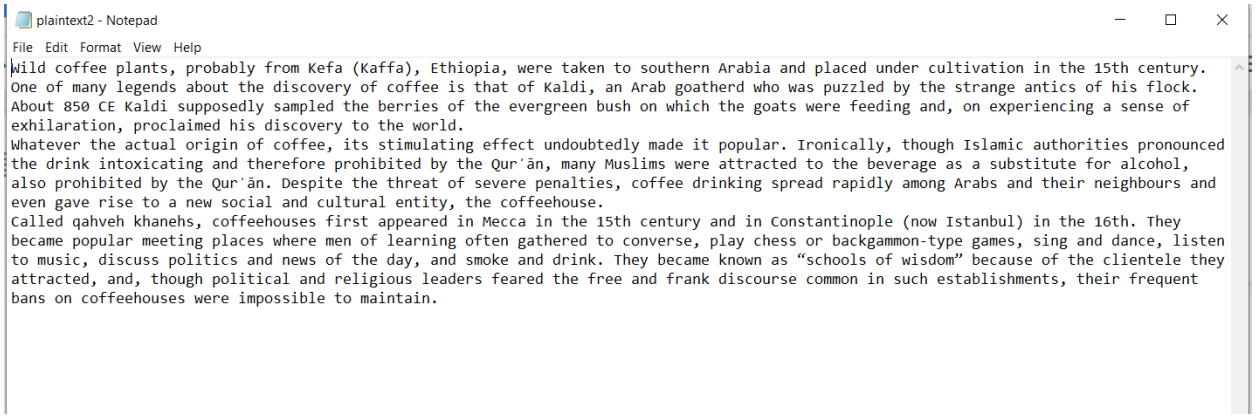
2] aes-128-cbc



After encryption the text is:



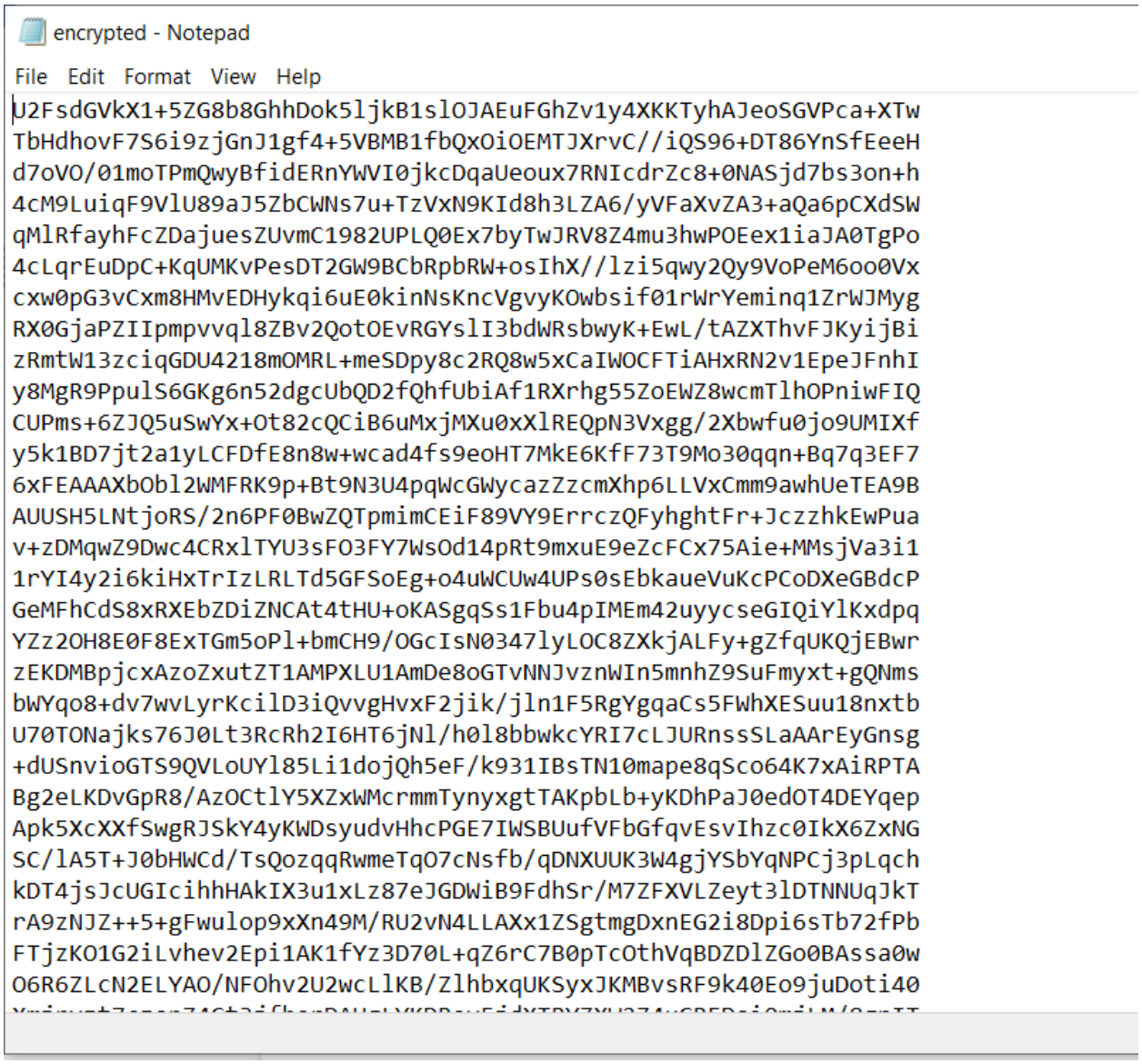
After decryption the text is:



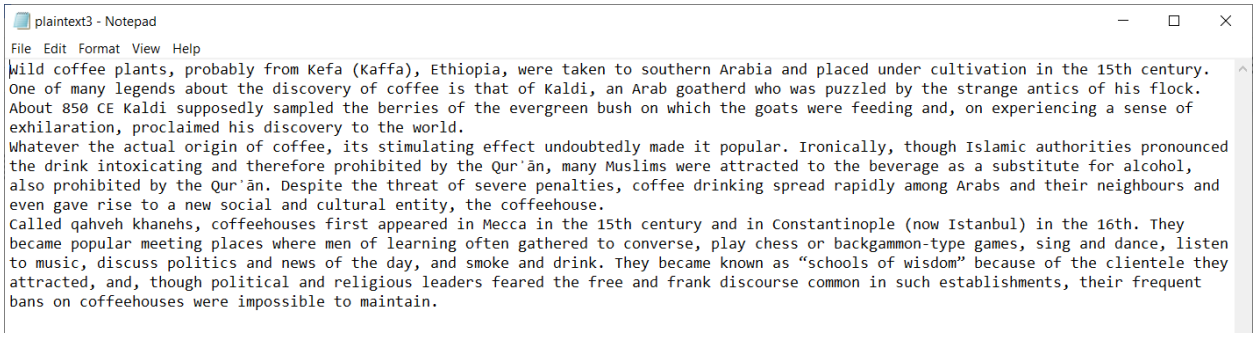
3] Encryption using aes-128-cfb:

```
C:\Users\USER\Desktop>openssl aes-128-cfb -salt -a -e -in coffee.txt -out encrypted.txt
enter aes-128-cfb encryption password:
Verifying - enter aes-128-cfb encryption password:

C:\Users\USER\Desktop>encrypted.txt

C:\Users\USER\Desktop>openssl aes-128-cfb -salt -a -d -in encrypted.txt -out plaintext3.txt
enter aes-128-cfb decryption password:

C:\Users\USER\Desktop>plaintext3.txt
```

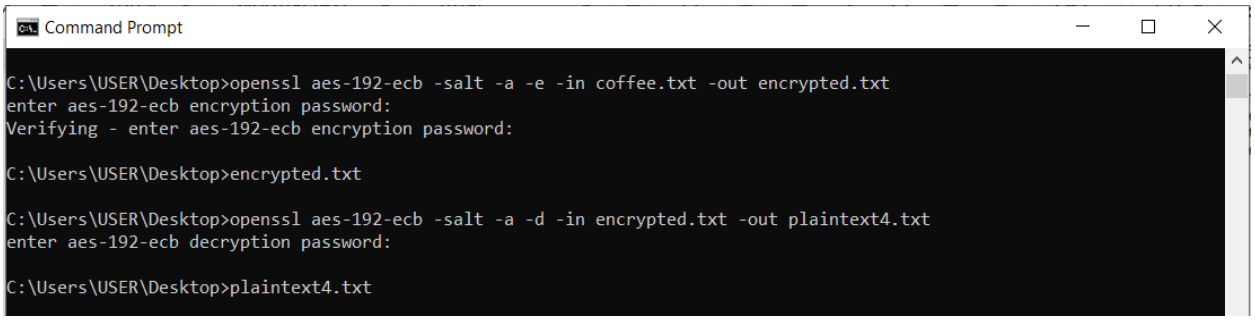
After encryption:



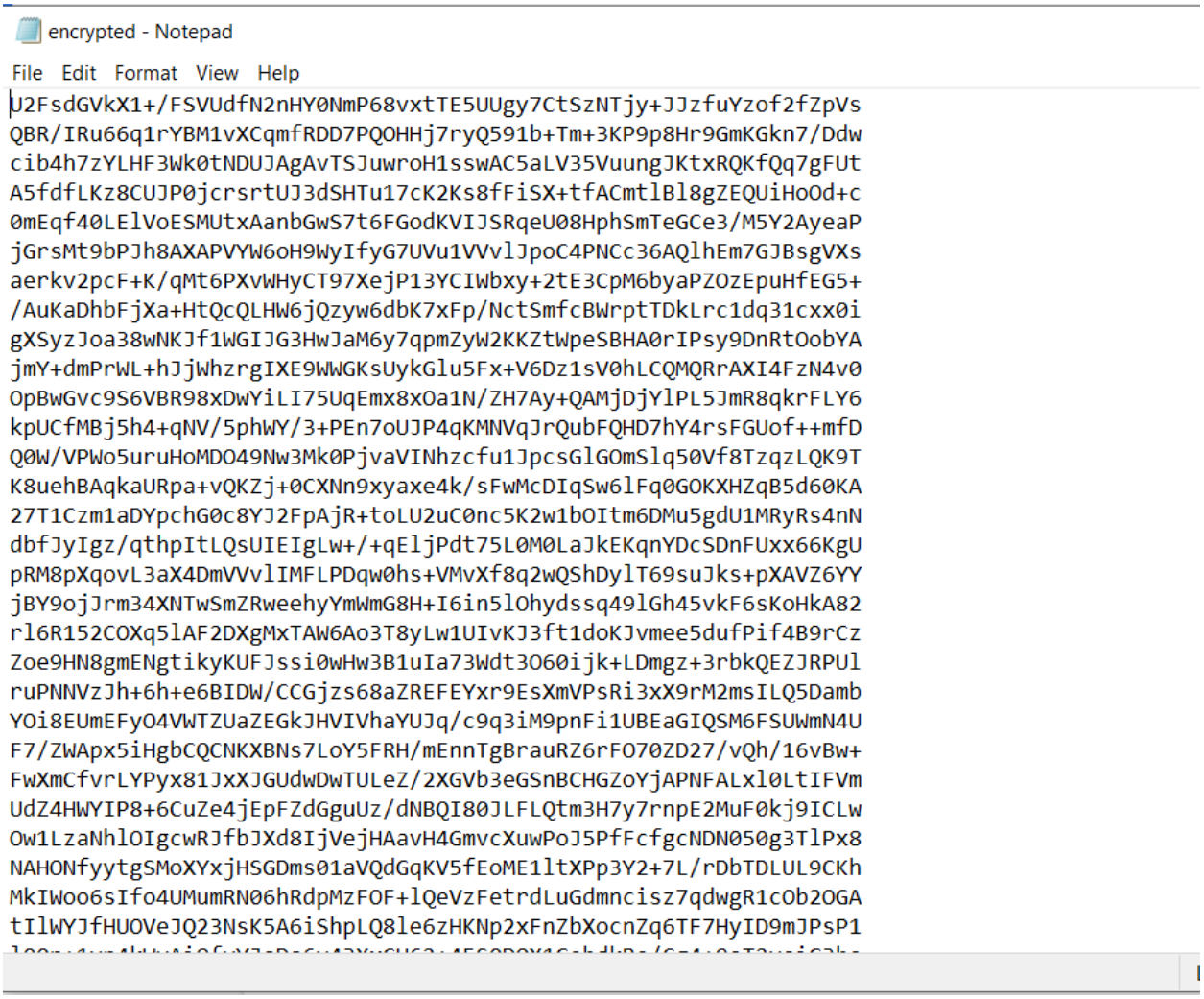
After decryption:



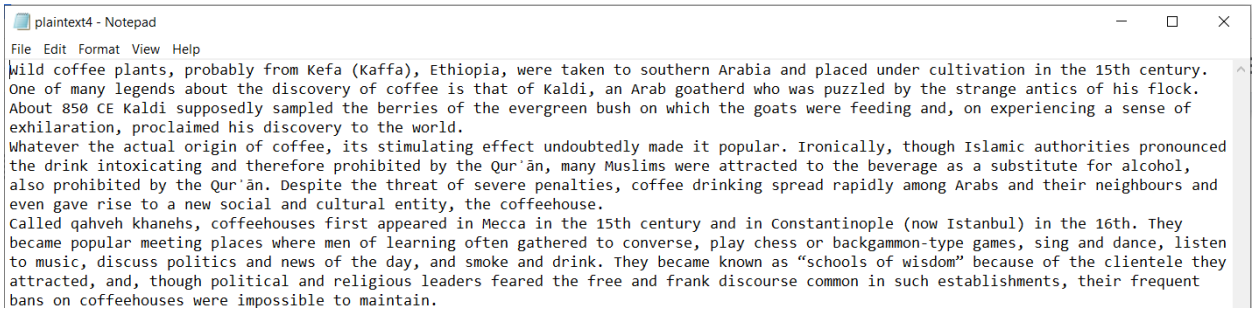
4] Encryption using aes-192-ecb:



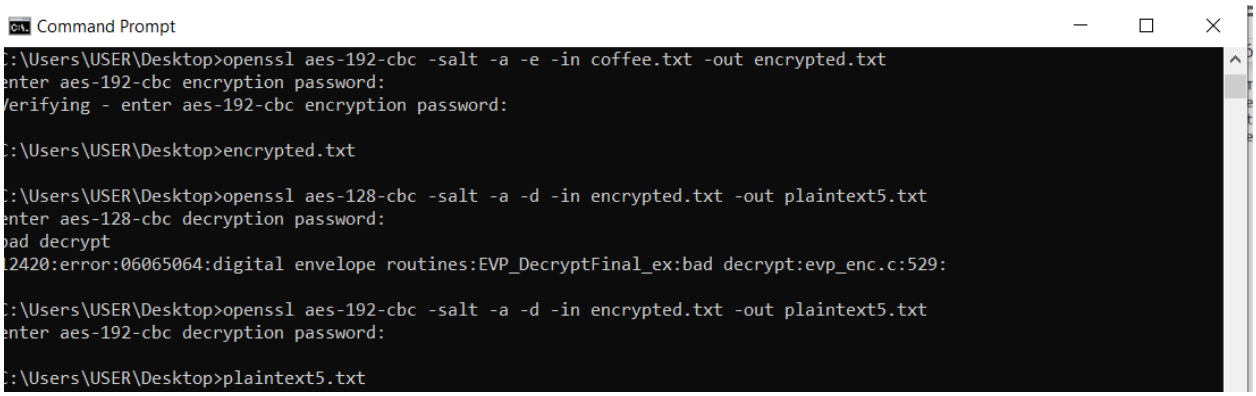
After encryption:



After decryption:



5] Encryption using aes-192-cbc:



After encryption:

encrypted - Notepad

File Edit Format View Help

```
U2FsdGVkX19N+obayPOor6//SkKDiRSraBvv1HFXvvu7rYB/eYn4AxxcHhngs284
Elh1MuqPA0EJRtVYqaep5y9z0hXJ1sBCuI9wZknSSKZSyESDdxW98btarU16FmC/
iKf3ou8IOg3HVEXlEvM55g/uKHBkoznEZUM3R4cwOrdi1KQuUb9qQI6BYllpwBA3
ObXMHTR+iJ6KNSv+ahJWgTGsTyrZSy8dunSpYIZnv5dtzBATNh/WuIt41bgwESMv
lEYI5pBstj2rnnmmaV46htLNdq212DfALlg76kQbOz+UWnrolfwRtATZq2IbODlw
yYLTyueU41gSZ6hI/kmuiIEN/5Dlu7gBubjgS5TV8TEFZ2BP+yFAZFZBaBvpl0qA
EaiR22nf6wpXvXD6g484xU57TGFEF3qM8A3gLGwHoxK8JcNKHkxp1LfUhqHE56DH
nJ2nqFa6rvxfOwLSjzgg9/2Abr+ElkiYaT2ZdDSKOrybBJcOmbQJ/Spxoa8L8iW9
JY/2WukDLYCPJPSLHZ0gGszVSrrSnxQu8Omzc0hP17OL4JVcD+Dx4yFHbqBNq8We
WLs2GN7BDMcQjcgkO40Q/re7dNeOUBuU6WIuaZL/G649VPqe6mPvPlTCUO4o5UwV
sjDP0FrUbJ5Ka78wP0mK0NQoNPoi9lsgb4apjLcfpiOO/wtbSn8KtvQy5NN0OjYx
fbmH1PvGX0S07qqTCcbq2qVqN9Uk+xM9OCsNPedhS//clNDBGGqZd1JudlmQklWT
NrGGeKaYW5/ca+8kW08D5fJ3Iw6d1vadZwRllv0nzKMH6jJiZtxfY8oJ7BGR0LCq
nAo5OI8YZN7+OPRimx+EK1+5qT386EPX5WIrHtux3KWvHipJnV30ED/5UkoHQkqU
TANoAYA52s47cGJmCd/B4icD3aPPB/XwVDArUvJBj6DuaxDUWET5T58bX2dJ5zae
3+AR56sZla/nrY/GRwFTIH2iKrGNhsSsTQN50nKYfyhwt5rgy6pXZuIXHau01Pm6
T5J9wuwJolI0DPvCGEQj+o0RSsvtDWEZ/0VgYBayqBVHCJ6TqBXAHgKLdt3cDSu4
BTgVxBFx/5pBMqJMwzy1Yiv0OzU05qeuguAcA1dnqSIM4rvlVUx+fjCrLOnce+X5
QfpKZMK7GAFz2WHOGfI+wrs1QbbgHebc0gCYrf1vqEexfV9moq7Yk/9YZv0NSxjl
FcXPmjp7Ibqih69GUrelve9v3fNV+uUUT5YGf4cUNnSJkcNlAlPMBl1xQWsZnAZQ
pQcS4HP3WObUuDqWvd4USTJVPgVLE0/D7NznEQy0hvw0CLFmT+EmdErL4kLrSihB
X92aaS62IjQPWsj7bf79Ag43gDkzMpdo7vLNdh88MjSp6o4Iq5zzey4GrhMzA8jl
QV8U9mhTGLd/2OV22yJ1K6r1Apoytf2+J/yMRO9VtK+Na3fROjb3lW8gOjAzwYtF
l1XpqiQs5KioxviXsFvluedK559/zq7VMPO2zlSQO7meBj5JEuPTQ4Qf6xWMllRr
BKtR6EftrYiSp5zAP3r8gYSt6xSD3acUwiHlYVJfLE80Ye5A3gz/2k7Ml70GAbSH
yyNaHfHgvkLp5nXfQPrdL0oI41T55gaxWPbeZP2rfKYZLPzB9UYpSrAQj198+xgV
RaU+kD3NtrHnvSItf8yNljxW0r1oySCnW3uRk83pgDKFxzq70IB+kWSC/G+OG+3j
kyZgza898wRq9v3jYhAUGcFdUsbdMBU/M+731bITABm6XNylGzoVsETTBjrVl7Vh
ZV7zmfQn9FJ9BgdvUONsB8CX4KjL8MBuXwW/4XQkvmgWHpAFLVefQQBB/S5Zd8o2
```

After decryption:

plaintext5 - Notepad

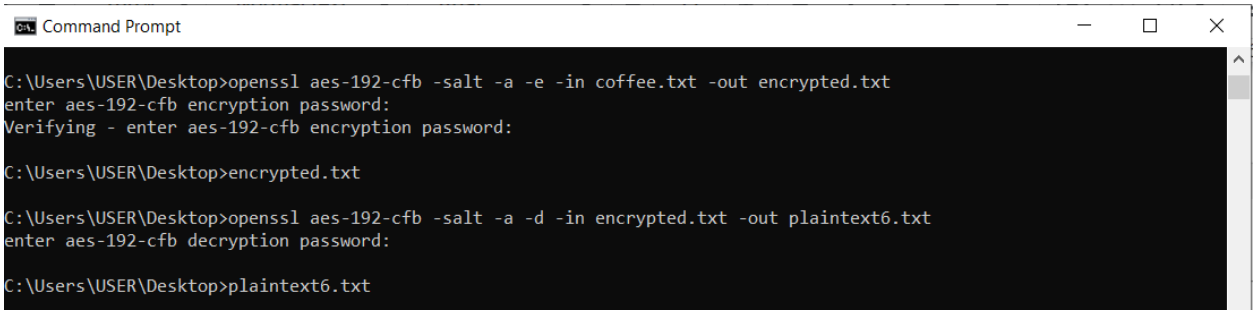
File Edit Format View Help

Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century. One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock. About 850 CE Kaldi supposedly sampled the berries of the evergreen bush on which the goats were feeding and, on experiencing a sense of exhilaration, proclaimed his discovery to the world.

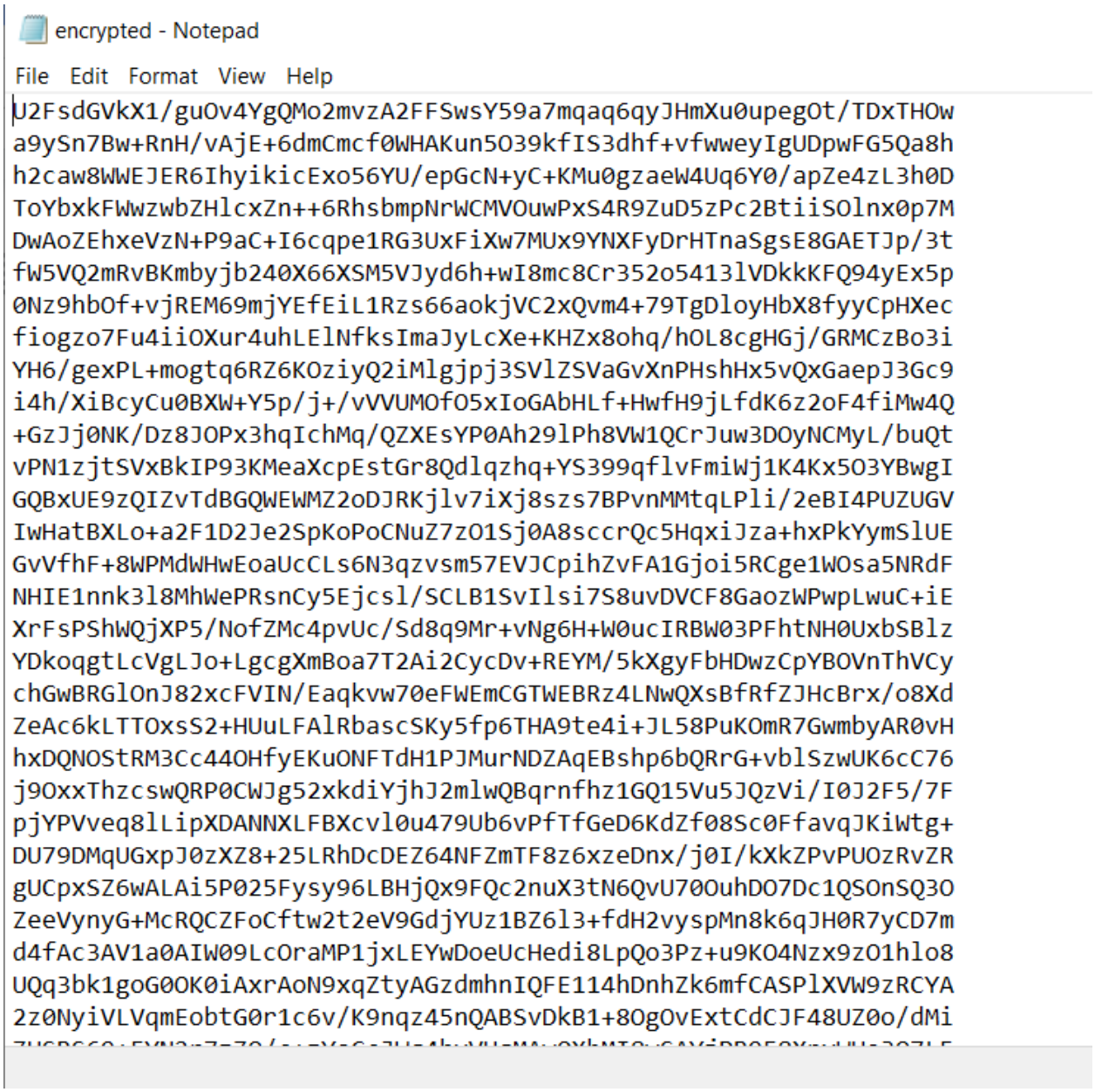
Whatever the actual origin of coffee, its stimulating effect undoubtedly made it popular. Ironically, though Islamic authorities pronounced the drink intoxicating and therefore prohibited by the Qurʾān, many Muslims were attracted to the beverage as a substitute for alcohol, also prohibited by the Qurʾān. Despite the threat of severe penalties, coffee drinking spread rapidly among Arabs and their neighbours and even gave rise to a new social and cultural entity, the coffeehouse.

Called qahveh khanehs, coffeehouses first appeared in Mecca in the 15th century and in Constantinople (now Istanbul) in the 16th. They became popular meeting places where men of learning often gathered to converse, play chess or backgammon-type games, sing and dance, listen to music, discuss politics and news of the day, and smoke and drink. They became known as “schools of wisdom” because of the clientele they attracted, and, though political and religious leaders feared the free and frank discourse common in such establishments, their frequent bans on coffeehouses were impossible to maintain.

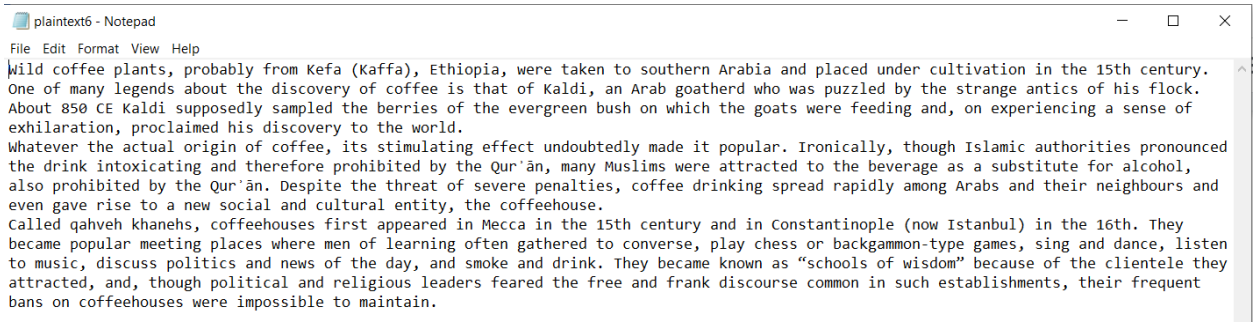
6]Encryption using aes-192-cfb:



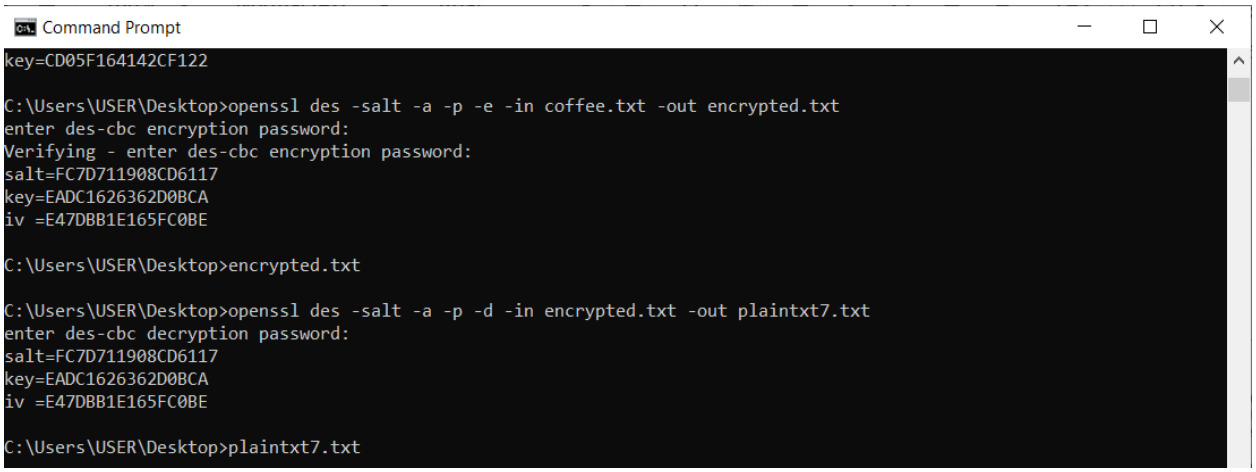
After encryption:



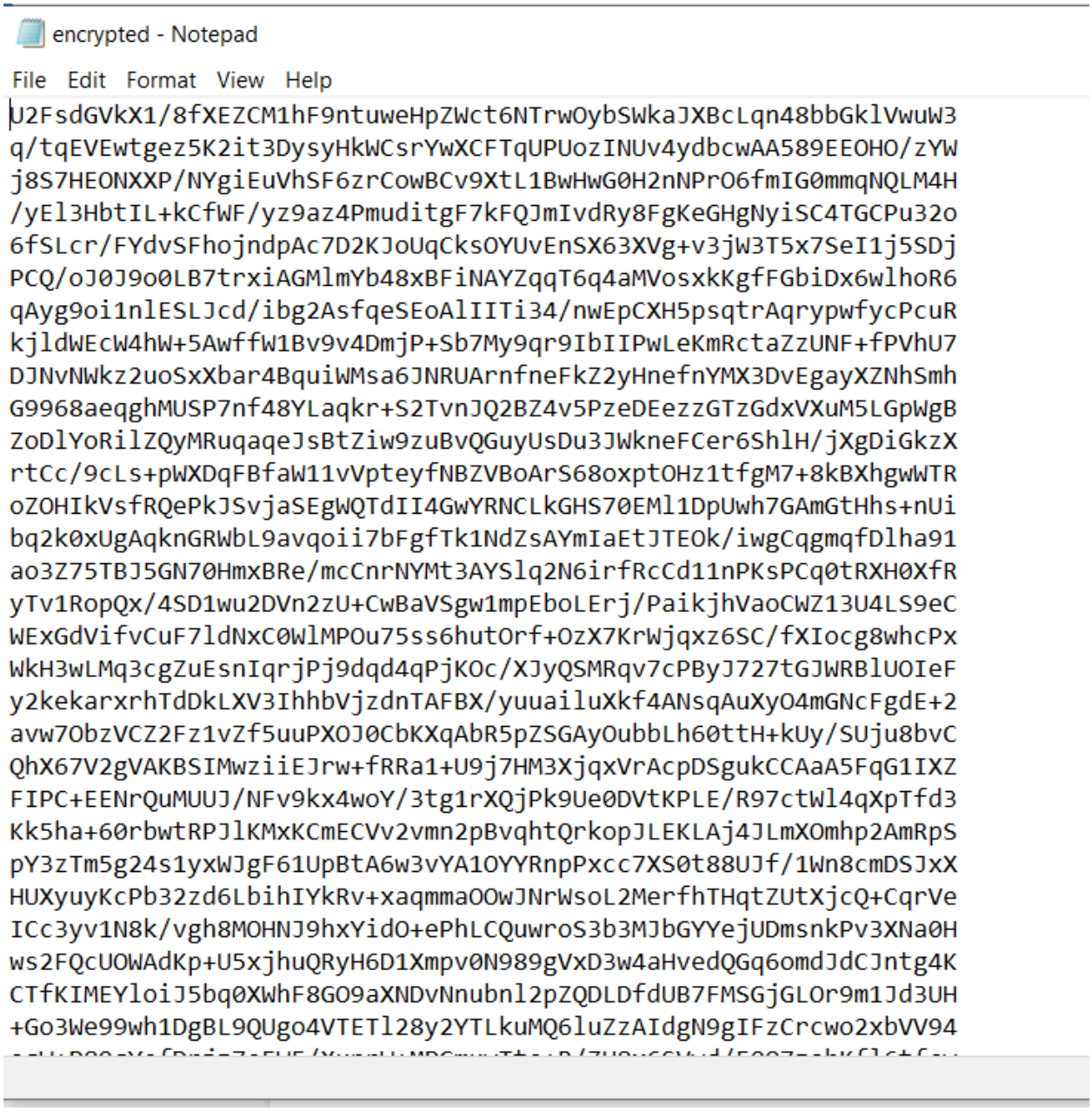
After decryption:



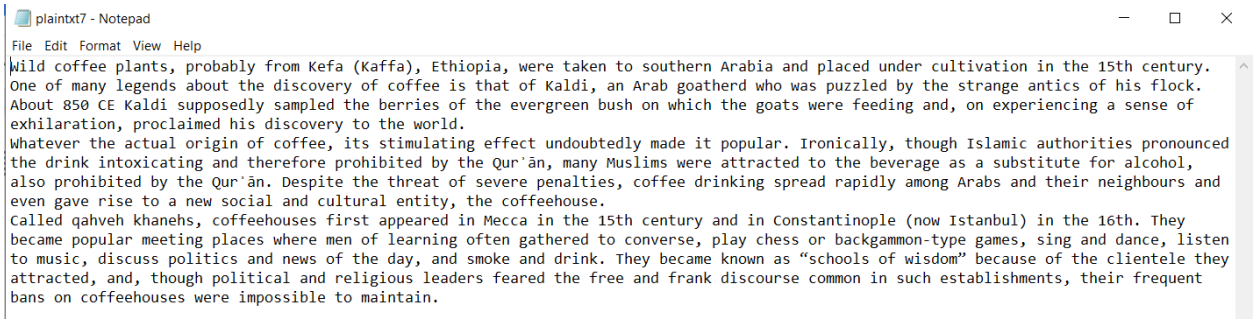
7]Encryption using des-ecb:



After encryption:



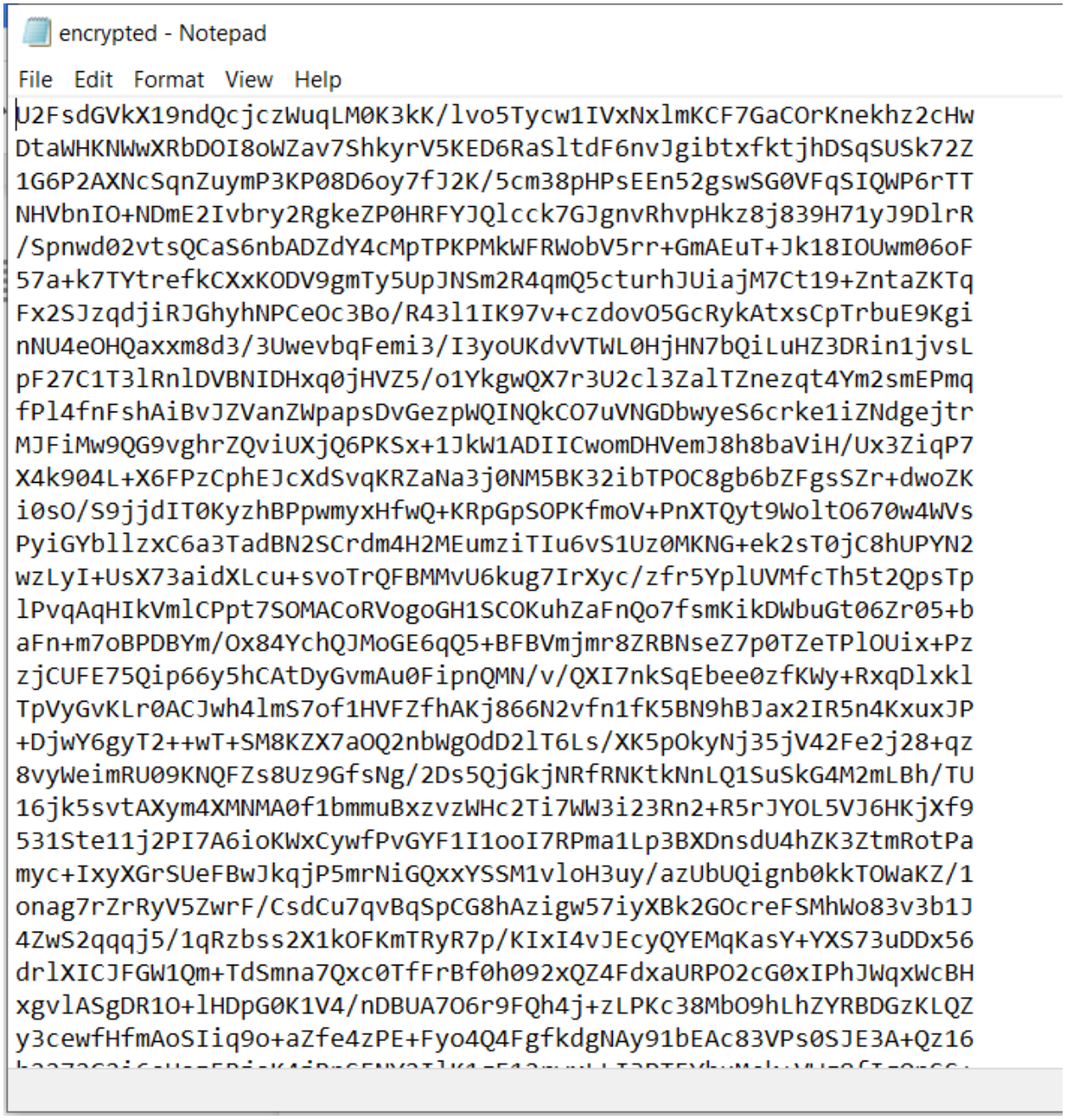
After decryption:



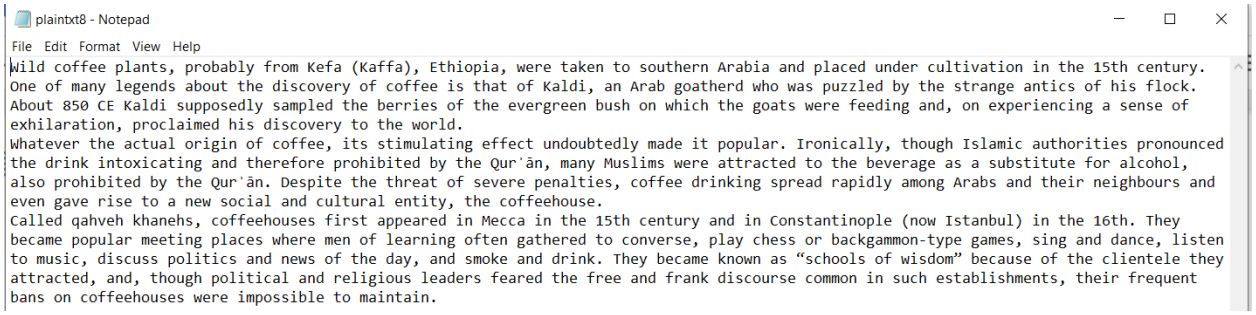
8] des-cbc:

```
C:\Users\USER\Desktop>openssl des-cbc -salt -a -p -e -in coffee.txt -out encrypted.txt
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
salt=F44A1F3F3714FB7E
key=466AFE4B068B2702
iv =8956DCF4D9D8FD86

C:\Users\USER\Desktop>openssl des-cbc -salt -a -p -d -in encrypted.txt -out plaintxt8.txt
enter des-cbc decryption password:
salt=F44A1F3F3714FB7E
key=466AFE4B068B2702
iv =8956DCF4D9D8FD86

C:\Users\USER\Desktop>plaintxt8.txt
```

After encryption:



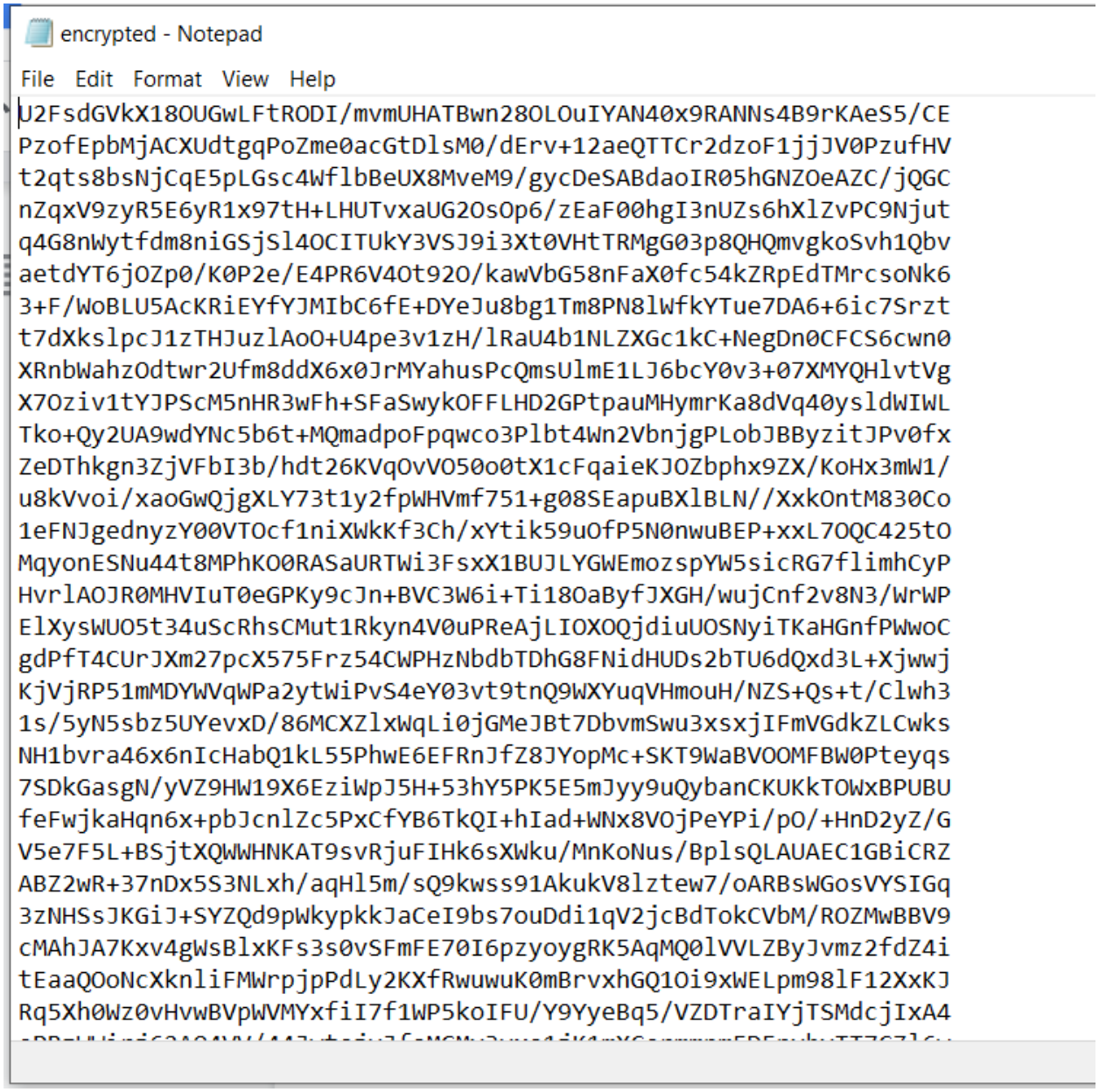
After decryption:



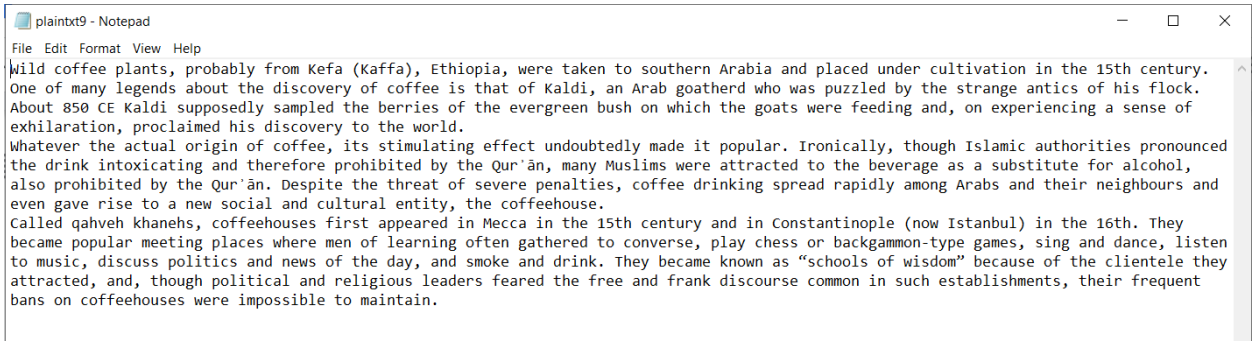
9] des-cfb:

```
C:\Users\USER\Desktop>openssl des-cfb -salt -a -p -e -in coffee.txt -out encrypted.txt
enter des-cfb encryption password:
Verifying - enter des-cfb encryption password:
salt=0E506C0B16D44E0C
key=7584734E0A03B431
iv =6FBF92D454373B2B

C:\Users\USER\Desktop>encrypted.txt

C:\Users\USER\Desktop>openssl des-cfb -salt -a -p -d -in encrypted.txt -out plaintxt9.txt
enter des-cfb decryption password:
salt=0E506C0B16D44E0C
key=7584734E0A03B431
iv =6FBF92D454373B2B

C:\Users\USER\Desktop>plaintxt9.txt
```

After encryption:

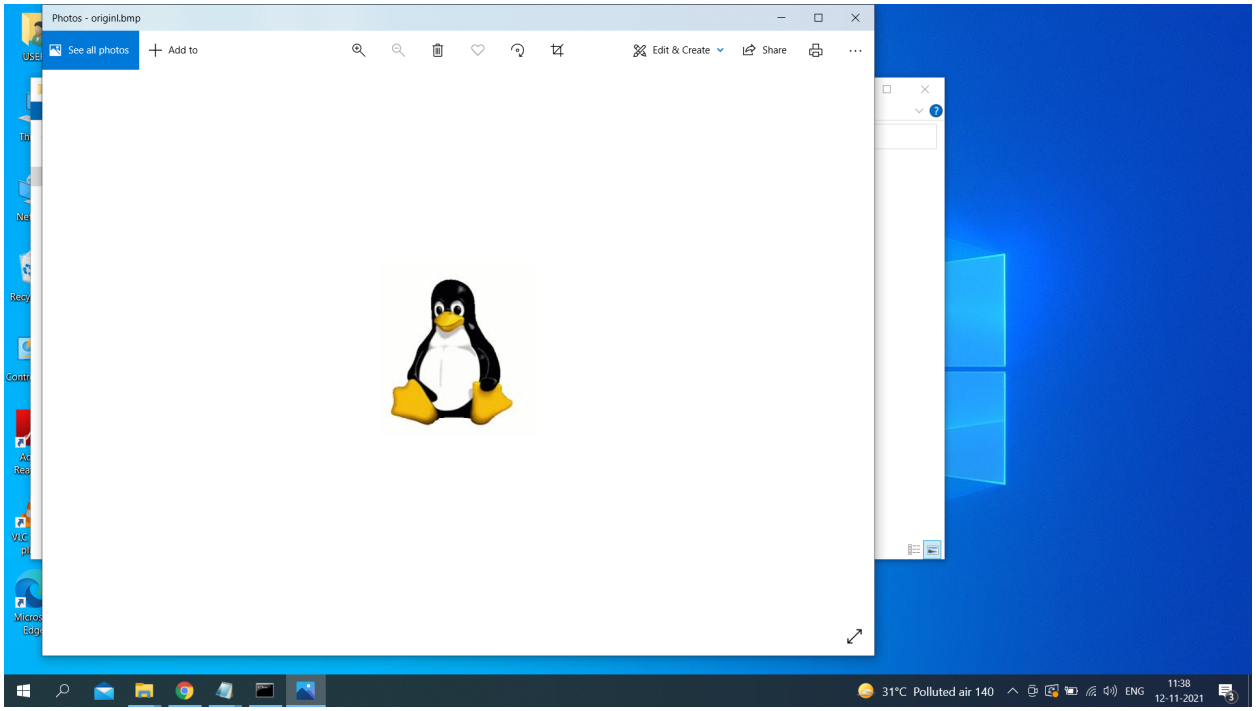


After decryption:



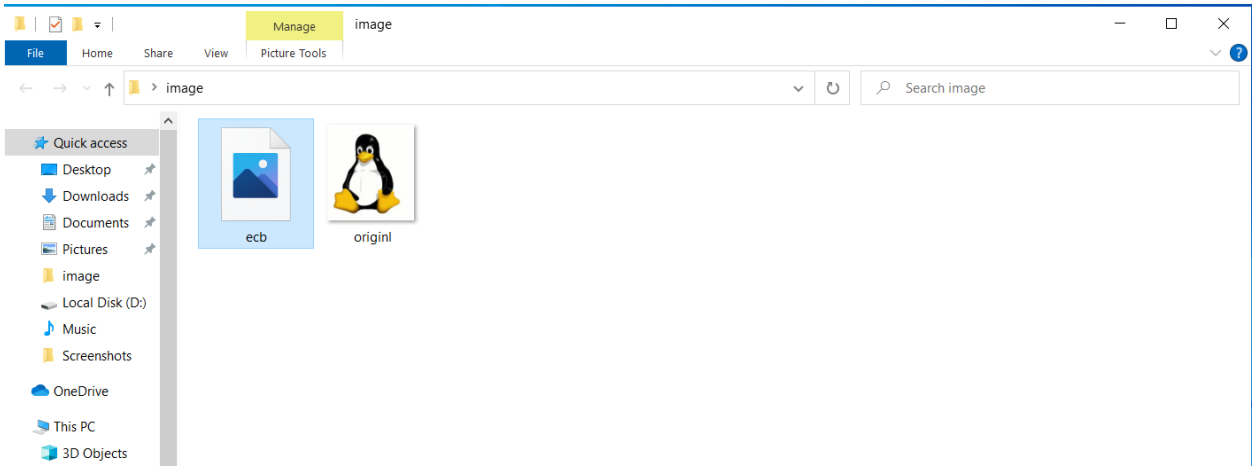
Conclusion:
1] In the AES I observed that the kery length can be changed but in DES it cannot be because DES only supports a key length of 56 bits. AES supports the key length of 128,192 and 256 bits.
2] The encrypted text is longer as compared to the actual plain text because the encryption is providing redundancy to the plain text.
3] ECB is the simplest and weakest, because repeating plaintext generates repeating ciphertext. As a result, anyone can easily derive the secret keys to break the encryption and decrypt the ciphertext. ECB may also leave obvious plaintext patterns in the resulting ciphertext.
4]In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block.In CBC parallel encryption is not possible since every encryption requires a previous cipher.
5] AES and DES are symmetric key algorithm using the same keys to encrypt and decrypt the data.

TASK:2
Original image:

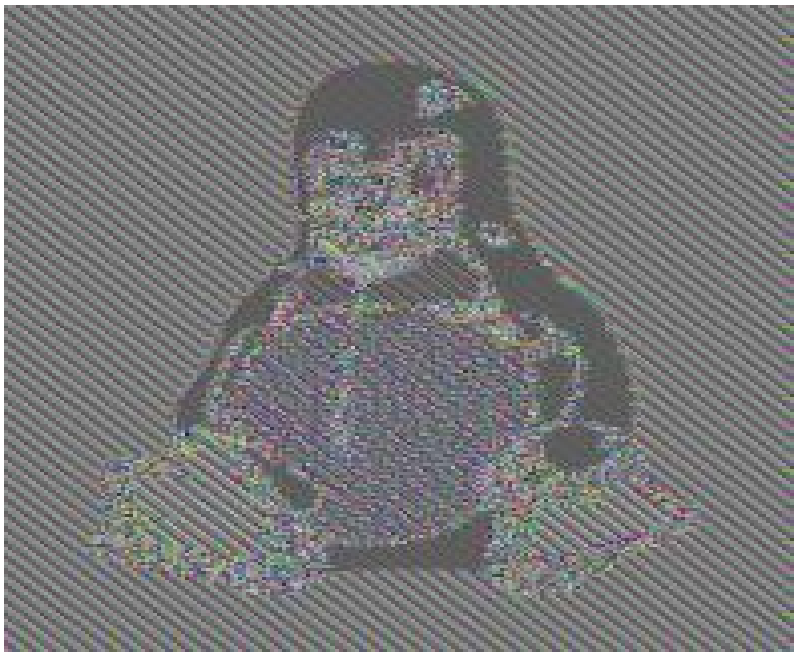


a) Using the cipher type -aes-256-ecb:

```
C:\Users\USER\Desktop\image>openssl enc -aes-256-ecb -e -p -in originl.bmp -out ecb.bmp
enter aes-256-ecb encryption password:
Verifying - enter aes-256-ecb encryption password:
salt=56FC5EF28876B48A
key=FBD39990EA902D16C147E0F7DD65B05E1BB4E16CA43D0BD530553A3D434E6835

C:\Users\USER\Desktop\image>
```



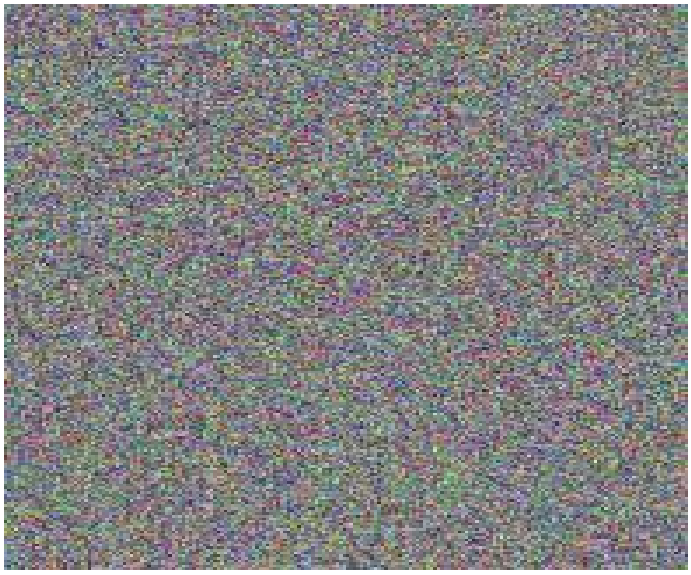
Ecb image:



b) Using the cipher type -aes-256-cbc:

```
C:\Users\USER\Desktop\image>openssl enc -aes-256-cbc -e -p -in originl.bmp -out cbc.bmp
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
salt=867EA63F945A7DFB
key=F37A992A5336A71CDBE20475687C1F95F5617D24F1ADBF0EAD3733F26572CC5C
iv =761C7DFBA41350DA7995F7FE150709D2
```

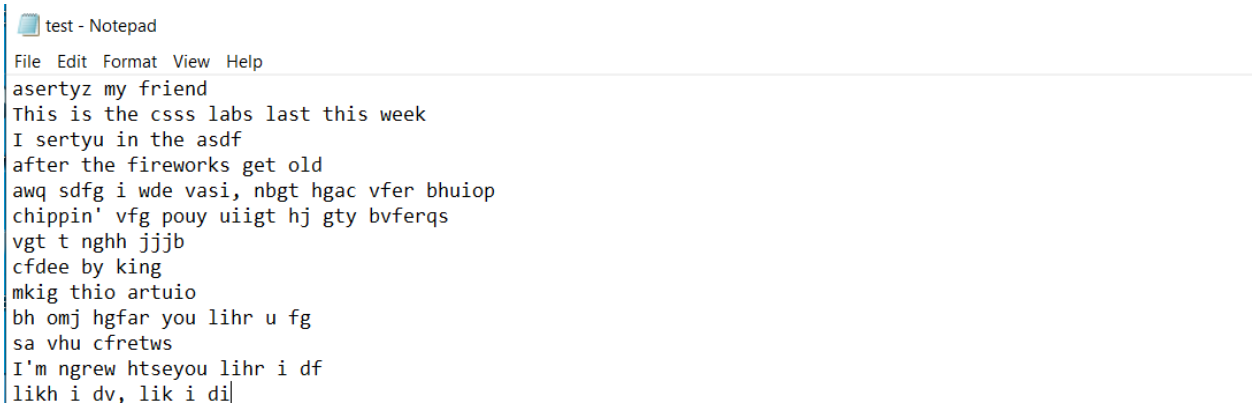
Cbc image:



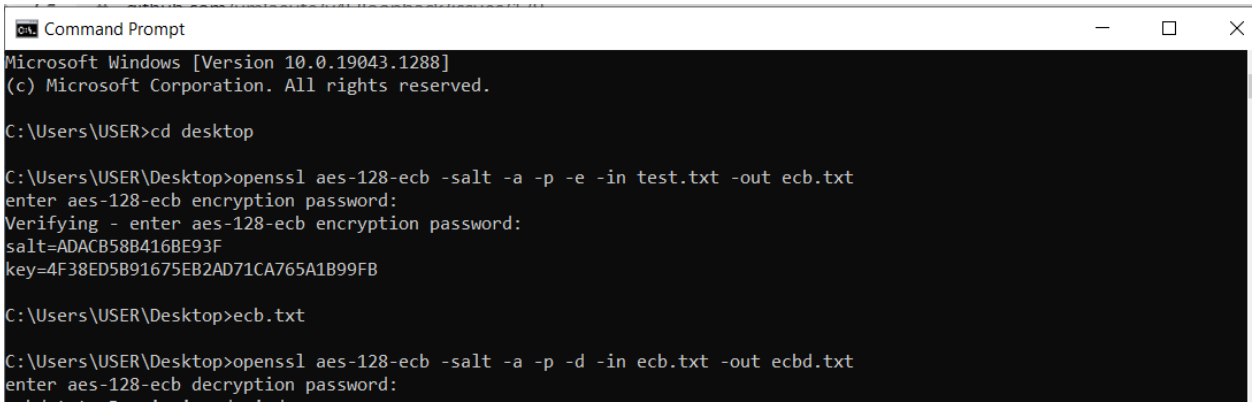
Observation:
1] The image encrypted using ECB mode, we can still see some colors or shape of the image from which we can try to figure out the actual image.
2] The image encrypted using CBC mode, the entire image is fully distorted and there is no way by which we can try to figure out the actual image.

TASK:3

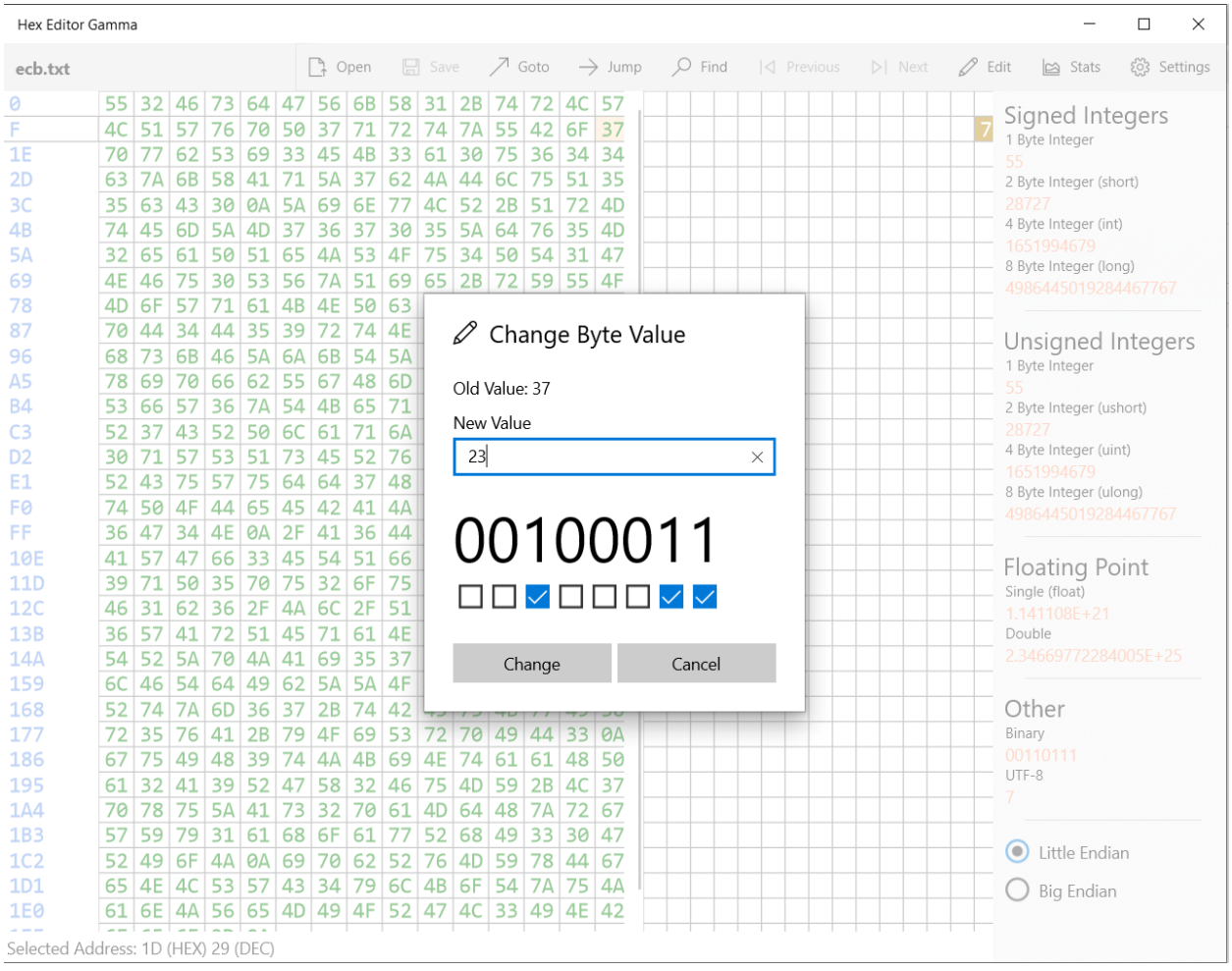
Plain text:



1] aes-128-ecb:



Corrupting 30 byte

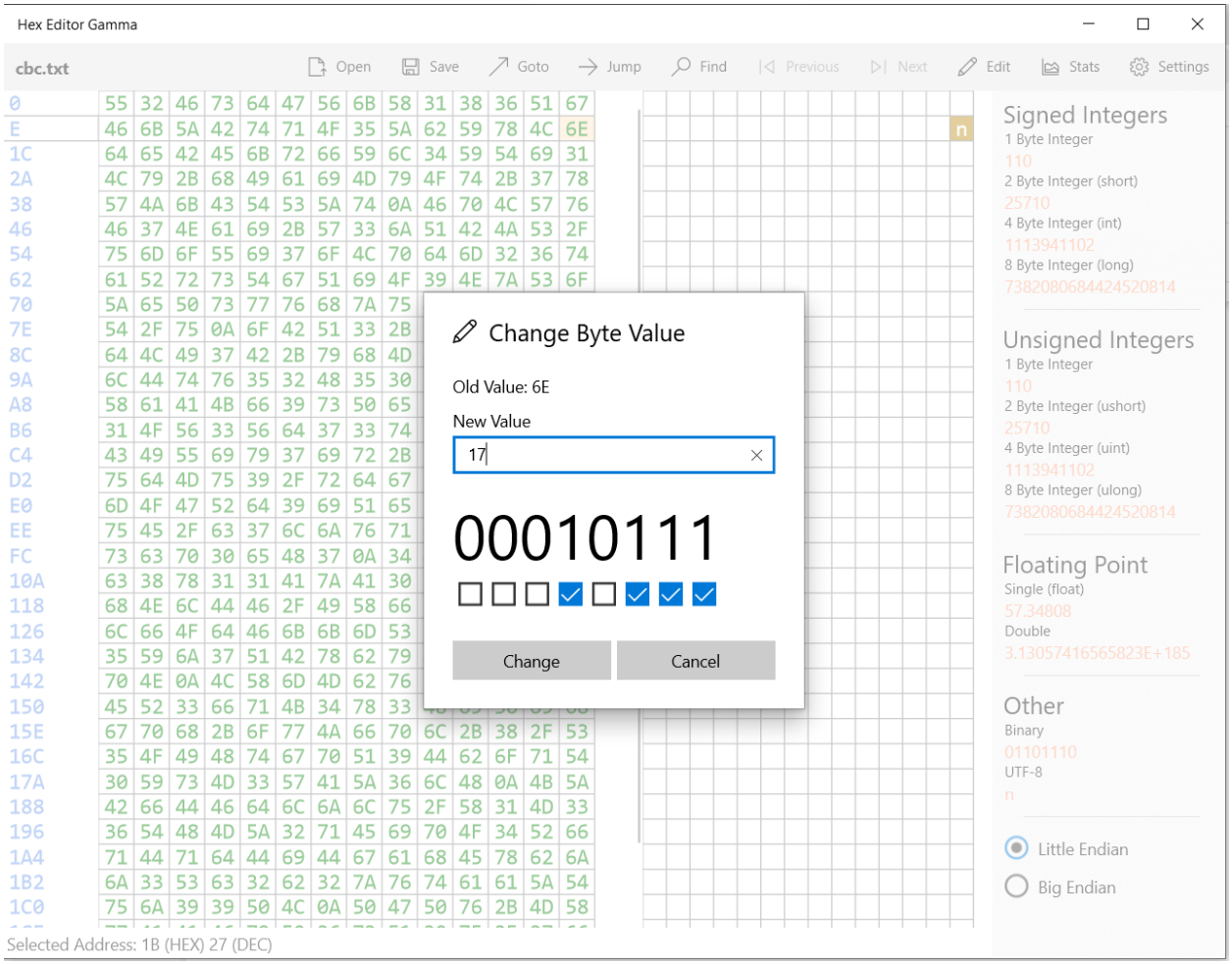


Decrypting file:

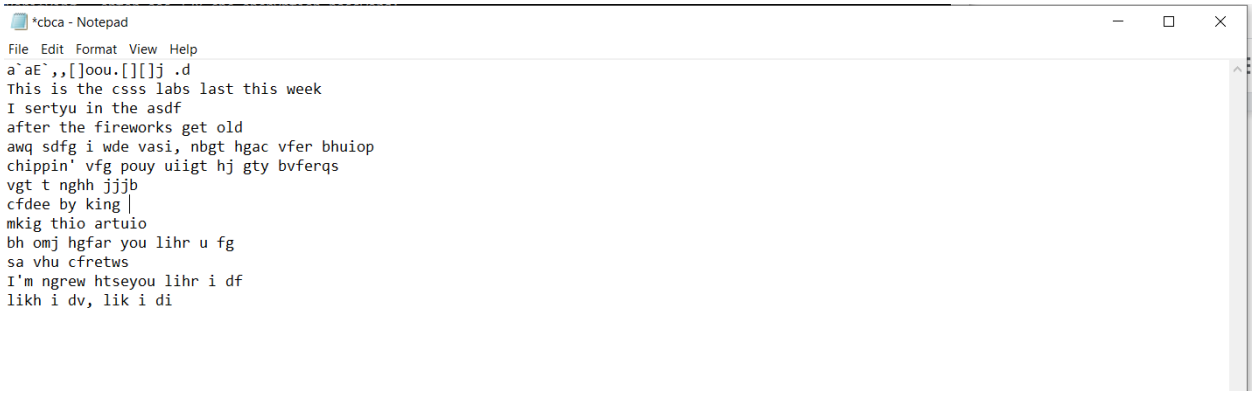
2] aes-128-cbc:

```
C:\Users\USER\Desktop>openssl aes-128-cbc -salt -a -p -d -in cbc.txt -out cbca.txt
enter aes-128-cbc decryption password:
salt=3A420164641B6A3B
key=FC2288F0E4D04A1937BE58D70D7519BB
iv =F13E0DB001FBC53D7AD5BDC3F5C7B510

C:\Users\USER\Desktop>cbca.txt

C:\Users\USER\Desktop>
```

Corrupting 30 byte



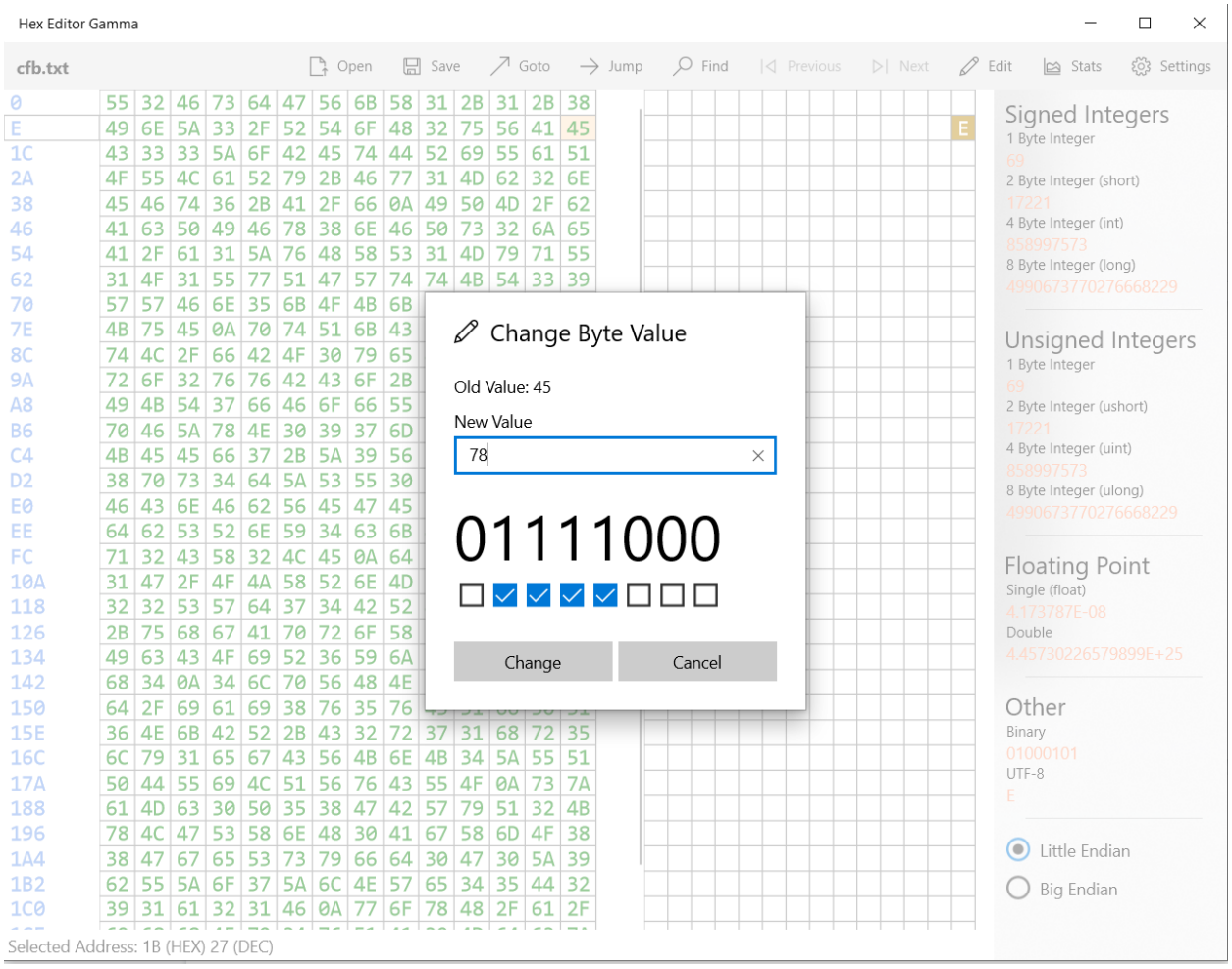
Decrypt file:



3] aes-128-cfb:

```
C:\Users\USER\Desktop>openssl aes-128-cfb -salt -a -p -e -in test.txt -out cfb.txt
enter aes-128-cfb encryption password:
Verifying - enter aes-128-cfb encryption password:
salt=B5FBC227677FD14E
key=6FD09EA1A3207407F05AB66D068ABD5E
iv =A31ECFDD9E0C50CE1F2834086805734A

C:\Users\USER\Desktop>openssl aes-128-cfb -salt -a -p -d -in cfb.txt -out cfba.txt
enter aes-128-cfb decryption password:
salt=B5FBC227677FD14E
key=6FD09EA1A3207407F05AB66D068ABD5E
iv =A31ECFDD9E0C50CE1F2834086805734A

C:\Users\USER\Desktop>cfba.txt
```

Corrupting 30 byte

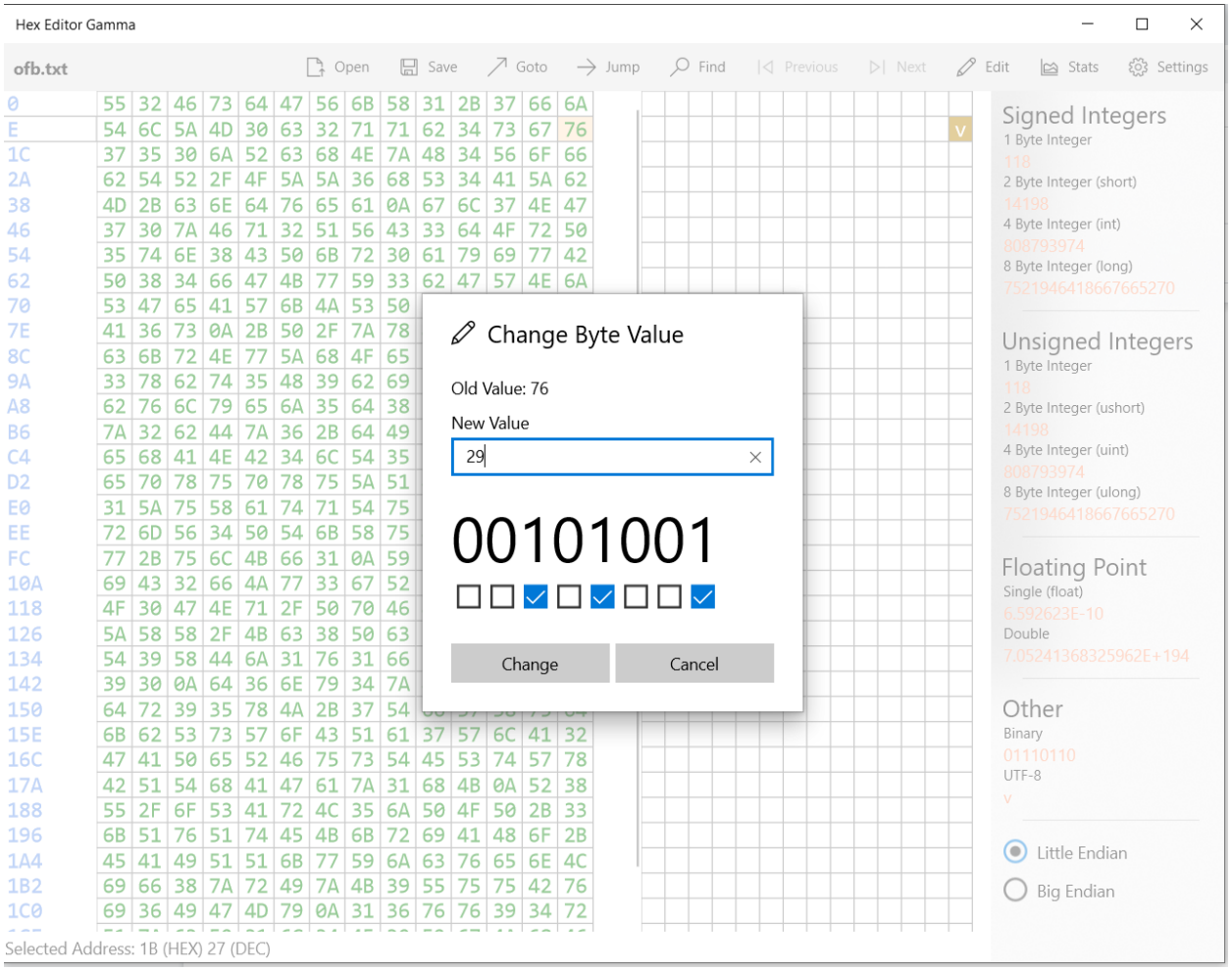


Decrypt file:

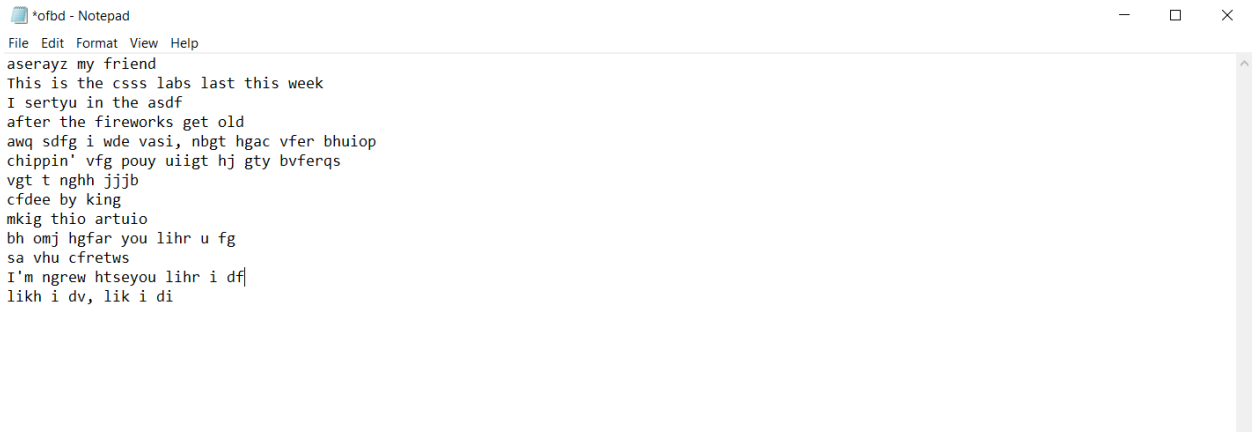
4] aes-128-ofb:

```
C:\Users\USER\Desktop>openssl aes-128-ofb -salt -a -p -e -in test.txt -out ofb.txt
enter aes-128-ofb encryption password:
Verifying - enter aes-128-ofb encryption password:
salt=BB7E34E564CD1CDA
key=BAB5DE5D800076398F2CFC665910F2AC
iv =7F2E17D518300DE3FF0C1CF5A8818D64

C:\Users\USER\Desktop>openssl aes-128-ofb -salt -a -p -d -in ofb.txt -out ofbd.txt
enter aes-128-ofb decryption password:
salt=BB7E34E564CD1CDA
key=BAB5DE5D800076398F2CFC665910F2AC
iv =7F2E17D518300DE3FF0C1CF5A8818D64

C:\Users\USER\Desktop>ofbd.txt
```

Corrupting 30 byte:



Decrypt file:



Observation:

1] In ECB mode , only one block is affected when any problem in the ciphertext happens. Each block is decrypted independently.An advantage of this mode is that there is no dependency

upon other blocks, the encryption and decryption can be carried out by many threads simultaneously.

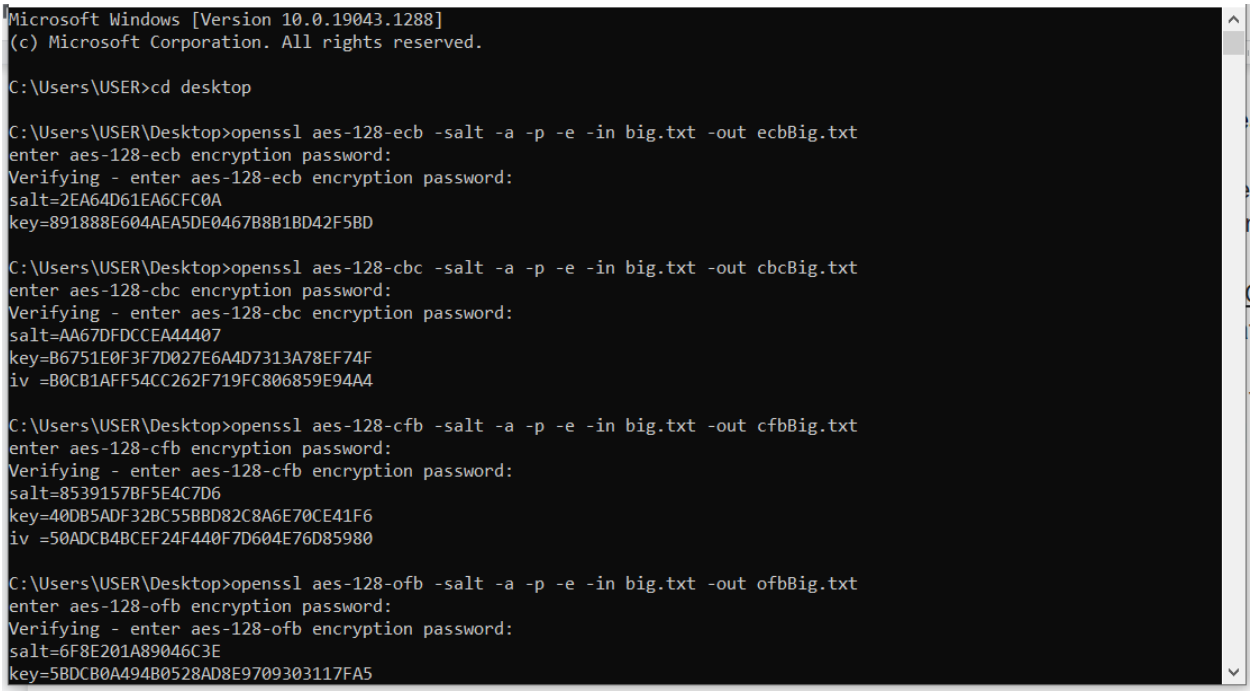
2] Cipher block chaining (CBC) is a mode of operation for a block cipher -- one in which a sequence of bits are encrypted as a single unit, or block, with a cipher key applied to the entire block. . A single bit error in a ciphertext block affects the decryption of all subsequent blocks.

3] In CFB mode, the previous ciphertext block is encrypted and the output is XORed (see XOR) with the current plaintext block to create the current ciphertext block. The XOR operation conceals plaintext patterns.

4]In OFB mode ,the single digit of the 30 th byte is corrupted , then in plain text only that character is corrupted. Thus , only OFB mode shows the ost promising result and almost all the text is recovered.

TASK:4

Big.txt:



Small.txt:

```
iv =9DF17D384C6231EB3A7C77270EA9B292

C:\Users\USER\Desktop>openssl aes-128-ecb -salt -a -p -e -in small.txt -out ecbSmall.txt
enter aes-128-ecb encryption password:
Verifying - enter aes-128-ecb encryption password:
salt=34F99C287303AEED
key=6672FD6B02E1A23A5191582CFE0C13AB

C:\Users\USER\Desktop>openssl aes-128-cbc -salt -a -p -e -in small.txt -out cbcSmall.txt
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
salt=F222E27345815F7B
key=51246FF138FE0CA585DEDD32D1B858FF
iv =55CEC942009B4F3F49A26A7E90B12CCB

C:\Users\USER\Desktop>openssl aes-128-cfb -salt -a -p -e -in small.txt -out cfbSmall.txt
enter aes-128-cfb encryption password:
Verifying - enter aes-128-cfb encryption password:
salt=6D783D5C3ECAEC93
key=8B39D6A7EC2D66522F83F9DC77BA4113
iv =590676AC01C47AC2251EC5EB8482CE29

C:\Users\USER\Desktop>openssl aes-128-ofb -salt -a -p -e -in small.txt -out ofbSmall.txt
enter aes-128-ofb encryption password:
Verifying - enter aes-128-ofb encryption password:
salt=BF497186168D7D8C
key=E5694B27BAEF12982D20F9594A04A675
iv =16429424F4A00237D7779883AE68739F

C:\Users\USER\Desktop>
```

After encrypting both the files through all the modes:

```
Microsoft Windows [Version 10.0.19043.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER>cd desktop

C:\Users\USER\Desktop>cd csss

C:\Users\USER\Desktop\csss>dir
 Volume in drive C has no label.
 Volume Serial Number is 5C0C-8774

 Directory of C:\Users\USER\Desktop\csss

12-11-2021  19:56    <DIR>          .
12-11-2021  19:56    <DIR>          ..
12-11-2021  19:17                32 big.txt
12-11-2021  19:41                90 cbcBig.txt
12-11-2021  19:46                65 cbcSmall.txt
12-11-2021  19:42                65 cfbBig.txt
12-11-2021  19:46                53 cfbSmall.txt
12-11-2021  19:40                90 ecbBig.txt
12-11-2021  19:45                65 ecbSmall.txt
12-11-2021  19:42                65 ofbBig.txt
12-11-2021  19:46                53 ofbSmall.txt
12-11-2021  19:18                21 small.txt
              10 File(s)            599 bytes
               2 Dir(s)  55,370,166,272 bytes free

C:\Users\USER\Desktop\csss>
```

Small.txt (decryption)

```
Microsoft Windows [Version 10.0.19043.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER>cd desktop

C:\Users\USER\Desktop>cd csss

C:\Users\USER\Desktop\csss>openssl aes-128-ecb -salt -nopad -a -p -d -in ecbSmall.txt -out ecbSmalldec.txt
enter aes-128-ecb decryption password:
salt=34F99C287303AEED
key=6672FD6B02E1A23A5191582CFE0C13AB

C:\Users\USER\Desktop\csss>openssl aes-128-cbc -salt -nopad -a -p -d -in cbcSmall.txt -out cbcSmalldec.txt
enter aes-128-cbc decryption password:
salt=F222E27345815F7B
key=51246FF138FE0CA585DEDD32D1B858FF
iv =55CEC942009B4F3F49A26A7E90B12CCB

C:\Users\USER\Desktop\csss>openssl aes-128-cfb -salt -nopad -a -p -d -in cfbSmall.txt -out cfbSmalldec.txt
enter aes-128-cfb decryption password:
salt=6D783D5C3ECAEC93
key=8B39D6A7EC2D66522F83F9DC77BA4113
iv =590676AC01C47AC2251EC5EB8482CE29

C:\Users\USER\Desktop\csss>openssl aes-128-ofb -salt -nopad -a -p -d -in ofbSmall.txt -out ofbSmalldec.txt
enter aes-128-ofb decryption password:
salt=BF497186168D7D8C
key=E5694B27BAEF12982D20F9594A04A675
iv =16429424F4A00237D7779883AE68739F
```

Big.txt:

```
C:\Users\USER\Desktop\csss>openssl aes-128-ecb -salt -nopad -a -p -d -in ecbBig.txt -out ecbBigdec.txt
enter aes-128-ecb decryption password:
salt=2EA64D61EA6CFC0A
key=891888E604AEA5DE0467B8B1BD42F5BD

C:\Users\USER\Desktop\csss>openssl aes-128-cbc -salt -nopad -a -p -d -in cbcBig.txt -out cbcBigdec.txt
enter aes-128-cbc decryption password:
salt=AA67DFDCCEA44407
key=B6751E0F3F7D027E6A4D7313A78EF74F
iv =B0CB1AFF54CC262F719FC806859E94A4

C:\Users\USER\Desktop\csss>openssl aes-128-cfb -salt -nopad -a -p -d -in cfbBig.txt -out cfbBigdec.txt
enter aes-128-cfb decryption password:
salt=8539157BF5E4C7D6
key=40DB5ADF32BC55BBD82C8A6E70CE41F6
iv =50ADCB4BCEF24F440F7D604E76D85980

C:\Users\USER\Desktop\csss>openssl aes-128-ofb -salt -nopad -a -p -d -in ofbBig.txt -out ofbBigdec.txt
enter aes-128-ofb decryption password:
salt=6F8E201A89046C3E
key=5BDCB0A494B0528AD8E9709303117FA5
iv =9DF17D384C6231EB3A7C77270EA9B292

C:\Users\USER\Desktop\csss>
```

Decrypted file:

```
C:\Users\USER\Desktop\csss>dir
 Volume in drive C has no label.
 Volume Serial Number is 5C0C-8774

 Directory of C:\Users\USER\Desktop\csss

12-11-2021  20:10    <DIR>          .
12-11-2021  20:10    <DIR>          ..
12-11-2021  19:17                32 big.txt
12-11-2021  19:41                90 cbcBig.txt
12-11-2021  20:10                48 cbcBigdec.txt
12-11-2021  19:46                65 cbcSmall.txt
12-11-2021  20:07                32 cbcSmalldec.txt
12-11-2021  19:42                65 cfbBig.txt
12-11-2021  20:10                32 cfbBigdec.txt
12-11-2021  19:46                53 cfbSmall.txt
12-11-2021  20:07                21 cfbSmalldec.txt
12-11-2021  19:40                90 ecbBig.txt
12-11-2021  20:09                48 ecbBigdec.txt
12-11-2021  19:45                65 ecbSmall.txt
12-11-2021  20:06                32 ecbSmalldec.txt
12-11-2021  19:42                65 ofbBig.txt
12-11-2021  20:10                32 ofbBigdec.txt
12-11-2021  19:46                53 ofbSmall.txt
12-11-2021  20:08                21 ofbSmalldec.txt
12-11-2021  19:18                21 small.txt
              18 File(s)            865 bytes
               2 Dir(s)  55,379,976,192 bytes free

C:\Users\USER\Desktop\csss>
```

Observation:

1] The padding is needed for ECB and CBC encryption modes.ECB and CBC are block cipher and for block cipher length of input must be an exact multiple of block length.If this is not the case then padding must be needed to make it so.

2] In OFB and CFB, the padding is not required because they are stream cipher and the ciphertext is always the same length as plain text.

TASK-5:

```
from Crypto.Cipher import AES
from Crypto.util.Padding import pad

plainText = b"This is a top secret."
cipherText = "8d20e56a8d24d0462ce74e4904c1b513e10d1df4a2ef2ad4540faelca0aaf9"
myFile = open ('engwords.txt', 'r')
lines = myFile.readlines()
words = [str.strip(line) for line in lines]
arr = []
for word in words:
   if len(word)<16:
        word=word.lower()
        key=word.encode()+b' '*(16-len(word))
        getCipher=AES.new(key, AES.MODE_CBC , iv=bytes.fromhex('0'*32))
        ciphertext=getCipher.encrypt(pad(plainText, AES.block_size))
        match="no"
   if bytes.hex(ciphertext)==ciphertext:
     match="yes"
```

```
      arr.append(word)
   print(word,match)
print("\n\nThe final key is:" , arr)
```

OUTPUT:

Final key is median.

Conclusion:

I observed that the pycryptodome library is present in python and with the given plain text,cipher text and iv i will be able to find the key by brute force approach.