OpenSSL - Lab Assignment 2

Harshal Patel

August 27, 2019

1 OpenSSL

- OpenSSL provides a command line application to perform a wide variety of cryptography tasks, such as creating and handling certificates and related files.
- We can obtain a list of available ciphers by using the **list-cipher-algorithms** command

  ```
  $ openssl list −cipher−algorithms
  ```

- Options

  1. **-in filename**: Specifies the input file
  2. **-out filename**: Specifies the output file
  3. **-e or -d**: Specifies whether to encrypt (-e) or to decrypt (-d).
  4. **-a, -base64**: These flags tell OpenSSL to apply Base64 encoding before or after cryptographic operation
  5. **-iv IV**: specifies the initialization vector IV as hexadecimal number
  6. **-K key**: allows us to set the key used for encryption or decryption.
  7. **-salt, -nosalt**: Allows to switch salting on or off.

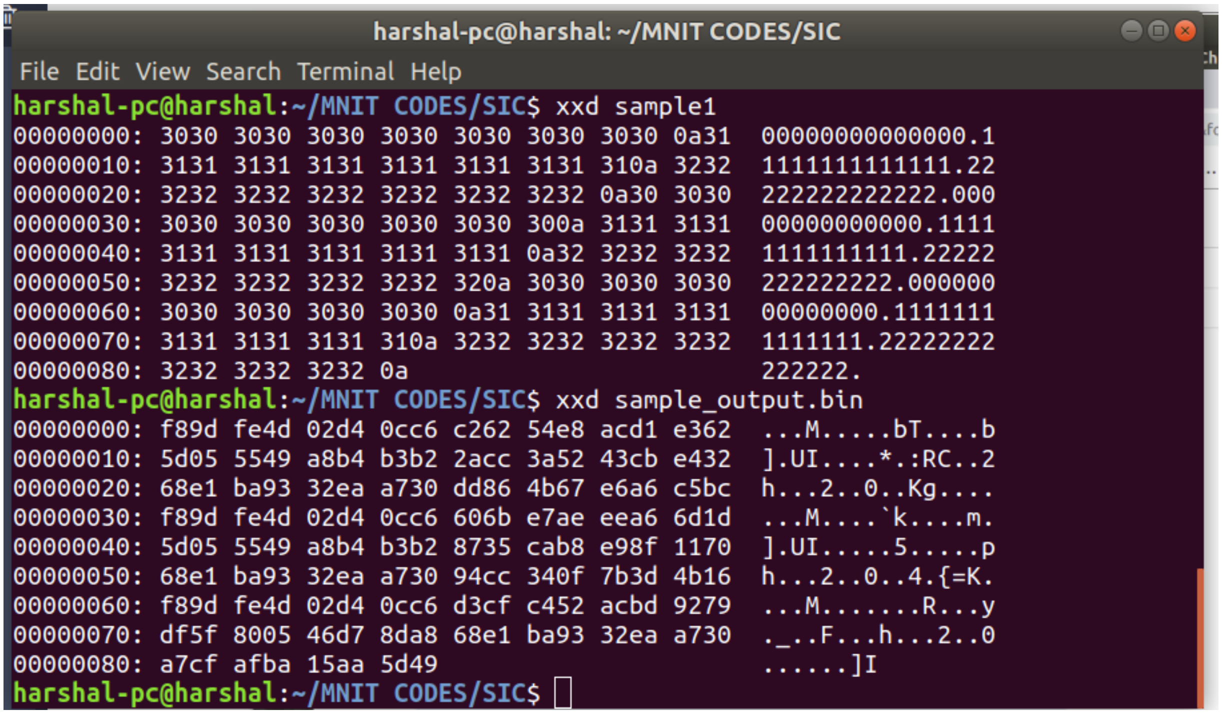
2 OBSERVATIONS

2.1 Electronic Code Book (ECB)

```
$ openssl enc −des−ecb −nosalt −e −in sample1 −out
  sample_output
```

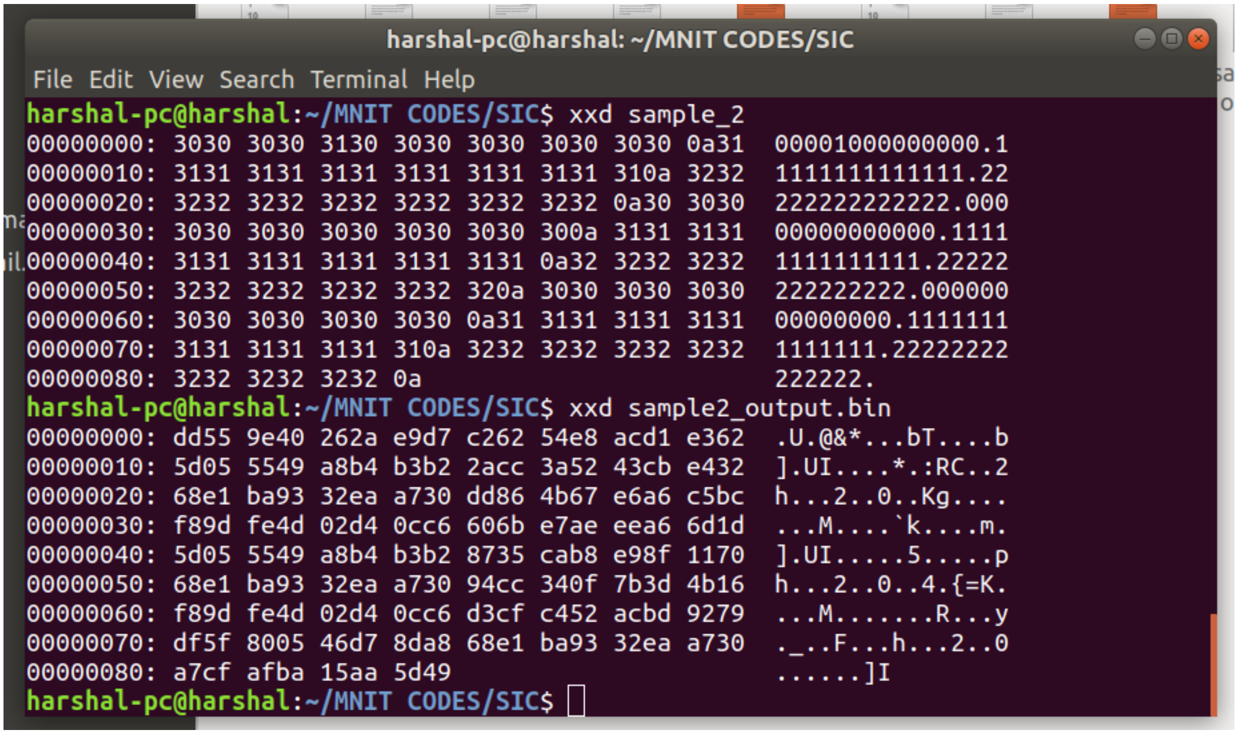
- This command reads our message which is written in input.bin file, **encrypts it** and writes the output in sample$_outputfile$.

- Using the **xxd sample1** and **xxd sample**$_outputfile.binweobservethehexdumpcodesofthisfiles$


harshal-pc@harshal: ~/MNIT CODES/SIC
File Edit View Search Terminal Help

```
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample1
00000000: 3030 3030 3030 3030 3030 3030 3030 0a31  00000000000000.1
00000010: 3131 3131 3131 3131 3131 3131 310a 3232  1111111111111.22
00000020: 3232 3232 3232 3232 3232 3232 0a30 3030  222222222222.000
00000030: 3030 3030 3030 3030 3030 300a 3131 3131  00000000000.1111
00000040: 3131 3131 3131 3131 3131 0a32 3232 3232  1111111111.22222
00000050: 3232 3232 3232 3232 320a 3030 3030 3030  222222222.000000
00000060: 3030 3030 3030 3030 0a31 3131 3131 3131  00000000.1111111
00000070: 3131 3131 3131 310a 3232 3232 3232 3232  1111111.22222222
00000080: 3232 3232 3232 0a                        222222.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample_output.bin
00000000: f89d fe4d 02d4 0cc6 c262 54e8 acd1 e362  ...M.....bT....b
00000010: 5d05 5549 a8b4 b3b2 2acc 3a52 43cb e432  ].UI....*.:RC..2
00000020: 68e1 ba93 32ea a730 dd86 4b67 e6a6 c5bc  h...2..0..Kg....
00000030: f89d fe4d 02d4 0cc6 606b e7ae eea6 6d1d  ...M....`k....m.
00000040: 5d05 5549 a8b4 b3b2 8735 cab8 e98f 1170  ].UI.....5.....p
00000050: 68e1 ba93 32ea a730 94cc 340f 7b3d 4b16  h...2..0..4.{=K.
00000060: f89d fe4d 02d4 0cc6 d3cf c452 acbd 9279  ...M.......R...y
00000070: df5f 8005 46d7 8da8 68e1 ba93 32ea a730  ._..F...h...2..0
00000080: a7cf afba 15aa 5d49                      ......]I
harshal-pc@harshal:~/MNIT CODES/SIC$ 
```

When we change some values in the input file, we can see the resulting change in corresponding output file. Here I have made changes in last digit of second line.

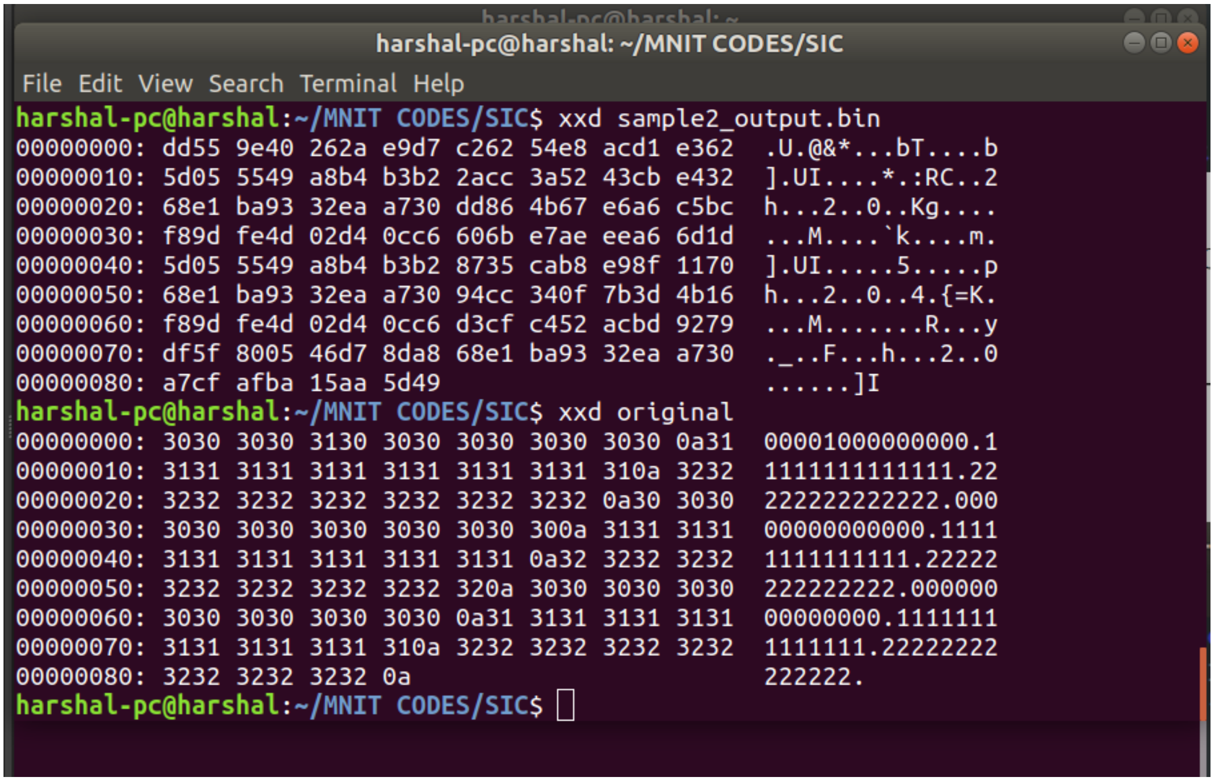


harshal-pc@harshal: ~/MNIT CODES/SIC
File Edit View Search Terminal Help

```
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample_2
00000000: 3030 3030 3130 3030 3030 3030 3030 0a31  00001000000000.1
00000010: 3131 3131 3131 3131 3131 3131 310a 3232  1111111111111.22
00000020: 3232 3232 3232 3232 3232 3232 0a30 3030  222222222222.000
00000030: 3030 3030 3030 3030 3030 300a 3131 3131  00000000000.1111
00000040: 3131 3131 3131 3131 3131 0a32 3232 3232  1111111111.22222
00000050: 3232 3232 3232 3232 320a 3030 3030 3030  222222222.000000
00000060: 3030 3030 3030 3030 0a31 3131 3131 3131  00000000.1111111
00000070: 3131 3131 3131 310a 3232 3232 3232 3232  1111111.22222222
00000080: 3232 3232 3232 0a                        222222.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample2_output.bin
00000000: dd55 9e40 262a e9d7 c262 54e8 acd1 e362  .U.@&*...bT....b
00000010: 5d05 5549 a8b4 b3b2 2acc 3a52 43cb e432  ].UI....*.:RC..2
00000020: 68e1 ba93 32ea a730 dd86 4b67 e6a6 c5bc  h...2..0..Kg....
00000030: f89d fe4d 02d4 0cc6 606b e7ae eea6 6d1d  ...M....`k....m.
00000040: 5d05 5549 a8b4 b3b2 8735 cab8 e98f 1170  ].UI.....5.....p
00000050: 68e1 ba93 32ea a730 94cc 340f 7b3d 4b16  h...2..0..4.{=K.
00000060: f89d fe4d 02d4 0cc6 d3cf c452 acbd 9279  ...M.......R...y
00000070: df5f 8005 46d7 8da8 68e1 ba93 32ea a730  ._..F...h...2..0
00000080: a7cf afba 15aa 5d49                      ......]I
harshal-pc@harshal:~/MNIT CODES/SIC$
```

When we decrypt it we get the following results, we need to use the same key for decryption.

$ openssl enc –des–ecb –nosalt –d –in sample2_output.bin –out original



harshal-pc@harshal: ~/MNIT CODES/SIC
File Edit View Search Terminal Help

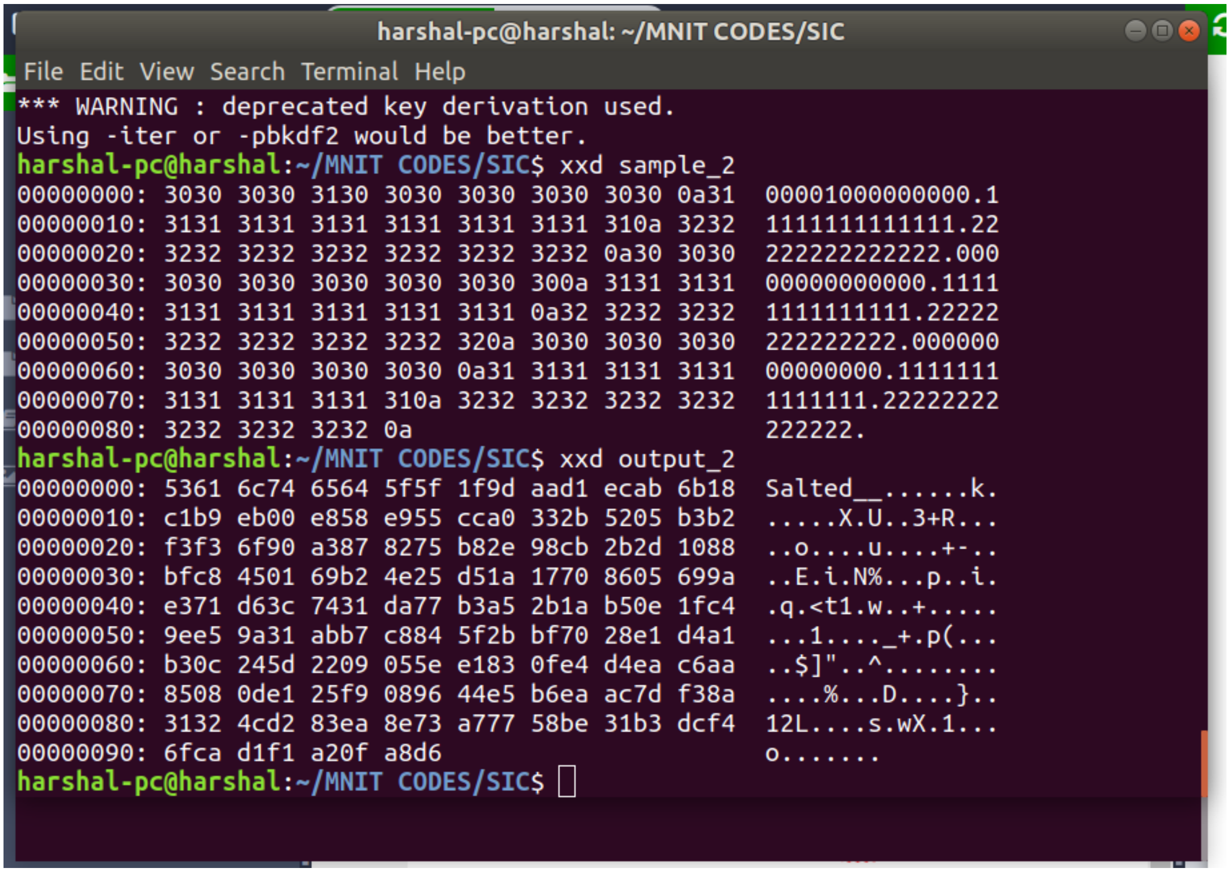
```
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample2_output.bin
00000000: dd55 9e40 262a e9d7 c262 54e8 acd1 e362  .U.@&*...bT....b
00000010: 5d05 5549 a8b4 b3b2 2acc 3a52 43cb e432  ].UI....*.:RC..2
00000020: 68e1 ba93 32ea a730 dd86 4b67 e6a6 c5bc  h...2..0..Kg....
00000030: f89d fe4d 02d4 0cc6 606b e7ae eea6 6d1d  ...M....`k....m.
00000040: 5d05 5549 a8b4 b3b2 8735 cab8 e98f 1170  ].UI.....5.....p
00000050: 68e1 ba93 32ea a730 94cc 340f 7b3d 4b16  h...2..0..4.{=K.
00000060: f89d fe4d 02d4 0cc6 d3cf c452 acbd 9279  ...M.......R...y
00000070: df5f 8005 46d7 8da8 68e1 ba93 32ea a730  ._..F...h...2..0
00000080: a7cf afba 15aa 5d49                      ......]I
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd original
00000000: 3030 3030 3130 3030 3030 3030 3030 0a31  00001000000000.1
00000010: 3131 3131 3131 3131 3131 3131 310a 3232  1111111111111.22
00000020: 3232 3232 3232 3232 3232 3232 0a30 3030  222222222222.000
00000030: 3030 3030 3030 3030 3030 300a 3131 3131  00000000000.1111
00000040: 3131 3131 3131 3131 3131 0a32 3232 3232  1111111111.22222
00000050: 3232 3232 3232 3232 320a 3030 3030 3030  222222222.000000
00000060: 3030 3030 3030 3030 0a31 3131 3131 3131  00000000.1111111
00000070: 3131 3131 3131 310a 3232 3232 3232 3232  1111111.22222222
00000080: 3232 3232 3232 0a                        222222.
harshal-pc@harshal:~/MNIT CODES/SIC$ 
```

2.2 Cipher Block Chaining (CBC)

- Here we need to mention the intial vector (IV) option in the command.

  $ openssl enc −des−cbc −e −iv 0000000000000000 −in sample_2 −out output_2

- Here we observe that, only the first line of hex code is same as that of EBC mode hex code.


harshal-pc@harshal: ~/MNIT CODES/SIC
File Edit View Search Terminal Help

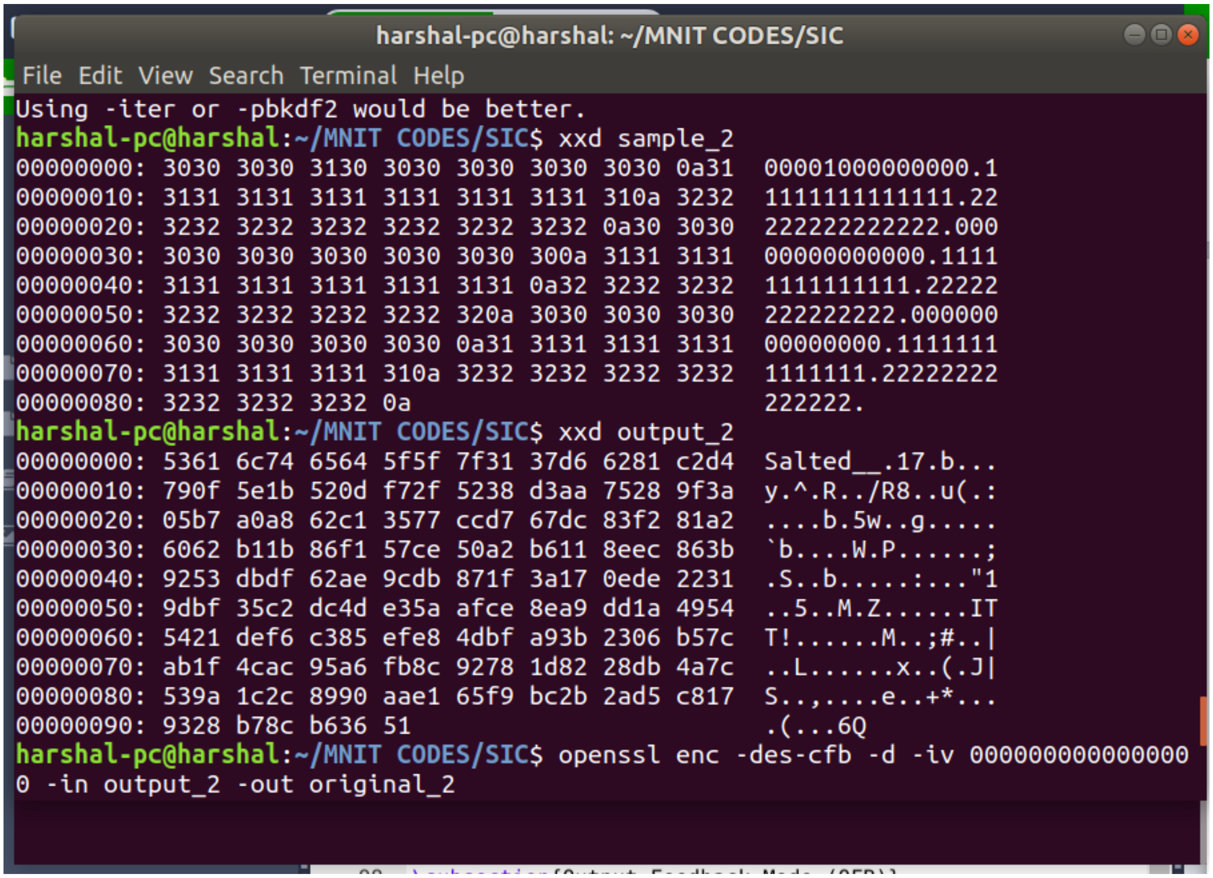
```
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample_2
00000000: 3030 3030 3130 3030 3030 3030 3030 0a31  00001000000000.1
00000010: 3131 3131 3131 3131 3131 3131 310a 3232  1111111111111.22
00000020: 3232 3232 3232 3232 3232 3232 0a30 3030  222222222222.000
00000030: 3030 3030 3030 3030 3030 300a 3131 3131  00000000000.1111
00000040: 3131 3131 3131 3131 3131 0a32 3232 3232  1111111111.22222
00000050: 3232 3232 3232 3232 320a 3030 3030 3030  222222222.000000
00000060: 3030 3030 3030 3030 0a31 3131 3131 3131  00000000.1111111
00000070: 3131 3131 3131 310a 3232 3232 3232 3232  1111111.22222222
00000080: 3232 3232 3232 0a                        222222.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd output_2
00000000: 5361 6c74 6564 5f5f 1f9d aad1 ecab 6b18  Salted__......k.
00000010: c1b9 eb00 e858 e955 cca0 332b 5205 b3b2  .....X.U..3+R...
00000020: f3f3 6f90 a387 8275 b82e 98cb 2b2d 1088  ..o....u....+-..
00000030: bfc8 4501 69b2 4e25 d51a 1770 8605 699a  ..E.i.N%...p..i.
00000040: e371 d63c 7431 da77 b3a5 2b1a b50e 1fc4  .q.<t1.w..+.....
00000050: 9ee5 9a31 abb7 c884 5f2b bf70 28e1 d4a1  ...1...._+.p(...
00000060: b30c 245d 2209 055e e183 0fe4 d4ea c6aa  ..$]"..^........
00000070: 8508 0de1 25f9 0896 44e5 b6ea ac7d f38a  ....%...D....}..
00000080: 3132 4cd2 83ea 8e73 a777 58be 31b3 dcf4  12L....s.wX.1...
00000090: 6fca d1f1 a20f a8d6                      o.......
harshal-pc@harshal:~/MNIT CODES/SIC$ 
```

2.3 Cipher Feedback Mode (CFB)

- As we can see that there are no similarities between CFB and ECB or CBC mode.
- The encryption and decryption commands are -

  $openssl enc −des−cfb −e −iv 0000000000000000 −in sample_2 −out output_2

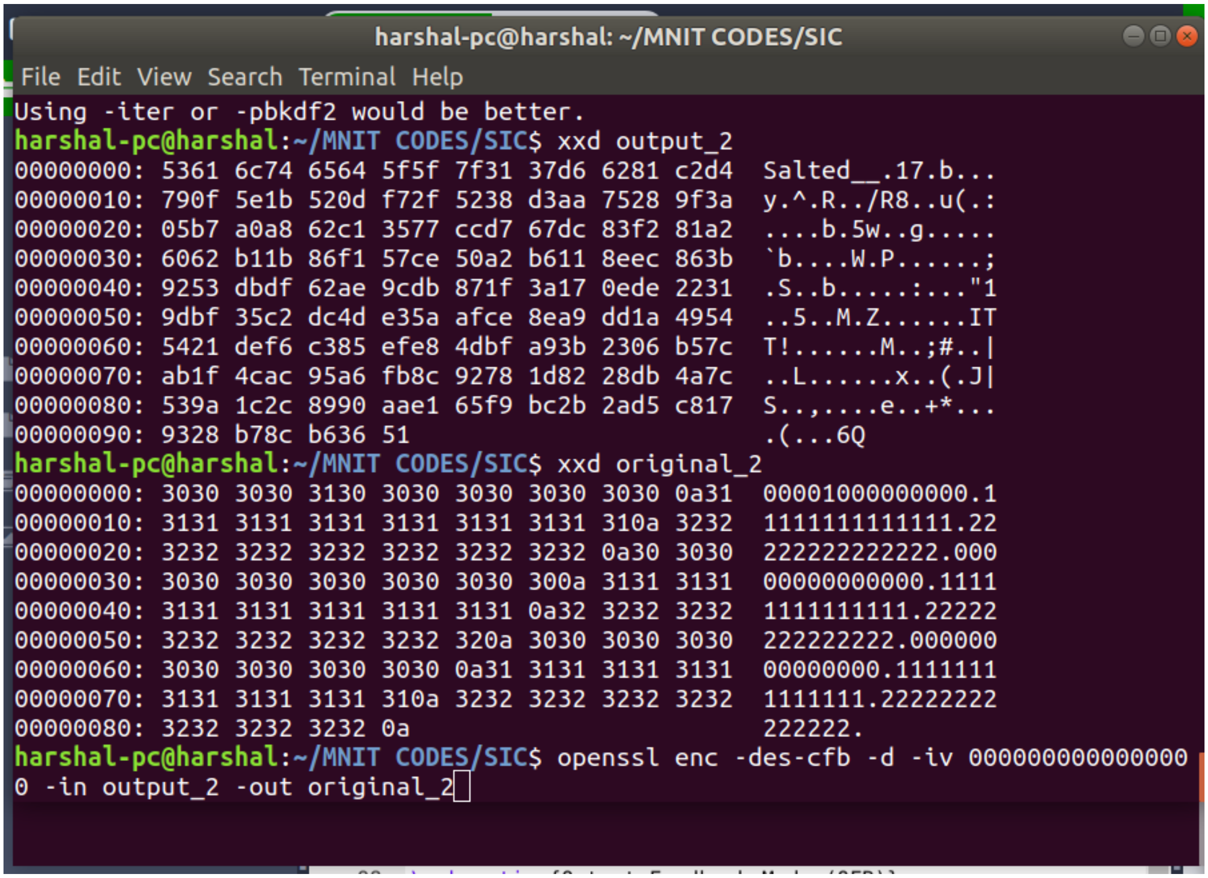
  $ openssl enc −des−cfb −d −iv 0000000000000000 −in output_2 −out original_2



harshal-pc@harshal: ~/MNIT CODES/SIC
File Edit View Search Terminal Help

```
Using -iter or -pbkdf2 would be better.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample_2
00000000: 3030 3030 3130 3030 3030 3030 3030 0a31  00001000000000.1
00000010: 3131 3131 3131 3131 3131 3131 310a 3232  1111111111111.22
00000020: 3232 3232 3232 3232 3232 3232 0a30 3030  222222222222.000
00000030: 3030 3030 3030 3030 3030 300a 3131 3131  00000000000.1111
00000040: 3131 3131 3131 3131 3131 0a32 3232 3232  1111111111.22222
00000050: 3232 3232 3232 3232 320a 3030 3030 3030  222222222.000000
00000060: 3030 3030 3030 3030 0a31 3131 3131 3131  00000000.1111111
00000070: 3131 3131 3131 310a 3232 3232 3232 3232  1111111.22222222
00000080: 3232 3232 3232 0a                        222222.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd output_2
00000000: 5361 6c74 6564 5f5f 7f31 37d6 6281 c2d4  Salted__.17.b...
00000010: 790f 5e1b 520d f72f 5238 d3aa 7528 9f3a  y.^.R../R8..u(.:
00000020: 05b7 a0a8 62c1 3577 ccd7 67dc 83f2 81a2  ....b.5w..g.....
00000030: 6062 b11b 86f1 57ce 50a2 b611 8eec 863b  `b....W.P......;
00000040: 9253 dbdf 62ae 9cdb 871f 3a17 0ede 2231  .S..b.....:..."1
00000050: 9dbf 35c2 dc4d e35a afce 8ea9 dd1a 4954  ..5..M.Z......IT
00000060: 5421 def6 c385 efe8 4dbf a93b 2306 b57c  T!......M..;#..|
00000070: ab1f 4cac 95a6 fb8c 9278 1d82 28db 4a7c  ..L.......x..(.J|
00000080: 539a 1c2c 8990 aae1 65f9 bc2b 2ad5 c817  S..,....e..+*...
00000090: 9328 b78c b636 51                        .(...6Q
harshal-pc@harshal:~/MNIT CODES/SIC$ openssl enc -des-cfb -d -iv 000000000000000
0 -in output_2 -out original_2
```

- Also observe the bits changed due to single error bit.

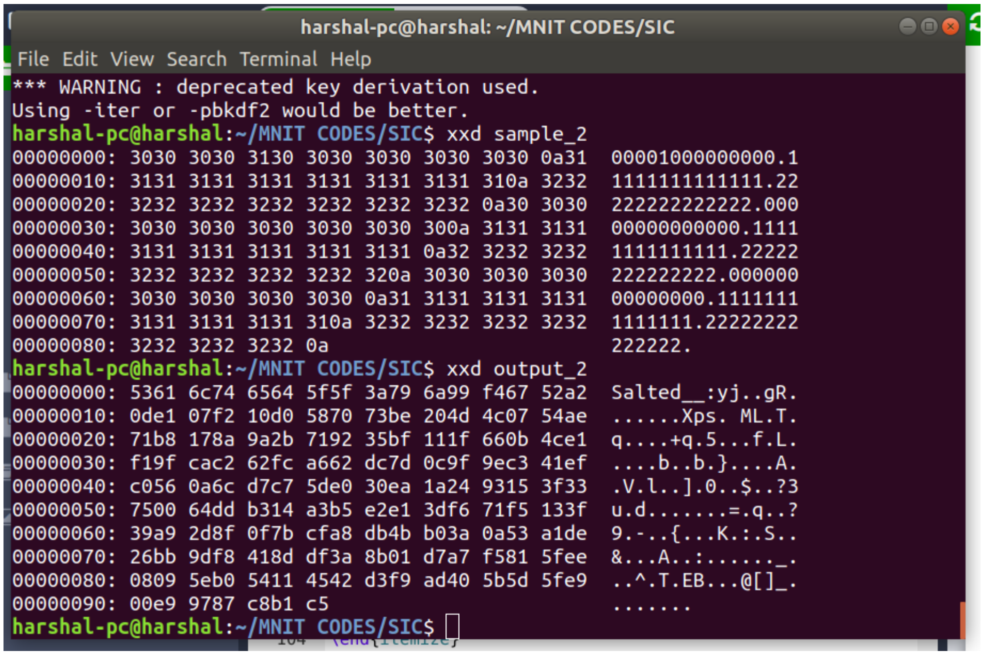


harshal-pc@harshal: ~/MNIT CODES/SIC
File Edit View Search Terminal Help

```
Using -iter or -pbkdf2 would be better.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd output_2
00000000: 5361 6c74 6564 5f5f 7f31 37d6 6281 c2d4  Salted__.17.b...
00000010: 790f 5e1b 520d f72f 5238 d3aa 7528 9f3a  y.^.R../R8..u(.:
00000020: 05b7 a0a8 62c1 3577 ccd7 67dc 83f2 81a2  ....b.5w..g.....
00000030: 6062 b11b 86f1 57ce 50a2 b611 8eec 863b  `b....W.P......;
00000040: 9253 dbdf 62ae 9cdb 871f 3a17 0ede 2231  .S..b.....:..."1
00000050: 9dbf 35c2 dc4d e35a afce 8ea9 dd1a 4954  ..5..M.Z......IT
00000060: 5421 def6 c385 efe8 4dbf a93b 2306 b57c  T!......M..;#..|
00000070: ab1f 4cac 95a6 fb8c 9278 1d82 28db 4a7c  ..L......x..(.J|
00000080: 539a 1c2c 8990 aae1 65f9 bc2b 2ad5 c817  S..,....e..+*...
00000090: 9328 b78c b636 51                        .(...6Q
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd original_2
00000000: 3030 3030 3130 3030 3030 3030 3030 0a31  0000100000000.1
00000010: 3131 3131 3131 3131 3131 3131 310a 3232  1111111111111.22
00000020: 3232 3232 3232 3232 3232 3232 0a30 3030  222222222222.000
00000030: 3030 3030 3030 3030 3030 300a 3131 3131  00000000000.1111
00000040: 3131 3131 3131 3131 3131 0a32 3232 3232  1111111111.22222
00000050: 3232 3232 3232 3232 320a 3030 3030 3030  222222222.000000
00000060: 3030 3030 3030 3030 0a31 3131 3131 3131  00000000.1111111
00000070: 3131 3131 3131 310a 3232 3232 3232 3232  1111111.22222222
00000080: 3232 3232 3232 0a                        222222.
harshal-pc@harshal:~/MNIT CODES/SIC$ openssl enc -des-cfb -d -iv 000000000000000
0 -in output_2 -out original_2
```

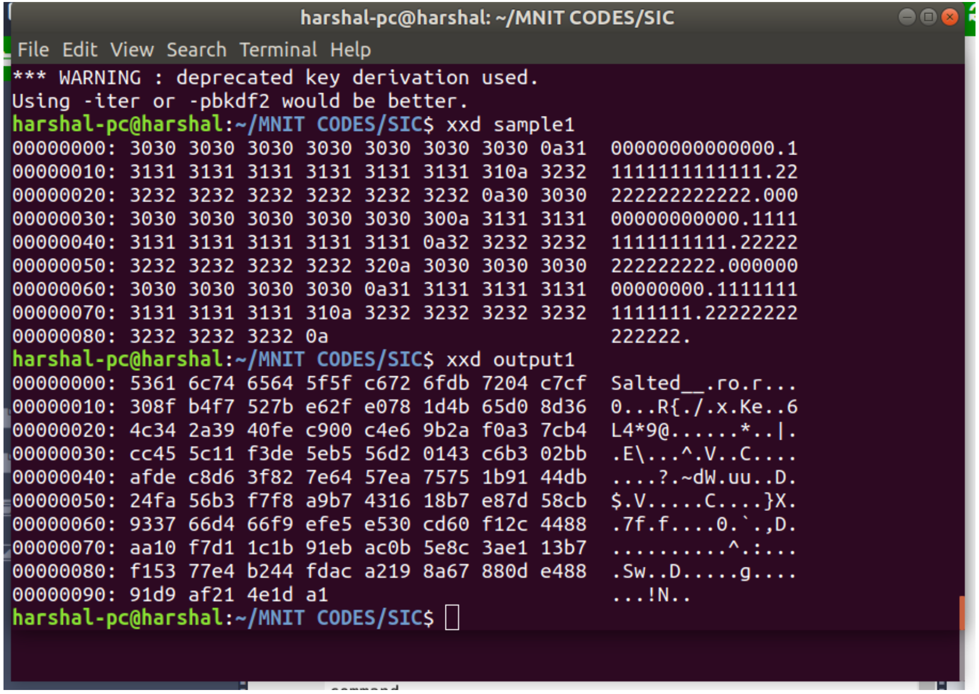
2.4 Output Feedback Mode (OFB)

- Here we observe that, due to a single error bit only one bit is being changed in the encrypted file.



harshal-pc@harshal: ~/MNIT CODES/SIC
File Edit View Search Terminal Help

```
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample_2
00000000: 3030 3030 3130 3030 3030 3030 3030 0a31  00001000000000.1
00000010: 3131 3131 3131 3131 3131 3131 310a 3232  1111111111111.22
00000020: 3232 3232 3232 3232 3232 3232 0a30 3030  222222222222.000
00000030: 3030 3030 3030 3030 3030 300a 3131 3131  00000000000.1111
00000040: 3131 3131 3131 3131 3131 0a32 3232 3232  1111111111.22222
00000050: 3232 3232 3232 3232 320a 3030 3030 3030  222222222.000000
00000060: 3030 3030 3030 3030 0a31 3131 3131 3131  00000000.1111111
00000070: 3131 3131 3131 310a 3232 3232 3232 3232  1111111.22222222
00000080: 3232 3232 3232 0a                        222222.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd output_2
00000000: 5361 6c74 6564 5f5f 3a79 6a99 f467 52a2  Salted__:yj..gR.
00000010: 0de1 07f2 10d0 5870 73be 204d 4c07 54ae  ......Xps. ML.T.
00000020: 71b8 178a 9a2b 7192 35bf 111f 660b 4ce1  q....+q.5...f.L.
00000030: f19f cac2 62fc a662 dc7d 0c9f 9ec3 41ef  ....b..b.}....A.
00000040: c056 0a6c d7c7 5de0 30ea 1a24 9315 3f33  .V.l..].0..$..?3
00000050: 7500 64dd b314 a3b5 e2e1 3df6 71f5 133f  u.d.......=.q..?
00000060: 39a9 2d8f 0f7b cfa8 db4b b03a 0a53 a1de  9.-..{...K.:.S..
00000070: 26bb 9df8 418d df3a 8b01 d7a7 f581 5fee  &...A..:......_.
00000080: 0809 5eb0 5411 4542 d3f9 ad40 5b5d 5fe9  ..^.T.EB...@[]_.
00000090: 00e9 9787 c8b1 c5                        .......
harshal-pc@harshal:~/MNIT CODES/SIC$ 
```



harshal-pc@harshal: ~/MNIT CODES/SIC
File Edit View Search Terminal Help

```
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd sample1
00000000: 3030 3030 3030 3030 3030 3030 3030 0a31  00000000000000.1
00000010: 3131 3131 3131 3131 3131 3131 310a 3232  1111111111111.22
00000020: 3232 3232 3232 3232 3232 3232 0a30 3030  222222222222.000
00000030: 3030 3030 3030 3030 3030 300a 3131 3131  00000000000.1111
00000040: 3131 3131 3131 3131 3131 0a32 3232 3232  1111111111.22222
00000050: 3232 3232 3232 3232 320a 3030 3030 3030  222222222.000000
00000060: 3030 3030 3030 3030 0a31 3131 3131 3131  00000000.1111111
00000070: 3131 3131 3131 310a 3232 3232 3232 3232  1111111.22222222
00000080: 3232 3232 3232 0a                        222222.
harshal-pc@harshal:~/MNIT CODES/SIC$ xxd output1
00000000: 5361 6c74 6564 5f5f c672 6fdb 7204 c7cf  Salted__.ro.r...
00000010: 308f b4f7 527b e62f e078 1d4b 65d0 8d36  0...R{./.x.Ke..6
00000020: 4c34 2a39 40fe c900 c4e6 9b2a f0a3 7cb4  L4*9@......*..|.
00000030: cc45 5c11 f3de 5eb5 56d2 0143 c6b3 02bb  .E\...^.V..C....
00000040: afde c8d6 3f82 7e64 57ea 7575 1b91 44db  ....?.~dW.uu..D.
00000050: 24fa 56b3 f7f8 a9b7 4316 18b7 e87d 58cb  $.V.....C....}X.
00000060: 9337 66d4 66f9 efe5 e530 cd60 f12c 4488  .7f.f....0.`.,D.
00000070: aa10 f7d1 1c1b 91eb ac0b 5e8c 3ae1 13b7  ..........^.:...
00000080: f153 77e4 b244 fdac a219 8a67 880d e488  .Sw..D.....g....
00000090: 91d9 af21 4e1d a1                        ...!N..
harshal-pc@harshal:~/MNIT CODES/SIC$ 
```

2.5 Counter Mode

- This is not possible using **openssl enc -des** command