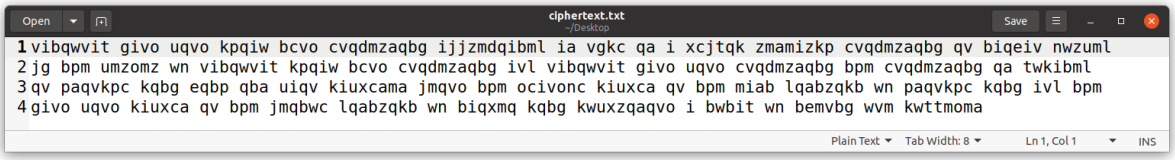
姓名：蔡佩蓉　　學號：109511286

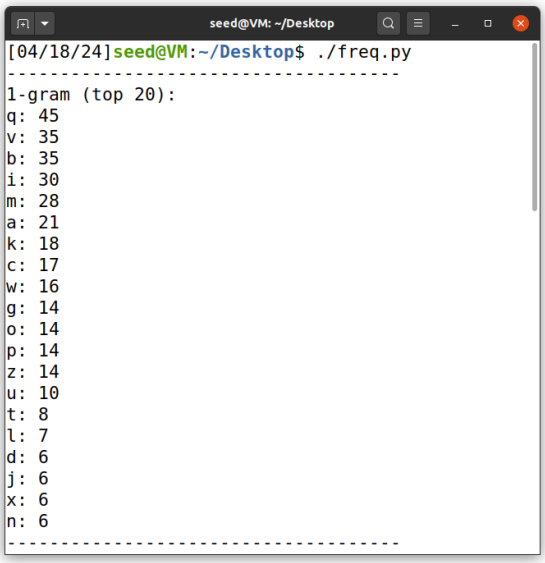
Secret-Key Encryption Lab (Lab2)

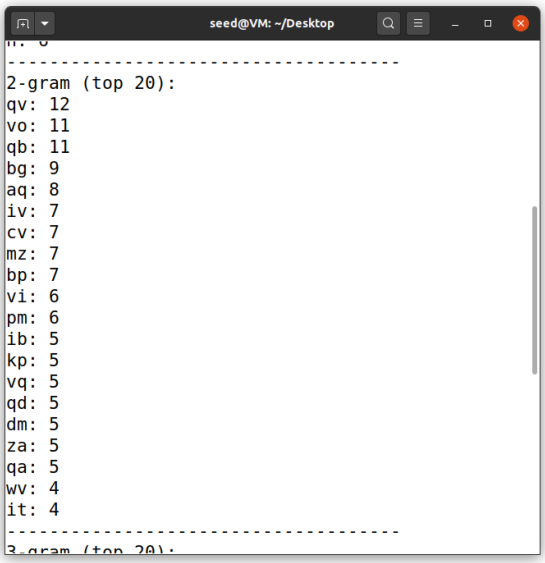
Task 1: Frequency Analysis

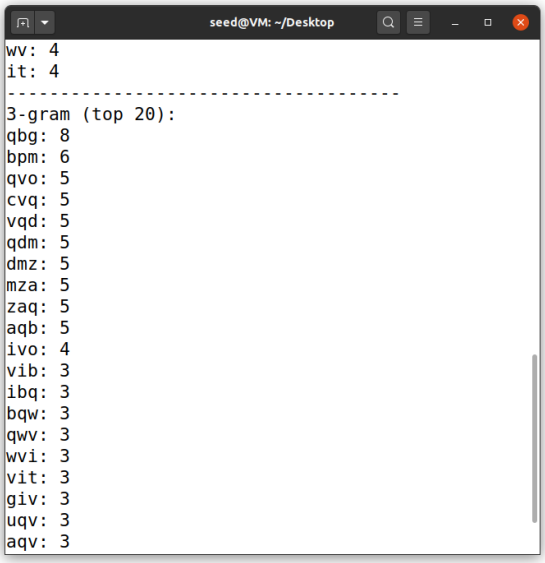
Content of ciphertext used is from file1.txt given.

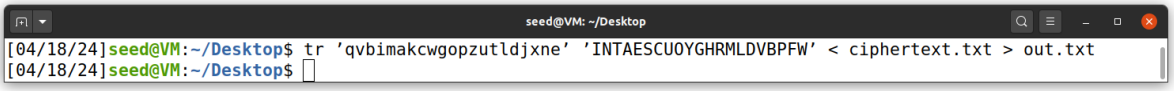


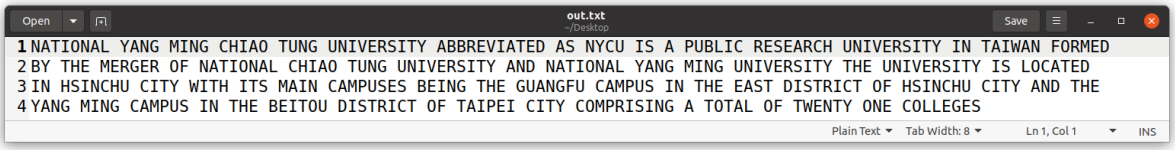
Analyze the frequency of ciphertext.txt









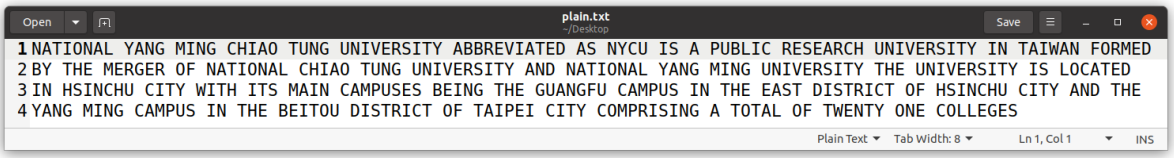


References:

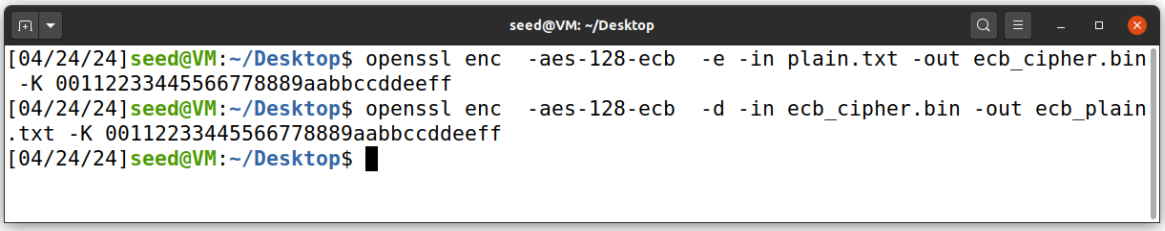
[1] https://en.wikipedia.org/wiki/Frequency_analysis
[2] https://en.wikipedia.org/wiki/Letter_frequency
[3] https://en.wikipedia.org/wiki/Bigram
[4] https://en.wikipedia.org/wiki/Trigram

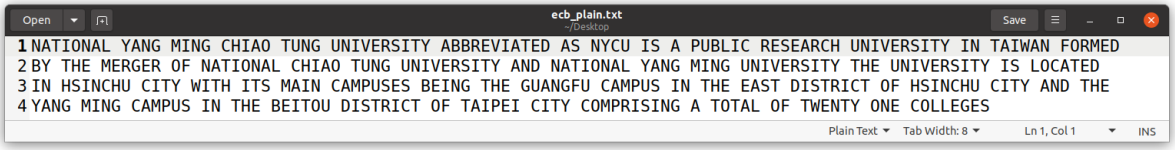
Task 2: Encryption using Different Ciphers and Modes

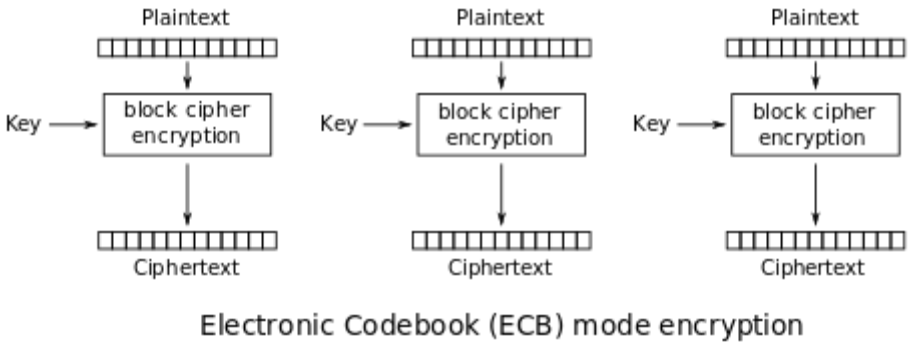
Plaintext:



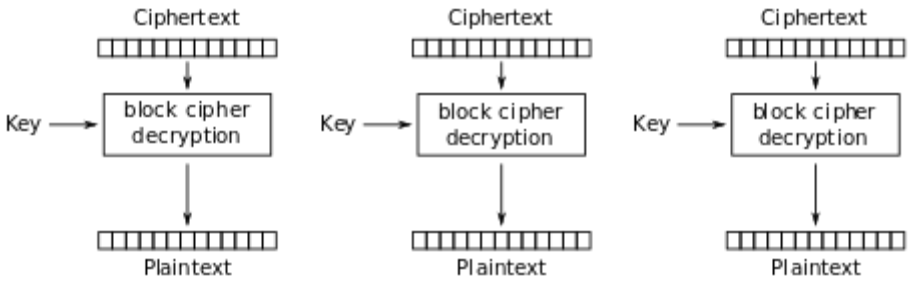
AES-128-ECB:







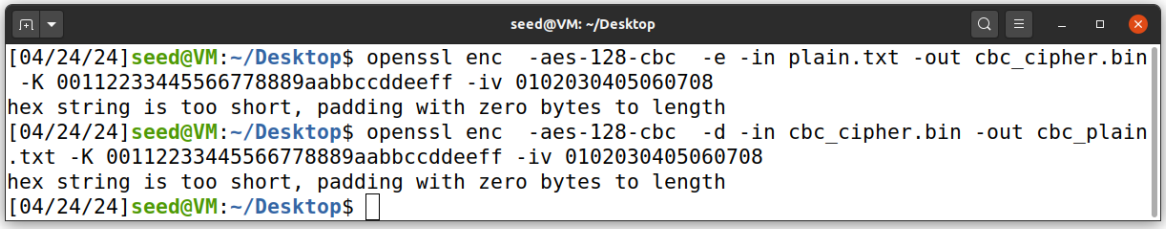
Electronic Codebook (ECB) mode encryption

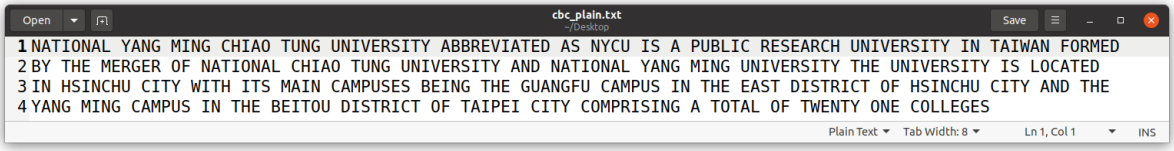


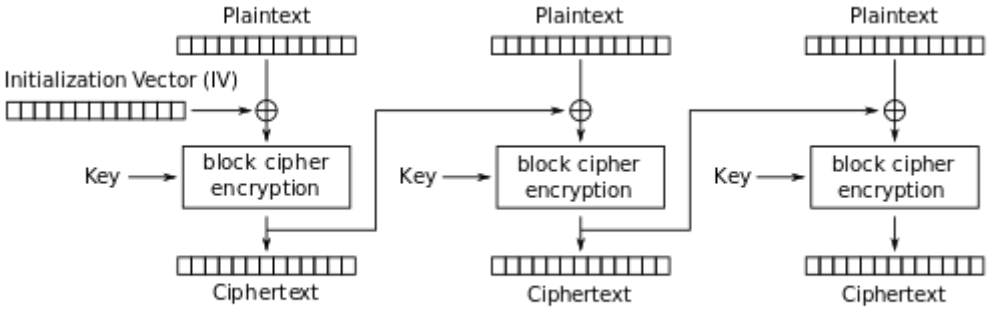
Electronic Codebook (ECB) mode decryption

Each block of plaintext is encrypted independently with the same key, leading to identical plaintext blocks being encrypted into identical ciphertext blocks, which can leak information and lacks diffusion.

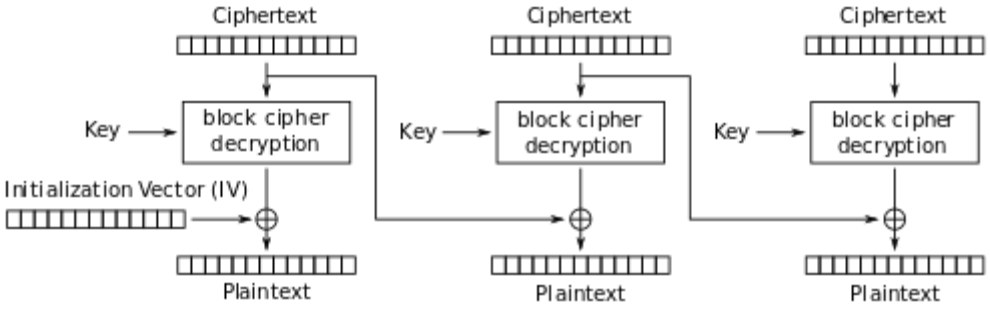
AES-128-CBC:







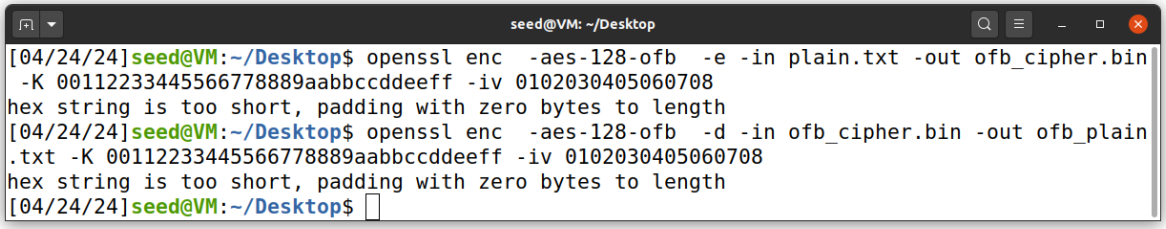
Cipher Block Chaining (CBC) mode encryption

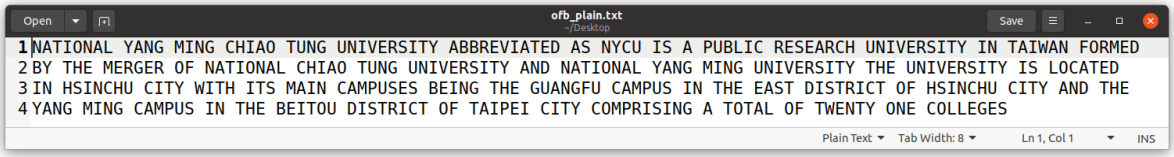


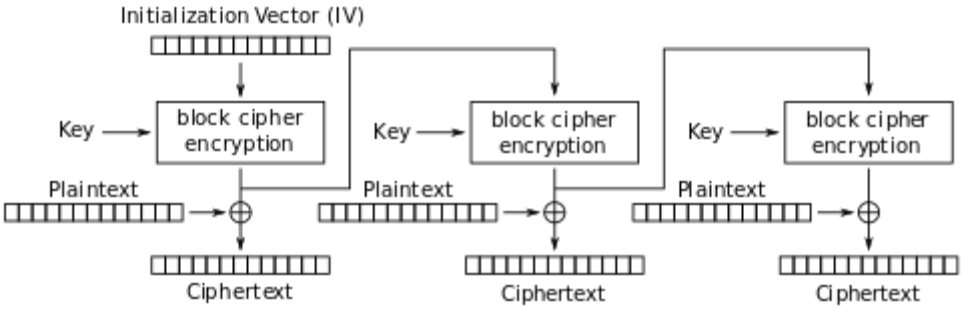
Cipher Block Chaining (CBC) mode decryption

Each plaintext block is XORed with the previous ciphertext block before encryption, enhancing security by introducing diffusion and preventing identical plaintext blocks from encrypting to the same ciphertext blocks.

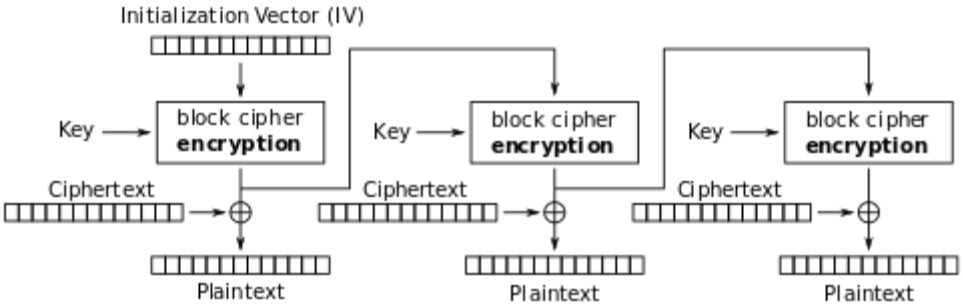
AES-128-OFB:







Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

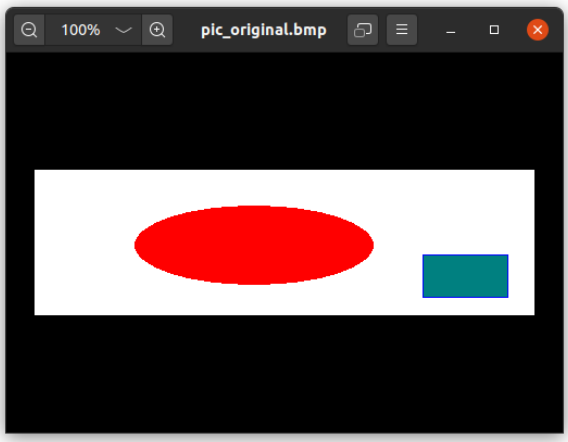
The encryption of the previous ciphertext block is used to generate a keystream, which is then XORed with the plaintext to produce the ciphertext, providing a stream cipher-like operation that does not depend on the plaintext and offers parallelization.

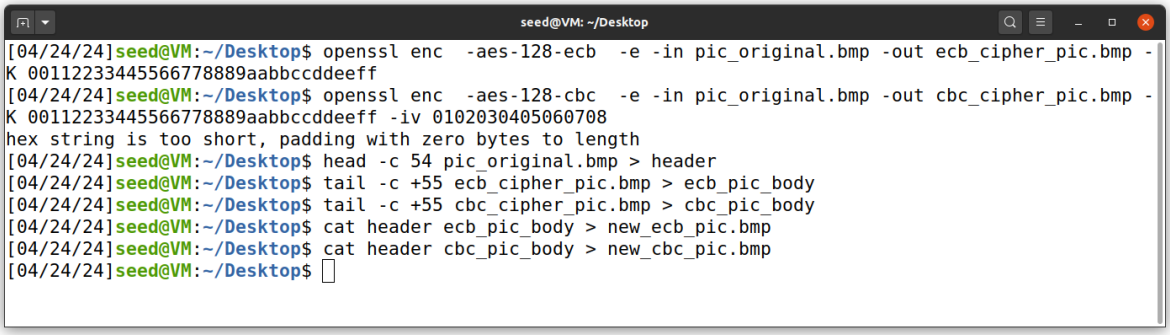
Reference (Manuals):

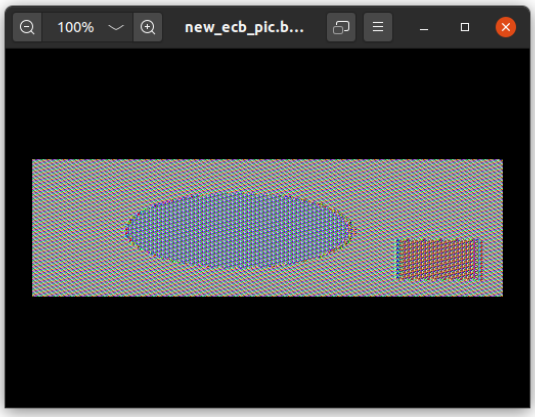
[1] https://www.openssl.org/docs/manmaster/man1/openssl.html
[2] https://www.openssl.org/docs/man1.0.2/man1/openssl-enc.html
[3] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

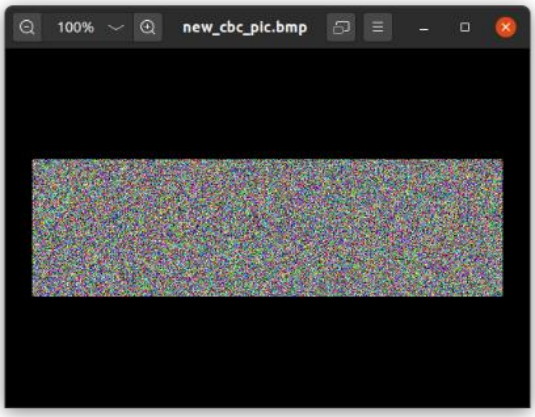
Task 3: Encryption Mode – ECB vs. CBC

Part I:



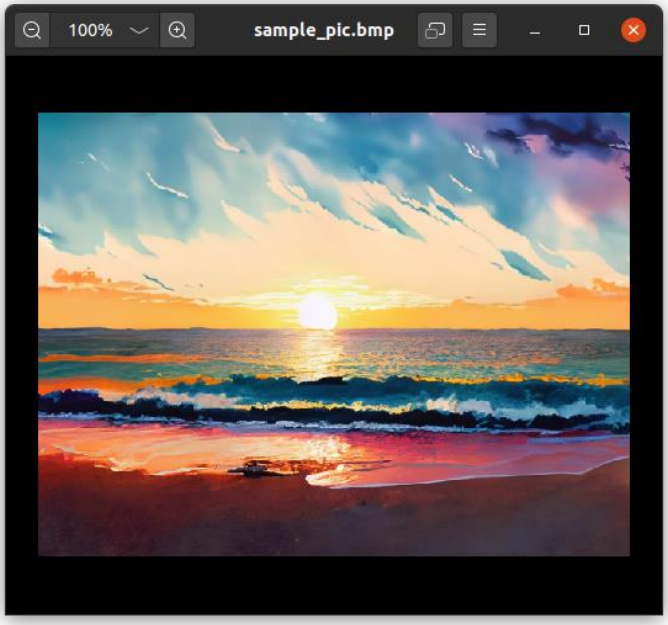




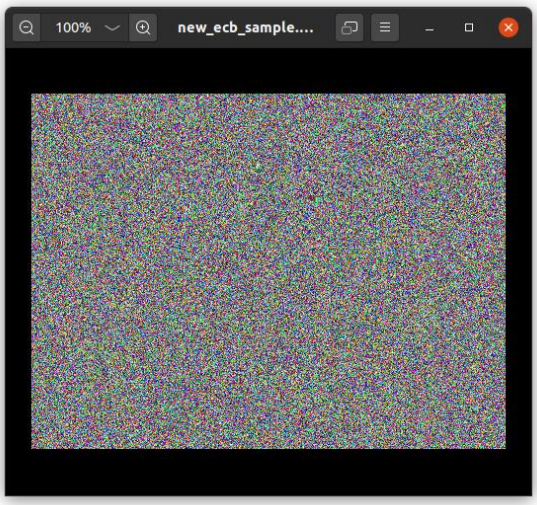


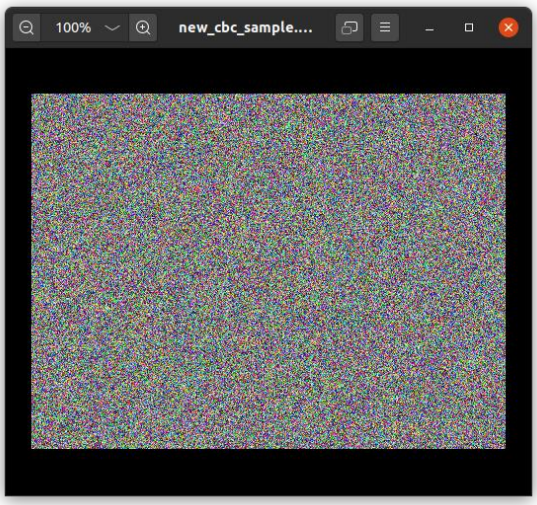
The output encrypted picture seems similar to the original picture in some way for encryption using ECB.

Part II:



```
seed@VM: ~/Desktop
[04/24/24]seed@VM:~/Desktop$ openssl enc  -aes-128-ecb  -e -in sample_pic.bmp -out ecb_cipher_sample.bmp
-K 00112233445566778889aabbccddeeff
[04/24/24]seed@VM:~/Desktop$ openssl enc  -aes-128-cbc  -e -in sample_pic.bmp -out cbc_cipher_sample.bmp
-K 00112233445566778889aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[04/24/24]seed@VM:~/Desktop$ head -c 54 sample_pic.bmp > sample_header
[04/24/24]seed@VM:~/Desktop$ tail -c +55 ecb_cipher_sample.bmp > ecb_sample_body
[04/24/24]seed@VM:~/Desktop$ tail -c +55 cbc_cipher_sample.bmp > cbc_sample_body
[04/24/24]seed@VM:~/Desktop$ cat sample_header ecb_sample_body > new_ecb_sample.bmp
[04/24/24]seed@VM:~/Desktop$ cat sample_header cbc_sample_body > new_cbc_sample.bmp
[04/24/24]seed@VM:~/Desktop$
```





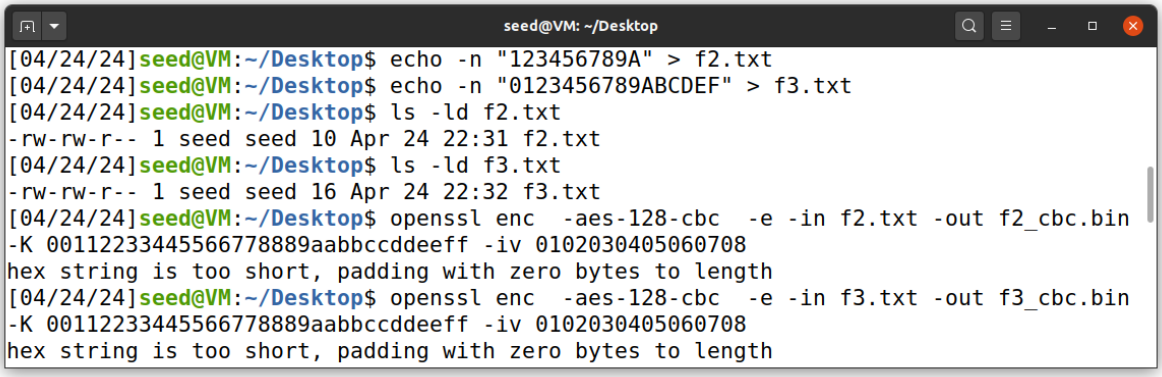
We observed that the output encrypted picture for both the encryption using ECB and CBC is no longer similar to the original picture. Hence, we can say that the more complex the image the better the encryption, although ECB will still be worser than CBC (derived from Part I).

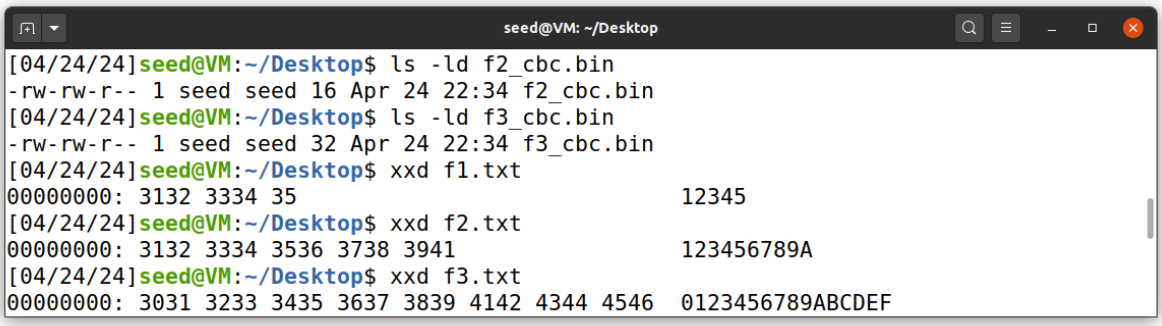
Task 4: Padding

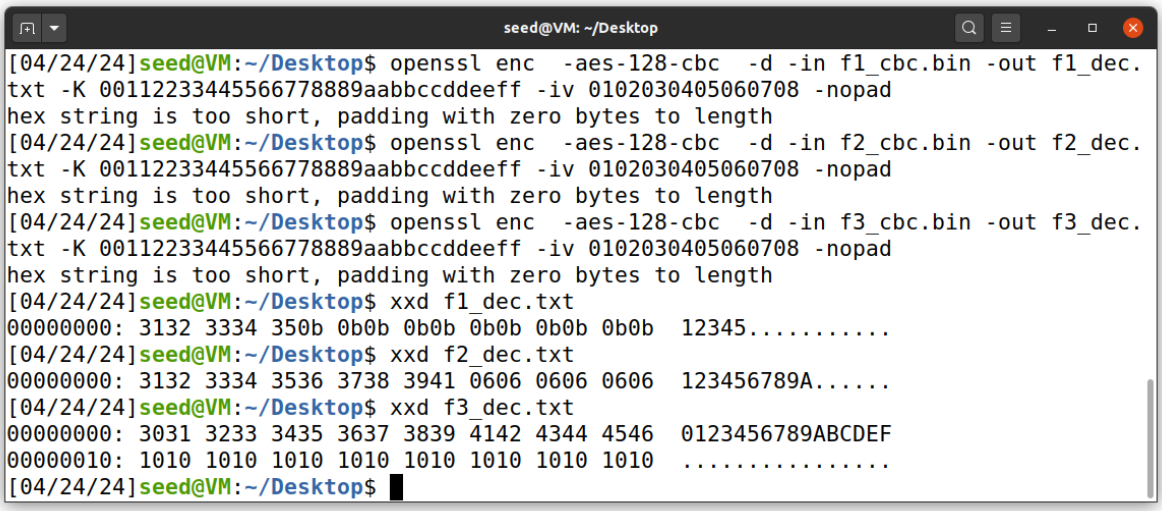
```
seed@VM: ~/Desktop
[04/24/24]seed@VM:~/Desktop$ echo -n "12345" > f1.txt
[04/24/24]seed@VM:~/Desktop$ ls -ld f1.txt
-rw-rw-r-- 1 seed seed 5 Apr 24 22:21 f1.txt
[04/24/24]seed@VM:~/Desktop$ openssl enc  -aes-128-ecb  -e -in f1.txt -out f1_ecb.bin
-K 00112233445566778889aabbccddeeff
[04/24/24]seed@VM:~/Desktop$ openssl enc  -aes-128-cbc  -e -in f1.txt -out f1_cbc.bin
-K 00112233445566778889aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[04/24/24]seed@VM:~/Desktop$ openssl enc  -aes-128-cfb  -e -in f1.txt -out f1_cfb.bin
-K 00112233445566778889aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[04/24/24]seed@VM:~/Desktop$ openssl enc  -aes-128-ofb  -e -in f1.txt -out f1_ofb.bin
-K 00112233445566778889aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[04/24/24]seed@VM:~/Desktop$ ls -ld f1_ecb.bin
-rw-rw-r-- 1 seed seed 16 Apr 24 22:24 f1_ecb.bin
[04/24/24]seed@VM:~/Desktop$ ls -ld f1_cbc.bin
-rw-rw-r-- 1 seed seed 16 Apr 24 22:25 f1_cbc.bin
[04/24/24]seed@VM:~/Desktop$ ls -ld f1_cfb.bin
-rw-rw-r-- 1 seed seed 5 Apr 24 22:25 f1_cfb.bin
[04/24/24]seed@VM:~/Desktop$ ls -ld f1_ofb.bin
-rw-rw-r-- 1 seed seed 5 Apr 24 22:26 f1_ofb.bin
[04/24/24]seed@VM:~/Desktop$
```

Observed that ECB and CBC are padded, but CFB and OFB are not.

ECB and CBC modes require padding because they operate on blocks of fixed size (usually 128 bits or 16 bytes). If the plaintext is not an exact multiple of the block size, padding is needed to fill the last block. CFB and OFB modes are stream cipher modes, meaning they operate on streams of data rather than fixed-size blocks. They generate a keystream that is XORed with the plaintext to produce the ciphertext. Since they operate on a continuous stream, they do not require padding. The keystream generation can continue until all the plaintext is encrypted, regardless of its length.



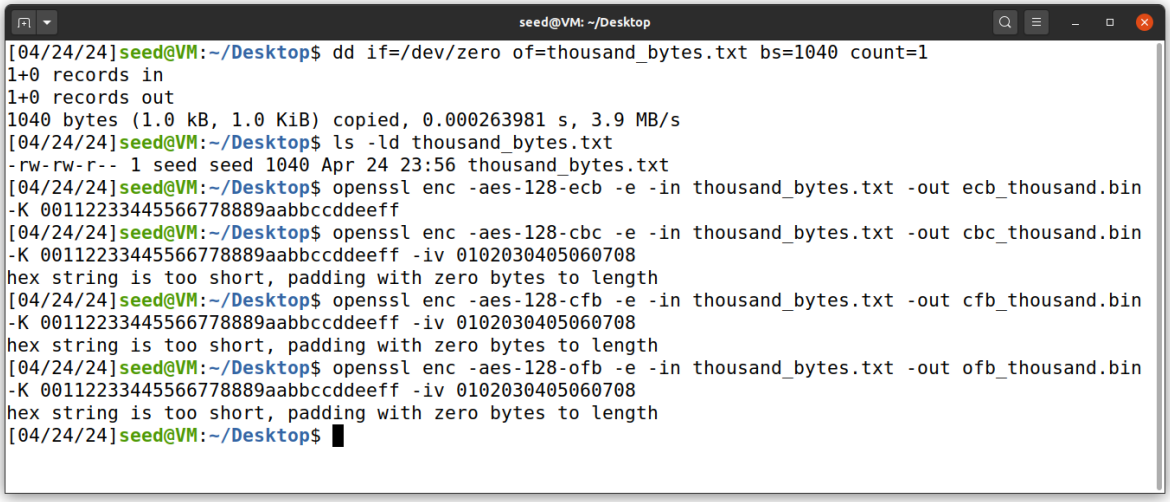




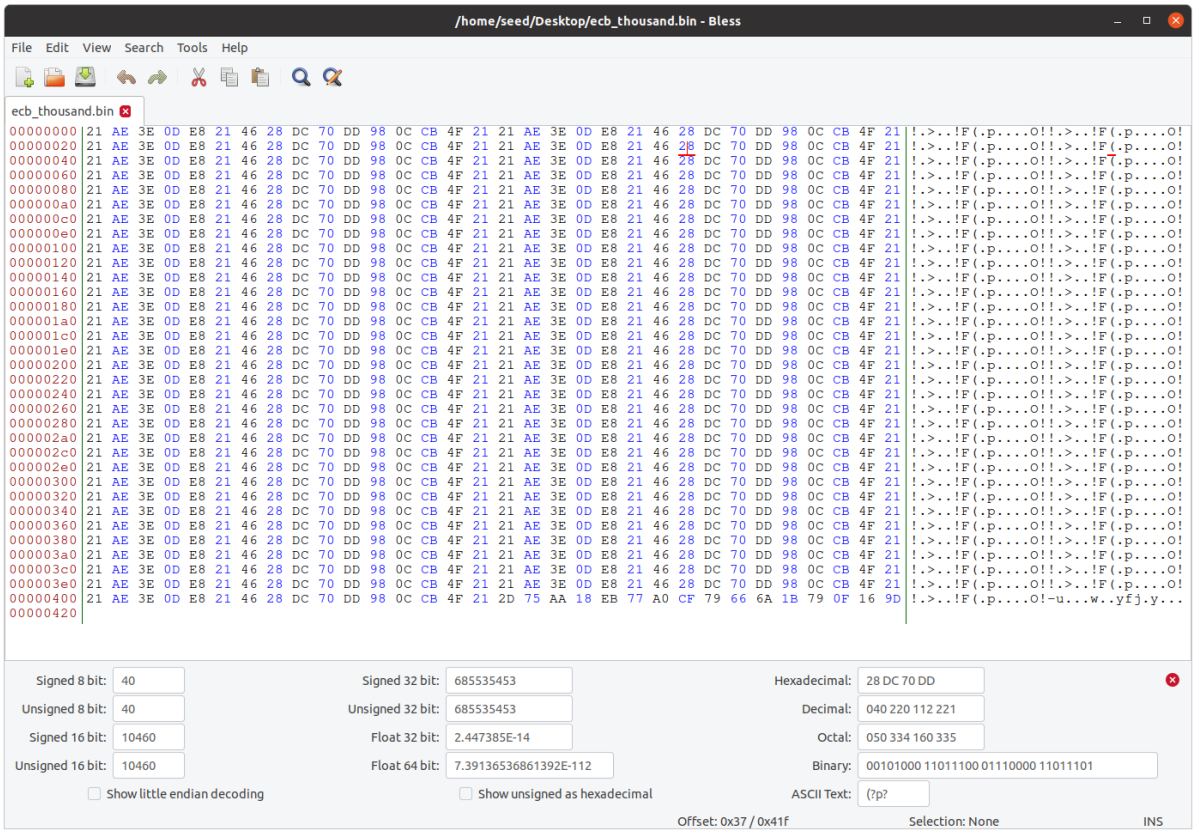
For files whose size is a multiple of the block size (16 bytes for AES), the size of the encrypted file will increase slightly due to the addition of padding. While for files whose size is not a multiple of the block size, padding will be added to make it a multiple of the block

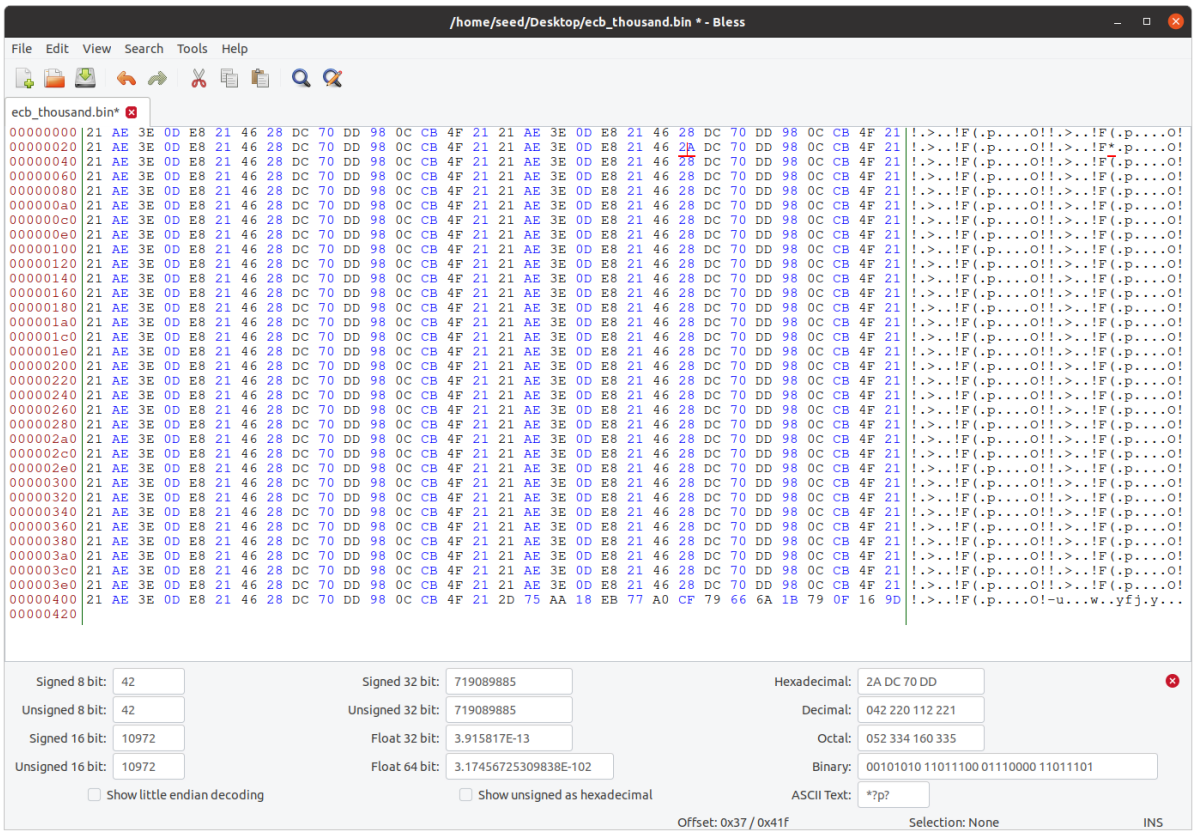
size before encryption. The size of the resulting encrypted file will depend on the original file size and the added padding.

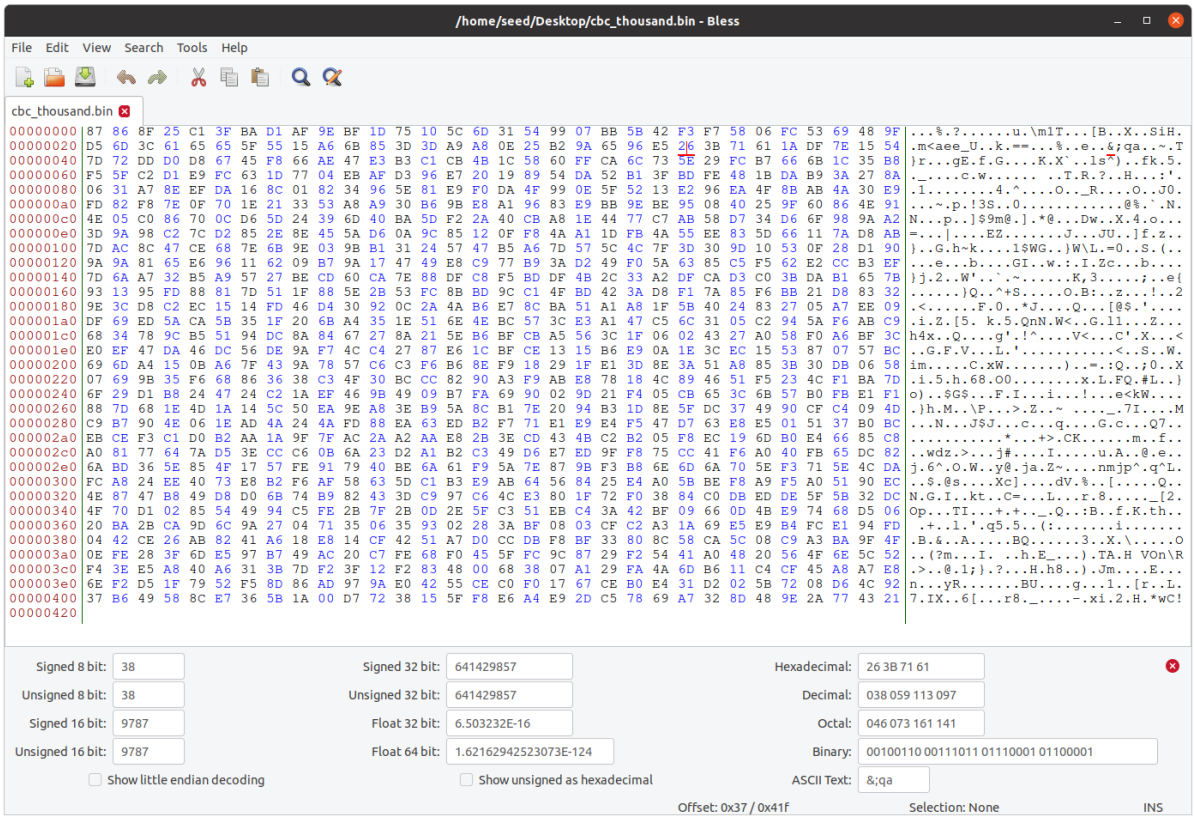
Task 5: Error Propagation – Corrupted Cipher Text

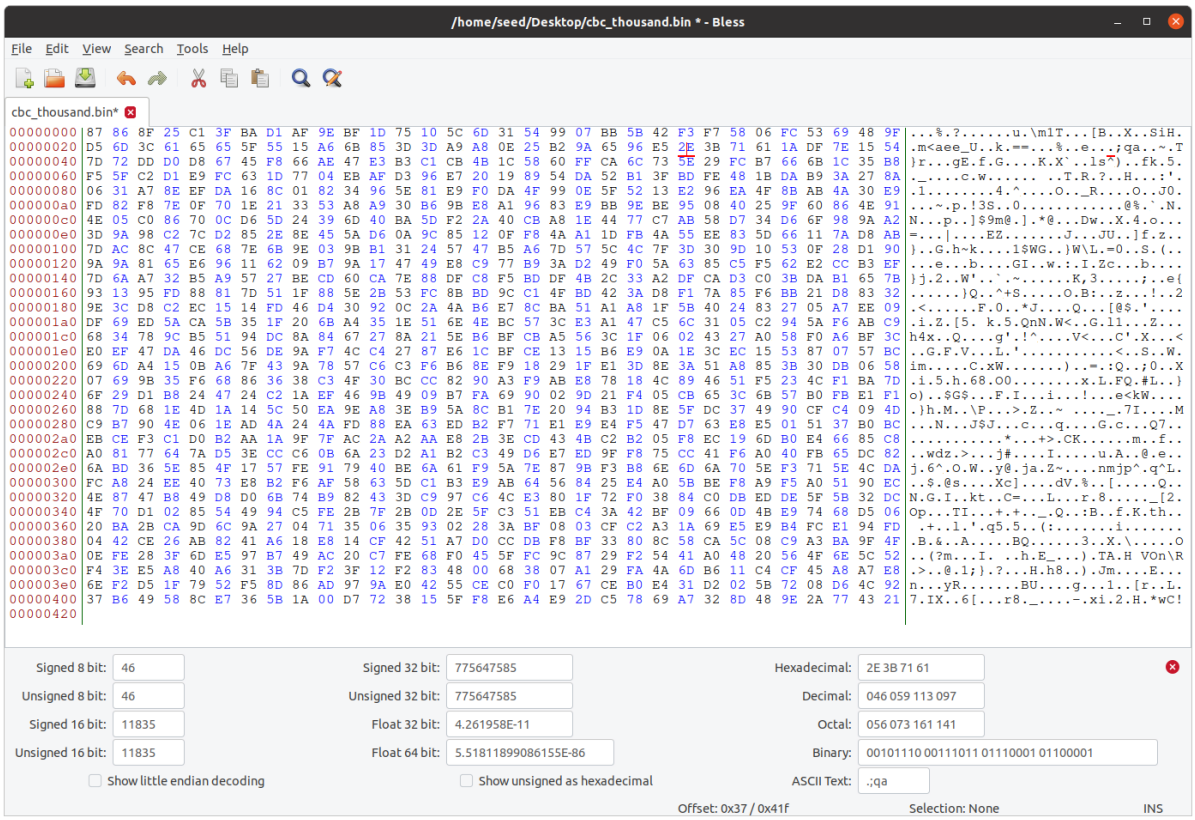


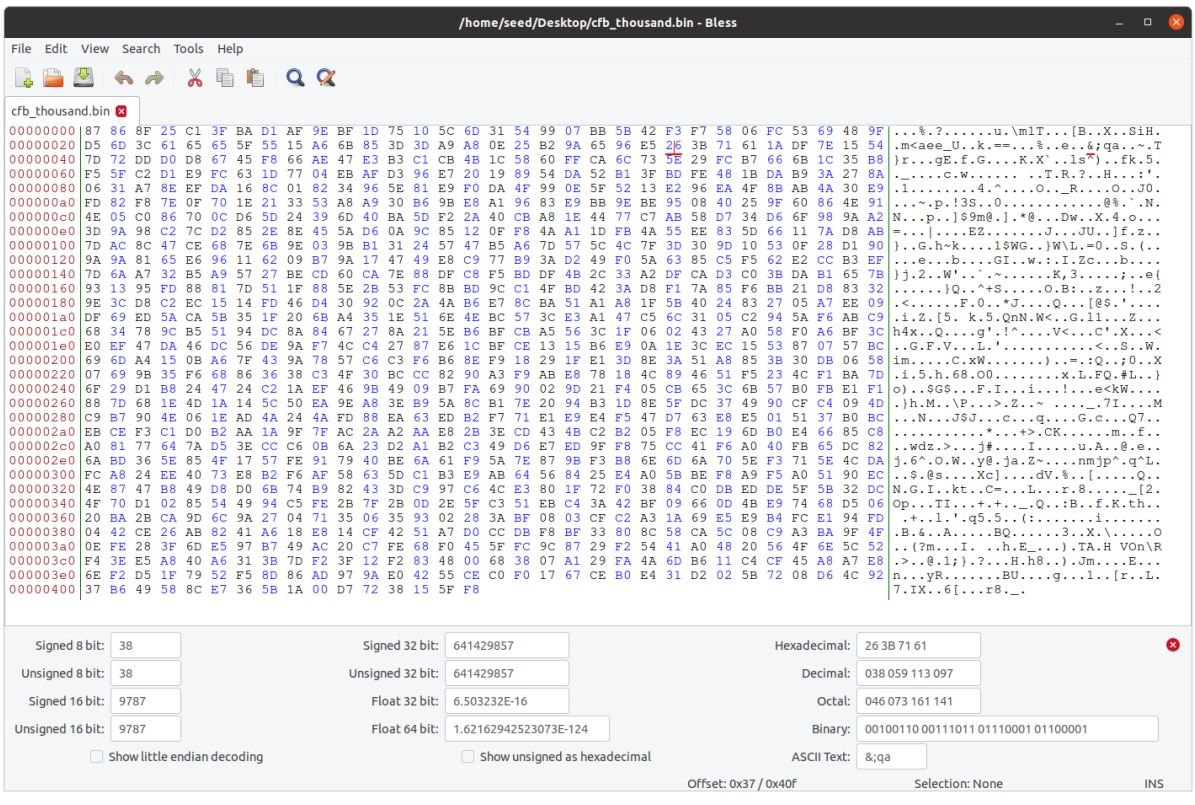
A single bit of the 55th byte in the encrypted file got corrupted:

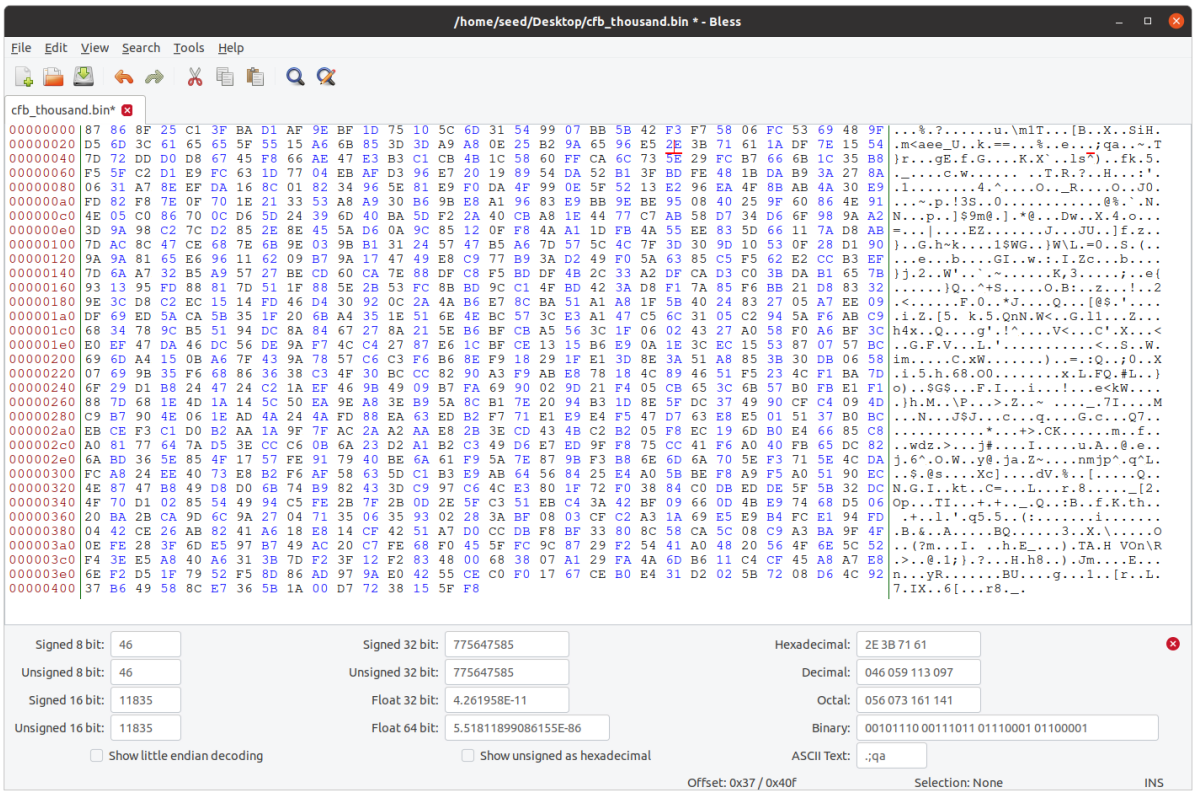


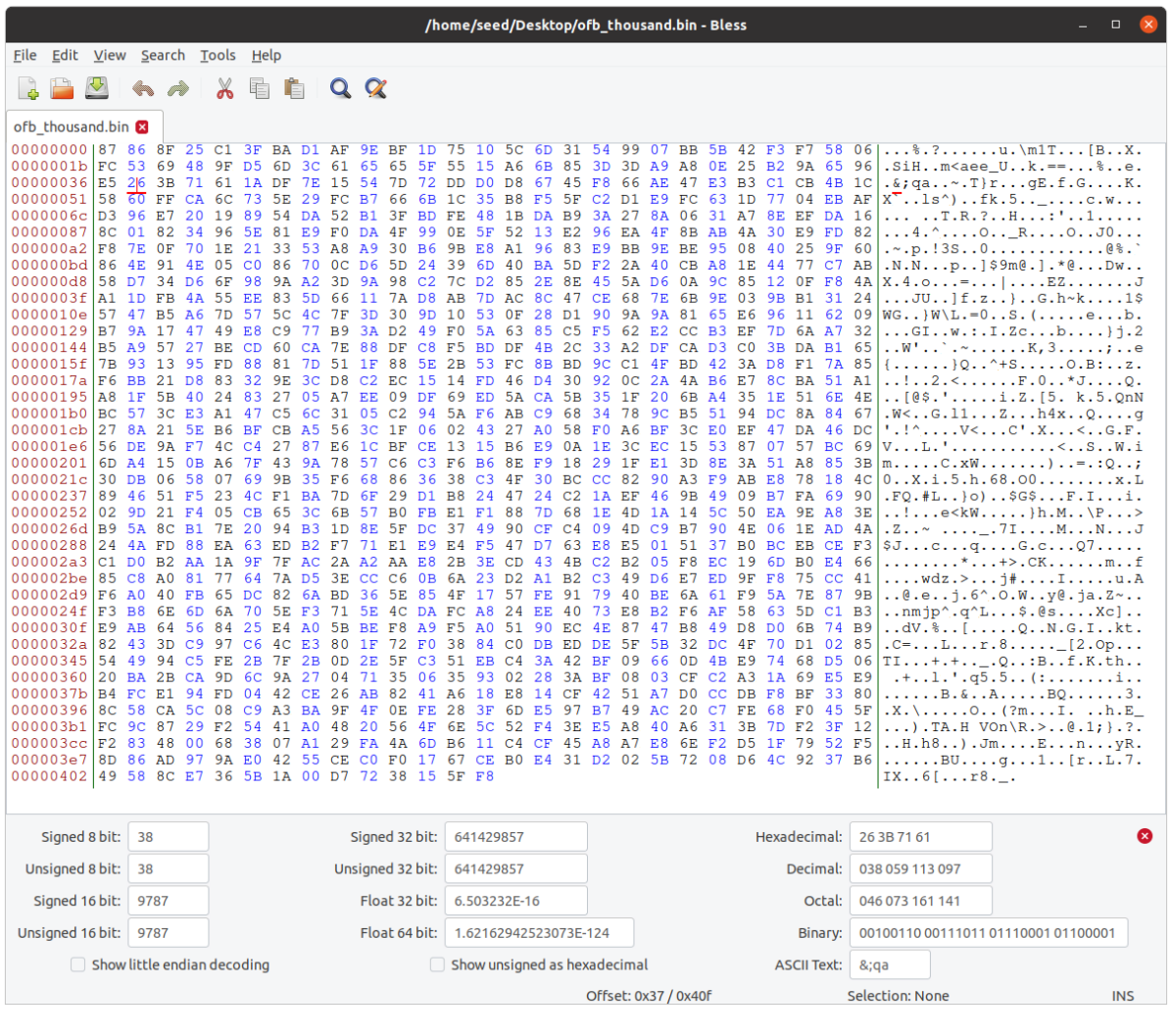

/home/seed/Desktop/ecb_thousand.bin * - Bless
File Edit View Search Tools Help
ecb_thousand.bin*
00000000 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000020 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 2A DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F*.p....O!
00000040 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000060 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000080 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000000a0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000000c0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000000e0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000100 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000120 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000140 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000160 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000180 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000001a0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000001c0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000001e0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000200 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000220 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000240 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000260 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000280 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000002a0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000002c0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000002e0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000300 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000320 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000340 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000360 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000380 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000003a0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000003c0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
000003e0 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 !.>..!F(.p....O!!.>..!F(.p....O!
00000400 21 AE 3E 0D E8 21 46 28 DC 70 DD 98 0C CB 4F 21 2D 75 AA 18 EB 77 A0 CF 79 66 6A 1B 79 0F 16 9D !.>..!F(.p....O!-u...w..yfj.y....
00000420
Signed 8 bit: 42
Signed 32 bit: 719089885
Hexadecimal: 2A DC 70 DD
Unsigned 8 bit: 42
Unsigned 32 bit: 719089885
Decimal: 042 220 112 221
Signed 16 bit: 10972
Float 32 bit: 3.915817E-13
Octal: 052 334 160 335
Unsigned 16 bit: 10972
Float 64 bit: 3.17456725309838E-102
Binary: 00101010 11011100 01110000 11011101
Show little endian decoding
Show unsigned as hexadecimal
ASCII Text: *?p?
Offset: 0x37 / 0x41f
Selection: None
INS

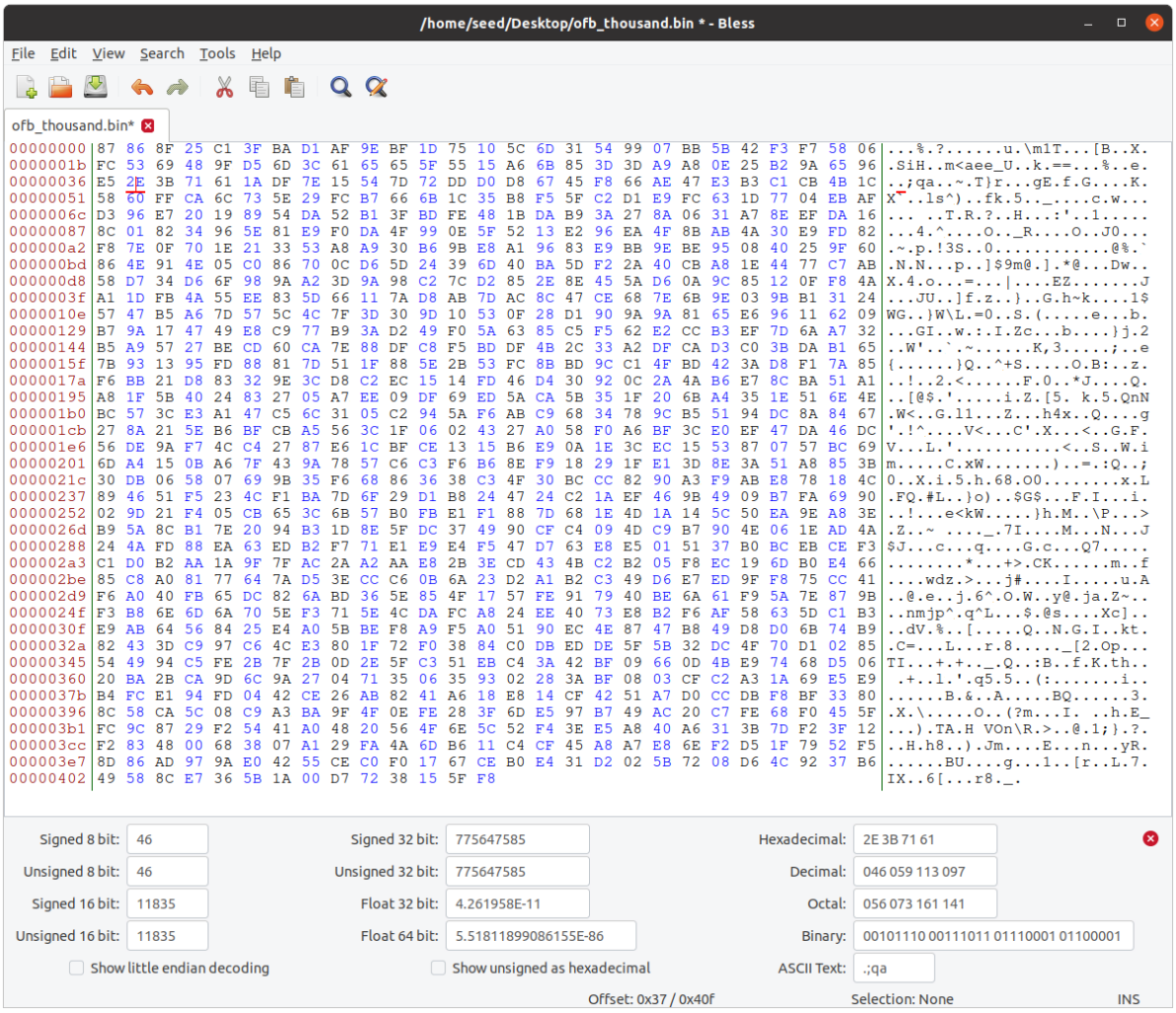

/home/seed/Desktop/cbc_thousand.bin - Bless
File Edit View Search Tools Help
cbc_thousand.bin
00000000 87 86 8F 25 C1 3F BA D1 AF 9E BF 1D 75 10 5C 6D 31 54 99 07 BB 5B 42 F3 F7 58 06 FC 53 69 48 9F ...%.?......u.\m1T...[B..X..SiH.
00000020 D5 6D 3C 61 65 65 5F 55 15 A6 6B 85 3D 3D A9 A8 0E 25 B2 9A 65 96 E5 26 3B 71 61 1A DF 7E 15 54 .m<aee_U..k.==...%..e..&;qa..~.T
00000040 7D 72 DD D0 D8 67 45 F8 66 AE 47 E3 B3 C1 CB 4B 1C 58 60 FF CA 6C 73 5E 29 FC B7 66 6B 1C 35 B8 }r...gE.f.G....K.X`..ls^)..fk.5.
00000060 F5 5F C2 D1 E9 FC 63 1D 77 04 EB AF D3 96 E7 20 19 89 54 DA 52 B1 3F BD FE 48 1B DA B9 3A 27 8A ._....c.w..... ..T.R.?..H...:'.
00000080 06 31 A7 8E EF DA 16 8C 01 82 34 96 5E 81 E9 F0 DA 4F 99 0E 5F 52 13 E2 96 EA 4F 8B AB 4A 30 E9 .1........4.^....O.._R....O..J0.
000000a0 FD 82 F8 7E 0F 70 1E 21 33 53 A8 A9 30 B6 9B E8 A1 96 83 E9 BB 9E BE 95 08 40 25 9F 60 86 4E 91 ...~.p.!3S..0.............@%.`.N.
000000c0 4E 05 C0 86 70 0C D6 5D 24 39 6D 40 BA 5D F2 2A 40 CB A8 1E 44 77 C7 AB 58 D7 34 D6 6F 98 9A A2 N...p..]$9m@.].*@...Dw..X.4.o...
000000e0 3D 9A 98 C2 7C D2 85 2E 8E 45 5A D6 0A 9C 85 12 0F F8 4A A1 1D FB 4A 55 EE 83 5D 66 11 7A D8 AB =...|....EZ.......J...JU..]f.z..
00000100 7D AC 8C 47 CE 68 7E 6B 9E 03 9B B1 31 24 57 47 B5 A6 7D 57 5C 4C 7F 3D 30 9D 10 53 0F 28 D1 90 }..G.h~k....1$WG..}W\L.=0..S.(..
00000120 9A 9A 81 65 E6 96 11 62 09 B7 9A 17 47 49 E8 C9 77 B9 3A D2 49 F0 5A 63 85 C5 F5 62 E2 CC B3 EF ...e...b....GI..w.:.I.Zc....b....
00000140 7D 6A A7 32 B5 A9 57 27 BE CD 60 CA 7E 88 DF C8 F5 BD DF 4B 2C 33 A2 DF CA D3 C0 3B DA B1 65 7B }j.2..W'..`.~.......K,3.....;..e{
00000160 93 13 95 FD 88 81 7D 51 1F 88 5E 2B 53 FC 8B BD 9C C1 4F BD 42 3A D8 F1 7A 85 F6 BB 21 D8 83 32 ......}Q..^+S.....O.B:..z...!..2
00000180 9E 3C D8 C2 EC 15 14 FD 46 D4 30 92 0C 2A 4A B6 E7 8C BA 51 A1 A8 1F 5B 40 24 83 27 05 A7 EE 09 .<......F.0..*J....Q...[@$.'....
000001a0 DF 69 ED 5A CA 5B 35 1F 20 6B A4 35 1E 51 6E 4E BC 57 3C E3 A1 47 C5 6C 31 05 C2 94 5A F6 AB C9 .i.Z.[5. k.5.QnN.W<..G.l1...Z...
000001c0 68 34 78 9C B5 51 94 DC 8A 84 67 27 8A 21 5E B6 BF CB A5 56 3C 1F 06 02 43 27 A0 58 F0 A6 BF 3C h4x..Q....g'.!^....V<...C'.X...<
000001e0 E0 EF 47 DA 46 DC 56 DE 9A F7 4C C4 27 87 E6 1C BF CE 13 15 B6 E9 0A 1E 3C EC 15 53 87 07 57 BC ..G.F.V...L.'..........<..S..W.
00000200 69 6D A4 15 0B A6 7F 43 9A 78 57 C6 C3 F6 B6 8E F9 18 29 1F E1 3D 8E 3A 51 A8 85 3B 30 DB 06 58 im.....C.xW.......)..=.:Q..;0..X
00000220 07 69 9B 35 F6 68 86 36 38 C3 4F 30 BC CC 82 90 A3 F9 AB E8 78 18 4C 89 46 51 F5 23 4C F1 BA 7D .i.5.h.68.O0........x.L.FQ.#L..}
00000240 6F 29 D1 B8 24 47 24 C2 1A EF 46 9B 49 09 B7 FA 69 90 02 9D 21 F4 05 CB 65 3C 6B 57 B0 FB E1 F1 o)..G...F.I...i...!...e<kW....
00000260 88 7D 68 1E 4D 1A 14 5C 50 EA 9E A8 3E B9 5A 8C B1 7E 20 94 B3 1D 8E 5F DC 37 49 90 CF C4 09 4D .}h.M..\P...>.Z..~ ...._.7I....M
00000280 C9 B7 90 4E 06 1E AD 4A 24 4A FD 88 EA 63 ED B2 F7 71 E1 E9 E4 F5 47 D7 63 E8 E5 01 51 37 B0 BC ...N...J$J...c...q....G.c...Q7..
000002a0 EB CE F3 C1 D0 B2 AA 1A 9F 7F AC 2A A2 AA E8 2B 3E CD 43 4B C2 B2 05 F8 EC 19 6D B0 E4 66 85 C8 ....*...+>.CK.....m..f..
000002c0 A0 81 77 64 7A D5 3E CC C6 0B 6A 23 D2 A1 B2 C3 49 D6 E7 ED 9F F8 75 CC 41 F6 A0 40 FB 65 DC 82 ..wdz.>...j#....I.....u.A..@.e..
000002e0 6A BD 36 5E 85 4F 17 57 FE 91 79 40 BE 6A 61 F9 5A 7E 87 9B F3 B8 6E 6D 6A 70 5E F3 71 5E 4C DA j.6^.O.W..y@.ja.Z~....nmjp^.q^L.
00000300 FC A8 24 EE 40 73 E8 B2 F6 AF 58 63 5D C1 B3 E9 AB 64 56 84 25 E4 A0 5B BE F8 A9 F5 A0 51 90 EC ..$.@s....Xc]....dV.%..[.....Q..
00000320 4E 87 47 B8 49 D8 D0 6B 74 B9 82 43 3D C9 97 C6 4C E3 80 1F 72 F0 38 84 C0 DB ED DE 5F 5B 32 DC N.G.I..kt..C=...L...r.8....._[2.
00000340 4F 70 D1 02 85 54 49 94 C5 FE 2B 7F 2B 0D 2E 5F C3 51 EB C4 3A 42 BF 09 66 0D 4B E9 74 68 D5 06 Op...TI...+.+._.Q..:B..f.K.th..
00000360 20 BA 2B CA 9D 6C 9A 27 04 71 35 06 35 93 02 28 3A BF 08 03 CF C2 A3 1A 69 E5 E9 B4 FC E1 94 FD .+..l.'.q5.5..(:.......i.......
00000380 04 42 CE 26 AB 82 41 A6 18 E8 14 CF 42 51 A7 D0 CC DB F8 BF 33 80 8C 58 CA 5C 08 C9 A3 BA 9F 4F .B.&..A.....BQ.....3..X.\.....O
000003a0 0E FE 28 3F 6D E5 97 B7 49 AC 20 C7 FE 68 F0 45 5F FC 9C 87 29 F2 54 41 A0 48 20 56 4F 6E 5C 52 ..(?m...I. ..h.E_...).TA.H VOn\R
000003c0 F4 3E E5 A8 40 A6 31 3B 7D F2 3F 12 F2 83 48 00 68 38 07 A1 29 FA 4A 6D B6 11 C4 CF 45 A8 A7 E8 .>..@.1;}.?...H.h8..).Jm....E...
000003e0 6E F2 D5 1F 79 52 F5 8D 86 AD 97 9A E0 42 55 CE C0 F0 17 67 CE B0 E4 31 D2 02 5B 72 08 D6 4C 92 n...yR.......BU....g...1..[r..L.
00000400 37 B6 49 58 8C E7 36 5B 1A 00 D7 72 38 15 5F F8 E6 A4 E9 2D C5 78 69 A7 32 8D 48 9E 2A 77 43 21 7.IX..6[...r8._....-.xi.2.H.*wC!
00000420
Signed 8 bit: 38
Signed 32 bit: 641429857
Hexadecimal: 26 3B 71 61
Unsigned 8 bit: 38
Unsigned 32 bit: 641429857
Decimal: 038 059 113 097
Signed 16 bit: 9787
Float 32 bit: 6.503232E-16
Octal: 046 073 161 141
Unsigned 16 bit: 9787
Float 64 bit: 1.62162942523073E-124
Binary: 00100110 00111011 01110001 01100001
Show little endian decoding
Show unsigned as hexadecimal
ASCII Text: &;qa
Offset: 0x37 / 0x41f
Selection: None
INS

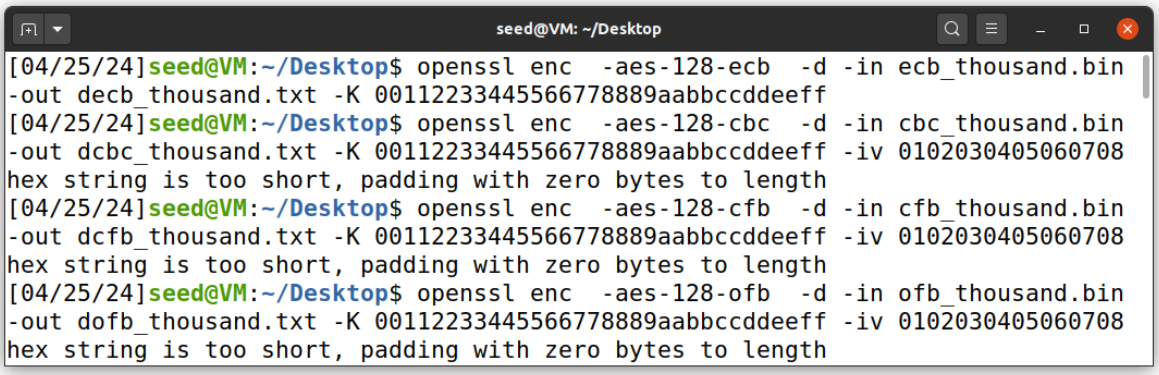

/home/seed/Desktop/cbc_thousand.bin * - Bless
File Edit View Search Tools Help
cbc_thousand.bin*
00000000 87 86 8F 25 C1 3F BA D1 AF 9E BF 1D 75 10 5C 6D 31 54 99 07 BB 5B 42 F3 F7 58 06 FC 53 69 48 9F ...%.?......u.\m1T...[B..X..SiH.
00000020 D5 6D 3C 61 65 65 5F 55 15 A6 6B 85 3D 3D A9 A8 0E 25 B2 9A 65 96 E5 2E 3B 71 61 1A DF 7E 15 54 .m<aee_U..k.==...%..e..;qa..~.T
00000040 7D 72 DD D0 D8 67 45 F8 66 AE 47 E3 B3 C1 CB 4B 1C 58 60 FF CA 6C 73 5E 29 FC B7 66 6B 1C 35 B8 }r...gE.f.G....K.X`..ls^)..fk.5.
00000060 F5 5F C2 D1 E9 FC 63 1D 77 04 EB AF D3 96 E7 20 19 89 54 DA 52 B1 3F BD FE 48 1B DA B9 3A 27 8A ._....c.w..... ..T.R.?..H...:'.
00000080 06 31 A7 8E EF DA 16 8C 01 82 34 96 5E 81 E9 F0 DA 4F 99 0E 5F 52 13 E2 96 EA 4F 8B AB 4A 30 E9 .1........4.^....O.._R....O..J0.
000000a0 FD 82 F8 7E 0F 70 1E 21 33 53 A8 A9 30 B6 9B E8 A1 96 83 E9 BB 9E BE 95 08 40 25 9F 60 86 4E 91 ...~.p.!3S..0.............@%.`.N.
000000c0 4E 05 C0 86 70 0C D6 5D 24 39 6D 40 BA 5D F2 2A 40 CB A8 1E 44 77 C7 AB 58 D7 34 D6 6F 98 9A A2 N...p..]$9m@.].*@...Dw..X.4.o...
000000e0 3D 9A 98 C2 7C D2 85 2E 8E 45 5A D6 0A 9C 85 12 0F F8 4A A1 1D FB 4A 55 EE 83 5D 66 11 7A D8 AB =...|....EZ.......J...JU..]f.z..
00000100 7D AC 8C 47 CE 68 7E 6B 9E 03 9B B1 31 24 57 47 B5 A6 7D 57 5C 4C 7F 3D 30 9D 10 53 0F 28 D1 90 }..G.h~k....1$WG..}W\L.=0..S.(..
00000120 9A 9A 81 65 E6 96 11 62 09 B7 9A 17 47 49 E8 C9 77 B9 3A D2 49 F0 5A 63 85 C5 F5 62 E2 CC B3 EF ...e...b....GI..w.:.I.Zc...b....
00000140 7D 6A A7 32 B5 A9 57 27 BE CD 60 CA 7E 88 DF C8 F5 BD DF 4B 2C 33 A2 DF CA D3 C0 3B DA B1 65 7B }j.2..W'..`.~.......K,3.....;..e{
00000160 93 13 95 FD 88 81 7D 51 1F 88 5E 2B 53 FC 8B BD 9C C1 4F BD 42 3A D8 F1 7A 85 F6 BB 21 D8 83 32 ......}Q..^+S.....O.B:..z...!..2
00000180 9E 3C D8 C2 EC 15 14 FD 46 D4 30 92 0C 2A 4A B6 E7 8C BA 51 A1 A8 1F 5B 40 24 83 27 05 A7 EE 09 .<......F.0..*J....Q...[@$.'....
000001a0 DF 69 ED 5A CA 5B 35 1F 20 6B A4 35 1E 51 6E 4E BC 57 3C E3 A1 47 C5 6C 31 05 C2 94 5A F6 AB C9 .i.Z.[5. k.5.QnN.W<..G.l1...Z...
000001c0 68 34 78 9C B5 51 94 DC 8A 84 67 27 8A 21 5E B6 BF CB A5 56 3C 1F 06 02 43 27 A0 58 F0 A6 BF 3C h4x..Q....g'.!^....V<...C'.X...<
000001e0 E0 EF 47 DA 46 DC 56 DE 9A F7 4C C4 27 87 E6 1C BF CE 13 15 B6 E9 0A 1E 3C EC 15 53 87 07 57 BC ..G.F.V...L.'...........<..S..W.
00000200 69 6D A4 15 0B A6 7F 43 9A 78 57 C6 C3 F6 B6 8E F9 18 29 1F E1 3D 8E 3A 51 A8 85 3B 30 DB 06 58 im.....C.xW.......)..=.:Q..;0..X
00000220 07 69 9B 35 F6 68 86 36 38 C3 4F 30 BC CC 82 90 A3 F9 AB E8 78 18 4C 89 46 51 F5 23 4C F1 BA 7D .i.5.h.68.O0........x.L.FQ.#L..}
00000240 6F 29 D1 B8 24 47 24 C2 1A EF 46 9B 49 09 B7 FA 69 90 02 9D 21 F4 05 CB 65 3C 6B 57 B0 FB E1 F1 o)..G...F.I...i...!...e<kW....
00000260 88 7D 68 1E 4D 1A 14 5C 50 EA 9E A8 3E B9 5A 8C B1 7E 20 94 B3 1D 8E 5F DC 37 49 90 CF C4 09 4D .}h.M..\P...>.Z..~ ...._.7I....M
00000280 C9 B7 90 4E 06 1E AD 4A 24 4A FD 88 EA 63 ED B2 F7 71 E1 E9 E4 F5 47 D7 63 E8 E5 01 51 37 B0 BC ...N...J$J...c...q....G.c...Q7..
000002a0 EB CE F3 C1 D0 B2 AA 1A 9F 7F AC 2A A2 AA E8 2B 3E CD 43 4B C2 B2 05 F8 EC 19 6D B0 E4 66 85 C8 ....*...+>.CK......m..f..
000002c0 A0 81 77 64 7A D5 3E CC C6 0B 6A 23 D2 A1 B2 C3 49 D6 E7 ED 9F F8 75 CC 41 F6 A0 40 FB 65 DC 82 ..wdz.>...j#....I.....u.A..@.e..
000002e0 6A BD 36 5E 85 4F 17 57 FE 91 79 40 BE 6A 61 F9 5A 7E 87 9B F3 B8 6E 6D 6A 70 5E F3 71 5E 4C DA j.6^.O.W..y@.ja.Z~....nmjp^.q^L.
00000300 FC A8 24 EE 40 73 E8 B2 F6 AF 58 63 5D C1 B3 E9 AB 64 56 84 25 E4 A0 5B BE F8 A9 F5 A0 51 90 EC ..$.@s....Xc]....dV.%..[.....Q..
00000320 4E 87 47 B8 49 D8 D0 6B 74 B9 82 43 3D C9 97 C6 4C E3 80 1F 72 F0 38 84 C0 DB ED DE 5F 5B 32 DC N.G.I..kt..C=...L...r.8....._[2.
00000340 4F 70 D1 02 85 54 49 94 C5 FE 2B 7F 2B 0D 2E 5F C3 51 EB C4 3A 42 BF 09 66 0D 4B E9 74 68 D5 06 Op...TI...+.+._.Q..:B..f.K.th..
00000360 20 BA 2B CA 9D 6C 9A 27 04 71 35 06 35 93 02 28 3A BF 08 03 CF C2 A3 1A 69 E5 E9 B4 FC E1 94 FD .+..l.'.q5.5..(:.......i.......
00000380 04 42 CE 26 AB 82 41 A6 18 E8 14 CF 42 51 A7 D0 CC DB F8 BF 33 80 8C 58 CA 5C 08 C9 A3 BA 9F 4F .B.&..A.....BQ.....3..X.\.....O
000003a0 0E FE 28 3F 6D E5 97 B7 49 AC 20 C7 FE 68 F0 45 5F FC 9C 87 29 F2 54 41 A0 48 20 56 4F 6E 5C 52 ..(?m...I. ..h.E_...).TA.H VOn\R
000003c0 F4 3E E5 A8 40 A6 31 3B 7D F2 3F 12 F2 83 48 00 68 38 07 A1 29 FA 4A 6D B6 11 C4 CF 45 A8 A7 E8 .>..@.1;}.?...H.h8..).Jm....E...
000003e0 6E F2 D5 1F 79 52 F5 8D 86 AD 97 9A E0 42 55 CE C0 F0 17 67 CE B0 E4 31 D2 02 5B 72 08 D6 4C 92 n...yR.......BU....g...1..[r..L.
00000400 37 B6 49 58 8C E7 36 5B 1A 00 D7 72 38 15 5F F8 E6 A4 E9 2D C5 78 69 A7 32 8D 48 9E 2A 77 43 21 7.IX..6[...r8._....-.xi.2.H.*wC!
00000420
Signed 8 bit: 46
Unsigned 8 bit: 46
Signed 16 bit: 11835
Unsigned 16 bit: 11835
Signed 32 bit: 775647585
Unsigned 32 bit: 775647585
Float 32 bit: 4.261958E-11
Float 64 bit: 5.51811899086155E-86
Hexadecimal: 2E 3B 71 61
Decimal: 046 059 113 097
Octal: 056 073 161 141
Binary: 00101110 00111011 01110001 01100001
ASCII Text: .;qa
Show little endian decoding
Show unsigned as hexadecimal
Offset: 0x37 / 0x41f
Selection: None
INS

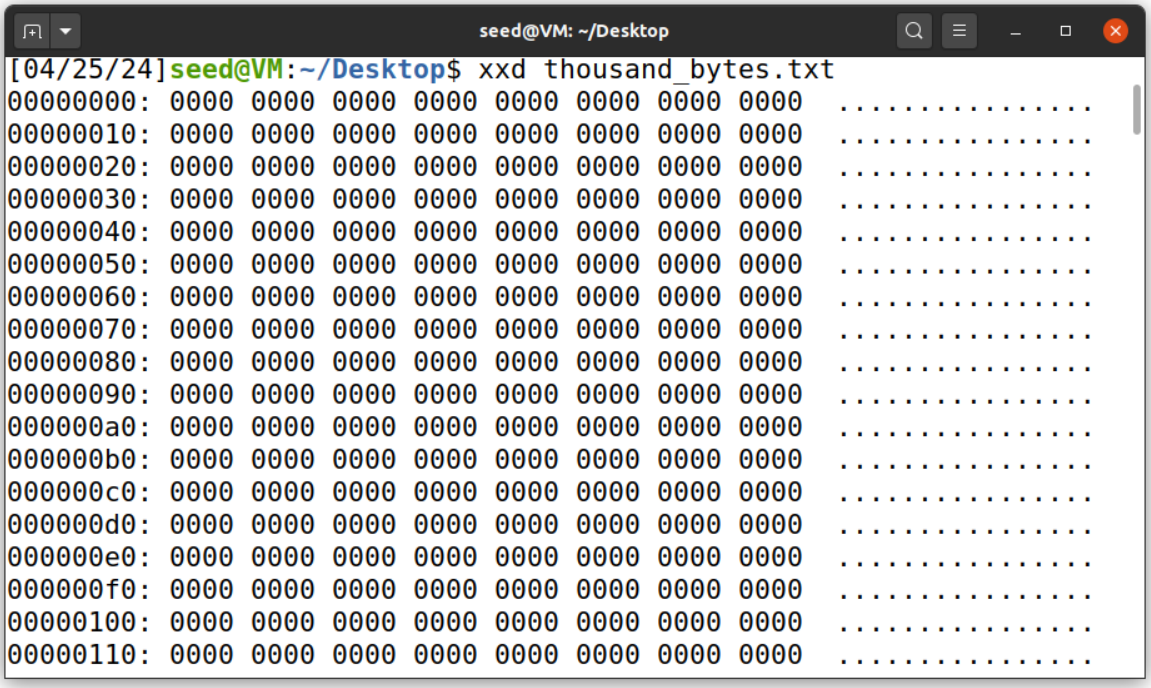

/home/seed/Desktop/cfb_thousand.bin - Bless
File Edit View Search Tools Help
cfb_thousand.bin
00000000 87 86 8F 25 C1 3F BA D1 AF 9E BF 1D 75 10 5C 6D 31 54 99 07 BB 5B 42 F3 F7 58 06 FC 53 69 48 9F ...%.?......u.\m1T...[B..X..SiH.
00000020 D5 6D 3C 61 65 65 5F 55 15 A6 6B 85 3D 3D A9 A8 0E 25 B2 9A 65 96 E5 26 3B 71 61 1A DF 7E 15 54 .m<aee_U..k.==...%..e..&;qa..~.T
00000040 7D 72 DD D0 D8 67 45 F8 66 AE 47 E3 B3 C1 CB 4B 1C 58 60 FF CA 6C 73 5E 29 FC B7 66 6B 1C 35 B8 }r...gE.f.G....K.X`..ls^)..fk.5.
00000060 F5 5F C2 D1 E9 FC 63 1D 77 04 EB AF D3 96 E7 20 19 89 54 DA 52 B1 3F BD FE 48 1B DA B9 3A 27 8A ._....c.w..... ..T.R.?..H...:'.
00000080 06 31 A7 8E EF DA 16 8C 01 82 34 96 5E 81 E9 F0 DA 4F 99 0E 5F 52 13 E2 96 EA 4F 8B AB 4A 30 E9 .1........4.^....O.._R....O..J0.
000000a0 FD 82 F8 7E 0F 70 1E 21 33 53 A8 A9 30 B6 9B E8 A1 96 83 E9 BB 9E BE 95 08 40 25 9F 60 86 4E 91 ...~.p.!3S..0.............@%.`.N.
000000c0 4E 05 C0 86 70 0C D6 5D 24 39 6D 40 BA 5D F2 2A 40 CB A8 1E 44 77 C7 AB 58 D7 34 D6 6F 98 9A A2 N...p..]$9m@.].*@...Dw..X.4.o...
000000e0 3D 9A 98 C2 7C D2 85 2E 8E 45 5A D6 0A 9C 85 12 0F F8 4A A1 1D FB 4A 55 EE 83 5D 66 11 7A D8 AB =...|....EZ.......J...JU..]f.z..
00000100 7D AC 8C 47 CE 68 7E 6B 9E 03 9B B1 31 24 57 47 B5 A6 7D 57 5C 4C 7F 3D 30 9D 10 53 0F 28 D1 90 }..G.h~k....1$WG..}W\L.=0..S.(..
00000120 9A 9A 81 65 E6 96 11 62 09 B7 9A 17 47 49 E8 C9 77 B9 3A D2 49 F0 5A 63 85 C5 F5 62 E2 CC B3 EF ...e...b....GI..w.:.I.Zc...b....
00000140 7D 6A A7 32 B5 A9 57 27 BE CD 60 CA 7E 88 DF C8 F5 BD DF 4B 2C 33 A2 DF CA D3 C0 3B DA B1 65 7B }j.2..W'..`.~.......K,3.....;..e{
00000160 93 13 95 FD 88 81 7D 51 1F 88 5E 2B 53 FC 8B BD 9C C1 4F BD 42 3A D8 F1 7A 85 F6 BB 21 D8 83 32 ......}Q..^+S.....O.B:..z...!..2
00000180 9E 3C D8 C2 EC 15 14 FD 46 D4 30 92 0C 2A 4A B6 E7 8C BA 51 A1 A8 1F 5B 40 24 83 27 05 A7 EE 09 .<......F.0..*J....Q...[@$.'....
000001a0 DF 69 ED 5A CA 5B 35 1F 20 6B A4 35 1E 51 6E 4E BC 57 3C E3 A1 47 C5 6C 31 05 C2 94 5A F6 AB C9 .i.Z.[5. k.5.QnN.W<..G.l1...Z...
000001c0 68 34 78 9C B5 51 94 DC 8A 84 67 27 8A 21 5E B6 BF CB A5 56 3C 1F 06 02 43 27 A0 58 F0 A6 BF 3C h4x..Q....g'.!^....V<...C'.X...<
000001e0 E0 EF 47 DA 46 DC 56 DE 9A F7 4C C4 27 87 E6 1C BF CE 13 15 B6 E9 0A 1E 3C EC 15 53 87 07 57 BC ..G.F.V...L.'...........<..S..W.
00000200 69 6D A4 15 0B A6 7F 43 9A 78 57 C6 C3 F6 B6 8E F9 18 29 1F E1 3D 8E 3A 51 A8 85 3B 30 DB 06 58 im.....C.xW.......)..=.:Q..;0..X
00000220 07 69 9B 35 F6 68 86 36 38 C3 4F 30 BC CC 82 90 A3 F9 AB E8 78 18 4C 89 46 51 F5 23 4C F1 BA 7D .i.5.h.68.O0........x.L.FQ.#L..}
00000240 6F 29 D1 B8 24 47 24 C2 1A EF 46 9B 49 09 B7 FA 69 90 02 9D 21 F4 05 CB 65 3C 6B 57 B0 FB E1 F1 o)..G...F.I...i...!...e<kW....
00000260 88 7D 68 1E 4D 1A 14 5C 50 EA 9E A8 3E B9 5A 8C B1 7E 20 94 B3 1D 8E 5F DC 37 49 90 CF C4 09 4D .}h.M..\P...>.Z..~ ...._.7I....M
00000280 C9 B7 90 4E 06 1E AD 4A 24 4A FD 88 EA 63 ED B2 F7 71 E1 E9 E4 F5 47 D7 63 E8 E5 01 51 37 B0 BC ...N...J$J...c...q....G.c...Q7..
000002a0 EB CE F3 C1 D0 B2 AA 1A 9F 7F AC 2A A2 AA E8 2B 3E CD 43 4B C2 B2 05 F8 EC 19 6D B0 E4 66 85 C8 ....*...+>.CK......m..f..
000002c0 A0 81 77 64 7A D5 3E CC C6 0B 6A 23 D2 A1 B2 C3 49 D6 E7 ED 9F F8 75 CC 41 F6 A0 40 FB 65 DC 82 ..wdz.>...j#....I.....u.A..@.e..
000002e0 6A BD 36 5E 85 4F 17 57 FE 91 79 40 BE 6A 61 F9 5A 7E 87 9B F3 B8 6E 6D 6A 70 5E F3 71 5E 4C DA j.6^.O.W..y@.ja.Z~....nmjp^.q^L.
00000300 FC A8 24 EE 40 73 E8 B2 F6 AF 58 63 5D C1 B3 E9 AB 64 56 84 25 E4 A0 5B BE F8 A9 F5 A0 51 90 EC ..$.@s....Xc]....dV.%..[.....Q..
00000320 4E 87 47 B8 49 D8 D0 6B 74 B9 82 43 3D C9 97 C6 4C E3 80 1F 72 F0 38 84 C0 DB ED DE 5F 5B 32 DC N.G.I..kt..C=...L...r.8....._[2.
00000340 4F 70 D1 02 85 54 49 94 C5 FE 2B 7F 2B 0D 2E 5F C3 51 EB C4 3A 42 BF 09 66 0D 4B E9 74 68 D5 06 Op...TI...+.+._.Q..:B..f.K.th..
00000360 20 BA 2B CA 9D 6C 9A 27 04 71 35 06 35 93 02 28 3A BF 08 03 CF C2 A3 1A 69 E5 E9 B4 FC E1 94 FD .+..l.'.q5.5..(:.......i.......
00000380 04 42 CE 26 AB 82 41 A6 18 E8 14 CF 42 51 A7 D0 CC DB F8 BF 33 80 8C 58 CA 5C 08 C9 A3 BA 9F 4F .B.&..A.....BQ.....3..X.\.....O
000003a0 0E FE 28 3F 6D E5 97 B7 49 AC 20 C7 FE 68 F0 45 5F FC 9C 87 29 F2 54 41 A0 48 20 56 4F 6E 5C 52 ..(?m...I. ..h.E_...).TA.H VOn\R
000003c0 F4 3E E5 A8 40 A6 31 3B 7D F2 3F 12 F2 83 48 00 68 38 07 A1 29 FA 4A 6D B6 11 C4 CF 45 A8 A7 E8 .>..@.1;}.?...H.h8..).Jm....E...
000003e0 6E F2 D5 1F 79 52 F5 8D 86 AD 97 9A E0 42 55 CE C0 F0 17 67 CE B0 E4 31 D2 02 5B 72 08 D6 4C 92 n...yR.......BU....g...1..[r..L.
00000400 37 B6 49 58 8C E7 36 5B 1A 00 D7 72 38 15 5F F8 7.IX..6[...r8._.
Signed 8 bit: 38
Unsigned 8 bit: 38
Signed 16 bit: 9787
Unsigned 16 bit: 9787
Signed 32 bit: 641429857
Unsigned 32 bit: 641429857
Float 32 bit: 6.503232E-16
Float 64 bit: 1.62162942523073E-124
Hexadecimal: 26 3B 71 61
Decimal: 038 059 113 097
Octal: 046 073 161 141
Binary: 00100110 00111011 01110001 01100001
ASCII Text: &;qa
Show little endian decoding
Show unsigned as hexadecimal
Offset: 0x37 / 0x40f
Selection: None
INS

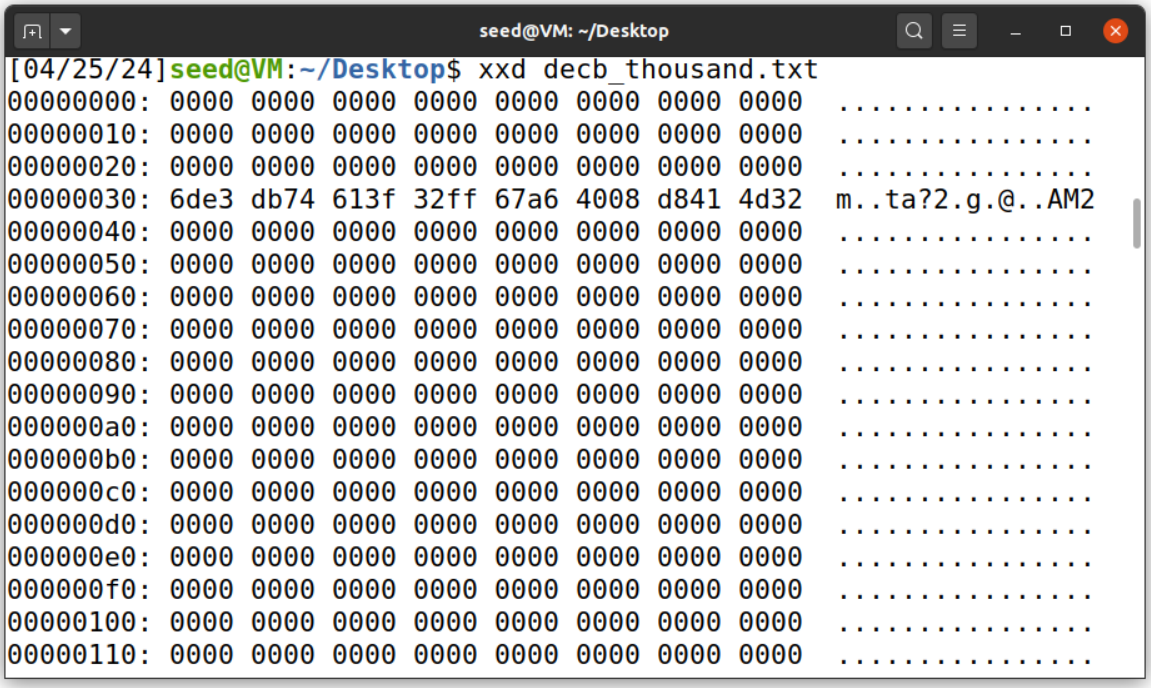

/home/seed/Desktop/cfb_thousand.bin * - Bless
File Edit View Search Tools Help
cfb_thousand.bin*
00000000 87 86 8F 25 C1 3F BA D1 AF 9E BF 1D 75 10 5C 6D 31 54 99 07 BB 5B 42 F3 F7 58 06 FC 53 69 48 9F
00000020 D5 6D 3C 61 65 65 5F 55 15 A6 6B 85 3D 3D A9 A8 0E 25 B2 9A 65 96 E5 2E 3B 71 61 1A DF 7E 15 54
00000040 7D 72 DD D0 D8 67 45 F8 66 AE 47 E3 B3 C1 CB 4B 1C 58 60 FF CA 6C 73 5E 29 FC B7 66 6B 1C 35 B8
00000060 F5 5F C2 D1 E9 FC 63 1D 77 04 EB AF D3 96 E7 20 19 89 54 DA 52 B1 3F BD FE 48 1B DA B9 3A 27 8A
00000080 06 31 A7 8E EF DA 16 8C 01 82 34 96 5E 81 E9 F0 DA 4F 99 0E 5F 52 13 E2 96 EA 4F 8B AB 4A 30 E9
000000a0 FD 82 F8 7E 0F 70 1E 21 33 53 A8 A9 30 B6 9B E8 A1 96 83 E9 BB 9E BE 95 08 40 25 9F 60 86 4E 91
000000c0 4E 05 C0 86 70 0C D6 5D 24 39 6D 40 BA 5D F2 2A 40 CB A8 1E 44 77 C7 AB 58 D7 34 D6 6F 98 9A A2
000000e0 3D 9A 98 C2 7C D2 85 2E 8E 45 5A D6 0A 9C 85 12 0F F8 4A A1 1D FB 4A 55 EE 83 5D 66 11 7A D8 AB
00000100 7D AC 8C 47 CE 68 7E 6B 9E 03 9B B1 31 24 57 47 B5 A6 7D 57 5C 4C 7F 3D 30 9D 10 53 0F 28 D1 90
00000120 9A 9A 81 65 E6 96 11 62 09 B7 9A 17 47 49 E8 C9 77 B9 3A D2 49 F0 5A 63 85 C5 F5 62 E2 CC B3 EF
00000140 7D 6A A7 32 B5 A9 57 27 BE CD 60 CA 7E 88 DF C8 F5 BD DF 4B 2C 33 A2 DF CA D3 C0 3B DA B1 65 7B
00000160 93 13 95 FD 88 81 7D 51 1F 88 5E 2B 53 FC 8B BD 9C C1 4F BD 42 3A D8 F1 7A 85 F6 BB 21 D8 83 32
00000180 9E 3C D8 C2 EC 15 14 FD 46 D4 30 92 0C 2A 4A B6 E7 8C BA 51 A1 A8 1F 5B 40 24 83 27 05 A7 EE 09
000001a0 DF 69 ED 5A CA 5B 35 1F 20 6B A4 35 1E 51 6E 4E BC 57 3C E3 A1 47 C5 6C 31 05 C2 94 5A F6 AB C9
000001c0 68 34 78 9C B5 51 94 DC 8A 84 67 27 8A 21 5E B6 BF CB A5 56 3C 1F 06 02 43 27 A0 58 F0 A6 BF 3C
000001e0 E0 EF 47 DA 46 DC 56 DE 9A F7 4C C4 27 87 E6 1C BF CE 13 15 B6 E9 0A 1E 3C EC 15 53 87 07 57 BC
00000200 69 6D A4 15 0B A6 7F 43 9A 78 57 C6 C3 F6 B6 8E F9 18 29 1F E1 3D 8E 3A 51 A8 85 3B 30 DB 06 58
00000220 07 69 9B 35 F6 68 86 36 38 C0 4F 30 BC CC 82 90 A3 F9 AB E8 78 18 4C 89 46 51 F5 23 4C F1 BA 7D
00000240 6F 29 D1 B8 24 47 24 C2 1A EF 46 9B 49 09 B7 FA 69 90 02 9D 21 F4 05 CB 65 3C 6B 57 B0 FB E1 F1
00000260 88 7D 68 1E 4D 1A 14 5C 50 EA 9E A8 3E B9 5A 8C B1 7E 20 94 B3 1D 8E 5F DC 37 49 90 CF C4 09 4D
00000280 C9 B7 90 4E 06 1E AD 4A 24 4A FD 88 EA 63 ED B2 F7 71 E1 E9 E4 F5 47 D7 63 E8 E5 01 51 37 B0 BC
000002a0 EB CE F3 C1 D0 B2 AA 1A 9F 7F AC 2A A2 AA E8 2B 3E CD 43 4B C2 B2 05 F8 EC 19 6D B0 E4 66 85 C8
000002c0 A0 81 77 64 7A D5 3E CC C6 0B 6A 23 D2 A1 B2 C3 49 D6 E7 ED 9F F8 75 CC 41 F6 A0 40 FB 65 DC 82
000002e0 6A BD 36 5E 85 4F 17 57 FE 91 79 40 BE 6A 61 F9 5A 7E 87 9B F3 B8 6E 6D 6A 70 5E F3 71 5E 4C DA
00000300 FC A8 24 EE 40 73 E8 B2 F6 AF 58 63 5D C1 B3 E9 AB 64 56 84 25 E4 A0 5B BE F8 A9 F5 A0 51 90 EC
00000320 4E 87 47 B8 49 D8 D0 6B 74 B9 82 43 3D C9 97 C6 4C E3 80 1F 72 F0 38 84 C0 DB ED DE 5F 5B 32 DC
00000340 4F 70 D1 02 85 54 49 94 C5 FE 2B 7F 2B 0D 2E 5F C3 51 EB C4 3A 42 BF 09 66 0D 4B E9 74 68 D5 06
00000360 20 BA 2B CA 9D 6C 9A 27 04 71 35 06 35 93 02 28 3A BF 08 03 CF C2 A3 1A 69 E5 E9 B4 FC E1 94 FD
00000380 04 42 CE 26 AB 82 41 A6 18 E8 14 CF 42 51 A7 D0 CC DB F8 BF 33 80 8C 58 CA 5C 08 C9 A3 BA 9F 4F
000003a0 0E FE 28 3F 6D E5 97 B7 49 AC 20 C7 FE 68 F0 45 5F FC 9C 87 29 F2 54 41 A0 48 20 56 4F 6E 5C 52
000003c0 F4 3E E5 A8 40 A6 31 3B 7D F2 3F 12 F2 83 48 00 68 38 07 A1 29 FA 4A 6D B6 11 C4 CF 45 A8 A7 E8
000003e0 6E F2 D5 1F 79 52 F5 8D 86 AD 97 9A E0 42 55 CE C0 F0 17 67 CE B0 E4 31 D2 02 5B 72 08 D6 4C 92
00000400 37 B6 49 58 8C E7 36 5B 1A 00 D7 72 38 15 5F F8
Signed 8 bit: 46
Unsigned 8 bit: 46
Signed 16 bit: 11835
Unsigned 16 bit: 11835
Signed 32 bit: 775647585
Unsigned 32 bit: 775647585
Float 32 bit: 4.261958E-11
Float 64 bit: 5.51811899086155E-86
Hexadecimal: 2E 3B 71 61
Decimal: 046 059 113 097
Octal: 056 073 161 141
Binary: 00101110 00111011 01110001 01100001
ASCII Text: .;qa
Show little endian decoding
Show unsigned as hexadecimal
Offset: 0x37 / 0x40f
Selection: None
INS


/home/seed/Desktop/ofb_thousand.bin - Bless
File Edit View Search Tools Help
ofb_thousand.bin
00000000 87 86 8F 25 C1 3F BA D1 AF 9E BF 1D 75 10 5C 6D 31 54 99 07 BB 5B 42 F3 F7 58 06
0000001b FC 53 69 48 9F D5 6D 3C 61 65 65 5F 55 15 A6 6B 85 3D 3D A9 A8 0E 25 B2 9A 65 96
00000036 E5 26 3B 71 61 1A DF 7E 15 54 7D 72 DD D0 D8 67 45 F8 66 AE 47 E3 B3 C1 CB 4B 1C
00000051 58 60 FF CA 6C 73 5E 29 FC B7 66 6B 1C 35 B8 F5 5F C2 D1 E9 FC 63 1D 77 04 EB AF
0000006c D3 96 E7 20 19 89 54 DA 52 B1 3F BD FE 48 1B DA B9 3A 27 8A 06 31 A7 8E EF DA 16
00000087 8C 01 82 34 96 5E 81 E9 F0 DA 4F 99 0E 5F 52 13 E2 96 EA 4F 8B AB 4A 30 E9 FD 82
000000a2 F8 7E 0F 70 1E 21 33 53 A8 A9 30 B6 9B E8 A1 96 83 E9 BB 9E BE 95 08 40 25 9F 60
000000bd 86 4E 91 4E 05 C0 86 70 0C D6 5D 24 39 6D 40 BA 5D F2 2A 40 CB A8 1E 44 77 C7 AB
000000d8 58 D7 34 D6 6F 98 9A A2 3D 9A 98 C2 7C D2 85 2E 8E 45 5A D6 0A 9C 85 12 0F F8 4A
0000003f A1 1D FB 4A 55 EE 83 5D 66 11 7A D8 AB 7D AC 8C 47 CE 68 7E 6B 9E 03 9B B1 31 24
0000010e 57 47 B5 A6 7D 57 5C 4C 7F 3D 30 9D 10 53 0F 28 D1 90 9A 9A 81 65 E6 96 11 62 09
00000129 B7 9A 17 47 49 E8 C9 77 B9 3A D2 49 F0 5A 63 85 C5 F5 62 E2 CC B3 EF 7D 6A A7 32
00000144 B5 A9 57 27 BE CD 60 CA 7E 88 DF C8 F5 BD DF 4B 2C 33 A2 DF CA D3 C0 3B DA B1 65
0000015f 7B 93 13 95 FD 88 81 7D 51 1F 88 5E 2B 53 FC 8B BD 9C C1 4F BD 42 3A D8 F1 7A 85
0000017a F6 BB 21 D8 83 32 9E 3C D8 C2 EC 15 14 FD 46 D4 30 92 0C 2A 4A B6 E7 8C BA 51 A1
00000195 A8 1F 5B 40 24 83 27 05 A7 EE 09 DF 69 ED 5A CA 5B 35 1F 20 6B A4 35 1E 51 6E 4E
000001b0 BC 57 3C E3 A1 47 C5 6C 31 05 C2 94 5A F6 AB C9 68 34 78 9C B5 51 94 DC 8A 84 67
000001cb 27 8A 21 5E B6 BF CB A5 56 3C 1F 06 02 43 27 A0 58 F0 A6 BF 3C E0 EF 47 DA 46 DC
000001e6 56 DE 9A F7 4C C4 27 87 E6 1C BF CE 13 15 B6 E9 0A 1E 3C EC 15 53 87 07 57 BC 69
00000201 6D A4 15 0B A6 7F 43 9A 78 57 C6 C3 F6 B6 8E F9 18 29 1F E1 3D 8E 3A 51 A8 85 3B
0000021c 30 DB 06 58 07 69 9B 35 F6 68 86 36 38 C3 4F 30 BC CC 82 90 A3 F9 AB E8 78 18 4C
00000237 89 46 51 F5 23 4C F1 BA 7D 6F 29 D1 B8 24 47 24 C2 1A EF 46 9B 49 09 B7 FA 69 90
00000252 02 9D 21 F4 05 CB 65 3C 6B 57 B0 FB E1 F1 88 7D 68 1E 4D 1A 14 5C 50 EA 9E A8 3E
0000026d B9 5A 8C B1 7E 20 94 B3 1D 8E 5F DC 37 49 90 CF C4 09 4D C9 B7 90 4E 06 1E AD 4A
00000288 24 4A FD 88 EA 63 ED B2 F7 71 E1 E9 E4 F5 47 D7 63 E8 E5 01 51 37 B0 BC EB CE F3
000002a3 C1 D0 B2 AA 1A 9F 7F AC 2A A2 AA E8 2B 3E CD 43 4B C2 B2 05 F8 EC 19 6D B0 E4 66
000002be 85 C8 A0 81 77 64 7A D5 3E CC C6 0B 6A 23 D2 A1 B2 C3 49 D6 E7 ED 9F F8 75 CC 41
000002d9 F6 A0 40 FB 65 DC 82 6A BD 36 5E 85 4F 17 57 FE 91 79 40 BE 6A 61 F9 5A 7E 87 9B
0000024f F3 B8 6E 6D 6A 70 5E F3 71 5E 4C DA FC A8 24 EE 40 73 E8 B2 F6 AF 58 63 5D C1 B3
0000030f E9 AB 64 56 84 25 E4 A0 5B BE F8 A9 F5 A0 51 90 EC 4E 87 47 B8 49 D8 D0 6B 74 B9
0000032a 82 43 3D C9 97 C6 4C E3 80 1F 72 F0 38 84 C0 DB ED DE 5F 5B 32 DC 4F 70 D1 02 85
00000345 54 49 94 C5 FE 2B 7F 2B 0D 2E 5F C3 51 EB C4 3A 42 BF 09 66 0D 4B E9 74 68 D5 06
00000360 20 BA 2B CA 9D 6C 9A 27 04 71 35 06 35 93 02 28 3A BF 08 03 CF C2 A3 1A 69 E5 E9
0000037b B4 FC E1 94 FD 04 42 CE 26 AB 82 41 A6 18 E8 14 CF 42 51 A7 D0 CC DB F8 BF 33 80
00000396 8C 58 CA 5C 08 C9 A3 BA 9F 4F 0E FE 28 3F 6D E5 97 B7 49 AC 20 C7 FE 68 F0 45 5F
000003b1 FC 9C 87 29 F2 54 41 A0 48 20 56 4F 6E 5C 52 F4 3E E5 A8 40 A6 31 3B 7D F2 3F 12
000003cc F2 83 48 00 68 38 07 A1 29 FA 4A 6D B6 11 C4 CF 45 A8 A7 E8 6E F2 D5 1F 79 52 F5
000003e7 8D 86 AD 97 9A E0 42 55 CE C0 F0 17 67 CE B0 E4 31 D2 02 5B 72 08 D6 4C 92 37 B6
00000402 49 58 8C E7 36 5B 1A 00 D7 72 38 15 5F F8
Signed 8 bit: 38
Unsigned 8 bit: 38
Signed 16 bit: 9787
Unsigned 16 bit: 9787
Signed 32 bit: 641429857
Unsigned 32 bit: 641429857
Float 32 bit: 6.503232E-16
Float 64 bit: 1.62162942523073E-124
Hexadecimal: 26 3B 71 61
Decimal: 038 059 113 097
Octal: 046 073 161 141
Binary: 00100110 00111011 01110001 01100001
ASCII Text: &;qa
Show little endian decoding
Show unsigned as hexadecimal
Offset: 0x37 / 0x40f
Selection: None
INS

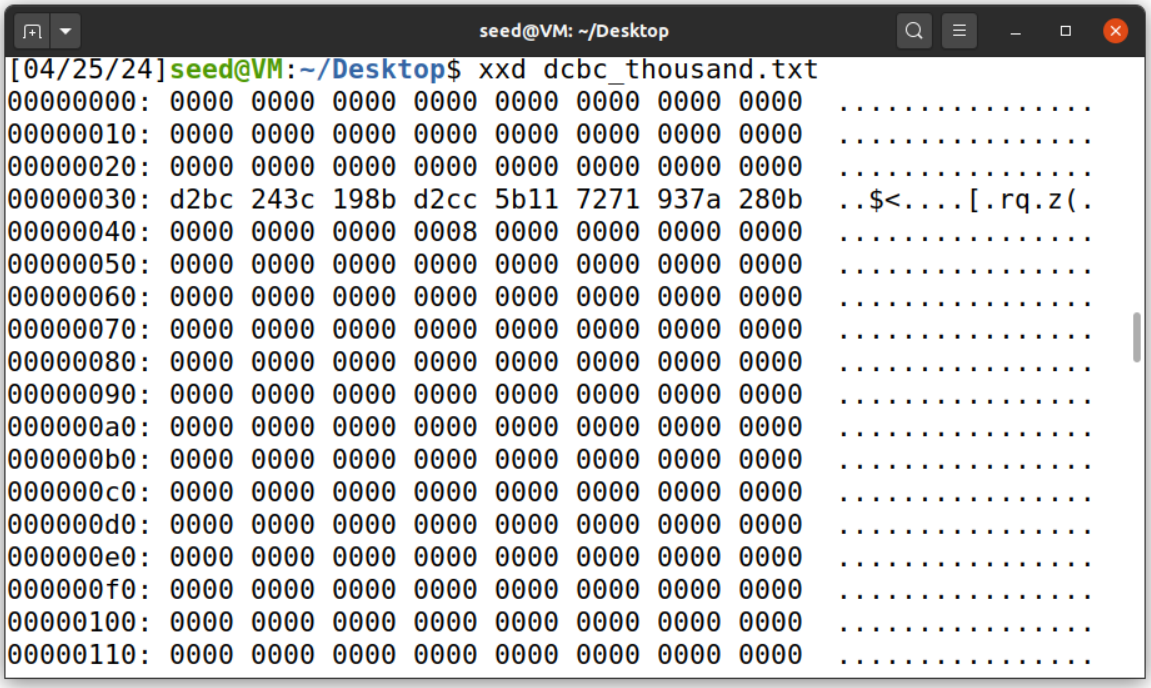

/home/seed/Desktop/ofb_thousand.bin * - Bless
File Edit View Search Tools Help
ofb_thousand.bin*
00000000 87 86 8F 25 C1 3F BA D1 AF 9E BF 1D 75 10 5C 6D 31 54 99 07 BB 5B 42 F3 F7 58 06 ...%.?......u.\m1T...[B..X.
0000001b FC 53 69 48 9F D5 6D 3C 61 65 65 5F 55 15 A6 6B 85 3D 3D A9 A8 0E 25 B2 9A 65 96 .SiH..m<aee_U..k.==...%..e.
00000036 E5 2E 3B 71 61 1A DF 7E 15 54 7D 72 DD D0 D8 67 45 F8 66 AE 47 E3 B3 C1 CB 4B 1C ..;qa..~.T}r...gE.f.G....K.
00000051 58 60 FF CA 6C 73 5E 29 FC B7 66 6B 1C 35 B8 F5 5F C2 D1 E9 FC 63 1D 77 04 EB AF X`..ls^)..fk.5._....c.w...
0000006c D3 96 E7 20 19 89 54 DA 52 B1 3F BD FE 48 1B DA B9 3A 27 8A 06 31 A7 8E EF DA 16 ... ..T.R.?..H...:'..1.....
00000087 8C 01 82 34 96 5E 81 E9 F0 DA 4F 99 0E 5F 52 13 E2 96 EA 4F 8B AB 4A 30 E9 FD 82 ...4.^....O.._R....O..J0...
000000a2 F8 7E 0F 70 1E 21 33 53 A8 A9 30 B6 9B E8 A1 96 83 E9 BB 9E BE 95 08 40 25 9F 60 .~.p.!3S..0.............@%.`
000000bd 86 4E 91 4E 05 C0 86 70 0C D6 5D 24 39 6D 40 BA 5D F2 2A 40 CB A8 1E 44 77 C7 AB .N.N...p..]$9m@.].*@...Dw..
000000d8 58 D7 34 D6 6F 98 9A A2 3D 9A 98 C2 7C D2 85 2E 8E 45 5A D6 0A 9C 85 12 0F F8 4A X.4.o...=...|....EZ.......J
0000003f A1 1D FB 4A 55 EE 83 5D 66 11 7A D8 AB 7D AC 8C 47 CE 68 7E 6B 9E 03 9B B1 31 24 ...JU..]f.z..}..G.h~k....1$
0000010e 57 47 B5 A6 7D 57 5C 4C 7F 3D 30 9D 10 53 0F 28 D1 90 9A 9A 81 65 E6 96 11 62 09 WG..}W\L.=0..S.(.....e...b.
00000129 B7 9A 17 47 49 E8 C9 77 B9 3A D2 49 F0 5A 63 85 C5 F5 62 E2 CC B3 EF 7D 6A A7 32 ...GI..w.:.I.Zc...b....}j.2
00000144 B5 A9 57 27 BE CD 60 CA 7E 88 DF C8 F5 BD DF 4B 2C 33 A2 DF CA D3 C0 3B DA B1 65 ..W'..`.~......K,3.....;..e
0000015f 7B 93 13 95 FD 88 81 7D 51 1F 88 5E 2B 53 FC 8B BD 9C C1 4F BD 42 3A D8 F1 7A 85 {.....}Q..^+S.....O.B:..z.
0000017a F6 BB 21 D8 83 32 9E 3C D8 C2 EC 15 14 FD 46 D4 30 92 0C 2A 4A B6 E7 8C BA 51 A1 ..!..2.<......F.0..*J....Q.
00000195 A8 1F 5B 40 24 83 27 05 A7 EE 09 DF 69 ED 5A CA 5B 35 1F 20 6B A4 35 1E 51 6E 4E ..[@$.'.....i.Z.[5. k.5.QnN
000001b0 BC 57 3C E3 A1 47 C5 6C 31 05 C2 94 5A F6 AB C9 68 34 78 9C B5 51 94 DC 8A 84 67 .W<..G.l1...Z...h4x..Q....g
000001cb 27 8A 21 5E B6 BF CB A5 56 3C 1F 06 02 43 27 A0 58 F0 A6 BF 3C E0 EF 47 DA 46 DC '.!^....V<...C'.X...<..G.F.
000001e6 56 DE 9A F7 4C C4 27 87 E6 1C BF CE 13 15 B6 E9 0A 1E 3C EC 15 53 87 07 57 BC 69 V...L.'..........<..S..W.i
00000201 6D A4 15 0B A6 7F 43 9A 78 57 C6 C3 F6 B6 8E F9 18 29 1F E1 3D 8E 3A 51 A8 85 3B m.....C.xW.......)..=.:Q..;
0000021c 30 DB 06 58 07 69 9B 35 F6 68 86 36 38 C3 4F 30 BC CC 82 90 A3 F9 AB E8 78 18 4C 0..X.i.5.h.68.O0.........x.L
00000237 89 46 51 F5 23 4C F1 BA 7D 6F 29 D1 B8 24 47 24 C2 1A EF 46 9B 49 09 B7 FA 69 90 .FQ.#L..}o)..G...F.I...i.
00000252 02 9D 21 F4 05 CB 65 3C 6B 57 B0 FB E1 F1 88 7D 68 1E 4D 1A 14 5C 50 EA 9E A8 3E ..!...e<kW.....}h.M..\P...>
0000026d B9 5A 8C B1 7E 20 94 B3 1D 8E 5F DC 37 49 90 CF C4 09 4D C9 B7 90 4E 06 1E AD 4A .Z..~ ...._.7I....M...N...J
00000288 24 4A FD 88 EA 63 ED B2 F7 71 E1 E9 E4 F5 47 D7 63 E8 E5 01 51 37 B0 BC EB CE F3 $J...c...q....G.c...Q7.....
000002a3 C1 D0 B2 AA 1A 9F 7F AC 2A A2 AA E8 2B 3E CD 43 4B C2 B2 05 F8 EC 19 6D B0 E4 66 ....*...+>.CK.....m..f
000002be 85 C8 A0 81 77 64 7A D5 3E CC C6 0B 6A 23 D2 A1 B2 C3 49 D6 E7 ED 9F F8 75 CC 41 ....wdz.>...j#....I.....u.A
000002d9 F6 A0 40 FB 65 DC 82 6A BD 36 5E 85 4F 17 57 FE 91 79 40 BE 6A 61 F9 5A 7E 87 9B ..@.e..j.6^.O.W..y@.ja.Z~..
0000024f F3 B8 6E 6D 6A 70 5E F3 71 5E 4C DA FC A8 24 EE 40 73 E8 B2 F6 AF 58 63 5D C1 B3 ..nmjp^.q^L...$.@s....Xc]..
0000030f E9 AB 64 56 84 25 E4 A0 5B BE F8 A9 F5 A0 51 90 EC 4E 87 47 B8 49 D8 D0 6B 74 B9 ..dV.%..[.....Q..N.G.I..kt.
0000032a 82 43 3D C9 97 C6 4C E3 80 1F 72 F0 38 84 C0 DB ED DE 5F 5B 32 DC 4F 70 D1 02 85 .C=...L...r.8....._[2.Op...
00000345 54 49 94 C5 FE 2B 7F 2B 0D 2E 5F C3 51 EB C4 3A 42 BF 09 66 0D 4B E9 74 68 D5 06 TI...+.+.._.Q.:B..f.K.th..
00000360 20 BA 2B CA 9D 6C 9A 27 04 71 35 06 35 93 02 28 3A BF 08 03 CF C2 A3 1A 69 E5 E9 .+..l.'.q5.5..(:.......i..
0000037b B4 FC E1 94 FD 04 42 CE 26 AB 82 41 A6 18 E8 14 CF 42 51 A7 D0 CC DB F8 BF 33 80 ......B.&..A.....BQ......3.
00000396 8C 58 CA 5C 08 C9 A3 BA 9F 4F 0E FE 28 3F 6D E5 97 B7 49 AC 20 C7 FE 68 F0 45 5F .X.\.....O..(?m...I. ..h.E_
000003b1 FC 9C 87 29 F2 54 41 A0 48 20 56 4F 6E 5C 52 F4 3E E5 A8 40 A6 31 3B 7D F2 3F 12 ...).TA.H VOn\R.>..@.1;}.?.
000003cc F2 83 48 00 68 38 07 A1 29 FA 4A 6D B6 11 C4 CF 45 A8 A7 E8 6E F2 D5 1F 79 52 F5 ..H.h8..).Jm....E...n...yR.
000003e7 8D 86 AD 97 9A E0 42 55 CE C0 F0 17 67 CE B0 E4 31 D2 02 5B 72 08 D6 4C 92 37 B6 ......BU....g...1..[r..L.7.
00000402 49 58 8C E7 36 5B 1A 00 D7 72 38 15 5F F8 IX..6[...r8._.
Signed 8 bit: 46
Unsigned 8 bit: 46
Signed 16 bit: 11835
Unsigned 16 bit: 11835
Signed 32 bit: 775647585
Unsigned 32 bit: 775647585
Float 32 bit: 4.261958E-11
Float 64 bit: 5.51811899086155E-86
Hexadecimal: 2E 3B 71 61
Decimal: 046 059 113 097
Octal: 056 073 161 141
Binary: 00101110 00111011 01110001 01100001
ASCII Text: .;qa
Show little endian decoding
Show unsigned as hexadecimal
Offset: 0x37 / 0x40f
Selection: None
INS


seed@VM: ~/Desktop
[04/25/24]seed@VM:~/Desktop$ openssl enc -aes-128-ecb -d -in ecb_thousand.bin
-out decb_thousand.txt -K 00112233445566778889aabbccddeeff
[04/25/24]seed@VM:~/Desktop$ openssl enc -aes-128-cbc -d -in cbc_thousand.bin
-out dcbc_thousand.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[04/25/24]seed@VM:~/Desktop$ openssl enc -aes-128-cfb -d -in cfb_thousand.bin
-out dcfb_thousand.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[04/25/24]seed@VM:~/Desktop$ openssl enc -aes-128-ofb -d -in ofb_thousand.bin
-out dofb_thousand.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
hex string is too short, padding with zero bytes to length

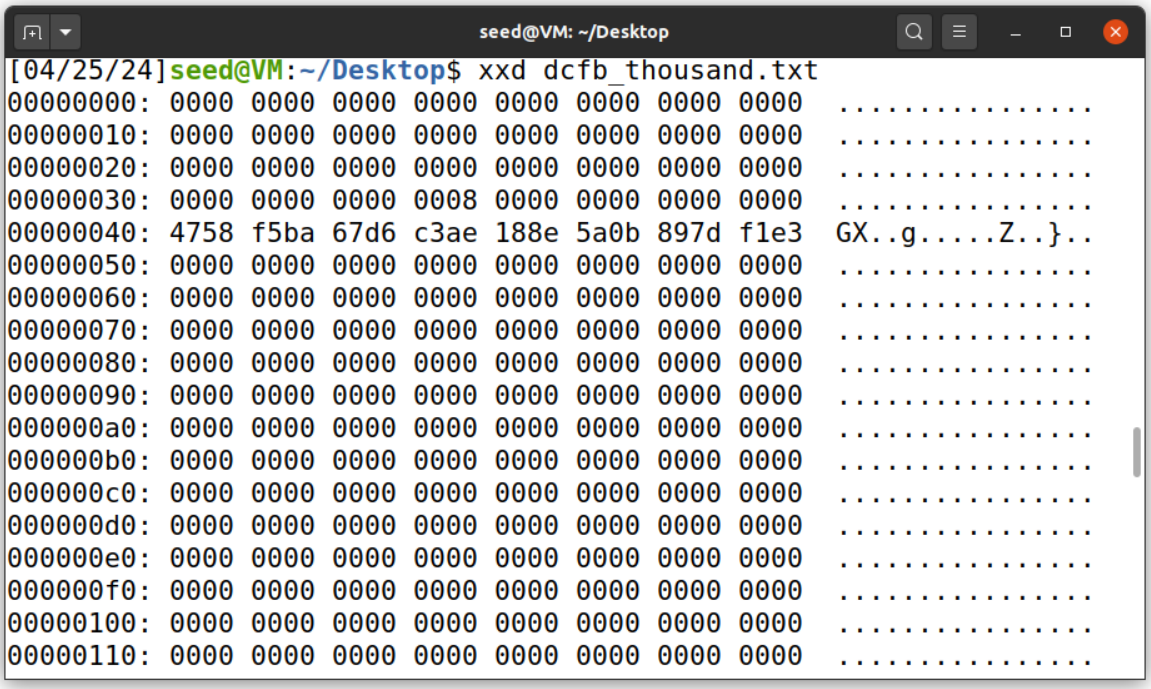




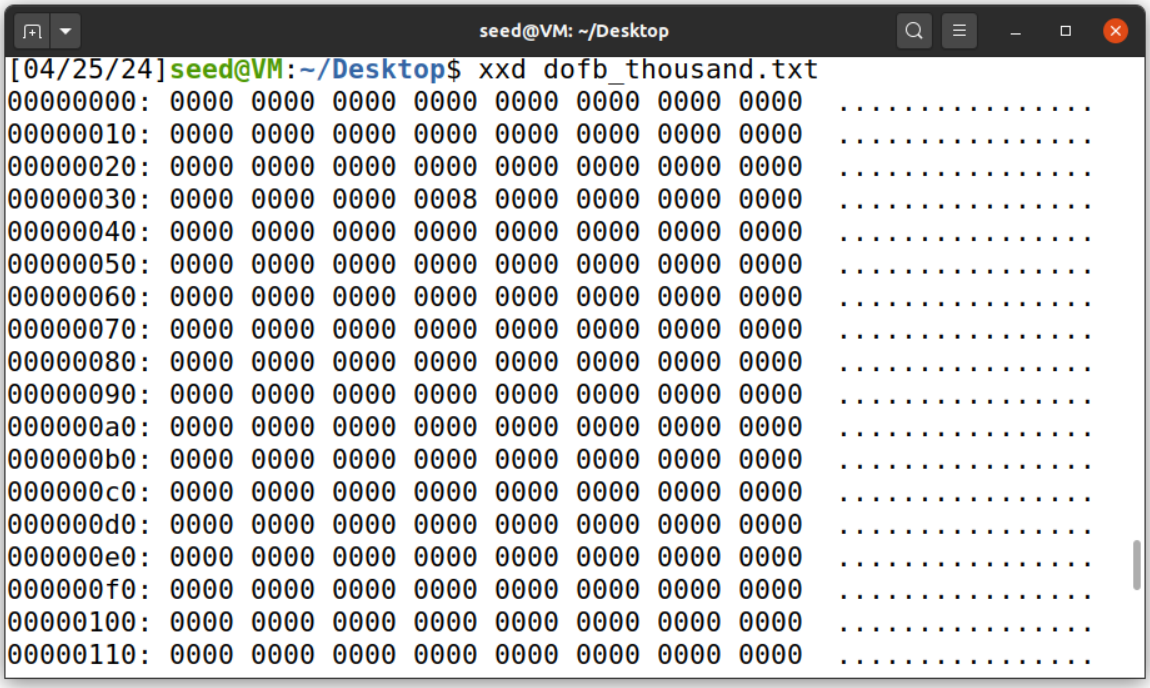
In ECB mode, each block (64 bit) of plaintext is encrypted independently. Therefore, if a single bit in the encrypted file is corrupted, only the corresponding bit in the decrypted plaintext block will be affected. The rest of the decrypted plaintext will remain intact.



In CBC mode, the decryption of each block (64 bit) depends on the previous ciphertext block. If a single bit in the encrypted file is corrupted, it will affect the decryption of the corresponding block and may propagate errors to subsequent blocks due to the chaining effect. This can lead to a larger portion of the decrypted plaintext being corrupted compared to ECB mode.



In CFB mode, the encryption operation is performed on the feedback shift register, and the resulting keystream is XORed with the plaintext to produce the ciphertext. If a single bit in the encrypted file is corrupted, it will only affect the corresponding bit in the keystream, resulting in corruption in the corresponding bit of the decrypted plaintext.

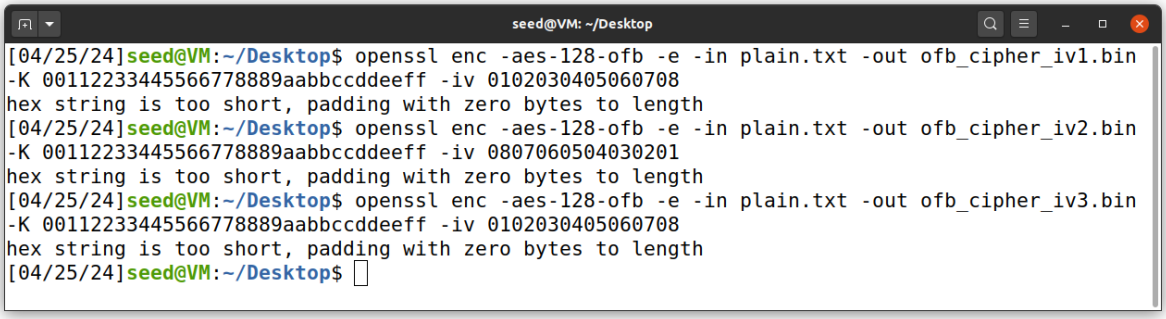


In OFB mode, the encryption operation is similar to CFB mode, where the keystream is generated independently of the plaintext. Therefore, if a single bit in the encrypted file is corrupted, it will only affect the corresponding bit in the keystream and will not propagate errors to subsequent blocks.

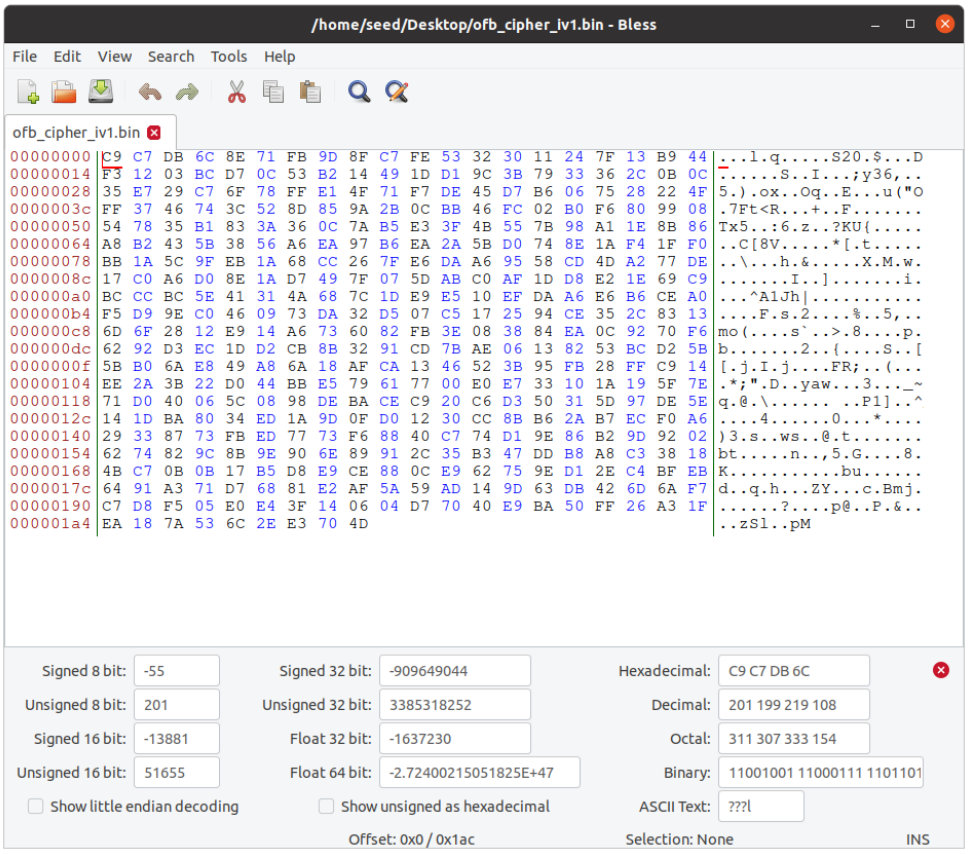
Mode	Different Bytes
ECB	16
CBC	17
CFB	17
OFB	1

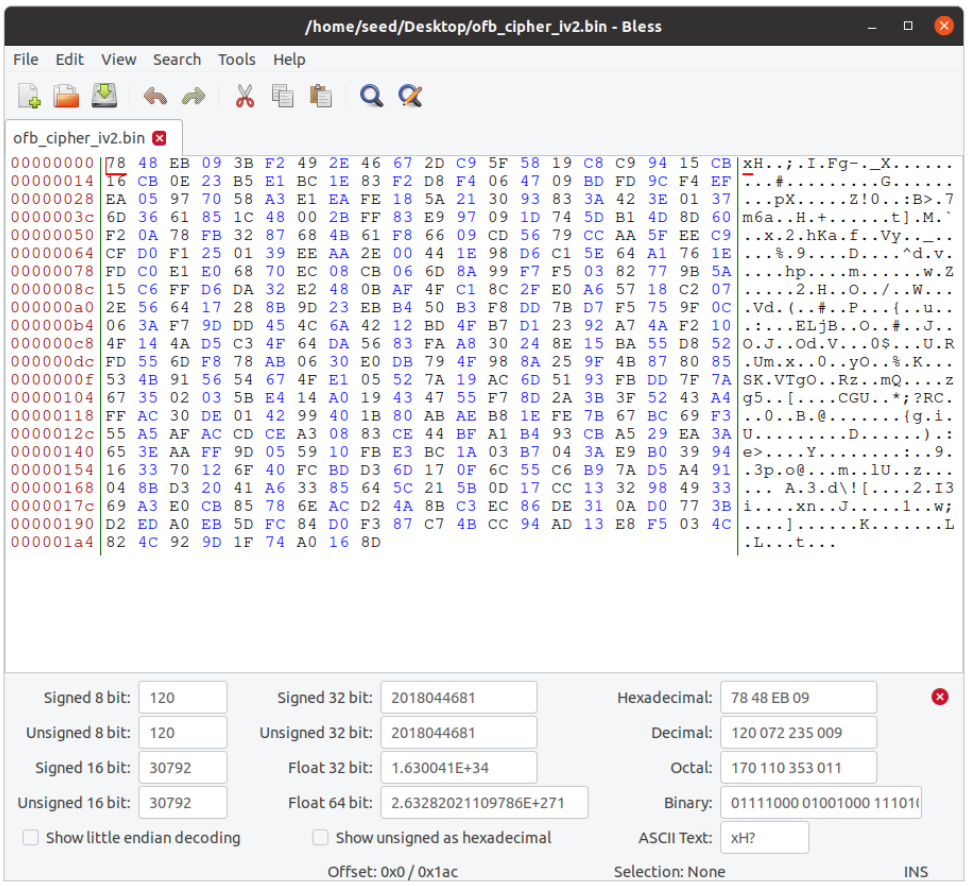
Task 6: Initial Vector (IV) and Common Mistakes

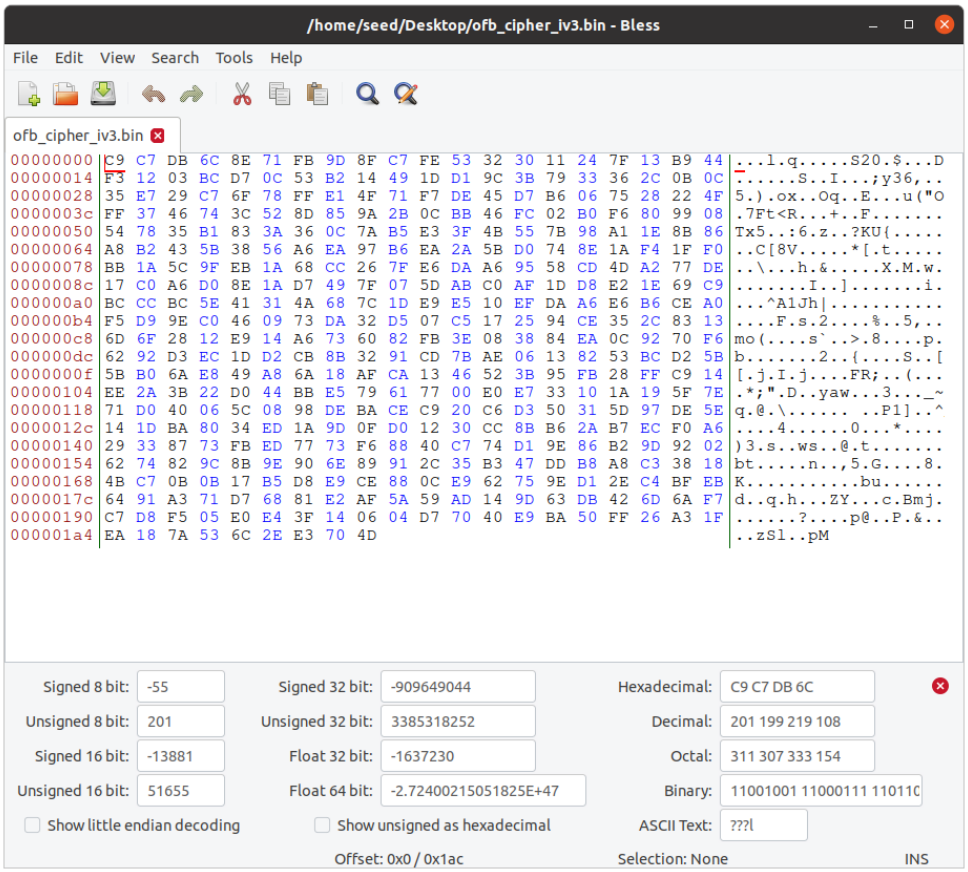
Task 6.1. IV Experiment



iv1 and iv2 different; iv1 and iv3 same.


/home/seed/Desktop/ofb_cipher_iv1.bin - Bless
File Edit View Search Tools Help
ofb_cipher_iv1.bin
00000000 C9 C7 DB 6C 8E 71 FB 9D 8F C7 FE 53 32 30 11 24 7F 13 B9 44 ...l.q.....S20.$...D
00000014 F3 12 03 BC D7 0C 53 B2 14 49 1D D1 9C 3B 79 33 36 2C 0B 0C ......S..I...;y36,..
00000028 35 E7 29 C7 6F 78 FF E1 4F 71 F7 DE 45 D7 B6 06 75 28 22 4F 5.).ox..Oq..E...u("O
0000003c FF 37 46 74 3C 52 8D 85 9A 2B 0C BB 46 FC 02 B0 F6 80 99 08 .7Ft<R...+..F.......
00000050 54 78 35 B1 83 3A 36 0C 7A B5 E3 3F 4B 55 7B 98 A1 1E 8B 86 Tx5..:6.z..?KU{.....
00000064 A8 B2 43 5B 38 56 A6 EA 97 B6 EA 2A 5B D0 74 8E 1A F4 1F F0 ..C[8V.....*[.t.....
00000078 BB 1A 5C 9F EB 1A 68 CC 26 7F E6 DA A6 95 58 CD 4D A2 77 DE ..\...h.&.....X.M.w.
0000008c 17 C0 A6 D0 8E 1A D7 49 7F 07 5D AB C0 AF 1D D8 E2 1E 69 C9 ....I..]........i.
000000a0 BC CC BC 5E 41 31 4A 68 7C 1D E9 E5 10 EF DA A6 E6 B6 CE A0 ...^A1Jh|...........
000000b4 F5 D9 9E C0 46 09 73 DA 32 D5 07 C5 17 25 94 CE 35 2C 83 13 ....F.s.2....%..5,..
000000c8 6D 6F 28 12 E9 14 A6 73 60 82 FB 3E 08 38 84 EA 0C 92 70 F6 mo(....s`..>.8....p.
000000dc 62 92 D3 EC 1D D2 CB 8B 32 91 CD 7B AE 06 13 82 53 BC D2 5B b.......2..{....S..[
0000000f 5B B0 6A E8 49 A8 6A 18 AF CA 13 46 52 3B 95 FB 28 FF C9 14 [.j.I.j....FR;..(...
00000104 EE 2A 3B 22 D0 44 BB E5 79 61 77 00 E0 E7 33 10 1A 19 5F 7E .*;".D..yaw...3..._~
00000118 71 D0 40 06 5C 08 98 DE BA CE C9 20 C6 D3 50 31 5D 97 DE 5E q.@.\...... ..P1]..^
0000012c 14 1D BA 80 34 ED 1A 9D 0F D0 12 30 CC 8B B6 2A B7 EC F0 A6 ....4......0...*....
00000140 29 33 87 73 FB ED 77 73 F6 88 40 C7 74 D1 9E 86 B2 9D 92 02)3.s..ws..@.t.......
00000154 62 74 82 9C 8B 9E 90 6E 89 91 2C 35 B3 47 DD B8 A8 C3 38 18 bt.....n..,5.G....8.
00000168 4B C7 0B 0B 17 B5 D8 E9 CE 88 0C E9 62 75 9E D1 2E C4 BF EB K...........bu......
0000017c 64 91 A3 71 D7 68 81 E2 AF 5A 59 AD 14 9D 63 DB 42 6D 6A F7 d..q.h...ZY...c.Bmj.
00000190 C7 D8 F5 05 E0 E4 3F 14 06 04 D7 70 40 E9 BA 50 FF 26 A3 1F ......?....p@..P.&..
000001a4 EA 18 7A 53 6C 2E E3 70 4D ..zSl..pM
Signed 8 bit: -55
Signed 32 bit: -909649044
Hexadecimal: C9 C7 DB 6C
Unsigned 8 bit: 201
Unsigned 32 bit: 3385318252
Decimal: 201 199 219 108
Signed 16 bit: -13881
Float 32 bit: -1637230
Octal: 311 307 333 154
Unsigned 16 bit: 51655
Float 64 bit: -2.72400215051825E+47
Binary: 11001001 11000111 1101101
Show little endian decoding
Show unsigned as hexadecimal
ASCII Text: ???l
Offset: 0x0 / 0x1ac
Selection: None
INS


/home/seed/Desktop/ofb_cipher_iv2.bin - Bless
File Edit View Search Tools Help
ofb_cipher_iv2.bin
00000000 78 48 EB 09 3B F2 49 2E 46 67 2D C9 5F 58 19 C8 C9 94 15 CB xH..;.I.Fg-._X......
00000014 16 CB 0E 23 B5 E1 BC 1E 83 F2 D8 F4 06 47 09 BD FD 9C F4 EF ...#.........G......
00000028 EA 05 97 70 58 A3 E1 EA FE 18 5A 21 30 93 83 3A 42 3E 01 37 ...pX.....Z!0..:B>.7
0000003c 6D 36 61 85 1C 48 00 2B FF 83 E9 97 09 1D 74 5D B1 4D 8D 60 m6a..H.+......t].M.`
00000050 F2 0A 78 FB 32 87 68 4B 61 F8 66 09 CD 56 79 CC AA 5F EE C9 ..x.2.hKa.f..Vy..._..
00000064 CF D0 F1 25 01 39 EE AA 2E 00 44 1E 98 D6 C1 5E 64 A1 76 1E ...%.9....D....^d.v.
00000078 FD C0 E1 E0 68 70 EC 08 CB 06 6D 8A 99 F7 F5 03 82 77 9B 5A ....hp....m......w.Z
0000008c 15 C6 FF D6 DA 32 E2 48 0B AF 4F C1 8C 2F E0 A6 57 18 C2 07 .....2.H..O../..W...
000000a0 2E 56 64 17 28 8B 9D 23 EB B4 50 B3 F8 DD 7B D7 F5 75 9F 0C .Vd.(..#..P...{..u..
000000b4 06 3A F7 9D DD 45 4C 6A 42 12 BD 4F B7 D1 23 92 A7 4A F2 10 .:...ELjB..O..#..J..
000000c8 4F 14 4A D5 C3 4F 64 DA 56 83 FA A8 30 24 8E 15 BA 55 D8 52 O.J..Od.V...0$...U.R
000000dc FD 55 6D F8 78 AB 06 30 E0 DB 79 4F 98 8A 25 9F 4B 87 80 85 .Um.x..0..yO..%.K...
0000000f 53 4B 91 56 54 67 4F E1 05 52 7A 19 AC 6D 51 93 FB DD 7F 7A SK.VTgO..Rz..mQ....z
00000104 67 35 02 03 5B E4 14 A0 19 43 47 55 F7 8D 2A 3B 3F 52 43 A4 g5..[....CGU..*;?RC.
00000118 FF AC 30 DE 01 42 99 40 1B 80 AB AE B8 1E FE 7B 67 BC 69 F3 ..0..B.@.......{g.i.
0000012c 55 A5 AF AC CD CE A3 08 83 CE 44 BF A1 B4 93 CB A5 29 EA 3A U.........D......):
00000140 65 3E AA FF 9D 05 59 10 FB E3 BC 1A 03 B7 04 3A E9 B0 39 94 e>....Y........:..9.
00000154 16 33 70 12 6F 40 FC BD D3 6D 17 0F 6C 55 C6 B9 7A D5 A4 91 .3p.o@...m..lU..z...
00000168 04 8B D3 20 41 A6 33 85 64 5C 21 5B 0D 17 CC 13 32 98 49 33 ... A.3.d\![....2.I3
0000017c 69 A3 E0 CB 85 78 6E AC D2 4A 8B C3 EC 86 DE 31 0A D0 77 3B i....xn..J.....1..w;
00000190 D2 ED A0 EB 5D FC 84 D0 F3 87 C7 4B CC 94 AD 13 E8 F5 03 4C ....]......K.......L
000001a4 82 4C 92 9D 1F 74 A0 16 8D .L...t...
Signed 8 bit: 120
Signed 32 bit: 2018044681
Hexadecimal: 78 48 EB 09
Unsigned 8 bit: 120
Unsigned 32 bit: 2018044681
Decimal: 120 072 235 009
Signed 16 bit: 30792
Float 32 bit: 1.630041E+34
Octal: 170 110 353 011
Unsigned 16 bit: 30792
Float 64 bit: 2.63282021109786E+271
Binary: 01111000 01001000 111010
Show little endian decoding
Show unsigned as hexadecimal
ASCII Text: xH?
Offset: 0x0 / 0x1ac
Selection: None
INS

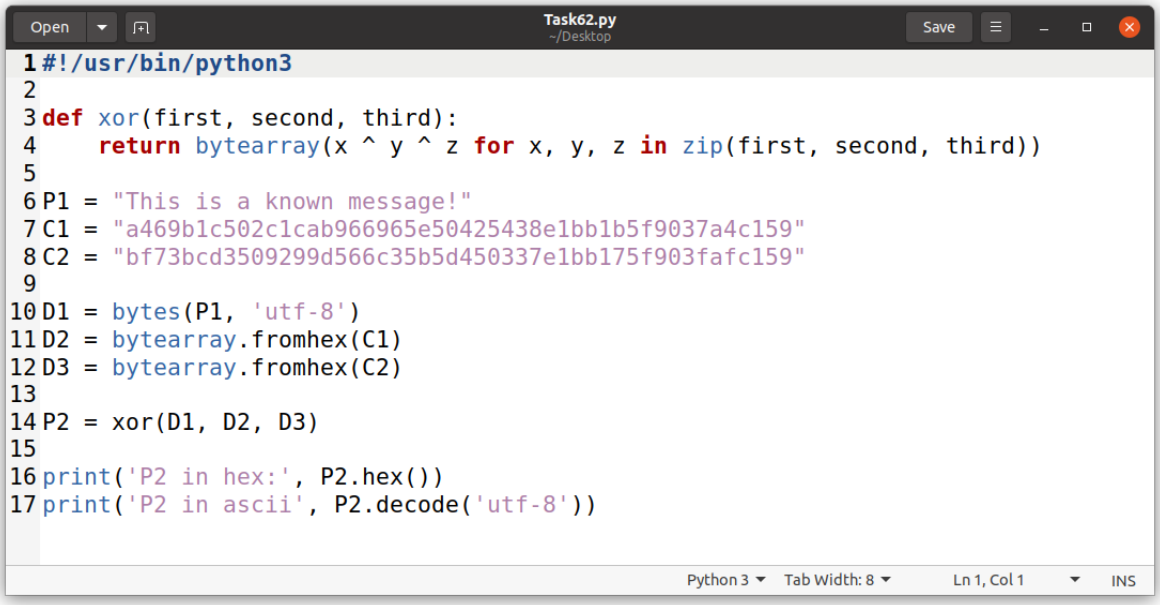


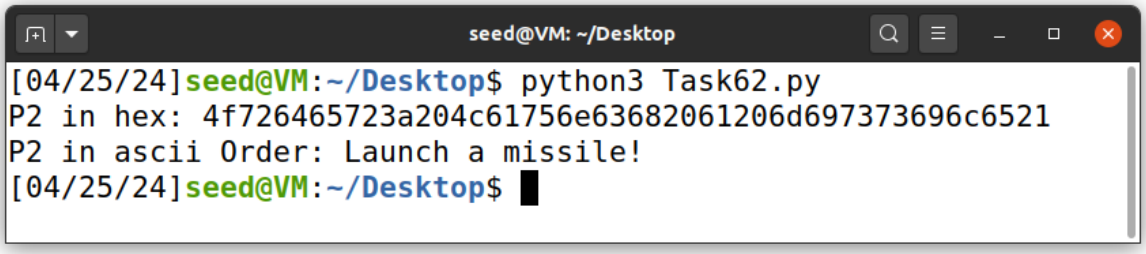
When plaintexts and keys are the same, using the same IV leads to the same ciphertexts.

Task 6.2. Common Mistake: Use the Same IV

Output stream = P1 XOR C1; P2 = output stream XOR C2

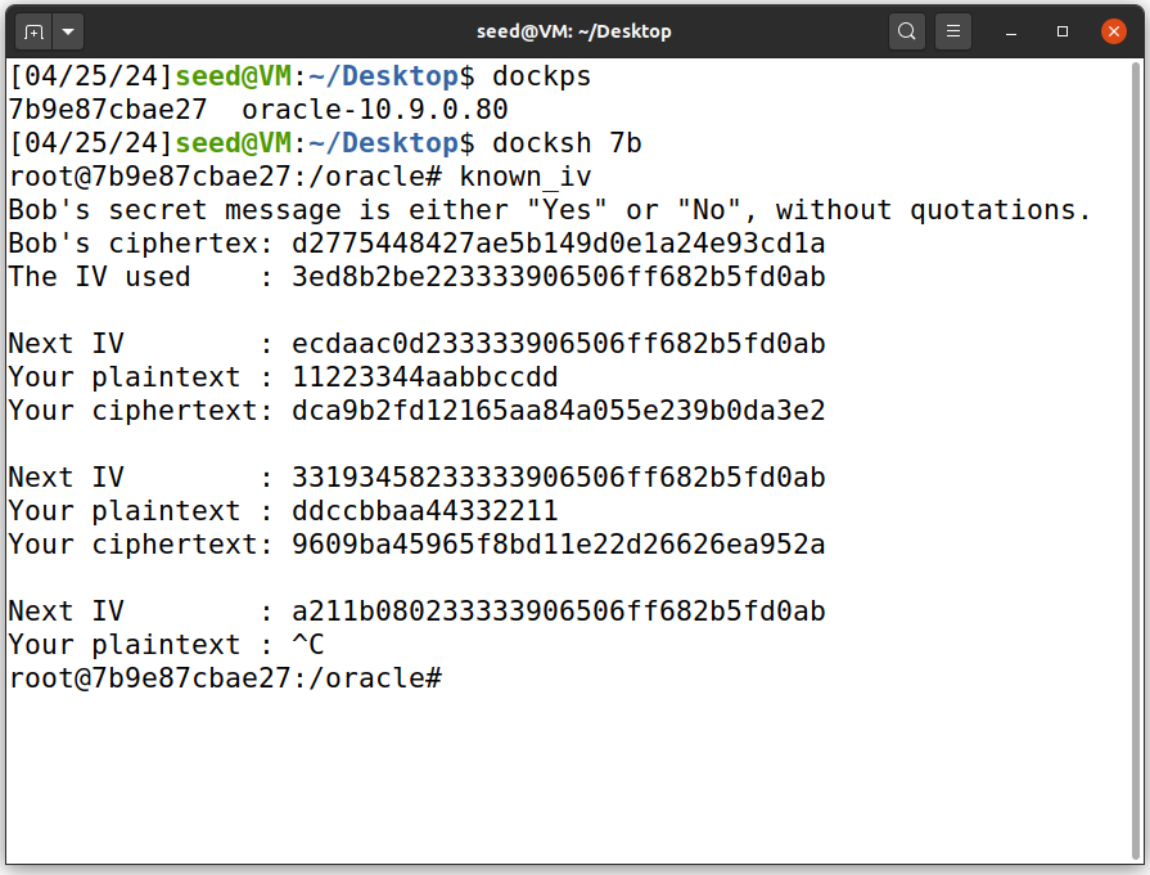
Hence, P2 = P1 XOR C1 XOR C2





For CFB mode, it depends on the length of IV, content (ciphertext) longer than the length of IV will not be able to be decrypted normally. As we know that a plaintext attack can get IV through XOR but cannot get the key value, then with CFB encryption, the attacker will not be able to calculate the output stream before solving the key, hence, the following content cannot be decrypted. On the contrary, attacking OFB after knowing the plaintext, without getting the key value, we can obtain a output stream with a length equivalent to the plaintext, and as long as the key and IV remain unchanged, it can attack any ciphertext whose length is not greater than the known plaintext length.

Task 6.3. Common Mistake: Use a Predictable IV



Task 7: Programming using the Crypto Library

Task7.py
~/Desktop

```python
#!/usr/bin/python3

from Crypto.Cipher import AES
from Crypto.Util.Padding import pad

P = b"This is a top secret."
C = bytes.fromhex("764aa26b55a4da654df6b19e4bce00f4ed05e09346fb0e762583cb7da2ac93a2")
IV = bytes.fromhex("aabbccddeeff00998877665544332211")

assert len(P) == 21

with open('words.txt') as file:
    keys = [line.strip().encode('utf-8') for line in file]

padded_P = pad(P, 16)

for k in keys:
    if len(k) <= 16:
        key = k.ljust(16, b'#')
        cipher = AES.new(key=key, mode=AES.MODE_CBC, iv=IV)
        guess = cipher.encrypt(padded_P)
        if guess == C:
            print("Key found:", key.decode('utf-8'))
            exit(0)

print("Key not found.")
```

Python 3 Tab Width: 8 Ln 1, Col 1 INS

seed@VM: ~/Desktop

```
[04/25/24]seed@VM:~/Desktop$ python3 Task7.py
Key found: Syracuse########
[04/25/24]seed@VM:~/Desktop$
```