

## **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)

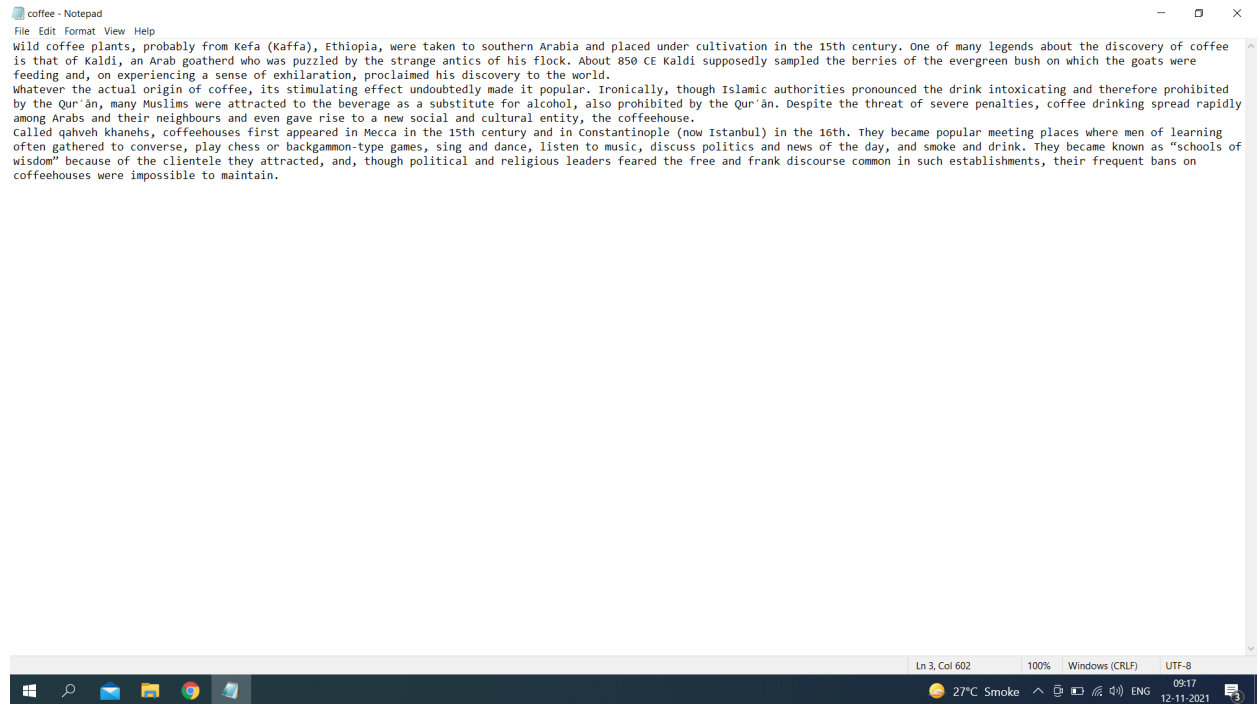
Task 3: Encryption Mode – Corrupted Cipher Text

Task4 : Padding

Task 5: Programming using the Crypto Library

## TASK-1:

### Plain text:



### Using the cipher type -aes

#### 1] Encryption using aes-128-ecb

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

C:\Users\USER>cd desktop

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

C:\Users\USER\Desktop>encrpted.txt
'encrpted.txt' is not recognized as an internal or external command,
operable program or batch file.

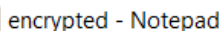
C:\Users\USER\Desktop>encrypted.txt

C:\Users\USER\Desktop>openssl aes-128-ecb -salt -a -d -in encrypted.txt -out plaintext1.txt
enter aes-128-ecb decryption password:

C:\Users\USER\Desktop>plaintext1.txt

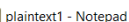
C:\Users\USER\Desktop>
```

After Encryption the text is:



|J2fSdGvKx18BrtJ182odLojcoPlo4e1ESLhk8vvRkcyqoYn/SEwGc8XAbTuy8A  
yZt1ro95HNfS714sYstwwUAP2fiRLD3oM/3D6YFLy6U0lZqK6/C+5KcZiaVKuWQo  
SRzs1AVD/Zzr24ijfYNS9R9KyJhCL7MqCPJgRRD1PdG/zxbnq1q1/aoxFv1i2dKz  
YQMBU7iz30fh+eAOiA9iNacWLiAxhKOJjhZICa6mVBI76t88b20eny8YQf+9u/FI  
P/pLLswJwI/728UqvGPWyBFhc0XRbe9yQCTd9YX3zinTSv5gvzxDcpav/d6Cbxix  
yiz0r4GL65QBAmI+qd9vjyZVBECSVKN+xWg1c7JLIvVlPc/7U+Mm36A1nmoxn1Lv  
+iz9BMovJbTM7wLciwv3iloJyWbtgeMdplA8lZbwARiXUoiqWBimfM+kkz1UySFi  
Voh20zIO97G/dv2ezm8T4zuqNFijZ8dlAylMqcpG75QwPY57QvTuT8DinItc1heO  
ZNCa1+p59jrmS00f90jZpiSE2gQ5ve/ZFq7PYrUhsCzr6yiQiEuizqI1DwWacJ5b  
YxsgoKLS/Look7nVAEMVHwZ9zbE6RBwGwde1wF40KxDGTOXfY9oTcZrQxarpFS/  
PPmiXnlxVwKDZKRfy4chOm/zkTATxUMirKZiee4QxYm/FwD1ReedMIQUUCDpZkk8  
0jj5wqo1KLc5MdJuyh9Gtx/jGviQhIfcH6Qw6ppfnbg7ySft3bUiMi9BjqcEL5nu  
hRTmdXbs/oXaxeHt236qHnqnud4PnEg+vY9LpPwBt65ogCn4G+VSzNjVmL8rqQXJ  
QRFMWA2Vbt68z0reCf9xUIQ0MD9zugKv7exs8wxcS+7qYl12ZXPqfjt9P56ZzXHU  
+ovSuZUYc188rmU9PB9KNs57LSXmkyzUaZYKCJvQS/L4m3deKBbPS8jYu/D+ZQax  
Lx+KZy2zNSWOWS1V45ThbAmVOPEzVFIEAkQqzisduE8zIrb09NSC2sCahn7spZCc  
K5QRUoZc0Gdp6LVpVb73QrXozHV5QTW4evplRiELQbmRsaMrrCQC9ESjeNnmRhiV  
TSwy7U/zqj6PLHtOXuEDF0WGWZ7Y5zzXP6COELq0syjfeHudEdAlP1m+10rpOnTua  
XF9bjsiEXBsXwo8AAuK1xRQ+GknqV0WWBsn3jXeJ2fDoylVJS6PDSygl38eA0FHK  
RSwF1TxV6pBvNyzLuj9DZrmJZWViAmrLUWxqoV+aK9e/yEMWmaSNVdYrx3bBTrcy  
cjFd8/cU0fuA7pjr860aYYqJvllgg300sjy/pg5wfswr10MpLEZ/nA0HwKvCMXzx  
Vb1xgPlmJvVwWCh293TuZvfev1ZPTT5HTORock/Y2UPRegRzPQfcc2bTnkKG9wAA  
z20KdQdv/18a6Ww8vEIOJWzvr0e+2WuRKGDdDYay5nzcSL0HfQU1PSL6EGr/Gce  
YsJxJwte0bVSQbXcjw20bk3Iv9pMaeISBvRL9ZEmO5VGpCMPrgSgk5IdTMpnQ6M0  
kqsdEpVY5sTf7c1EaflD/EeIf6HOu+lyz71hce6JJemqUwsX7aIIVx50DQpTp2+7  
6+3b65i00Yp5Sx0bb3Z/GVZDwJYekQDnAfZNJtz6xKcboB0QD7wrPK9EaxXxPBqC  
Q+TFK5a3qj7J4B+fs2jsLtwWY+GDnJ6fi0bBvoryQT74go5qepsBRKyDgAysww76  
ULZpdVAc106h7Lqa/DM4rx+ZpDNLPetA+EgiYLRoC0u4wEtaBnQ4cXyN+d5vwo9w  
c5vNUD7nLgSbkdvu0zTLZp0vEmCSkhlfCfQDc71BK26M80F0K7Gz/86epPIFg/j3j  
3eSantU8e8yKvYud153u5ilp/cxL70uLwq2Bhd73b6713Y5Yw

After decryption the text is:



Wild coffee plants, probably from Kera (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 Qur'ān, many Muslims were attracted to the beverage as a substitute for alcohol, also prohibited by the Qur'ān. 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.

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

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

C:\Users\USER\Desktop>openssl aes-128-cbc -salt -a -d -in encrypted.txt -out plaintext2.txt
enter aes-128-cbc decryption password:

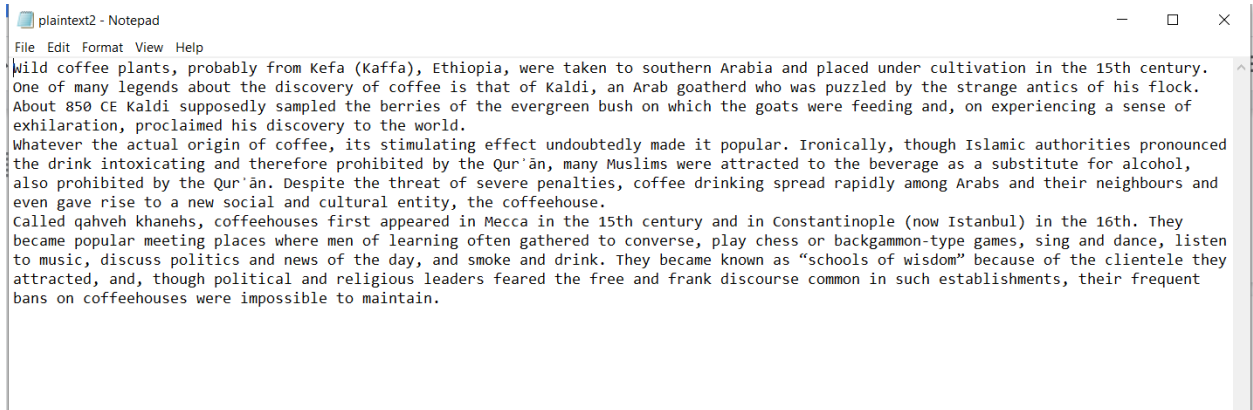
C:\Users\USER\Desktop>plaintext2.txt

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

After encryption the text is:

```
encrypted - Notepad
File Edit Format View Help
J2FsdGVkX18C2cyPF22qUGdZXKI6W5jTDltXtrVtNvr4nVYi04UEq067AjfVwKXd
K0F9K2cjkjKbNRA4m7KA9ZgPwC/0Pkpu0oNnTRMjneqMYt02fh+zu6qkKG9AGwUp
ylfOp7mF083JkbF0C2lJGhEb3BTaw+piLf7X2nL8btw1YRT7UPDQX2s0oEoPD90g
f7XNVi/yXr3KIS0q20jWZDkDbUrFD19+0m7pJx+NTFAYxqKtW/rdtT1Qk2FiF9S1
TcfoyJC54ug2bINTd0eKSA6Bm480iAJ4Q2cTQMUVFJF88gUeXR01AGTMwnbXoH9J
BR2Vl2IPFsLOQUNsb+CvAlYaQ386W/BrB4Wwtip88jenAWEnid8Gj60hBQ7AqT5S
56Wv10mjIKisc5GZLNNWyxfdksJRj6ZwoIOIBfYApkdfIGu/PyfTGd9x8mG7b1/5
qSgNTH00aqlao9b7+6JllustM5+yyppWyDQVsUmHsAs+jODUGRCbrTQAHer7BvAtx
Sou8eEFZBOVLX4Hg1IXG0LC0b1EV0yB0jnl4c6ur6YFfzUmbIARXUNcHPheiyOPK
dHvX6Xc4cVVUxZS1rFb8zfWqlmgQCLTGVAU0Kx/Ct/LfvtgYbBjIvRjZOLLJEL3
pH4hIo3phwzVumqk7m62BxWGFcdGUAXJ85v8Q0aDj9+8igSGLBY8s1ho+KoHn3M
spmiL5hiMyBwQ8ygMeATKgyOsZOX/JfswlyI8akfDgqYNpPGPL48BXPcws36lKYN
5CR67wGZ6MfmcqAvFoNing4dNbsRb0bIV5gIOMrvoWCVEF88upM1z1Ba/IinTF/
4Pd8OFzj0ejbm6PsRepXLKRuwjMzYx7q7gGmbXhEQ48DAjUDwPVVSndjiixWKIv
GX30+hAhsrBT9++CiPPtRANRgPd00uCUgKadcPGZzgt4kqia0yv47dZ78KaUFW8e
iEaiqqjp92krSiesPI1DwZCz5F6HZ5wPmnpro7TVHsjQoQgaSYZMA9N3kBPPQHU
90vYWiN8rSAHxU+SVZo+XQZQC0KQ9gAlHcXhk/09YZZaGIOXQ1oHNRkQJwJBrv1e
Es5HhrPY32fplg1on1bfslyxrsdrTcnshij5QbZZfTCNPqt4PscMHMLW3zDvUh
xAqnGwaXuzt/fa27E/1JhiSueDJE98oM4GTKEzAqxL8m+3sJyhoeEWNWDTF7j1w
Q00KBHoXIRrsn47VSyqYdXULerdh9xsB5RarsH1HgBiNkyPwoewvUPH+f/3Ghwda
QabfHpxRQoiY8UZTKMcLiFEP59v/ShvkTDbi7vjVwPz1v14/XML6tsb7Xj61w095
8QXK0uC07Zg4DM4DcOHuMiFhdFbs4Eg7GBGLuTka5QFXwoNeS5NfIndgg0r2aH/Z
bXKgnj/sxQ04XVnBBwv0tbbxFnhv9ofSQHz2SzaRZWdtvVpGxPC7Eg6C0wyk534a
wdKEBlu9iglmwVZ2HcHKYruinZ8+VsGFY3jYh6WGXl9g8pb/0t186PqIGpMhzGGT
eyXiG+bXm6rj0IaiTMuKiCyhta2J5zaUBtNKJ+tNDN1XxU7qCITCSjAT8x9vfaZn
NW0/1mZU09kG1bQSSrWAZQ+QMnuXOygSS+LlNv10Plz5FFIILqX4KEH4+M7w+Kxn
pQ2+KHcWvohJwHvbmKqWC3h09r/OsfdGK27M+DIv/82e/kkr9w6mTPuCurVAVfF
WUOcgg1BeCRM8wHeHrJhLTsj6/7Ep6+k1wBLowaIbc5ojJTQtXAY9rU94qPND/iv
Hkcp4y5viw6wmEuHex+CpDPBDIdpHPxil05EcSEuPfn9ozJFM+WVXAHEEEggJqm/
CpDPBDIdpHPxil05EcSEuPfn9ozJFM+WVXAHEEEggJqm/
```

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:



encrypted - Notepad

File Edit Format View Help

U2Fs dGVkX1+5ZG8b8GhhDok51j kB1s10JAEuFGhZv1y4XKKTyhAJeoSGVPca+XTw  
TbHdhovF7S6i9zjGnJ1gf4+5VBMB1fbQx0iOEMTJXrvC//iQS96+DT86YnSfEeeH  
d7oVO/01moTPmQwyBfidERNYwVI0jkcDqaUeoux7RNIcdRZc8+0NASjd7bs3on+h  
4cM9LuiqF9VlU89aJ5ZbCWns7u+TzVxN9KId8h3LZA6/yVFaXvZA3+aQa6pCXdSw  
qMlRfayhFcZDajuesZUvmC1982UPLQ0Ex7byTwJRV8Z4mu3hwPOEex1iaJA0TgPo  
4cLqrEuDpC+KqUMKvPesDT2GW9BCbRpbrW+osIhX//lzi5qwy2Qy9VoPeM6oo0Vx  
cxw0pG3vCxm8HmVEDHykqi6uE0kinNsKncVgvyKOWbsif01rWrYeminqlZrWJMyg  
RX0GJaPZIIpmpvq18ZBv2Qot0EvRGysLI3bdWRsbwyK+EwL/tAZXThvFJKyijBi  
zRmtW13zciqGDU4218mOMRL+meSDpy8c2RQ8w5xCaIWOCFTiAHxRN2v1EpeJFnhI  
y8MgR9PpulS6GKg6n52dgcUbQD2fQhFubiAf1RXrhg55ZoEWZ8wcmTlhoPniwFIQ  
CUPms+6ZJQ5uSwYx+Ot82cQCIB6uMxjMXu0xXlREQpN3Vxgg/2Xbwfu0jo9UMIXf  
y5k1BD7jt2a1yLCDFeE8n8w+wcad4fs9eoHT7Mke6Kff73T9Mo30qqn+Bq7q3EF7  
6xFEAAAXbOb12WMFRK9p+Bt9N3U4pqWcGwycZzcmXhp6LLVxCmm9awhUeTEA9B  
AUUSH5LntjORS/2n6PF0BwZQTpmimCEiF89VY9ErrczQFyhghtFr+JczzhkEwPua  
v+zDMqwZ9Dwc4CRx1TYU3sF03FY7WsOd14pRt9mxuE9eZcFCx75Aie+MMsjVa3i1  
1rYI4y2i6kiHxTrIzLRLTd5GFSoEg+o4uWCUw4UPS0sEbkaueVuKcPCoDXeGBdcP  
GeMFhCdS8xRXEbZDiZNCat4tHU+oKASgqSs1Fbu4pIMEm42uyycseGIQiYlKxdpq  
YZz20H8E0F8EXtGm5oPl+bmCH9/OGcIsN0347lyLOC8ZXkjALFy+gzfQUKQJEBwr  
zEKDMBpjcxAZoZxutZT1AMPXLU1AmDe8oGTvNNJvznWIn5mnhZ9SuFmyxt+gQNms  
bWYqo8+dv7wvLyrKciLD3iQvvgHvxF2jik/jln1F5RgYgqCs5FWhXESuu18nxtb  
U70TONajks76J0Lt3RcRh2I6HT6jNl/h0l8bbwkcyRI7cLJURnssSLaAARyGnsg  
+dUSnvioGTS9QVLoUYl85Li1dojQh5eF/k931IBsTN10mape8qSco64K7xAiRPTA  
Bg2eLKdVgPr8/AzOctlY5XZxWMcrmmTynxgtTAKpblb+yKdHPaJ0edOT4DEYqep  
Apk5XcXXfSwgRJSky4yKWdsyudvHhcPGE7IWSBUufVfBgfqvEsvIhzc0IkX6ZxNG  
SC/LA5T+J0bHWcd/TsQozqqRwmeTq07cNsfb/qDNXUUK3W4gjYSbYqNPCj3pLqch  
kDT4jsJcUGIcihhHAKIX3u1xLz87eJGDWiB9Fdhsr/M7ZFXVLZeyt3lDTNNUqJkT  
rA9zNJJZ++5+gFwulop9xXn49M/RU2vN4LLAXx1ZSgtmgDxnEG2i8Dpi6sTb72fPb  
FTjzK01G2ilvhev2Epi1AK1fYz3D70L+qZ6rC7B0pTc0thVqBDZlZGo0BAssa0w  
O6R6ZLcN2ELyAO/NFOhv2U2wcLlKB/ZlhbXqUKSyxJKMBvsRF9k40Eo9juDoti40  
Xmfmv47m474623fChwDAMuVXG8p+5f4XTDvZVU374uG8EP+50w51M/Gm7T

After decryption:



plaintext3 - 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 Qur'an, many Muslims were attracted to the beverage as a substitute for alcohol, also prohibited by the Qur'an. 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.

4] Encryption using aes-192-ecb:







plaintext4 - 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 Qur'an, many Muslims were attracted to the beverage as a substitute for alcohol, also prohibited by the Qur'an. 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.

## 5] Encryption using aes-192-cbc:

Command Prompt

```
C:\Users\USER\Desktop>openssl aes-192-cbc -salt -a -e -in coffee.txt -out encrypted.txt
enter aes-192-cbc encryption password:
Verifying - enter aes-192-cbc encryption password:

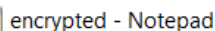
C:\Users\USER\Desktop>encrypted.txt

C:\Users\USER\Desktop>openssl aes-128-cbc -salt -a -d -in encrypted.txt -out plaintext5.txt
enter aes-128-cbc decryption password:
bad decrypt
12420:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:evp_enc.c:529:

C:\Users\USER\Desktop>openssl aes-192-cbc -salt -a -d -in encrypted.txt -out plaintext5.txt
enter aes-192-cbc decryption password:

C:\Users\USER\Desktop>plaintext5.txt
```

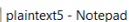
After encryption:



File Edit Format View Help

J2FsdGVkX19N+obayPOor6//SkKDlRSraBvv1HFXvvu7rYB/eYn4AXxcHhngs284  
Elh1MuqPAOEJRTvYqaep5y9z0hXJ1sBCuI9wZknSSKZSyESDdxw98btarU16FmC/  
ikf3ou8IOg3HVEXlEvM55g/uKHBkoznEZUM3R4cwOrd1KQuUb9qQI6BYlLPwBA3  
ObXMHTR+iJ6KNSv+ahJWgTgSyrZSy8dunSpYIZnv5dtzBATNhw/WuIt41bgwESMv  
lEYI5pBstj2rnnmmaV46htLNdq212DfAlLg76kQbOz+UWnrolfwrtATZq2IbODlw  
yYLTYueU41gSZ6hI/kmuiIEN/5Dlu7gBubjgS5TV8TEFZ2BP+yFAZFZBaBvpl0qA  
Eair22nf6wpXvXD6g484xU57TGFEF3qM8A3gLwHoxK8JcNKHKxp1LfUhqHE56DH  
nJ2nqFa6rvxf0wLSjzgg9/2Abr+ElkiYaT2ZDskOrybBJcOmbQJ/Spxoa8L8iW9  
JY/2WukDLYCPJPSLHZ0gGszVSrrSnxQu80mzc0hP17OL4JVCd+Dx4yFhbqBNq8we  
WLS2GN7BDMcQjcgk040Q/re7dNeOUBuU6WIuaZL/G649VPqe6mPvPlTCU04o5UwV  
sJDP0FrubJ5Ka78wP0mK0NQONPoi9lsgb4apjLcfpi00/wtbSn8KtvQy5NN00jYx  
fbmH1PvGX0S07qqTCcbq2qVqN9Uk+xM90CSNPedhs//cLNDGGQzD1JudlmQklWT  
NrGGeKaYw5/ca+8kw08D5fJ3Iw6d1vadZwRllv0nzKMH6jJiztxfy8oJ7BGR0LCq  
nAo5OI8YZN7+OPRimx+EK1+5qT386EPX5WIrHtux3KwvHipJnV30ED/5UkoHQkqU  
TANoAYA52s47cGJmCd/B4icD3aPPB/XwVDArUvJBj6DuaxDUWET5T58bX2dJ5zae  
3+AR56sZla/nrY/GRWFTIH2iKrGNhsSsTQN50nKYfyhwt5rgy6pXZuIXHau01Pm6  
T5J9uwuJoIi0DPvCGEQj+o0RSsvtDWEZ/0VgYBayqBVHCJ6TqBXAHgKldt3cDSu4  
BTGvXBFx/5pBMqJmWzy1Yiv00zU05qeuguAcA1dnqSIM4rvlVUx+fjCrLOnce+X5  
QfpkZMK7GAFz2WHOGfI+wrs1QbbgHebc0gCYrf1vqEexfv9moq7Yk/9YZv0NSxjl  
FcXPmjP7Ibqih69Gurelve9v3fNV+uUUT5YGF4cUNnsJkcNlAlPMB1xQwsZnAZQ  
pQcS4HP3W0BUuDqWvd4USTJVPgVLE0/D7NznEQy0hvW0CLFmT+EmdErL4kLrSiHb  
X92aaS62IjQpWsj7bf79Ag43gDkzMpd07vLNdH88MjSp6o4Iq5zzey4GrhMzA8jl  
QV8U9mhTGLd/2OV22yJ1K6r1Apoytf2+J/YMRO9VtK+Na3fROjb3lW8g0jAzWyt  
l1XpqiQs5KioxviXsFvluedK559/zq7VMP02zLSQ07meBj5JEuPTQ4Qf6xwMl1Rr  
BKtr6EFtrYiSp5zAP3r8gYST6xSD3acUwiHlYVJfLE80Ye5A3gz/2k7Ml70GABSH  
yyNaHfHgVklP5nXfQPrdL0oI41T55gaxWPbeZP2rfKYZLPzB9UYpSrAQj198+XgV  
RaU+kD3NtrHnvSiTf8yNljxW0r1oyScnW3uRk83pgDKFxxzq70IB+kwSC/G+OG+3j  
kyZgza898wRq9v3jYhAUGCFdUsbdMBU/M+731bITABm6XNylGzoVsETTBjrVl7Vh  
ZV7zmfQn9FJ9BgdvUONsB8CX4KjL8MBuXww/4XQkvmgWHPaFLVefQQBB/S5Zd8o2

After decryption:



File Edit Format View Help

Wild coffee plants, probably from kera (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 Qur'ān, many Muslims were attracted to the beverage as a substitute for alcohol, also prohibited by the Qur'ān. 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:

```
Command Prompt
C:\Users\USER\Desktop>openssl aes-192-cfb -salt -a -e -in coffee.txt -out encrypted.txt
enter aes-192-cfb encryption password:
Verifying - enter aes-192-cfb encryption password:

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

C:\Users\USER\Desktop>openssl aes-192-cfb -salt -a -d -in encrypted.txt -out plaintext6.txt
enter aes-192-cfb decryption password:

C:\Users\USER\Desktop>plaintext6.txt
```

After encryption:

```
encrypted - Notepad
File Edit Format View Help
|J2Fs dGVkX1/guOv4YgQMo2mvzA2FFSwsY59a7mqaq6qyJHmXu0upegOt/TDxTH0w
a9ySn7Bw+RnH/vAjE+6dmCmc f0WHAKun5039kfIS3dhf+vfwweyIgUDpwFG5Qa8h
h2caw8WWEJER6IhyikicExo56YU/epGcN+yC+KMu0gzaew4Uq6Y0/apZe4zL3h0D
ToYbxkFwwzwbZHLcxZn++6RhsbmpNrWCMVOuwPxS4R9ZuD5zPc2Btiis0lnx0p7M
DwAoZEhxeVzN+P9aC+I6cqpe1RG3UxFiXw7Mux9YNXFyDrHTnaSgsE8GAETJp/3t
fw5VQ2mRvBKmbyjb240X66XSM5VJyd6h+wI8mc8Cr352o5413lVDkkKFQ94yEx5p
0Nz9hb0f+vjREM69mjYEFiL1Rzs66aokjVC2xQvm4+79TgDloyHbX8fyyCpHXec
fiogzo7Fu4iioXur4uhLElNfksImaJyLcXe+KHZx8ohq/hOL8cgHGj/GRMCzBo3i
YH6/gexPL+mogtq6RZ6KOziyQ2iMlgjpj3SVLZSVaGvXnPHshHx5vQxGaepJ3Gc9
i4h/XiBcyCu0BXW+Y5p/j+/vVVUMOf05xIoGABHLf+HwfH9jLf dK6z2oF4fiMw4Q
+GzJj0NK/Dz8JOPx3hqIchMq/QZXESYP0Ah29lPh8VW1QCrJuw3DOyNCMyL/buQt
vPN1zjtSVxBkIP93KMeaXcpEstGr8Qdlqzhq+YS399qflvFmiWj1K4Kx503YBwgI
GQBxUE9zQIZvTdBQWEWMZ2oDJRKjl v7ixj8szs7BPvnMMtqLPli/2eBI4PUZUGV
IwHatBXLo+a2F1D2Je2SpKoPoCNUz7z01Sj0A8sccrQc5HqxiJza+hxPkYymSlUE
GvVfhF+8WPMdWHwEoaUcCLs6N3qzvsm57EVJCpihZvFA1Gjoi5RCge1W0sa5NRdF
NHIE1nnk3l8MhwePRsnCy5Ejcs1/SCLB1svIlsi7S8uvDVCF8GaozWPwPLwuC+iE
XrFspShwQjXP5/NofZMc4pvUc/Sd8q9Mr+vNg6H+W0ucIRBW03PFhtNH0UxbSBlz
YDkoqgtLcVgLJo+LgcgXmBoa7T2Ai2CycDv+REYM/5kXgyFbHDwzCpYBOVnThVCy
chGwBRG10nJ82xcFVIN/Eaqkvw70eFWE mCGTWEBRz4LNwQXsBfRfZJHcBrx/o8Xd
ZeAc6kLTT0xsS2+HUuLFA1RbascSKy5fp6THA9te4i+JL58PuK0mR7GwmbYAR0vH
hxDQNOSTrM3Cc44OHfyEKuONFTdH1PJMurNDZAqEBshp6bQRrG+vblSzwUK6cC76
j90xxThzcsWQRP0CWJg52xkdiYjhJ2mlwQBqrfhz1GQ15Vu5JQzVi/I0J2F5/7F
pjYPVveq8lLipXDANNXLFBXcvl0u479Ub6vPfTfGeD6KdZf08Sc0FfavqJKiWtg+
DU79DMqUGxpJ0zXZ8+25LRhDcDEZ64NFZmTF8z6xzeDnx/j0I/kXkZPvPUOzRvZR
gUCpxSZ6wALAI5P025Fysy96LBHjQx9FQc2nuX3tN6QvU700uhD07Dc1QSONSQ30
ZeeVynyG+McRQCZFoCftw2t2eV9GdjYUz1BZ6l3+fdH2vyspMn8k6qJH0R7yCD7m
d4fAc3AV1a0AIW09LcOraMP1jxLEYwDoeUcHedi8LpQo3Pz+u9K04Nzx9z01hlo8
UQq3bk1goG00K0iAxAoN9xqZtyAGZdmhnIQFE114hDnhZk6mfCASPLXVW9zRCYA
2z0NyivLVqmEobtg0r1c6v/K9nqz45nQABSVdKB1+80g0vExtCdCJF48UZ0o/dmi
7u6p60+5v48+7+70/++v+G+7u+4h+4u+M+0xhMT0+GAYf88050x+4u+30715
```

After decryption:

```
plaintext6 - 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 Qur'ân, many Muslims were attracted to the beverage as a substitute for alcohol, also prohibited by the Qur'ân. 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.
```

## 7]Encryption using des-ecb:

```
Command Prompt
key=CD05F164142CF122
C:\Users\USER\Desktop>openssl des -salt -a -p -e -in coffee.txt -out encrypted.txt
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
salt=FC7D711908CD6117
key=EADC1626362D0BCA
iv =E47DBB1E165FC0BE
C:\Users\USER\Desktop>encrypted.txt
C:\Users\USER\Desktop>openssl des -salt -a -p -d -in encrypted.txt -out plaintext7.txt
enter des-cbc decryption password:
salt=FC7D711908CD6117
key=EADC1626362D0BCA
iv =E47DBB1E165FC0BE
C:\Users\USER\Desktop>plaintext7.txt
```

After encryption:





encrypted - Notepad

File Edit Format View Help

U2FsdGVkX1/8fXEZCM1hF9ntuweHpZWct6NTRwOybSWkaJXBcLqn48bbGklVwuW3  
q/tqEVEwtgez5K2it3DysyHkWCSrYwXCFTqUPUozINUv4ydbcwAA589EE0HO/zYW  
j8S7HEONXXP/NYgiEuVhSF6zrCowBCv9XtL1BwHwG0H2nNPrO6fmIG0mmqNQLM4H  
/yEl3HbtIL+kcfWF/yz9az4PmuditgF7kFQJmIvdRy8FgKeGHgNyISC4TGCPu32o  
6fSLcr/FYdvSFhojndpAc7D2KJoUqCksOYUvEnSX63XVg+v3jW3T5x7SeI1j5SDj  
PCQ/oJ0J9o0LB7trxiAGMlmYb48xBFiNAYZqqT6q4aMVosxkKgffGbiDx6wlhoR6  
qAyg9oi1nLESLJcd/ibg2AsfqeSEoAlIITi34/nwEpCXH5psqtrAqrypwfycPcuR  
kjldWEcW4hw+5AwffW1Bv9v4DmjP+Sb7My9qr9IbIIPwLeKmRctaZzUNF+fPVhU7  
DJNvNwKz2uoSxXbar4BquiWmsa6JNRUArnfnFkZ2yHnefnYMX3DvEgayXZNhSmh  
G9968aeqghMUSP7nf48YLaqkr+S2TvnJQ2BZ4v5PzeDEeZzGTzGdxVXuM5LGpWgB  
ZoDlYoRilZQyMRuqaqeJsBtZiw9zuBvQGUYusDu3JWkneFCer6ShlH/jXgDiGkzX  
rtCc/9cLs+pWXDqBfaw11vVpteyfNBZVBoArS68oxptOHZ1tfgM7+8kBXhgWTR  
oZOHIKvsfRQePkJSvjaSEgWQTdII4GWYRNCLkGHS70EMl1DpUwh7GAMGtHhs+nUi  
bq2k0xUGaQknGRWbL9avqoi17bFgfTk1NdZsAYmIaEtJTEOk/iwgCqgmqfDlha91  
ao3Z75TBJ5GN70HmxBrE/mcCnrNYMt3AYS1q2N6irfRcCd11nPKsPCq0tRXH0Xfr  
yTv1RopQx/4SD1wu2DVn2zU+CwBaVSgw1mpEboLErj/PaikjhVaoCWZ13U4LS9eC  
WExGdVifvCuF7ldNXC0WlMPou75ss6hutOrf+OzX7KrwjQxz6SC/fXIocg8whcPx  
WkH3wLMq3cgZuEsnIqrjPj9dqd4qPjKoc/XJyQSMRqv7cPByJ727tGJWRB1UOIeF  
y2kekarxrhTdDkLXV3IhhbvjzdnTAFBX/yuuailuXkf4ANSqAuXyO4mGncFgdE+2  
avw70bzVCZ2Fz1vZf5uuPX0J0CbKXqABR5pZSGAyOubblh60ttH+kUy/SUju8bvC  
QhX67V2gVAKBSIMwziiEJrw+fRRa1+U9j7HM3XjQxVrAcPDSgukCCAA5FqG1IXZ  
FIPC+EENrQuMUUJ/NFv9kx4woY/3tg1rXQjPk9Ue0DVtKPLE/R97ctw14qXpTfd3  
Kk5ha+60rbwtrPJlKMxKCMecVv2vmn2pBvqhtQrkopJLEKLAj4JLmX0mhp2AmRpS  
pY3zTm5g24s1yxWJgF61UpBtA6w3vYA10YYRnpPxcc7XS0t88UJf/1Wn8cmDSJxx  
HUXyuyKcPb32zd6LbiHlYkRv+xaqmma00WJNrWsoL2MerfhTHqtZUtXjCq+CqrVe  
ICc3yv1N8k/vgh8MOHNJ9hxyid0+ePhLCQuwros3b3MJbGYyejUDmsnkPv3XNa0H  
ws2FQCuOWAdKp+U5xjhuQRyH6D1Xmpv0N989gVxD3w4aHvedQGq6omdJdCJntg4K  
CTfKIMEYloiJ5bq0XWhF8G09aXNDvNnubn12pZQDLdfDUB7FMSGjGLor9m1Jd3UH  
+Go3We99wh1DgBL9QUgo4VTETl28y2YTLkuMQ6luZzAIdgN9gIFzCrcwo2xbVV94

After decryption:



plaintext7 - 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 Qur'an, many Muslims were attracted to the beverage as a substitute for alcohol, also prohibited by the Qur'an. 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.

8] des-cbc:

```

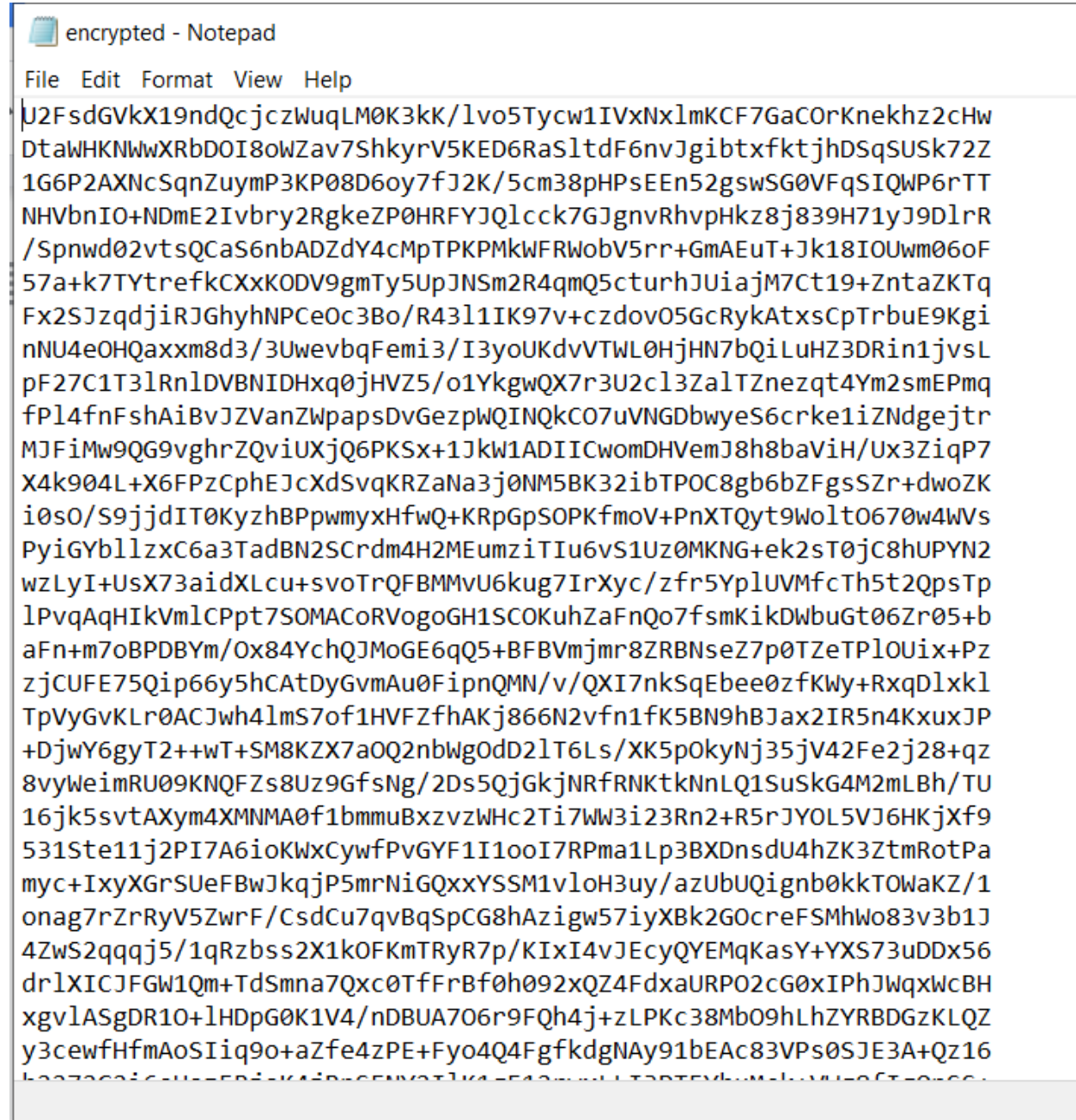
C:\Users\USER\Desktop>openssl des-cbc -salt -a -p -e -in coffee.txt -out encrypted.txt
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
salt=F44A1F3F3714FB7E
key=466AFE4B068B2702
iv =8956DCF4D9D8FD86

C:\Users\USER\Desktop>openssl des-cbc -salt -a -p -d -in encrypted.txt -out plaintext8.txt
enter des-cbc decryption password:
salt=F44A1F3F3714FB7E
key=466AFE4B068B2702
iv =8956DCF4D9D8FD86

C:\Users\USER\Desktop>plaintext8.txt

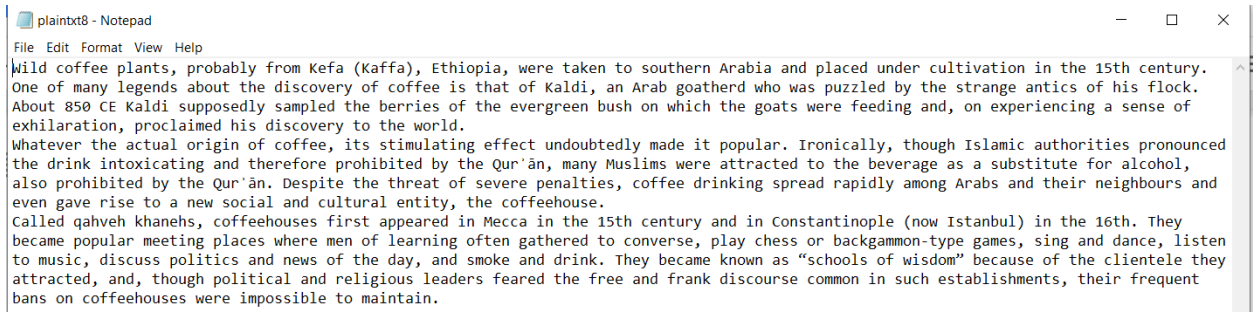
```

After encryption:



The screenshot shows a Notepad window with the title "encrypted - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The main text area contains a single line of encrypted data, which is a long, continuous string of alphanumeric characters. The text is displayed in a monospaced font, typical of code editors or Notepad.

After decryption:



```
plaintext8 - 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 Qur'ân, many Muslims were attracted to the beverage as a substitute for alcohol,
also prohibited by the Qur'ân. 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.
```

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 plaintext9.txt
enter des-cfb decryption password:
salt=0E506C0B16D44E0C
key=7584734E0A03B431
iv =6FBF92D454373B2B

C:\Users\USER\Desktop>plaintext9.txt
```

After encryption:



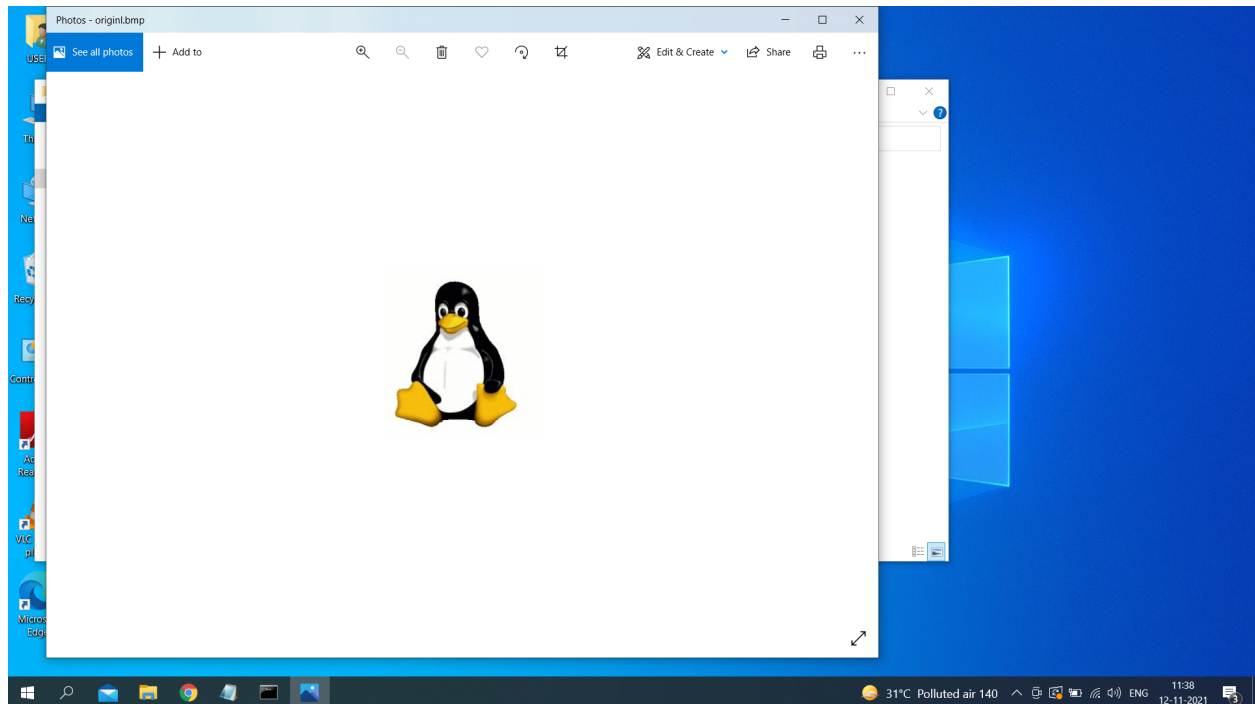


## Conclusion:

- 1] In the AES I observed that the key 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.

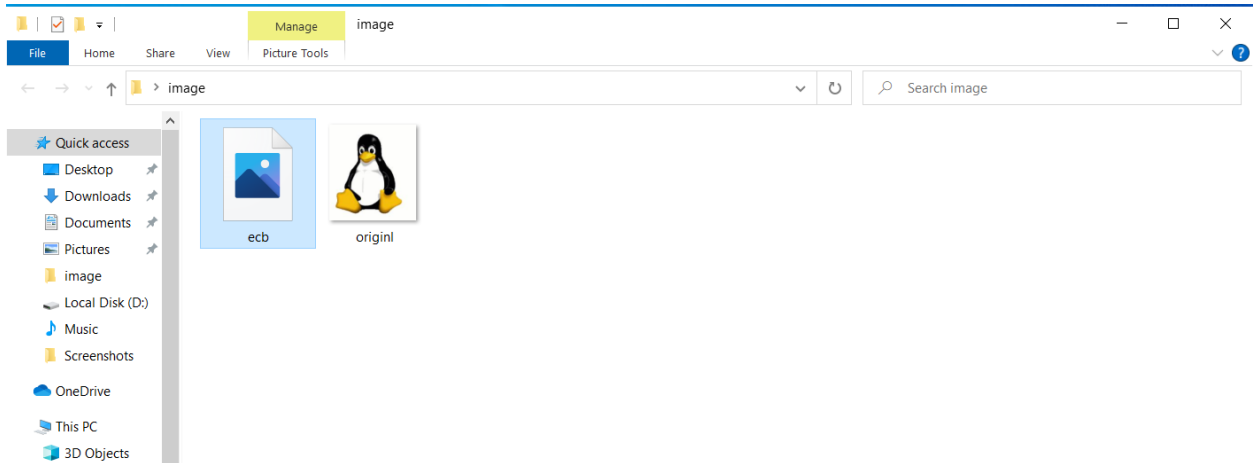
## TASK:2

Original image:

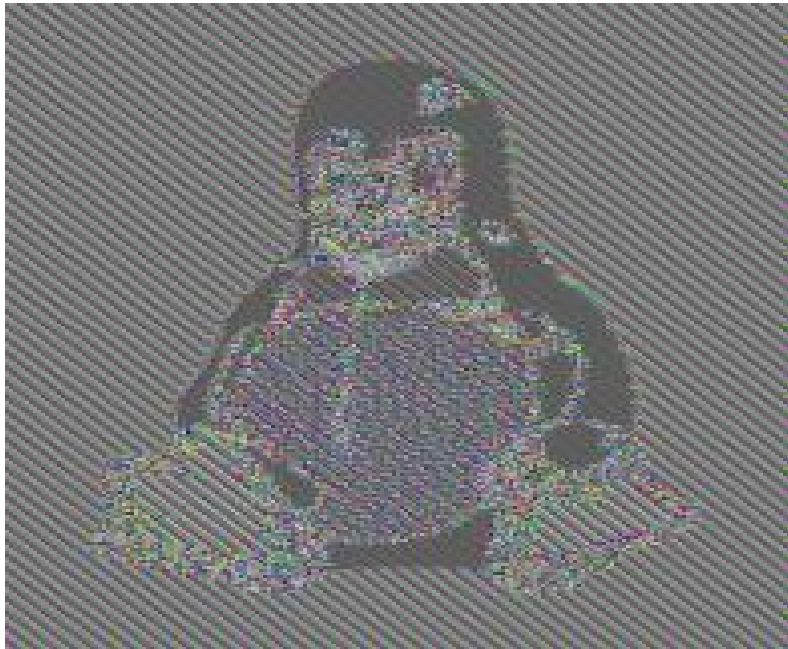


a) Using the cipher type -aes-256-ecb:

```
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>
```



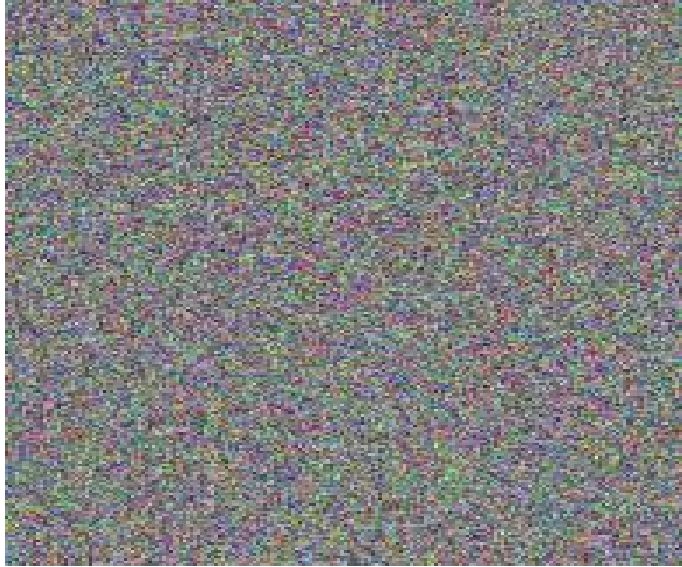
Ecb image:



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=F37A992A5336A71CDBE20475687C1F95F5617D24F1ADBFEAD3733F26572CC5C
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:

```
test - Notepad
File Edit Format View Help
asertyz my friend
This is the csss labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuiop
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou lihr i df
likh i dv, lik i di
```

1] aes-128-ecb:

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

C:\Users\USER>cd desktop

C:\Users\USER\Desktop>openssl aes-128-ecb -salt -a -p -e -in test.txt -out ecb.txt
enter aes-128-ecb encryption password:
Verifying - enter aes-128-ecb encryption password:
salt=ADACB58B416BE93F
key=4F38ED5B91675EB2AD71CA765A1B99FB

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

C:\Users\USER\Desktop>openssl aes-128-ecb -salt -a -p -d -in ecb.txt -out ecdb.txt
enter aes-128-ecb decryption password:
```

## Corrupting 30 byte

Hex Editor Gamma

ecb.txt

0	55	32	46	73	64	47	56	6B	58	31	2B	74	72	4C	57
F	4C	51	57	76	70	50	37	71	72	74	7A	55	42	6F	37
1E	70	77	62	53	69	33	45	4B	33	61	30	75	36	34	34
2D	63	7A	6B	58	41	71	5A	37	62	4A	44	6C	75	51	35
3C	35	63	43	30	0A	5A	69	6E	77	4C	52	2B	51	72	4D
4B	74	45	6D	5A	4D	37	36	37	30	35	5A	64	76	35	4D
5A	32	65	61	50	51	65	4A	53	4F	75	34	50	54	31	47
69	4E	46	75	30	53	56	7A	51	69	65	2B	72	59	55	4F
78	4D	6F	57	71	61	4B	4E	50	63						
87	70	44	34	44	35	39	72	74	4E						
96	68	73	6B	46	5A	6A	6B	54	5A						
A5	78	69	70	66	62	55	67	48	6D						
B4	53	66	57	36	7A	54	4B	65	71						
C3	52	37	43	52	50	6C	61	71	6A						
D2	30	71	57	53	51	73	45	52	76						
E1	52	43	75	57	75	64	64	37	48						
F0	74	50	4F	44	65	45	42	41	4A						
FF	36	47	34	4E	0A	2F	41	36	44						
10E	41	57	47	66	33	45	54	51	66						
11D	39	71	50	35	70	75	32	6F	75						
12C	46	31	62	36	2F	4A	6C	2F	51						
13B	36	57	41	72	51	45	71	61	4E						
14A	54	52	5A	70	4A	41	69	35	37						
159	6C	46	54	64	49	62	5A	5A	4F						
168	52	74	7A	6D	36	37	2B	74	42						
177	72	35	76	41	2B	79	4F	69	53	72	70	49	44	33	0A
186	67	75	49	48	39	74	4A	4B	69	4E	74	61	61	48	50
195	61	32	41	39	52	47	58	32	46	75	4D	59	2B	4C	37
1A4	70	78	75	5A	41	73	32	70	61	4D	64	48	7A	72	67
1B3	57	59	79	31	61	68	6F	61	77	52	68	49	33	30	47
1C2	52	49	6F	4A	0A	69	70	62	52	76	4D	59	78	44	67
1D1	65	4E	4C	53	57	43	34	79	6C	4B	6F	54	7A	75	4A
1E0	61	6E	4A	56	65	4D	49	4F	52	47	4C	33	49	4E	42

Selected Address: 1D (HEX) 29 (DEC)

Change Byte Value

Old Value: 37

New Value

23

00100011

☐ ☐ ☒ ☐ ☐ ☒ ☒

Change Cancel

### Signed Integers

- 1 Byte Integer: 55
- 2 Byte Integer (short): 28727
- 4 Byte Integer (int): 1651994679
- 8 Byte Integer (long): 4986445019284467767

### Unsigned Integers

- 1 Byte Integer: 55
- 2 Byte Integer (ushort): 28727
- 4 Byte Integer (uint): 1651994679
- 8 Byte Integer (ulong): 4986445019284467767

### Floating Point

- Single (float): 1.141108E+21
- Double: 2.34669772284005E+25

### Other

- Binary: 00110111
- UTF-8: 7

☒ Little Endian

☐ Big Endian

Decrypting file:

```
ecba - Notepad
File Edit Format View Help
}IGÇ? }+lÂ?)YE2d
This is the csss labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuio
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou lihr i df
likh i dv, lik i di
```

## 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

Hex Editor Gamma

cbc.txt

Open Save Goto Jump Find Previous Next Edit Stats Settings

0	55	32	46	73	64	47	56	68	58	31	38	36	51	67
E	46	68	5A	42	74	71	4F	35	5A	62	59	78	4C	6E
1C	64	65	42	45	6B	72	66	59	6C	34	59	54	69	31
2A	4C	79	2B	68	49	61	69	4D	79	4F	74	2B	37	78
38	57	4A	6B	43	54	53	5A	74	0A	46	70	4C	57	76
46	46	37	4E	61	69	2B	57	33	6A	51	42	4A	53	2F
54	75	6D	6F	55	69	37	6F	4C	70	64	6D	32	36	74
62	61	52	72	73	54	67	51	69	4F	39	4E	7A	53	6F
70	5A	65	50	73	77	76	68	7A	75					
7E	54	2F	75	0A	6F	42	51	33	2B					
8C	64	4C	49	37	42	2B	79	68	4D					
9A	6C	44	74	76	35	32	48	35	30					
A8	58	61	41	4B	66	39	73	50	65					
B6	31	4F	56	33	56	64	37	33	74					
C4	43	49	55	69	79	37	69	72	2B					
D2	75	64	4D	75	39	2F	72	64	67					
E0	6D	4F	47	52	64	39	69	51	65					
EE	75	45	2F	63	37	6C	6A	76	71					
FC	73	63	70	30	65	48	37	0A	34					
10A	63	38	78	31	31	41	7A	41	30					
118	68	4E	6C	44	46	2F	49	58	66					
126	6C	66	4F	64	46	6B	6B	6D	53					
134	35	59	6A	37	51	42	78	62	79					
142	70	4E	0A	4C	58	6D	4D	62	76					
150	45	52	33	66	71	4B	34	78	33					
15E	67	70	68	2B	6F	77	4A	66	70	6C	2B	38	2F	53
16C	35	4F	49	48	74	67	70	51	39	44	62	6F	71	54
17A	30	59	73	4D	33	57	41	5A	36	6C	48	0A	4B	5A
188	42	66	44	46	64	6C	6A	6C	75	2F	58	31	4D	33
196	36	54	48	4D	5A	32	71	45	69	70	4F	34	52	66
1A4	71	44	71	64	44	69	44	67	61	68	45	78	62	6A
1B2	6A	33	53	63	32	62	32	7A	76	74	61	61	5A	54
1C0	75	6A	39	39	50	4C	0A	50	47	50	76	2B	4D	58
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Selected Address: 1B (HEX) 27 (DEC)

Change Byte Value

Old Value: 6E

New Value

00010111

☐ ☐ ☐ ☒ ☐ ☒ ☒ ☒

Change Cancel

### Signed Integers

1 Byte Integer  
110

2 Byte Integer (short)  
25710

4 Byte Integer (int)  
1113941102

8 Byte Integer (long)  
7382080684424520814

### Unsigned Integers

1 Byte Integer  
110

2 Byte Integer (ushort)  
25710

4 Byte Integer (uint)  
1113941102

8 Byte Integer (ulong)  
7382080684424520814

### Floating Point

Single (float)  
57.34808

Double  
3.13057416565823E+185

### Other

Binary  
01101110

UTF-8  
n

☒ Little Endian

☐ Big Endian

## Decrypt file:

\*cbca - Notepad

File Edit Format View Help

```

a`aE`,,[]oou.[][]j .d
This is the csss labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuio
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king |
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou lihr i df
likh i dv, lik i di

```

## 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

Hex Editor Gamma

cfb.txt

Open Save Goto Jump Find Previous Next Edit Stats Settings

0	55	32	46	73	64	47	56	6B	58	31	2B	31	2B	38
E	49	6E	5A	33	2F	52	54	6F	48	32	75	56	41	45
1C	43	33	33	5A	6F	42	45	74	44	52	69	55	61	51
2A	4F	55	4C	61	52	79	2B	46	77	31	4D	62	32	6E
38	45	46	74	36	2B	41	2F	66	0A	49	50	4D	2F	62
46	41	63	50	49	46	78	38	6E	46	50	73	32	6A	65
54	41	2F	61	31	5A	76	48	58	53	31	4D	79	71	55
62	31	4F	31	55	77	51	47	57	74	74	4B	54	33	39
70	57	57	46	6E	35	68	4F	48	6B					
7E	4B	75	45	0A	70	74	51	6B	43					
8C	74	4C	2F	66	42	4F	30	79	65					
9A	72	6F	32	76	76	42	43	6F	2B					
A8	49	4B	54	37	66	46	6F	66	55					
B6	70	46	5A	78	4E	30	39	37	6D					
C4	4B	45	45	66	37	2B	5A	39	56					
D2	38	70	73	34	64	5A	53	55	30					
E0	46	43	6E	46	62	56	45	47	45					
EE	64	62	53	52	6E	59	34	63	6B					
FC	71	32	43	58	32	4C	45	0A	64					
10A	31	47	2F	4F	4A	58	52	6E	4D					
118	32	32	53	57	64	37	34	42	52					
126	2B	75	68	67	41	70	72	6F	58					
134	49	63	43	4F	69	52	36	59	6A					
142	68	34	0A	34	6C	70	56	48	4E					
150	64	2F	69	61	69	38	76	35	76					
15E	36	4E	6B	42	52	2B	43	32	72	37	31	68	72	35
16C	6C	79	31	65	67	43	56	4B	6E	4B	34	5A	55	51
17A	50	44	55	69	4C	51	56	76	43	55	4F	0A	73	7A
188	61	4D	63	30	50	35	38	47	42	57	79	51	32	4B
196	78	4C	47	53	58	6E	48	30	41	67	58	6D	4F	38
1A4	38	47	67	65	53	73	79	66	64	30	47	30	5A	39
1B2	62	55	5A	6F	37	5A	6C	4E	57	65	34	35	44	32
1C0	39	31	61	32	31	46	0A	77	6F	78	48	2F	61	2F

Selected Address: 1B (HEX) 27 (DEC)

Change Byte Value

Old Value: 45

New Value

78

01111000

☐ ☒ ☒ ☒ ☒ ☐ ☐ ☐

Change Cancel

### Signed Integers

1 Byte Integer  
69

2 Byte Integer (short)  
17221

4 Byte Integer (int)  
858997573

8 Byte Integer (long)  
4990673770276668229

### Unsigned Integers

1 Byte Integer  
69

2 Byte Integer (ushort)  
17221

4 Byte Integer (uint)  
858997573

8 Byte Integer (ulong)  
4990673770276668229

### Floating Point

Single (float)  
4.173787E-08

Double  
4.45730226579899E+25

### Other

Binary  
01000101

UTF-8  
E

☒ Little Endian

☐ Big Endian

Decrypt file:

```
*cfba - Notepad
File Edit Format View Help
asert.z my frienBp[][[f`~,m@ast labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuiop
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou lihr i df
likh i dv, lik i di |
```

#### 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:

Hex Editor Gamma

ofb.txt

Open Save Goto Jump Find Previous Next Edit Stats Settings

0	55	32	46	73	64	47	56	68	58	31	2B	37	66	6A
E	54	6C	5A	4D	30	63	32	71	71	62	34	73	67	76
1C	37	35	30	6A	52	63	68	4E	7A	48	34	56	6F	66
2A	62	54	52	2F	4F	5A	5A	36	68	53	34	41	5A	62
38	4D	2B	63	6E	64	76	65	61	0A	67	6C	37	4E	47
46	37	30	7A	46	71	32	51	56	43	33	64	4F	72	50
54	35	74	6E	38	43	50	68	72	30	61	79	69	77	42
62	50	38	34	66	47	4B	77	59	33	62	47	57	4E	6A
70	53	47	65	41	57	6B	4A	53	50					
7E	41	36	73	0A	2B	50	2F	7A	78					
8C	63	6B	72	4E	77	5A	68	4F	65					
9A	33	78	62	74	35	48	39	62	69					
A8	62	76	6C	79	65	6A	35	64	38					
B6	7A	32	62	44	7A	36	2B	64	49					
C4	65	68	41	4E	42	34	6C	54	35					
D2	65	70	78	75	70	78	75	5A	51					
E0	31	5A	75	58	61	74	71	54	75					
EE	72	6D	56	34	50	54	6B	58	75					
FC	77	2B	75	6C	4B	66	31	0A	59					
10A	69	43	32	66	4A	77	33	67	52					
118	4F	30	47	4E	71	2F	50	70	46					
126	5A	58	58	2F	4B	63	38	50	63					
134	54	39	58	44	6A	31	76	31	66					
142	39	30	0A	64	36	6E	79	34	7A					
150	64	72	39	35	78	4A	2B	37	54					
15E	6B	62	53	73	57	6F	43	51	61	37	57	6C	41	32
16C	47	41	50	65	52	46	75	73	54	45	53	74	57	78
17A	42	51	54	68	41	47	61	7A	31	68	4B	0A	52	38
188	55	2F	6F	53	41	72	4C	35	6A	50	4F	50	2B	33
196	6B	51	76	51	74	45	4B	6B	72	69	41	48	6F	2B
1A4	45	41	49	51	51	6B	77	59	6A	63	76	65	6E	4C
1B2	69	66	38	7A	72	49	7A	4B	39	55	75	75	42	76
1C0	69	36	49	4D	79	0A	31	36	76	76	39	34	72	

Selected Address: 1B (HEX) 27 (DEC)

Change Byte Value

Old Value: 76

New Value

00101001

☐ ☐ ☒ ☐ ☒ ☐ ☐ ☒

Change Cancel

Signed Integers

1 Byte Integer

118

2 Byte Integer (short)

14198

4 Byte Integer (int)

808793974

8 Byte Integer (long)

7521946418667665270

Unsigned Integers

1 Byte Integer

118

2 Byte Integer (ushort)

14198

4 Byte Integer (uint)

808793974

8 Byte Integer (ulong)

7521946418667665270

Floating Point

Single (float)

6.592623E-10

Double

7.05241368325962E+194

Other

Binary

01110110

UTF-8

v

☒ Little Endian

☐ Big Endian

## Decrypt file:

\*ofbd - Notepad

File Edit Format View Help

```

aserayz my friend
This is the csss labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuio
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou lihr i df
likh i dv, lik i di

```

## 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

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-ecb -e -in small.txt -out small_ecb_20.txt -k 00112233445566778899aabbccddeeff

C:\Users\USER\Desktop\csss>openssl enc -aes-128-ecb -e -in large.txt -out large_ecb_32.txt -k 00112233445566778899aabbccddeeff

C:\Users\USER\Desktop\csss>openssl enc -aes-128-cbc -e -in small.txt -out small_cbc_20.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708

C:\Users\USER\Desktop\csss>openssl enc -aes-128-cbc -e -in large.txt -out large_cbc_32.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708

C:\Users\USER\Desktop\csss>openssl enc -aes-128-cfb -e -in small.txt -out small_cfb_20.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708

C:\Users\USER\Desktop\csss>openssl enc -aes-128-cfb -e -in large.txt -out large_cfb_32.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708

C:\Users\USER\Desktop\csss>openssl enc -aes-128-ofb -e -in small.txt -out small_ofb_20.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708

C:\Users\USER\Desktop\csss>openssl enc -aes-128-ofb -e -in large.txt -out large_ofb_32.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708

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

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-ofb -e -in large.txt -out large_ofb_32.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708
```

```
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
```

```
26-11-2021  22:43    <DIR>          .
26-11-2021  22:43    <DIR>          ..
26-11-2021  22:34             32 large.txt
26-11-2021  22:42             64 large_cbc_32.txt
26-11-2021  22:43             48 large_cfb_32.txt
26-11-2021  22:40             64 large_ecb_32.txt
26-11-2021  22:43             48 large_ofb_32.txt
26-11-2021  22:35             20 small.txt
26-11-2021  22:41             48 small_cbc_20.txt
26-11-2021  22:42             36 small_cfb_20.txt
26-11-2021  22:40             48 small_ecb_20.txt
26-11-2021  22:43             36 small_ofb_20.txt
                10 File(s)              444 bytes
                2 Dir(s)  26,146,361,344 bytes free
```

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

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-ecb -d -nopad -in large_ecb_32.txt -out large_ecb_dec.txt -k 00112233445566778899aabbccddeeff
```

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-ecb -d -nopad -in small_ecb_20.txt -out small_ecb_dec.txt -k 00112233445566778899aabbccddeeff
```

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-ecb -d -nopad -in large_cbc_32.txt -out large_cbc_dec.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
```

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-cbc -d -nopad -in large_cbc_32.txt -out large_cbc_dec.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708
```

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-cbc -d -nopad -in small_cbc_20.txt -out small_cbc_dec.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708
```

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-cfb -d -nopad -in large_cfb_32.txt -out large_cfb_dec.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708
```

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-cfb -d -nopad -in small_cfb_20.txt -out small_cfb_dec.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708
```

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-ofb -d -nopad -in large_ofb_32.txt -out large_ofb_dec.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708
```

```
C:\Users\USER\Desktop\csss>openssl enc -aes-128-ofb -d -nopad -in small_ofb_20.txt -out small_ofb_dec.txt -k 00112233445566778899aabbccddeeff -iv 0102030405060708
```

```

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

26-11-2021  22:54  <DIR>          .
26-11-2021  22:54  <DIR>          ..
26-11-2021  22:34             32 large.txt
26-11-2021  22:42             64 large_cbc_32.txt
26-11-2021  22:52             48 large_cbc_dec.txt
26-11-2021  22:43             48 large_cfb_32.txt
26-11-2021  22:53             32 large_cfb_dec.txt
26-11-2021  22:40             64 large_ecb_32.txt
26-11-2021  22:50             48 large_ecb_dec.txt
26-11-2021  22:43             48 large_ofb_32.txt
26-11-2021  22:54             32 large_ofb_dec.txt
26-11-2021  22:35             20 small.txt
26-11-2021  22:41             48 small_cbc_20.txt
26-11-2021  22:53             32 small_cbc_dec.txt
26-11-2021  22:42             36 small_cfb_20.txt
26-11-2021  22:54             20 small_cfb_dec.txt
26-11-2021  22:40             48 small_ecb_20.txt
26-11-2021  22:51             32 small_ecb_dec.txt
26-11-2021  22:43             36 small_ofb_20.txt
26-11-2021  22:54             20 small_ofb_dec.txt
                18 File(s)              708 bytes
                2 Dir(s)  26,144,866,304 bytes free

```

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 ciphers 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:



```
Command Prompt
Zungaria NO
Zuni NO
Zunian NO
Zunyite NO
Zunis NO
Zupanate NO
Zupus NO
Zurbar NO
Zurbarán NO
Zurek NO
Zurheide NO
Zurich NO
Zurkow NO
Zurliite NO
Zurn NO
Zurvan NO
Zisman NO
Zutugil NO
Zuurveldt NO
Zuza NO
Zuzana NO
Zuzu NO
Zwanziger NO
Zwart NO
Zwei NO
Zweig NO
Zwick NO
Zwickau NO
Zwicky NO
Zwieback NO
Zwiebacks NO
Zwibel NO
Zwieselite NO
Zwingle NO
Zwingli NO
Zwinglian NO
Zwinglianise NO
Zwinglianist NO
Zwitter NO
Zwitterion NO
Zwitterionic NO
Zwolle NO
Zworykin NO
ZZ NO
ZZT NO
ZZZ NO

The final key is : ['median']
```

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.



