

Task 1: Frequency Analysis

Frequency analysis table for English alphabets

E	11.1607%	56.88	M	3.0129%	15.36
A	8.4966%	43.31	H	3.0034%	15.31
R	7.5809%	38.64	G	2.4705%	12.59
I	7.5448%	38.45	B	2.0720%	10.56
O	7.1635%	36.51	F	1.8121%	9.24
T	6.9509%	35.43	Y	1.7779%	9.06
N	6.6544%	33.92	W	1.2899%	6.57
S	5.7351%	29.23	K	1.1016%	5.61
L	5.4893%	27.98	V	1.0074%	5.13
C	4.5388%	23.13	X	0.2902%	1.48
U	3.6308%	18.51	Z	0.2722%	1.39
D	3.3844%	17.25	J	0.1965%	1.00
P	3.1671%	16.14	Q	0.1962%	(1)

Given cipher text is:-

hfcnkopw ahyplhp ya wznysgj hxzlvylv oxp qfwgs qyox lpq spdpfncploa xznnplylv pdpwj
 szj z wyvfwfka pskhzoyfl hcceylylv oxp oxpfwj fu ylufwczoyfl zls hfcnkkozoyfl qyox xlslafl
 ajaopca zls afuoqzwp spayvl ya oxp ipj of akhhpaa za flp fu oxp fgspao hfcnkopw ahyplhp
 spnzwoocploa yl oxp hxyhzvf zwpz oxp ha spnzwoocplo zo yyo xza z gflv xyaofwj fu cppoylv
 oxya hxzggplvp oxwfkvx mkzgyoj pskhzoyfl yl aczgg hgzaawffc pldywflcploa zgflv qyox
 ylopwlaxyn zls wpapzwhx fnnfwoklyoypa yl ylskaowj zls lzoyflzg gzfewzofwypa
 yyo aoksploa qfwj qyox fkw uzhkgoj fl qfwgshgzaa wpapzwhx yl zwpza oxzo ylhgksp szoz
 ahyplhp syaowyekops ajaopca ylufwczoyfl wpowypdzg hfcnkopw lpoqfwiyv ylopddyvpl
 ylufwczoyfl ajaopca zls zgvfywoxca
 oxp spnzwoocplo fuupwa ezhxpgfw fu ahyplhp czaopw fu ahyplhp nwfupaayflzg czaopw zls
 nxs spvwppa ngka vwzskzop hpwoyuyhzopa zhpgpwzops hfkwapa zls lfspvwpp aoksj
 nzwooycp aoksploa hzl ozip pdplylv hgzaapa zls gflvsyaozlhp aoksploa hzl pzwl czaopwa
 spvwppa flgylp aoksploa wzop fkw opzhxylv za zcflv oxp epao zo oxp klydpwayoj zls fkw
 uzhkgoj xzdp qfl lkcpwfka opzhxylv zqzwsa
 oxp aphwpo aploplhp ya vffs bfe vkja

Frequency analysis for our cipher text:

	11	11	11	11
P	116.	12.07%	■	■
O	93.	9.68%	■	■
L	85.	8.84%	■	■
A	81.	8.43%	■	■
Z	79.	8.22%	■	■
Y	68.	7.08%	■	■
F	64.	6.66%	■	■
W	61.	6.35%	■	■
H	45.	4.68%	■	■
S	41.	4.27%	■	■
X	35.	3.64%	■	■
K	31.	3.23%	■	■
G	30.	3.12%	■	■
C	26.	2.71%	■	■
V	26.	2.71%	■	■
N	18.	1.87%	■	■
J	16.	1.66%	■	■
U	15.	1.56%	■	■
Q	12.	1.25%	■	■
D	7.	0.73%	■	■
E	6.	0.62%	■	■
I	4.	0.42%	■	■
M	1.	0.1%	■	■
B	1.	0.1%	■	■
#N : 24 Σ = 961.00 Σ = 100.00 #N : 24				

Decrypting cipher text -> plain text:

We can observe that cipher text has unigram that is ‘z’

Substitute **z** -> **A**

Using command ‘grep a cipher.txt’, we will find the occurrences of ‘a’ in ‘cipher.txt’

We observe that ‘a’ has occurred as the initial letter, middle letter and last letter

Most frequent final letters in English are -> e s d n t

Most frequent initial letters in English are -> t a s o i

By analysing our cipher text, substitute **a** -> **S**

After substitution we observe yS, yl

These can be is, in so let’s substitute **y** -> **I(i)** and **I(L)** -> **N**

Based on the frequency analysis tables of english and cipher text

p is the most frequent letter in cipher text

E is the most frequent letter in English language **p** -> **E**

By observing cipher text we find,

ANs, ShIENhE, Oxe, Ao, Ilo

Substitute,

s -> **D**, **h** -> **C**, **o** -> **T**

After the substitution we observe words like

TxAT, TxE, TxIS

Substitute, **x** -> **H**

Now , we observe words like qITH, TEACHINv, STkDENTS, cEETING

By prediction we can substitute, **q** -> **W**, **v**->**G**, **k** -> **U**, **c** -> **M**

After substitution of the above we observe words like EDUCATIfN, SjSTEMS, MASTEwS, DEGwEES

By prediction we can substitute **f** -> **O**, **j** -> **Y**, **w** -> **R**

After substitution of the above we observe COMnUTER here we can substitute **n** -> **P**

After substitution of the above we observe RAPIDgY here we can substitute **g** -> **L**

After the above substitution we observe DEdELOPMENTS, COMeINING,
INuORMATION, iEY

By prediction we substitute **d** -> **V**, **e** -> **B**, **u** -> **F**, **i** -> **K**

After substitution of the above we observe mUALITY

By prediction we substitute **m** -> **Q**

After substitution of the above we observe bOB

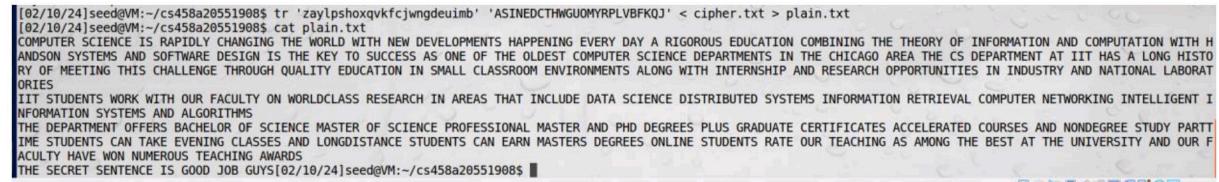
To predict this we can know that 3 letter words ending with ‘OB’ are
bob,cob,dod,fob,gob,hob,job,.....

Here, in our context ‘job’ can be the predicted word

So, substitute **b** -> **J**

Finally the below command is used to convert the cipher text into our predicted plaintext:

```
tr 'zaylpshoxqvfcjwngdeuimb' 'ASINEDCTHWGUOMYRPLVBFKQJ' < cipher.txt >  
plain.txt
```



```
[02/10/24]seed@VM:~/cs458a205519085 tr 'zaylpshoxqvfcjwngdeuimb' 'ASINEDCTHWGUOMYRPLVBFKQJ' < cipher.txt > plain.txt  
[02/10/24]seed@VM:~/cs458a205519085 cat plain.txt  
COMPUTER SCIENCE IS RAPIDLY CHANGING THE WORLD WITH NEW DEVELOPMENTS HAPPENING EVERY DAY A RIGOROUS EDUCATION COMBINING THE THEORY OF INFORMATION AND COMPUTATION WITH H  
ANDSON SYSTEMS AND SOFTWARE DESIGN IS THE KEY TO SUCCESS AS ONE OF THE OLDEST COMPUTER SCIENCE DEPARTMENTS IN THE CHICAGO AREA THE CS DEPARTMENT AT IIT HAS A LONG HISTO  
RY OF MEETING THIS CHALLENGE THROUGH QUALITY EDUCATION IN SMALL CLASSROOM ENVIRONMENTS ALONG WITH INTERNSHIP AND RESEARCH OPPORTUNITIES IN INDUSTRY AND NATIONAL LABORAT  
ORIES  
IIT STUDENTS WORK WITH OUR FACULTY ON WORLDCLASS RESEARCH IN AREAS THAT INCLUDE DATA SCIENCE DISTRIBUTED SYSTEMS INFORMATION RETRIEVAL COMPUTER NETWORKING INTELLIGENT I  
NFORMATION SYSTEMS AND ALGORITHMS  
THE DEPARTMENT OFFERS BACHELOR OF SCIENCE MASTER OF SCIENCE PROFESSIONAL MASTER AND PhD DEGREES PLUS GRADUATE CERTIFICATES ACCELERATED COURSES AND NONDEGREE STUDY PARTI  
IME STUDENTS CAN TAKE EVENING CLASSES AND LONGDISTANCE STUDENTS CAN EARN MASTERS DEGREES ONLINE STUDENTS RATE OUR TEACHING AS AMONG THE BEST AT THE UNIVERSITY AND OUR F  
ACULTY HAVE WON NUMEROUS TEACHING AWARDS  
THE SECRET SENTENCE IS GOOD JOB GUYS[02/10/24]seed@VM:~/cs458a205519085$
```

TASK-2 Encryption using Different Ciphers and Modes

Creating a file using ‘touch’ and writing file contents using ‘gedit’. ‘cat’ is used to display the contents of the file

```
[02/10/24]seed@M:~/cs458a20551908$ touch file.txt
[02/10/24]seed@M:~/cs458a20551908$ gedit file.txt
[02/10/24]seed@M:~/cs458a20551908$ cat file.txt
Information Security is very important from day to day life to protect your Information online. Learning how to protect yourself online can benefit you in many ways by keeping your identity from being stolen or your bank account being compromised. Everyday people are led into scams to take information to use it for their own cause. Also learning Infosec is easy to get into. There are many websites and articles to read on to learn about attacks and what to do in a situation.
[02/10/24]seed@M:~/cs458a20551908$
```

BLOWFISH

bf-cbc(BLOWFISH-CIPHER BLOCK CHAINING)

```
[02/10/24]seed@M:~/cs458a20551908$ openssl enc -bf-cbc -e -in file.txt -out bfcbc.bin -K 00010203040506070809aabcccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/10/24]seed@M:~/cs458a20551908$ xxd bfcbc.bin
00000000: ab96 b0fa d643 9e0b 5720 c8ce c8b7 59a0 ...dc..W....Y.
00000010: 41b9 bb7f 57a5 a082 57f1 e623 a1c3 7b10 A..W..W.#.{.
00000020: f706 087d a5dc 10f8 3d78 7927 e786 5ac4 }...=X'..Z.
00000030: 9821 2f3f 8bd5 fd12 a243 b3f4 989f dbee !?/.C.....
00000040: f165 734a 2ef8 0bd6 66a3 7b85 fa02 1b6d .esj...f{....m
00000050: c377 33e6 9821 4679 0396 3215 1b03 cf53 .w3..!Fy..2...S
00000060: bf73 1362 81d4 182b la1a 8cfc 5ec1 e11b ..b...+...^...
00000070: 8a42 0479 b81e 7c2b cf23 5054 3e24 64b6 .B.y..|+.#PT>sd
00000080: e9e6 2f57 b4df db3b d2d9 f8c1 38c7 abb2 .W..0b..8.
00000090: bebc 7a16 fbcb 3b2a e7e1 d686 9ef9 7ae7 .z...*...z.
000000a0: 3878 6873 7b5b ab5b c548 78a2 946a c497 8xhs{[.Hx...
000000b0: 4ef6 f584 8819 2c28 af51 044a 2637 0ffe N...{.0.J67...
000000c0: a827 729a ad06 532d 0d75 abcd 49ef b1bd 'r..S)u.I.
000000d0: 99d3 4ed1 830a 17af d8c0 bd35 0152 17e5 'N...u...5.R.
000000e0: b8c2 6e65 10b6 b726 4a67 c3d4 4925 5b73 ne...&Jg.I%{s
000000f0: 8986 86b6 1368 3adb 4f3f 0bea 8984 27d3 ..h:07...
00000100: 4fea cd2b 90b0 8418 8776 b7dc d458 8da7 0.+...p..X.
00000110: 09dd 2d8c 0e4d 4378 9ed0 06a3 ca4c 2c37 .-.MCx...N7
00000120: 73fb 4174 8225 489c 5fce aad3 8ad7 0b21 s.At.%H...I
00000130: 2c8b 295a 6f5e 6f69 69b2 d821 5afe 4b76 )Zo...i..!Z.Kv
00000140: cf1e 8ef9 25b6 65fc d086 7027 8e23 d2cf ...%e...p.#.
00000150: 1fb6 d015 3602 9699 365d b7ee afff6 f80a ...6...6)...
00000160: e4ac 6462 0cd8 59fe la75 8d36 c7d3 85f6 db..Y..u.6...o
00000170: 3257 a982 3807 b41e a7d5 13bc 21d3 9412 2W..8...|...
00000180: 8972 230d 3d86 42da 6a39 e9f9 29b3 0207 #.=B.J9...)...
00000190: 206d 68dc cba5 e73c e980 cc79 10f2 78d3 m...<...y.x.
000001a0: 925d 6866 ae6e a962 4661 6725 0d1e 61bb ljf..Fa.%o.
000001b0: 2d59 4f36 47bc 5a11 5fb0 719d a5c5 3713 -Y06G.J...7.
000001c0: 55fc 1391 ead2 1860 ae34 a7e4 39e2 89fc U....m.4.t9...
000001d0: 80a3 9929 53a2 4419 lcde 97c1 84a6 4f99 ...)S.D.....o.
[02/10/24]seed@M:~/cs458a20551908$
```

bf-ofb(BLOWFISH-OUTPUT FEEDBACK)

```
[02/10/24]seed@M:~/cs458a20551908$ openssl enc -bf-ofb -e -in file.txt -out bfofb.bin -K 00010203040506070809aabcccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/10/24]seed@M:~/cs458a20551908$ xxd bfofb.bin
00000000: ea17 9982 d250 1fcc 718d f0a8 4496 348c ...P..q...D.
00000010: d8e5 1ba9 95e7 12a8 8ff3 04ec 8272 632b ...r...r...rc.
00000020: 3332 1812 ddb5 e8ad 05b2 a79c 54f3 f8d1 32...T...
00000030: 24a2 123b b984 193b 7391 8d40 6898 2a03 $..8...s..gh*.
00000040: 805a b0c7 bfaa 6ab9 455a 6786 7848 e42b Z...j..E'g..xN+.
00000050: dc5b 1d0c 94e3 4fa1 d4ea 576e e85b 1e99 [..OA..W..l..
00000060: 2a49 cd91 d6c1 2d7d 50e3 948c d10b 1d7a *1...P....z
00000070: 7312 5046 13a0 1a10 61a1 d1c6 1d4a d.VF..K..+4...z
00000080: 177f 017f 017f 017f 017f 017f 017f 017f X...D5.v
00000090: 64fa a06c c16a a029 514c brd6 f048 41fb d..l..j..QL..HA.
000000a0: b689 9b98 3d17 7ff8 ae19 2c9f 1aef 2090 ...r...r...r...r...
000000b0: 8fb6 219e c8bd ab72 8368 9e94 9538 4147 ...l...r.r.h...8AG
000000c0: 4dd2 8390 0751 7f38 9872 4c8b d5c3 748f M...0..8..R..t..
000000d0: 24aa 6fab 66b0 208e 22e2 45ae 7a85 e42e S.o.f..".E.z..
000000e0: 64bb 5787 1f5e 9d8c 1bcc 15da cf25 1b33 d.W...|.3
000000f0: 3bfa c89f 6e5c 7e08 6d04 b11c 7c1b 5b6f ;...~\m...|..o
00000100: 89ec 821f f20f 0ead 4b3a fc1a a844 7c04 .....K8..D].
00000110: 523d 4b77 98d7 4a8a 1rd9 0740 1318 eb8a R=Kw..J...@...
00000120: 334a 226a 3ca5 6f09 8108 3ce9 e4de d60d ...r...r...r...r...
00000130: a51b 2226 3ca5 6f09 8108 3ce9 e4de d60d ...6<...<...
00000140: 8e43 7869 eb65 2d64 e11c 5844 5b6b 0bfe .Cx1.e-d..XD[K...
00000150: 33a5 bf6f b968 6e0d d7d3 af86 75c4 7a0c 3..o..h..n..u.z.
00000160: 95ab 0846 0e97 3a1e 97b7 0e3e af8e 97a6 ...F...:...>...
00000170: 90a8 17b8 f4fc 53d7 2af5 6b96 f537 4775 ...S..*.K..7Gu
00000180: d60c 455b bc22 707d 7d1a fe44 de97 2c8d E.."p)].D...
00000190: e4d5 a6ff ale8 ca3b ab3e 74ea 3785 1961 ...;..>t.7..a
000001a0: a6c3 f1d0 960f e21b 4cfb d268 19ba .....L..(+.
000001b0: 3a1e f493 9e86 9078 8c58 b341 cc75 724a ....x.X.A.u;r]
000001c0: 3681 9126 cc5e a624 4b58 0662 7a38 46a3 6...&.^SKX..zBF.
000001d0: fc6d 3343 58d4 a779 4b93 8d99 2701 .m3CX..yK...'.
[02/10/24]seed@M:~/cs458a20551908$
```

bf-cfb(BLOWFISH-CIPHER FEEDBACK)

```
[02/18/24]seed@M:~/cs458a20551908$ openssl enc -bf-cfb -e -in file.txt -out bfcfb.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/18/24]seed@M:~/cs458a20551908$ xxd bfcfb.bin
00000000: ea17 9902 d250 lfcc 5dc1 3d3d 6384 3f1f .....P..].==c.?
00000010: 5a01 9585 leed bfae 3c99 5421 c9fe 8821 Z.....<|T|..!
00000020: lab5 6b95 48a9 4f0e 3b99 7c88 2152 acbd ..K.H..|.IR.
00000030: 69df e4c4 0e7d db27 5513 994f 6031 4109 i....}.P_0'1A.
00000040: 61b4 bbf4 8e5d c211 c350 7e87 0f21 85b6 =0...G.^~ca6.
00000050: b904 3d40 8b12 0147 a10e 5e23 6361 2687 q.....r!!0..T
00000060: d03c d67b c6e6 37b2 8aa1 3634 478f c967 <...&..646..o
00000070: 7169 1fe9 10d9 8672 9121 5d1e 4fc3 b054 q.....r!!0..T
00000080: 44bb 61d3 2261 55e3 b0f5 0e5a 1781 0b7c D.a..au..Z...
00000090: f62a 3b68 3ec3 46f1 1581 539c 0818 4071 *;>;F..S..@q
000000a0: 1791 89d1 cec7 93ac 04eb d479 f0bf fb7c ....y...
000000b0: 66c5 9693 9789 46f9 2f97 832d e6b1 85ae ....F/...
000000c0: f63b 9296 7a56 abd4 639c 438c f8a8 2d2b ;zV..C.C...+
000000d0: 9947 a5a0 8751 098c 4d67 3e98 f707 33ce G.....Mg>..3.
000000e0: a5ad ee93 d435 3044 7533 d240 2ea7 856e ..500u3.Q..n
000000f0: 270a f5d5 fd3c d226 0f1b 2b19 be1a 0ddd ..<..&..+.
00000100: la2f a5a5 412d e6c6 749c cel9 fd07 70aa ./A..L}.p.
00000110: e63f 5ac3 e1f4 9f2e f43c 3fd8 9bb4 ff03 ?Z.....?.
00000120: 7167 0019 c1d7 3c5c ce59 e81a 0786 de81 qq..<..Y...
00000130: 59ef 1cbc 7e48 0157 b6a2 c6ae 3b15 899f Y..H..W..;...
00000140: eeeb c7bc 3fd8 2ca7 ee63 8433 3c55 b389 ....;..c.3<U.
00000150: 6a6e a0e5 dc19 0478 b50b d6a2 d3c7 7b7b jn.....
00000160: 61fd 451f 2b3e 2086 a90a 6d6b 7e8f 6b58 a.E..>..m..-X
00000170: 3deb cd94 elab e479 2994 8878 5ad9 a23d =....y).xZ..=
00000180: 05a5 6ecf dc6c 4dct cd99 3138 cc39 87f5 .n..M..18.9.
00000190: de96 2bc5 31bd a1f2 3d93 b253 6835 c1a4 ..+..1..=.5h5..
000001a0: c622 922 8260 05e2 6434 3c81 ee65 fd6e ..'.d4<.e.n
000001b0: c354 a561 afab a951 8e69 7a3e ad89 0b6d <T.a..0.iz>..m
000001c0: dc97 d7a4 6b5c 94db 560f alae 1399 ...k..v.....
000001d0: 7371 44ea 1a33 d6a0 c992 6f11 39b2 sqd..3..o.9.
[02/18/24]seed@M:~/cs458a20551908$
```

bf-ecb(BLOWFISH-ELECTRONIC CODEBOOK)

```
[02/18/24]seed@M:~/cs458a20551908$ openssl enc -bf-ecb -e -in file.txt -out bfecb.bin -K 00010203040506070809aabccddeff
[02/18/24]seed@M:~/cs458a20551908$ xxd bfecb.bin
00000000: 5494 b8b1 d060 46ba 6d38 050b af5f 3d84 T....F.mB..Z.
00000010: 6d8d fde5 7927 12ba 814c 3b51 c3a9 m...y/....L;0..
00000020: 6ff8 b842 5a5d c478 ddab 5f8b abb2 o..B..x....
00000030: 0eff 16b9 7722 721b cb09 4898 3946 ec1b ..w^r..H.9F..
00000040: 762b a17e 0665 0b6d bd67 fc2f 4e94 94c6 v+..~.e..g./N..
00000050: f888 4eec 85fc 94ec 94f1 488c 65af 53b6 .N.....H.e.S.
00000060: 640a bdd4 0404 1cb2 03d6 0a4f 0ee0 4684 d.....O.F.
00000070: 762b a17e 0665 0b6d 18e8 d5ec 9e40 746c v+..~.e.....@t1
00000080: 1b91 1714 62f8 78fc 25cc 3abc c51a dc46 ..b.x.%....F
00000090: 9c38 c330 7997 089f f488 ab56 4978 fb43 8.0y.....VIX.C
000000a0: c5e9 ee6a b785 a261 75bb da6b e32a 63d7 ..au..k.$c.
000000b0: 44df 6f61 26aa b66b 93c5 d068 63e1 839b D.o&..K..c...
000000c0: 63b2 e0d0 2910 d18c 0d9d b4ed 2de9 323c C...)......3#
000000d0: 16ac 8a48 affa 07ca dfec 9e8a 1df7 bb1b C...H.....3#
000000e0: 5865 68ab ca6b 404e 3745 e4f0 86a6 489d Xeh..k@N7E..H.
000000f0: a762 20fd 7e01 6c94 71f6 55b6 f48b ead9 ..b..~.l.q.U.
00000100: 0ed5 21a7 50f0 ca9b 7436 40d0 1bf3 8a57 ..I.P..t@..W
00000110: e14d 2933 4068 cle1 be59 fd75 5cd5 cf3d ..M.s@h..Y.u\..-
00000120: d0e7 e7bd 9381 592f 8466 b977 2515 c4a3 ..,...V/.f.W%..-
00000130: 1378 035c 3fed 9b1e 3d18 f6f0 df33 x...?..=...3
00000140: fc11 7b46 0244 e5df 4177 e44a d6e3 757d ..{..D..Aw..J..u.
00000150: f247 0f61 3937 47be dbb2 d5a1 989a 3306 G..a976..3.
00000160: lc18 adba 5470 9c0f 4884 5a45 aeed 8794 ...Tp..H.T....
00000170: 1521 25cd a6e3 d185 2eeb 4717 sf05 322f /%. ..G.._2/
00000180: 6d53 3d96 82d1 ba83 8474 46a1 a19c 068a ms=.....|F.....
00000190: 6bec ab2a fc2e d556 fe69 a516 dafc 6c93 k...V....l.
000001a0: 14a4 4af2 922c e7ac eaas 0b8c 9d3e db3a J...,.V....6.
000001b0: 7d6b 2c65 a5c3 7712 6f41 cfae 679a 338f Jk..e..w..oA..g.3.
000001c0: 4d5f 668b 3782 d7a1 8811 d5b3 ea64 a831 M..f.7.....d.1
000001d0: 155a 97da ec22 379e 17d4 0342 569a 218d Z...=...BV!.
[02/18/24]seed@M:~/cs458a20551908$
```

DES

Des-cbc(DATA ENCRYPTION STANDARD-CIPHER BLOCK CHAINING)

```
[02/18/24]seed@M:~/cs458a20551908$ openssl enc -des-cbc -e -in file.txt -out descbc.bin -K 0001020304050607 -iv 010203040506070809
[02/18/24]seed@M:~/cs458a20551908$ xxd descbc.bin
00000000: 9566 c983 b131 343c 24c8 7cc0 67cc 692b f...14..H|g.i+
00000010: 0351 1662 bd4d 86ab 3a3e 02a3 8867 fd59 ..0.b.M..;18a...
00000020: 52b9 actd b619 ca99 1431 3861 b7c5 11ac R..k..k...18a...
00000030: 87f4 7fe2 e5e5 1356 6a1c 2164 d151 6026 .....Vj..d.0'f
00000040: 2658 62d0 1778 586e e381 b755 a2fd 1472 .6xb..xx...U..f
00000050: 3e8c 132a 8402 99ee 1433 35b8 f716 9c7b >.*...35...{.
00000060: 5981 2a99 169b 8bb8 d200 e458 9ec1 1016 Y.*...x...
00000070: 1466 49b1 7bd9 d7c2 2a3d f3f1 0571 2b91 I..{..|=?1.0+
00000080: 88a3 5eel 3d7e 332c c3c5 celc 3c82 46d8 ..^=-3...<F
00000090: 471b 0819 289e 8328 b987 24e0 bd24 b502 G...(.$.$..
000000a0: 5819 5e0d 5639 f61b b7c3 65b8 34d4 e8a2 X.^V9....e.4.
000000b0: 9564 868c 06e1 54fc b4b2 lae9 c0bf c35c ..d...T....\'
000000c0: dee6 650d 0fae 8167 c820 a0ef f434 cf82 ..e...g...4.
000000d0: fd82 b57e 3d5a d8c9 2e56 c3a9 3881 ..-z...V\..8.
000000e0: 6dcc 074f 17a2 0960 99ab 92a0 bfba4 c6ff m..0.....
000000f0: 7884 3417 194c cbf1 8c8c 972f 9221 c5f7 4..L..../.!..
00000100: 3421 ceff a677 9df6 7a4d 51b5 dcaf fe00 41..w..M0..
00000110: f16c 3bd5 1266 666e 41b7 118d 46ed6 fc78 l..ffnA..Fm.x
00000120: 7996 847c bf73 ffe8 ae06 3f7e 7096 a857 y..|..s..?..p..W
00000130: 39d9 3b72 63aa c528 40f1 0d8e 3d38 4a49 9..rc..(@..=0JI
00000140: e803 e3fb d68b 5e37 588e 6413 4b26 990c ..h'Wx.d.K6..
00000150: 3ad1 20f2 757d 7088 010e 181c 6099 f0f7 ..:..up.....
00000160: 28c5 60d6 851c c8c8 056e 34e5 2107 eddc ..(....4...
00000170: 45dc 5449 155f 7c58 6e80 7cce 6fad 2c52 E..T1..|Xn.|..o..R
00000180: b9b9 a94b 261e a84a e6a7 da6c b571 0711 ..K..J..l.q...
00000190: ec57 d2b6 aac5 46d3 6026 8f1e 10d4 7908 ..W...F..&..y.
000001a0: 7555 25fb 7e30 c919 8271 7860 1731 1ca4 u0%..0..gx..1.
000001b0: bee8 1c76 19be 2cb1 4946 f466 e5b6 7310 ..v...I..f..s.
000001c0: 3b77 71e8 ae8b f1a9 eb91 ba29 6034 3437 ;wQ.....)=47
000001d0: tbf1 06ee 5f21 9fec f721 a116 aa48 6bb4 ....!..!..H...
[02/18/24]seed@M:~/cs458a20551908$
```

Des-cfb(DATA ENCRYPTION STANDARD-CIPHER FEEDBACK)

```
[02/18/24]seed@VM:~/cs458a205519085 openssl enc -des-cfb -e -in file.txt -out descfb.bin -K 0001020304050607 -iv 010203040506070809
[02/18/24]seed@VM:~/cs458a205519085 xxd descfb.bin
00000000: 23a2 4620 fc96 adb3 17d6 0683 d186 436b #.F .....,.ck
00000010: 4db9 e223 23fc 4b0f 4080 7f97 2f69 2586 M..##.K.@@.../%.A
00000020: 0871 3a73 0279 05d1 e4ac 7d6f 70b4 1c41 ..:s.y..,.l}op..A
00000030: bca5 73b5 a81d e751 6a5c 8eda 7791 ae05 .s....0j..w...
00000040: a9fd ed7c 0b8e 948b 1e5e 383b d8f1b 5569 .l....^8;..Ui
00000050: b4aa 0ff6 2bf3 1738 2e72 1cf3 aa2d f1e2 .m+..8r...-
00000060: 8e3f 062e c961 430a a0f8 fd54 b91e e554 ?..aC..T...T
00000070: 17c1 34c7 ed23 85b3 c1a6 d791 f6e5 fc53 4..#...5
00000080: d30c 3039 7a24 fa2e e79d c978 f731 3994 .09z5...x.19.
00000090: cbd1 ead2 3551 d615 ba61 39d2 2661 efce .50..a9.&.
000000a0: 00b4 21c9 11a0 6f1e a63a f6fc 3615 6c1a .!...o...6.l.
000000b0: 367b 048c b5ba 0144 f2cc 4922 7c86 f6aa 6f...D..@!.
000000c0: 8938 467f c87a 61ae 8986 73dc bb47 3934 .8F..za...s..G94
000000d0: 1256 e340 df44 148d 404f ab21 9c88 83b7 .V..@.0..@0.!
000000e0: fb66 9e65 db93 8582 a031 4761 df45 864c .n.e...1G@.E.L
000000f0: 5ac8 2eda a067 2788 5e20 a3le a4e8 ad72 Z...g'..^...r
00000100: 1775 30df 2b0c 2c49 29eb 3a79 3552 d3d1 .u@...I...;5R.
00000110: 96b0 3d38 8aa2 799e 7fea 137d 3e34 c489 .-8...>4L.
00000120: ce45 5fc5 b65a 27ca 839d 6823 e57b 6890 .E..Z...h#.(h
00000130: 41de b691 c301 4bcf 7cab 75c9 8824 7cb4 A...,.K..l.u..<|
00000140: 5b6f -761 bcfd 936c 37f6 4fb3 6d44 801c [o.a...l7v0.mB.
00000150: b25d 42a9 94de 94b1 d048 31b7 92b6 0f8e .JB...H1...
00000160: 5538 407a 2e83 348c 9e9f 97d5 5327 c650 u082...4...S..P
00000170: 61f1b 61a7 d535 09fe 8df4 8aa8 c597 8d5c o.a..5.....\.
00000180: 292d 1957 9ba6 77d7 e3d9 6afe 5a11 .)W....Mj.Z.
00000190: 0291 3679 e723 70a0 186f 4136 d561 973f .6..#p..o.6.a.?
00000196: 1633 9446 3b05 76cd 8909 42bc d076 5599 .3.F; v...B..vU.
000001a0: fe13 3b0e 16a0 8266 e608 76e1 bdb2 98d3 ;.n...f.hv...
000001c0: 37a9 fb34 c47e 2948 ac84 e6df 5bd0 4097 7...4.-)H...[.@"
000001d0: 11f0 9dff e2e0 a133 0639 bcd8 2282 .....3.9...|.
[02/18/24]seed@VM:~/cs458a205519085
```

Des-ofb (DATA ENCRYPTION STANDARD-OUTPUT FEEDBACK)

```
[02/18/24]seed@VM:~/cs458a205519085 openssl enc -des-ofb -e -in file.txt -out desofb.bin -K 0001020304050607 -iv 010203040506070809
[02/18/24]seed@VM:~/cs458a205519085 xxd desofb.bin
00000000: 23a2 4620 fc96 adb3 744a 607d 0ea1 37a6 #.F ....tJ)..7.
00000010: 4e13 9b16 24fc 4fdb 4c9b 44b1 9db2 77fe N...$.....D....
00000020: 48bc eb9f 3d89 fc76 4038 fcle 819f 2bac H....=.w@...+.
00000030: 5d9a c28e a9f6 0352 90d3 3a00 e527 dc6d J....R....\.
00000040: 40b3 e528 8a02 8fa0 f1b8 8c62 c807 4a4e @.({....b..JN
00000050: d837 e382 4f07 689e d10f afde a893 ccda .7..0.h.....
00000060: 4f6b 9e9c 536c 4f12 cc82 9aae fe66 4de0 OK..S10....JM
00000070: 35b6 9eb5 38c8 1688 9ac2 61c4 8292 b7e4 5..8....a....
00000080: bba8 7efd cf1d cb69 69b9 f2b8 5cd6 288d .~...ii....(.
00000090: c4fd c2f2 1c03 8df9 638d 70c5 cce9 93a6 .C.p...
000000a0: 84c5 86b2 658a e6fa 62fa ad88 9ab0 1207 .e..b.....
000000b0: a050 94ce ebf5 8787 8967 da1b a6f0 0203 .P....g.....
000000c0: 9c1c 43f6 32f8 9857 5f54 9562 40e6 4605 C.2..W.T.b@F.
000000d0: 6c80 1289 dd6e 5b3e 1e7a cc57 7284 6f28 l....>_Z.Wr.o(
000000e0: defa 901b 2db1 69df 1c1c c67f fd68 9d54 .i...g.h.T
000000f0: b4a9 f99e ba53 c10b 067f 263c 20fd 6398 .&..c.
00000100: 5e7c 885a ddc2 0239 flia4 a97d dc68 cffa .`1..Z...9...j.h.
00000110: 0711 4cdc 995f b1bb bd8b 666f c853 980a .,...,f.o.S.
00000120: 77c5 2ala d31b 77bc 6539 lec6 0108 7009 w.*..w.e9...p.
00000130: e193 be97 4949 65c2 3827 0247 e5b6 7166 .I!e.'8..G..f
00000140: 1978 b80f 9477 2559 939f 9cd3 81a3 2664 x...W%Y?....d
00000150: 2b4f 342c e2b1 0a61 82e3 51le 6868 2964 +04...a.0.h)d
00000160: e639 3677 69fe 8bad fc86 426f f1fb 6f7d .96w1...Bo..o}
00000170: 3bd4 a290 8850 923e ee04 9678 4c91 216a ;...P>...XL!j
00000180: 78f7 c861 ca40 3d28 520b 75e7 1f22 8a69 x..a.K=(R.u..^i
00000190: b6e2 e0a0 323b 605f 8ced 650c de2c e610 .2;...e.....
000001a0: 9d7b 82a3 d7aa 3a06 fe64 c050 7d71 41a2 {....;D)qA.
000001b0: 72e7 c750 fe34 790b a5f2 a245 1efd d370 r..P..4y...E..p
000001c0: 1295 bf3 0790 c467 fbf1 f69e 6ad1 10fe .....g...j...
000001d0: 49b6 4700 2668 339a 2265 badb e1b6 I.G.&H."e....
[02/18/24]seed@VM:~/cs458a205519085
```

Des-ecb(DATA ENCRYPTION STANDARD-ELECTRONIC CODEBOOK)

```
[02/18/24]seed@VM:~/cs458a205519085 openssl enc -des-ecb -e -in file.txt -out desecb.bin -K 0001020304050607
[02/18/24]seed@VM:~/cs458a205519085 xxd desecb.bin
00000000: 6b51 f624 c3d0 ace9 9af2 64c2 9937 57d5 k0o5....d..7W]
00000010: 4c27 de33 f3f0 46bf 0d74 3d2c 0073 9342 L..3..F..t2..s.B
00000020: 88e3 9c71 05a3 5c4f 0f55 be9b 2b51 ..q..L.U...+Q
00000030: bdd8 07b8 0805 5e27 3706 6661 dc80 3f7b .^...7..a?{_
00000040: 0c96 91a2 5eb2 9d2b blce a207 50d8 7a53 ^....P.zS
00000050: 98b1 be88 9e2f 5101 2d9b a82 a457 442a ./0...-..WD*
00000060: f64f d6ef 253a b1b9 b9db 37d7 8925 6216 .0..%...7..nb.
00000070: 0c96 91a2 5eb2 9d2b 99b3 0dfe 2453 b3b4 .^....$..
00000080: 7d23 ed97 1caa bbf4 9b92 5125 8308 c5a5 #)...%.
00000090: 4012 7447 4a1b fdc8 4cda 4809 6494 59b1 @.tGJ...L.H.d.Y.
000000a0: 7e54 46db bac9 e713 0867 c3ad 8a26 9312 .-TMK...g..&.
000000b0: fb7a 071c b369 32f2 3340 50f3 b32e f246 .z...12.3@P...:.
000000c0: bda0 2967 cedi eb28 0de1 967d 9982 af4f .)g...(.).o.
000000d0: 9c47 1ba1 a445 9011 d859 147c 47e7 d869 .6..E..Y..G..i
000000e0: 8ed3 3ff0 47f3 26fc f3e1 ffea e95b b845 .?..G..&..1..[.E
000000f0: af17 54f4 32eb 379f c518 f76c 2d03 fea4 .T.2.7...1-..
00000100: 34ab 1055 ceab abc8 83c4 5277 4803 70c5 4..U....RwH..p.
00000110: 84fa 1d89 ebe8 9bf4 fded d7ce 19a5 557e .-U-.
00000120: f2b7 6a7a 5025 8ef2 9832 ca7f f59a ff5d .12P...2...l
00000130: b078 c567 4843 f56a b894 62cb da71 61a8 x..gHC.j..b..qa.
00000140: 0e3d 1e3b 28bf 16d9 6dc4 82f9 fa0f c691 =;(.m.....
00000150: c976 808b f577 bc64 9fdf e591 7807 e65c v...w.d...x..\
00000160: 76d0 a0fe 1bad 7ed2 0e96 d115 5c84 7eda v...~...`..`..\
00000170: b07e fff1 a61f e4a7 6695 430e bcc0 3135 .-...f.C..15
00000180: d1ca 44cd 8ade d6cc 51bc f7a9 1f5f 4534 .L...Q...F4
00000190: 08ea ce3a 9a22 710d 6389 990c 0bdf 177a :;"q.c...1...
000001a0: cd38 6f8c 211b f215 8de5 8188 4a1c e596 8l..!...1...
000001b0: bb37 6296 2074 309e ac18 1739 6614 20fd .7b..t0...9f..
000001c0: c5e6 7210 5ac3 58b8 2a26 31b6 fdeb 8cf7 ..r.Z.X..61...
000001d0: d3be 74ed 2734 67f2 76af ff55 e5c8 9810 ..t.'4g.v..U...
[02/18/24]seed@VM:~/cs458a205519085
```

AES

aes-128-ecb(ADVANCED ENCRYPTION STANDARD(128)-ELECTRONIC CODE BOOK)

```
[02/10/24]seed@M:~/cs458a20551908$ openssl enc -aes-128-ecb -e -in file.txt -out aeseccb.bin -K 00010203040506070809aabcccddeff
[02/10/24]seed@M:~/cs458a20551908$ xxd aeseccb.bin
00000000: 6236 c6f8 a19e 3957 477e 6726 7197 ce7c b6...9wG-g6q..|
00000010: 1d3e c976 c6bb 8081 2c4b cd86 4ada f744 .>.v....K..J..D
00000020: f066 ceee c566 0a28 a04b a2aa a017 6a20 .f....f.(.K..)j
00000030: 8576 08d5 81d8 a9b3 23b5 4e58 3a6f ff42 .v.....#.Nx:o.B
00000040: 38e6 af59 e638 acf3 a8dc bb61 f7f0 c120 8..Y.8..a.
00000050: 60b8 ee95 c924 e7f6 75e8 2265 7871 b15f ...$.u."exq_.
00000060: ad85 4b1b 5f76 a4a4 bbb6 5b38 6e11 be96 ..K..v....8n_.
00000070: c23e 32aa ec15 8215 b5b6 207c 231f 54ea .>2....|.T.
00000080: 4813 e95a 63df bedb 75ad 5aa8 7e4b 1fd5 H..Zc..u.Z.-K.
00000090: 1671 4575 bbc5 4715 1d1b a39d 844b 73dc qEu.....Fs.
000000a0: 1339 8d91 1183 2d4c bb26 8d06 a97f 8975 9...-L...u.
000000b0: 6aa8 ae24 6e60 c20b d9a6 7039 5928 c84c .$.n...p9Y).L
000000c0: 0a54 ee0b 4b08 55ab 1f8d a82e e5f5 c8b7 T..K.X.....
000000d0: 8c3a 7626 2621 c30a e2cc 8795 0664 2e06 :.v6/..
000000e0: 06a1 7dd1 75ac 28dc 0461 f723 b7e6 227a .|.u.(.a#.z
000000f0: 2124 c987 a3ba 55c7 f337 0867 949a c355 !$...U..7.g..U
00000100: 4c49 6336 4238 2b1c f767 4c3a afb0 0eb4 L.688+.gl...
00000110: 6a27 57ec cd9d 0e90 b4f6 c5d8 ef46 3507 j.W..F5.
00000120: c807 e231 c2fd 96ba f91a 0550 c2c2 aee9 ..1....P...
00000130: b10d 8741 d8ce 1335 c6a1 089d 79f9 4276 ..A..S...Bv
00000140: e688 59a7 f05f 4c18 f75d 00d1 0874 1bcc .Y..L..j...t.
00000150: c9ce 25fb b3c6 7cb4 1262 4669 66bc 93f3 %.|..|.bf1f.?
00000160: a788 2a9f a8fa ba4d 3185 993b 98f1 a5ef .*...M1.|.
00000170: 343a 41c0 4587 536b 3c00 ba17 fdcc 6f95 4:A.E.Sk<...o.
00000180: b221 b3d0 b50d 7f29 d5e8 b8ee 4173 8f6d !....).As.m
00000190: c83f ad89 9363 5539 8e31 0389 f916 1c6a ?.cu9.1....j
000001a0: 8d1d 5b05 3453 6dc8 07d7 77f1 1b25 91ce [.45m..w.%.
000001b0: 98d6 b367 9bce 843b b567 a72d 2778 97b9 ...g...g.'.
000001c0: e9bc b23f a115 e758 75ad 2fd4 93e4 219c ...?..Xu./!...
000001d0: 8b36 e50b 46cb 4be9 47e0 4e2c 4ee9 dbb6 .6.F.K.G.N.N...
[02/10/24]seed@M:~/cs458a20551908$
```

aes-128-cbc(ADVANCED ENCRYPTION STANDARD(128)-CIPHER BLOCK CHAINING)

```
[02/10/24]seed@M:~/cs458a20551908$ openssl enc -aes-128-cbc -e -in file.txt -out aescbc.bin -K 00010203040506070809aabcccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/10/24]seed@M:~/cs458a20551908$ xxd aescbc.bin
00000000: f73d db5e f365 b1b9 379d 5b90 9726 05fe .=.^e.7.[.+.
00000010: c84b e2a8 c87c 1e6a 9409 f2a8 66e2 f31c ..K..|.j....f.
00000020: 4b4c 4074 bec7 f058 1a8c 878c a3cf cd7b K.@..X..{.
00000030: d6de 1a23 38d5 06d3 c052 784a 1039 6497 ...#...RxJ.9d.
00000040: c4b3 bd13 1b6d 318a 4c72 bb0b 6625 4c7e ....ml.Lr..f\$l-
00000050: 7910 d044 60d1 49fa 7b6e db40 d48f 990a y..@.I.{n@.o...
00000060: 86de 0330 83e8 5b28 bffd 9e38 2b54 1438 ..0..|[..8+1.8
00000070: f779 e6f5 066a ceb8 04e6 932b f78a e824 y..j...+.*.
00000080: ed1f 08e7 6c5b 8766 a37b 047f 17af e3e7 ..|..{....
00000090: 255b 2542 3e25 63c1 1125 6f1d 48e2 e4ec %`>..%..H...
000000a0: 1700 2294 7552 5a02 0e76 a62d c8f2 7ba7 .."uRZ..v..{.
000000b0: 01b6 984a 1031 a2ad f71c d0ae 7557 23ca ..J..1...u#.
000000c0: caaa 1e8b fa1b 3e1f 55e5 47e5 64cf 2437 ..>U.G.d.S7
000000d0: ee5e 6213 0e9b 8f9e 5852 1898 db28 f9b3 ^b...XR..(.
000000e0: ad46 bd1f 6fcc c0ce 17d4 b82a f3ff 7064 F..o...*..pd
000000f0: eb52 cc92 fd2f d16a 5321 87cb cdaf 1e7 R.../.js1.....
00000100: 184a e9b8 e800 ddd4 2a9a bf8b 80d4 189e J...*.
00000110: 7c79 1a1c c2ca 99ba 2576 13e5 4d52 8869 |y...%..MR.i
00000120: e572 0c7a 5c59 a91b 9259 0ce1 b941 ddc9 r.z\Y..Y..A.
00000130: 019f 6099 c3d2 748c 0e17 6876 59d9 2915 ..-t..hvY.).
00000140: cbc8 c30b 2d52 5101 76d9 518a 14db 0ebd ..R0.v.Q.
00000150: e6e2 5b37 69fa 37a1 510e 9068 31db 1f15 ..[91.7.0..1..
00000160: cd4f f85c b221 d0b5 cea4 e1cb 6761 7c53 ..0.\!....g9|5
00000170: 9ba6 3cc4 0a0d 499d dc11 8510 4f1a 4715 ..<....0.G.
00000180: 60d0 df1a f331 87a7 a12d 49c9 400b a5dd ..1...I.|.
00000190: 78fe 53a4 ef2c 8ecc 5eab acc3 e5da a075 X.S....^....u
000001a0: dfe1 570d 7307 e6c6 9a5e c297 082d 0ee9 ..W.s....^....u
000001b0: 56d6 a569 a7f2 db08 8a39 8d28 2aff 5477 V..0....0.*.Tw
000001c0: d2b1 5125 e4d1 d637 73dc 988f 5312 07ff ..0%...75...5...
000001d0: d29a 67e8 9b07 d6be 20f3 4a3e b7ad 9135 ..g.....>....
```

aes-128-cfb(ADVANCED ENCRYPTION STANDARD(128)-CIPHER FEEDBACK)

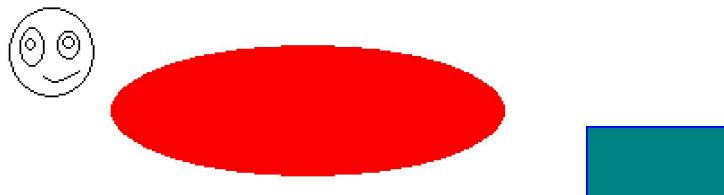
```
[02/18/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cfb -e -in file.txt -out aescfb.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/18/24]seed@VM:~/cs458a20551908$ xxd aescfb.bin
00000000: 8cd5 ef9a 5ee1 266b 3776 2b0c 42aa e59f ...^.&k7v+.B...
00000010: a35d a97a call 9bc2 ee69 a492 3a96 1e93 .j.z....i. .....
00000020: 5209 4d51 29f4 f646 3e40 1953 e21d 87d6 R.MQ...)F>@.S...
00000030: 7ebd 96c5 ddd9 97d9 72a9 fafc eb86 ab70 ~.....r.....p
00000040: ecac 210b f883 1e5f 9c11 4358 cf88 ddd2 .!....-CP...
00000050: efd2 7f6c 3dab 0683 le15 d47a 542e 67e7 ..=_...zT.g...
00000060: 5338 cccb 468a 9e14 4239 68d7 cdaa f13a SB..F...B9h...:.
00000070: 9a59 6072 981b 1086 e368 4488 3715 643c Y'g.....HD.7.d<
00000080: c8d7 3e79 bf06 ecc9 c98a 9728 835a feed .>y.....(Z. .....
00000090: b225 1f65 1513 b6e6 6e6b 6b20 a9e9 36e2 %..e...n.k.6...
00000099: 2889 010c 0b99 ef2f 996c 8914 1c5f 1280 (. .... /l. .....
000000a0: 5e64 6e68 4303 234d 578d 04bf 4f5f a43b `dnhC.#W..0...
000000a8: c52d bf66 e46d 5738 f0d1 eabe 36d4 9fa6 .-....W0...6...
000000d0: ca2e c2ac 6728 122b b9ef 56e7 a1f9 7f15 ..g(.+..V...
000000e0: 92cb 8f37 ac46 5ac2 8a9a 811e e265 blef ..7.FZ...e...
000000f0: 9325 ae8f 164c 82ad 32c6 0838 3cb1 8239 %.L.2..8<.9
00000100: 551f 1a15 9bc3 4d3c f3b1 a87f f82e fe0f U...M.....
00000110: f271 9fb8 581c 82cd 7ea0 ced6 5eef 6f73 ..X....^..os
00000120: 06bb ebef 2b8d d21f 063c 8117 b043 ff04 ..+....-.C...
00000130: d49e 5ffc 628b 000c a8c6 ba9a 9cd5 b9bf ..c.....
00000140: f877 2003 c766 c0db 0e9a 8f74 6b12 81fe ..tk.n...
00000150: f22b cae4 5b4d af2e d0c3 0ade fd8f caa2 +..[M...
00000160: 477c f73 39ed 1147 02b8 3148 edb4 8f61 G..s9..G..1H..a
00000170: 872e 3589 6e9a d4f8 2def fd0d 1a94 8d98 ..5..n.....
00000180: 0fa1 b6e4 5f4d 352a 13dc fdc3 1c2f 0fce ..M5**.....
00000190: fe1f 444d 833e 05f5 7875 ed15 4398 9f03 ..DM.8..xu..C...
000001a0: ce38 7cfa c659 23b2 a53a 20d1 fd65 bf1b2 8|..#.....
000001b0: c02a f4f6 9bd9 a337 bd1e 9e81 9c8a b6cc ..%....7.....
000001c0: 2d1e 1fb1 455e 1016 a398 c29b 72c8 c23c ..E'....r....
000001d0: f83e e3fe 3c2e 6449 6774 9fd2 5d30 ..>..<.digt..0
```

aes-128-ofb(ADVANCED ENCRYPTION STANDARD(128)-OUTPUT FEEDBACK)

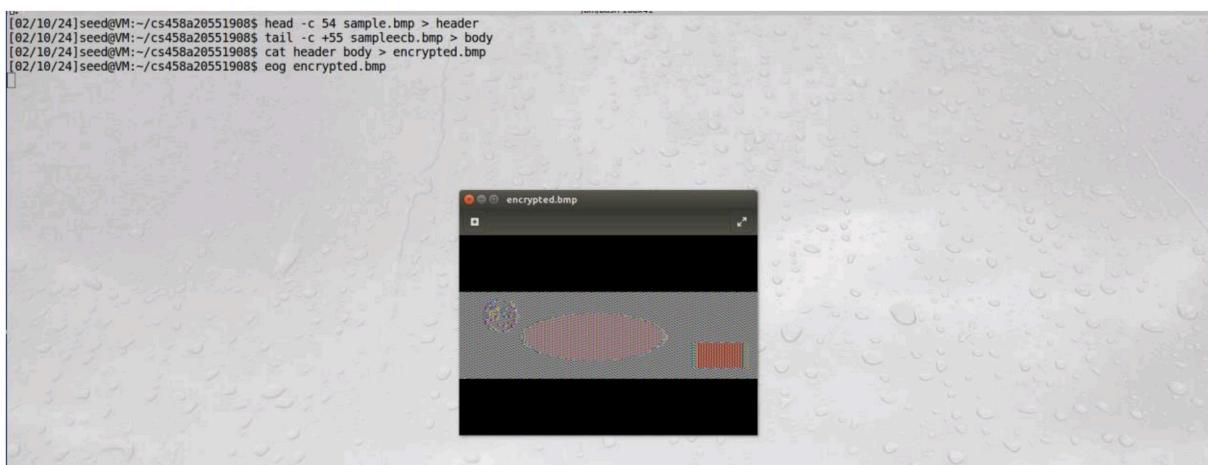
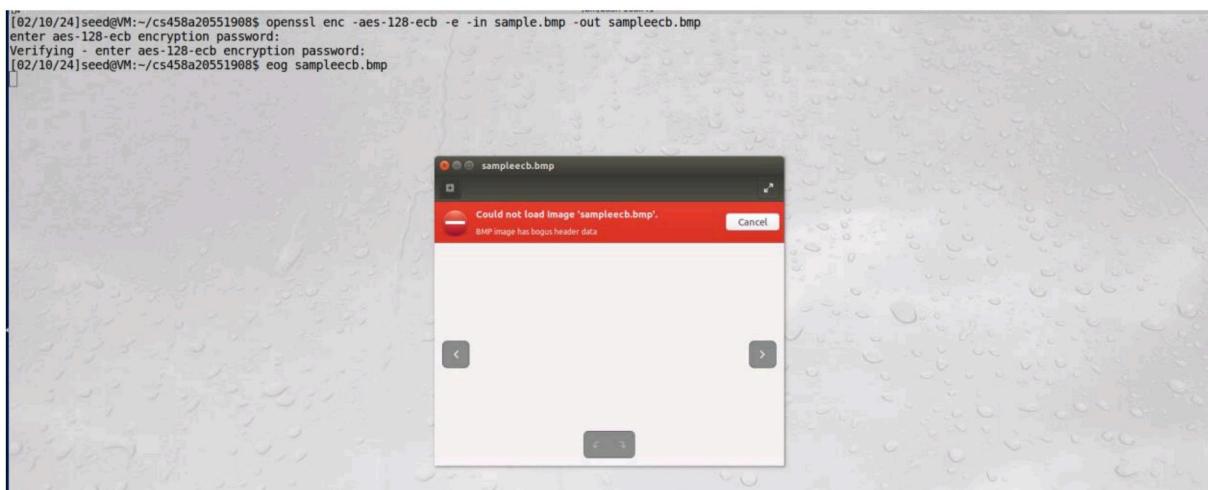
```
[02/18/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-ofb -e -in file.txt -out aesofofbin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/18/24]seed@VM:~/cs458a20551908$ xxd aesofofbin
00000000: 8cd5 ef9a 5ee1 266b 3776 2b0c 42aa e59f ...^.&k7v+.B...
00000010: b2f7 546c 7684 272c c1c3 2016 b714 e738 ..TLv....8
00000020: e8bf 5366 62d7 3610 8892 0144 6444 5664 ..Sfb.6...DdDvD
00000030: fe2b 8ca3 38f3 4848 aca1 aela 3ed5 f344 ..+..B.H1...>..D
00000040: 16c9 05cb c815 296d b9ef e50c 8f16 02fd ..)m...
00000050: ea93 30f6 096a 7e64 5b57 057a d494 2d2d ..0..j-d[W.z...
00000060: cd57 ebe2 391a 5d8d 90bb 776e 0f65 6686 ..W..9..].wn.f...
00000070: 680a d9b8 35cd 5d14 a848 db33 5e90 532b h..5..].H.3^..S+
00000080: 9481 b286 7f42 fa94 84c3 15a1 b705 cccff ..&B.....
00000090: 86d1 aa1c ef8f cee5 9322 94a2 6e5d d022 ..^....n]..
000000a0: ca5b 2529 3984 7638 110b 62ce 4c9a 5884 ..[%9.v8..b.L.P...
000000b0: ac7 0753 f06a fcff bdbe bf2b 02ce 1f98 ..S.j....+...
000000c0: 13de 27e4 f0f3 eb32 7995 1092 1668 8777 ..'.2y...h.w
000000d0: f663 8b30 ceb1 bf25 2577 15ad db98 5745 ..c.0...%w...WE
000000e0: d3ab 8f42 171f bdea 36b7 6beb a10 4826 ..B...6.k..H&
000000f0: 74b4 cf2f e971 f18a 0d59 dc97 7059 4172 t../.q..Y..pYar
00000100: 8858 e402 9d55 4aa3 cf0b 902e 8aa9 9787 ..X..UJ.....
00000110: 0f65 2a0e b418 1cff 8a0b 3d3c a8c9 fb2d e*....=...
00000120: e207 b112 cbcc 4d5a a6be 6b5b 246c c864 ..MZ..k[$1.d
00000130: 08f7 5b93 58c1 ale1 b226 7d1f 059a 9fdb ..[X....&)....
00000140: c69e a959 bf4d 83d5 b2c7 0239 51b1 b786 ..Y....90...
00000150: b8d7 394d 9442 c01e 0e4a f1a1 475c 97b ..91.B...J..Gv...
00000160: leaa a41e bbf7 ec9f 3d1f 0e73 16e4 fe01 ..=.ns...
00000170: 9b73 824f 2345 2207 3446 la7b 7a2a 6eff ..S.#E"4F..{z.n...
00000180: bda9 578c 0a19 7dd9 d157 2e6d dbd9 873b ..W..}.W.m...;
00000190: 74db f5ed bda6 a278 d978 f19b 1d8d da94 t../.x.x.....
000001a0: babf a4ea 8cc6 445d 4577 a4bf 0993 a4f6 ..D1Ew.....
000001b0: afcd 5a5b c193 2281 47d0 7b30 9564 0f2b ..Z|..G.(0.d+.
000001c0: a914 a6d7 4dch 7cdb 9bd9 ef65 d7cd f4ee ..M.|.....
000001d0: 79c2 b401 5e3b c15f 35e9 0b8c 846c y....;..5....l
```

TASK-3 Encryption Mode – ECB vs. CBC

SAMPLE IMAGE-



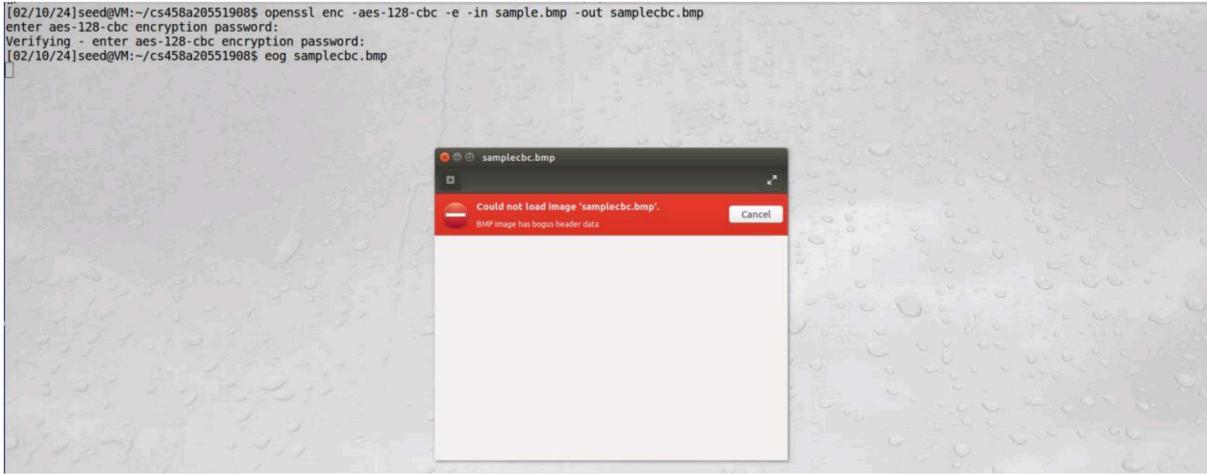
ECB(ELECTRONIC CODE BOOK)



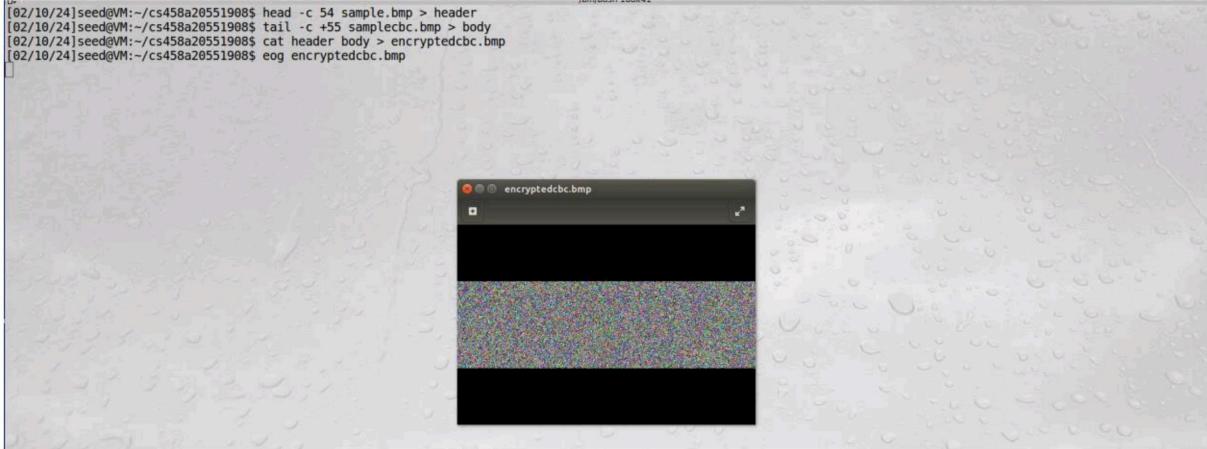
In the above picture, we are able to trace the sample image even after encryption using ecb mode. Therefore, using ecb we are able to derive information about the original picture as the encryption is done independently, identical blocks produce identical outputs ,making it vulnerable to certain attacks.

CBC(CIPHER BLOCK CHAINING)

```
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cbc -e -in sample.bmp -out samplecbc.bmp
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[02/10/24]seed@VM:~/cs458a20551908$ eog samplecbc.bmp
```



```
[02/10/24]seed@VM:~/cs458a20551908$ head -c 54 sample.bmp > header
[02/10/24]seed@VM:~/cs458a20551908$ tail -c +55 samplecbc.bmp > body
[02/10/24]seed@VM:~/cs458a20551908$ cat header body > encryptedcbc.bmp
[02/10/24]seed@VM:~/cs458a20551908$ eog encryptedcbc.bmp
```



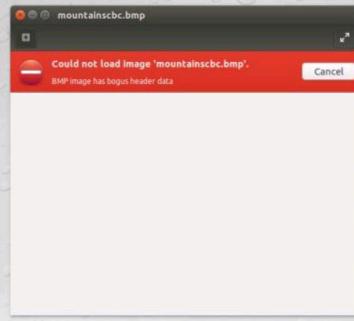
From the above observation, we can see that the picture is encrypted and we don't have any traces of the original picture using cbc mode. In this mode, we cannot derive any useful information from the encrypted picture. Here, encryption is not done independently for each block it is a chain where each ciphertext block is dependent on its previous block.

IMAGE-



CBC

```
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cbc -e -in mountains.bmp -out mountainscbc.bmp
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
Verify failure
bad password read
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cbc -e -in mountains.bmp -out mountainscbc.bmp
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[02/10/24]seed@VM:~/cs458a20551908$ eog mountainscbc.bmp
```

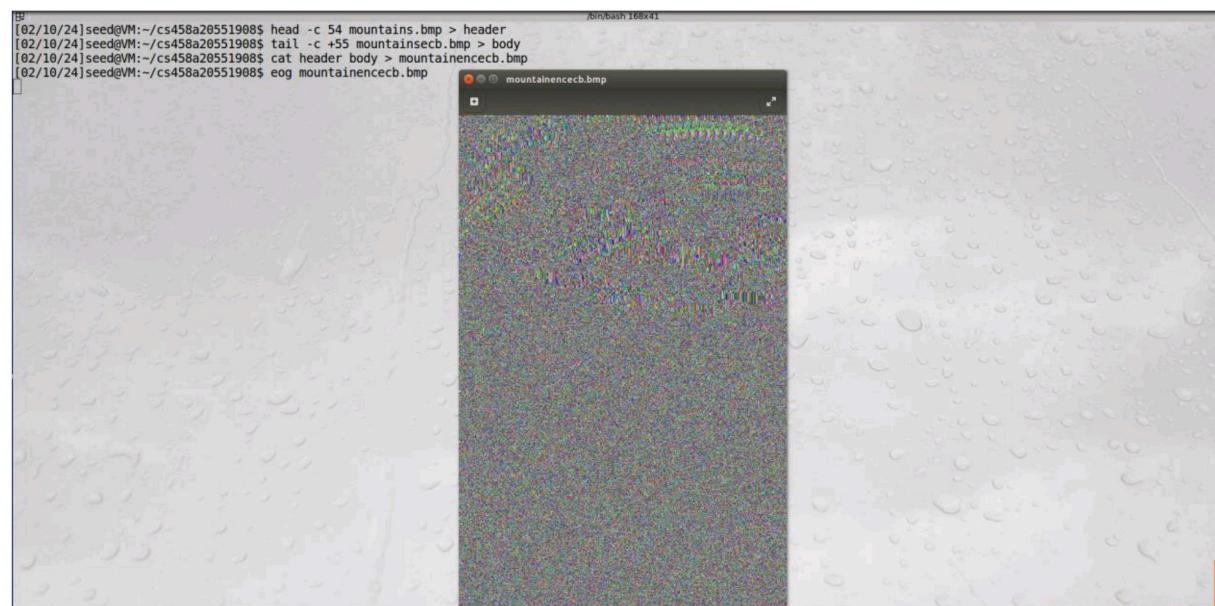
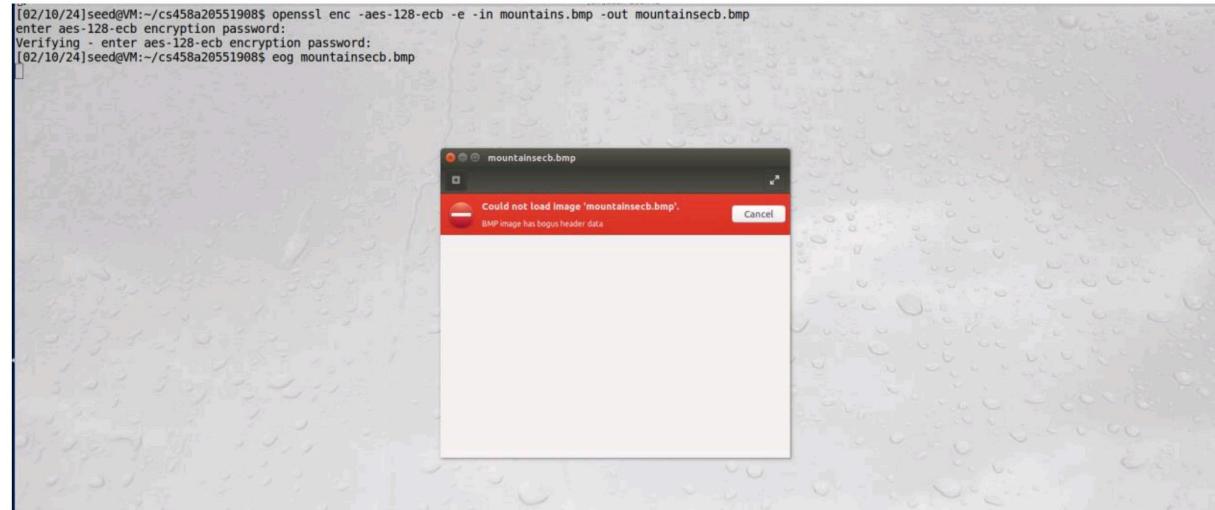


```
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cbc -e -in mountains.bmp -out mountainscbc.bmp
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
Verify failure
bad password read
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cbc
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[02/10/24]seed@VM:~/cs458a20551908$ eog mountainscbc.bmp
[02/10/24]seed@VM:~/cs458a20551908$ head -c 54 mountains.bmp
[02/10/24]seed@VM:~/cs458a20551908$ tail -c +55 mountainscbc
[02/10/24]seed@VM:~/cs458a20551908$ cat header body > mountai
[02/10/24]seed@VM:~/cs458a20551908$ eog mountainencbc.bmp
(eog:28421): EOG-WARNING **: Failed to open file '/home/seed/812acc9aee6.png': No such file or directory
```



In the above observation, attacker cannot predict the original image the whole image is encrypted leaving no trace for attack. As, this is CBC mode it is a chaining mechanism in which the ciphertext of one block affects the encryption of the next block. Similar blocks don't produce similar encrypted blocks.

ECB



In the above observation, even though the attacker cannot directly predict the original image but can observe some similar blocks in the encrypted image.

In conclusion, CBC is preferred over ECB due to its security while encrypting large amounts of data. CBC also eliminates the risk of pattern revealing. CBC requires proper IV selection.

TASK-4 Padding

- 1) Modes that require padding are CBC and ECB. CBC requires padding to ensure the length of plaintext is a multiple of block size to make sure that the last block is full we need padding. ECB encrypts the plain text independently using the same key, length of plain text should be a multiple of block size so when the plain text isn't multiple of block size it needs to be padded to make it equal to the block size.

Modes that does not require padding are CFB and OFB. CFB, in this the cipher text feedback is used for keystream creation, then XOR-ed with the plain text to produce the cipher text, keystream creation ensures plain text of any length to be encrypted without padding. OFB, in this the output of the encryption function is XOR-ed with the plain text to produce cipher text, this process allows plain text of any length to be encrypted without the need of padding.

2)

```
[02/10/24]seed@VM:~/cs458a20551908$ echo -n "12345" > file1.txt
[02/10/24]seed@VM:~/cs458a20551908$ echo -n "0123456789" > file2.txt
[02/10/24]seed@VM:~/cs458a20551908$ echo -n "0123456789123456" > file3.txt
[02/10/24]seed@VM:~/cs458a20551908$ ls -l
total 12024
-rw-rw-r-- 1 seed seed 480 Feb 10 18:31 aescbc.bin
-rw-rw-r-- 1 seed seed 478 Feb 10 18:32 aescfb.bin
-rw-rw-r-- 1 seed seed 480 Feb 10 18:35 aescbcb.bin
-rw-rw-r-- 1 seed seed 478 Feb 10 18:34 aescfb.bln
-rw-rw-r-- 1 seed seed 480 Feb 10 17:52 bfcbc.bln
-rw-rw-r-- 1 seed seed 478 Feb 10 17:54 bfcb.bln
-rw-rw-r-- 1 seed seed 480 Feb 10 17:55 bfccb.bln
-rw-rw-r-- 1 seed seed 478 Feb 10 17:53 bfcb.bln
-rw-rw-r-- 1 seed seed 1843226 Feb 10 20:23 body
-rw-rw-r-- 1 seed seed 1129 Feb 9 18:13 cipher.txt
-rw-rw-r-- 1 seed seed 488 Feb 10 18:25 descbc.bln
-rw-rw-r-- 1 seed seed 478 Feb 10 18:26 descfb.bln
-rw-rw-r-- 1 seed seed 480 Feb 10 17:58 desecb.bln
-rw-rw-r-- 1 seed seed 478 Feb 10 18:27 desofb.bln
-rw-rw-r-- 1 seed seed 184992 Feb 10 19:46 encrypted.bmp
-rw-rw-r-- 1 seed seed 184992 Feb 10 19:46 encrypteddcbc.bmp
-rw-rw-r-- 1 seed seed 5 Feb 10 20:40 file1.txt
-rw-rw-r-- 1 seed seed 10 Feb 10 20:40 file2.txt
-rw-rw-r-- 1 seed seed 16 Feb 10 20:40 file3.txt
-rw-rw-r-- 1 seed seed 478 Feb 10 17:47 file.txt
-rw-rw-r-- 1 seed seed 54 Feb 10 20:23 header
-rw-rw-r-- 1 seed seed 1843280 Feb 10 20:18 mountainccbc.bmp
-rw-rw-r-- 1 seed seed 1843280 Feb 10 20:23 mountainccb.bln
-rw-rw-r-- 1 seed seed 1843256 Feb 10 20:03 mountains.bmp
-rw-rw-r-- 1 seed seed 1843280 Feb 10 20:14 mountainscbc.bln
-rw-rw-r-- 1 seed seed 1843280 Feb 10 20:21 mountainsecb.bln
-rw-rw-r-- 1 seed seed 1129 Feb 10 16:27 plain.txt
-rw-rw-r-- 1 seed seed 184974 Feb 9 18:14 sample.bmp
-rw-rw-r-- 1 seed seed 184992 Feb 10 19:43 sampleccbc.bmp
-rw-rw-r-- 1 seed seed 184992 Feb 10 19:33 sampleccb.bmp
-rw-rw-r-- 1 seed seed 206662 Feb 9 18:13 words.txt
[02/10/24]seed@VM:~/cs458a20551908$
```

Size of file1 -> 5 bytes

Size of file2 -> 10 bytes

Size of file3 -> 16 bytes

ENCRYPTION

```
[02/10/24]seed@VM:~/cs458a205519085 openssl enc -aes-128-cbc -e -in file1.txt -out filelenc.txt -K 00010203040506070809aabcccddeeff -iv 0a0b0c0d0e0f010203040506070809  
[02/10/24]seed@VM:~/cs458a205519085 openssl enc -aes-128-cbc -e -in file2.txt -out file2enc.txt -K 00010203040506070809aabcccddeeff -iv 0a0b0c0d0e0f010203040506070809  
[02/10/24]seed@VM:~/cs458a205519085 openssl enc -aes-128-cbc -e -in file3.txt -out file3enc.txt -K 00010203040506070809aabcccddeeff -iv 0a0b0c0d0e0f010203040506070809  
[02/10/24]seed@VM:~/cs458a205519085 ls -l  
total 12036  
-rw-r--r-- 1 seed seed 480 Feb 10 18:31 aescbc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 18:32 aescfb.bin  
-rw-r--r-- 1 seed seed 480 Feb 10 18:35 aesebc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 18:34 aesofb.bin  
-rw-r--r-- 1 seed seed 480 Feb 10 17:52 bfcbc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 17:54 bfcbf.bin  
-rw-r--r-- 1 seed seed 480 Feb 10 17:55 bfccb.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 17:53 bfafb.bin  
-rw-r--r-- 1 seed seed 1843226 Feb 10 20:23 body  
-rw-r--r-- 1 seed seed 1129 Feb 9 18:13 cipher.txt  
-rw-r--r-- 1 seed seed 480 Feb 10 18:25 descbc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 18:26 descfb.bin  
-rw-r--r-- 1 seed seed 480 Feb 10 17:58 desebc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 18:27 desofb.bin  
-rw-r--r-- 1 seed seed 184992 Feb 10 19:40 encrypted.bmp  
-rw-r--r-- 1 seed seed 184992 Feb 10 19:46 encrypteddbc.bmp  
-rw-r--r-- 1 seed seed 16 Feb 10 20:45 filelenc.txt  
-rw-r--r-- 1 seed seed 5 Feb 10 20:40 file1.txt  
-rw-r--r-- 1 seed seed 16 Feb 10 20:45 file2enc.txt  
-rw-r--r-- 1 seed seed 10 Feb 10 20:40 file2.txt  
-rw-r--r-- 1 seed seed 32 Feb 10 20:46 file3enc.txt  
-rw-r--r-- 1 seed seed 16 Feb 10 20:40 file3.txt  
-rw-r--r-- 1 seed seed 478 Feb 10 17:47 file.txt  
-rw-r--r-- 1 seed seed 54 Feb 10 20:23 header  
-rw-r--r-- 1 seed seed 1843280 Feb 10 20:18 mountainenccbc.bmp  
-rw-r--r-- 1 seed seed 1843280 Feb 10 20:23 mountainencecb.bmp  
-rw-r--r-- 1 seed seed 1843256 Feb 10 20:03 mountains.bmp  
-rw-r--r-- 1 seed seed 1843280 Feb 10 20:14 mountainscbc.bmp  
-rw-r--r-- 1 seed seed 1843280 Feb 10 20:21 mountainsecb.bmp  
-rw-r--r-- 1 seed seed 1129 Feb 10 16:27 plain.txt  
-rw-r--r-- 1 seed seed 184974 Feb 9 18:14 sample.bmp  
-rw-r--r-- 1 seed seed 184992 Feb 10 19:43 samplecbc.bmp  
-rw-r--r-- 1 seed seed 184992 Feb 10 19:33 sampleccb.bmp  
-rw-r--r-- 1 seed seed 206662 Feb 9 18:13 words.txt  
[02/10/24]seed@VM:~/cs458a205519085
```

File size after encryption file1 after encryption is 16 bytes, file2 after encryption is 16 bytes, file3 after encryption is 32 bytes. Therefore,

5 bytes -> 16 bytes

10 bytes -> 16 bytes

16 bytes -> 32 bytes

DECRYPTION

```
[02/10/24]seed@VM:~/cs458a205519085 openssl enc -aes-128-cbc -d -nopad -in fileldec.txt -out file1dec.txt -K 00010203040506070809aabcccddeeff -iv 0a0b0c0d0e0f0102030405  
06070809  
[02/10/24]seed@VM:~/cs458a205519085 openssl enc -aes-128-cbc -d -nopad -in file2dec.txt -out file2dec.txt -K 00010203040506070809aabcccddeeff -iv 0a0b0c0d0e0f0102030405  
06070809  
[02/10/24]seed@VM:~/cs458a205519085 openssl enc -aes-128-cbc -d -nopad -in file3dec.txt -out file3dec.txt -K 00010203040506070809aabcccddeeff -iv 0a0b0c0d0e0f0102030405  
06070809  
[02/10/24]seed@VM:~/cs458a205519085 ls -l  
total 12048  
-rw-r--r-- 1 seed seed 480 Feb 10 18:31 aescbc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 18:32 aescfb.bin  
-rw-r--r-- 1 seed seed 480 Feb 10 18:35 aesebc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 18:34 aesofb.bin  
-rw-r--r-- 1 seed seed 480 Feb 10 17:52 bfcbc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 17:54 bfcbf.bin  
-rw-r--r-- 1 seed seed 480 Feb 10 17:55 bfccb.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 17:53 bfafb.bin  
-rw-r--r-- 1 seed seed 1843226 Feb 10 20:23 body  
-rw-r--r-- 1 seed seed 1129 Feb 9 18:13 cipher.txt  
-rw-r--r-- 1 seed seed 480 Feb 10 18:25 descbc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 18:26 descfb.bin  
-rw-r--r-- 1 seed seed 480 Feb 10 17:58 desebc.bin  
-rw-r--r-- 1 seed seed 478 Feb 10 18:27 desofb.bin  
-rw-r--r-- 1 seed seed 184992 Feb 10 19:40 encrypted.bmp  
-rw-r--r-- 1 seed seed 184992 Feb 10 19:46 encrypteddbc.bmp  
-rw-r--r-- 1 seed seed 16 Feb 10 20:49 fileldec.txt  
-rw-r--r-- 1 seed seed 16 Feb 10 20:48 filelenc.txt  
-rw-r--r-- 1 seed seed 5 Feb 10 20:40 file1.txt  
-rw-r--r-- 1 seed seed 16 Feb 10 20:49 file2dec.txt  
-rw-r--r-- 1 seed seed 16 Feb 10 20:45 file2enc.txt  
-rw-r--r-- 1 seed seed 10 Feb 10 20:40 file2.txt  
-rw-r--r-- 1 seed seed 32 Feb 10 20:49 file3dec.txt  
-rw-r--r-- 1 seed seed 32 Feb 10 20:46 file3enc.txt  
-rw-r--r-- 1 seed seed 16 Feb 10 20:40 file3.txt  
-rw-r--r-- 1 seed seed 478 Feb 10 17:47 file.txt  
-rw-r--r-- 1 seed seed 54 Feb 10 20:23 header  
-rw-r--r-- 1 seed seed 1843280 Feb 10 20:18 mountainenccbc.bmp  
-rw-r--r-- 1 seed seed 1843280 Feb 10 20:23 mountainencecb.bmp  
-rw-r--r-- 1 seed seed 1843256 Feb 10 20:03 mountains.bmp  
-rw-r--r-- 1 seed seed 1843280 Feb 10 20:14 mountainscbc.bmp  
-rw-r--r-- 1 seed seed 1843280 Feb 10 20:21 mountainsecb.bmp  
-rw-r--r-- 1 seed seed 1129 Feb 10 16:27 plain.txt
```

```
[02/10/24]seed@VM:~/cs458a205519085 xxd file1dec.txt  
00000000: 3132 3334 350b 0b0b 0b0b 0b0b 0b0b 12345.....  
[02/10/24]seed@VM:~/cs458a205519085 xxd file2dec.txt  
00000000: 3631 3233 3435 3637 3839 0606 0606 0606 0123456789.....  
[02/10/24]seed@VM:~/cs458a205519085 xxd file3dec.txt  
00000000: 3631 3233 3435 3637 3839 3132 3334 3536 0123456789123456  
00000010: 1010 1010 1010 1010 1010 1010 1010 1010 .....  
[02/10/24]seed@VM:~/cs458a205519085
```

```
[02/13/24]seed@VM:~$ cd cs458a20551908
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C file1.txt
00000000 31 32 33 34 35 |12345|
00000005
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C file2.txt
00000000 30 31 32 33 34 35 36 37 38 39 |0123456789|
0000000a
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C file3.txt
00000000 30 31 32 33 34 35 36 37 38 39 31 32 33 34 35 36 |0123456789123456|
00000010
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C filelenc.txt
00000000 af 8d 57 e0 df 5e e2 03 3e 77 d4 18 2d 81 dd 24 |..W..^..>w....$|
00000010
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C file2enc.txt
00000000 65 f7 14 6b 3f 1c 15 9d 58 60 2d 3b f6 a7 5c ee |e..k?...X`-;..\.|00000010
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C file3enc.txt
00000000 e1 d2 bb bb 28 2b 87 d2 77 7e 8d ba de 12 28 32 |....(+..w~....(2|
00000010 06 ca 3d 3f 33 2e 4d 1c 12 0a d8 0e b8 0e 53 99 |..=?3.M.....S.|00000020
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C file1dec.txt
00000000 31 32 33 34 35 0b |12345.....|00000010
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C file2dec.txt
00000000 30 31 32 33 34 35 36 37 38 39 06 06 06 06 06 |0123456789.....|00000010
[02/13/24]seed@VM:~/cs458a20551908$ hexdump -C file3dec.txt
00000000 30 31 32 33 34 35 36 37 38 39 31 32 33 34 35 36 |0123456789123456|
00000010 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 |.....|00000020
[02/13/24]seed@VM:~/cs458a20551908$ █
```

TASK-5 Error Propagation – Corrupted Cipher Text

```
[02/10/24]seed@VM:~/cs458a20551908$ ls -l
total 12052
-rw-rw-r-- 1 seed seed      480 Feb 10 18:31 aescbc.bin
-rw-rw-r-- 1 seed seed      478 Feb 10 18:32 aescfb.bin
-rw-rw-r-- 1 seed seed      480 Feb 10 18:35 aesecb.bin
-rw-rw-r-- 1 seed seed      478 Feb 10 18:34 aesofb.bin
-rw-rw-r-- 1 seed seed      480 Feb 10 17:52 bfcbc.bin
-rw-rw-r-- 1 seed seed      478 Feb 10 17:54 bfcfb.bin
-rw-rw-r-- 1 seed seed      480 Feb 10 17:55 bfecb.bin
-rw-rw-r-- 1 seed seed      478 Feb 10 17:53 bfafb.bin
-rw-rw-r-- 1 seed seed 1843226 Feb 10 20:23 body
-rw-rw-r-- 1 seed seed      1129 Feb 9 18:13 cipher.txt
-rw-rw-r-- 1 seed seed      480 Feb 10 18:25 descbc.bin
-rw-rw-r-- 1 seed seed      478 Feb 10 18:26 descfb.bin
-rw-rw-r-- 1 seed seed      480 Feb 10 17:58 desecb.bin
-rw-rw-r-- 1 seed seed      478 Feb 10 18:27 desofb.bin
-rw-rw-r-- 1 seed seed 184992 Feb 10 19:40 encrypted.bmp
-rw-rw-r-- 1 seed seed 184992 Feb 10 19:46 encryptedcbc.bmp
-rw-rw-r-- 1 seed seed      16 Feb 10 20:49 file1dec.txt
-rw-rw-r-- 1 seed seed      16 Feb 10 20:48 filelenc.txt
-rw-rw-r-- 1 seed seed      5 Feb 10 20:40 file1.txt
-rw-rw-r-- 1 seed seed      16 Feb 10 20:49 file2dec.txt
-rw-rw-r-- 1 seed seed      16 Feb 10 20:45 file2enc.txt
-rw-rw-r-- 1 seed seed      10 Feb 10 20:40 file2.txt
-rw-rw-r-- 1 seed seed      32 Feb 10 20:49 file3dec.txt
-rw-rw-r-- 1 seed seed      32 Feb 10 20:46 file3enc.txt
-rw-rw-r-- 1 seed seed      16 Feb 10 20:40 file3.txt
-rw-rw-r-- 1 seed seed      478 Feb 10 17:47 file.txt
-rw-rw-r-- 1 seed seed      54 Feb 10 20:23 header
-rw-rw-r-- 1 seed seed 1843280 Feb 10 20:18 mountainenccbc.bmp
-rw-rw-r-- 1 seed seed 1843280 Feb 10 20:23 mountainencecb.bmp
-rw-rw-r-- 1 seed seed 1843256 Feb 10 20:03 mountains.bmp
-rw-rw-r-- 1 seed seed 1843280 Feb 10 20:14 mountainscbc.bmp
-rw-rw-r-- 1 seed seed 1843280 Feb 10 20:21 mountainsecb.bmp
-rw-rw-r-- 1 seed seed      1129 Feb 10 16:27 plain.txt
-rw-rw-r-- 1 seed seed 184974 Feb 9 18:14 sample.bmp
-rw-rw-r-- 1 seed seed 184992 Feb 10 19:43 samplecbc.bmp
-rw-rw-r-- 1 seed seed 184992 Feb 10 19:33 sampleecb.bmp
-rw-rw-r-- 1 seed seed      1000 Feb 10 21:03 thousand.txt
-rw-rw-r-- 1 seed seed 206662 Feb 9 18:13 words.txt
[02/10/24]seed@VM:~/cs458a20551908$
```

```
[02/10/24]seed@VM:~/cs458a20551908$ cat thousand.txt
```

The internet has changed the way we live, work and communicate in ways that were once unimaginable. With just a click of a button, we can access an endless amount of information, connect with people from all over the world, and conduct business from the comfort of our own homes. However, as with any technological advancement, the internet also has its downsides. In this essay, I will argue that the internet is a blessing, but it is also a curse.

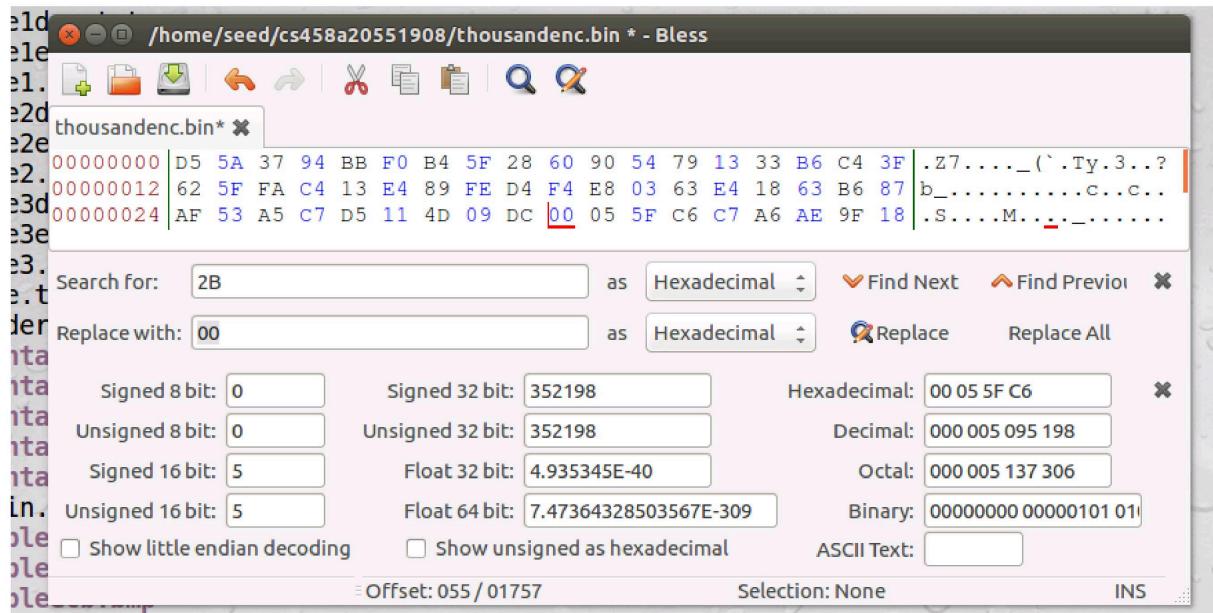
The internet has brought about many benefits to our daily lives. One of the most significant is the way it has changed the way we communicate. Social media platforms like Facebook, Twitter and Instagram have made it easy for people to stay connected with their friends and family, regardless of where they are located.

The internet has changed the way we live, work and communicate in ways that were once unimaginable. With just a click of a button, we can access an endless amount of information, connect with people from all over the world, an[02/10/24]seed@VM:~/cs458a20551908\$

CBC

Assumption: A single corrupted bit in a block of ciphertext will result in an inaccurate decryption of that block and the block after it, but not of the remaining blocks.

```
-rw-rw-r-- 1 seed seed 184992 Feb 18 19:46 encryptedcbc.bmp
-rw-rw-r-- 1 seed seed 16 Feb 18 20:49 file0
-rw-rw-r-- 1 seed seed 16 Feb 18 20:48 file1
-rw-rw-r-- 1 seed seed 5 Feb 18 20:49 file1
-rw-rw-r-- 1 seed seed 16 Feb 18 20:49 file2
-rw-rw-r-- 1 seed seed 16 Feb 18 20:45 file2d
-rw-rw-r-- 1 seed seed 16 Feb 18 20:40 file2e
-rw-rw-r-- 1 seed seed 32 Feb 18 20:49 file3d
-rw-rw-r-- 1 seed seed 32 Feb 18 20:46 file3e
-rw-rw-r-- 1 seed seed 16 Feb 18 20:40 file3
-rw-rw-r-- 1 seed seed 478 Feb 18 17:47 file.t
-rw-rw-r-- 1 seed seed 54 Feb 18 20:23 header
-rw-rw-r-- 1 seed seed 1843280 Feb 18 20:18 mounta
-rw-rw-r-- 1 seed seed 1843280 Feb 18 20:23 mounta
-rw-rw-r-- 1 seed seed 1843256 Feb 18 20:03 mounta
-rw-rw-r-- 1 seed seed 1843280 Feb 18 20:14 mounta
-rw-rw-r-- 1 seed seed 1843280 Feb 18 20:21 mounta
-rw-rw-r-- 1 seed seed 1129 Feb 18 16:27 plain
-rw-rw-r-- 1 seed seed 184974 Feb 9 18:14 sample
-rw-rw-r-- 1 seed seed 184992 Feb 18 19:43 sample
-rw-rw-r-- 1 seed seed 184992 Feb 18 19:33 sample
-rw-rw-r-- 1 seed seed 1000 Feb 18 21:03 thousand.txt
-rw-rw-r-- 1 seed seed 206662 Feb 9 18:13 words.txt
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cbc -e -in thousand.txt -out thousandenc.bin -K 00010203040506070809aabccddeeff -iv 0a0b0c0d0e0f010203040506070809
[02/10/24]seed@VM:~/cs458a20551908$ bless thousandenc.bin
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/export_patterns".
Could not find file "/home/seed/.config/bless/history.xml".
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
```

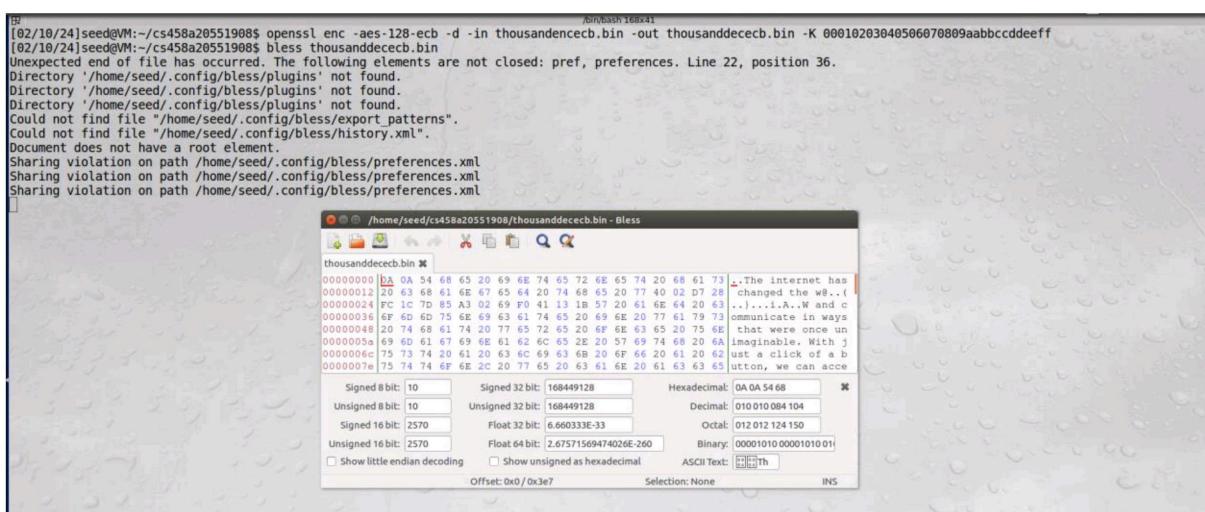
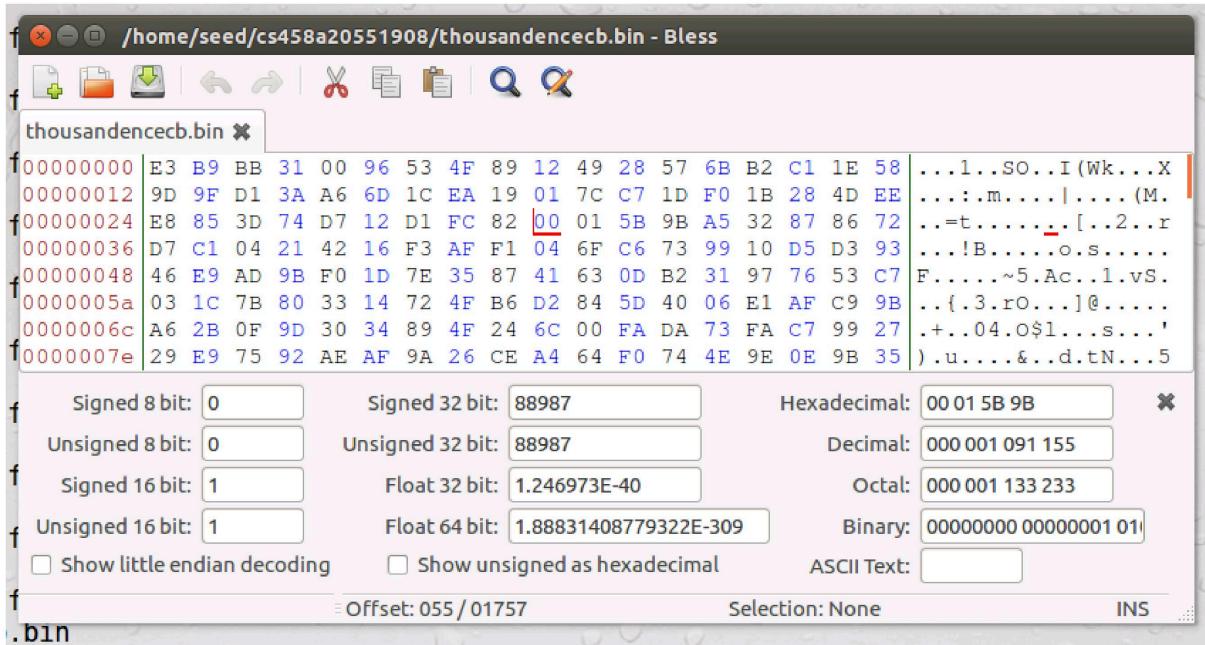


Observation: we can notice that the bits around the bit are corrupted and then after few bits are correct and another bit got corrupted.
Error propagation in this mode not just affects the decryption of the block but also affects the XOR operation with the previous ciphertext block and subsequent blocks.

ECB

Assumption: single corrupted block in the cipher text will affect only that block's decryption and will have no effect on subsequent blocks.

```
[02/10/24]seed@M-:~/cs458a20551908$ openssl enc -aes-128-cbc -e -in thousand.txt -out thousandeccb.bin -K 00010203040506070809aabccddeff
[02/10/24]seed@M-:~/cs458a20551908$ bless thousandeccb.bin
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/export_patterns".
Could not find file "/home/seed/.config/bless/history.xml".
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
```



```
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-ecb -d -in thousanddcecb.bin -out thousanddececb.bin -K 00010203040506070809aabccdddeff
[02/10/24]seed@VM:~/cs458a20551908$ bless thousanddececb.bin
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/export_patterns".
Could not find file "/home/seed/.config/bless/history.xml".
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
```

Observation: the corruption impacted on the specific block containing the modified byte and caused no effect to the subsequent blocks. This becomes evident in the decrypted result where we observe a change, in the text for a period before returning to normal.

Error propagation is not provided meaning only the corrupted byte's block is affected and has no effect on the subsequent blocks.

OFB

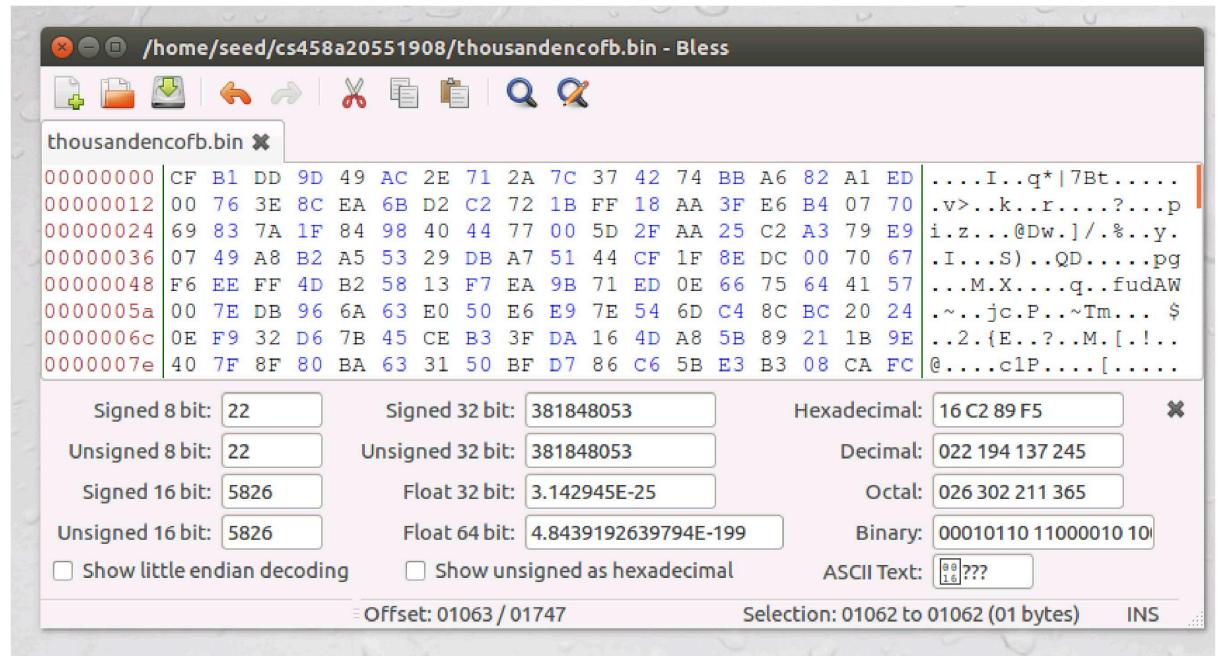
Assumption: Only that bit in the decrypted plaintext will be incorrect if one bit in a single block in the ciphertext is corrupted. There won't be any impact on the blocks and bits that follow.

```
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-ofb -e -in thousand.txt -out thousandencfb.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809aabccddeff
6070809
[02/10/24]seed@VM:~/cs458a20551908$ bless thousandencfb.bin
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/export_patterns".
Could not find file "/home/seed/.config/bless/history.xml".
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
```

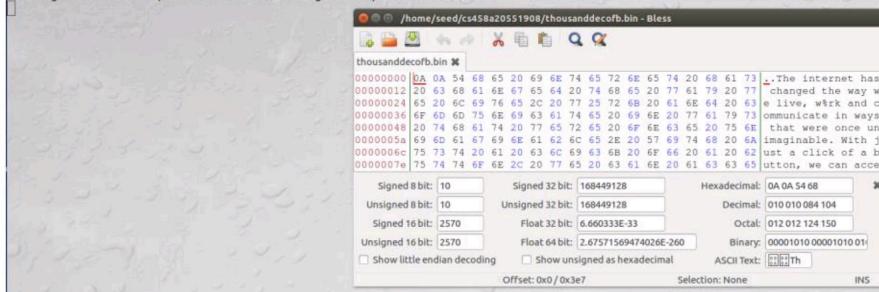
The screenshot shows the Bless hex editor interface. The file 'thousandencfb.bin' is open. The hex dump shows the first few bytes of the file, followed by a large amount of binary data. A tooltip is displayed above the hex dump, containing the following text:

```
CF B1 DD 9D 49 AC 2E 71 2A 7C 37 42 74 BB A6 82 A1 ED ...I..q*|7Bt.....
00 76 3E 8C EA 6B D2 C2 72 1B FF 18 AA 3F E6 B4 07 70 .v>..k..r....?....p
69 83 7A 1F 84 98 40 44 77 00 5D 2F AA 25 C2 A3 79 E9 i.z...@Dw.]/.%..y.
07 49 A8 B2 A5 53 29 DB A7 51 44 CF 1F 8E DC 00 70 67 .I...S)...QD.....pg
F6 EE FF 4D B2 58 13 F7 EA 9B 71 ED 0E 66 75 64 41 57 ...M.X....q..fudAW
00 7E DB 96 6A 63 E0 50 E6 E9 7E 54 6D C4 8C BC 20 24 ~..jc.P..~Tm... $ 
0E F9 32 D6 7B 45 CE B3 3F DA 16 4D A8 5B 89 21 1B 9E ..2.{E..?.M.[!...
40 7F 8F 80 BA 63 31 50 BF D7 86 C6 5B E3 B3 08 CA FC @....clP....[....]
```

Below the hex dump, there are several conversion boxes for different data types (Signed 8-bit, Unsigned 8-bit, Signed 16-bit, Unsigned 16-bit, Signed 32-bit, Unsigned 32-bit, Float 32-bit, Float 64-bit) and a Decimal/Octal/Binary/ASCII Text field. The selection range is set to 0x01747.



```
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-ofb -d -in thousanddecofb.bin -out thousanddecofb.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/10/24]seed@VM:~/cs458a20551908$ bless thousanddecofb.bin
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/export_patterns".
Could not find file "/home/seed/.config/bless/history.xml".
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
```



```
[02/10/24]seed@VM:~/cs458a20551908$ cat thousanddecofb.bin
```

The internet has changed the way we live, work and communicate in ways that were once unimaginable. With just a click of a button, we can access an endless amount of information, connect with people from all over the world, and conduct business from the comfort of our own homes. However, as with any technological advancement, the internet also has its downsides. In this essay, I will argue that the internet is a blessing, but it is also a curse.

The internet has brought about many benefits to our daily lives. One of the most significant is the way it has changed the way we communicate. Social media platforms like Facebook, Twitter and Instagram have made it easy for people to stay connected with their friends and family, regardless of where they are located.

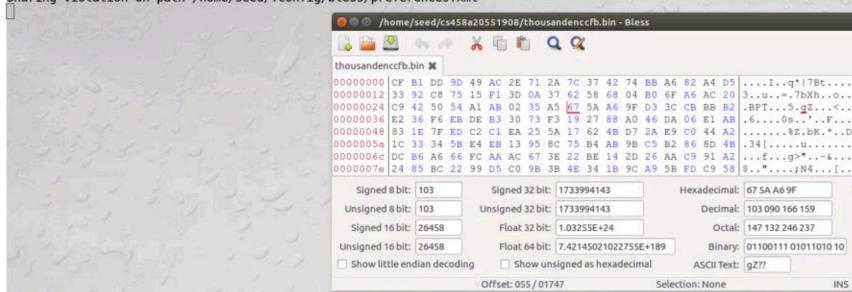
The internet has changed the way we live, work and communicate in ways that were once unimaginable. With just a click of a button, we can access an endless amount of information, connect with people from all over the world, an[02/10/24]seed@VM:~/cs458a20551908\$

Observation: the encryption feedback loop in OFB mode operates independently of the ciphertext and plaintext. Consequently, a bit error in a block of ciphertext will only affect the bit in the block that has been decrypted and will not impact blocks that come after it.

CFB

Assumption: One block in the ciphertext and many bits after it (or even the next block entirely) will be improperly decrypted if one bit of that block is corrupted.

```
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cfb -e -in thousand.txt -out thousandencfb.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/10/24]seed@VM:~/cs458a20551908$ bless thousandencfb.bin
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/export_patterns".
Could not find file "/home/seed/.config/bless/history.xml".
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
```



```
[02/10/24]seed@VM:~/cs458a20551908$ openssl enc -aes-128-cfb -e -in thousand.txt -out thousandccfb.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809aabccddeff
[02/10/24]seed@VM:~/cs458a20551908$ bless thousandccfb.bin
Unexpected end of file has occurred. The following elements are not closed: pref preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/preferences' not found.
Directory '/home/seed/.config/bless/preferences.xml' not found.
Could not find file "/home/seed/.thousandccfb.bin"
Could not find file "/home/seed/.thousandccfb.bin"
Document does not have a root element.
Sharing violation on path /home/seed/.thousandccfb.bin
Document does not have a root element.
[02/10/24]seed@VM:~/cs458a20551908$
```

Signed 32 bit: 0 Unsigned 32 bit: 5940895 Hexadecimal: 00 0A A6 9F Position 36.

Signed 8 bit: 0 Unsigned 8 bit: 0 Decimal: 000 090 166 159

Signed 16 bit: 90 Float 32 bit: 8.324967E-39 Octal: 000 132 246 237

Unsigned 16 bit: 90 Float 64 bit: 5.93001680239209E-307 Binary: 00000000 01011010 10

Show little endian decoding Show unsigned as hexadecimal ASCII Text:

Offset: 055 / 01747 Selection: None INS

Sharing violation on path /home/seed/.config/bless/preferences.XML
Sharing violation on path /home/seed/.config/bless/preferences.XML
Sharing violation on path /home/seed/.config/bless/preferences.XML

```
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.thousandccfb.bin" - Bless
Could not find file "/home/seed/.thousandccfb.bin" - Bless
Document does not have a root element.
Sharing violation on path /home/seed/.thousandccfb.bin
Document does not have a root element.
[02/10/24]seed@VM:~/cs458a20551908$
```

The internet has changed the way we live, work, and communicate. Social media platforms like Facebook, Twitter, and Instagram have made it easy for people to stay connected with their friends and family, regardless of where they are located.

Sharing violation on path /home/seed/.config/bless/preferences.XML
Sharing violation on path /home/seed/.config/bless/preferences.XML
Sharing violation on path /home/seed/.config/bless/preferences.XML

Signed 8 bit: 10 Signed 32 bit: 168449128 Hexadecimal: 0A 0A 54 68 Position 36.

Signed 8 bit: 10 Unsigned 32 bit: 168449128 Decimal: 010 010 084 104

Signed 16 bit: 2570 Float 32 bit: 0.600333E-33 Octal: 012 012 124 150

Unsigned 16 bit: 2570 Float 64 bit: 2.67571569474026E-260 Binary: 000001010 000001010 01

Show little endian decoding Show unsigned as hexadecimal ASCII Text:

Offset: 0x0 / 0x3e7 Selection: None INS

Sharing violation on path /home/seed/.config/bless/preferences.XML
Sharing violation on path /home/seed/.config/bless/preferences.XML
Sharing violation on path /home/seed/.config/bless/preferences.XML

[02/10/24]seed@VM:~/cs458a20551908\$ openssl enc -aes-128-cfb -d -in thousandccfb.bin -out thousanddeccfb.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809aabccddeff
[02/10/24]seed@VM:~/cs458a20551908\$ bless thousanddeccfb.bin
Unexpected end of file has occurred. The following elements are not closed: pref preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/preferences' not found.
Directory '/home/seed/.config/bless/preferences.xml' not found.
Could not find file "/home/seed/.thousanddeccfb.bin"
Could not find file "/home/seed/.thousanddeccfb.bin"
Document does not have a root element.
Sharing violation on path /home/seed/.thousanddeccfb.bin
Document does not have a root element.
[02/10/24]seed@VM:~/cs458a20551908\$

Sharing violation on path /home/seed/.config/bless/preferences.XML
Sharing violation on path /home/seed/.config/bless/preferences.XML
Sharing violation on path /home/seed/.config/bless/preferences.XML

7 in ways that were once unimaginable. With just a click of a button, we can access an endless amount of information, connect with people from all over the world, and conduct business from the comfort of our own homes. However, as with any technological advancement, the internet also has its downsides. In this essay, I will argue that the internet is a blessing, but it is also a curse.

The internet has brought about many benefits to our daily lives. One of the most significant is the way it has changed the way we communicate. Social media platforms like Facebook, Twitter and Instagram have made it easy for people to stay connected with their friends and family, regardless of where they are located.

The internet has changed the way we live, work and communicate in ways that were once unimaginable. With just a click of a button, we can access an endless amount of information, connect with people from all over the world, an[02/10/24]seed@VM:~/cs458a20551908\$

Observation: The plaintext is generated by first encrypting the previous ciphertext block and then combining it with the current block using an XOR operation. Therefore, a single bit error in a block of ciphertext will affect not only the block's decryption but also the encryption (including XOR) of many bytes in the block that follows.

TASK-6 Initial Vector (IV)

SAME

s like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media, etc.

```
[02/12/24]seed@M-:~/cs458a205519085 openssl enc -aes-128-cfb -d -in task6.txt -out task6enc.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809
[02/12/24]seed@M-:~/cs458a205519085 bless task6enc.bin
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/plugins/Bless"
Could not find file "/home/seed/.config/bles
Document does not have a root element.
Sharing violation on path /home/seed/.config
Sharing violation on path /home/seed/.config
Sharing violation on path /home/seed/.config
Document does not have a root element.
[02/12/24]seed@M-:~/cs458a205519085 openssl
[02/12/24]seed@M-:~/cs458a205519085 bless ta
Unexpected end of file has occurred. The fol
Directory '/home/seed/.config/bless/plugins'
Directory '/home/seed/.config/bless/plugins'
Directory '/home/seed/.config/bless/plugins'
Could not find file "/home/seed/.config/bles
Could not find file "/home/seed/.config/bles
Document does not have a root element.
Sharing violation on path /home/seed/.config
Sharing violation on path /home/seed/.config
Sharing violation on path /home/seed/.config
Document does not have a root element.
[02/12/24]seed@M-:~/cs458a205519085 openssl
[02/12/24]seed@M-:~/cs458a205519085 bless ta
Unexpected end of file has occurred. The fol
Directory '/home/seed/.config/bless/plugins'
Directory '/home/seed/.config/bless/plugins'
Directory '/home/seed/.config/bless/plugins'
Signed 8 bit: -116 Unsigned 16 bit: 14 Signed 32 bit: -1932136550 Unsigned 32 bit: 2362830746 Hexadecimal: BC D5 EF 9A Decimal: 140213239154
Signed 16 bit: -29483 Unsigned 32 bit: 3296205E-31 Float 32 bit: -3.296205E-31 Octal: 214325357232
Signed 16 bit: 36053 Unsigned 32 bit: 18432211579743E-247 Float 64 bit: -7.8432211579743E-247 Binary: 10001100 1101010111
Unsigned 16 bit: 0 Show little endian decoding Unsigned 32 bit: 0 Show unsigned as hexadeciml ASCII Text: ???? Selection: None INS
Offset: 0x0/0x24b
```

DIFFERENT

```
[19] Sharing violation on path /home/seed/.config/bless/preferences.xml  
Document does not have a root element.  
[02/12/24] seed@M:~/cs458a205519088 openssl enc -aes-128-cfb -e -in task6.txt -out task6e.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809  
[02/12/24] seed@M:~/cs458a205519088 bless task6e.bin  
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.  
Directory '/home/seed/.config/bless/plugins' not found.  
Directory '/home/seed/.config/bless/plugins' not found.  
Directory '/home/seed/.config/bless/nlmins' not found.  
Could not find file "/home/seed/.config/bless/nlmins".  
Could not find file "/home/seed/.config/bless/nlmins".  
Document does not have a root element.  
Sharing violation on path /home/seed/task6e.bin x  
Sharing violation on path /home/seed/task6e.bin  
Sharing violation on path /home/seed/task6e.bin  
Document does not have a root element.  
[02/12/24] seed@M:~/cs458a205519088 openssl enc -aes-128-cfb -e -in task6.txt -out task6e.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f010203040506070809  
[02/12/24] seed@M:~/cs458a205519088 bless task6e.bin  
Unexpected end of file has occurred.  
Directory '/home/seed/.config/bless/nlmins' not found.  
Directory '/home/seed/.config/bless/nlmins' not found.  
Directory '/home/seed/.config/bless/nlmins' not found.  
Signed 8 bit: 32  
Unsigned 8 bit: 32  
Signed 16 bit: 8415  
Unsigned 16 bit: 8415  
Offset: 0x0/0x24b  
Selection: None  
INISigned 32 bit: 551492251  
Unsigned 32 bit: 551492251  
Signed 32 bit: 20 DF 1A 9B  
Unsigned 32 bit: 032 223 026 155  
Decimal: 040 337 032 233  
Octal: 00100000 11011111 00  
Binary: 2.375514177727E-150  
Float 32 bit: 3.779528E-19  
Float 64 bit: 2.375514177727E-150  
Show little endian decoding  
Show unsigned as hexadecimal  
ASCII Text:  
6070809aabccddeff - iv 0a0b0c0d0e0f010203040506070809  
on 36.  
[02/12/24] seed@M:~/cs458a205519088 openssl enc -aes-128-cfb -e -in task6.txt -out task6e.bin -K 00010203040506070809aabccddeff -iv 0a0b0c0d0e0f09080706050403201  
[02/12/24] seed@M:~/cs458a205519088 bless task6e.bin  
Unexpected end of file has occurred. The following elements are not closed: pref, preferences. Line 22, position 36.  
Directory '/home/seed/.config/bless/plugins' not found.  
Directory '/home/seed/.config/bless/plugins' not found.  
Directory '/home/seed/.config/bless/plugins' not found.  
Could not find file "/home/seed/.config/bless/export_patterns".  
Could not find file "/home/seed/.config/bless/history.xml".  
Document does not have a root element.  
Sharing violation on path /home/seed/.config/bless/preferences.xml  
Sharing violation on path /home/seed/.config/bless/preferences.xml  
Sharing violation on path /home/seed/.config/bless/preferences.xml
```

Even if the plaintext stays the same, the ciphertext that is produced will vary if the IV is changed for every encryption. Reusing IVs with the same key reduces the security of the encryption process because attackers may be able to identify patterns in the ciphertexts and use that knowledge to deduce the plaintexts.

It has been noted that the encrypted value remained the same while the key was the same but the output file varied; nevertheless, the encrypted value also changed when the iv value was changed.

Task 6.2. Common Mistake: Use the Same IV

This is a known message!

Convert Text to Hex

546869732069732061206b6e6f776e206d65737361676521

Plain Text: 546869732069732061206b6e6f776e206d65737361676521
Cipher Text: a469b1c502c1cab966965e50425438e1bb1b5f9037a4c15913

padding plain text with '00' as it is short by 2 bits

After Padding

PT: 546869732069732061206b6e6f776e206d6573736167652100

K=PT (EX-OR) CT

The screenshot shows a hex calculator interface. At the top, there is a text input field containing the string "546869732069732061206b6e6f776e206d6573736167652100". Below it, another input field labeled "String 2" contains the string "a469b1c502c1cab966965e50425438e1bb1b5f9037a4c15913". Underneath these, a dropdown menu labeled "Output" is set to "Hexadecimal". At the bottom left is a blue "Calculate" button, and at the bottom right is a yellow "Steps" button. In the bottom right corner of the interface, there is a box labeled "Answer" containing the result: F001D8B622A8B99907B6353E2D2356C1D67E2CE356C3A47813.

K = F001D8B622A8B99907B6353E2D2356C1D67E2CE356C3A47813

PT2 = K (EX-OR) C2

The screenshot shows a web-based cipher tool interface. At the top, there is a header with the string value F001D8B622A8B99907B6353E2D2356C1D67E2CE356C3A47813. Below this, there are two input fields: 'String 1' with the value 00000000000000000000000000000000 and 'String 2' with the value bf73bcd3509299d566c35b5d450337e1bb175f903fafc15913. The 'Output' dropdown is set to 'Text'. There are two main buttons: a blue 'Calculate' button and an orange 'Steps' button. Below these buttons, there are two smaller buttons: 'Typeset' and 'Copy Answer'. The 'Copy Answer' button is highlighted with a blue border. At the bottom, there is a text area containing the result: Order: Launch a missile!.

PT2: Order: Launch a missile!

Task 6.3 Common Mistake: Use a Predictable IV

C1 = bef65565572ccee2a9f9553154ed9498 (known to both)
IV1 = 31323334353637383930313233343536 (known to both)
IV2 = 31323334353637383930313233343537 (known to both)
C1 = Encrypt key (IV1 XOR P1)

We have to generate plain text “P2” for Bob

P2 = IV1 XOR IV2 XOR “YES”

We do this because the IV2 operation gets cancelled out when the plain text is sent to bob for encryption.

This can be demonstrated as follows:

C2 = Encrypt key (IV2 XOR P2)

Now replacing P2 by our equation

C2 = Encrypt key (IV2 XOR IV1 XOR IV2 XOR “YES”)

a = Encrypt key (IV1 XOR “YES”)

Now this should create the same output as C1 if the original message was “YES”

If not, the original message is “NO”

Task 7: Programming using the Crypto Library - Extra Credit 5%

Python code:

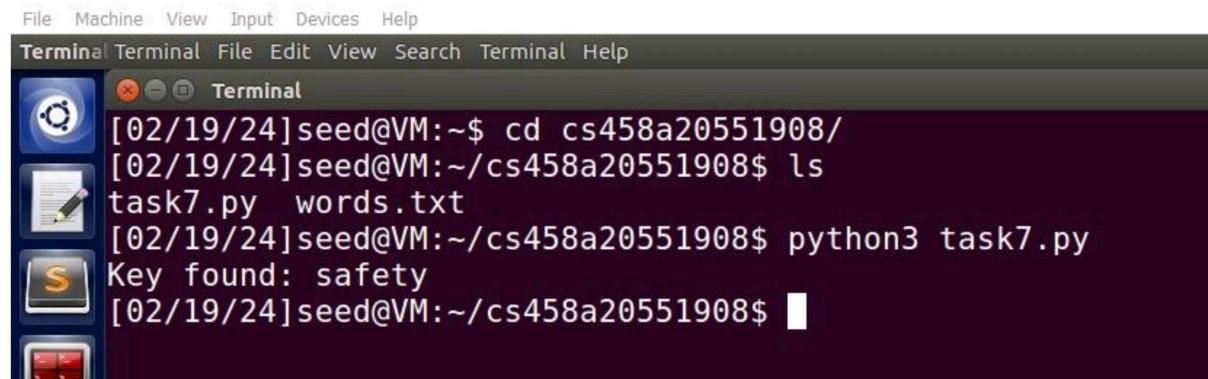
```
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad

iv = bytes.fromhex("010203040506070809000a0b0c0d0e0f")
cipher = bytes.fromhex("ece6753e938f8f903cabbbe12d395bf5f7eae38ad918a2d3e1c3a832476d5c7a")
message = b"This is a secret tool"

# Open the wordlist
with open("words.txt", "r") as file:
    words = file.readlines()
    # Iterate through wordlist to find the key
    for key in words:
        key = key.rstrip()
        key = key.lstrip()
        if len(key) < 16:
            key = key.ljust(16, '#')
        elif len(key) > 16 and len(key) < 24:
            key = key.ljust(24, '#')
        elif len(key) > 24 and len(key) < 32:
            key = key.ljust(32, '#')

        # Create AES cipher CBC mode obj
        obj = AES.new(key.encode(), AES.MODE_CBC, iv)
        # Decrypt the ciphertext
        decrypted_text = obj.decrypt(cipher)
        # Unpad the decrypted text
        try:
            decrypted_text = unpad(decrypted_text, AES.block_size)
        except ValueError:
            continue # If padding is invalid, try next key

        # Compare decrypted plaintext with original plaintext, if they match, print the key
        if decrypted_text == message:
            print("Key found:", key.replace('#', ''))
            break
```



As my system did not support installing pycrypto, I used another laptop for task 7 due to which the background colour is black and difference is seen for previous and this screen shot.