EXPERIMENT : 3

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

AIM :

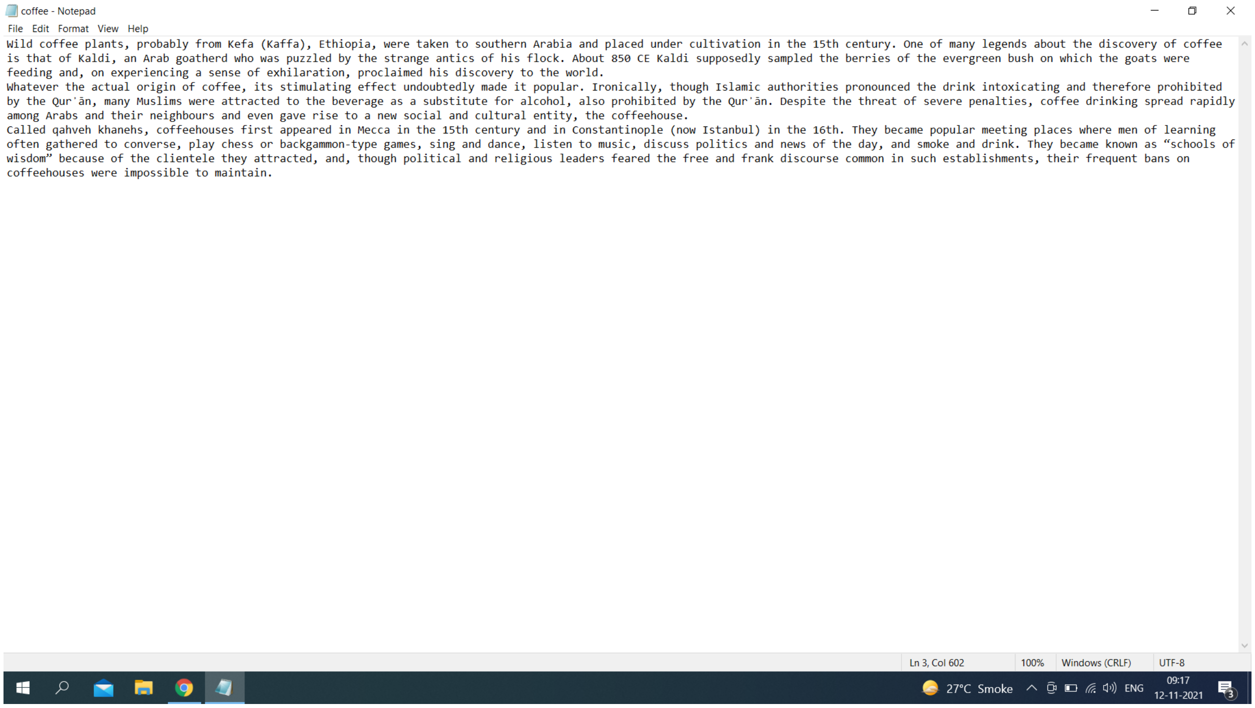
To get familiar with the concepts in secret-key encryption also gain first-hand experience on encryption algorithms, encryption modes, paddings, and initial vector (IV). After this lab should be able to use tools and write programs to encrypt/decrypt messages.

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:



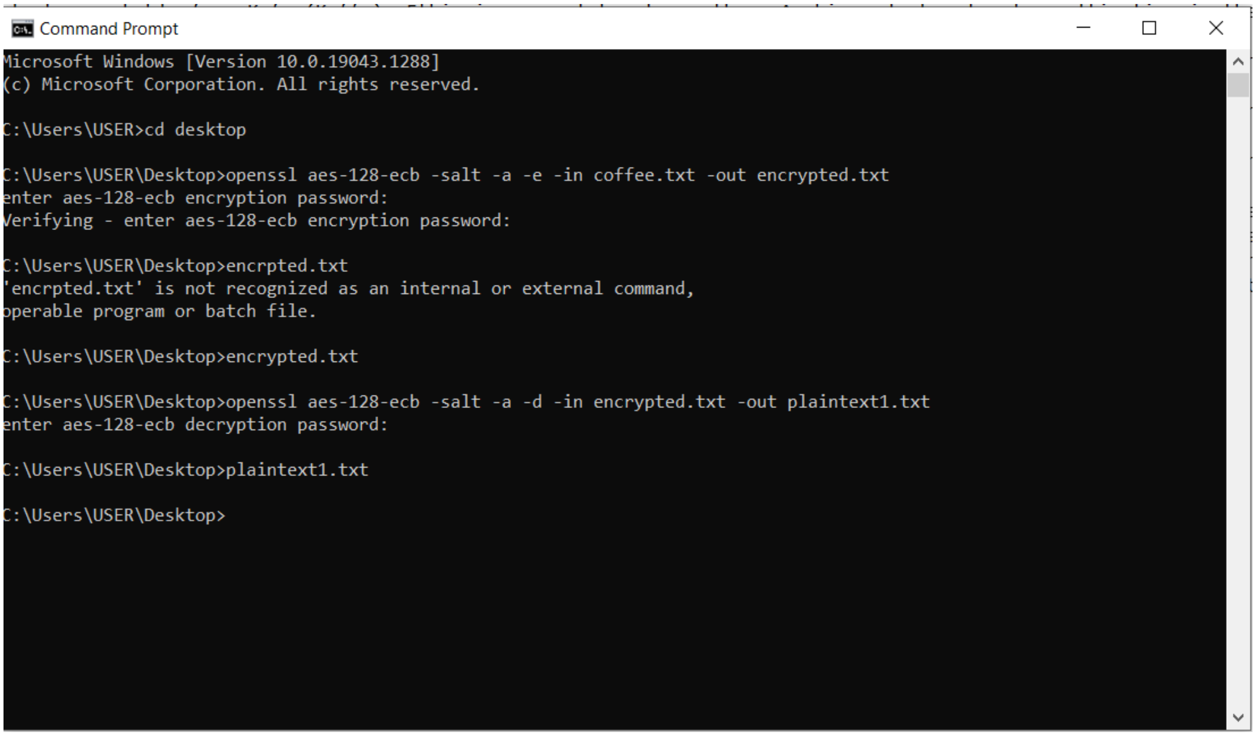
Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century. One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock. About 850 CE Kaldi supposedly 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.

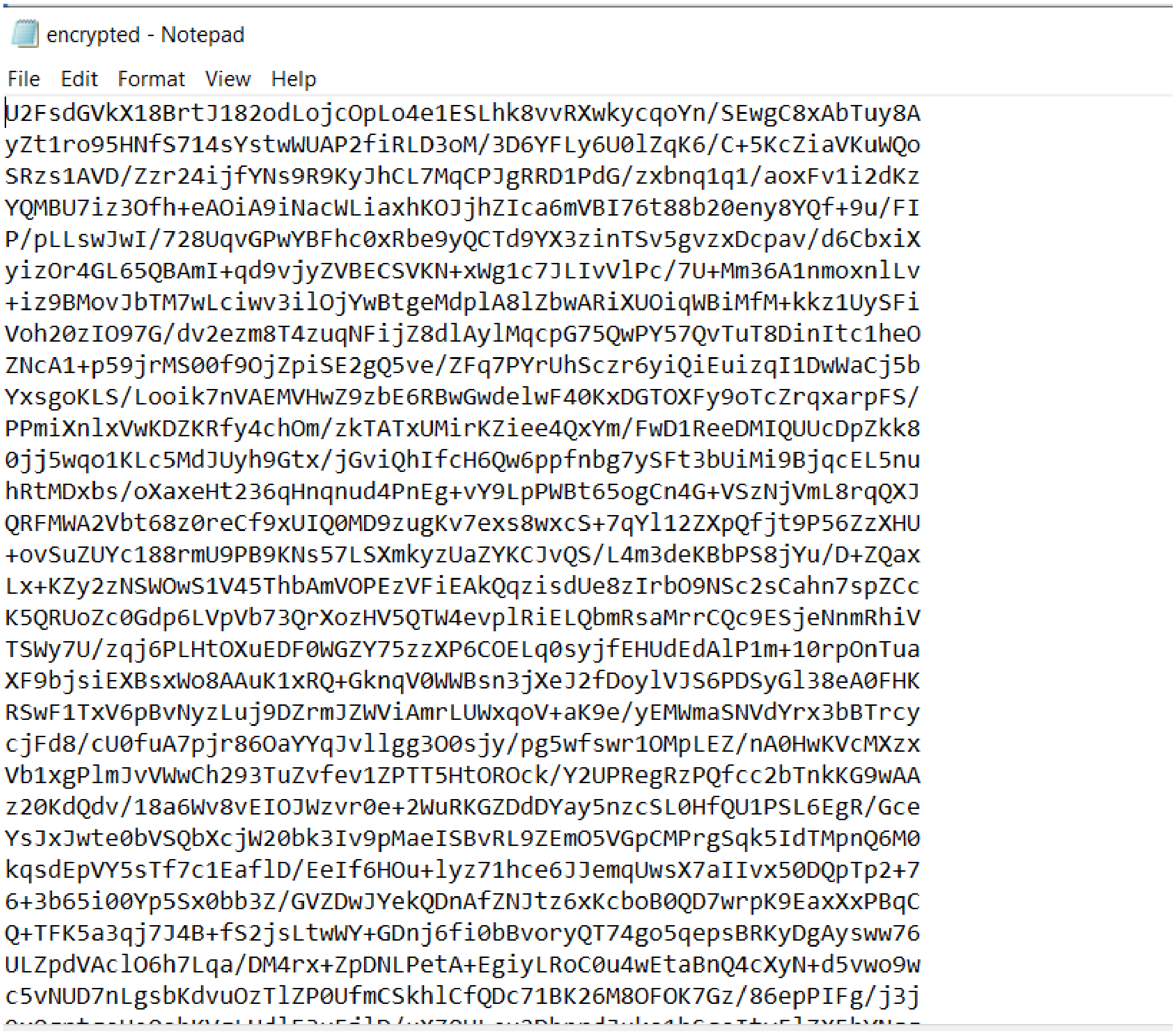
Using the cipher type -aes

1] Encryption using aes-128-ecb



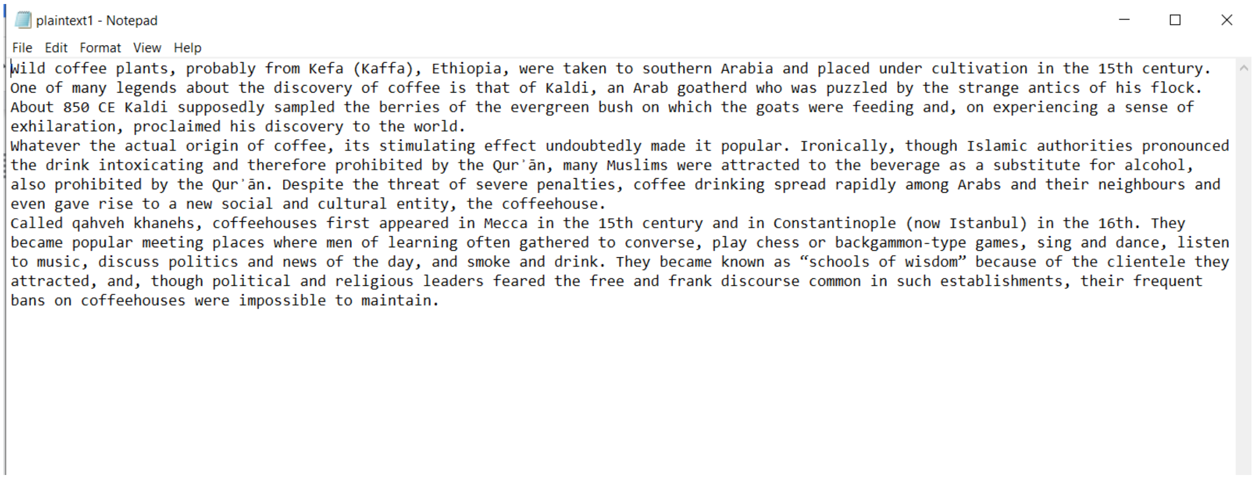
```
Microsoft Windows [Version 10.0.19043.1288]
(c) Microsoft Corporation. All rights reserved.

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:



```
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:

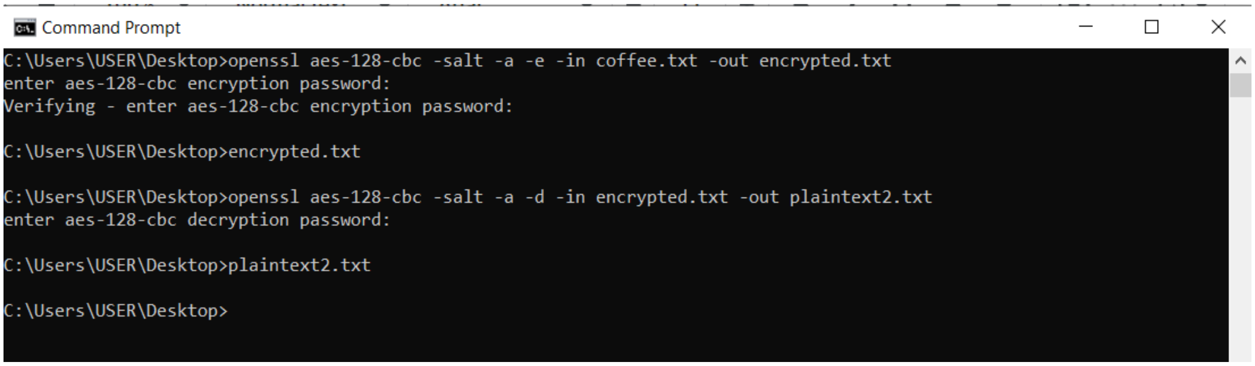


Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century. One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock. About 850 CE Kaldi supposedly 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.

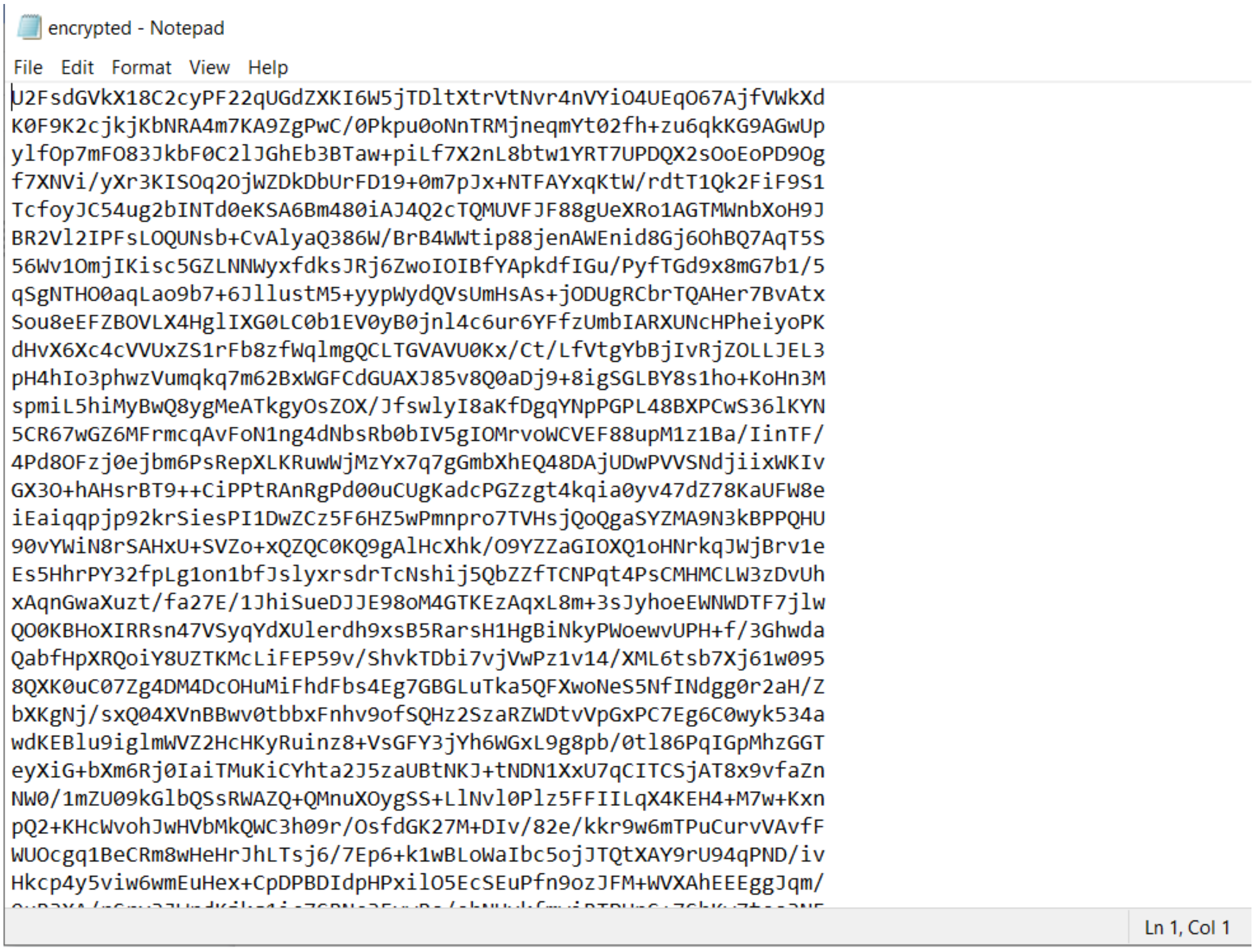
Called qahveh khanehs, coffeehouses first appeared in Mecca in the 15th century and in Constantinople (now Istanbul) in the 16th. They became popular meeting places where men of learning often gathered to converse, play chess or backgammon-type games, sing and dance, listen to music, discuss politics 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



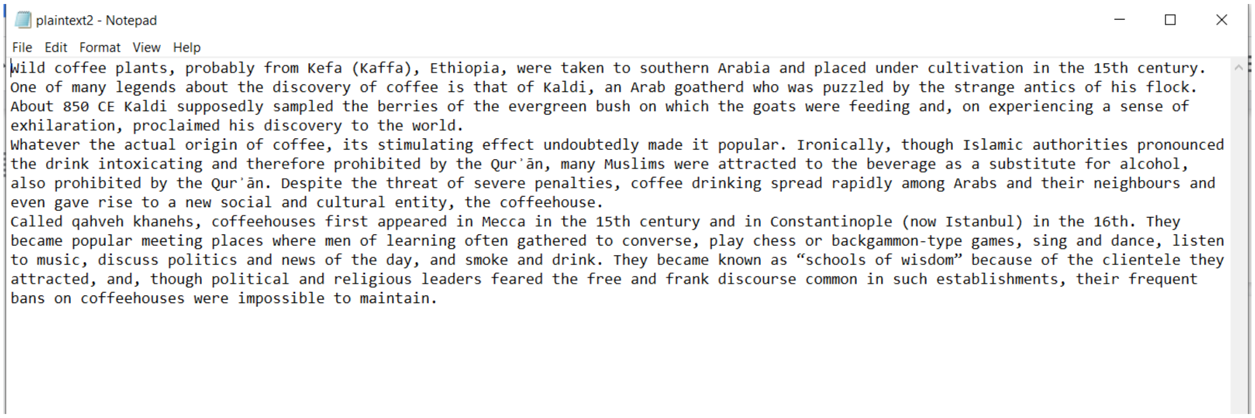
```
C:\Users\USER\Desktop>openssl aes-128-cbc -salt -a -e -in coffee.txt -out encrypted.txt
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:

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:



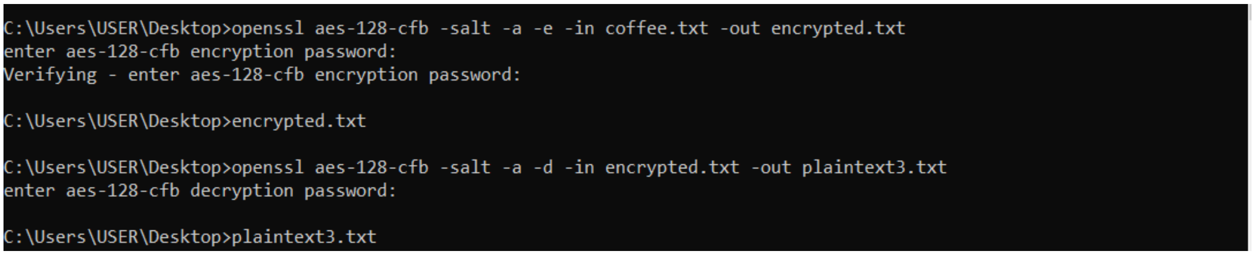
```
U2FsdGVkX18C2cyPF22qUGdZXKI6W5jTDltXtrVtNvr4nVYiO4UEqO67AjfVWkXd
K0F9K2cjkjKbNRA4m7KA9ZgPwC/0Pkpu0oNnTRMjneqmYt02fh+zu6qkKG9AGwUp
ylfOp7mFO83JkbF0C2lJGhEb3BTaw+piLf7X2nL8btw1YRT7UPDQX2sOoEoPD9Og
f7XNVi/yXr3KISOq2OjWZDkDbUrFD19+0m7pJx+NTFAYxqKtW/rdtT1Qk2FiF9S1
TcfoyJC54ug2bINTd0eKSA6Bm480iAJ4Q2cTQMUVFJF88gUeXRo1AGTMWnbXoH9J
BR2Vl2IPFsLOQUNsb+CvAlyaQ386W/BrB4WWtip88jenAWEnid8Gj6OhBQ7AqT5S
56Wv1OmjIKisc5GZLNNWyxfdksJRj6ZwoIOIBfYApkdfIGu/PyfTGd9x8mG7b1/5
qSgNTHO0aqLao9b7+6JllustM5+yypWydQVsUmHsAs+jODUgRCbrTQAHer7BvAtx
Sou8eEFZBOVLX4HglIXG0LC0b1EV0yB0jnl4c6ur6YFfzUmbIARXUNcHPheiyoPK
dHvX6Xc4cVVUxZS1rFb8zfWqlmgQCLTGVAVU0Kx/Ct/LfVtgYbBjIvRjZOLLJEL3
pH4hIo3phwzVumqkq7m62BxWGFCdGUAXJ85v8Q0aDj9+8igSGLBY8s1ho+KoHn3M
spmiL5hiMyBwQ8ygMeATkgyOsZOX/JfswlyI8aKfDgqYNpPGPL48BXPCwS36lKYN
5CR67wGZ6MFrmcqAvFoN1ng4dNbsRb0bIV5gIOMrvoWCVEF88upM1z1Ba/IinTF/
4Pd8OFzj0ejbm6PsRepXLKRuwWjMzYx7q7gGmbXhEQ48DAjUDwPVVSNdjiixWKIv
GX3O+hAHsrBT9++CiPPtRAnRgPd00uCUgKadcPGZzgt4kqia0yv47dZ78KaUFW8e
iEaiqqpjp92krSiesPI1DwZCz5F6HZ5wPmnpro7TVHsjQoQgaSYZMA9N3kBPPQHU
90vYWiN8rSAHxU+SVZo+xQZQC0KQ9gAlHcXhk/O9YZZaGIOXQ1oHNrkqJWjBrv1e
Es5HhrPY32fpLg1on1bfJslyxrsdrTcNshij5QbZZfTCNPqt4PsCMHMCLW3zDvUh
xAqnGwaXuzt/fa27E/1JhiSueDJJE98oM4GTKEzAqxL8m+3sJyhoeEWNWDTF7jlw
QO0KBHoXIRRsn47VSyqYdXUlerdh9xsB5RarsH1HgBiNkyPWoewvUPH+f/3Ghwda
QabfHpXRQoiY8UZTKMcLiFEP59v/ShvkTDbi7vjVwPz1v14/XML6tsb7Xj61w095
8QXK0uC07Zg4DM4DcOHuMiFhdFbs4Eg7GBGLuTka5QFXwoNeS5NfINdgg0r2aH/Z
bXKgNj/sxQ04XVnBBwv0tbbxFnhv9ofSQHz2SzaRZWDtvVpGxPC7Eg6C0wyk534a
wdKEBlu9iglmWVZ2HcHKyRuinz8+VsGFY3jYh6WGxL9g8pb/0tl86PqIGpMhzGGT
eyXiG+bXm6Rj0IaiTMuKiCYhta2J5zaUBtNKJ+tNDN1XxU7qCITCSjAT8x9vfaZn
NW0/1mZU09kGlbQSsRWAZQ+QMnuXOygSS+LlNvl0Plz5FFIILqX4KEH4+M7w+Kxn
pQ2+KHcWvohJwHVbMkQWC3h09r/OsfdGK27M+DIv/82e/kkr9w6mTPuCurvVAvfF
WUOcgq1BeCRm8wHeHrJhLTsj6/7Ep6+k1wBLoWaIbc5ojJTQtXAY9rU94qPND/iv
Hkcp4y5viw6wmEuHex+CpDPBDIdpHPxilO5EcSEuPfn9ozJFM+WVXAhEEEggJqm/
```

After decryption the text is:



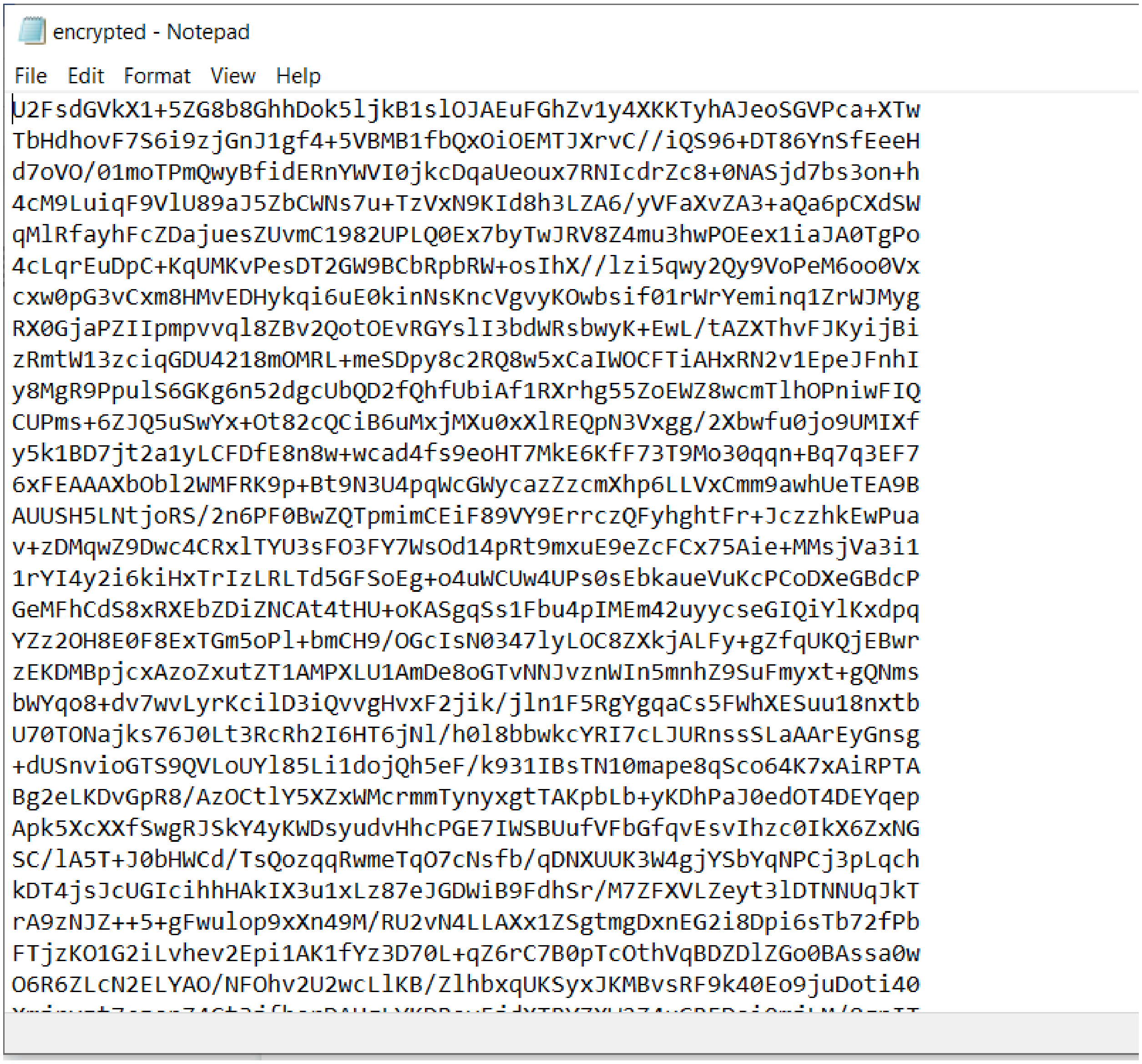
```
Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century.
One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock.
About 850 CE Kaldi supposedly 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.
```

3] Encryption using aes-128-cfb:



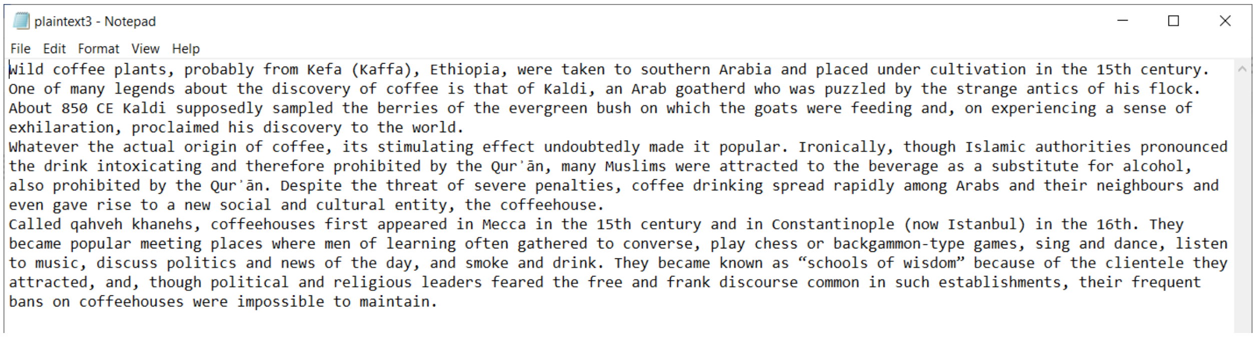
```
C:\Users\USER\Desktop>openssl aes-128-cfb -salt -a -e -in coffee.txt -out encrypted.txt
enter aes-128-cfb encryption password:
Verifying - enter aes-128-cfb encryption password:

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:



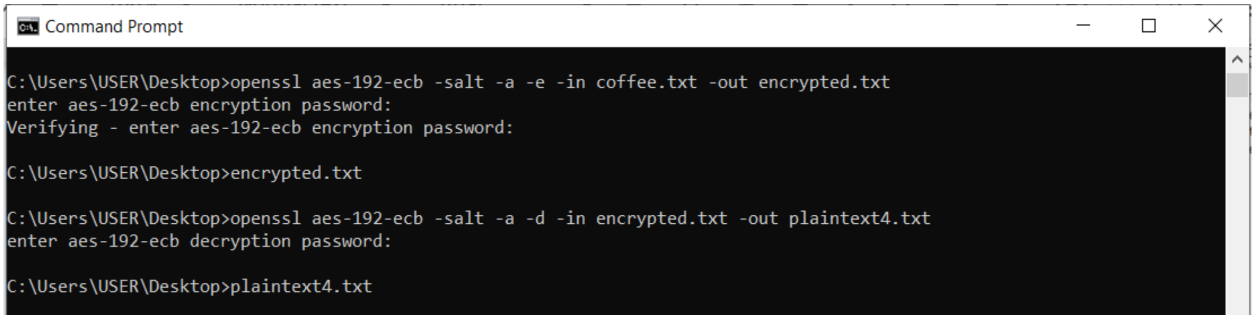
```
U2FsdGVkX1+5ZG8b8GhhDok5ljkB1slOJAEuFGhZv1y4XKKTyhAJeoSGVPca+XTw
TbHdhovF7S6i9zjGnJ1gf4+5VBMB1fbQxOiOEMTJXrvC//iQS96+DT86YnSfEeeH
d7oVO/01moTPmQwyBfidERnYWVI0jkcDqaUeoux7RNIcdrZc8+0NASjd7bs3on+h
4cM9LuiqF9VlU89aJ5ZbCWNs7u+TzVxN9KId8h3LZA6/yVFaXvZA3+aQa6pCXdSW
qMlRfayhFcZDajuesZUvmC1982UPLQ0Ex7byTwJRV8Z4mu3hwPOEex1iaJA0TgPo
4cLqrEuDpC+KqUMKvPesDT2GW9BCbRpbRW+osIhX//lzi5qwy2Qy9VoPeM6oo0Vx
cxw0pG3vCxm8HMvEDHykqi6uE0kinNsKncVgvyKOwbsif01rWrYeminq1ZrWJMyg
RX0GjaPZIIpmpvvql8ZBv2QotOEvRGYslI3bdWRsbwyK+EwL/tAZXThvFJKyijBi
zRmtW13zciqGDU4218mOMRL+meSDpy8c2RQ8w5xCaIWOCFTiAHxRN2v1EpeJFnhI
y8MgR9PpulS6GKg6n52dgcUbQD2fQhfUbiAf1RXrhg55ZoEWZ8wcmTlhOPniwFIQ
CUPms+6ZJQ5uSwYx+Ot82cQCiB6uMxjMXu0xXlREQpN3Vxgg/2Xbwfu0jo9UMIXf
y5k1BD7jt2a1yLCFDfE8n8w+wcad4fs9eoHT7MkE6KfF73T9Mo30qqn+Bq7q3EF7
6xFEAAAXbObl2WMFRK9p+Bt9N3U4pqWcGWycazZzcmXhp6LLVxCmm9awhUeTEA9B
AUUSH5LNtjoRS/2n6PF0BwZQTpmimCEiF89VY9ErrczQFyhghtFr+JczzhkEwPua
v+zDMqwZ9Dwc4CRxlTYU3sFO3FY7WsOd14pRt9mxuE9eZcFCx75Aie+MMsjVa3i1
1rYI4y2i6kiHxTrIzLRLTd5GFSoEg+o4uWCUw4UPs0sEbkaueVuKcPCoDXeGBdcP
GeMFhCdS8xRXEbZDiZNCAt4tHU+oKASgqSs1Fbu4pIMEm42uyycseGIQiYlKxdpq
YZz2OH8E0F8ExTGm5oPl+bmCH9/OGcIsN0347lyLOC8ZXkjALFy+gZfqUKQjEBwr
zEKDMBpjcxAzoZxutZT1AMPXLU1AmDe8oGTvNNJvznWIn5mnhZ9SuFmyxt+gQNms
bWYqo8+dv7wvLyrKcilD3iQvvgHvxF2jik/jln1F5RgYgqaCs5FWhXESuu18nxtb
U70TONajks76J0Lt3RcRh2I6HT6jNl/h0l8bbwkcYRI7cLJURnssSLaAArEyGnsg
+dUSnvioGTS9QVLoUYl85Li1dojQh5eF/k931IBsTN10mape8qSco64K7xAiRPTA
Bg2eLKDvGpR8/AzOCtlY5XZxWMcrmmTynyxgtTAKpbLb+yKDhPaJ0edOT4DEYqep
Apk5XcXXfSwgRJSkY4yKWDsyudvHhcPGE7IWSBUufVFbGfqvEsvIhzc0IkX6ZxNG
SC/lA5T+J0bHWCd/TsQozqqRwmeTqO7cNsfb/qDNXUUK3W4gjYSbYqNPCj3pLqch
kDT4jsJcUGIcihhHAkIX3u1xLz87eJGDWiB9FdhSr/M7ZFXVLZeyt3lDTNNUqJkT
rA9zNJZ++5+gFwulop9xXn49M/RU2vN4LLAXx1ZSgtmgDxnEG2i8Dpi6sTb72fPb
FTjzKO1G2iLvhev2Epi1AK1fYz3D70L+qZ6rC7B0pTcOthVqBDZDlZGo0BAssa0w
O6R6ZLcN2ELYAO/NFOhv2U2wcLlKB/ZlhbxqUKSyxJKMBvsRF9k40Eo9juDoti40
```

After decryption:



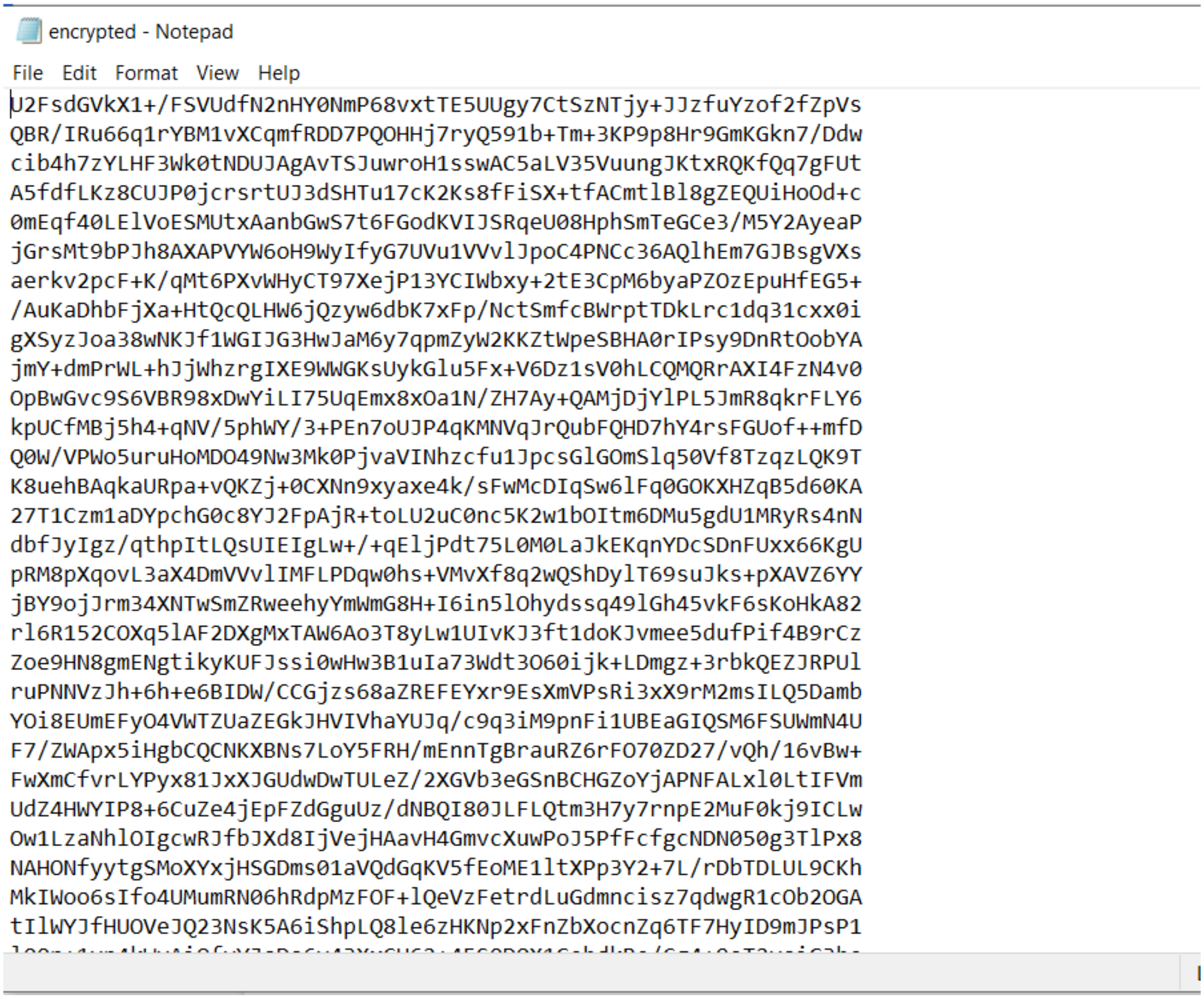
```
Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century.
One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock.
About 850 CE Kaldi supposedly 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.
```

4] Encryption using aes-192-ecb:



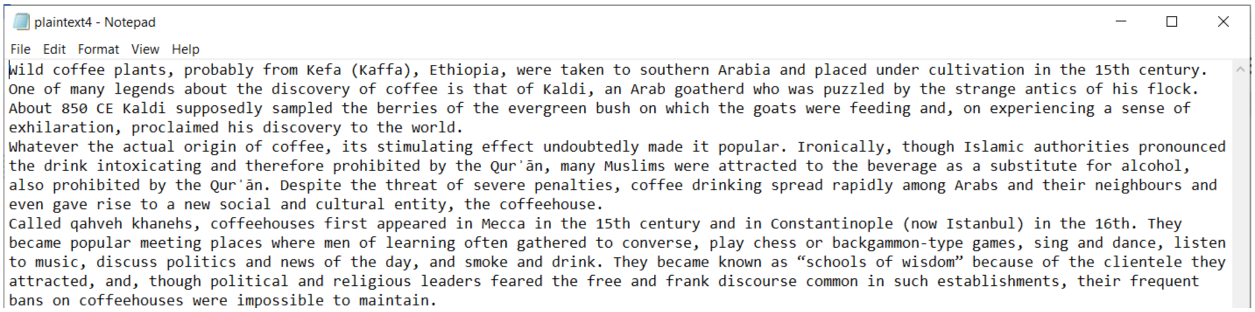
```
C:\Users\USER\Desktop>openssl aes-192-ecb -salt -a -e -in coffee.txt -out encrypted.txt
enter aes-192-ecb encryption password:
Verifying - enter aes-192-ecb encryption password:

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

C:\Users\USER\Desktop>openssl aes-192-ecb -salt -a -d -in encrypted.txt -out plaintext4.txt
enter aes-192-ecb decryption password:

C:\Users\USER\Desktop>plaintext4.txt
```

After encryption:



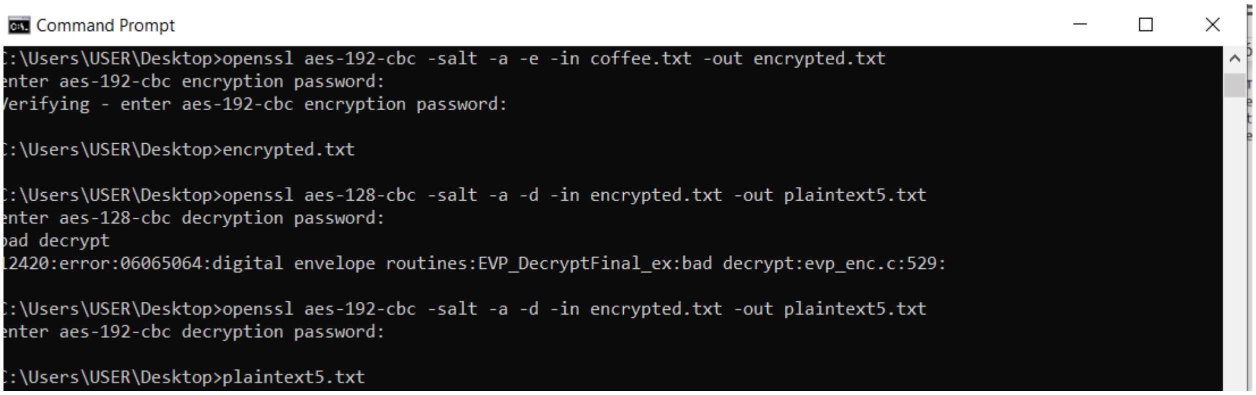
U2FsdGVkX1+/FSVUdfN2nHY0NmP68vxtTE5UUgy7CtSzNTjy+JJzfuYzof2fZpVs
QBR/IRu66q1rYBM1vXCqmfRDD7PQOHHj7ryQ591b+Tm+3KP9p8Hr9GmKGkn7/Ddw
cib4h7zYLHF3Wk0tNDUJAgAvTSJuwroH1sswAC5aLV35VuungJKtxRQKfQq7gFUt
A5fdfLKz8CUJP0jcrsrtUJ3dSHTu17cK2Ks8fFiSX+tfACmtlBl8gZEQUiHoOd+c
0mEqf40LElVoESMUtxAanbGwS7t6FGodKVIJSRqeU08HphSmTeGCe3/M5Y2AyeaP
jGrsMt9bPJh8AXAPVYW6oH9WyIfyG7UVu1VVvlJpoC4PNCc36AQlhEm7GJBsgVXs
aerkv2pcF+K/qMt6PXvWHyCT97XejP13YCIWbxy+2tE3CpM6byaPZOzEpuHfEG5+
/AuKaDhbFjXa+HtQcQLHW6jQzyw6dbK7xFp/NctSmfcBWrptTDkLrc1dq31cxx0i
gXSyzJoa38wNKJf1WGIJG3HwJaM6y7qpmZyW2KKZtWpeSBHA0rIPsy9DnRtOobYA
jmY+dmPrWL+hJjWhzrgIXE9WWGKsUykGlu5Fx+V6Dz1sV0hLCQMQRrAXI4FzN4v0
OpBwGvc9S6VBR98xDwYiLI75UqEmx8xOa1N/ZH7Ay+QAMjDjYlPL5JmR8qkrFLY6
kpUCfMBj5h4+qNV/5phWY/3+PEn7oUJP4qKMNVqJrQubFQHD7hY4rsFGUof++mfD
Q0W/VPWo5uruHoMDO49Nw3Mk0PjvaVINhzcfu1JpcsGlGOmSlq50Vf8TzqzLQK9T
K8uehBAqkaURpa+vQKZj+0CXNn9xyaxe4k/sFwMcDIqSw6lFq0GOKXHZqB5d60KA
27T1Czm1aDYpchG0c8YJ2FpAjR+toLU2uC0nc5K2w1bOItm6DMu5gdU1MRyRs4nN
dbfJyIgz/qthpItLQsUIEIgLw+/+qEljPdt75L0M0LaJkEKqnYDcSDnFUxx66KgU
pRM8pXqovL3aX4DmVVvlIMFLPDqw0hs+VMvXf8q2wQShDylT69suJks+pXAVZ6YY
jBY9ojJrm34XNTwSmZRweehyYmWmG8H+I6in5lOhydssq49lGh45vkF6sKoHkA82
rl6R152COXq5lAF2DXgMxTAW6Ao3T8yLw1UIvKJ3ft1doKJvmee5dufPif4B9rCz
Zoe9HN8gmENgtikyKUFJssi0wHw3B1uIa73Wdt3O60ijk+LDmgz+3rbkQEZJRPUl
ruPNNVzJh+6h+e6BIDW/CCGjzs68aZREFEYxr9EsXmVPsRi3xX9rM2msILQ5Damb
YOi8EUmEFyO4VWTZUaZEGkJHVIVhaYUJq/c9q3iM9pnFi1UBEaGIQSM6FSUWmN4U
F7/ZWApx5iHgbCQCNKXBNs7LoY5FRH/mEnnTgBrauRZ6rFO70ZD27/vQh/16vBw+
FwXmCfvrLYPyx81JxXJGUdwDwTULeZ/2XGVb3eGSnBCHGZoYjAPNFALxl0LtIFVm
UdZ4HWYIP8+6CuZe4jEpFZdGguUz/dNBQI80JLFLQtm3H7y7rnpE2MuF0kj9ICLw
Ow1LzaNhlOIgcwRJfbJXd8IjVejHAavH4GmvcXuwPoJ5PfFcfgcNDN050g3TlPx8
NAHONfyytgSMoXYxjHSGDms01aVQdGqKV5fEoME1ltXPp3Y2+7L/rDbTDLUL9CKh
MkIWoo6sIfo4UMumRN06hRdpMzFOF+lQeVzFetrdLuGdmncisz7qdwgR1cOb2OGA
tIlWYJfHUOVeJQ23NsK5A6iShpLQ8le6zHKNp2xFnZbXocnZq6TF7HyID9mJPsP1

After decryption:



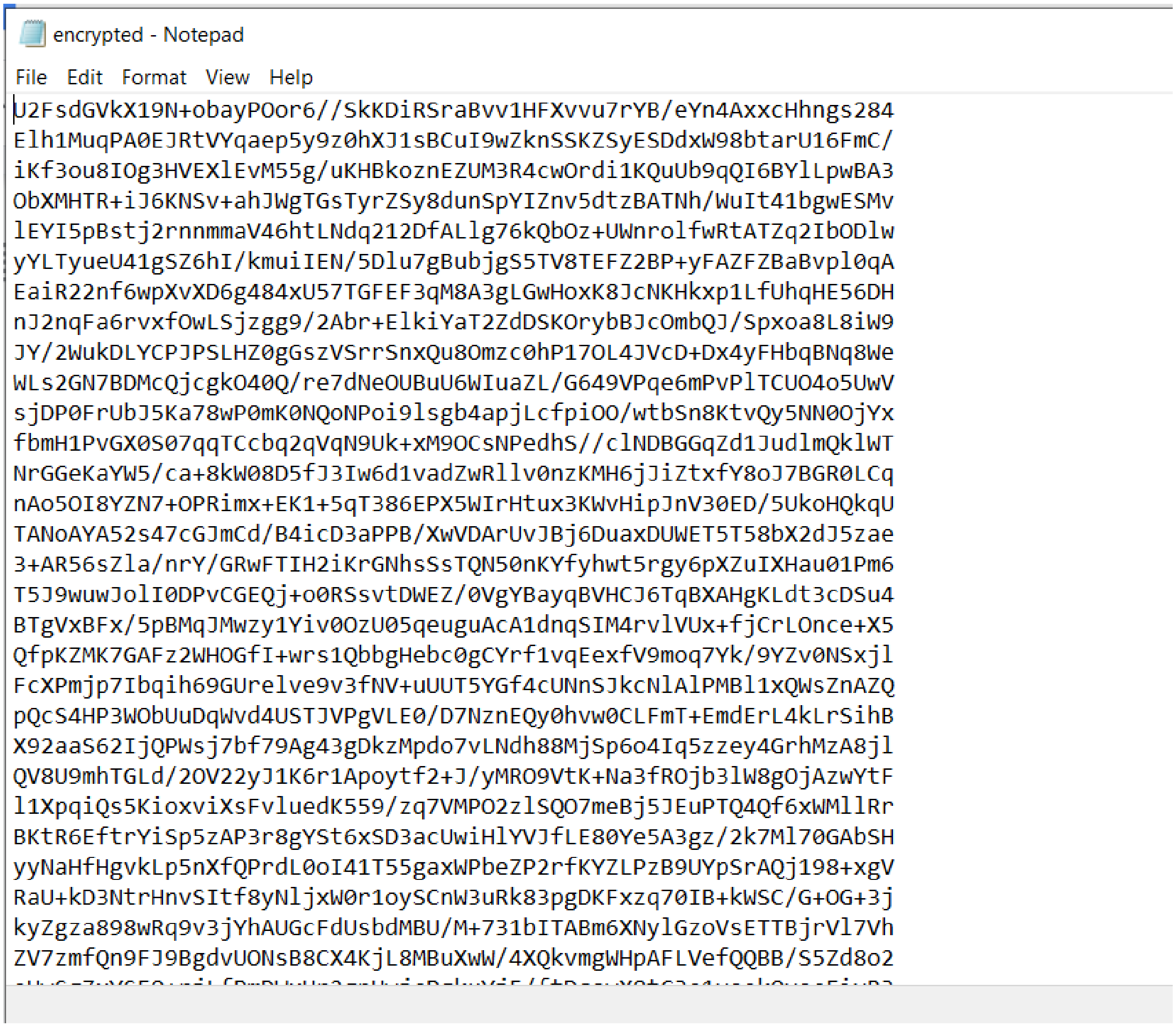
```
Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century.
One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock.
About 850 CE Kaldi supposedly 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'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.
```

5] Encryption using aes-192-cbc:



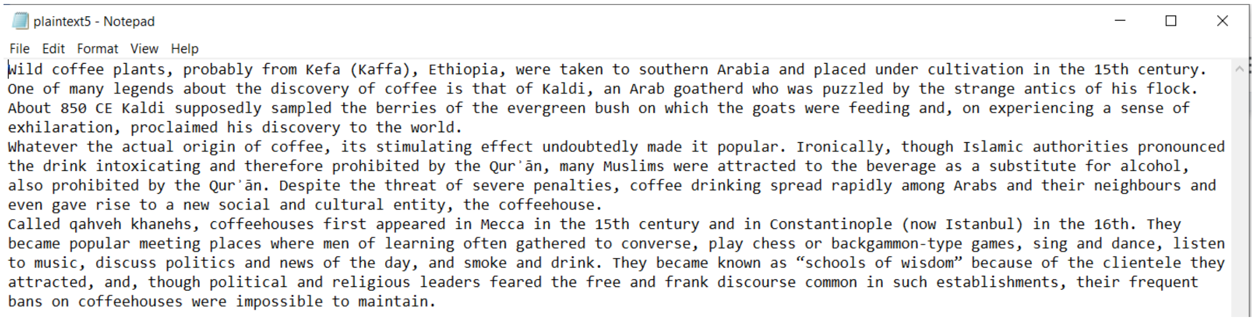
```
:\Users\USER\Desktop>openssl aes-192-cbc -salt -a -e -in coffee.txt -out encrypted.txt
nter aes-192-cbc encryption password:
erifying - enter aes-192-cbc encryption password:

:\Users\USER\Desktop>encrypted.txt

:\Users\USER\Desktop>openssl aes-128-cbc -salt -a -d -in encrypted.txt -out plaintext5.txt
nter aes-128-cbc decryption password:
ad decrypt
2420:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:evp_enc.c:529:

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

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

After encryption:



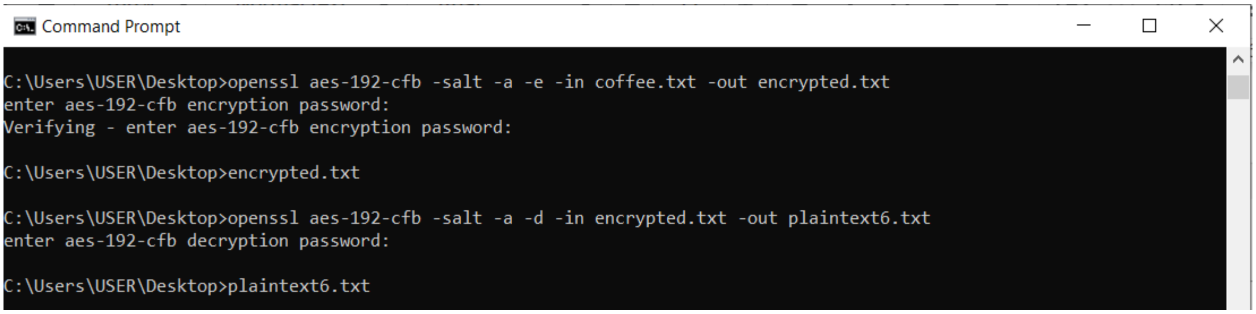
U2FsdGVkX19N+obayPOor6//SkKDiRSraBvv1HFXvvu7rYB/eYn4AxxcHhngs284
Elh1MuqPA0EJRtVYqaep5y9z0hXJ1sBCuI9wZknSSKZSyESDdxW98btarU16FmC/
iKf3ou8IOg3HVEXlEvM55g/uKHBkoznEZUM3R4cwOrdi1KQuUb9qQI6BYlLpwBA3
ObXMHTR+iJ6KNSv+ahJWgTGsTyrZSy8dunSpYIZnv5dtzBATNh/WuIt41bgwESMv
lEYI5pBstj2rnnmmaV46htLNdq212DfALlg76kQbOz+UWnrolfwRtATZq2IbODlw
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:



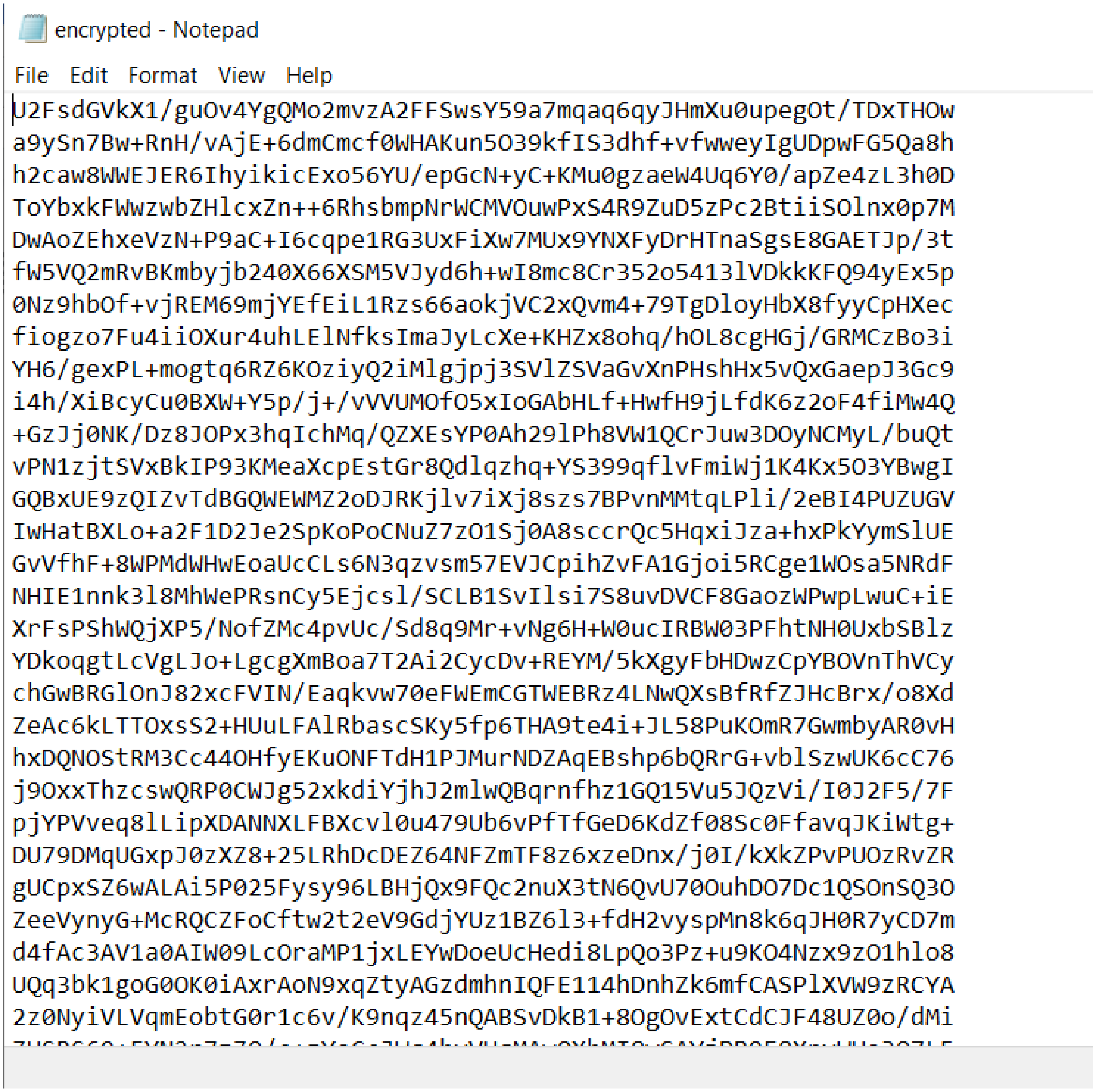
```
Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century.
One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock.
About 850 CE Kaldi supposedly 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:



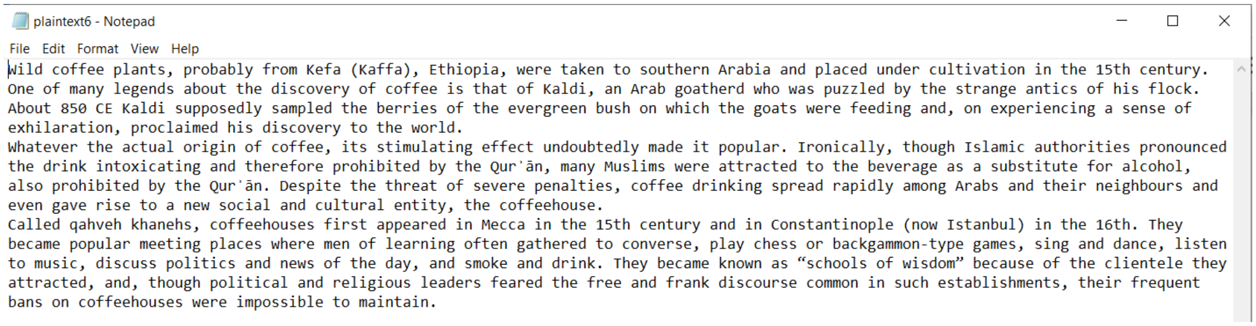
```
C:\Users\USER\Desktop>openssl aes-192-cfb -salt -a -e -in coffee.txt -out encrypted.txt
enter aes-192-cfb encryption password:
Verifying - enter aes-192-cfb encryption password:

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:



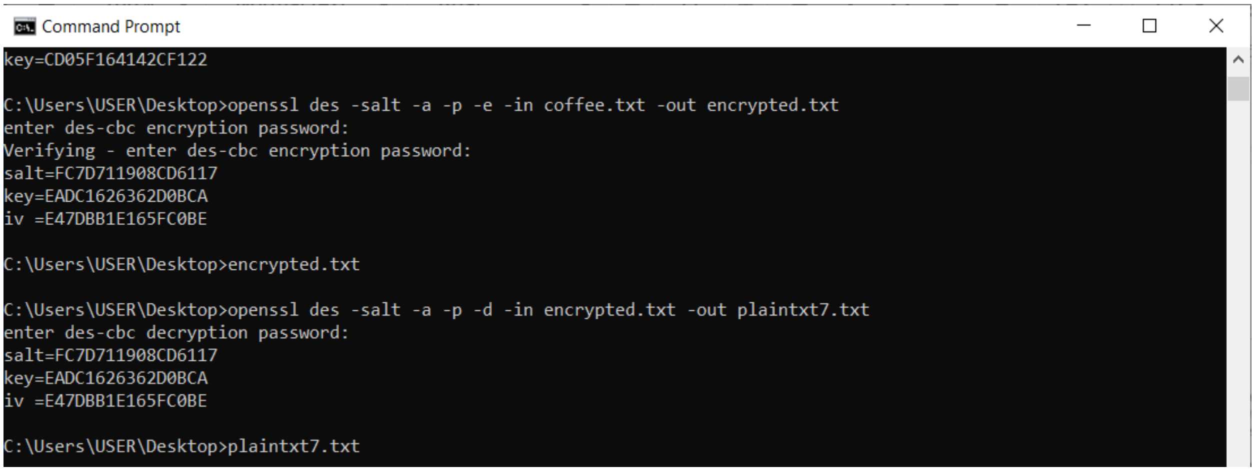
```
U2FsdGVkX1/guOv4YgQMo2mvzA2FFSwsY59a7mqaq6qyJHmXu0upegOt/TDxTHOw
a9ySn7Bw+RnH/vAjE+6dmCmcf0WHAKun5O39kfIS3dhf+vfwweyIgUDpwFG5Qa8h
h2caw8WWEJER6IhyikicExo56YU/epGcN+yC+KMu0gzaeW4Uq6Y0/apZe4zL3h0D
ToYbxkFWwzwbZHlcxZn++6RhsbmpNrWCMVOuwPxS4R9ZuD5zPc2BtiiSOlnx0p7M
DwAoZEhxeVzN+P9aC+I6cqpe1RG3UxFiXw7MUx9YNXFyDrHTnaSgsE8GAETJp/3t
fW5VQ2mRvBKmbyjb240X66XSM5VJyd6h+wI8mc8Cr352o5413lVDkkKFQ94yEx5p
0Nz9hbOf+vjREM69mjYEfEiL1Rzs66aokjVC2xQvm4+79TgDloyHbX8fyyCpHXec
fiogzo7Fu4iiOXur4uhLElNfksImaJyLcXe+KHZx8ohq/hOL8cgHGj/GRMCzBo3i
YH6/gexPL+mogtq6RZ6KOziyQ2iMlgjpj3SVlZSVaGvXnPHshHx5vQxGaepJ3Gc9
i4h/XiBcyCu0BXW+Y5p/j+/vVVUMOfO5xIoGAbHLf+HwfH9jLfdK6z2oF4fiMw4Q
+GzJj0NK/Dz8JOPx3hqIchMq/QZXEsYP0Ah29lPh8VW1QCrJuw3DOyNCMyL/buQt
vPN1zjtSVxBkIP93KMeaXcpEstGr8Qdlqzhq+YS399qflvFmiWj1K4Kx5O3YBwgI
GQBxUE9zQIZvTdBGQWEWMZ2oDJRKjlv7iXj8szs7BPvnMMtqLPli/2eBI4PUZUGV
IwHatBXLo+a2F1D2Je2SpKoPoCNuZ7zO1Sj0A8sccrQc5HqxiJza+hxPkYymSlUE
GvVfhF+8WPMdWHwEoaUcCLs6N3qzvsm57EVJCpihZvFA1Gjoi5RCge1WOsa5NRdF
NHIE1nnk3l8MhWePRsnCy5Ejcsl/SCLB1SvIlsi7S8uvDVCF8GaozWPwpLwuC+iE
XrFsPShWQjXP5/NofZMc4pvUc/Sd8q9Mr+vNg6H+W0ucIRBW03PFhtNH0UxbSBlz
YDkoqgtLcVgLJo+LgcgXmBoa7T2Ai2CycDv+REYM/5kXgyFbHDwzCpYBOVnThVCy
chGwBRGlOnJ82xcFVIN/Eaqkvw70eFWEmCGTWEBRz4LNwQXsBfRfZJHcBrx/o8Xd
ZeAc6kLTTOxsS2+HUuLFAlRbascSKy5fp6THA9te4i+JL58PuKOmR7GwmbyAR0vH
hxDQNOStRM3Cc44OHfyEKuONFTdH1PJMurNDZAqEBshp6bQRrG+vblSzwUK6cC76
j9OxxThzcswQRP0CWJg52xkdiYjhJ2mlwQBqrnfhz1GQ15Vu5JQzVi/I0J2F5/7F
pjYPVveq8lLipXDANNXLFBXcvl0u479Ub6vPfTfGeD6KdZf08Sc0FfavqJKiWtg+
DU79DMqUGxpJ0zXZ8+25LRhDcDEZ64NFZmTF8z6xzeDnx/j0I/kXkZPvPUOzRvZR
gUCpxSZ6wALAi5P025Fysy96LBHjQx9FQc2nuX3tN6QvU70OuhDO7Dc1QSOnSQ3O
ZeeVynyG+McRQCZFoCftw2t2eV9GdjYUz1BZ6l3+fdH2vyspMn8k6qJH0R7yCD7m
d4fAc3AV1a0AIW09LcOraMP1jxLEYwDoeUcHedi8LpQo3Pz+u9KO4Nzx9zO1hlo8
UQq3bk1goG0OK0iAxrAoN9xqZtyAGzdmhnIQFE114hDnhZk6mfCASPlXVW9zRCYA
2z0NyiVLVqmEobtG0r1c6v/K9nqz45nQABSvDkB1+8OgOvExtCdCJF48UZ0o/dMi
```

After decryption:



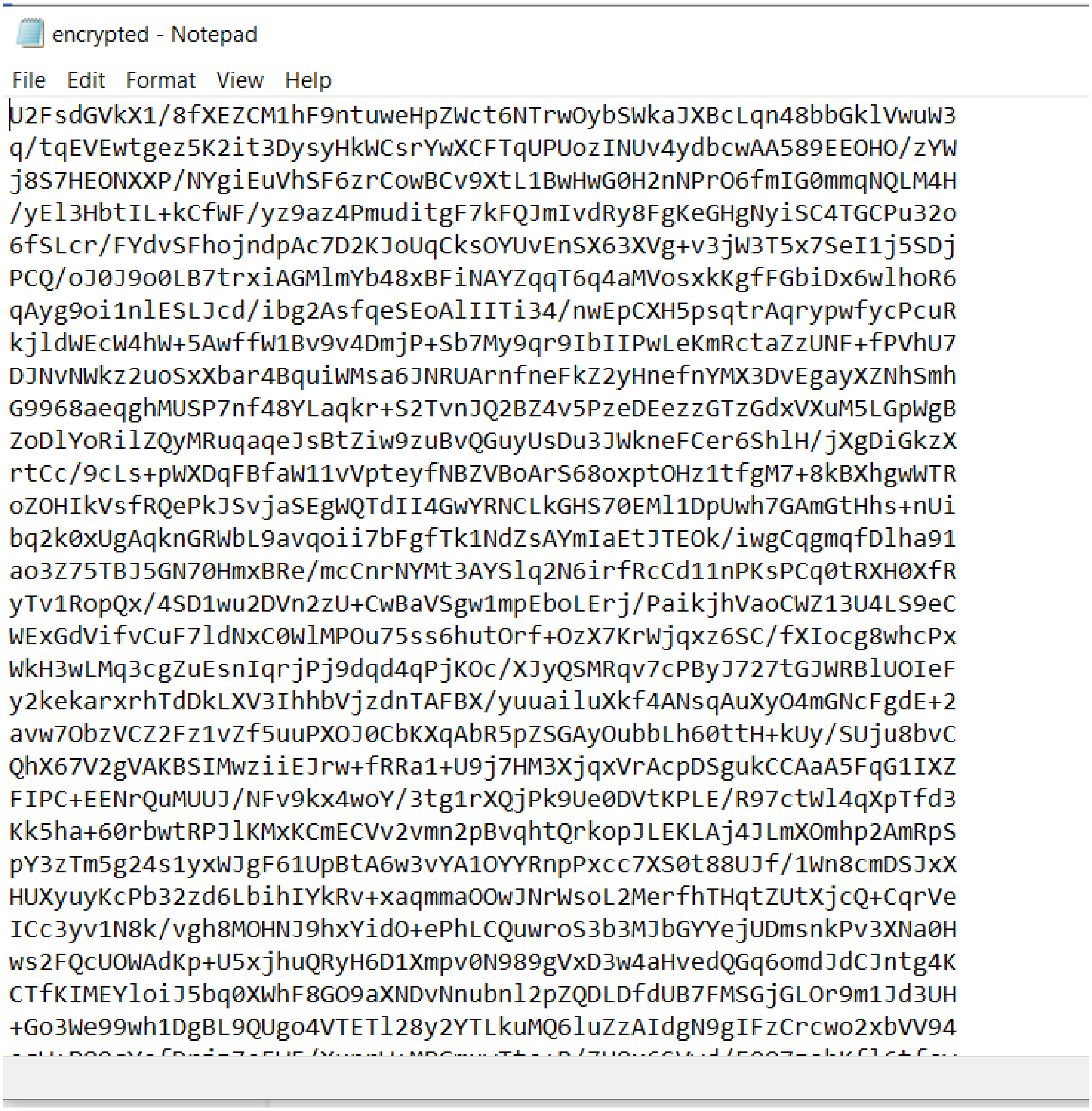
```
Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century.
One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock.
About 850 CE Kaldi supposedly 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.
```

7]Encryption using des-ecb:



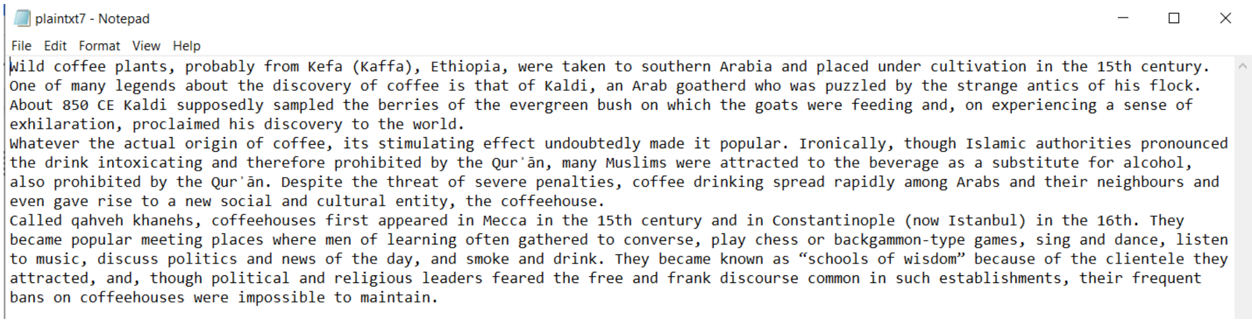
```
key=CD05F164142CF122

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 plaintxt7.txt
enter des-cbc decryption password:
salt=FC7D711908CD6117
key=EADC1626362D0BCA
iv =E47DBB1E165FC0BE

C:\Users\USER\Desktop>plaintxt7.txt
```

After encryption:



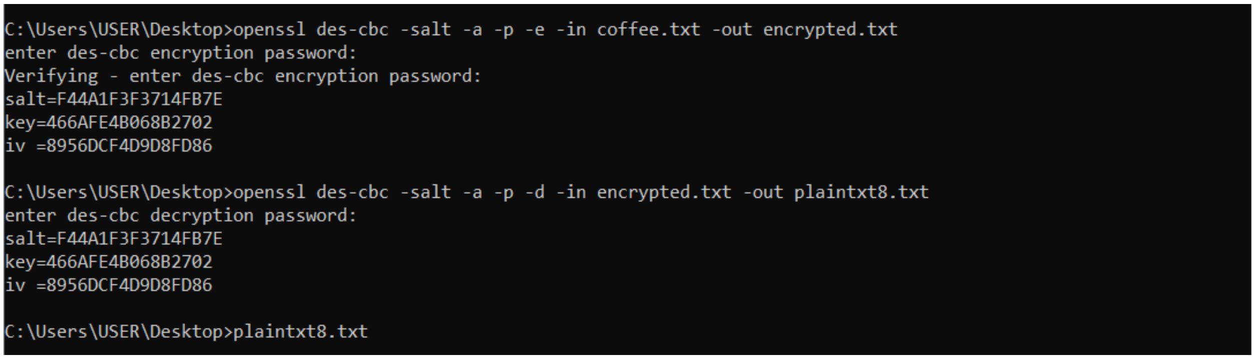
```
U2FsdGVkX1/8fXEZCM1hF9ntuweHpZWct6NTrwOybSWkaJXBcLqn48bbGklVwuW3
q/tqEVEwtgez5K2it3DysyHkWCsrYwXCFTqUPUozINUv4ydbcwAA589EEOHO/zYW
j8S7HEONXXP/NYgiEuVhSF6zrCowBCv9XtL1BwHwG0H2nNPrO6fmIG0mmqNQLM4H
/yEl3HbtIL+kCfWF/yz9az4PmuditgF7kFQJmIvdRy8FgKeGHgNyiSC4TGCPu32o
6fSLcr/FYdvSFhojndpAc7D2KJoUqCksOYUvEnSX63XVg+v3jW3T5x7SeI1j5SDj
PCQ/oJ0J9o0LB7trxiAGMlmYb48xBFiNAYZqqT6q4aMVosxkKgfFGbiDx6wlhoR6
qAyg9oi1nlESLJcd/ibg2AsfqeSEoAlIITi34/nwEpCXH5psqtrAqrypwfycPcuR
kjldWEcW4hW+5AwffW1Bv9v4DmjP+Sb7My9qr9IbIIPwLeKmRctaZzUNF+fPVhU7
DJNvNWkz2uoSxXbar4BquiWMsa6JNRUArnfneFkZ2yHnefnYMX3DvEgayXZNhSmh
G9968aeqghMUSP7nf48YLaqkr+S2TvnJQ2BZ4v5PzeDEezzGTzGdxVXuM5LGpWgB
ZoDlYoRilZQyMRuqaqeJsBtZiw9zuBvQGuyUsDu3JWkneFCer6ShlH/jXgDiGkzX
rtCc/9cLs+pWXDqFBfaW11vVpteyfNBZVBoArS68oxptOHz1tfgM7+8kBXhgwWTR
oZOHIkVsfRQePkJSvjaSEgWQTdII4GwYRNCLkGHS70EMl1DpUwh7GAmGtHhs+nUi
bq2k0xUgAqknGRWbL9avqoii7bFgfTk1NdZsAYmIaEtJTEOk/iwgCqgmqfDlha91
ao3Z75TBJ5GN70HmxBRe/mcCnrNYMt3AYSlq2N6irfRcCd11nPKsPCq0tRXH0XfR
yTv1RopQx/4SD1wu2DVn2zU+CwBaVSgw1mpEboLErj/PaikjhVaoCWZ13U4LS9eC
WExGdVifvCuF7ldNxC0WlMPOu75ss6hutOrf+OzX7KrWjqxz6SC/fXIocg8whcPx
WkH3wLMq3cgZuEsnIqrjPj9dqd4qPjKOc/XJyQSMRqv7cPByJ727tGJWRBlUOIeF
y2kekarxrhTdDkLXV3IhhbVjzdnTAFBX/yuuailuXkf4ANsqAuXyO4mGNcFgdE+2
avw7ObzVCZ2Fz1vZf5uuPXOJ0CbKXqAbR5pZSGAyOubbLh60ttH+kUy/SUju8bvC
QhX67V2gVAKBSIMwziiEJrw+fRRa1+U9j7HM3XjqxVrAcpDSgukCCAaA5FqG1IXZ
FIPC+EENrQuMUUJ/NFv9kx4woY/3tg1rXQjPk9Ue0DVtKPLE/R97ctWl4qXpTfd3
Kk5ha+60rbwtRPJlKMxKCmECVv2vmn2pBvqhtQrkopJLEKLAj4JLmXOmhp2AmRpS
pY3zTm5g24s1yxWJgF61UpBtA6w3vYA1OYYRnpPxcc7XS0t88UJf/1Wn8cmDSJxX
HUXyuyKcPb32zd6LbihIYkRv+xaqmmaOOwJNrWsoL2MerfhTHqtZUtXjcQ+CqrVe
ICc3yv1N8k/vgh8MOHNJ9hxYidO+ePhLCQuwroS3b3MJbGYYejUDmsnkPv3XNa0H
ws2FQcUOWAdKp+U5xjhuQRyH6D1Xmpv0N989gVxD3w4aHvedQGq6omdJdCJntg4K
CTfKIMEYloiJ5bq0XWhF8GO9aXNDvNnubnl2pZQDLDfdUB7FMSGjGLOr9m1Jd3UH
+Go3We99wh1DgBL9QUgo4VTETl28y2YTLkuMQ6luZzAIdgN9gIFzCrcwo2xbVV94
```

After decryption:



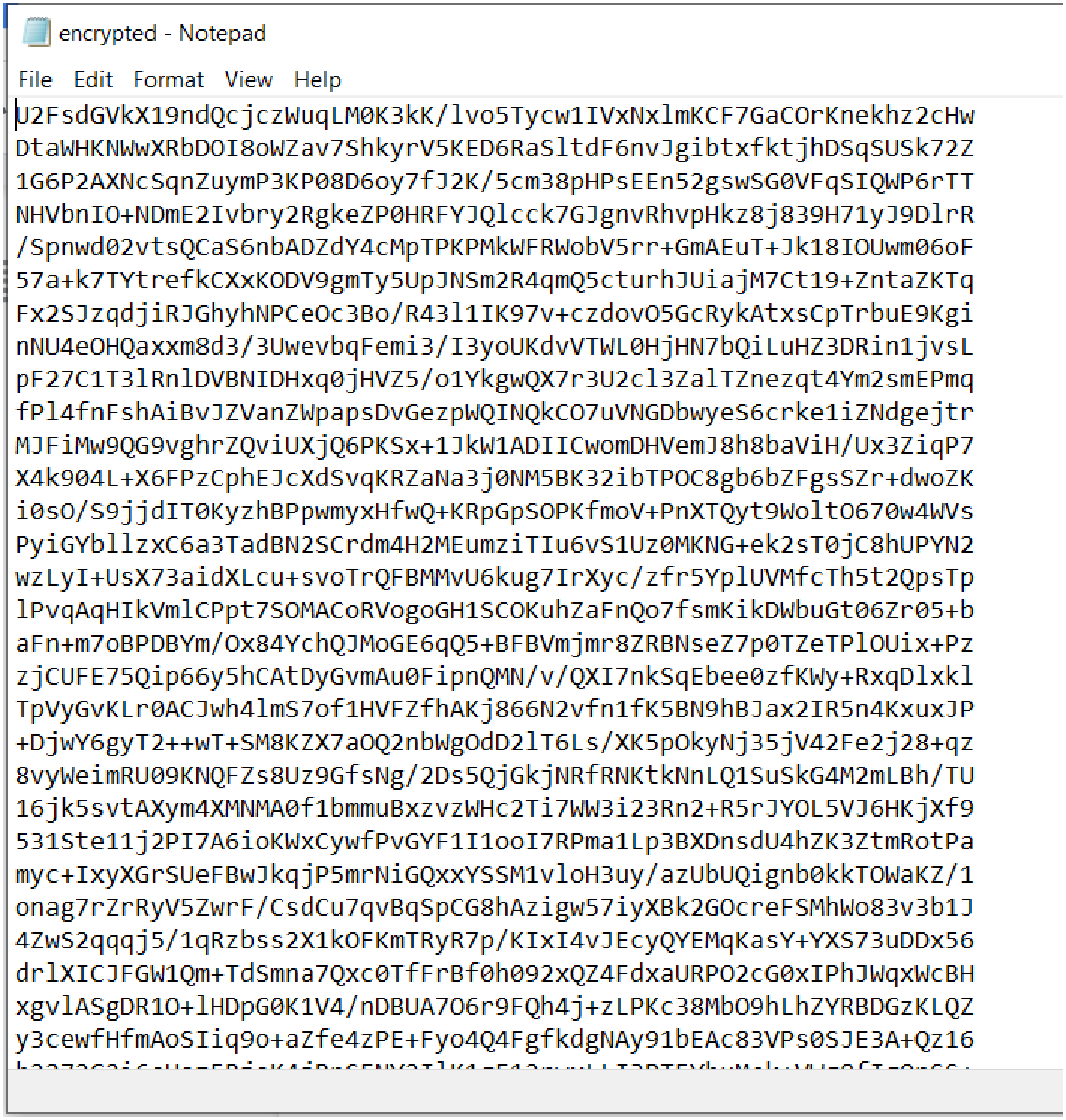
```
Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century.
One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock.
About 850 CE Kaldi supposedly 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.
```

8] des-cbc:



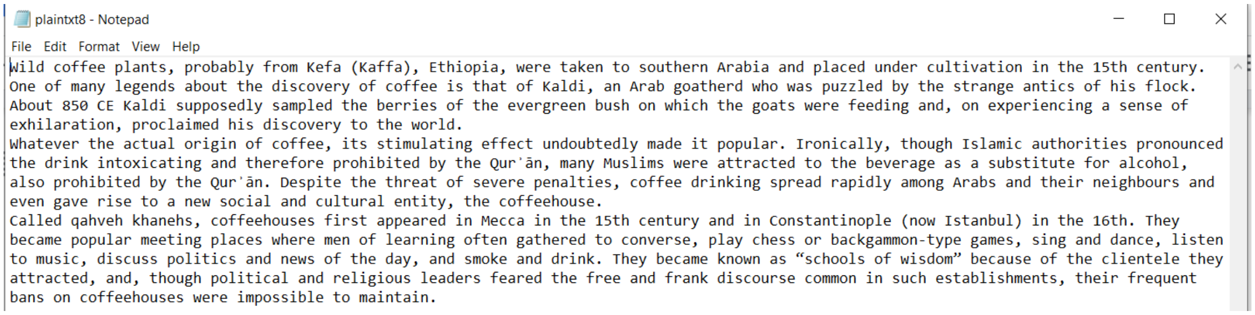
```
C:\Users\USER\Desktop>openssl des-cbc -salt -a -p -e -in coffee.txt -out encrypted.txt
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
salt=F44A1F3F3714FB7E
key=466AFE4B068B2702
iv =8956DCF4D9D8FD86

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:



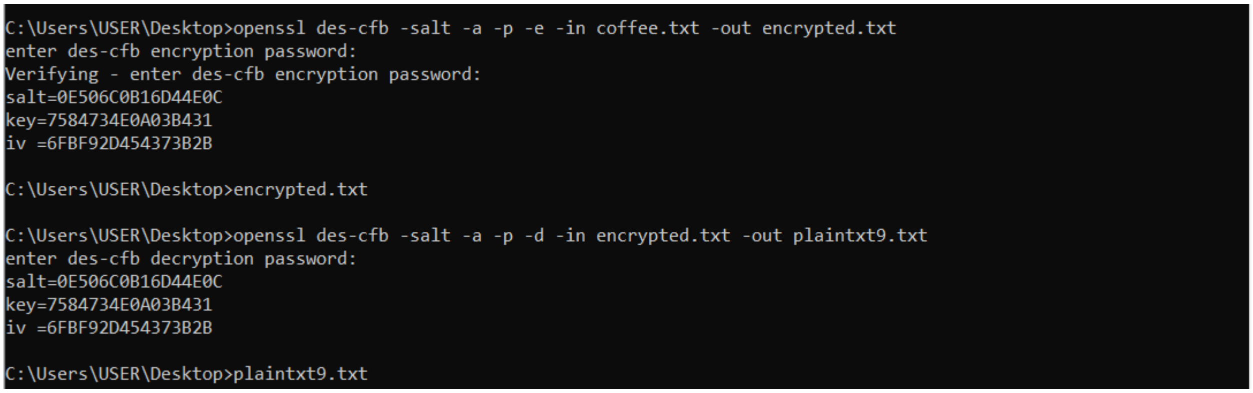
```
U2FsdGVkX19ndQcjczWuqLM0K3kK/lvo5Tycw1IVxNxlmKCF7GaCOrKnekhz2cHw
DtaWHKNWwXRbDOI8oWZav7ShkyrV5KED6RaSltdF6nvJgibtxfktjhDSqSUSk72Z
1G6P2AXNcSqnZuymP3KP08D6oy7fJ2K/5cm38pHPsEEn52gswSG0VFqSIQWP6rTT
NHVbnIO+NDmE2Ivbry2RgkeZP0HRFYJQlcck7GJgnvRhvpHkz8j839H71yJ9DlrR
/Spnwd02vtsQCaS6nbADZdY4cMpTPKPMkWFRWobV5rr+GmAEuT+Jk18IOUwm06oF
57a+k7TYtrefkCXxKODV9gmTy5UpJNSm2R4qmQ5cturhJUiajM7Ct19+ZntaZKTq
Fx2SJzqdjiRJGhyhNPCeOc3Bo/R43l1IK97v+czdovO5GcRykAtxsCpTrbuE9Kgi
nNU4eOHQaxxm8d3/3UwevbqFemi3/I3yoUKdvVTWL0HjHN7bQiLuHZ3DRin1jvsL
pF27C1T3lRnlDVBNIDHxq0jHVZ5/o1YkgwQX7r3U2cl3ZalTZnezqt4Ym2smEPmq
fPl4fnFshAiBvJZVanZWpapsDvGezpWQINQkCO7uVNGDbwyeS6crke1iZNdgejtr
MJFiMw9QG9vghrZQviUXjQ6PKSx+1JkW1ADIICwomDHVemJ8h8baViH/Ux3ZiqP7
X4k904L+X6FPzCphEJcXdSvqKRZaNa3j0NM5BK32ibTPOC8gb6bZFgsSZr+dwoZK
i0sO/S9jjdIT0KyzhBPpwmyxHfwQ+KRpGpSOPKfmoV+PnXTQyt9WoltO670w4WVs
PyiGYbllzxC6a3TadBN2SCrdm4H2MEumziTIu6vS1Uz0MKNG+ek2sT0jC8hUPYN2
wzLyI+UsX73aidXLcu+svoTrQFBMMvU6kug7IrXyc/zfr5YplUVMfcTh5t2QpsTp
lPvqAqHIkVmlCPpt7SOMACoRVogoGH1SCOKuhZaFnQo7fsmKikDWbuGt06Zr05+b
aFn+m7oBPDBYm/Ox84YchQJMoGE6qQ5+BFBVmjmr8ZRBNseZ7p0TZeTPlOUix+Pz
zjCUFE75Qip66y5hCAtDyGvmAu0FipnQMN/v/QXI7nkSqEbee0zfKWy+RxqDlxkl
TpVyGvKLr0ACJwh4lmS7of1HVFZfhAKj866N2vfn1fK5BN9hBJax2IR5n4KxuxJP
+DjwY6gyT2++wT+SM8KZX7aOQ2nbWgOdD2lT6Ls/XK5pOkyNj35jV42Fe2j28+qz
8vyWeimRU09KNQFZs8Uz9GfsNg/2Ds5QjGkjNRfRNKtkNnLQ1SuSkG4M2mLBh/TU
16jk5svtAXym4XMNMA0f1bmmuBxzvzWHc2Ti7WW3i23Rn2+R5rJYOL5VJ6HKjXf9
531Ste11j2PI7A6ioKWxCywfPvGYF1I1ooI7RPma1Lp3BXDnsdU4hZK3ZtmRotPa
myc+IxyXGrSUeFBwJkqjP5mrNiGQxxYSSM1vloH3uy/azUbUQignb0kkTOWaKZ/1
onag7rZrRyV5ZwrF/CsdCu7qvBqSpCG8hAzigw57iyXBk2GOcreFSMhWo83v3b1J
4ZwS2qqqj5/1qRzbss2X1kOFKmTRyR7p/KIxI4vJEcyQYEMqKasY+YXS73uDDx56
drlXICJFGW1Qm+TdSmna7Qxc0TfFrBf0h092xQZ4FdxaURPO2cG0xIPhJWqxWcBH
xgvlASgDR1O+lHDpG0K1V4/nDBUA7O6r9FQh4j+zLPKc38MbO9hLhZYRBDGzKLQZ
y3cewfHfmAoSIiq9o+aZfe4zPE+Fyo4Q4FgfkdgNAy91bEAc83VPs0SJE3A+Qz16
```

After decryption:



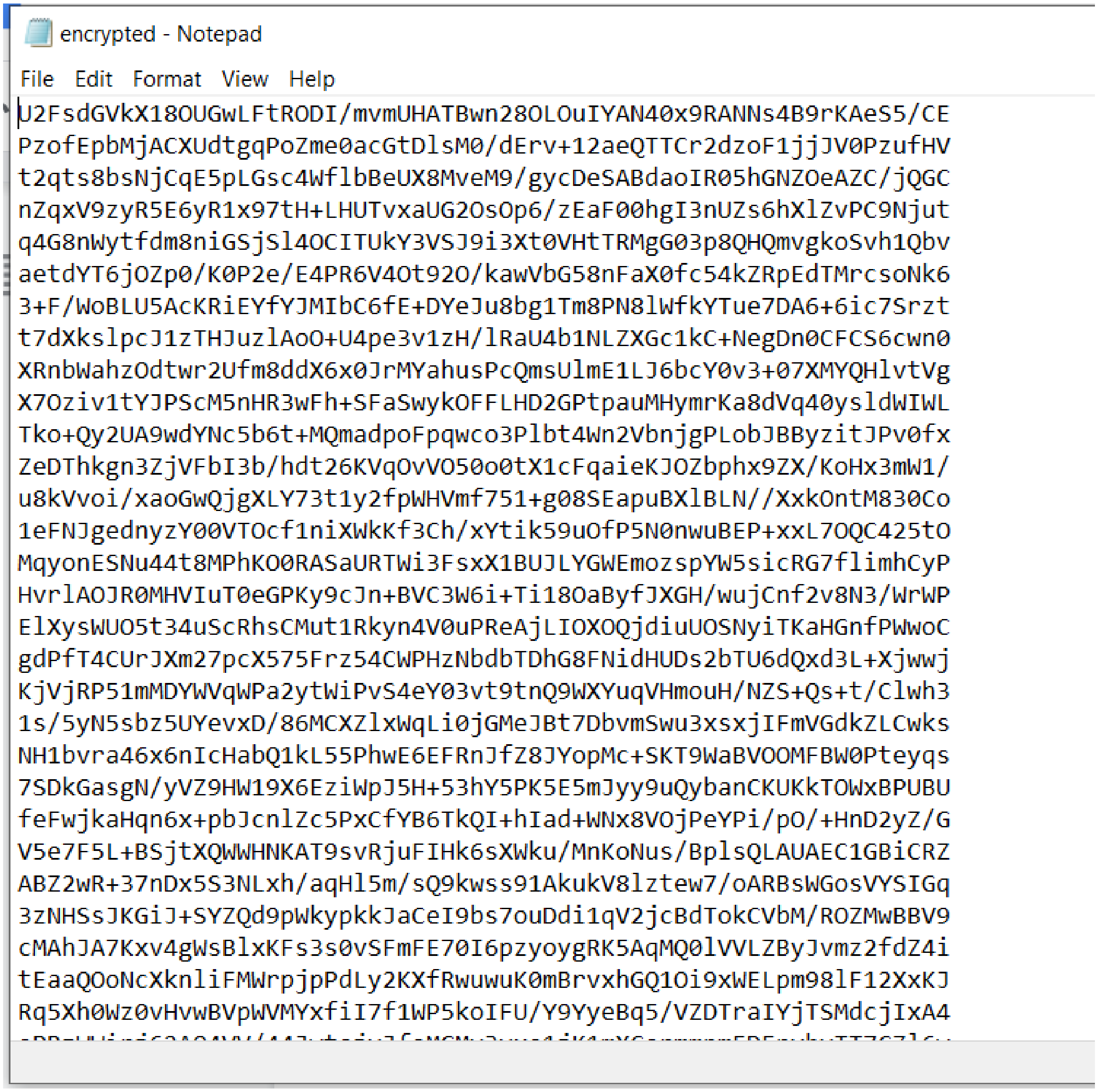
```
Wild coffee plants, probably from Kefa (Kaffa), Ethiopia, were taken to southern Arabia and placed under cultivation in the 15th century.
One of many legends about the discovery of coffee is that of Kaldi, an Arab goatherd who was puzzled by the strange antics of his flock.
About 850 CE Kaldi supposedly 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.
```

9] des-cfb:



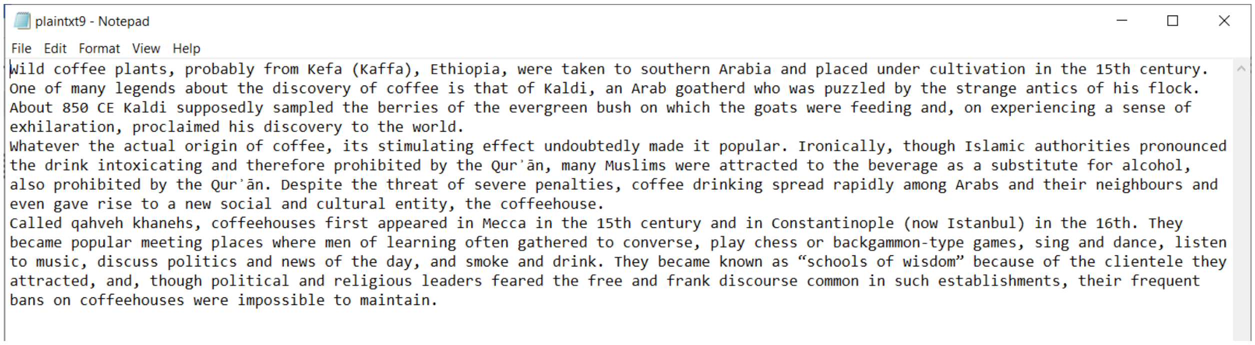
```
C:\Users\USER\Desktop>openssl des-cfb -salt -a -p -e -in coffee.txt -out encrypted.txt
enter des-cfb encryption password:
Verifying - enter des-cfb encryption password:
salt=0E506C0B16D44E0C
key=7584734E0A03B431
iv =6FBF92D454373B2B

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:



```
U2FsdGVkX18OUGwLFtRODI/mvmUHATBwn28OLOuIYAN40x9RANNs4B9rKAeS5/CE
PzofEpbMjACXUdtgqPoZme0acGtDlsM0/dErv+12aeQTTCr2dzoF1jjJV0PzufHV
t2qts8bsNjCqE5pLGsc4WflbBeUX8MveM9/gycDeSABdaoIR05hGNZOeAZC/jQGC
nZqxV9zyR5E6yR1x97tH+LHUTvxaUG2OsOp6/zEaF00hgI3nUZs6hXlZvPC9Njut
q4G8nWytfdm8niGSjSl4OCITUkY3VSJ9i3Xt0VHtTRMgG03p8QHQmvgkoSvh1Qbv
aetdYT6jOZp0/K0P2e/E4PR6V4Ot92O/kawVbG58nFaX0fc54kZRpEdTMrcsoNk6
3+F/WoBLU5AcKRiEYfYJMIbC6fE+DYeJu8bg1Tm8PN8lWfkYTue7DA6+6ic7Srzt
t7dXkslpcJ1zTHJuzlAoO+U4pe3v1zH/lRaU4b1NLZXGc1kC+NegDn0CFCS6cwn0
XRnbWahzOdtwr2Ufm8ddX6x0JrMYahusPcQmsUlmE1LJ6bcY0v3+07XMYQHlvtVg
X7Oziv1tYJPScM5nHR3wFh+SFaSwykOFFLHD2GPtpauMHymrKa8dVq40ysldWIWL
Tko+Qy2UA9wdYNc5b6t+MQmadpoFpqwco3Plbt4Wn2VbnjgPLobJBByzitJPv0fx
ZeDThkgn3ZjVFbI3b/hdt26KVqOvVO50o0tX1cFqaieKJOZbphx9ZX/KoHx3mW1/
u8kVvoi/xaoGwQjgXLY73t1y2fpWHVmf751+g08SEapuBXlBLN//XxkOntM830Co
1eFNJgednyzY00VTOcf1niXWkKf3Ch/xYtik59uOfP5N0nwuBEP+xxL7OQC425tO
MqyonESNu44t8MPhKO0RASaURTWi3FsxX1BUJLYGWEmozspYW5sicRG7flimhCyP
HvrlAOJR0MHVIuT0eGPKy9cJn+BVC3W6i+Ti18OaByfJXGH/wujCnf2v8N3/WrWP
ElXysWUO5t34uScRhsCMut1Rkyn4V0uPReAjLIOXOQjdiuUOSNyiTKaHGnfPWwoC
gdPfT4CUrJXm27pcX575Frz54CWPHzNbdbTDhG8FNidHUDs2bTU6dQxd3L+Xjwwj
KjVjRP51mMDYWVqWPa2ytWiPvS4eY03vt9tnQ9WXYuqVHmouH/NZS+Qs+t/Clwh3
1s/5yN5sbz5UYevxD/86MCXZlxWqLi0jGMeJBt7DbvmSwu3xsxjIFmVGdkZLCwks
NH1bvra46x6nIcHabQ1kL55PhwE6EFRnJfZ8JYopMc+SKT9WaBVOOMFBW0Pteyqs
7SDkGasgN/yVZ9HW19X6EziWpJ5H+53hY5PK5E5mJyy9uQybanCKUKkTOWxBPUBU
feFwjkaHqn6x+pbJcnlZc5PxCfYB6TkQI+hIad+WNx8VOjPeYPi/pO/+HnD2yZ/G
V5e7F5L+BSjtXQWWHNKAT9svRjuFIHk6sXWku/MnKoNus/BplsQLAUAEC1GBiCRZ
ABZ2wR+37nDx5S3NLxh/aqHl5m/sQ9kwss91AkukV8lztew7/oARBsWGosVYSIGq
3zNHSsJKGiJ+SYZQd9pWkypkkJaCeI9bs7ouDdi1qV2jcBdTokCVbM/ROZMwBBV9
cMAhJA7Kxv4gWsBlxKFs3s0vSFmFE70I6pzyoygRK5AqMQ0lVVLZByJvmz2fdZ4i
tEaaQOoNcXknliFMWrpjpPdLy2KXfRwuwuK0mBrvxhGQ1Oi9xWELpm98lF12XxKJ
Rq5Xh0Wz0vHvwBVpWVMYxfiI7f1WP5koIFU/Y9YyeBq5/VZDTraIYjTSMdcjIxA4
```

After decryption:



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.

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.

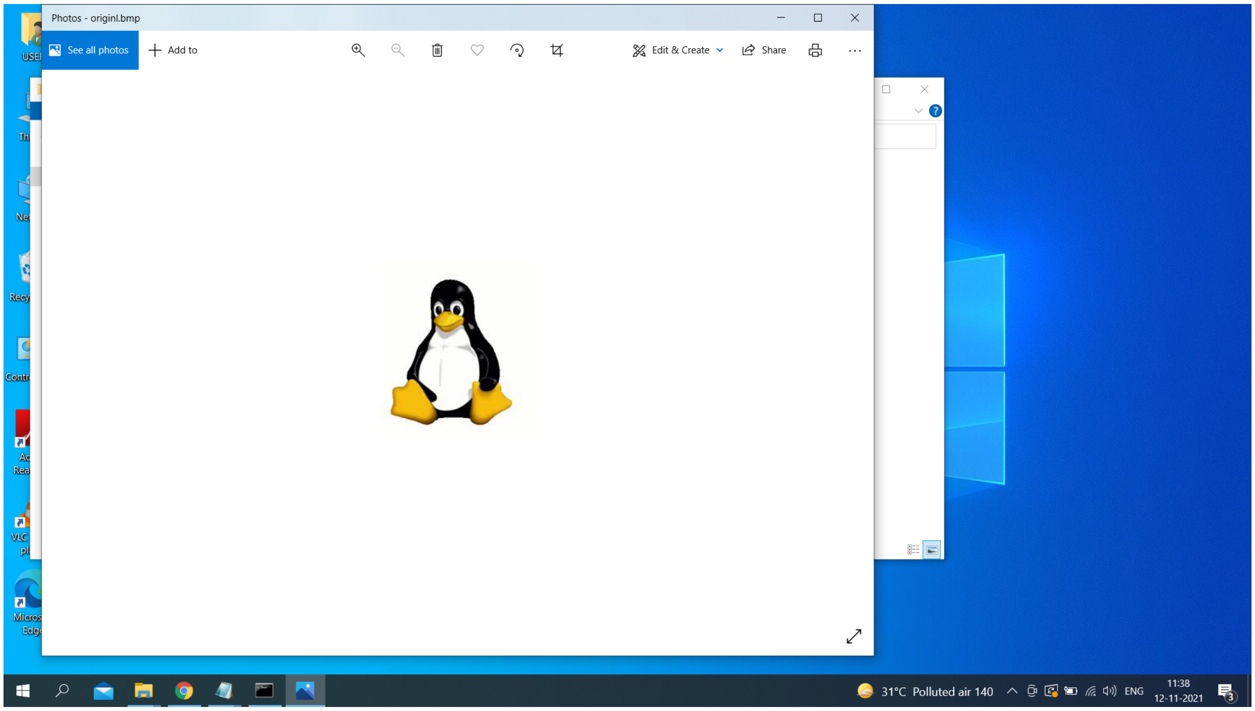
3] ECB is the simplest and weakest, because repeating plaintext generates repeating ciphertext. As a result, anyone can easily derive the secret keys to break the encryption and decrypt the ciphertext. ECB may also leave obvious plaintext patterns in the resulting ciphertext.

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.

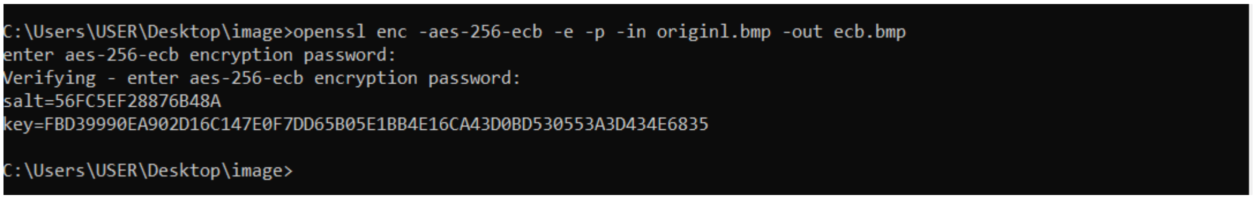
5] AES and DES are symmetric key algorithm using the same keys to encrypt and decrypt the data.

TASK:2

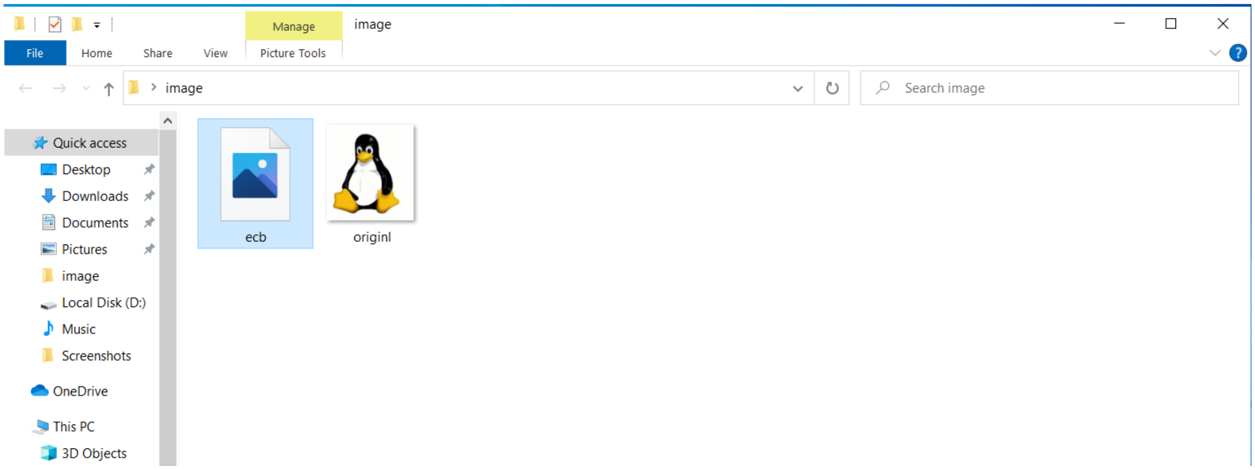
Original image:



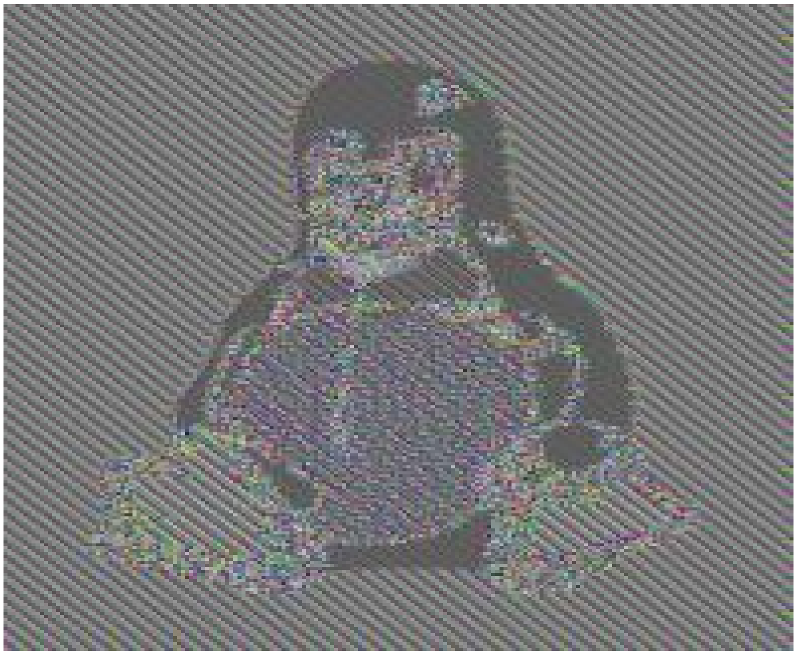
a) Using the cipher type -aes-256-ecb:



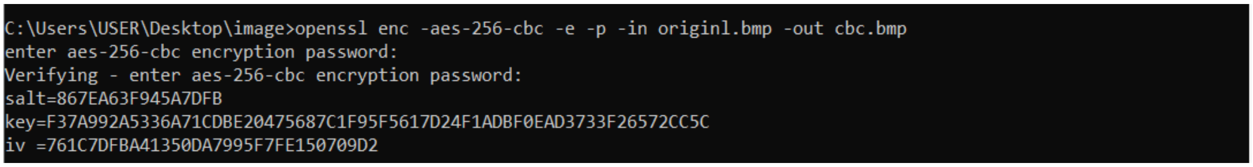
```
C:\Users\USER\Desktop\image>openssl enc -aes-256-ecb -e -p -in originl.bmp -out ecb.bmp
enter aes-256-ecb encryption password:
Verifying - enter aes-256-ecb encryption password:
salt=56FC5EF28876B48A
key=FBD39990EA902D16C147E0F7DD65B05E1BB4E16CA43D0BD530553A3D434E6835

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



Ecb image:

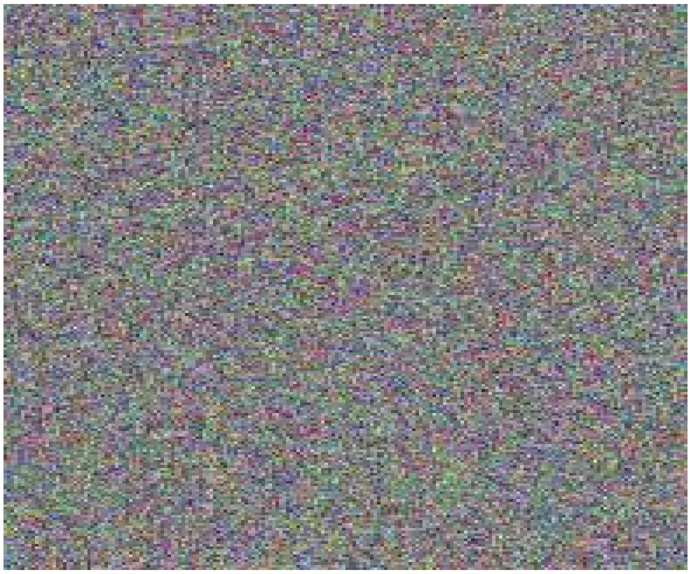


b) Using the cipher type -aes-256-cbc:



```
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
```

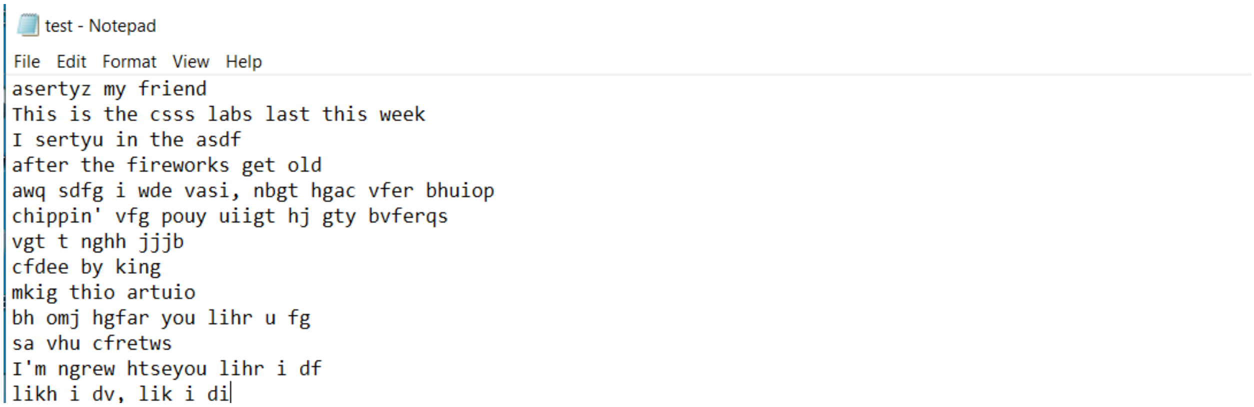
Cbc image:



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.

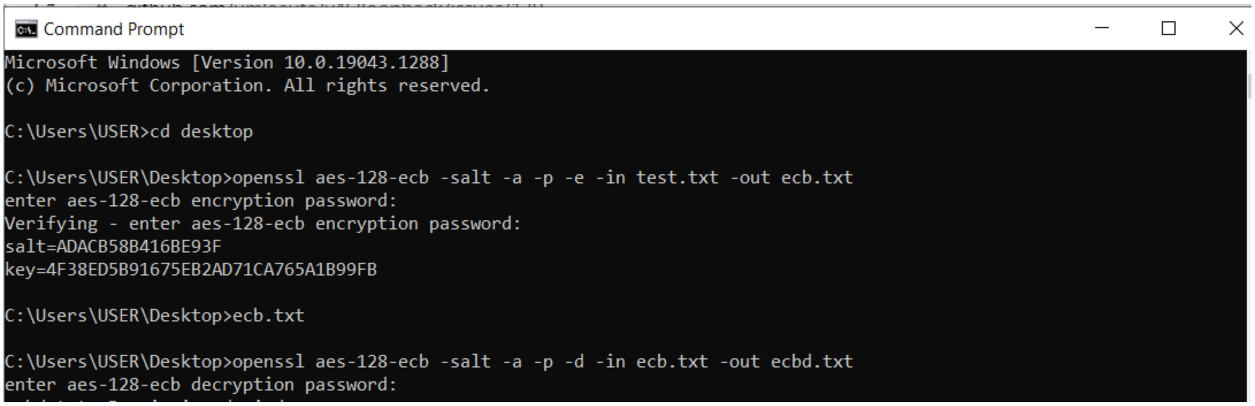
TASK:3

Plain text:



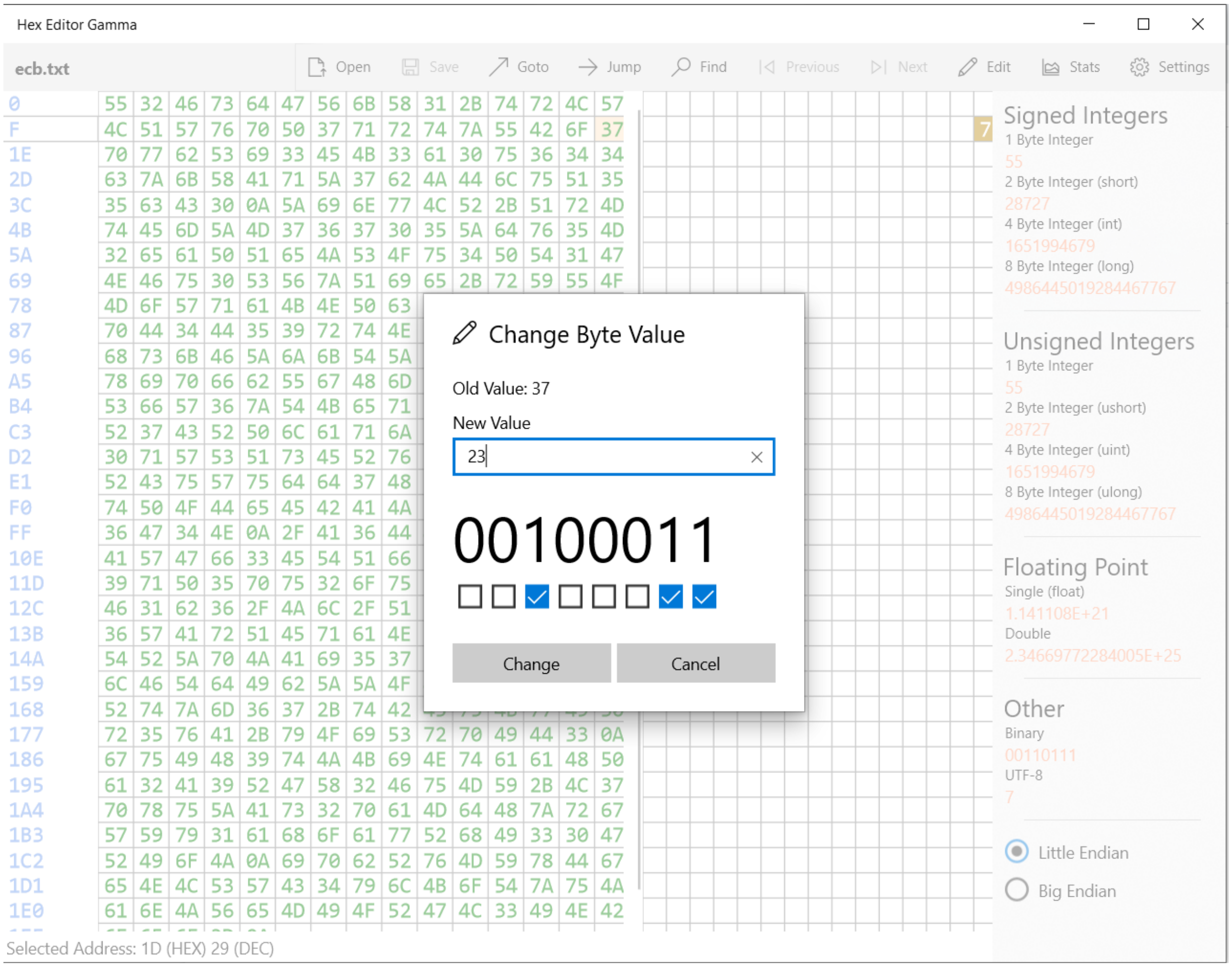
```
asertyz my friend
This is the csss labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuiop
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou lihr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

1] aes-128-ecb:



```
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 ecbd.txt
enter aes-128-ecb decryption password:
```

Corrupting 30 byte



```
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
```

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

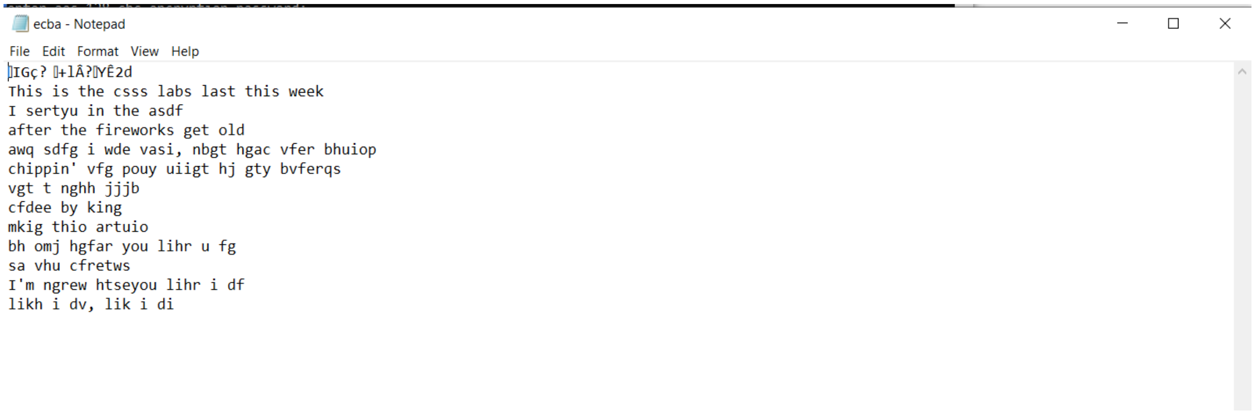
Floating Point
Single (float): 1.141108E+21
Double: 2.34669772284005E+25

Other
Binary: 00110111
UTF-8: 7

● Little Endian
○ Big Endian

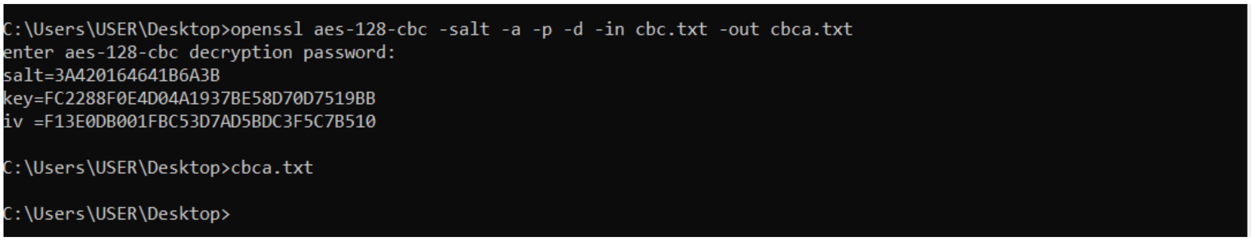
Selected Address: 1D (HEX) 29 (DEC)

Decrypting file:



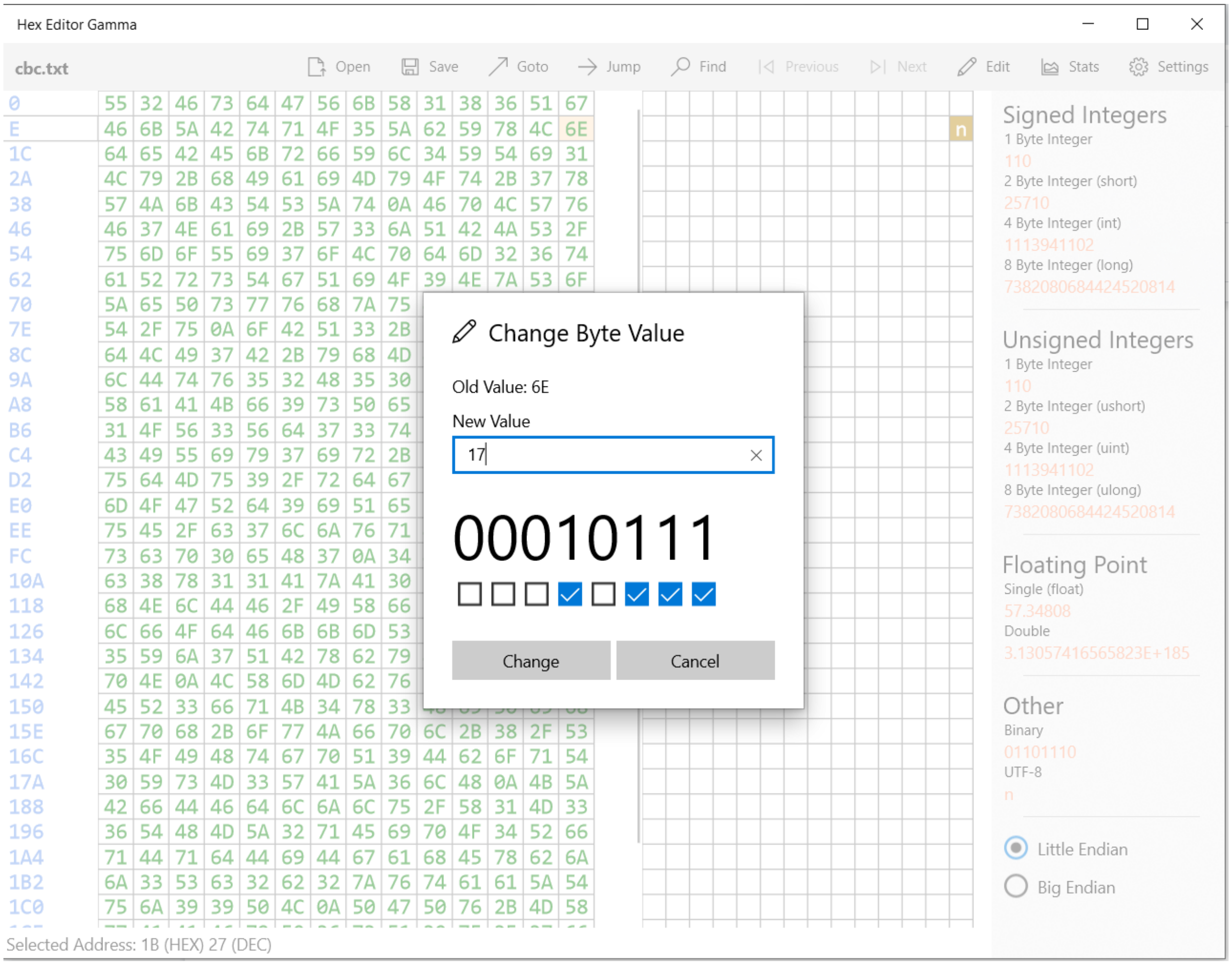
```
▯IGç? ▯+lÂ?▯YÊ2d
This is the csss labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuiop
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou lihr i df
likh i dv, lik i di
```

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



```
0    55 32 46 73 64 47 56 6B 58 31 38 36 51 67
E    46 6B 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
```

Change Byte Value

Old Value: 6E

New Value

17

00010111

□ □ □ ☑ □ ☑ ☑ ☑

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

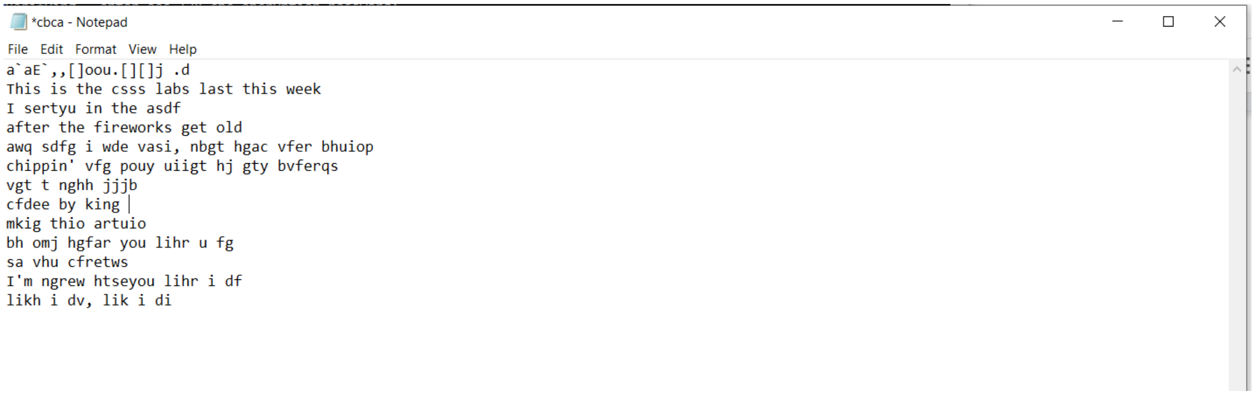
Floating Point
Single (float)
57.34808
Double
3.13057416565823E+185

Other
Binary
01101110
UTF-8
n

● Little Endian
○ Big Endian

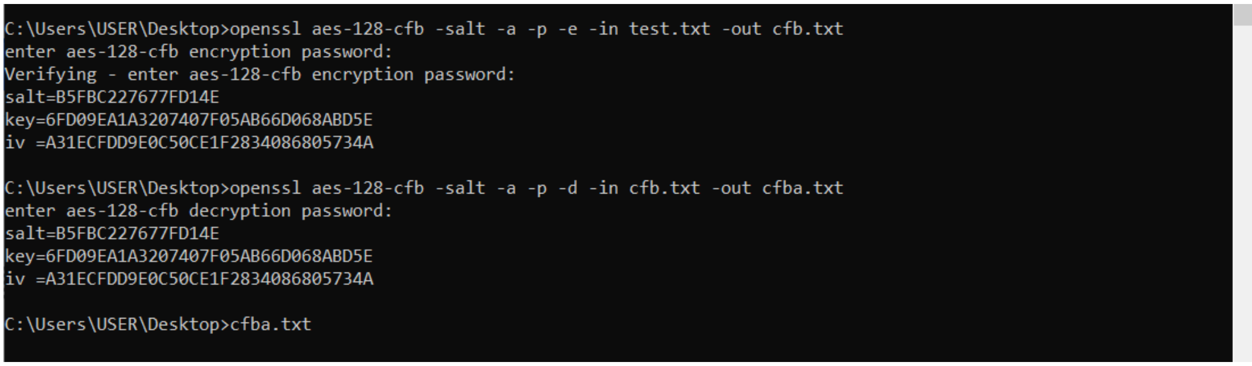
Selected Address: 1B (HEX) 27 (DEC)

Decrypt file:



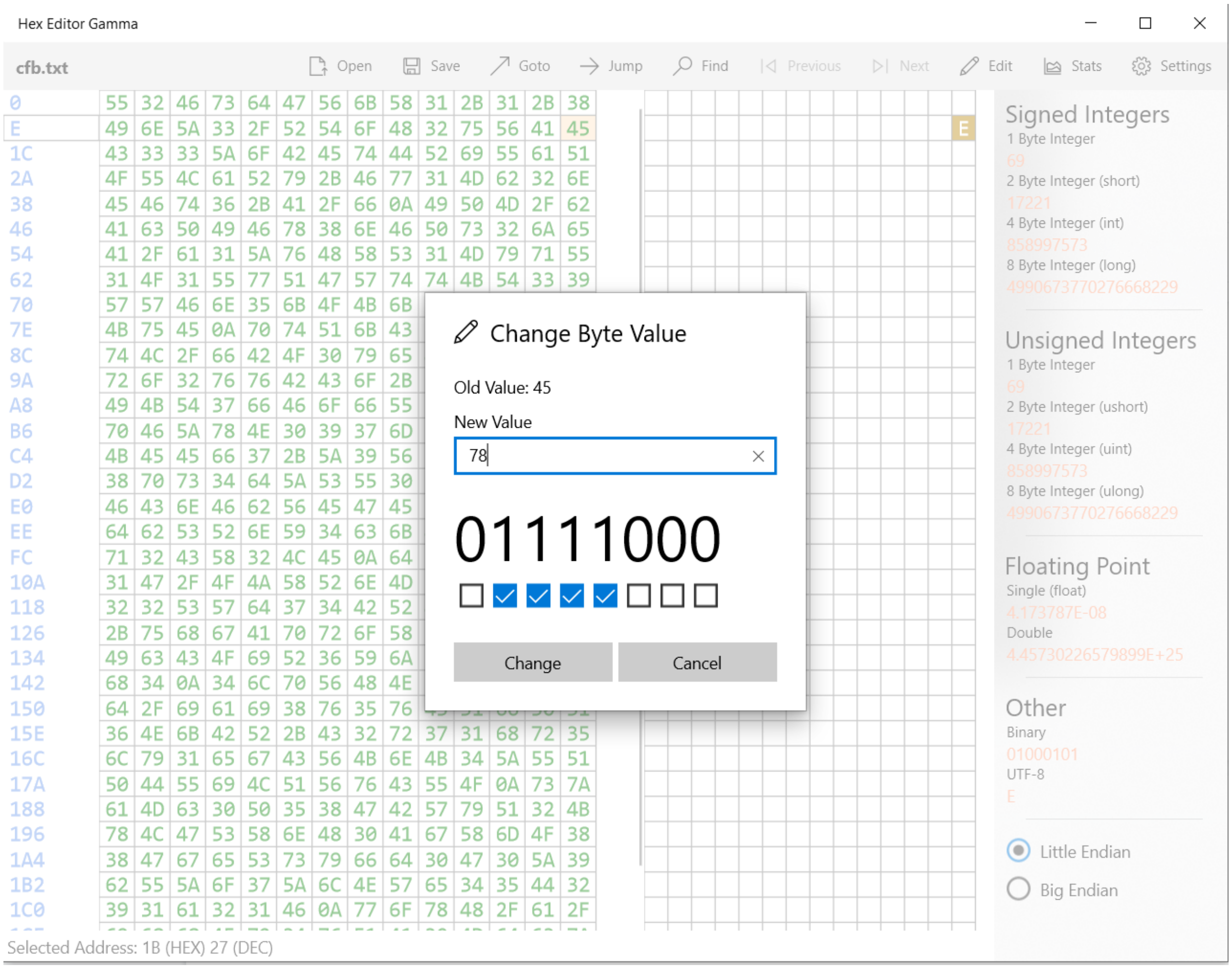
```
a`aE`,,[]oou.[][]j .d
This is the csss labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuiop
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou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

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



```
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 6B 4F 4B 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
```

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

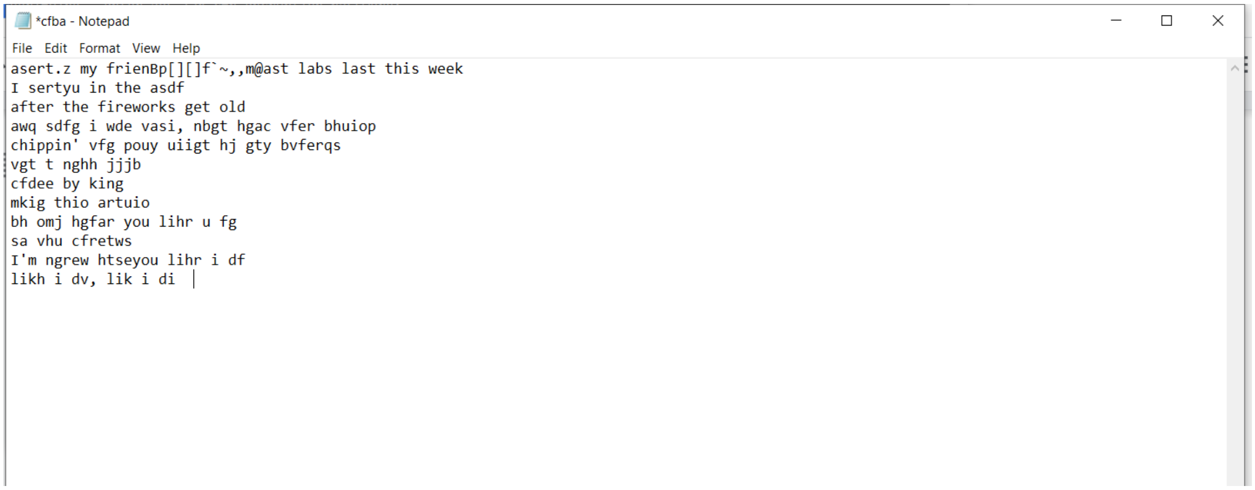
Floating Point
Single (float)
4.173787E-08
Double
4.45730226579899E+25

Other
Binary
01000101
UTF-8
E

● Little Endian
○ Big Endian

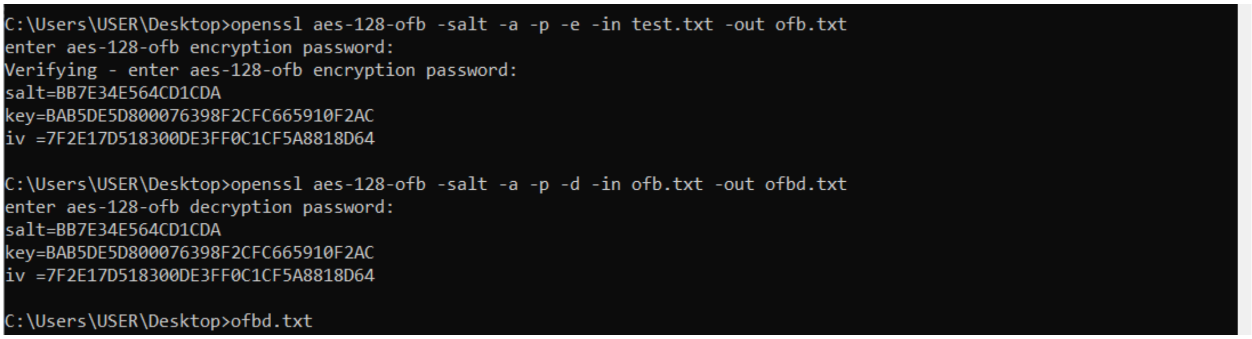
Selected Address: 1B (HEX) 27 (DEC)

Decrypt file:



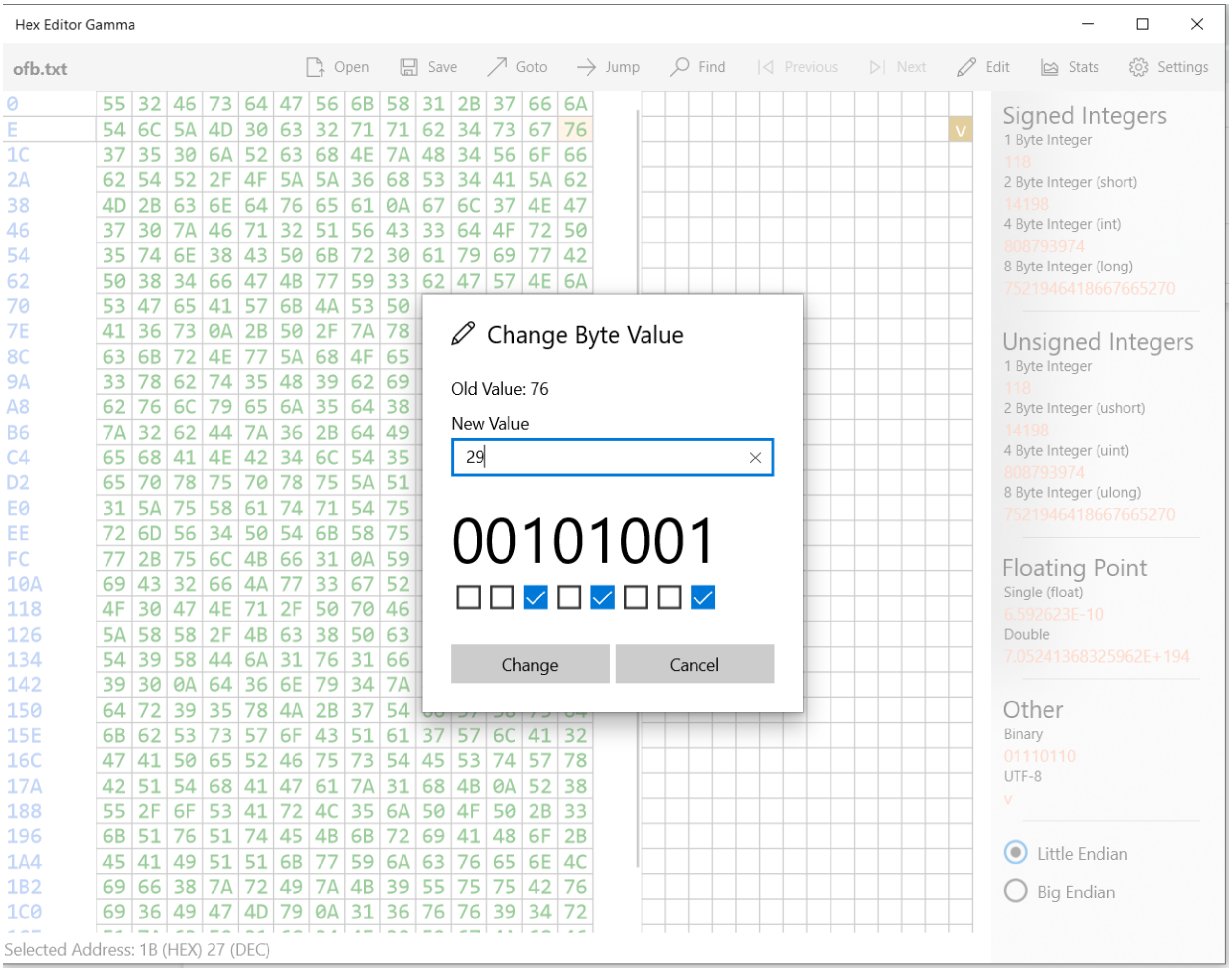
```
asert.z my frienBp[][]f`~,,m@ast labs last this week
I sertyu in the asdf
after the fireworks get old
awq sdfg i wde vasi, nbgt hgac vfer bhuiop
chippin' vfg pouy uiigt hj gty bvferqs
vgt t nghh jjjb
cfdee by king
mkig thio artuio
bh omj hgfar you lihr u fg
sa vhu cfretws
I'm ngrew htseyou lihr i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



```
0     55 32 46 73 64 47 56 6B 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 6B 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 47 4D 79 0A 31 36 76 76 39 34 72
```

Change Byte Value

Old Value: 76

New Value

29

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

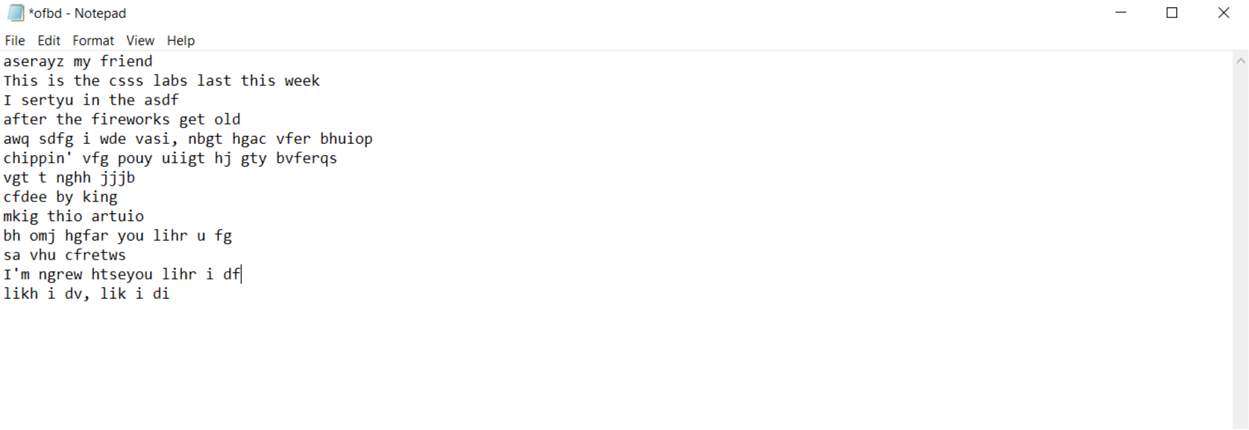
Floating Point
Single (float)
6.592623E-10
Double
7.05241368325962E+194

Other
Binary
01110110
UTF-8
v

● Little Endian
○ Big Endian

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

Decrypt file:



```
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 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
```

Observation:

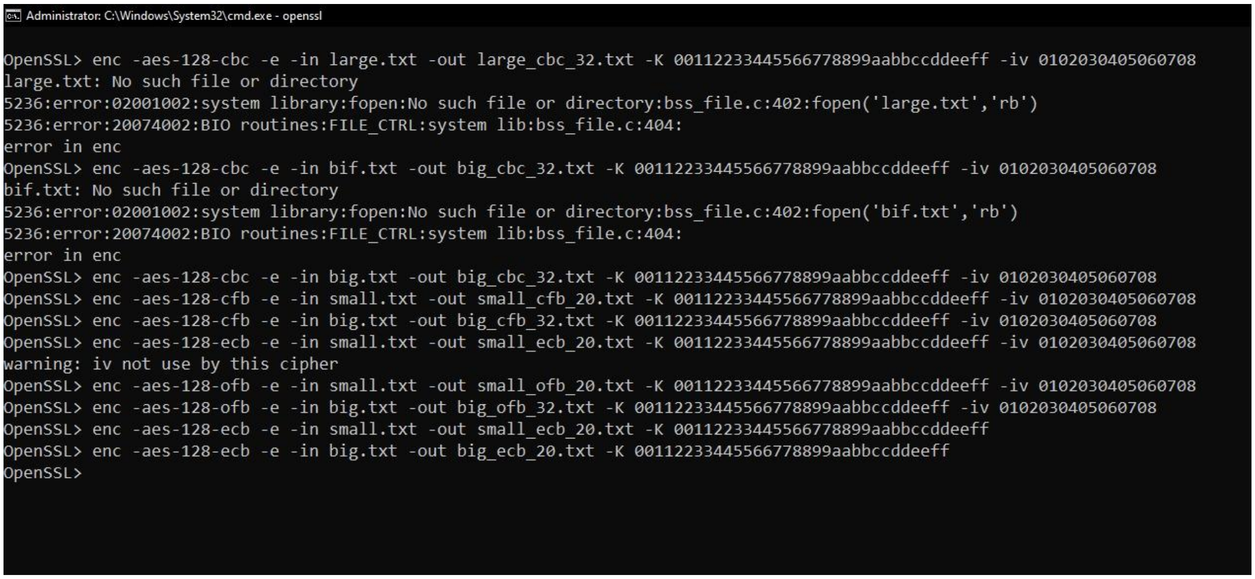
1] In ECB mode , only one block is affected when any problem in the ciphertext happens. Each block is decrypted independently.An advantage of this mode is that there is no dependency upon other blocks, the encryption and decryption can be carried out by many threads simultaneously.

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.

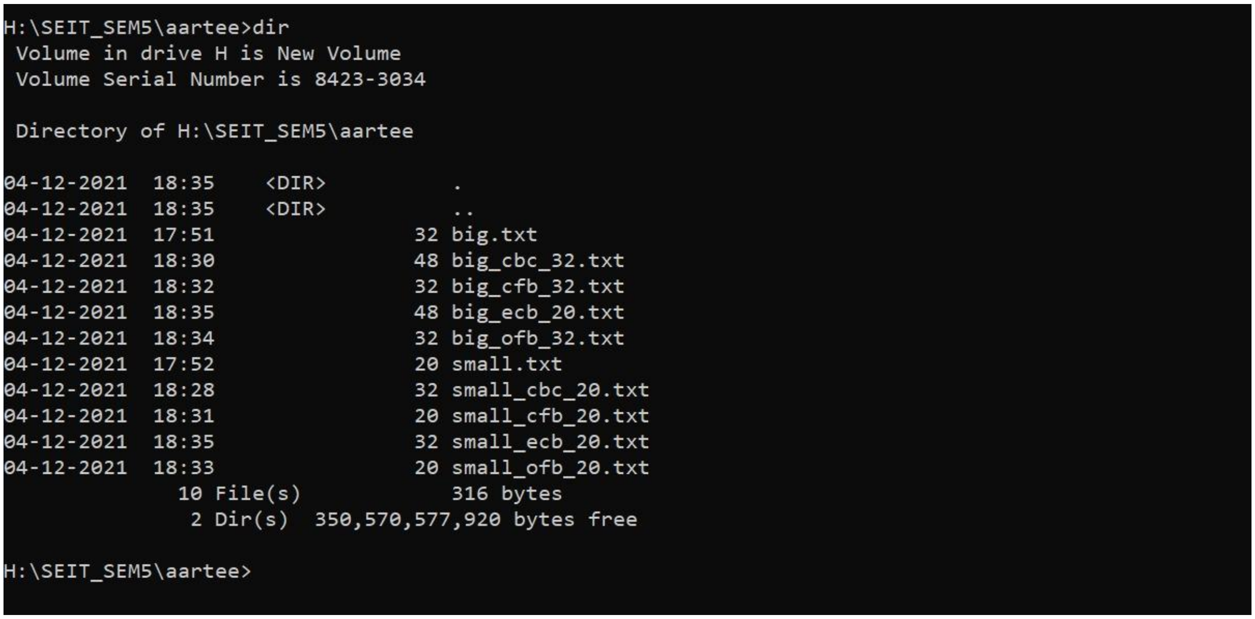
3] In CFB mode, the previous ciphertext block is encrypted and the output is XORed (see XOR) with the current plaintext block to create the current ciphertext block. The XOR operation conceals plaintext patterns.

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.

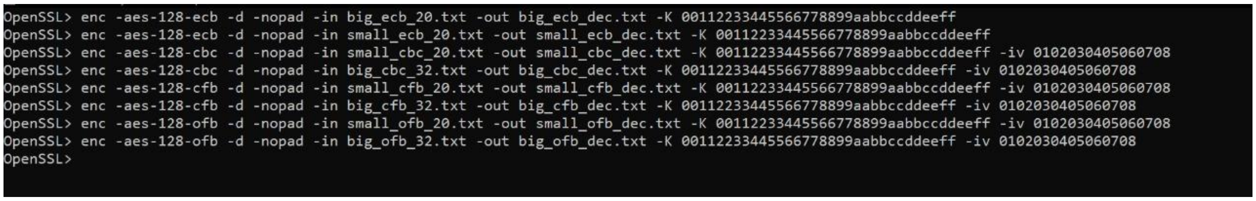
TASK:4



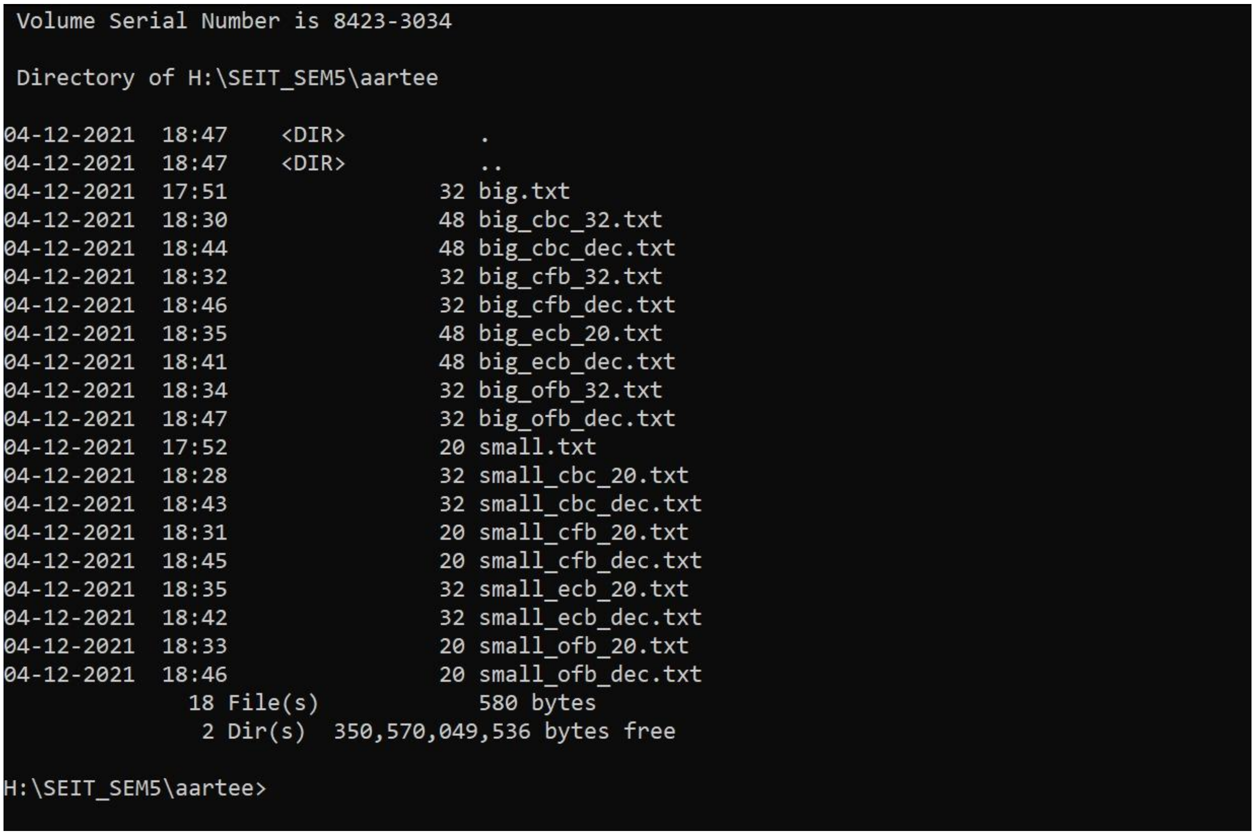
```
OpenSSL> enc -aes-128-cbc -e -in large.txt -out large_cbc_32.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
large.txt: No such file or directory
5236:error:02001002:system library:fopen:No such file or directory:bss_file.c:402:fopen('large.txt','rb')
5236:error:20074002:BIO routines:FILE_CTRL:system lib:bss_file.c:404:
error in enc
OpenSSL> enc -aes-128-cbc -e -in bif.txt -out big_cbc_32.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
bif.txt: No such file or directory
5236:error:02001002:system library:fopen:No such file or directory:bss_file.c:402:fopen('bif.txt','rb')
5236:error:20074002:BIO routines:FILE_CTRL:system lib:bss_file.c:404:
error in enc
OpenSSL> enc -aes-128-cbc -e -in big.txt -out big_cbc_32.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-cfb -e -in small.txt -out small_cfb_20.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-cfb -e -in big.txt -out big_cfb_32.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-ecb -e -in small.txt -out small_ecb_20.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
OpenSSL> enc -aes-128-ofb -e -in small.txt -out small_ofb_20.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-ofb -e -in big.txt -out big_ofb_32.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-ecb -e -in small.txt -out small_ecb_20.txt -K 00112233445566778899aabbccddeeff
OpenSSL> enc -aes-128-ecb -e -in big.txt -out big_ecb_20.txt -K 00112233445566778899aabbccddeeff
OpenSSL>
```



```
H:\SEIT_SEM5\aartee>dir
 Volume in drive H is New Volume
 Volume Serial Number is 8423-3034

 Directory of H:\SEIT_SEM5\aartee

04-12-2021  18:35    <DIR>          .
04-12-2021  18:35    <DIR>          ..
04-12-2021  17:51                32 big.txt
04-12-2021  18:30                48 big_cbc_32.txt
04-12-2021  18:32                32 big_cfb_32.txt
04-12-2021  18:35                48 big_ecb_20.txt
04-12-2021  18:34                32 big_ofb_32.txt
04-12-2021  17:52                20 small.txt
04-12-2021  18:28                32 small_cbc_20.txt
04-12-2021  18:31                20 small_cfb_20.txt
04-12-2021  18:35                32 small_ecb_20.txt
04-12-2021  18:33                20 small_ofb_20.txt
              10 File(s)            316 bytes
               2 Dir(s)  350,570,577,920 bytes free

H:\SEIT_SEM5\aartee>
```



```
OpenSSL> enc -aes-128-ecb -d -nopad -in big_ecb_20.txt -out big_ecb_dec.txt -K 00112233445566778899aabbccddeeff
OpenSSL> enc -aes-128-ecb -d -nopad -in small_ecb_20.txt -out small_ecb_dec.txt -K 00112233445566778899aabbccddeeff
OpenSSL> enc -aes-128-cbc -d -nopad -in small_cbc_20.txt -out small_cbc_dec.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-cbc -d -nopad -in big_cbc_32.txt -out big_cbc_dec.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-cfb -d -nopad -in small_cfb_20.txt -out small_cfb_dec.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-cfb -d -nopad -in big_cfb_32.txt -out big_cfb_dec.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-ofb -d -nopad -in small_ofb_20.txt -out small_ofb_dec.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-ofb -d -nopad -in big_ofb_32.txt -out big_ofb_dec.txt -K 00112233445566778899aabbccddeeff -iv 0102030405060708
OpenSSL>
```



```
 Volume Serial Number is 8423-3034

 Directory of H:\SEIT_SEM5\aartee

04-12-2021  18:47    <DIR>          .
04-12-2021  18:47    <DIR>          ..
04-12-2021  17:51                32 big.txt
04-12-2021  18:30                48 big_cbc_32.txt
04-12-2021  18:44                48 big_cbc_dec.txt
04-12-2021  18:32                32 big_cfb_32.txt
04-12-2021  18:46                32 big_cfb_dec.txt
04-12-2021  18:35                48 big_ecb_20.txt
04-12-2021  18:41                48 big_ecb_dec.txt
04-12-2021  18:34                32 big_ofb_32.txt
04-12-2021  18:47                32 big_ofb_dec.txt
04-12-2021  17:52                20 small.txt
04-12-2021  18:28                32 small_cbc_20.txt
04-12-2021  18:43                32 small_cbc_dec.txt
04-12-2021  18:31                20 small_cfb_20.txt
04-12-2021  18:45                20 small_cfb_dec.txt
04-12-2021  18:35                32 small_ecb_20.txt
04-12-2021  18:42                32 small_ecb_dec.txt
04-12-2021  18:33                20 small_ofb_20.txt
04-12-2021  18:46                20 small_ofb_dec.txt
              18 File(s)            580 bytes
               2 Dir(s)  350,570,049,536 bytes free

H:\SEIT_SEM5\aartee>
```

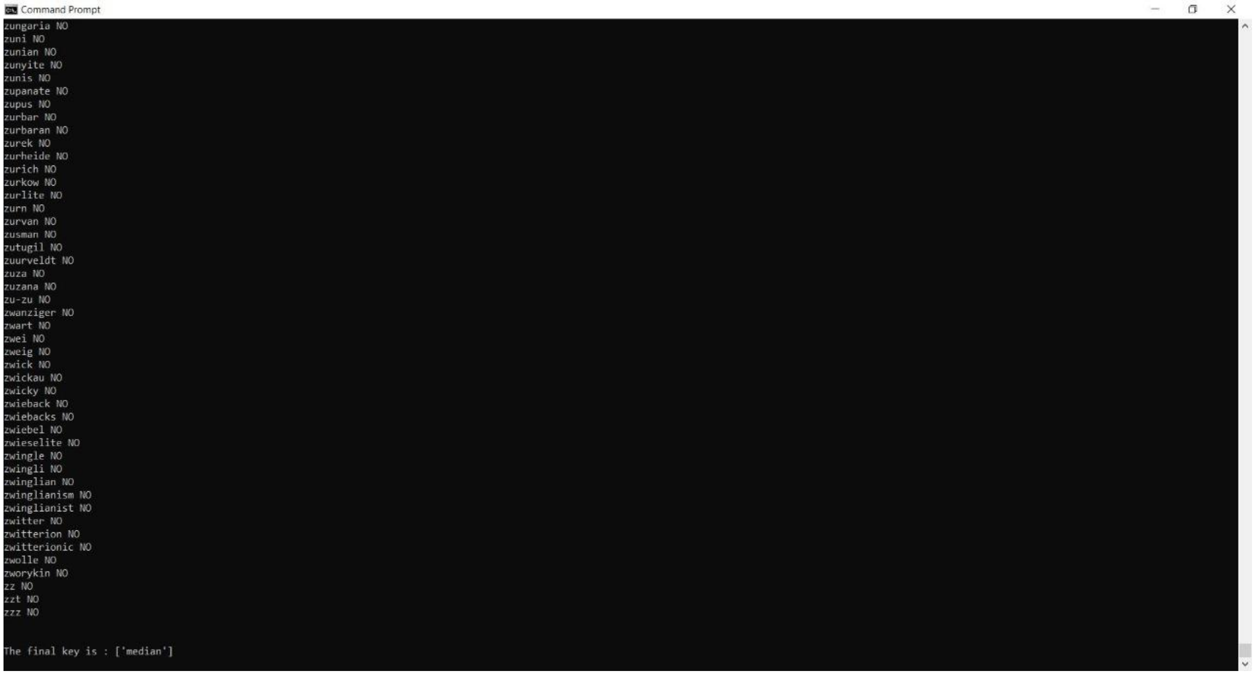
Observation:
1] The padding is needed for ECB and CBC encryption modes.ECB and CBC are block cipher and for block cipher length of input must be an exact multiple of block length.If this is not the case then padding must be needed to make it so.
2] In OFB and CFB, the padding is not required because 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:



```
zungaria NO
zuni NO
zunian NO
zunyite NO
zunis NO
zupanate NO
zupus NO
zurbar NO
zurbaran NO
zurek NO
zurheide NO
zurich NO
zurkow NO
zurlite NO
zurn NO
zurvan NO
zusman NO
zutugil NO
zuurveldt NO
zuza NO
zuzana NO
zu-zu NO
zwanziger NO
zwart NO
zwei NO
zweig NO
zwick NO
zwickau NO
zwicky NO
zwieback NO
zwiebacks NO
zwiebel NO
zwieselite NO
zwingle NO
zwingli NO
zwinglian NO
zwinglianism 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.