Name: Vishal Salvi
UID: 2019230069
Batch: c
Class: TE Comps

Experiment 3:	**Crypto Encryption**

Note: Students are advised to read through this lab sheet before doing experiment. On-the-spot evaluation may be carried out during or at the end of the experiment. Your performance, teamwork effort, and learning attitude will count towards the marks.

Experiment 4: Crypto Lab – Secret-Key Encryption

1 OBJECTIVE

The learning objective of this lab is for students to get familiar with the concepts in the secret-key encryption. After finishing the lab, students should be able to gain a first-hand experience on encryption algorithms, encryption modes, paddings, and initial vector (IV). Moreover, students will be able to use tools and write programs to encrypt/decrypt messages.

2 LAB ENVIRONMENT

Installing OpenSSL. In this lab, we will use openssl commands and libraries. We have already in-stalled openssl binaries in our VM. It should be noted that if you want to use openssl libraries in your programs, you need to install several other things for the programming environment, including the header files, libraries, manuals, etc. We have already downloaded the necessary files under the directory openssl-1.0.1. To configure and install openssl libraries, run the following commands.

You should read the INSTALL file first:

```
% ./config
% make
% make test
% sudo make install
```

Installing GHex. In this lab, we need to be able to view and modify files of binary format. We have installed in our VM GHex a hex editor for GNOME. It allows the user to load data from any file, view and edit it in either hex or ascii.

3 LAB TASKS

3.1 Task 1: Encryption using different ciphers and modes

In this task, we will play with various encryption algorithms and modes. You can use the following openssl enc command to encrypt/decrypt a file. To see the manuals, you can type man openssl and man enc.

```
% openssl enc ciphertype -e -in plain.txt -out cipher.bin \ -K
                    00112233445566778889aabbccddeeff \
                    -iv 0102030405060708
```

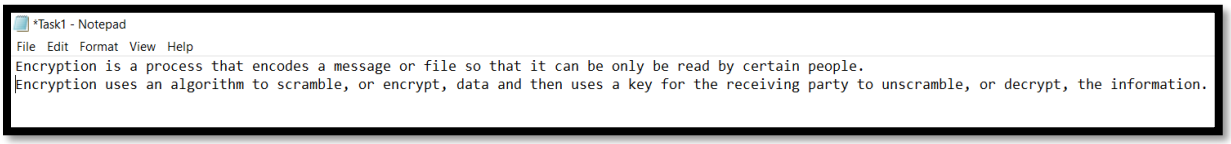
Please replace the ciphertype with a specific cipher type, such as -aes-128-cbc, -aes-128-cfb, -bf-cbc, etc. In this task, you should try at least 3 different ciphers and three different modes. You can find the meaning of the command-line options and all the supported cipher types by typing "man enc". We include some common options for the openssl enc command in the following:

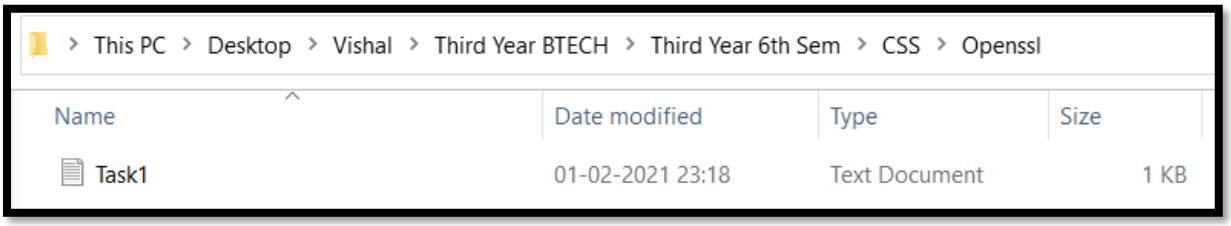
-in <file>	input file
-out <file>	output file
-e	encrypt
-d	decrypt
-K/-iv	key/iv in hex is the next argument
-[pP]	print the iv/key (then exit if -P)

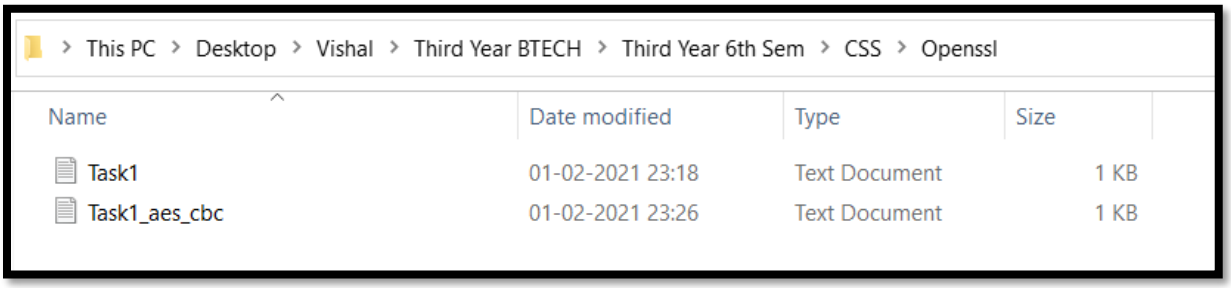
Task 1:

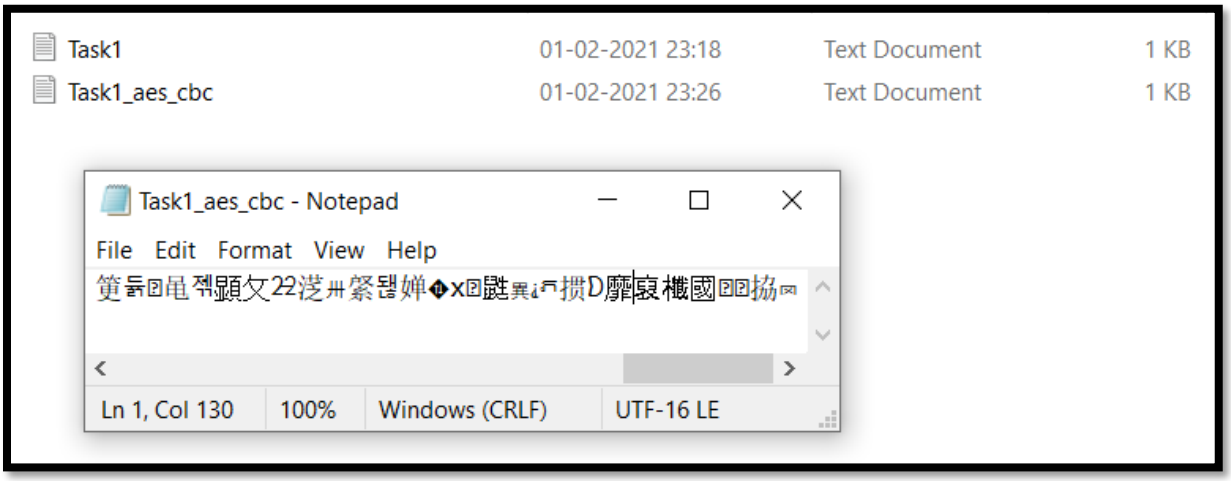
1)-aes-128-cbc Encryption:

```
OpenSSL> enc -aes-128-cbc -e -in Task1.txt -out Task1_aes_cbc.txt -k 1234abcd -iv 1234567890
OpenSSL>
```









Task1_aes_cbc.txt | Task1_aes_cbc_dec.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   53 61 6C 74 65 64 5F 5F 23 FB 30 BF 3C 67 B1 3B  Salted__#û0¿<g±;
00000010   99 A7 49 D7 61 E6 E6 C7 29 96 0D E9 B2 80 53 DB  ™§I×aææÇ)–.é²€SÛ
00000020   BB 49 46 B9 3A 3F AF F7 5C E7 5A EF 8E 6F 4A B7  »IF¹:?¯÷\çZïŽoJ·
00000030   3A BB 80 03 A1 66 59 35 50 F9 AB 3E C8 B4 89 0A  :»€.¡fY5Pù«>È´‰.
00000040   DD 4B 93 07 F0 F0 5A 29 67 AD 3A F5 F1 40 EC A9  ÝK".ððZ)g.:õñ@ì©
00000050   23 DA DE 96 6B 73 87 8B AB AD 79 65 B9 35 6D 8F  #ÚÞ–ks‡‹«.ye¹5m.
00000060   BA 6A 56 AD D3 A1 97 CB 3D 5B 55 CB 5B 7A D2 0A  ºjV.Ó¡—Ë=[UË[zÒ.
00000070   B8 0C 0C CB 94 41 2A 44 F6 C8 55 DA 5C C6 85 2D  ¸..Ë”A*DöÈUÚ\Æ…-
00000080   17 CB 75 13 31 11 6E C4 82 17 B2 F2 F2 C4 B6 12  .Ëu.1.nÄ‚.²òòÄ¶.
00000090   B3 15 F4 A3 27 93 A1 0B A6 1D 3E B9 F6 94 F1 F8  ³.ô£'"¡.¦.>¹ö”ñø
000000A0   2D 0E 7A 38 1F F5 A4 72 28 01 56 2E B9 67 A7 BE  -.z8.õ¤r(.V.¹g§¾
000000B0   65 68 FC 27 8C AE FF 8F 4A 6C 1C 61 3F BF 3A 15  ehü'Œ®ÿ.Jl.a?¿:.
000000C0   65 36 89 9B 0B 82 77 D1 7F 24 90 E5 54 57 29 2B  e6‰›.‚wÑ.$.åTW)+
000000D0   C2 34 76 76 7B 7B C9 B4 4F F3 FE 9E 56 C8 55 98  Â4vv{{É´Oóþ‘VÈU˜
000000E0   35 65 E0 A5 00 3D 3A 30 DC 42 02 B4 75 5A D6 26  5eà¥.=:0ÜB.´uZÖ&
000000F0   78 00 F5 F2 2A 9F 62 F9 18 2E 97 17 BC 63 E4 15  x.õò*Ÿbù..—.¼cä.
00000100   61 97 D2 88 FC 6A 0B 57 C1 E1 DD EB F9 62 B1 2E  a—Ò^üj.WÁáÝëùb±.
```

Decryption:

```
OpenSSL> enc -aes-128-cbc -d -in Task1_aes_cbc.txt -out Task1_aes_cbc_dec.txt -k 1234abcd -iv 1234567890
OpenSSL>
```

This PC > Desktop > Vishal > Third Year BTECH > Third Year 6th Sem > CSS > Openssl

Name	Date modified	Type	Size
Task1	01-02-2021 23:18	Text Document	1 KB
Task1_aes_cbc	01-02-2021 23:26	Text Document	1 KB
Task1_aes_cbc_dec	01-02-2021 23:50	Text Document	1 KB

*Task1_aes_cbc_dec - Notepad

File Edit Format View Help

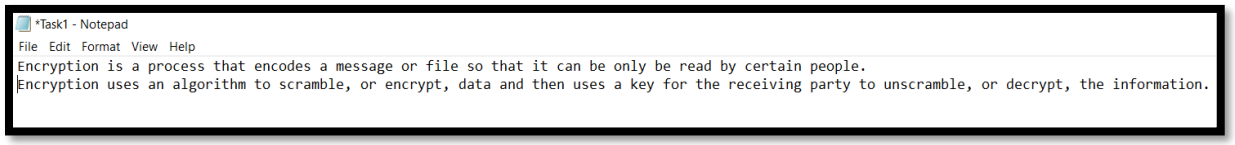
```
Encryption is a process that encodes a message or file so that it can be only be read by certain people.
Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information.
```

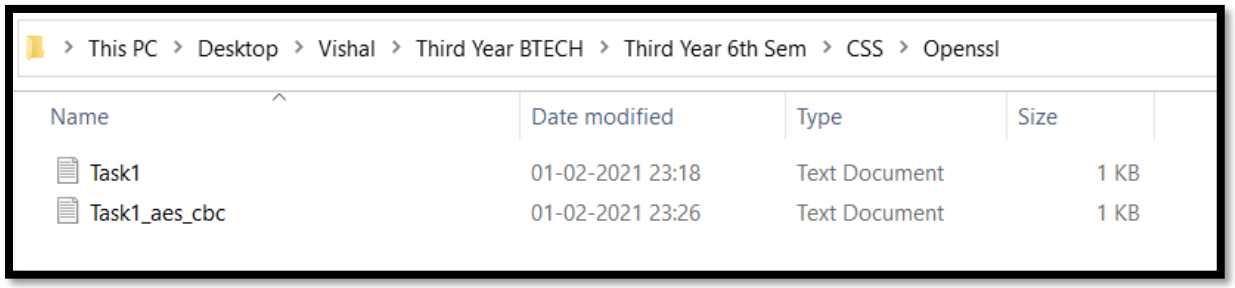
Task1_aes_cbc.txt | Task1_aes_cbc_dec.txt

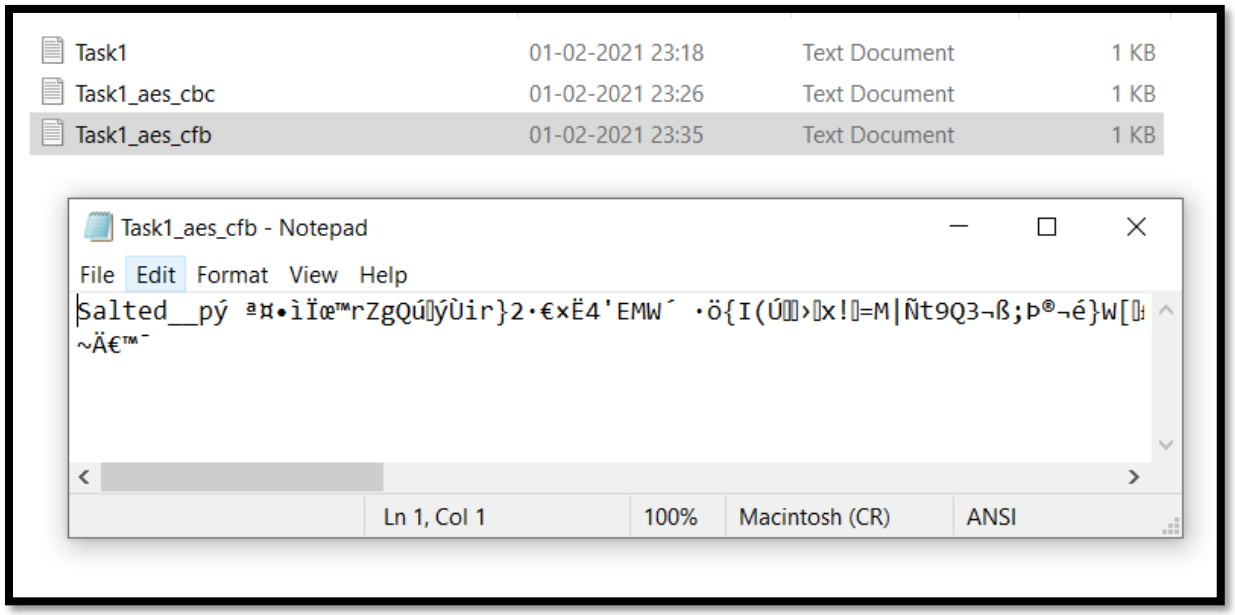
```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   45 6E 63 72 79 70 74 69 6F 6E 20 69 73 20 61 20  Encryption is a
00000010   70 72 6F 63 65 73 73 20 74 68 61 74 20 65 6E 63  process that enc
00000020   6F 64 65 73 20 61 20 6D 65 73 73 61 67 65 20 6F  odes a message o
00000030   72 20 66 69 6C 65 20 73 6F 20 74 68 61 74 20 69  r file so that i
00000040   74 20 63 61 6E 20 62 65 20 6F 6E 6C 79 20 62 65  t can be only be
00000050   20 72 65 61 64 20 62 79 20 63 65 72 74 61 69 6E   read by certain
00000060   20 70 65 6F 70 6C 65 2E 20 0D 0A 45 6E 63 72 79   people. ..Encry
00000070   70 74 69 6F 6E 20 75 73 65 73 20 61 6E 20 61 6C  ption uses an al
00000080   67 6F 72 69 74 68 6D 20 74 6F 20 73 63 72 61 6D  gorithm to scram
00000090   62 6C 65 2C 20 6F 72 20 65 6E 63 72 79 70 74 2C  ble, or encrypt,
000000A0   20 64 61 74 61 20 61 6E 64 20 74 68 65 6E 20 75   data and then u
000000B0   73 65 73 20 61 20 6B 65 79 20 66 6F 72 20 74 68  ses a key for th
000000C0   65 20 72 65 63 65 69 76 69 6E 67 20 70 61 72 74  e receiving part
000000D0   79 20 74 6F 20 75 6E 73 63 72 61 6D 62 6C 65 2C  y to unscramble,
000000E0   20 6F 72 20 64 65 63 72 79 70 74 2C 20 74 68 65   or decrypt, the
000000F0   20 69 6E 66 6F 72 6D 61 74 69 6F 6E 2E            information.
```

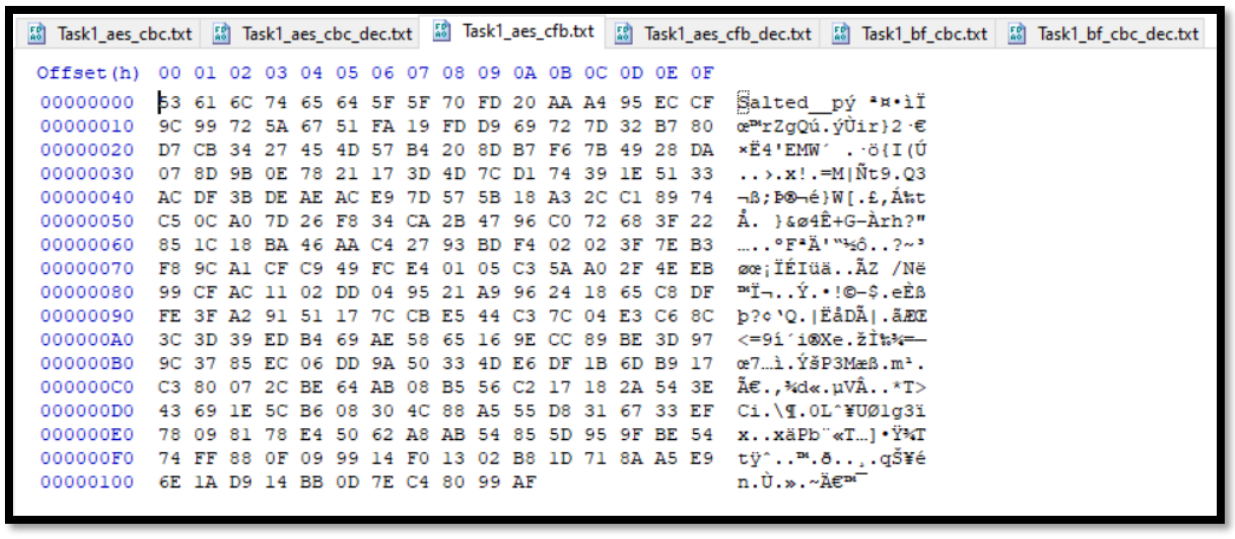
2) -aes-128-cfb Encryption

```
OpenSSL> enc -aes-128-cfb -e -in Task1.txt -out Task1_aes_cfb.txt -k 1234abcd -iv 1234567890
OpenSSL>
```



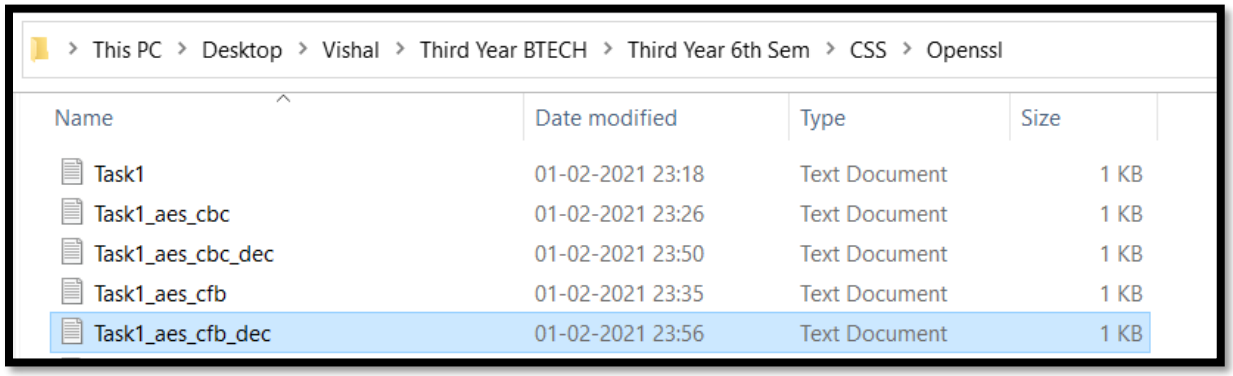


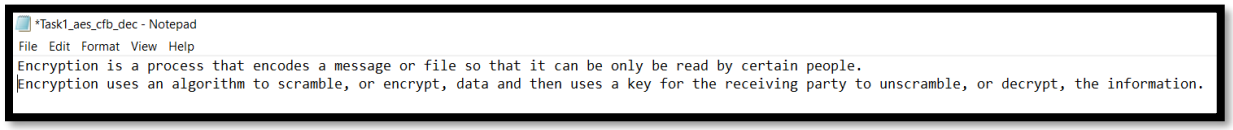


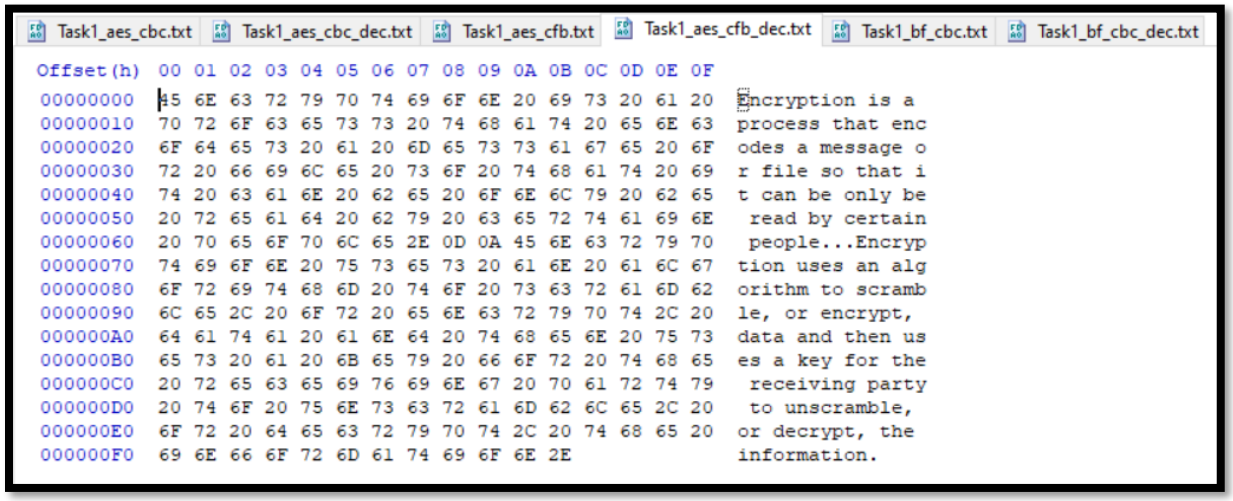


Decryption:

```
OpenSSL> enc -aes-128-cfb -d -in Task1_aes_cfb.txt -out Task1_aes_cfb_dec.txt -k 1234abcd -iv 1234567890
OpenSSL>
```

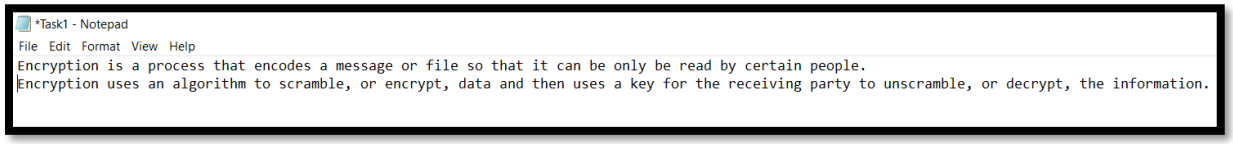


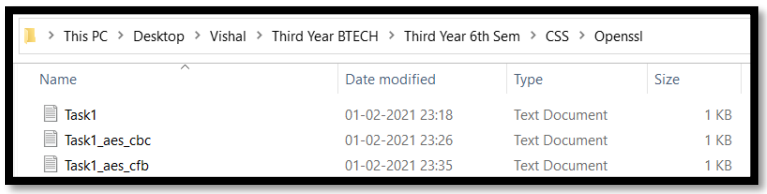


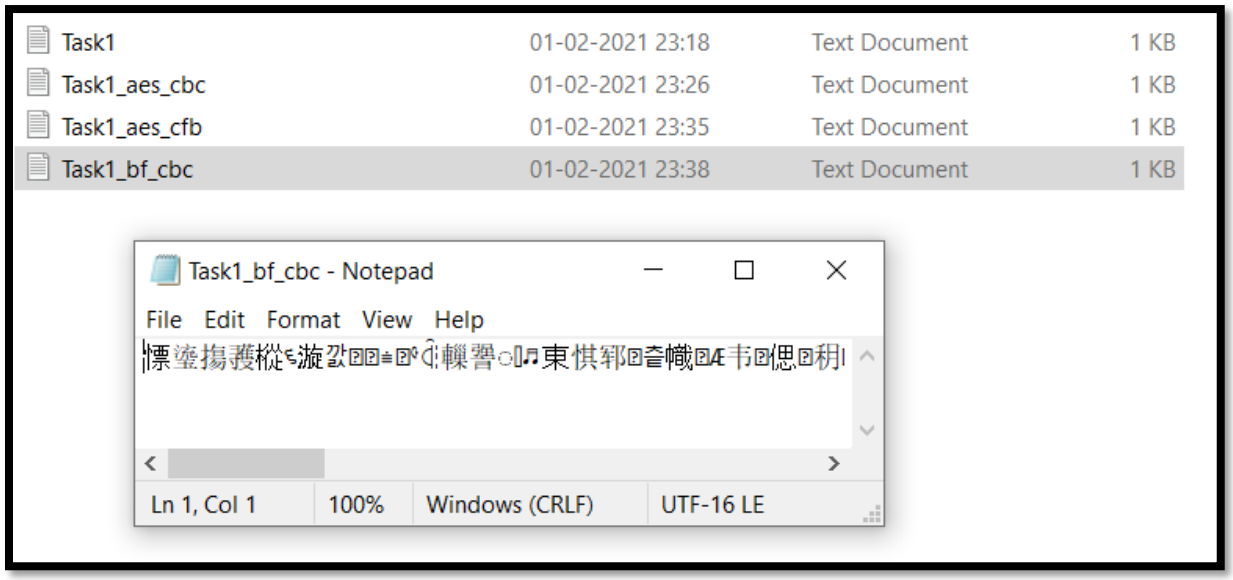


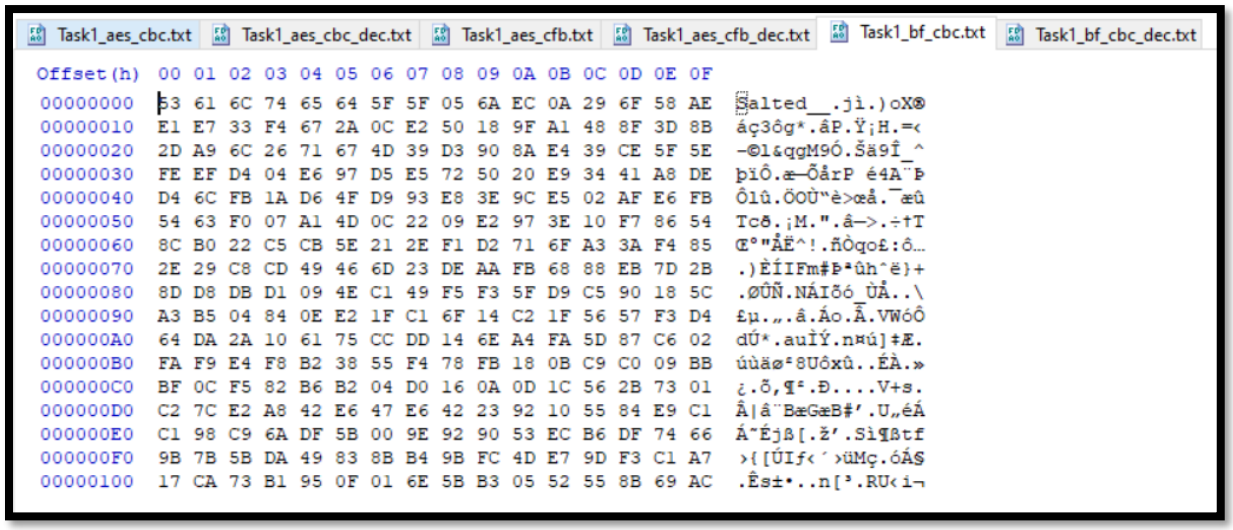
3)-bf_cbc Encryption:

```
OpenSSL> enc -bf-cbc -e -in Task1.txt -out Task1_bf_cbc.txt -k 1234abcd -iv 1234567890
OpenSSL>
```



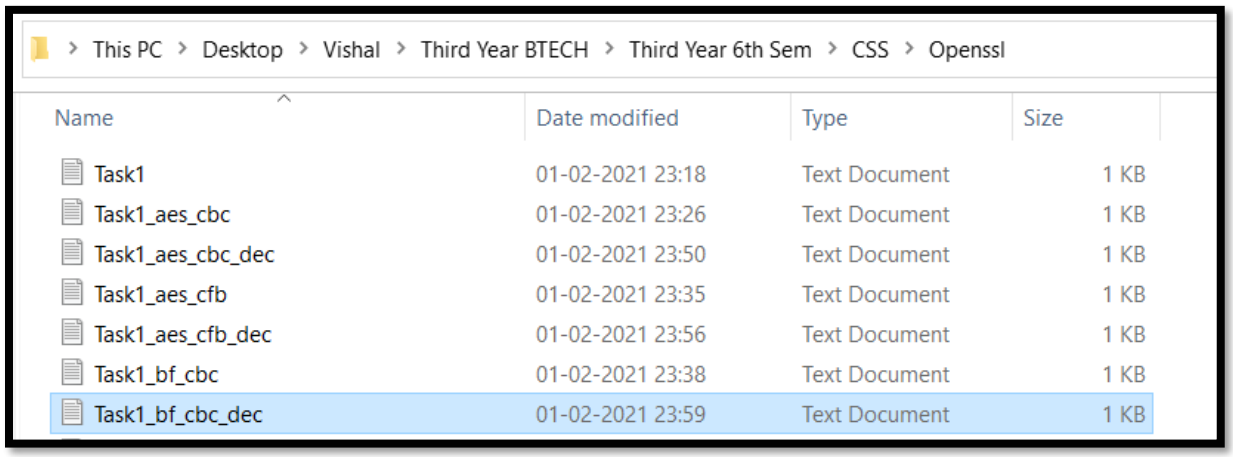


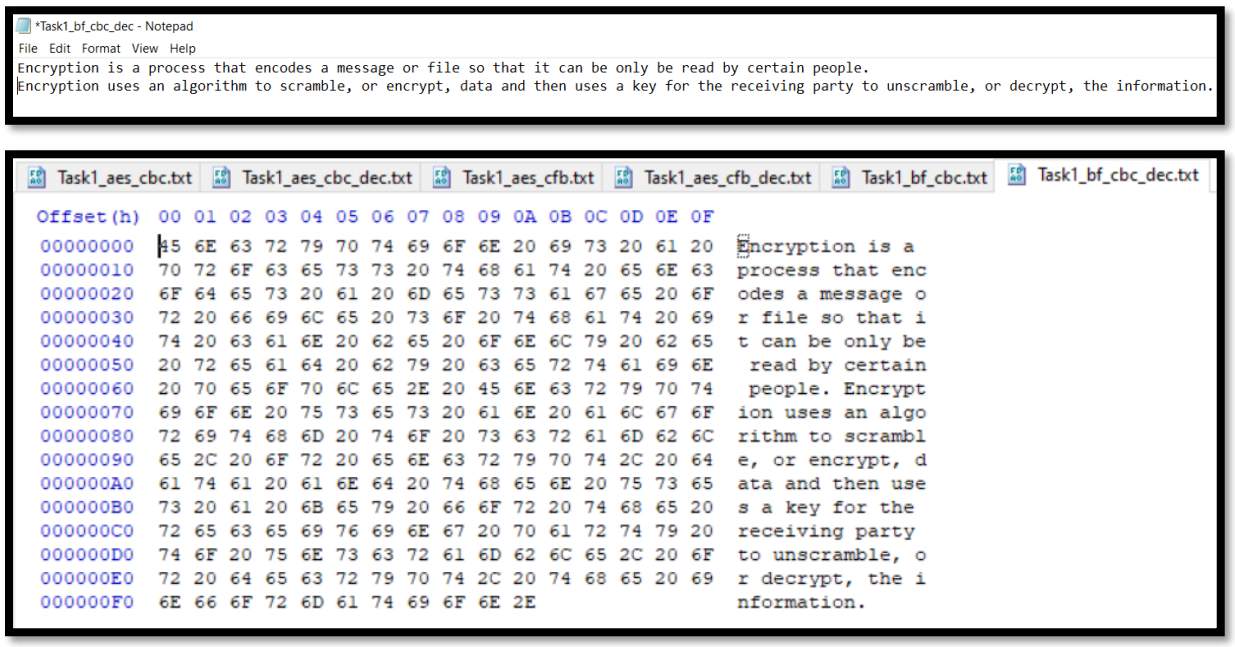




Decryption:

```
OpenSSL> enc -bf-cbc -d -in Task1_bf_cbc.txt -out Task1_bf_cbc_dec.txt -k 1234abcd -iv 1234567890
OpenSSL>
```





3.2 Task 2: Encryption Mode – ECB vs. CBC

The file pic original.bmp contains a simple picture. We would like to encrypt this picture, so people without the encryption keys cannot know what is in the picture. Please encrypt the file using the ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes, and then do the following:

1. Let us treat the encrypted picture as a picture, and use a picture viewing software to display it. However, For the .bmp file, the first 54 bytes contain the header information about the picture, we have to set it correctly, so the encrypted file can be treated as a legitimate .bmp file. We will replace the header of the encrypted picture with that of the original picture. You can use the ghex tool to directly modify binary files.

2. Display the encrypted picture using any picture viewing software. Can you derive any useful infor-mation about the original picture from the encrypted picture? Please explain your observations.

Task 2:

original1.bmp | original1_enc_cbc.bmp | original1_enc_ecb.bmp

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   FF D8 FF DB 00 84 00 03 02 02 03 02 02 03 03 03  ÿØÿÛ.„..........
00000010   03 04 03 03 04 05 08 05 05 04 04 05 0A 07 07 06  ................
00000020   08 0C 0A 0C 0C 0B 0A 0B 0B 0D 0E 12 10 0D 0E 11  ................
00000030   0E 0B 0B 10 16 10 11 13 14 15 15 15 0C 0F 17 18  ................
00000040   16 14 18 12 14 15 14 01 03 04 04 05 04 05 09 05  ................
00000050   05 09 14 0D 0B 0D 14 14 14 14 14 14 14 14 14 14  ................
00000060   14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14  ................
00000070   14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14  ................
00000080   14 14 14 14 14 14 14 14 FF C0 00 11 08 00 86 01  ........ÿÀ....†.
00000090   CC 03 01 22 00 02 11 01 03 11 01 FF C4 01 A2 00  Ì.."........ÿÄ.¢.
000000A0   00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00  ................
000000B0   00 01 02 03 04 05 06 07 08 09 0A 0B 10 00 02 01  ................
000000C0   03 03 02 04 03 05 05 04 04 00 00 01 7D 01 02 03  ............}...
000000D0   00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14  .....!1A..Qa."q.
000000E0   32 81 91 A1 08 23 42 B1 C1 15 52 D1 F0 24 33 62  2.'¡.#B±Á.RÑð$3b
000000F0   72 82 09 0A 16 17 18 19 1A 25 26 27 28 29 2A 34  r,.......%&'()*4
00000100   35 36 37 38 39 3A 43 44 45 46 47 48 49 4A 53 54  56789:CDEFGHIJST
00000110   55 56 57 58 59 5A 63 64 65 66 67 68 69 6A 73 74  UVWXYZcdefghijst
00000120   75 76 77 78 79 7A 83 84 85 86 87 88 89 8A 92 93  uvwxyzƒ„…†‡ˆ‰Š'"
00000130   94 95 96 97 98 99 9A A2 A3 A4 A5 A6 A7 A8 A9 AA  "•—˜™š¢£¤¥¦§¨©ª
00000140   B2 B3 B4 B5 B6 B7 B8 B9 BA C2 C3 C4 C5 C6 C7 C8  ²³´µ¶·¸¹ºÂÃÄÅÆÇÈ
00000150   C9 CA D2 D3 D4 D5 D6 D7 D8 D9 DA E1 E2 E3 E4 E5  ÉÊÒÓÔÕÖ×ØÙÚáâãäå
00000160   E6 E7 E8 E9 EA F1 F2 F3 F4 F5 F6 F7 F8 F9 FA 01  æçèéêñòóôõö÷øùú.
00000170   00 03 01 01 01 01 01 01 01 01 01 00 00 00 00 00  ................
00000180   00 01 02 03 04 05 06 07 08 09 0A 0B 11 00 02 01  ................
00000190   02 04 04 03 04 07 05 04 04 00 01 02 77 00 01 02  ............w...
000001A0   03 11 04 05 21 31 06 12 41 51 07 61 71 13 22 32  ....!1..AQ.aq."2
000001B0   81 08 14 42 91 A1 B1 C1 09 23 33 52 F0 15 62 72  ...B'¡±Á.#3Rð.br
000001C0   D1 0A 16 24 34 E1 25 F1 17 18 19 1A 26 27 28 29  Ñ..$4á%ñ....&'()
000001D0   2A 35 36 37 38 39 3A 43 44 45 46 47 48 49 4A 53  *56789:CDEFGHIJS
000001E0   54 55 56 57 58 59 5A 63 64 65 66 67 68 69 6A 73  TUVWXYZcdefghijs
000001F0   74 75 76 77 78 79 7A 82 83 84 85 86 87 88 89 8A  tuvwxyz‚ƒ„…†‡ˆ‰Š
00000200   92 93 94 95 96 97 98 99 9A A2 A3 A4 A5 A6 A7 A8  '"•—˜™š¢£¤¥¦§¨
00000210   A9 AA B2 B3 B4 B5 B6 B7 B8 B9 BA C2 C3 C4 C5 C6  ©ª²³´µ¶·¸¹ºÂÃÄÅÆ
00000220   C7 C8 C9 CA D2 D3 D4 D5 D6 D7 D8 D9 DA E2 E3 E4  ÇÈÉÊÒÓÔÕÖ×ØÙÚâãä
00000230   E5 E6 E7 E8 E9 EA F2 F3 F4 F5 F6 F7 F8 F9 FA FF  åæçèéêòóôõö÷øùúÿ
```

```
OpenSSL> enc -aes-128-ecb -e -in original1.bmp -out original1_enc_ecb.bmp -k 1234abcd -iv 1234567890
```

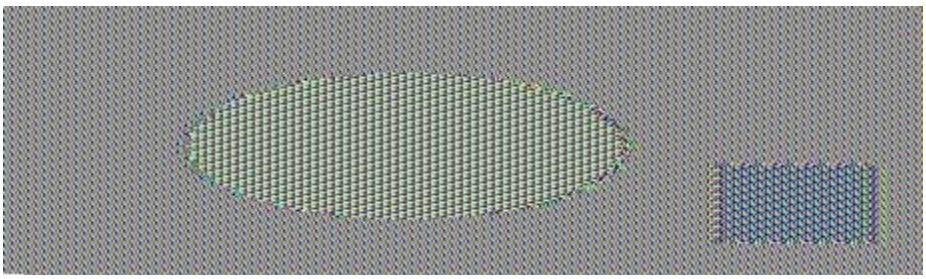
original1	11-02-2021 23:42	BMP File	7 KB
original1_enc_cbc	11-02-2021 23:50	BMP File	7 KB
original1_enc_cbc.bmp.bak	11-02-2021 23:46	BAK File	7 KB
original1_enc_ecb	11-02-2021 23:51	BMP File	7 KB
original1_enc_ecb.bmp.bak	11-02-2021 23:46	BAK File	7 KB

original1.bmp | original1_enc_cbc.bmp | original1_enc_ecb.bmp

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   53 61 6C 74 65 64 5F 5F 92 9B C2 AA 5B 16 F1 38  Salted__'›Âª[.ñ8
00000010   8E BB E3 B4 B6 26 DB D2 6C 19 30 0D 03 5C A0 BC  Ž»ã´¶&ÛÒl.0..\ ¼
00000020   E2 24 6F 6B 24 03 A1 A2 B6 66 C0 A4 45 55 CB 5C  â$ok$.¡¢¶fÀ¤EUË\
00000030   66 97 64 AE 24 D7 36 7D 53 FD 43 55 14 6C 23 6D  f—d®$×6}SýCU.l#m
00000040   2D 4B 74 2E 18 E1 9C C7 A6 B0 57 4F 38 49 B5 3B  -Kt..áœÇ¦°WO8Iµ;
00000050   4E 96 7A E6 58 19 2E 2D 03 2D 4A 80 0A C8 DD CF  N–zæX..-.-J€.ÈÝÏ
00000060   F8 D1 63 35 30 96 AC 26 24 E9 56 55 6E E5 CC A2  øÑc50–¬&$éVUnåÌ¢
00000070   02 2E CF 33 B2 37 BF 07 2F A1 23 AC 4A 89 B1 87  ..Ï3²7¿./¡#¬J‰±‡
00000080   02 2E CF 33 B2 37 BF 07 2F A1 23 AC 4A 89 B1 87  ..Ï3²7¿./¡#¬J‰±‡
00000090   B6 BB 5A 40 09 3D 11 16 27 ED 4D 66 20 BC 18 C5  ¶»Z@.=..'íMf ¼.Å
000000A0   C2 66 4D 01 EC 90 85 DC A1 7F 82 88 C2 C1 18 77  ÂfM.ì.…Ü¡.‚ˆÂÁ.w
000000B0   0A 05 5C F7 0E E5 83 5C 11 4A 8C 75 99 A1 03 20  ..\÷.åƒ\.JŒu™¡.
000000C0   C9 0E 7F F5 E9 4F B0 34 B9 E7 01 CD 32 BE F0 FE  É..õéO°4¹ç.Í2¾ðþ
000000D0   88 C7 B2 03 69 7F 2E 28 C2 7C DC 52 A9 E4 FE 10  ˆÇ².i..(Â|ÜR©äþ.
000000E0   48 C5 D7 92 43 09 58 A4 3B E7 9C B9 E4 B5 3E 26  HÅ×'C.X¤;çœ¹äµ>&
000000F0   9C DD 5E 26 A5 76 23 8F 56 C7 82 70 AB B3 73 1D  œÝ^&¥v#.VÇ‚p«³s.
```

original1.bmp | original1_enc_cbc.bmp | original1_enc_ecb.bmp

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   FF D8 FF DB 00 84 00 03 02 02 03 02 02 03 03 03  ÿØÿÛ.„..........
00000010   03 04 03 03 04 05 08 05 05 04 04 05 0A 07 07 06  ................
00000020   08 0C 0A 0C 0C 0B 0A 0B 0B 0D 0E 12 10 0D 0E 11  ................
00000030   0E 0B 0B 10 16 10 36 7D 53 FD 43 55 14 6C 23 6D  ......6}SýCU.l#m
00000040   2D 4B 74 2E 18 E1 9C C7 A6 B0 57 4F 38 49 B5 3B  -Kt..áœÇ¦°WO8Iµ;
00000050   4E 96 7A E6 58 19 2E 2D 03 2D 4A 80 0A C8 DD CF  N–zæX..-.-J€.ÈÝÏ
00000060   F8 D1 63 35 30 96 AC 26 24 E9 56 55 6E E5 CC A2  øÑc50–¬&$éVUnåÌ¢
00000070   02 2E CF 33 B2 37 BF 07 2F A1 23 AC 4A 89 B1 87  ..Ï3²7¿./¡#¬J‰±‡
00000080   02 2E CF 33 B2 37 BF 07 2F A1 23 AC 4A 89 B1 87  ..Ï3²7¿./¡#¬J‰±‡
00000090   B6 BB 5A 40 09 3D 11 16 27 ED 4D 66 20 BC 18 C5  ¶»Z@.=..'íMf ¼.Å
000000A0   C2 66 4D 01 EC 90 85 DC A1 7F 82 88 C2 C1 18 77  ÂfM.ì.…Ü¡.‚ˆÂÁ.w
```



```
OpenSSL> enc -aes-128-cbc -e -in original1.bmp -out original1_enc_cbc.bmp -k 1234abcd -iv 1234567890
OpenSSL>
```

original1	11-02-2021 23:42	BMP File	7 KB
original1_enc_cbc	11-02-2021 23:50	BMP File	7 KB
original1_enc_cbc.bmp.bak	11-02-2021 23:46	BAK File	7 KB

original1.bmp | original1_enc_cbc.bmp | original1_enc_ecb.bmp

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  53 61 6C 74 65 64 5F 5F 88 B3 C8 B0 1C D5 65 D7  Salted__ˆ³È°.Õe×
00000010  21 3B 02 27 AF DD 8F E6 5A 8C 1C F2 EE B9 28 A3  !;.'¯Ý.æZŒ.òî¹(£
00000020  04 45 31 43 70 79 C0 53 97 F4 7F FE 50 57 AE 41  .E1CpyÀS—ô.þPW®A
00000030  AB 0B E3 8A 73 77 84 0E D6 E9 96 14 DA 7E 6B 72  «.ãŠsw„.Öé–.Ú~kr
00000040  CB 01 8B DE EA 55 DE 50 58 9C D4 D8 E0 43 99 B4  Ë.‹ÞêUÞPXœÔØàC™´
00000050  E8 89 8E 8D ED 1C C1 A9 E6 10 22 08 DE 15 6D 12  è‰Ž.í.Á©æ.".Þ.m.
00000060  BC 83 35 D3 66 24 CE 0B D9 D1 11 35 B6 28 44 78  ¼ƒ5Óf$Î.ÙÑ.5¶(Dx
00000070  0B BD B4 15 4F 21 CC 8F 09 8B F6 64 23 16 FE 02  .½´.O!Ì..‹öd#.þ.
00000080  3F E9 A8 03 AA 23 E2 D3 7B 8E 40 66 30 E3 8A 46  ?é¨.ª#âÓ{Ž@f0ãŠF
00000090  8E 69 DB 1D 8D 0C 2B 64 0D C5 3F AE D1 05 30 F9  ŽiÛ...+d.Å?®Ñ.0ù
000000A0  79 A0 48 30 41 C2 AD EC 97 A6 C2 90 F3 73 F7 DF  y H0AÂ.ì—¦Â.ós÷ß
000000B0  C4 43 C6 1B BA CF 6C 26 B5 FF E1 C0 06 85 43 2B  ÄCÆ.ºÏl&µÿáÀ.…C+
000000C0  7D 32 80 DE FD 58 30 A2 E0 B8 1D AD 4A 6E 34 69  }2€ÞýX0¢à¸..Jn4i
000000D0  25 96 98 88 81 B4 03 44 7F D7 B0 C8 BF D5 2C AE  %–˜ˆ.´.D.×°È¿Õ,®
000000E0  11 32 1D 33 9C A1 9E 61 43 BE 21 9C 1C DE 58 C8  .2.3œ¡žaC¾!œ.ÞXÈ
000000F0  14 06 AE CD 62 EE 1C C0 7E 8D E7 6A 2C EE 85 94  ..®Íbî.À~.çj,î…"
```

original1.bmp | original1_enc_cbc.bmp | original1_enc_ecb.bmp

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  FF D8 FF DB 00 84 00 03 02 02 03 02 02 03 03 03  ÿØÿÛ.„..........
00000010  03 04 03 03 04 05 08 05 05 04 04 05 0A 07 07 06  ................
00000020  08 0C 0A 0C 0C 0B 0A 0B 0B 0D 0E 12 10 0D 0E 11  ................
00000030  0E 0B 0B 10 16 10 B4 0E D6 E9 96 14 DA 7E 6B 72  ......´.Öé–.Ú~kr
00000040  CB 01 8B DE EA 55 DE 50 58 9C D4 D8 E0 43 99 B4  Ë.‹ÞêUÞPXœÔØàC™´
00000050  E8 89 8E 8D ED 1C C1 A9 E6 10 22 08 DE 15 6D 12  è‰Ž.í.Á©æ.".Þ.m.
00000060  BC 83 35 D3 66 24 CE 0B D9 D1 11 35 B6 28 44 78  ¼ƒ5Óf$Î.ÙÑ.5¶(Dx
00000070  0B BD B4 15 4F 21 CC 8F 09 8B F6 64 23 16 FE 02  .½´.O!Ì..‹öd#.þ.
00000080  3F E9 A8 03 AA 23 E2 D3 7B 8E 40 66 30 E3 8A 46  ?é¨.ª#âÓ{Ž@f0ãŠF
00000090  8E 69 DB 1D 8D 0C 2B 64 0D C5 3F AE D1 05 30 F9  ŽiÛ...+d.Å?®Ñ.0ù
000000A0  79 A0 48 30 41 C2 AD EC 97 A6 C2 90 F3 73 F7 DF  y H0AÂ.ì—¦Â.ós÷ß
000000B0  C4 43 C6 1B BA CF 6C 26 B5 FF E1 C0 06 85 43 2B  ÄCÆ.ºÏl&µÿáÀ.…C+
000000C0  7D 32 80 DE FD 58 30 A2 E0 B8 1D AD 4A 6E 34 69  }2€ÞýX0¢à¸..Jn4i
000000D0  25 96 98 88 81 B4 03 44 7F D7 B0 C8 BF D5 2C AE  %–˜ˆ.´.D.×°È¿Õ,®
```

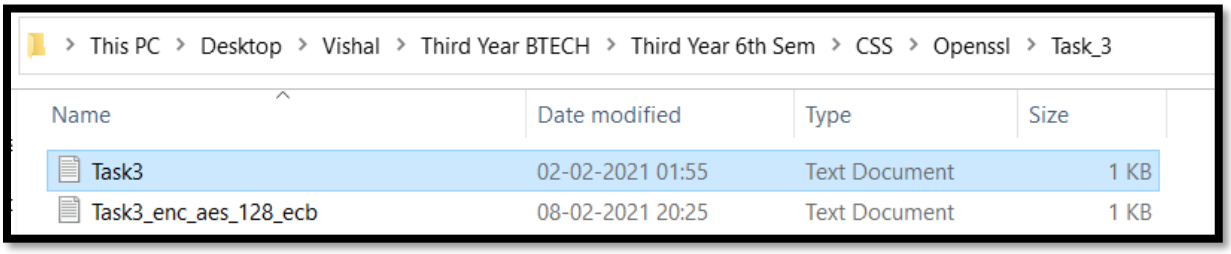
3.3 Task 3: Encryption Mode – Corrupted Cipher Text

To understand the properties of various encryption modes, we would like to do the following exercise:

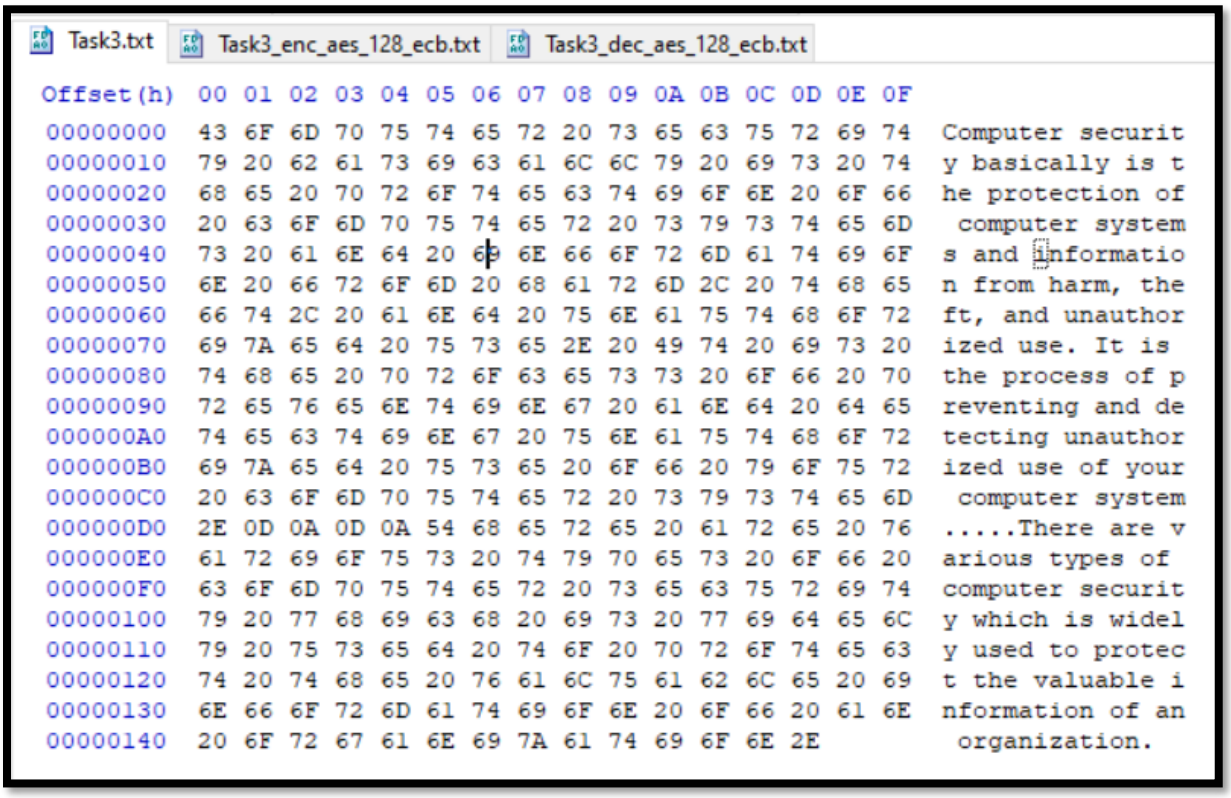
1. Create a text file that is at least 64 bytes long.
2. Encrypt the file using the AES-128 cipher.
3. Unfortunately, a single bit of the 30th byte in the encrypted file got corrupted. You can achieve this corruption using ghex.
4. Decrypt the corrupted file (encrypted) using the correct key and IV.

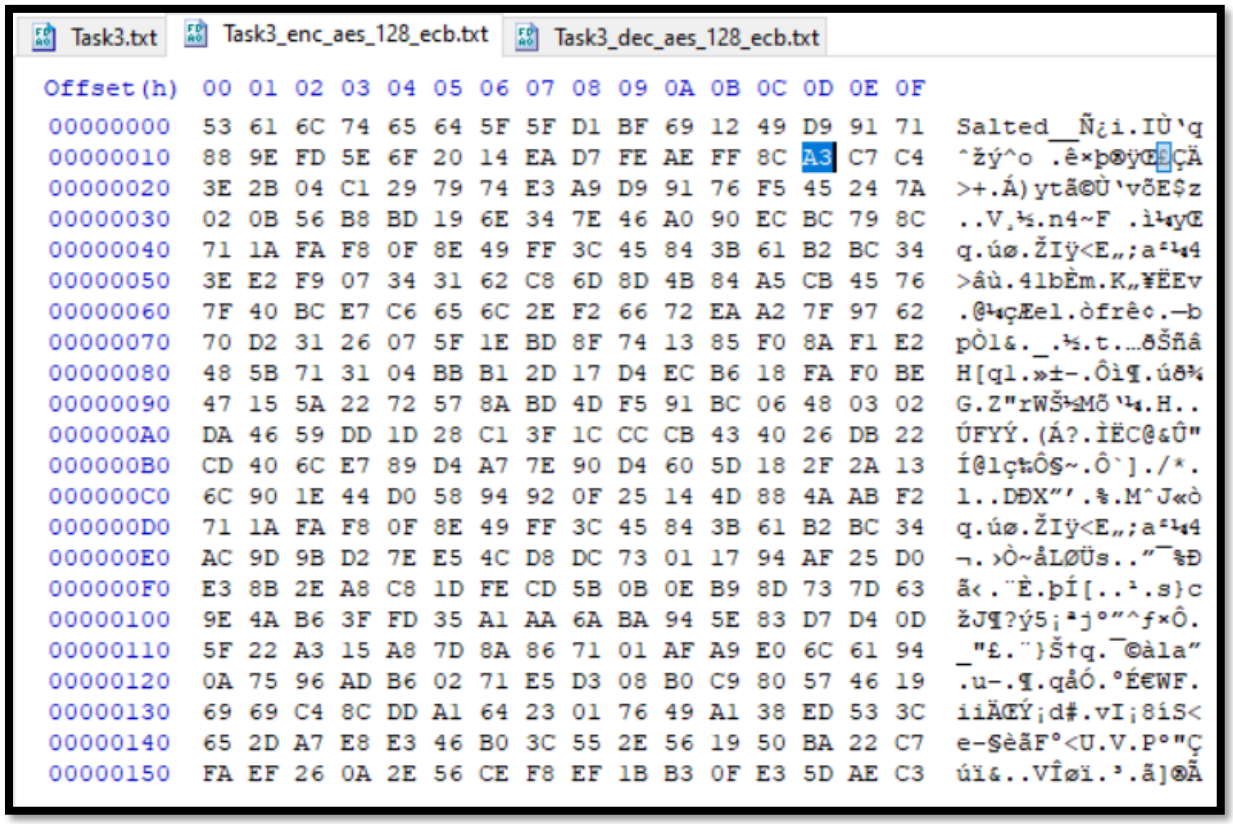
Please answer the following questions: (1) How much information can you recover by decrypting the corrupted file, if the encryption mode is ECB, CBC, CFB, or OFB, respectively? Please answer this question before you conduct this task, and then find out whether your answer is correct or wrong after you finish this task.
(2) Please explain why. (3) What are the implication of these differences?

Task3 :
Encryption mode – ECB




```
OpenSSL> enc -aes-128-ecb -e -in Task3.txt -out Task3_enc_aes_128_ecb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
```

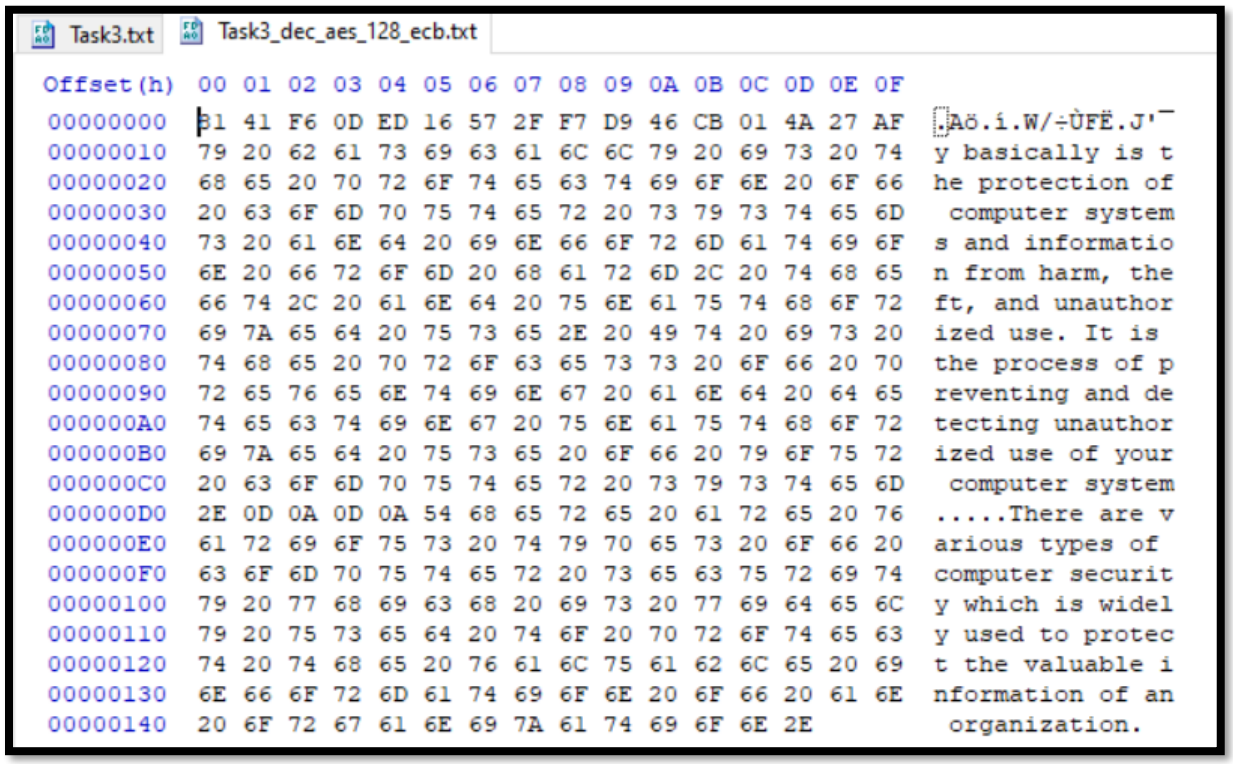




Task3.txt | Task3_enc_aes_128_ecb.txt | Task3_dec_aes_128_ecb.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   53 61 6C 74 65 64 5F 5F D1 BF 69 12 49 D9 91 71  Salted__Ñ¿i.IÙ'q
00000010   88 9E FD 5E 6F 20 14 EA D7 FE AE FF 8C A3 C7 C4  ^žý^o .ê×þ®ÿŒ£ÇÄ
00000020   3E 2B 04 C1 29 79 74 E3 A9 D9 91 76 F5 45 24 7A  >+.Á)ytã©Ù'võE$z
00000030   02 0B 56 B8 BD 19 6E 34 7E 46 A0 90 EC BC 79 8C  ..V¸½.n4~F .ì¼yŒ
00000040   71 1A FA F8 0F 8E 49 FF 3C 45 84 3B 61 B2 BC 34  q.úø.ŽIÿ<E„;a²¼4
00000050   3E E2 F9 07 34 31 62 C8 6D 8D 4B 84 A5 CB 45 76  >âù.41bÈm.K„¥ËEv
00000060   7F 40 BC E7 C6 65 6C 2E F2 66 72 EA A2 7F 97 62  .@¼çÆel.òfrê¢.—b
00000070   70 D2 31 26 07 5F 1E BD 8F 74 13 85 F0 8A F1 E2  pÒ1&._.½.t.…ðŠñâ
00000080   48 5B 71 31 04 BB B1 2D 17 D4 EC B6 18 FA F0 BE  H[q1.»±-.Ôì¶.úð¾
00000090   47 15 5A 22 72 57 8A BD 4D F5 91 BC 06 48 03 02  G.Z"rWŠ½Mõ'¼.H..
000000A0   DA 46 59 DD 1D 28 C1 3F 1C CC CB 43 40 26 DB 22  ÚFYÝ.(Á?.ÌËC@&Û"
000000B0   CD 40 6C E7 89 D4 A7 7E 90 D4 60 5D 18 2F 2A 13  Í@lç‰Ô§~.Ô`]./*.
000000C0   6C 90 1E 44 D0 58 94 92 0F 25 14 4D 88 4A AB F2  l..DÐX"'.%.MˆJ«ò
000000D0   71 1A FA F8 0F 8E 49 FF 3C 45 84 3B 61 B2 BC 34  q.úø.ŽIÿ<E„;a²¼4
000000E0   AC 9D 9B D2 7E E5 4C D8 DC 73 01 17 94 AF 25 D0  ¬.›Ò~åLØÜs..”¯%Ð
000000F0   E3 8B 2E A8 C8 1D FE CD 5B 0B 0E B9 8D 73 7D 63  ã‹.¨È.þÍ[..¹.s}c
00000100   9E 4A B6 3F FD 35 A1 AA 6A BA 94 5E 83 D7 D4 0D  žJ¶?ý5¡ªjº"^ƒ×Ô.
00000110   5F 22 A3 15 A8 7D 8A 86 71 01 AF A9 E0 6C 61 94  _"£.¨}Š†q.¯©àla"
00000120   0A 75 96 AD B6 02 71 E5 D3 08 B0 C9 80 57 46 19  .u-.¶.qåÓ.°É€WF.
00000130   69 69 C4 8C DD A1 64 23 01 76 49 A1 38 ED 53 3C  iiÄŒÝ¡d#.vI¡8íS<
00000140   65 2D A7 E8 E3 46 B0 3C 55 2E 56 19 50 BA 22 C7  e-§èãF°<U.V.Pº"Ç
00000150   FA EF 26 0A 2E 56 CE F8 EF 1B B3 0F E3 5D AE C3  úï&..VÎøï.³.ã]®Ã
```

```
OpenSSL> enc -aes-128-ecb -d -in Task3_enc_aes_128_ecb.txt -out Task3_dec_aes_128_ecb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
OpenSSL>
```

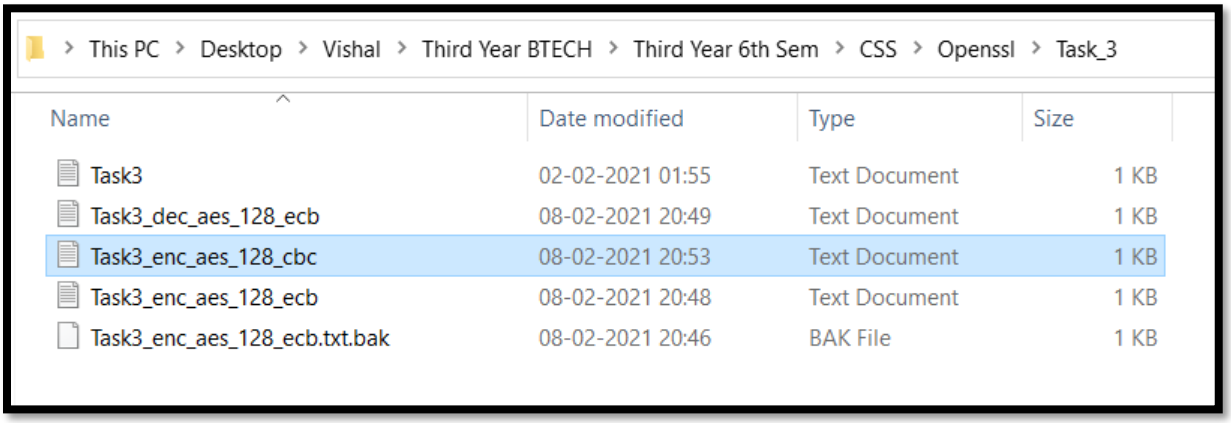


Task3.txt | Task3_dec_aes_128_ecb.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   31 41 F6 0D ED 16 57 2F F7 D9 46 CB 01 4A 27 AF  1Aö.í.W/÷ÙFË.J'¯
00000010   79 20 62 61 73 69 63 61 6C 6C 79 20 69 73 20 74  y basically is t
00000020   68 65 20 70 72 6F 74 65 63 74 69 6F 6E 20 6F 66  he protection of
00000030   20 63 6F 6D 70 75 74 65 72 20 73 79 73 74 65 6D   computer system
00000040   73 20 61 6E 64 20 69 6E 66 6F 72 6D 61 74 69 6F  s and informatio
00000050   6E 20 66 72 6F 6D 20 68 61 72 6D 2C 20 74 68 65  n from harm, the
00000060   66 74 2C 20 61 6E 64 20 75 6E 61 75 74 68 6F 72  ft, and unauthor
00000070   69 7A 65 64 20 75 73 65 2E 20 49 74 20 69 73 20  ized use. It is
00000080   74 68 65 20 70 72 6F 63 65 73 73 20 6F 66 20 70  the process of p
00000090   72 65 76 65 6E 74 69 6E 67 20 61 6E 64 20 64 65  reventing and de
000000A0   74 65 63 74 69 6E 67 20 75 6E 61 75 74 68 6F 72  tecting unauthor
000000B0   69 7A 65 64 20 75 73 65 20 6F 66 20 79 6F 75 72  ized use of your
000000C0   20 63 6F 6D 70 75 74 65 72 20 73 79 73 74 65 6D   computer system
000000D0   2E 0D 0A 0D 0A 54 68 65 72 65 20 61 72 65 20 76  .....There are v
000000E0   61 72 69 6F 75 73 20 74 79 70 65 73 20 6F 66 20  arious types of
000000F0   63 6F 6D 70 75 74 65 72 20 73 65 63 75 72 69 74  computer securit
00000100   79 20 77 68 69 63 68 20 69 73 20 77 69 64 65 6C  y which is widel
00000110   79 20 75 73 65 64 20 74 6F 20 70 72 6F 74 65 63  y used to protec
00000120   74 20 74 68 65 20 76 61 6C 75 61 62 6C 65 20 69  t the valuable i
00000130   6E 66 6F 72 6D 61 74 69 6F 6E 20 6F 66 20 61 6E  nformation of an
00000140   20 6F 72 67 61 6E 69 7A 61 74 69 6F 6E 2E          organization.
```

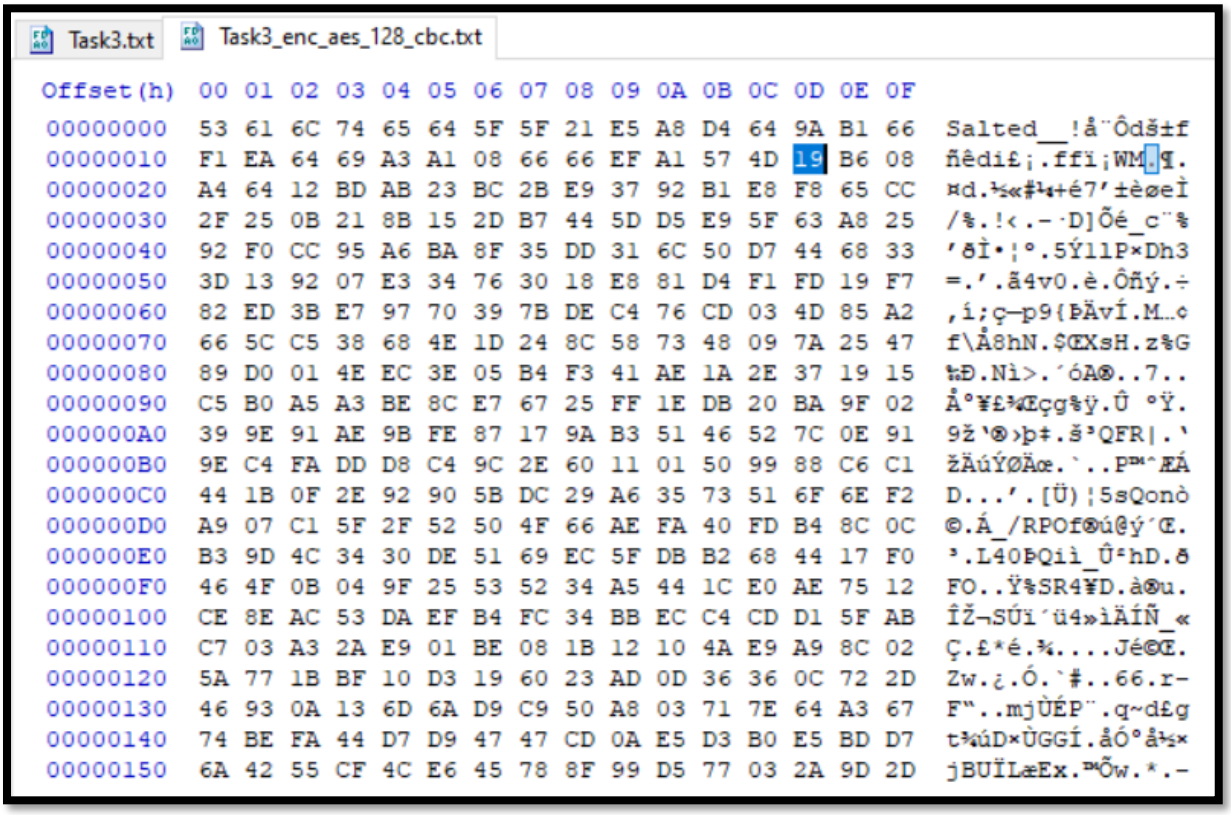
Encryption mode – CBC

```
OpenSSL> enc -aes-128-cbc -e -in Task3.txt -out Task3_enc_aes_128_cbc.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```



This PC › Desktop › Vishal › Third Year BTECH › Third Year 6th Sem › CSS › Openssl › Task_3

Name	Date modified	Type	Size
Task3	02-02-2021 01:55	Text Document	1 KB
Task3_dec_aes_128_ecb	08-02-2021 20:49	Text Document	1 KB
Task3_enc_aes_128_cbc	08-02-2021 20:53	Text Document	1 KB
Task3_enc_aes_128_ecb	08-02-2021 20:48	Text Document	1 KB
Task3_enc_aes_128_ecb.txt.bak	08-02-2021 20:46	BAK File	1 KB



Task3.txt | Task3_enc_aes_128_cbc.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   53 61 6C 74 65 64 5F 5F 21 E5 A8 D4 64 9A B1 66  Salted__!å¨Ôdš±f
00000010   F1 EA 64 69 A3 A1 08 66 66 EF A1 57 4D 19 B6 08  ñêdi£¡.ffï¡WM.¶.
00000020   A4 64 12 BD AB 23 BC 2B E9 37 92 B1 E8 F8 65 CC  ¤d.½«#¼+é7'±èøeÌ
00000030   2F 25 0B 21 8B 15 2D B7 44 5D D5 E9 5F 63 A8 25  /%.!‹.-·D]Õé_c¨%
00000040   92 F0 CC 95 A6 BA 8F 35 DD 31 6C 50 D7 44 68 33  'ðÌ•¦º.5Ý1lP×Dh3
00000050   3D 13 92 07 E3 34 76 30 18 E8 81 D4 F1 FD 19 F7  =.'.ã4v0.è.Ôñý.÷
00000060   82 ED 3B E7 97 70 39 7B DE C4 76 CD 03 4D 85 A2  ‚í;ç—p9{ÞÄvÍ.M…¢
00000070   66 5C C5 38 68 4E 1D 24 8C 58 73 48 09 7A 25 47  f\Å8hN.$ŒXsH.z%G
00000080   89 D0 01 4E EC 3E 05 B4 F3 41 AE 1A 2E 37 19 15  ‰Ð.Nì>.´óA®..7..
00000090   C5 B0 A5 A3 BE 8C E7 67 25 FF 1E DB 20 BA 9F 02  Å°¥£¾Œçg%ÿ.Û º.
000000A0   39 9E 91 AE 9B FE 87 17 9A B3 51 46 52 7C 0E 91  9ž'®›þ‡.š³QFR|.'
000000B0   9E C4 FA DD D8 C4 9C 2E 60 11 01 50 99 88 C6 C1  žÄúÝØÄœ.`..P™ˆÆÁ
000000C0   44 1B 0F 2E 92 90 5B DC 29 A6 35 73 51 6F 6E F2  D...'.[Ü)¦5sQonò
000000D0   A9 07 C1 5F 2F 52 50 4F 66 AE FA 40 FD B4 8C 0C  ©.Á_/RPOf®ú@ý´Œ.
000000E0   B3 9D 4C 34 30 DE 51 69 EC 5F DB B2 68 44 17 F0  ³.L40ÞQiì_Û²hD.ð
000000F0   46 4F 0B 04 9F 25 53 52 34 A5 44 1C E0 AE 75 12  FO..Ÿ%SR4¥D.à®u.
00000100   CE 8E AC 53 DA EF B4 FC 34 BB EC C4 CD D1 5F AB  ÎŽ¬SÚï´ü4»ìÄÍÑ_«
00000110   C7 03 A3 2A E9 01 BE 08 1B 12 10 4A E9 A9 8C 02  Ç.£*é.¾....Jé©Œ.
00000120   5A 77 1B BF 10 D3 19 60 23 AD 0D 36 36 0C 72 2D  Zw.¿.Ó.`#..66.r-
00000130   46 93 0A 13 6D 6A D9 C9 50 A8 03 71 7E 64 A3 67  F"..mjÙÉP¨.q~d£g
00000140   74 BE FA 44 D7 D9 47 47 CD 0A E5 D3 B0 E5 BD D7  t¾úD×ÙGGÍ.åÓ°å½×
00000150   6A 42 55 CF 4C E6 45 78 8F 99 D5 77 03 2A 9D 2D  jBUÏLæEx.™Õw.*.-
```

Task3.txt | Task3_enc_aes_128_cbc.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   53 61 6C 74 65 64 5F 5F 63 54 D5 C7 FF D2 45 4C  Salted__cTÕÇÿÒEL
00000010   C7 D9 DF A3 81 2B ED 63 0A 2B 99 83 22 34 2C E2  ÇÙß£.+íc.+™ƒ"4,â
00000020   65 2C 9D DB 6A F8 39 08 21 2F 01 6B 77 30 5C 6B  e,.Ûjø9.!/.kw0\k
00000030   4D E3 70 84 7D CB 46 F8 7A 76 9A D7 4D B4 71 DB  Mãp„}ËFøzvš×M´qÛ
00000040   C9 58 76 B6 DC 92 C9 6A 2B 9B 66 3D 19 D4 82 C0  ÉXv¶Ü'Éj+›f=.Ô‚À
00000050   7B 67 C7 D1 7E 45 44 B7 9B 9E 0D 12 3B BA B4 6A  {gÇÑ~ED·›ž..;º´j
00000060   FD 68 0F 9B 9E 5E AC 8B B9 9C 25 80 E6 F4 E3 D1  ýh.›ž^¬‹¹œ%€æôãÑ
00000070   00 8A A5 C4 66 65 FC 8A A9 4D 4F 7F B9 65 3C A0  .Š¥ÄfeüŠ©MO.¹e< 
00000080   75 B7 B9 95 B4 0D E2 75 84 2D 44 CF E5 08 94 BD  u·¹•´.âu„-DÏå.”½
00000090   09 AA F8 15 6F 6C 6B EA AC A3 03 12 CF A3 70 28  .ªø.olkê¬£..Ï£p(
000000A0   21 21 6A F9 2B A2 57 7B 8C D7 B1 C9 ED DD 66 8C  !!jù+¢W{Œ×±ÉíÝfŒ
000000B0   56 F4 BE 16 0B BE D1 0D 05 90 EF 0F CC 83 AD D2  Vô¾..¾Ñ...ï.Ìƒ.Ò
000000C0   1B 8F 40 A1 39 D9 38 9B 7E 45 83 45 DE EA A2 C2  ..@¡9Ù8›~EƒEÞê¢Â
000000D0   36 13 06 4A 7A 7E 50 46 B0 A7 9E 30 78 25 34 8E  6..Jz~PF°§ž0x%4Ž
000000E0   C4 27 C8 5C D5 BD 0B 11 B3 9A 17 BB 3E D6 B6 BF  Ä'È\Õ½..³š.»>Ö¶¿
000000F0   C8 44 05 3D 0F 86 E1 C3 5C A9 06 32 4A 7E 12 D0  ÈD.=.†áÃ\©.2J~.Ð
00000100   52 41 ED 3A E2 C3 D1 62 58 5F 01 DC 20 17 24 A5  RAí:âÃÑbX_.Ü .$¥
00000110   52 BA 5E D1 C5 AB 94 68 A2 0B 45 AC 98 5E B1 7C  R°^ÑÅ«”h¢.E¬˜^±|
00000120   5F A0 B6 FA A3 37 74 7E 0F 2C 20 F5 2D 30 00 A5  _ ¶ú£7t~., õ-0.¥
00000130   75 16 F7 51 34 82 EF FC 57 7F 62 01 5E EE AA 37  u.÷Q4‚ïüW.b.^îª7
00000140   56 8E 8A FC 20 14 D3 1D AF AA 6C 4A D7 9F 24 AC  VŽŠü .Ó.¯ªlJ×Ÿ$¬
00000150   6D 6D 1B F5 8E D2 44 C8 BD 7B D2 6C D1 0C 53 E0  mm.õŽÒDȽ{ÒlÑ.Sà
```

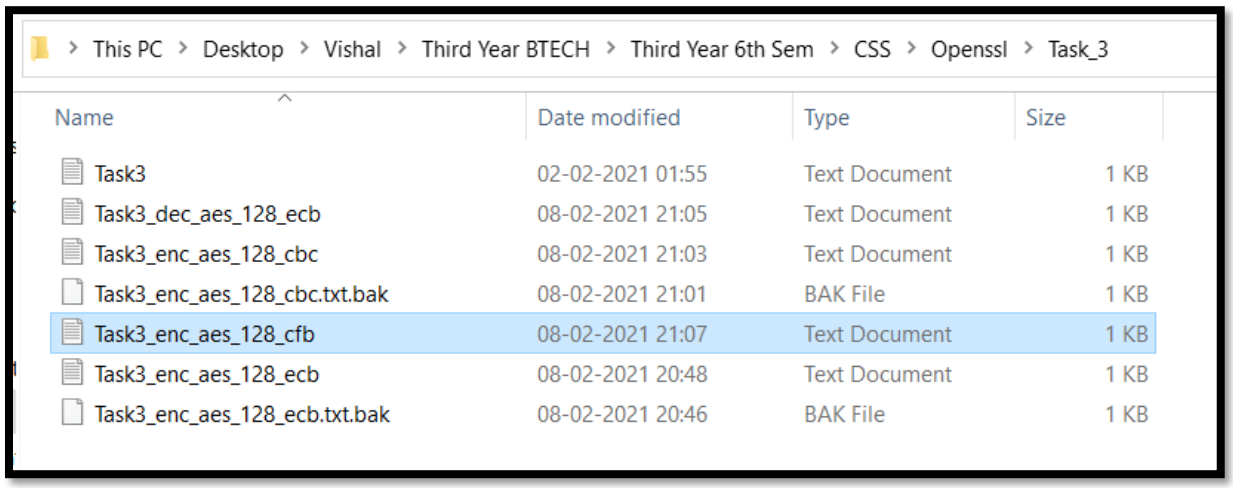
```
OpenSSL> enc -aes-128-cbc -d -in Task3_enc_aes_128_cbc.txt -out Task3_dec_aes_128_cbc.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```

Task3.txt | Task3_dec_aes_128_cbc.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   61 1A 9B FB 4B 25 49 50 1F C0 40 88 A7 DD 78 02  a.›ûK%IP.À@ˆ§Ýx.
00000010   79 20 62 61 73 69 63 61 6C 6C 79 20 69 53 20 74  y basically iS t
00000020   68 65 20 70 72 6F 74 65 63 74 69 6F 6E 20 6F 66  he protection of
00000030   20 63 6F 6D 70 75 74 65 72 20 73 79 73 74 65 6D   computer system
00000040   73 20 61 6E 64 20 69 6E 66 6F 72 6D 61 74 69 6F  s and informatio
00000050   6E 20 66 72 6F 6D 20 68 61 72 6D 2C 20 74 68 65  n from harm, the
00000060   66 74 2C 20 61 6E 64 20 75 6E 61 75 74 68 6F 72  ft, and unauthor
00000070   69 7A 65 64 20 75 73 65 2E 20 49 74 20 69 73 20  ized use. It is
00000080   74 68 65 20 70 72 6F 63 65 73 73 20 6F 66 20 70  the process of p
00000090   72 65 76 65 6E 74 69 6E 67 20 61 6E 64 20 64 65  reventing and de
000000A0   74 65 63 74 69 6E 67 20 75 6E 61 75 74 68 6F 72  tecting unauthor
000000B0   69 7A 65 64 20 75 73 65 20 6F 66 20 79 6F 75 72  ized use of your
000000C0   20 63 6F 6D 70 75 74 65 72 20 73 79 73 74 65 6D   computer system
000000D0   2E 0D 0A 0D 0A 54 68 65 72 65 20 61 72 65 20 76  .....There are v
000000E0   61 72 69 6F 75 73 20 74 79 70 65 73 20 6F 66 20  arious types of
000000F0   63 6F 6D 70 75 74 65 72 20 73 65 63 75 72 69 74  computer securit
00000100   79 20 77 68 69 63 68 20 69 73 20 77 69 64 65 6C  y which is widel
00000110   79 20 75 73 65 64 20 74 6F 20 70 72 6F 74 65 63  y used to protec
00000120   74 20 74 68 65 20 76 61 6C 75 61 62 6C 65 20 69  t the valuable i
00000130   6E 66 6F 72 6D 61 74 69 6F 6E 20 6F 66 20 61 6E  nformation of an
00000140   20 6F 72 67 61 6E 69 7A 61 74 69 6F 6E 2E         organization.
```

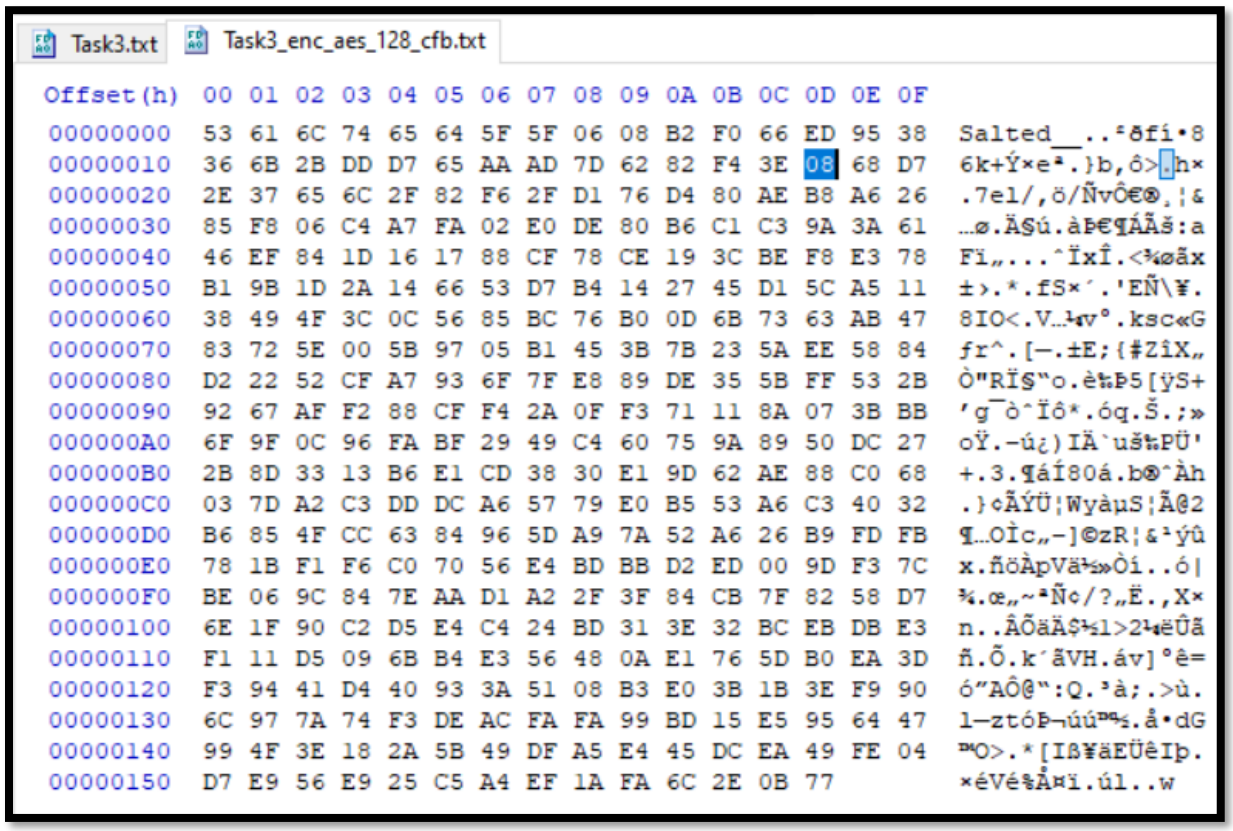
Encryption mode – CFB

```
OpenSSL> enc -aes-128-cfb -e -in Task3.txt -out Task3_enc_aes_128_cfb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```



This PC › Desktop › Vishal › Third Year BTECH › Third Year 6th Sem › CSS › Openssl › Task_3

Name	Date modified	Type	Size
Task3	02-02-2021 01:55	Text Document	1 KB
Task3_dec_aes_128_ecb	08-02-2021 21:05	Text Document	1 KB
Task3_enc_aes_128_cbc	08-02-2021 21:03	Text Document	1 KB
Task3_enc_aes_128_cbc.txt.bak	08-02-2021 21:01	BAK File	1 KB
Task3_enc_aes_128_cfb	08-02-2021 21:07	Text Document	1 KB
Task3_enc_aes_128_ecb	08-02-2021 20:48	Text Document	1 KB
Task3_enc_aes_128_ecb.txt.bak	08-02-2021 20:46	BAK File	1 KB



Task3.txt | Task3_enc_aes_128_cfb.txt

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	53	61	6C	74	65	64	5F	5F	06	08	B2	F0	66	ED	95	38	Salted__..²ðfí•8
00000010	36	6B	2B	DD	D7	65	AA	AD	7D	62	82	F4	3E	08	68	D7	6k+Ý×eª.}b,ô>.h×
00000020	2E	37	65	6C	2F	82	F6	2F	D1	76	D4	80	AE	B8	A6	26	.7el/,ö/ÑvÔ€®¸¦&
00000030	85	F8	06	C4	A7	FA	02	E0	DE	80	B6	C1	C3	9A	3A	61	…ø.Ä§ú.àÞ€¶ÁÃš:a
00000040	46	EF	84	1D	16	17	88	CF	78	CE	19	3C	BE	F8	E3	78	Fï„...ˆÏxÎ.<¾øãx
00000050	B1	9B	1D	2A	14	66	53	D7	B4	14	27	45	D1	5C	A5	11	±›.*.fS×´.'EÑ\¥.
00000060	38	49	4F	3C	0C	56	85	BC	76	B0	0D	6B	73	63	AB	47	8IO<.V…¼v°.ksc«G
00000070	83	72	5E	00	5B	97	05	B1	45	3B	7B	23	5A	EE	58	84	ƒr^.[—.±E;{#ZîX„
00000080	D2	22	52	CF	A7	93	6F	7F	E8	89	DE	35	5B	FF	53	2B	Ò"RÏ§"o.è‰Þ5[ÿS+
00000090	92	67	AF	F2	88	CF	F4	2A	0F	F3	71	11	8A	07	3B	BB	'g¯ò^Ïô*.óq.Š.;»
000000A0	6F	9F	0C	96	FA	BF	29	49	C4	60	75	9A	89	50	DC	27	oŸ.–ú¿)IÄ`uš‰PÜ'
000000B0	2B	8D	33	13	B6	E1	CD	38	30	E1	9D	62	AE	88	C0	68	+.3.¶áÍ80á.b®ˆÀh
000000C0	03	7D	A2	C3	DD	DC	A6	57	79	E0	B5	53	A6	C3	40	32	.}¢ÃÝÜ¦WyàµS¦Ã@2
000000D0	B6	85	4F	CC	63	84	96	5D	A9	7A	52	A6	26	B9	FD	FB	¶…OÌc„–]©zR¦&¹ýû
000000E0	78	1B	F1	F6	C0	70	56	E4	BD	BB	D2	ED	00	9D	F3	7C	x.ñöÀpVä½»Òí..ó|
000000F0	BE	06	9C	84	7E	AA	D1	A2	2F	3F	84	CB	7F	82	58	D7	¾.œ„~ªÑ¢/?„Ë.‚X×
00000100	6E	1F	90	C2	D5	E4	C4	24	BD	31	3E	32	BC	EB	DB	E3	n..ÂÕäÄ$½1>2¼ëÛã
00000110	F1	11	D5	09	6B	B4	E3	56	48	0A	E1	76	5D	B0	EA	3D	ñ.Õ.k´ãVH.áv]°ê=
00000120	F3	94	41	D4	40	93	3A	51	08	B3	E0	3B	1B	3E	F9	90	ó”AÔ@“:Q.³à;.>ù.
00000130	6C	97	7A	74	F3	DE	AC	FA	FA	99	BD	15	E5	95	64	47	l—ztóÞ¬úú™½.å•dG
00000140	99	4F	3E	18	2A	5B	49	DF	A5	E4	45	DC	EA	49	FE	04	™O>.*[Iß¥äEÜêIþ.
00000150	D7	E9	56	E9	25	C5	A4	EF	1A	FA	6C	2E	0B	77			×éVé%Å¤ï.úl..w

Task3.txt | Task3_enc_aes_128_cfb.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   53 61 6C 74 65 64 5F 5F 06 08 B2 F0 66 ED 95 38  Salted__..²ðfí•8
00000010   36 6B 2B DD D7 65 AA AD 7D 62 82 F4 3E 18 68 D7  6k+Ý×eª.}b‚ô>.h×
00000020   2E 37 65 6C 2F 82 F6 2F D1 76 D4 80 AE B8 A6 26  .7el/‚ö/ÑvÔ€®¸¦&
00000030   85 F8 06 C4 A7 FA 02 E0 DE 80 B6 C1 C3 9A 3A 61  …ø.Ä§ú.àÞ€¶ÁÃš:a
00000040   46 EF 84 1D 16 17 88 CF 78 CE 19 3C BE F8 E3 78  Fï„...ˆÏxÎ.<¾øãx
00000050   B1 9B 1D 2A 14 66 53 D7 B4 14 27 45 D1 5C A5 11  ±›.*.fS×´.'EÑ\¥.
00000060   38 49 4F 3C 0C 56 85 BC 76 B0 0D 6B 73 63 AB 47  8IO<.V…¼v°.ksc«G
00000070   83 72 5E 00 5B 97 05 B1 45 3B 7B 23 5A EE 58 84  ƒr^.[—.±E;{#ZîX„
00000080   D2 22 52 CF A7 93 6F 7F E8 89 DE 35 5B FF 53 2B  Ò"RÏ§"o.è‰Þ5[ÿS+
00000090   92 67 AF F2 88 CF F4 2A 0F F3 71 11 8A 07 3B BB  'g¯ò^ÏôÓ*.óq.Š.;»
000000A0   6F 9F 0C 96 FA BF 29 49 C4 60 75 9A 89 50 DC 27  oŸ.–ú¿)IÄ`uš‰PÜ'
000000B0   2B 8D 33 13 B6 E1 CD 38 30 E1 9D 62 AE 88 C0 68  +.3.¶áÍ80á.b®ˆÀh
000000C0   03 7D A2 C3 DD DC A6 57 79 E0 B5 53 A6 C3 40 32  .}¢ÃÝÜ¦Wyàµs¦Ã@2
000000D0   B6 85 4F CC 63 84 96 5D A9 7A 52 A6 26 B9 FD FB  ¶…OÌc„–]©zR¦&¹ýû
000000E0   78 1B F1 F6 C0 70 56 E4 BD BB D2 ED 00 9D F3 7C  x.ñöÀpVä½»Òí..ó|
000000F0   BE 06 9C 84 7E AA D1 A2 2F 3F 84 CB 7F 82 58 D7  ¾.œ„~ªÑ¢/?„Ë.‚X×
00000100   6E 1F 90 C2 D5 E4 C4 24 BD 31 3E 32 BC EB DB E3  n..ÂÕäÄ$½1>2¼ëÛã
00000110   F1 11 D5 09 6B B4 E3 56 48 0A E1 76 5D B0 EA 3D  ñ.Õ.k´ãVH.áv]°ê=
00000120   F3 94 41 D4 40 93 3A 51 08 B3 E0 3B 1B 3E F9 90  ó”AÔ@“:Q.³à;.>ù.
00000130   6C 97 7A 74 F3 DE AC FA FA 99 BD 15 E5 95 64 47  l—ztóÞ¬úú™½.å•dG
00000140   99 4F 3E 18 2A 5B 49 DF A5 E4 45 DC EA 49 FE 04  ™O>.*[Iß¥äEÜêIþ.
00000150   D7 E9 56 E9 25 C5 A4 EF 1A FA 6C 2E 0B 77        ×éVé%Å¤ï.úl..w
```

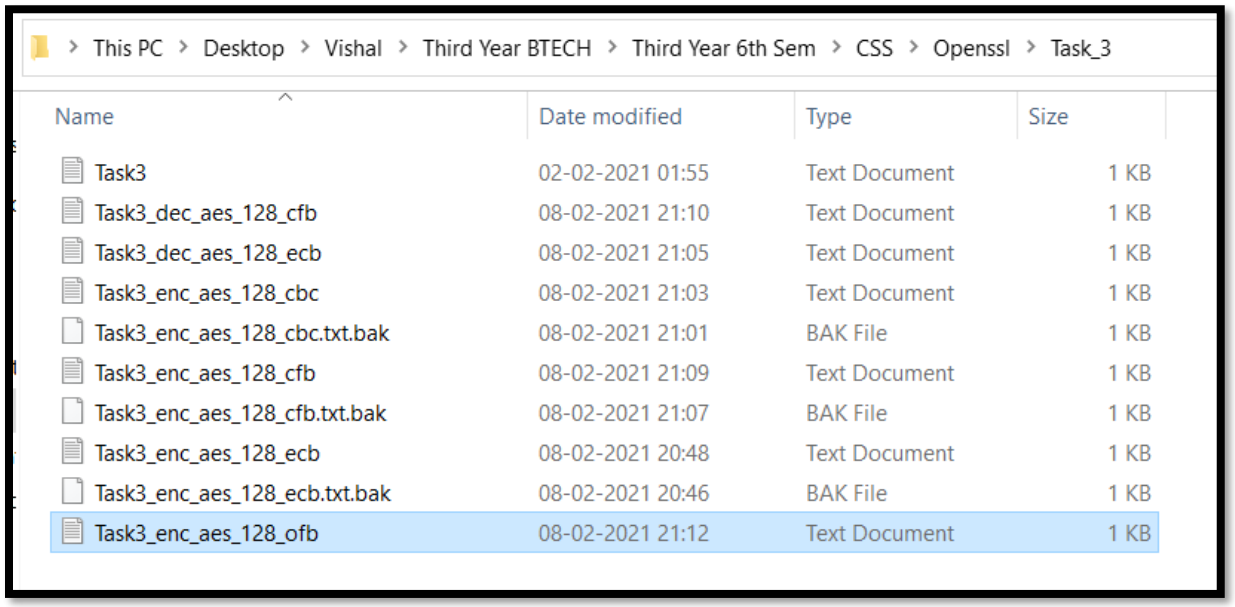
```
OpenSSL> enc -aes-128-cfb -d -in Task3_enc_aes_128_cfb.txt -out Task3_dec_aes_128_cfb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```

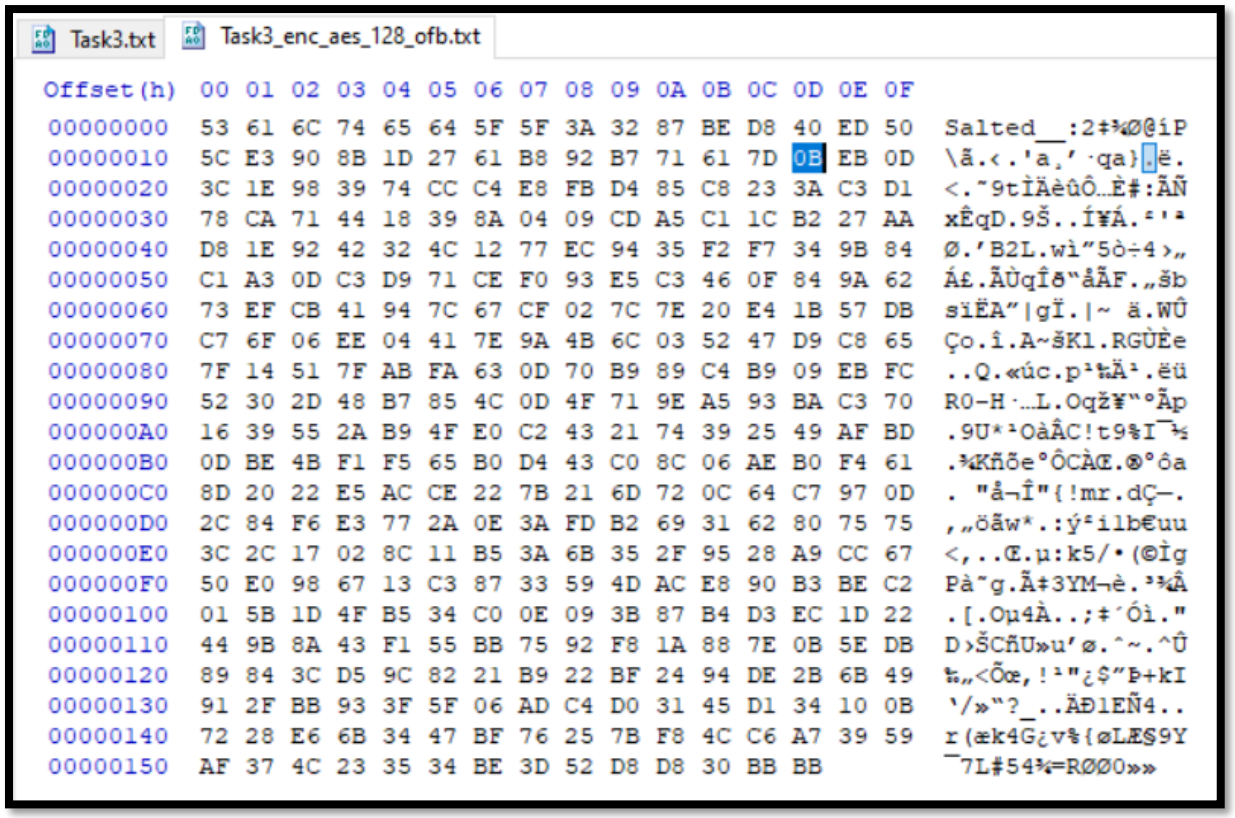
Task3.txt | Task3_enc_aes_128_cfb.txt | Task3_dec_aes_128_cfb.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   43 6F 6D 70 75 74 65 72 20 73 65 63 75 62 69 74  Computer secubit
00000010   7F 87 24 51 88 EB 43 8A 15 AA 97 73 20 04 04 9F  .‡$Qˆ‰CŠ.ª—s ..Ÿ
00000020   68 65 20 70 72 6F 74 65 63 74 69 6F 6E 20 6F 66  he protection of
00000030   20 63 6F 6D 70 75 74 65 72 20 73 79 73 74 65 6D   computer system
00000040   73 20 61 6E 64 20 69 6E 66 6F 72 6D 61 74 69 6F  s and informatio
00000050   6E 20 66 72 6F 6D 20 68 61 72 6D 2C 20 74 68 65  n from harm, the
00000060   66 74 2C 20 61 6E 64 20 75 6E 61 75 74 68 6F 72  ft, and unauthor
00000070   69 7A 65 64 20 75 73 65 2E 20 49 74 20 69 73 20  ized use. It is
00000080   74 68 65 20 70 72 6F 63 65 73 73 20 6F 66 20 70  the process of p
00000090   72 65 76 65 6E 74 69 6E 67 20 61 6E 64 20 64 65  reventing and de
000000A0   74 65 63 74 69 6E 67 20 75 6E 61 75 74 68 6F 72  tecting unauthor
000000B0   69 7A 65 64 20 75 73 65 20 6F 66 20 79 6F 75 72  ized use of your
000000C0   20 63 6F 6D 70 75 74 65 72 20 73 79 73 74 65 6D   computer system
000000D0   2E 0D 0A 0D 0A 54 68 65 72 65 20 61 72 65 20 76  .....There are v
000000E0   61 72 69 6F 75 73 20 74 79 70 65 73 20 6F 66 20  arious types of
000000F0   63 6F 6D 70 75 74 65 72 20 73 65 63 75 72 69 74  computer securit
00000100   79 20 77 68 69 63 68 20 69 73 20 77 69 64 65 6C  y which is widel
00000110   79 20 75 73 65 64 20 74 6F 20 70 72 6F 74 65 63  y used to protec
00000120   74 20 74 68 65 20 76 61 6C 75 61 62 6C 65 20 69  t the valuable i
00000130   6E 66 6F 72 6D 61 74 69 6F 6E 20 6F 66 20 61 6E  nformation of an
00000140   20 6F 72 67 61 6E 69 7A 61 74 69 6F 6E 2E         organization.
```

Encryption mode – OFB

```
OpenSSL> enc -aes-128-ofb -e -in Task3.txt -out Task3_enc_aes_128_ofb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```





Task3.txt | Task3_enc_aes_128_ofb.txt

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	53	61	6C	74	65	64	5F	5F	3A	32	87	BE	D8	40	ED	50	Salted__:2‡¾Ø@íP
00000010	5C	E3	90	8B	1D	27	61	B8	92	B7	71	61	7D	1B	EB	0D	\ã.‹.'a¸'·qa}.ë.
00000020	3C	1E	98	39	74	CC	C4	E8	FB	D4	85	C8	23	3A	C3	D1	<.˜9tÌÄèûÔ…È#:ÃÑ
00000030	78	CA	71	44	18	39	8A	04	09	CD	A5	C1	1C	B2	27	AA	xÊqD.9Š..Í¥Á.²'ª
00000040	D8	1E	92	42	32	4C	12	77	EC	94	35	F2	F7	34	9B	84	Ø.'B2L.wì"5ò÷4›„
00000050	C1	A3	0D	C3	D9	71	CE	F0	93	E5	C3	46	0F	84	9A	62	Á£.ÃÙqÎð"åÃF.„šb
00000060	73	EF	CB	41	94	7C	67	CF	02	7C	7E	20	E4	1B	57	DB	sïËA"|gÏ.|~ ä.WÛ
00000070	C7	6F	06	EE	04	41	7E	9A	4B	6C	03	52	47	D9	C8	65	Ço.î.A~šKl.RGÙÈe
00000080	7F	14	51	7F	AB	FA	63	0D	70	B9	89	C4	B9	09	EB	FC	..Q.«úc.p¹‰Ä¹.ëü
00000090	52	30	2D	48	B7	85	4C	0D	4F	71	9E	A5	93	BA	C3	70	R0-H·…L.Oqž¥"ºÃp
000000A0	16	39	55	2A	B9	4F	E0	C2	43	21	74	39	25	49	AF	BD	.9U*¹OàÂC!t9%I¯½
000000B0	0D	BE	4B	F1	F5	65	B0	D4	43	C0	8C	06	AE	B0	F4	61	.¾Kñõe°ÔCÀŒ.®°ôa
000000C0	8D	20	22	E5	AC	CE	22	7B	21	6D	72	0C	64	C7	97	0D	. "å¬Î"{!mr.dÇ—.
000000D0	2C	84	F6	E3	77	2A	0E	3A	FD	B2	69	31	62	80	75	75	,„öãw*.:ý²ilb€uu
000000E0	3C	2C	17	02	8C	11	B5	3A	6B	35	2F	95	28	A9	CC	67	<,..Œ.µ:k5/•(©Ìg
000000F0	50	E0	98	67	13	C3	87	33	59	4D	AC	E8	90	B3	BE	C2	Pà˜g.Ã‡3YM¬è.³¾Â
00000100	01	5B	1D	4F	B5	34	C0	0E	09	3B	87	B4	D3	EC	1D	22	.[.Oµ4À..;‡´Óì."
00000110	44	9B	8A	43	F1	55	BB	75	92	F8	1A	88	7E	0B	5E	DB	D›ŠCñU»u'ø.ˆ~.^Û
00000120	89	84	3C	D5	9C	82	21	B9	22	BF	24	94	DE	2B	6B	49	‰„<Õœ‚!¹"¿$"Þ+kI
00000130	91	2F	BB	93	3F	5F	06	AD	C4	D0	31	45	D1	34	10	0B	'/»"?_..ÄÐ1EÑ4..
00000140	72	28	E6	6B	34	47	BF	76	25	7B	F8	4C	C6	A7	39	59	r(æk4G¿v%{øLÆ§9Y
00000150	AF	37	4C	23	35	34	BE	3D	52	D8	D8	30	BB	BB			¯7L#54¾=RØØ0»»

```
OpenSSL> enc -aes-128-ofb -d -in Task3_enc_aes_128_ofb.txt -out Task3_dec_aes_128_ofb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```

Task3.txt | Task3_enc_aes_128_cfb.txt | Task3_dec_aes_128_ofb.txt

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	43	6F	6D	70	75	74	65	72	20	73	65	63	75	62	69	74	Computer secubit
00000010	79	20	62	61	73	69	63	61	6C	79	20	69	73	20	74		y basically is t
00000020	68	65	20	70	72	6F	74	65	63	74	69	6F	6E	20	6F	66	he protection of
00000030	20	63	6F	6D	70	75	74	65	72	20	73	79	73	74	65	6D	computer system
00000040	73	20	61	6E	64	20	69	6E	66	6F	72	6D	61	74	69	6F	s and informatio
00000050	6E	20	66	72	6F	6D	20	68	61	72	6D	2C	20	74	68	65	n from harm, the
00000060	66	74	2C	20	61	6E	64	20	75	6E	61	75	74	68	6F	72	ft, and unauthor
00000070	69	7A	65	64	20	75	73	65	2E	20	49	74	20	69	73	20	ized use. It is
00000080	74	68	65	20	70	72	6F	63	65	73	73	20	6F	66	20	70	the process of p
00000090	72	65	76	65	6E	74	69	6E	67	20	61	6E	64	20	64	65	reventing and de
000000A0	74	65	63	74	69	6E	67	20	75	6E	61	75	74	68	6F	72	tecting unauthor
000000B0	69	7A	65	64	20	75	73	65	20	6F	66	20	79	6F	75	72	ized use of your
000000C0	20	63	6F	6D	70	75	74	65	72	20	73	79	73	74	65	6D	computer system
000000D0	2E	0D	0A	0D	0A	54	68	65	72	65	20	61	72	65	20	76	.....There are v
000000E0	61	72	69	6F	75	73	20	74	79	70	65	73	20	6F	66	20	arious types of
000000F0	63	6F	6D	70	75	74	65	72	20	73	65	63	75	72	69	74	computer securit
00000100	79	20	77	68	69	63	68	20	69	73	20	77	69	64	65	6C	y which is widel
00000110	79	20	75	73	65	64	20	74	6F	20	70	72	6F	74	65	63	y used to protec
00000120	74	20	74	68	65	20	76	61	6C	75	61	62	6C	65	20	69	t the valuable i
00000130	6E	66	6F	72	6D	61	74	69	6F	6E	20	6F	66	20	61	6E	nformation of an
00000140	20	6F	72	67	61	6E	69	7A	61	74	69	6F	6E	2E			organization.

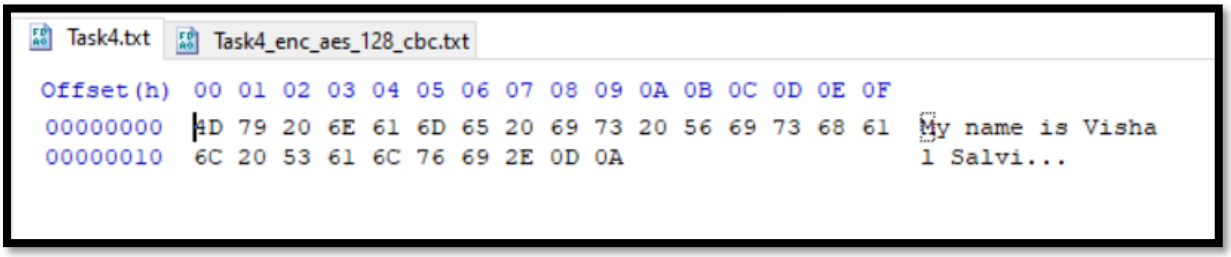
3.4 Task4 : Padding

For block ciphers, when the size of the plaintex is not the multiple of the block size, padding may be required. In this task, we will study the padding schemes. Please do the following exercises:

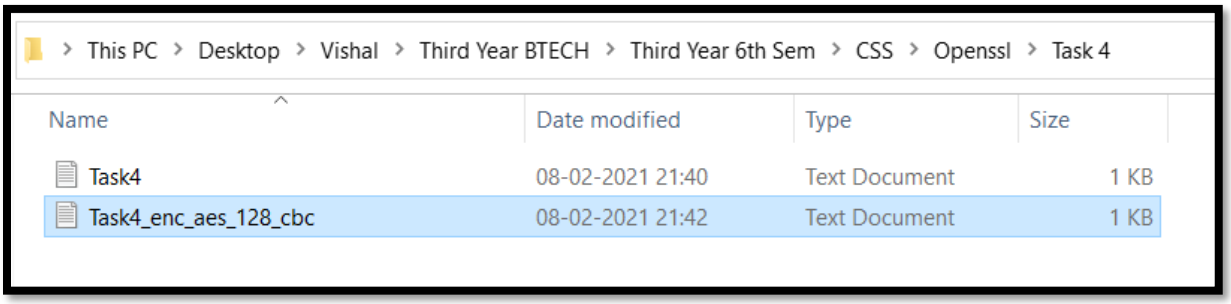
1. The openssl manual says that openssl uses PKCS5 standard for its padding. Please design an experiment to verify this. In particular, use your experiment to figure out the paddings in the AES encryption when the length of the plaintext is 20 octets and 32 octets.

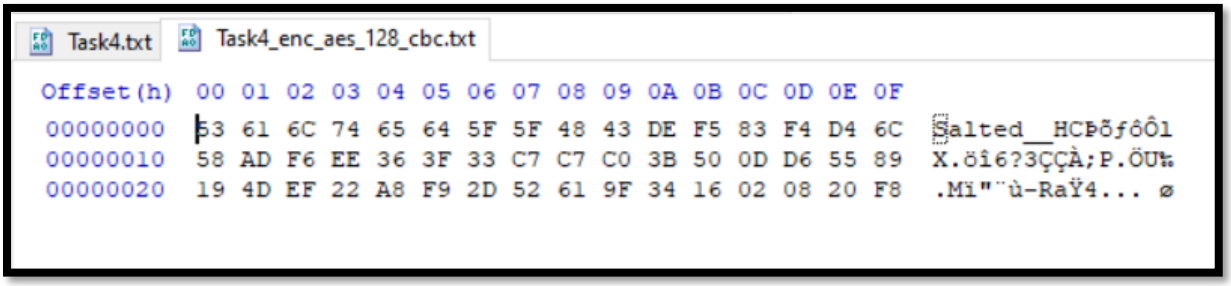
2. Please use ECB, CBC, CFB, and OFB modes to encrypt a file (you can pick any cipher). Please report which modes have paddings and which ones do not. For those that do not need paddings, please explain why.

Task 4:

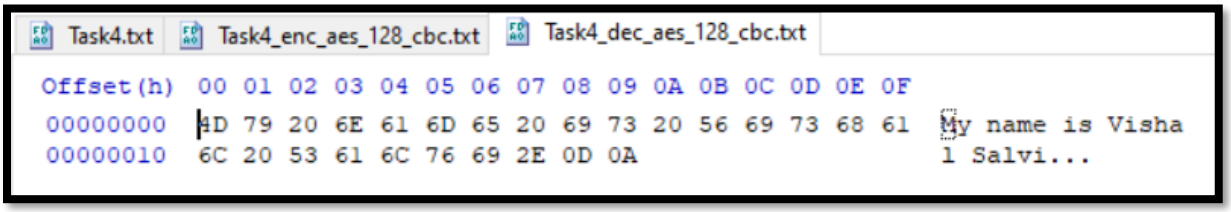


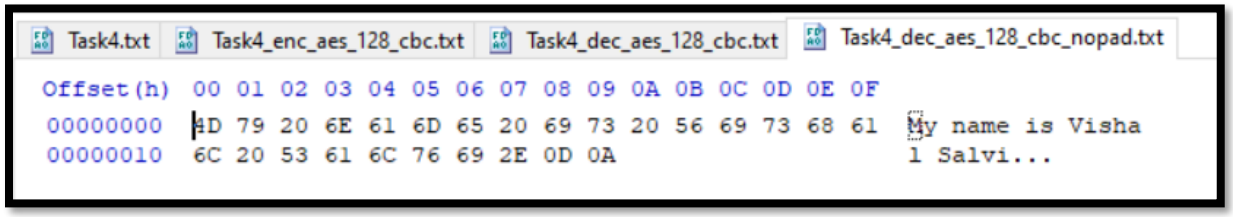

```
C:\>cd C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4>openssl
OpenSSL> enc -aes-128-cbc -e -in Task4.txt -out Task4_enc_aes_128_cbc.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```



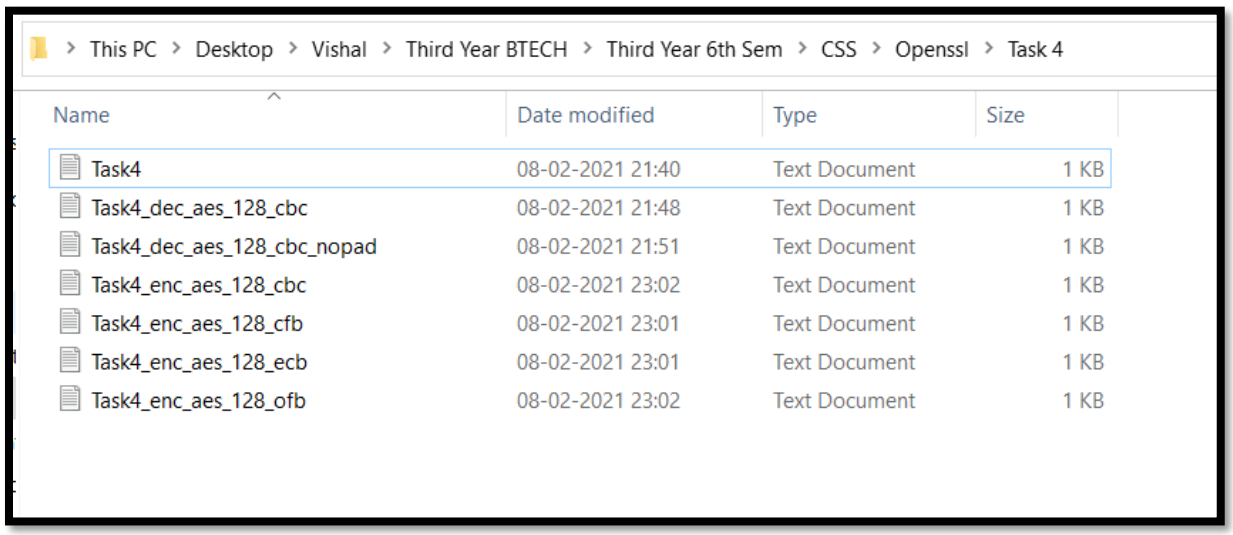



```
OpenSSL> enc -aes-128-cbc -d -in Task4_enc_aes_128_cbc.txt -out Task4_dec_aes_128_cbc.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-cbc -d -in Task4_enc_aes_128_cbc.txt -out Task4_dec_aes_128_cbc_nopad.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```

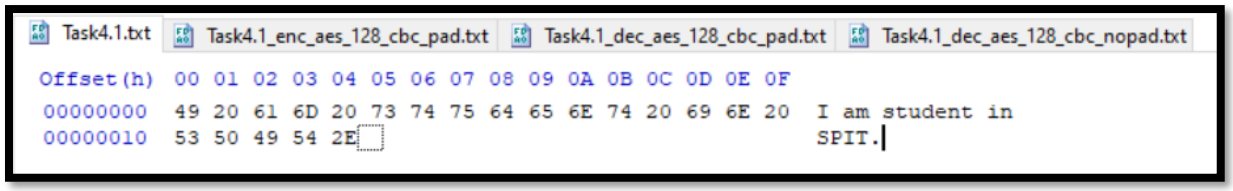




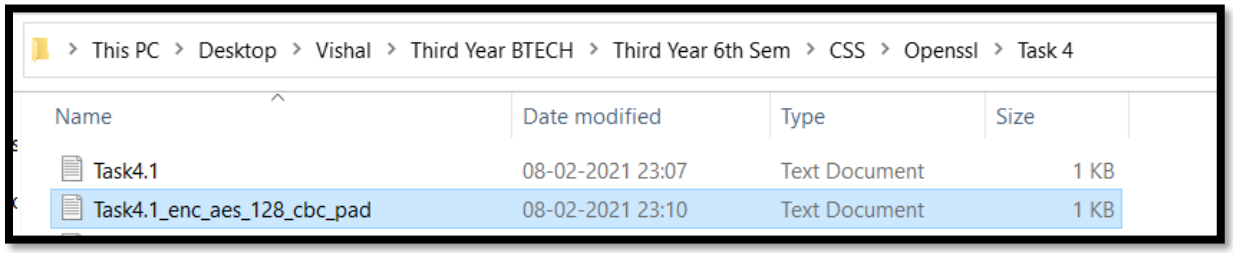

```
C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4>dir
 Volume in drive C is Windows-SSD
 Volume Serial Number is BE73-BD16

 Directory of C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4

08-02-2021  21:51    <DIR>          .
08-02-2021  21:51    <DIR>          ..
08-02-2021  21:40                26 Task4.txt
08-02-2021  21:48                26 Task4_dec_aes_128_cbc.txt
08-02-2021  21:51                26 Task4_dec_aes_128_cbc_nopad.txt
08-02-2021  21:48                48 Task4_enc_aes_128_cbc.txt
               4 File(s)            126 bytes
               2 Dir(s)  343,829,057,536 bytes free

OpenSSL> enc -aes-128-ecb -e -in Task4.txt -out Task4_enc_aes_128_ecb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
warning: iv not use by this cipher
OpenSSL> enc -aes-128-cfb -e -in Task4.txt -out Task4_enc_aes_128_cfb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-cbc -e -in Task4.txt -out Task4_enc_aes_128_cbc.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL> enc -aes-128-ofb -e -in Task4.txt -out Task4_enc_aes_128_ofb.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```

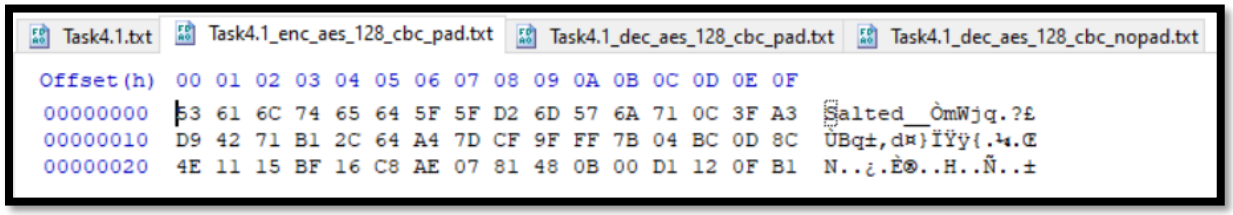



```
C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4>dir
 Volume in drive C is Windows-SSD
 Volume Serial Number is BE73-BD16

 Directory of C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4

08-02-2021  23:02    <DIR>          .
08-02-2021  23:02    <DIR>          ..
08-02-2021  21:40                26 Task4.txt
08-02-2021  21:48                26 Task4_dec_aes_128_cbc.txt
08-02-2021  21:51                26 Task4_dec_aes_128_cbc_nopad.txt
08-02-2021  23:02                48 Task4_enc_aes_128_cbc.txt
08-02-2021  23:01                42 Task4_enc_aes_128_cfb.txt
08-02-2021  23:01                48 Task4_enc_aes_128_ecb.txt
08-02-2021  23:02                42 Task4_enc_aes_128_ofb.txt
               7 File(s)            258 bytes
               2 Dir(s)  343,823,687,680 bytes free

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4>
```

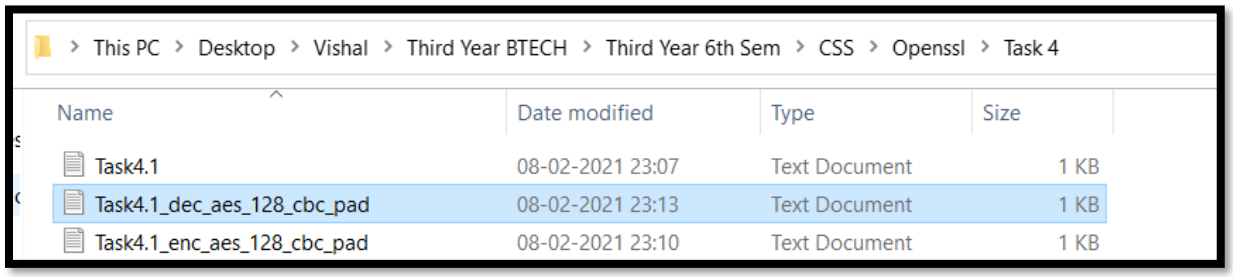


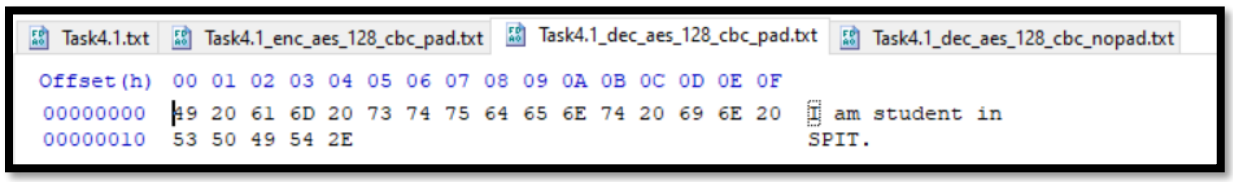

```
OpenSSL> enc -aes-128-cbc -e -in Task4.1.txt -out Task4.1_enc_aes_128_cbc_pad.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```



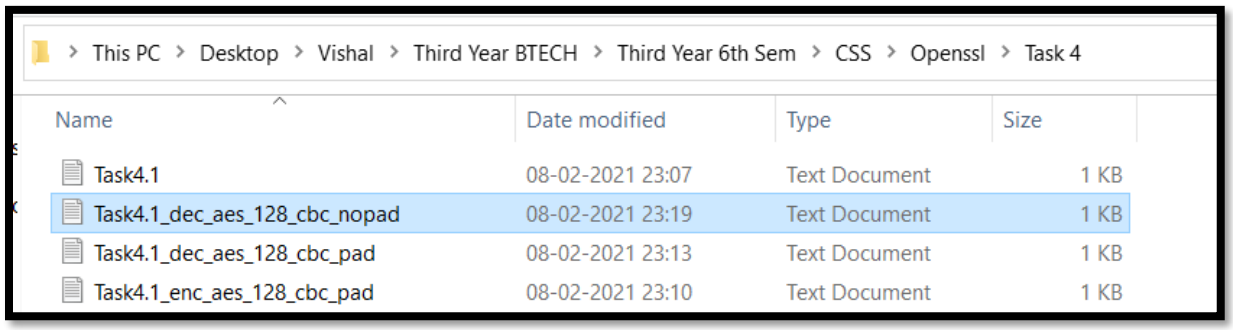


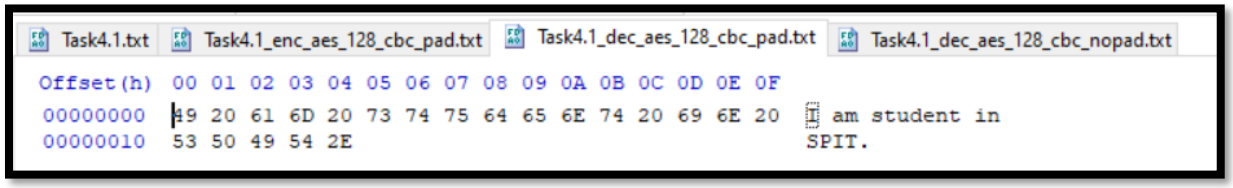

```
OpenSSL> enc -aes-128-cbc -d -in Task4.1_enc_aes_128_cbc_pad.txt -out Task4_dec_aes_128_cbc_pad.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```






```
OpenSSL> enc -aes-128-cbc -d -in Task4.1_enc_aes_128_cbc_pad.txt -out Task4.1_dec_aes_128_cbc_nopad.txt -k 00112233445566778889aabbccddeeff -iv 0102030405060708
OpenSSL>
```






```
C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4>dir
 Volume in drive C is Windows-SSD
 Volume Serial Number is BE73-BD16

 Directory of C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4

08-02-2021  23:16    <DIR>          .
08-02-2021  23:16    <DIR>          ..
08-02-2021  23:07                21 Task4.1.txt
08-02-2021  23:19                21 Task4.1_dec_aes_128_cbc_nopad.txt
08-02-2021  23:13                21 Task4.1_dec_aes_128_cbc_pad.txt
08-02-2021  23:10                48 Task4.1_enc_aes_128_cbc_pad.txt
08-02-2021  21:40                26 Task4.txt
08-02-2021  21:48                26 Task4_dec_aes_128_cbc.txt
08-02-2021  21:51                26 Task4_dec_aes_128_cbc_nopad.txt
08-02-2021  23:12                21 Task4_dec_aes_128_cbc_pad.txt
08-02-2021  23:02                48 Task4_enc_aes_128_cbc.txt
08-02-2021  23:01                42 Task4_enc_aes_128_cfb.txt
08-02-2021  23:01                48 Task4_enc_aes_128_ecb.txt
08-02-2021  23:02                42 Task4_enc_aes_128_ofb.txt
              12 File(s)            390 bytes
               2 Dir(s)  343,817,687,040 bytes free

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task 4>
```

3.5 Task 5: Programming using the Crypto Library

So far, we have learned how to use the tools provided by openssl to encrypt and decrypt messages. In this task, we will learn how to use openssl's crypto library to encrypt/descrypt messages in programs.

OpenSSL provides an API called EVP, which is a high-level interface to cryptographic functions. Although OpenSSL also has direct interfaces for each individual encryption algorithm, the EVP library provides a common interface for various encryption algorithms. To ask EVP to use a specific algorithm, we simply need to pass our choice to the EVP interface. A sample code is given in http://www.openssl.org/docs/crypto/EVP_EncryptInit.html. Please get yourself familiar with this program, and then do the following exercise.

You are given a plaintext and a ciphertext, and you know that aes-128-cbc is used to generate the ciphertext from the plaintext, and you also know that the numbers in the IV are all zeros (not the ASCII character '0'). Another clue that you have learned is that the key used to encrypt this plaintext is an English word shorter than 16 characters; the word that can be found from a typical English dictionary. Since the word has less than 16 characters (i.e. 128 bits), space characters (hexadecimal value 0x20) are appended to the end of the word to form a key of 128 bits. Your goal is to write a program to find out this key. You can download a English word list from the Internet. We have also linked one on the web page of this lab. The plaintext and ciphertext is in the following:

Plaintext (total 21 characters): This is a top secret. Ciphertext (in hex format):
8d20e5056a8d24d0462ce74e4904c1b5
13e10d1df4a2ef2ad4540fae1ca0aaf9

Note 1: If you choose to store the plaintex message in a file, and feed the file to your program, you need to check whether the file length is 21. Some editors may add a special character to the end of the file. If that happens, you can use the ghex tool to remove the special character.

Note 2: In this task, you are supposed to write your own program to invoke the crypto library. No credit will be given if you simply use the openssl commands to do this task.

Note 3: To compile your code, you may need to include the header files in openssl, and link to openssl libraries. To do that, you need to tell your compiler where those files are. In your Makefile, you may want to specify the following:

```
INC=/usr/local/ssl/include/
 LIB=/usr/local/ssl/lib/

 all:
		gcc -I$(INC) -L$(LIB) -o enc yourcode.c -lcrypto -ldl
```

CODE:

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad

plain_text = b"This is a top secret."
cipher_hex = "8d20e5056a8d24d0462ce74e4904c1b513e10d1df4a2ef2ad4540fae1ca0aaf9"

res_keys = []

file = open('data.txt', 'r')
lines = file.readlines()
print(len(lines))
words = [str.strip(line) for line in lines]

for word in words:
    if len(word) >= 16:
        continue
    key = word.encode() + b' '*(16-len(word))
    cipher = AES.new(key, AES.MODE_CBC, iv=bytes.fromhex('0'*32))
    ciphertext = cipher.encrypt(pad(plain_text, AES.block_size))

    is_matched = "NOT MATCHED"
    if bytes.hex(ciphertext) == cipher_hex:
        is_matched = "MATCHED"
        res_keys.append(word)

    print(word, bytes.hex(ciphertext), is_matched)

print("\n\nResulting Key:",res_keys)
```

Output:

```
meager 38be561ae5b3beb41f504fe230bedef52ef012cd59384b9a024b9f20884fd9cd NOT MATCHED
meal 6d55a5f17450a789a75d89ea1d61f8ebbe861004c174be30d4e314c364a1fcc4 NOT MATCHED
mealtime 1f8e67108b2997f9607165f9f7d462b4f9b3f75b2040508095797c651be0c28d NOT MATCHED
mealy 3dfcadd9c24056651d0fca6a4cf3eeb0f44ed1262d5f6ad92e3774618c6eae87 NOT MATCHED
mean 30ecc69310edd6e2d64394e08ba973bf2c5db8c4a44e35f1b3dea002debe124d NOT MATCHED
meander 33182770e70b9e5320d7c095f841ff7d875a6f2d772479c8bba27454bc5f2962 NOT MATCHED
meaningful 84e790d14440885375248 93f8031a6e4e1c497ed58c28f81ce6d2bf3b55223d7 NOT MATCHE
meant 62ef97e629724e142ea6949cce5f94b0f67e9977b89acf13f10d85e2cb6b5a95 NOT MATCHED
meantime 4ef086519c64489ad29c7a7868feced85ce413b91551f9cd38af12db0665f5ec NOT MATCHED
meanwhile 16f5ade5454eb04eac1353df71bd84b52054af53d243ed7498b408834b82c9e1 NOT MATCHE
measle 791e343443bfbb1c4c5147b1a6dcc33dae286d5bdf631e4ab65fa3f1a8eb024f NOT MATCHED
measure ad8ba9c3d1117412750a84073223bc0041fba8ca56d5047893d488bfe7f39e71 NOT MATCHED
meat 9f3008f60b2cca02e0086a66213d53b683cef9449070afb32c8457044a3d515a NOT MATCHED
meaty 0da3eae452b5c23e692d1e1b9d35f8042a81db90ca5cdbe74f7b61594bcadf96 NOT MATCHED
Mecca 4fcf20a497f2112a31c108652d2bc61ced8be59af80ba44fd31007eef67e4540 NOT MATCHED
mechanic 5e76f7f0e8eb57339231d61182be1e126844862fcbd819bf201563f7b3d7c635 NOT MATCHED
mechanism f4b3f29cfcdce6d69efd6f79cc13d770f68d342c1ce03f543b8f95cdee6104ab NOT MATCHE
mechanist 29c7527eafb37e305b8cb6c5728c6fdcc52e3050408a5ddeeb49b3d655c71e76 NOT MATCHE
mecum 51351f615611fd30d8595950c3b956b5e3d0e0fcf88b1b0a7c7a7e32a8e516b3 NOT MATCHED
medal f130196d3000e5837af86a57202283e0820f5d1590e6637d60b1bab73054d892 NOT MATCHED
medallion cbd853975b222ca12b1ab3eddfd92624631645f6bd20a039ecf46e98cd0e41eb NOT MATCHE
meddle fc7a5e2b8ed5acd499aa28c044599da60e4137762b55efd599b5ea4732faf633 NOT MATCHED
Medea 44ab4aefafcfc5d5a0cf5aaaecd3be0368a1299e776d6b98f60478b98050151f NOT MATCHED
Medford 33bb64c14be3abe1bc76de3f4ebedcde232d64a5837a6d1ed890c459c8efeb92 NOT MATCHED
media f4bdb140224e39a9a6b188155713cd3d6a44fba20af75b9f27ba167b4a4d0406 NOT MATCHED
medial f051ba4b9985d82e8d5619df1c2344c66d40d14702586f2d2d87bc7913543a9d NOT MATCHED
median 8d20e5056a8d24d0462ce74e4904c1b513e10d1df4a2ef2ad4540fae1ca0aaf9 MATCHED
mediate b7a2bed5a98b4ef90ead7b4267a988798679f29a2258a8cc08537902b84dc127 NOT MATCHED
medic 7fb63f817731ff588fdcad48eaad614d56aff4a4bd29ad2c70c84f77c1397dc6 NOT MATCHED
medicate a3842267eac86e091e0b217797b83df2cd3711d4adceae7be0de35be0a67e6eb NOT MATCHED
```

```
zing f907a0ad5be217e0c71bfee99c7d6be0046ee0d6df524d2433159272095c4490 NOT MATCHED
Zion 91923eb0c90eb2b4a7b6610e07848b63c802026b2e10a1bd2ef4d81c36949d8a NOT MATCHED
Zionism de40f1e5200eb205e887357c71bb4bed607d05077e3fb4847892067cbd85f14c NOT MATCHED
zip a3505f2264d430c100d53342f0074497f8060ace858936bff783e108a8f59488 NOT MATCHED
zippy 6cd6bb040a19e505b3a0b599d5f26d490ffbe37845d0501dfd27b2990ce4933d NOT MATCHED
zircon 3e67f3da7fdf47b698bfb0c83d1a640ebd5a18459c0ee4fdbc4ee415b34dbdb7 NOT MATCHED
zirconium 4dfeaf712686e075196990c0ebc0140ec0454f716b63e27ce8c520bc4631393c NOT MATCHED
zloty 445a85f023ed28e7792dc64d2a7a541228648b0b4d8e9aa8ebef6824f3e3a0ee NOT MATCHED
zodiac f60249772facc36ece6b066e4d28318f3ee807962e6792b7ab4aa4f480b95eb1 NOT MATCHED
zodiacal d4a0fc67c0b1e3149cd61b9fd3ef70e57786b2af52cd493592874a922e8687fa NOT MATCHED
Zoe 7f40facd9077eec53ba1c74a12f6cc6d668fad5bc734035b919159b96166fd7a NOT MATCHED
Zomba 891aa32e7b28050c42fcf3906640c724a293b4859f9e8e814f52fe1b7aa709a4 NOT MATCHED
zombie bf33265884ec3bf9cfa7ad29104b41ba6f53c05502eb621df6d552d595ec5055 NOT MATCHED
zone 6402508dac10daffa266ff136cd450d3a9c749f9997ef9fc3fb178394124f399 NOT MATCHED
zoo 194962aa8e88ee06b3181559ddd6ed77df1b37d26d9e8bb9c02d1ef7fe0331a1 NOT MATCHED
zoology ea12d5f693cdbd45288980aa414e6b382e8321f99bc6734ac6c5e04d288c6cbb NOT MATCHED
zoom c7160fce104f33d04a4234aefae607855891738043635f6abc4a67716db45c40 NOT MATCHED
Zorn 7be43a4c15ada4d0672a2f638f1088a3c09f78cbbb9d819798cc25d206efb540 NOT MATCHED
Zoroaster 2443c9f0280438d8ab2f775257d6c14a0c0d1ea08a49bd4df6f0b5e7a8c31f42 NOT MATCHED
Zoroastrian cc1af4a4dcc779dc9b99c42b7ab0b4de6f78a1606c4ef34506aa59c149c5e887 NOT MATCHED
zounds e1f04902b3a88d87857020411e46332a325a6ba96452103b18ba585a0b348a09 NOT MATCHED
z's add4648882d8499e11f8e0bf3eb28aacaa7c5adbe2e4adf58f23d1f5a2a4d93a NOT MATCHED
zucchini d484c4616dfd87c70b537e9ad5a576792c9cb9f576dfd6e5b26c08287ee378cf NOT MATCHED
Zurich adb6b664241480d9e580cbbc0a9f4b3dd405a0830fe1cb413599cd0f58492007 NOT MATCHED
zygote a9c299cc65c3ef64bd2870ba7b5b7ebde968894b23aa476f54a2ac19e0014820 NOT MATCHED


Resulting Key: ['median']
```

Conclusion:

- ✓ Learnt about OpenSSL and used it for encryption and decryption.
- ✓ Studied the difference between ECB, CBC, CFB and OFB modes.
- ✓ I know more about libraries in Python which can be used for encryption and decryption.
- ✓ Successfully wrote a program in Python to find the key used for encrypting given plain text using brute force method.