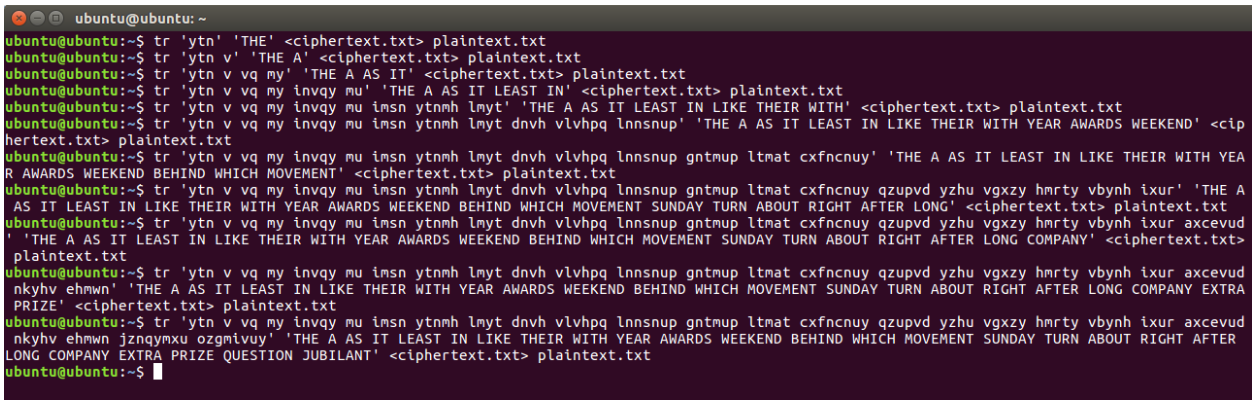
LAB 2

Course name: ***Cryptography*** *- Class code:* ***NT219.L21.ANTT.1***
Lecturer: ***Van Thien Luan***

Team's info and task allocation *(actual workload per each member)*	**Team member 1** Student's ID: 19520506 Full name: Nguyễn Thị Hải Hà Task allocation: 2,3,4,5,6.1 **Team member 2** Student's ID: 19520499 Full name: Lê Thị Hương Giang Task allocation: 1, 6.2

Task 1:

- Dựa theo tần số 1 chữ cái xuất hiện, từ 2 chữ xuất hiện và từ 3 chữ xuất hiện nhiều nhất, ta thay dần như sau:



- Kết quả:


```
THE OSCARS TURN  ON SUNDAY WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE
AWARDS TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO

THE AWARDS RACE WAS BOOKENDED BY THE DEMISE OF HARVEY WEINSTEIN AT ITS OUTSET
AND THE APPARENT IMPLOSION OF HIS FILM COMPANY AT THE END AND IT WAS SHAPED BY
THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVISM AND
A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE
OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT JUST SEEM EXTRA LONG IT WAS
EXTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MARCH TO
AVOID CONFLICTING WITH THE CLOSING CEREMONY OF THE WINTER OLYMPICS THANKS
PYEONGCHANG

ONE BIG QUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE
CEREMONY WILL ADDRESS METOO ESPECIALLY AFTER THE GOLDEN GLOBES WHICH BECAME
A JUBILANT COMINGOUT PARTY FOR TIMES UP THE MOVEMENT SPEARHEADED BY
POWERFUL HOLLYWOOD WOMEN WHO HELPED RAISE MILLIONS OF DOLLARS TO FIGHT SEXUAL
HARASSMENT AROUND THE COUNTRY

SIGNALING THEIR SUPPORT GOLDEN GLOBES ATTENDEES SWATHED THEMSELVES IN BLACK
SPORTED LAPEL PINS AND SOUNDED OFF ABOUT SEXIST POWER IMBALANCES FROM THE RED
CARPET AND THE STAGE ON THE AIR E WAS CALLED OUT ABOUT PAY INEQUITY AFTER
ITS FORMER ANCHOR CATT SADLER QUIT ONCE SHE LEARNED THAT SHE WAS MAKING FAR
LESS THAN A MALE COHOST AND DURING THE CEREMONY NATALIE PORTMAN TOOK A BLUNT
AND SATISFYING DIG AT THE ALLMALE ROSTER OF NOMINATED DIRECTORS HOW COULD
THAT BE TOPPED

AS IT TURNS OUT AT LEAST IN TERMS OF THE OSCARS IT PROBABLY WONT BE

WOMEN INVOLVED IN TIMES UP SAID THAT ALTHOUGH THE GLOBES SIGNIFIED THE
INITIATIVES LAUNCH THEY NEVER INTENDED IT TO BE JUST AN AWARDS SEASON
CAMPAIGN OR ONE THAT BECAME ASSOCIATED ONLY WITH REDCARPET ACTIONS INSTEAD
A SPOKESWOMAN SAID THE GROUP IS WORKING BEHIND CLOSED DOORS AND HAS SINCE
AMASSED  MILLION FOR ITS LEGAL DEFENSE FUND WHICH AFTER THE GLOBES WAS
FLOODED WITH THOUSANDS OF DONATIONS OF  OR LESS FROM PEOPLE IN SOME
COUNTRIES


NO CALL TO WEAR BLACK GOWNS WENT OUT IN ADVANCE OF THE OSCARS THOUGH THE
MOVEMENT WILL ALMOST CERTAINLY BE REFERENCED BEFORE AND DURING THE CEREMONY
ESPECIALLY SINCE VOCAL METOO SUPPORTERS LIKE ASHLEY JUDD LAURA DERN AND
NICOLE KIDMAN ARE SCHEDULED PRESENTERS

ANOTHER FEATURE OF THIS SEASON NO ONE REALLY KNOWS WHO IS GOING TO WIN BEST
PICTURE ARGUABLY THIS HAPPENS A LOT OF THE TIME INARGUABLY THE NAILBITER
NARRATIVE ONLY SERVES THE AWARDS HYPE MACHINE BUT OFTEN THE PEOPLE FORECASTING
THE RACE SOCALLED OSCAROLOGISTS CAN MAKE ONLY EDUCATED GUESSES
```

NO CALL TO WEAR BLACK GOWNS WENT OUT IN ADVANCE OF THE OSCARS THOUGH THE MOVEMENT WILL ALMOST CERTAINLY BE REFERENCED BEFORE AND DURING THE CEREMONY ESPECIALLY SINCE VOCAL METOO SUPPORTERS LIKE ASHLEY JUDD LAURA DERN AND NICOLE KIDMAN ARE SCHEDULED PRESENTERS

ANOTHER FEATURE OF THIS SEASON NO ONE REALLY KNOWS WHO IS GOING TO WIN BEST PICTURE ARGUABLY THIS HAPPENS A LOT OF THE TIME INARGUABLY THE NAILBITER NARRATIVE ONLY SERVES THE AWARDS HYPE MACHINE BUT OFTEN THE PEOPLE FORECASTING THE RACE SOCALLED OSCAROLOGISTS CAN MAKE ONLY EDUCATED GUESSES

THE WAY THE ACADEMY TABULATES THE BIG WINNER DOESNT HELP IN EVERY OTHER CATEGORY THE NOMINEE WITH THE MOST VOTES WINS BUT IN THE BEST PICTURE CATEGORY VOTERS ARE ASKED TO LIST THEIR TOP MOVIES IN PREFERENTIAL ORDER IF A MOVIE GETS MORE THAN PERCENT OF THE FIRSTPLACE VOTES IT WINS WHEN NO MOVIE MANAGES THAT THE ONE WITH THE FEWEST FIRSTPLACE VOTES IS ELIMINATED AND ITS VOTES ARE REDISTRIBUTED TO THE MOVIES THAT GARNERED THE ELIMINATED BALLOTS SECONDPLACE VOTES AND THIS CONTINUES UNTIL A WINNER EMERGES

IT IS ALL TERRIBLY CONFUSING BUT APPARENTLY THE CONSENSUS FAVORITE COMES OUT AHEAD IN THE END THIS MEANS THAT ENDOFSEASON AWARDS CHATTER INVARIABLY INVOLVES TORTURED SPECULATION ABOUT WHICH FILM WOULD MOST LIKELY BE VOTERS SECOND OR THIRD FAVORITE AND THEN EQUALLY TORTURED CONCLUSIONS ABOUT WHICH FILM MIGHT PREVAIL

IN IT WAS A TOSSUP BETWEEN BOYHOOD AND THE EVENTUAL WINNER BIRDMAN
IN WITH LOTS OF EXPERTS BETTING ON THE REVENANT OR THE BIG SHORT THE PRIZE WENT TO SPOTLIGHT LAST YEAR NEARLY ALL THE FORECASTERS DECLARED LA LA LAND THE PRESUMPTIVE WINNER AND FOR TWO AND A HALF MINUTES THEY WERE CORRECT BEFORE AN ENVELOPE SNAFU WAS REVEALED AND THE RIGHTFUL WINNER MOONLIGHT WAS CROWNED

THIS YEAR AWARDS WATCHERS ARE UNEQUALLY DIVIDED BETWEEN THREE BILLBOARDS OUTSIDE EBBING MISSOURI THE FAVORITE AND THE SHAPE OF WATER WHICH IS THE BAGGERS PREDICTION WITH A FEW FORECASTING A HAIL MARY WIN FOR GET OUT

BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE SHAPE OF WATER HAS NOMINATIONS MORE THAN ANY OTHER FILM AND WAS ALSO NAMED THE YEARS BEST BY THE PRODUCERS AND DIRECTORS GUILDS YET IT WAS NOT NOMINATED FOR A SCREEN ACTORS GUILD AWARD FOR BEST ENSEMBLE AND NO FILM HAS WON BEST PICTURE WITHOUT PREVIOUSLY LANDING AT LEAST THE ACTORS NOMINATION SINCE BRAVEHEART IN THIS YEAR THE BEST ENSEMBLE SAG ENDED UP GOING TO THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE ACTORS MAKE UP THE ACADEMYS LARGEST BRANCH THAT FILM WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST DIRECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN

Task 2: Encryption using Different Ciphers and Modes

- Mã hóa file bằng 3 mode khác nhau

```
┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -e -in plaintext6-1.txt -out cbc2.bin -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff

┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cfb -e -in plaintext6-1.txt -out cfb.bin -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff

┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-ecb -e -in plaintext6-1.txt -out ecb2.bin -K 00112233445566778889aabbccddeeff
```

Task 3:Encryption Mode – ECB vs. CBC

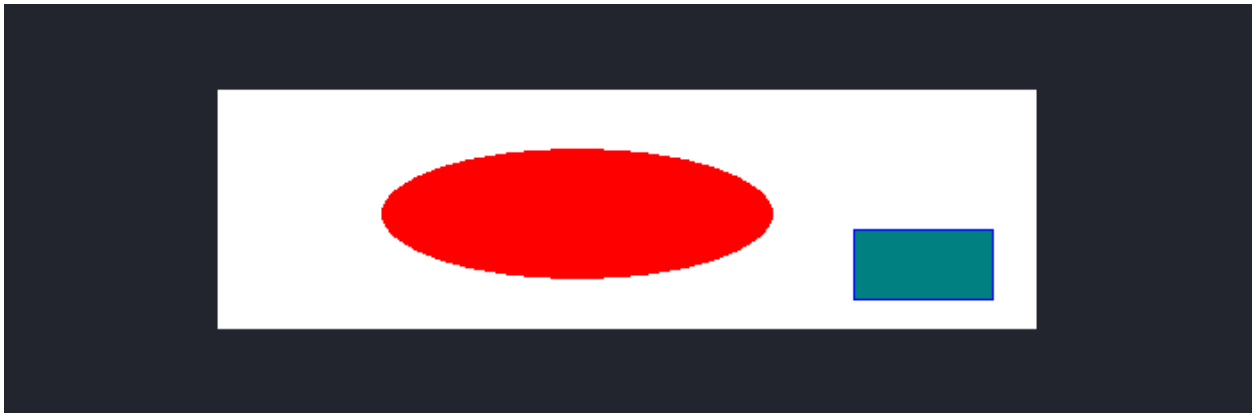


Figure 1: Pic_original.bmp

- Mã hóa file hình ảnh pic_original.bmp bằng aes-128-cbc, sau đó ghép header của file gốc với tail của file đã được mã hóa thành một hình ảnh.

```
┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -e -in pic_original.bmp -out cbc4.bmp  -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff

┌──(haha㉿haha)-[~]
└─$ head -c 54 pic_original.bmp >header

┌──(haha㉿haha)-[~]
└─$ tail -c +55 cbc4.bmp >body

┌──(haha㉿haha)-[~]
└─$ cat header body >cbc4.bmp
```

- Mở file hình ảnh vừa mới được ghép lên

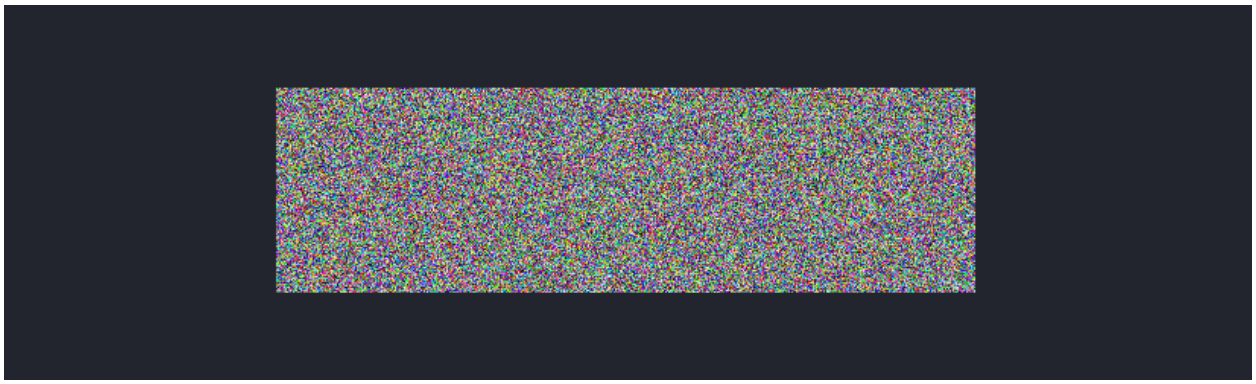


Figure 2: Hình ảnh được mã hóa bởi mode CBC

- Mã hóa file hình ảnh pic_original.bmp bằng mode ECB, và ghép thành hình ảnh

```
┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-ecb -e -in pic_original.bmp -out ecb4.bmp  -K 00112233445566778889aabbccddeeff

┌──(haha㉿haha)-[~]
└─$ head -c 54 pic_original.bmp >header

┌──(haha㉿haha)-[~]
└─$ tail -c +55 ecb4.bmp >body

┌──(haha㉿haha)-[~]
└─$ cat header body >ecb4.bmp
```

- Mở file hình ảnh được mã hóa bởi ECB

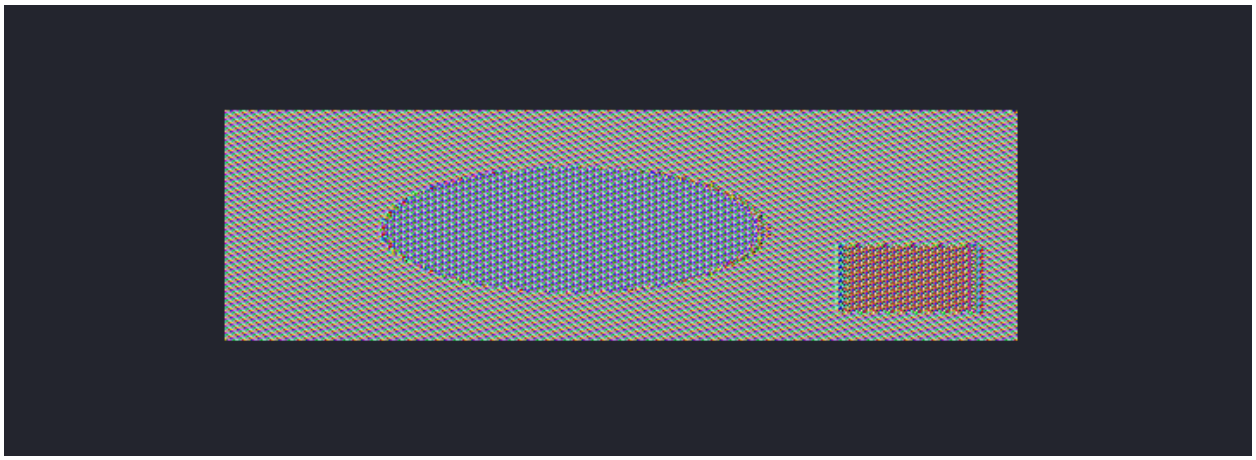


Figure 3: Hình ảnh được mã hóa bởi mode ECB

- Chọn một hình ảnh bất kỳ và mã hóa với hai mode ECB, CBC để so sánh

Figure 4: Ảnh gốc trước khi được mã hóa

- Mã hóa hình ảnh bằng mode ECB

```
┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-ecb -e -in basic.bmp -out ecb4-1.bmp  -K 00112233445566778889aabbccddeeff

┌──(haha㉿haha)-[~]
└─$ head -c 54 basic.bmp >header

┌──(haha㉿haha)-[~]
└─$ tail -c +55 ecb4-1.bmp >body

┌──(haha㉿haha)-[~]
└─$ cat header body >ecb4-1.bmp
```

- Mở hình ảnh được mã hóa

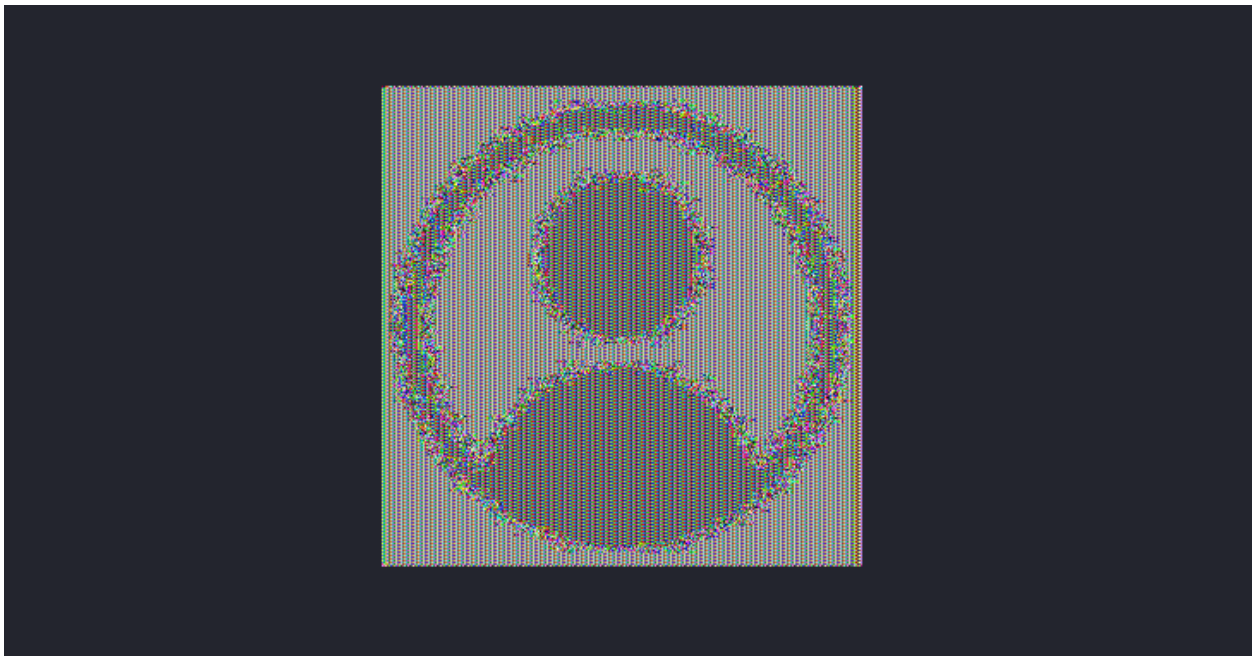


Figure 5: Hình ảnh được mã hóa bởi mode ECB

- Mã hóa hình ảnh bằng CBC

```
┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -e -in basic.bmp -out cbc4-1.bmp  -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff

┌──(haha㉿haha)-[~]
└─$ head -c 54 basic.bmp >header

┌──(haha㉿haha)-[~]
└─$ tail -c +55 cbc4-1.bmp >body

┌──(haha㉿haha)-[~]
└─$ cat header body >cbc4-1.bmp
```

- Mở hình ảnh được mã hóa:

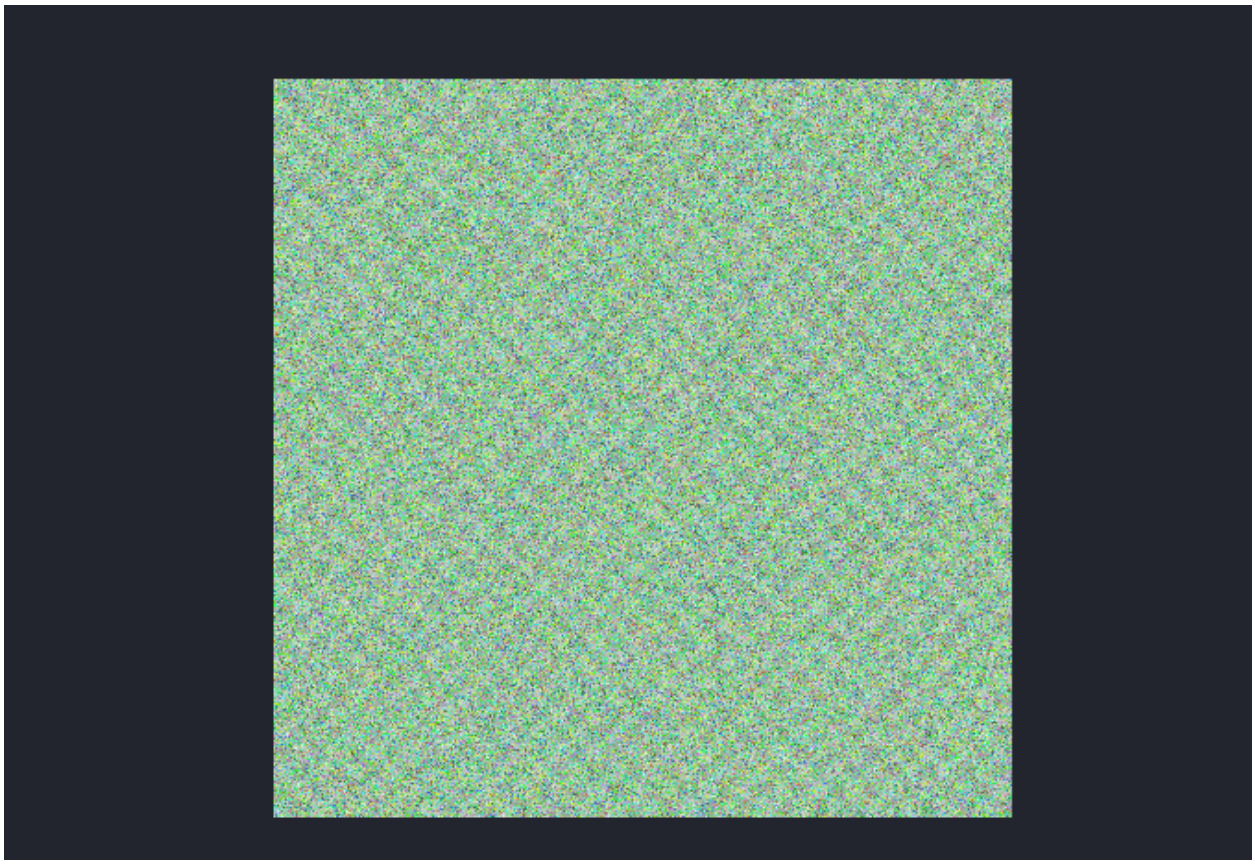


Figure 6: Hình ảnh được mã hóa bởi mode CBC

Task 4: Padding

- Tạo ba file có size lần lượt là 5, 10, 15 bytes

```
┌──(haha㉿haha)-[~]
└─$ echo -n "12345" > f1.txt

┌──(haha㉿haha)-[~]
└─$ echo -n "1234567890" > f2.txt

┌──(haha㉿haha)-[~]
└─$ echo -n "123456789012345" > f3.txt
```

- Sau đó encrypt các file bằng aes-128-cbc với khóa K và IV tự tạo

```
┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -e -in f1.txt -out 4-f1.bin -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff

┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -e -in f2.txt -out 4-f2.bin -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff

┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -e -in f3.txt -out 4-f3.bin -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff
```

- Tiếp theo, decrypt các file đã mã hóa ở trên trở về plaintext, sử dụng các câu lệnh sau để xem padding được thêm vào của mỗi file sau khi giải mã.

```
┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -d -in 4-f3.bin -out 4-f3.txt  -K 00112233445566
778889aabbccddeeff -iv 01020304050607088889aabbccddeeff -nopad

┌──(haha㉿haha)-[~]
└─$ hexdump -C 4-f3.txt
00000000  31 32 33 34 35 36 37 38  39 30 31 32 33 34 35 01  |123456789012345.|
|
00000010

┌──(haha㉿haha)-[~]
└─$ xxd 4-f3.txt
00000000: 3132 3334 3536 3738 3930 3132 3334 3501  123456789012345.

┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -d -in 4-f2.bin -out 4-f2.txt  -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff -nopad

┌──(haha㉿haha)-[~]
└─$ hexdump -C 4-f2.txt
00000000  31 32 33 34 35 36 37 38  39 30 06 06 06 06 06 06  |1234567890......|
00000010

┌──(haha㉿haha)-[~]
└─$ xxd 4-f2.txt
00000000: 3132 3334 3536 3738 3930 0606 0606 0606  1234567890......

┌──(haha㉿haha)-[~]
└─$ openssl enc -aes-128-cbc -d -in 4-f1.bin -out 4-f1.txt  -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff -nopad

┌──(haha㉿haha)-[~]
└─$ hexdump -C 4-f1.txt
00000000  31 32 33 34 35 0b 0b 0b  0b 0b 0b 0b 0b 0b 0b 0b  |12345...........|
00000010

┌──(haha㉿haha)-[~]
└─$ xxd 4-f1.txt
00000000: 3132 3334 350b 0b0b 0b0b 0b0b 0b0b 0b0b  12345...........
```

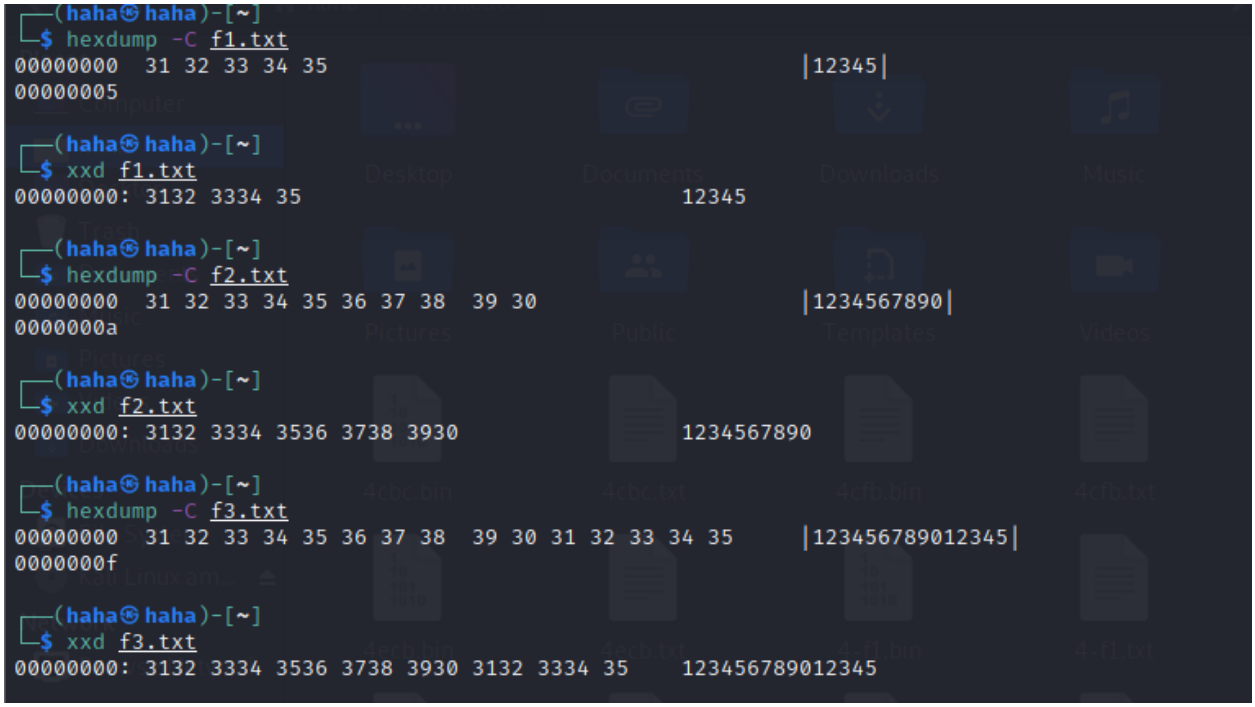


Figure 7: Nội dung file gốc trước khi được mã hóa

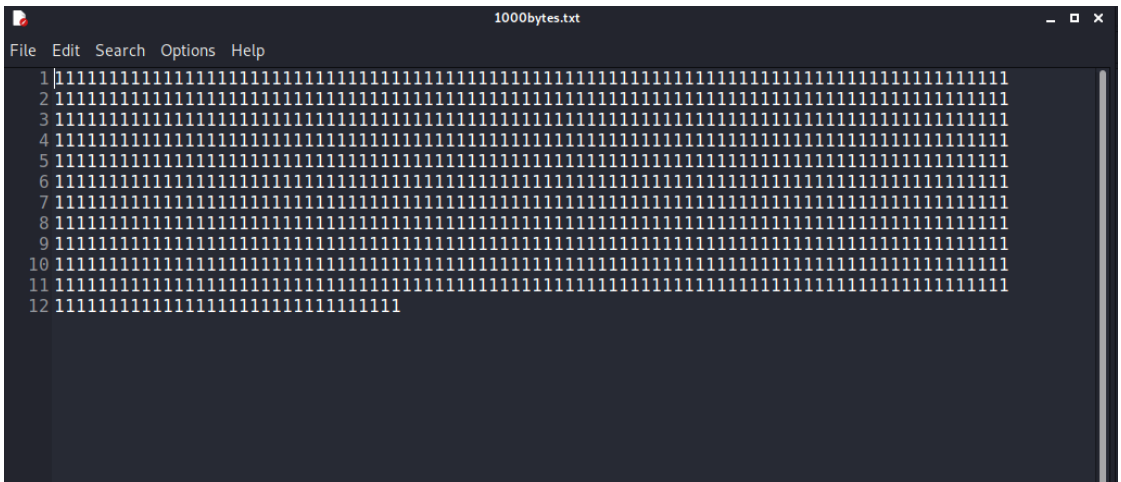
Task 5: Error Propagation – Corrupted Cipher Text

Câu hỏi: Số thông tin có thể tim được khi giải mã file đã được sửa khi sử dụng các mode ECB, CBC, CFB, OFB?

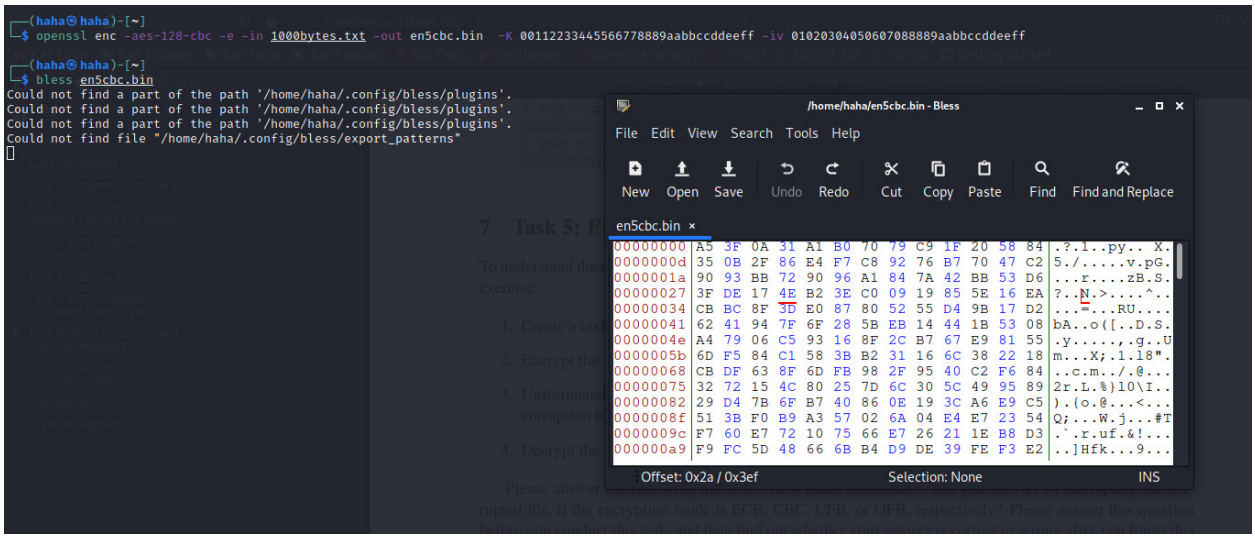
Trả lời: Với mode

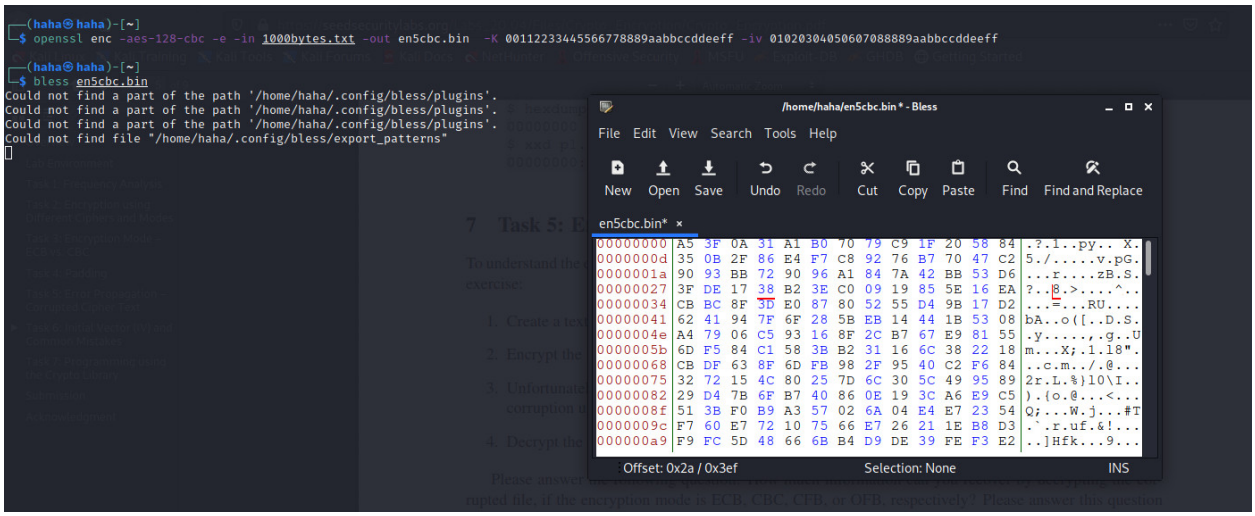
+ ECB, OFB : thì ta sẽ tìm được tất cả các byte trừ byte đã bị sửa.
+ CBC, CFB: thì số byte từ byte bị sửa trở đi sẽ bị sai toàn bộ

- Đầu tiên, tạo một file chứa 1000 bytes tên là 1000bytes.txt

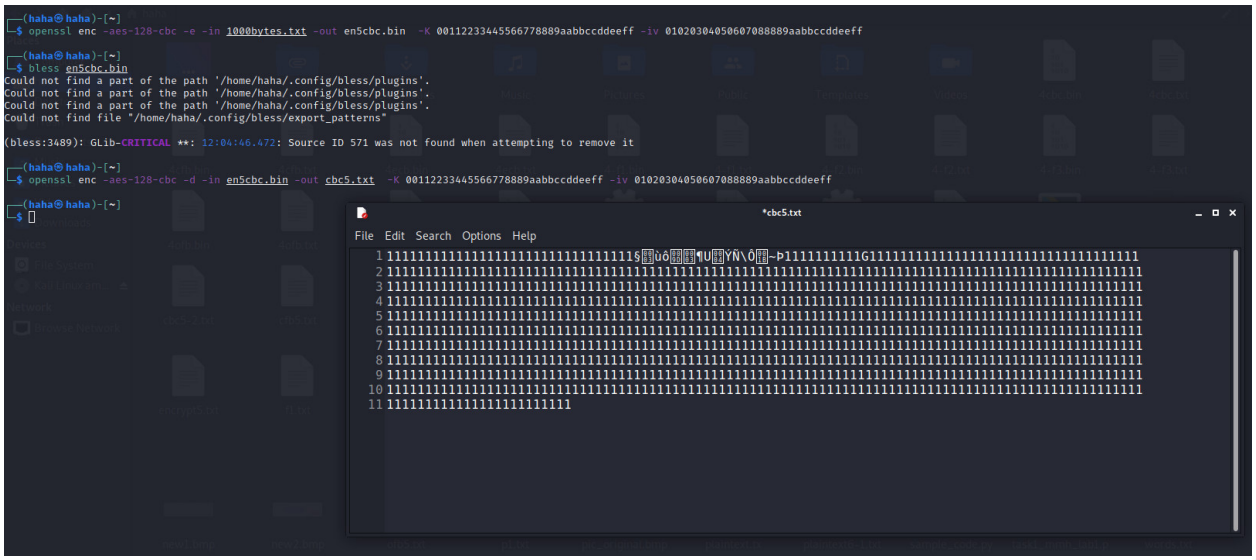


- Tiếp theo, encrypt file 1000bytes.txt bằng aes-128-cbc, sau đó sử dụng bless editor để sửa byte thứ 55 trong file đã được encrypt tên là en5cbc.bin

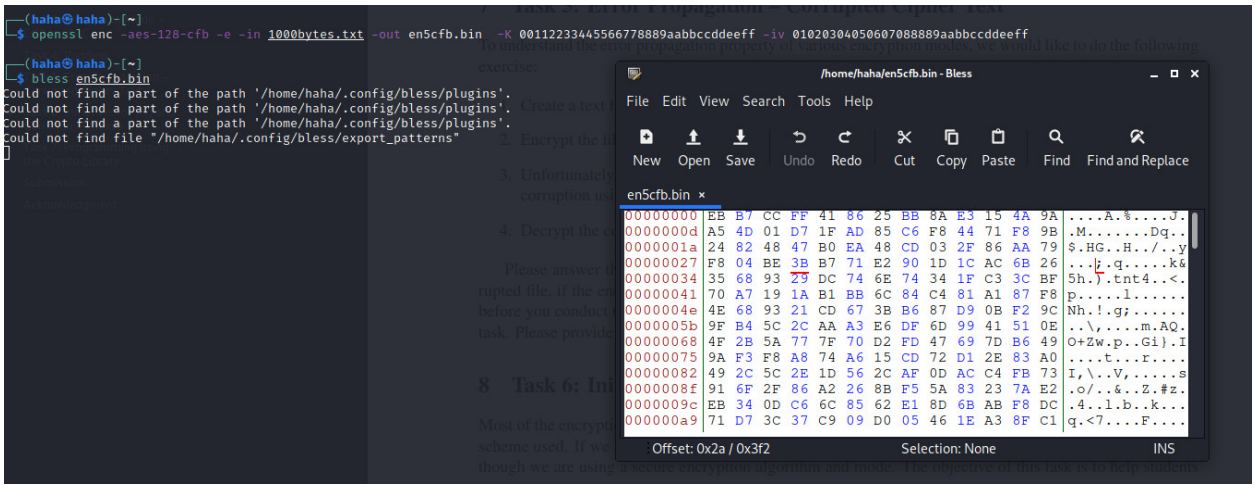


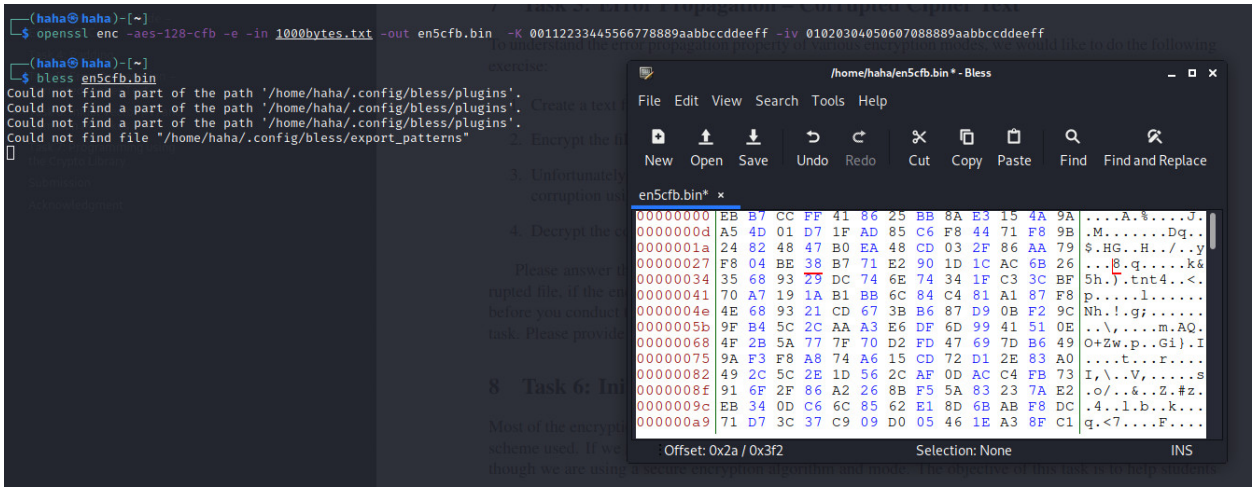


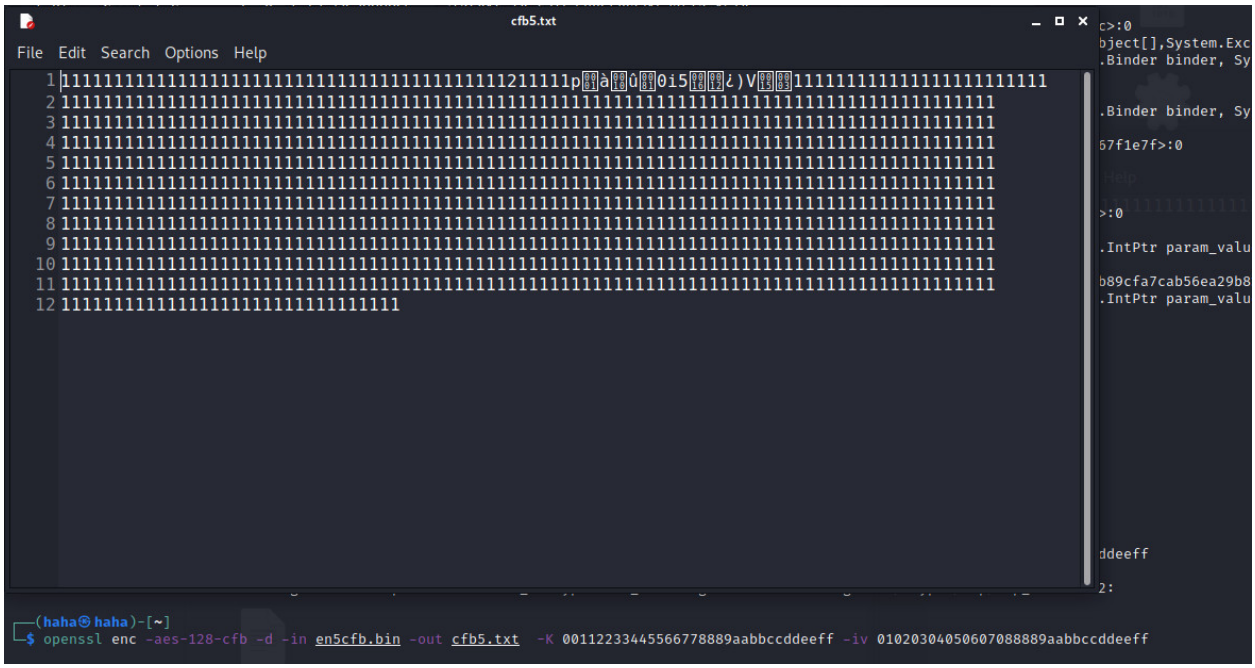
- Cuối cùng, decrypt file encrypt đã được chỉnh sửa và mở ra xem, so sánh với plaintext ban đầu là file 1000bytes.txt thì thấy được có một số byte bị sai.



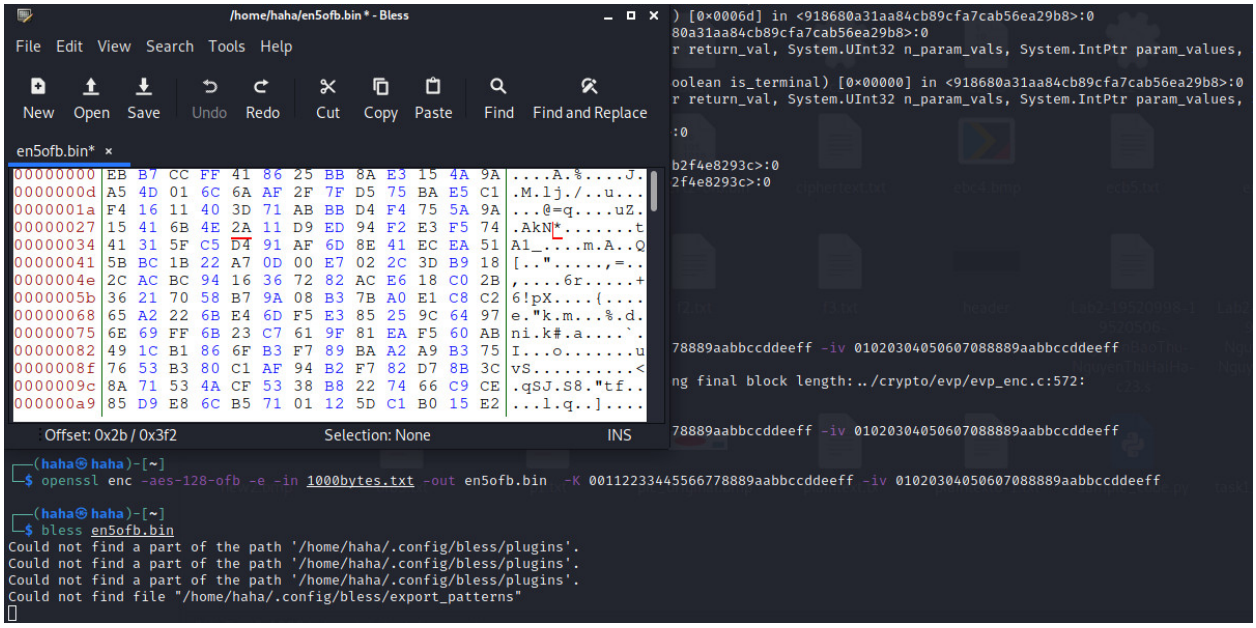
- Với CFB:

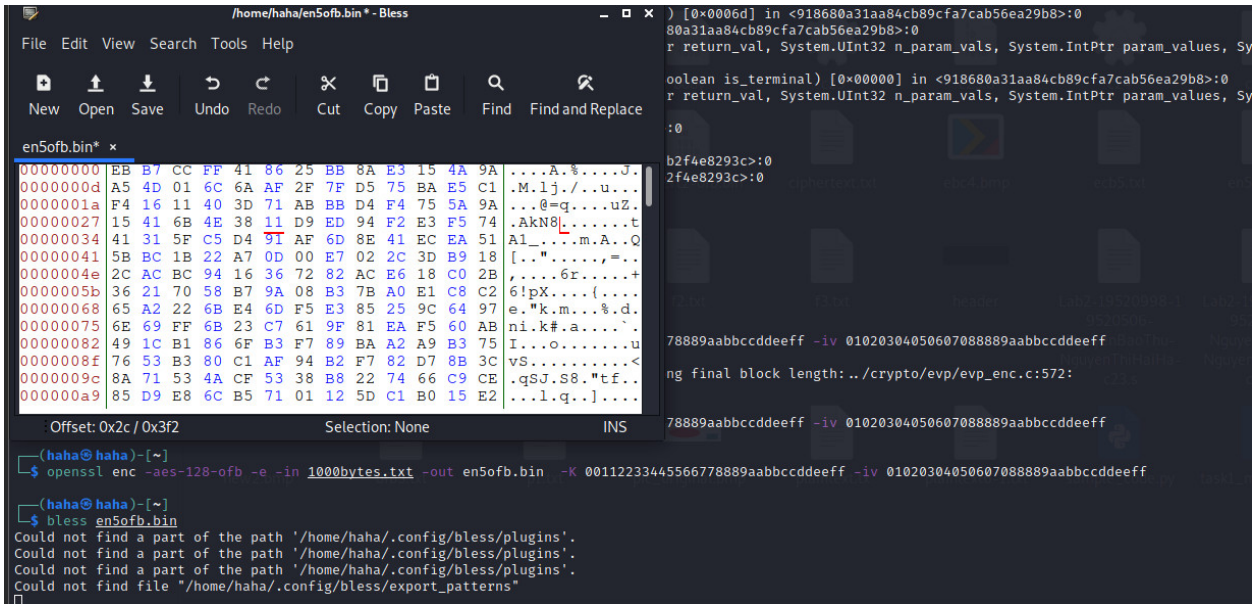



(haha㉿haha)-[~]
$ openssl enc -aes-128-cfb -e -in 1000bytes.txt -out en5cfb.bin -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff
(haha㉿haha)-[~]
$ bless en5cfb.bin
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find file "/home/haha/.config/bless/export_patterns"
/home/haha/en5cfb.bin* - Bless
File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
en5cfb.bin* ×
00000000 EB B7 CC FF 41 86 25 BB 8A E3 15 4A 9A ....A.%....J.
0000000d A5 4D 01 D7 1F AD 85 C6 F8 44 71 F8 9B .M.......Dq..
0000001a 24 82 48 47 B0 EA 48 CD 03 2F 86 AA 79 $.HG..H../..y
00000027 F8 04 BE 38 B7 71 E2 90 1D 1C AC 6B 26 ...8.q.....k&
00000034 35 68 93 29 DC 74 6E 74 34 1F C3 3C BF 5h.).tnt4..<.
00000041 70 A7 19 1A B1 BB 6C 84 C4 81 A1 87 F8 p.....l.....
0000004e 4E 68 93 21 CD 67 3B B6 87 D9 0B F2 9C Nh.!.g;.....
0000005b 9F B4 5C 2C AA A3 E6 DF 6D 99 41 51 0E ..\,....m.AQ.
00000068 4F 2B 5A 77 7F 70 D2 FD 47 69 7D B6 49 O+Zw.p..Gi}.I
00000075 9A F3 F8 A8 74 A6 15 CD 72 D1 2E 83 A0 ....t...r....
00000082 49 2C 5C 2E 1D 56 2C AF 0D AC C4 FB 73 I,\..V,.....s
0000008f 91 6F 2F 86 A2 26 8B F5 5A 83 23 7A E2 .o/..&..Z.#z.
0000009c EB 34 0D C6 6C 85 62 E1 8D 6B AB F8 DC .4..l.b..k...
000000a9 71 D7 3C 37 C9 09 D0 05 46 1E A3 8F C1 q.<7....F....
Offset: 0x2a / 0x3f2
Selection: None
INS

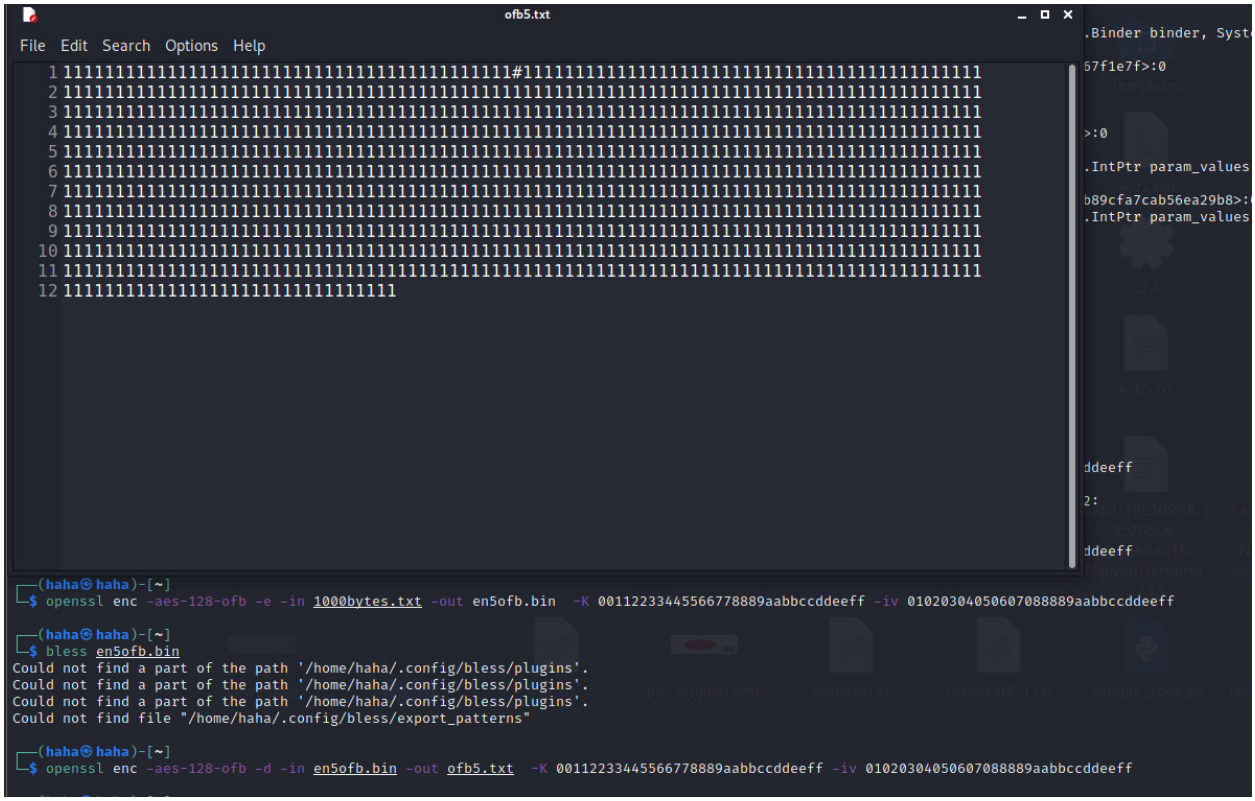

cfb5.txt
File Edit Search Options Help
(haha㉿haha)-[~]
$ openssl enc -aes-128-cfb -d -in en5cfb.bin -out cfb5.txt -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff

- Với OFB: làm các bước tương tự như trên

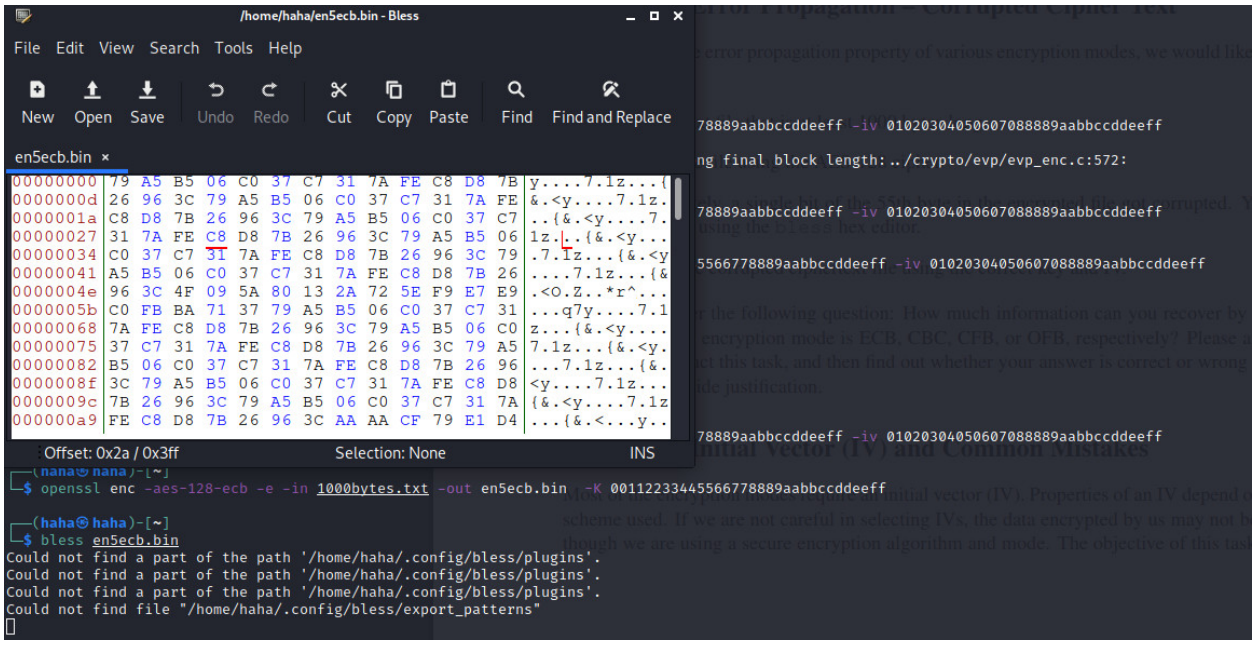


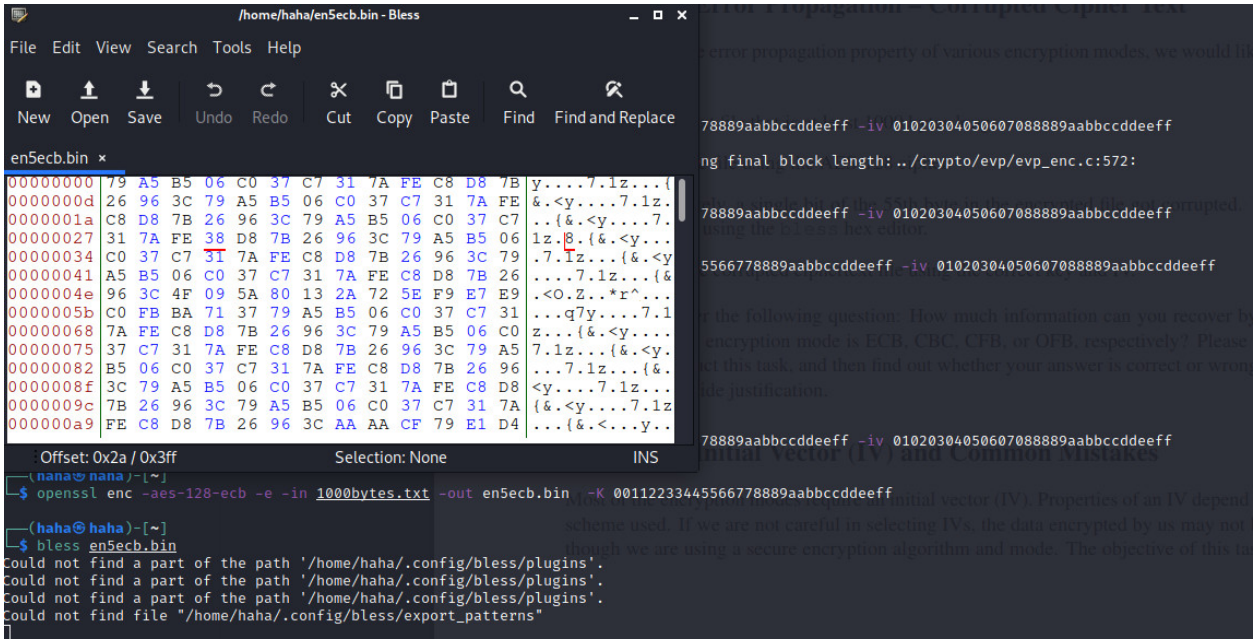


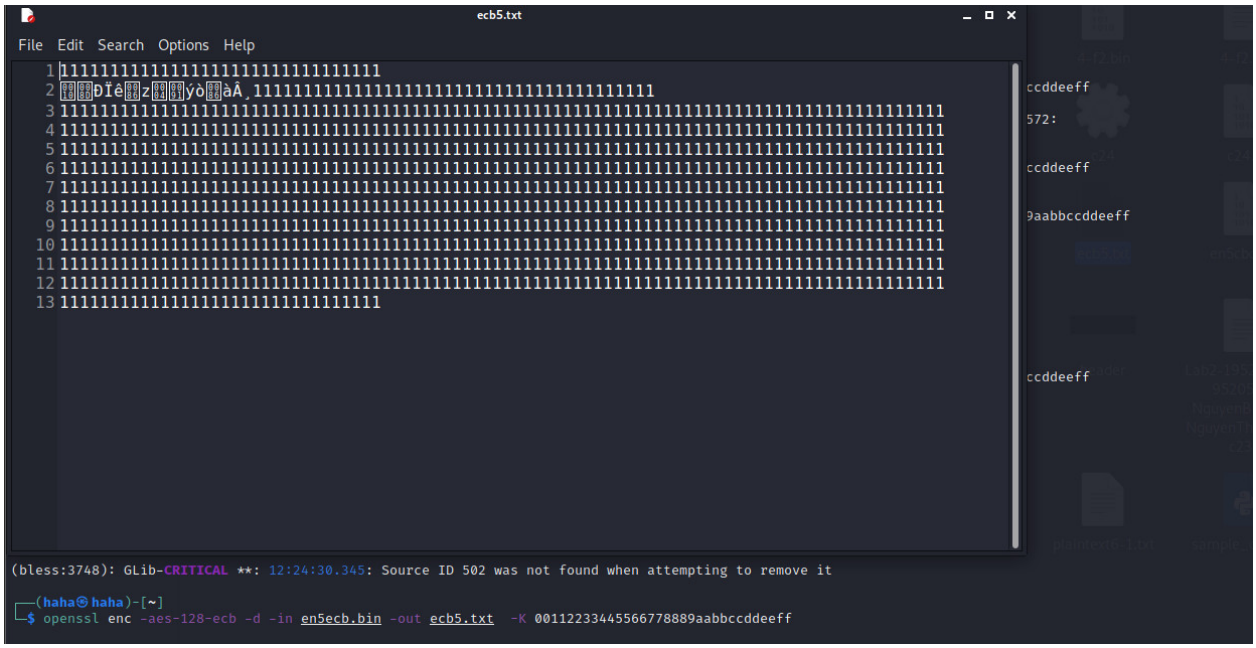
- So sánh với plaintext thấy sai một byte


ofb5.txt
File Edit Search Options Help
(haha㉿haha)-[~]
$ openssl enc -aes-128-ofb -e -in 1000bytes.txt -out en5ofb.bin -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff
(haha㉿haha)-[~]
$ bless en5ofb.bin
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find file "/home/haha/.config/bless/export_patterns"
(haha㉿haha)-[~]
$ openssl enc -aes-128-ofb -d -in en5ofb.bin -out ofb5.txt -K 00112233445566778889aabbccddeeff -iv 01020304050607088889aabbccddeeff

- Với ECB:


/home/haha/en5ecb.bin - Bless
File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
en5ecb.bin
Offset: 0x2a / 0x3ff Selection: None INS
$ openssl enc -aes-128-ecb -e -in 1000bytes.txt -out en5ecb.bin -K 00112233445566778889aabbccddeeff
(haha㉿haha)-[~]
$ bless en5ecb.bin
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find file "/home/haha/.config/bless/export_patterns"

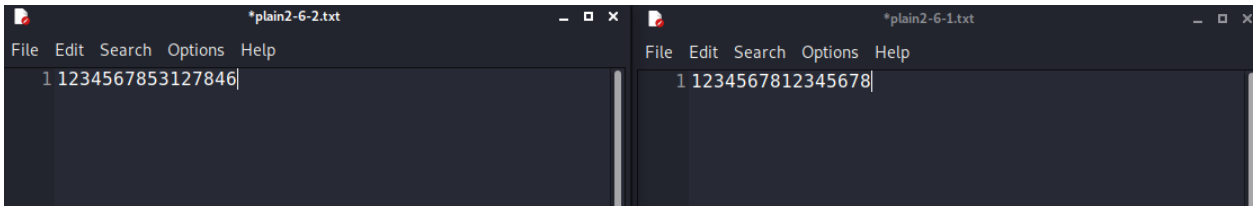

/home/haha/en5ecb.bin - Bless
File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
en5ecb.bin
00000000 79 A5 B5 06 C0 37 C7 31 7A FE C8 D8 7B
0000000d 26 96 3C 79 A5 B5 06 C0 37 C7 31 7A FE
0000001a C8 D8 7B 26 96 3C 79 A5 B5 06 C0 37 C7
00000027 31 7A FE 38 D8 7B 26 96 3C 79 A5 B5 06
00000034 C0 37 C7 31 7A FE C8 D8 7B 26 96 3C 79
00000041 A5 B5 06 C0 37 C7 31 7A FE C8 D8 7B 26
0000004e 96 3C 4F 09 5A 80 13 2A 72 5E F9 E7 E9
0000005b C0 FB BA 71 37 79 A5 B5 06 C0 37 C7 31
00000068 7A FE C8 D8 7B 26 96 3C 79 A5 B5 06 C0
00000075 37 C7 31 7A FE C8 D8 7B 26 96 3C 79 A5
00000082 B5 06 C0 37 C7 31 7A FE C8 D8 7B 26 96
0000008f 3C 79 A5 B5 06 C0 37 C7 31 7A FE C8 D8
0000009c 7B 26 96 3C 79 A5 B5 06 C0 37 C7 31 7A
000000a9 FE C8 D8 7B 26 96 3C AA AA CF 79 E1 D4
Offset: 0x2a / 0x3ff
Selection: None
INS
$ openssl enc -aes-128-ecb -e -in 1000bytes.txt -out en5ecb.bin -K 00112233445566778889aabbccddeeff
$ bless en5ecb.bin
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find a part of the path '/home/haha/.config/bless/plugins'.
Could not find file "/home/haha/.config/bless/export_patterns"


ecb5.txt
File Edit Search Options Help
(bless:3748): GLib-CRITICAL **: 12:24:30.345: Source ID 502 was not found when attempting to remove it
$ openssl enc -aes-128-ecb -d -in en5ecb.bin -out ecb5.txt -K 00112233445566778889aabbccddeeff

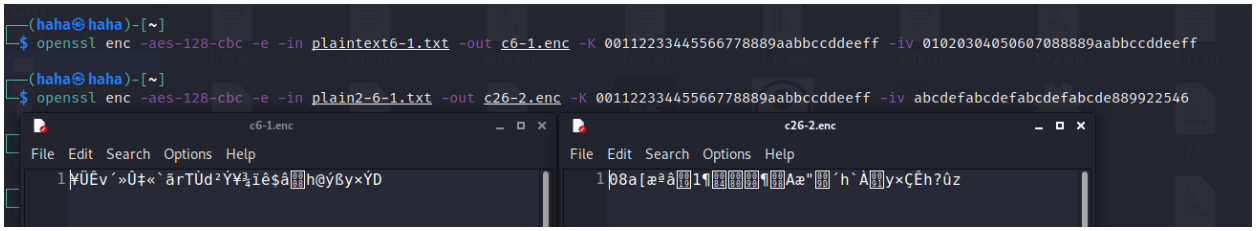
Task 6:

6.1 . IV Experiment

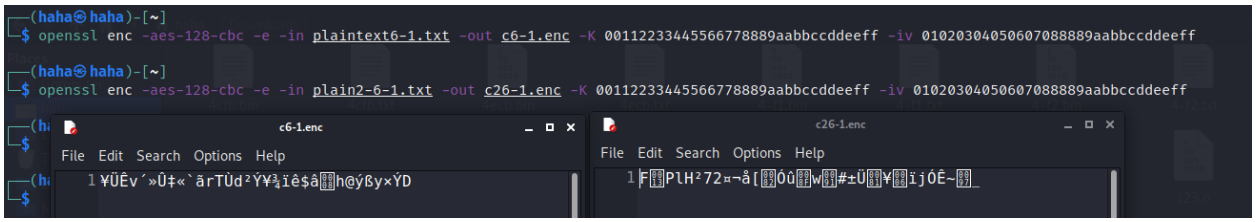
- Tạo hai plaintext có nội dung gần giống nhau



- Mã hóa hai plaintext hai lần với cùng 1 key và 2 IV khác nhau, ta thấy đoạn mã hóa hoàn toàn khác nhau



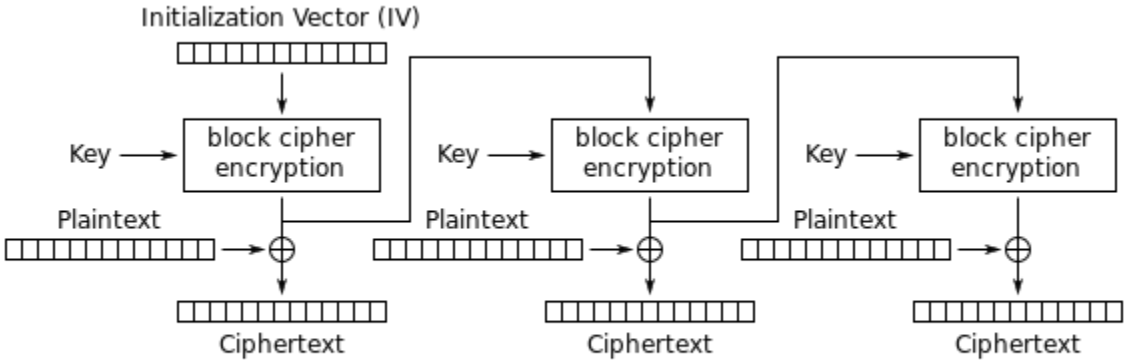
- Mã hóa hai plaintext hai lần với cùng 1 key và 1 IV, có vài điểm giống nhau



Câu hỏi: Tại sao IV cần phải độc nhất?

Trả lời: Khi sử dụng chung một IV, thì ta có thể nhìn ra sự liên quan giữa hai plaintext, do đó có thể bị tấn công khi họ suy ra được IV.

6.2 Common Mistake: Use the Same IV



Output Feedback (OFB) mode encryption

- Nếu plaintext không lặp lại, việc sử dụng chung một IV không an toàn.
  + Lấy P1 XOR C1 ta được O1

    Vì ta dùng cùng IV và Key nên O1 cũng bằng với O2

  + Lấy C2 XOR O2 ta được P2

    => Ta có thể tìm P2 bằng cách lấy P1 XOR C1 XOR C2

    (*) Ví dụ minh họa:

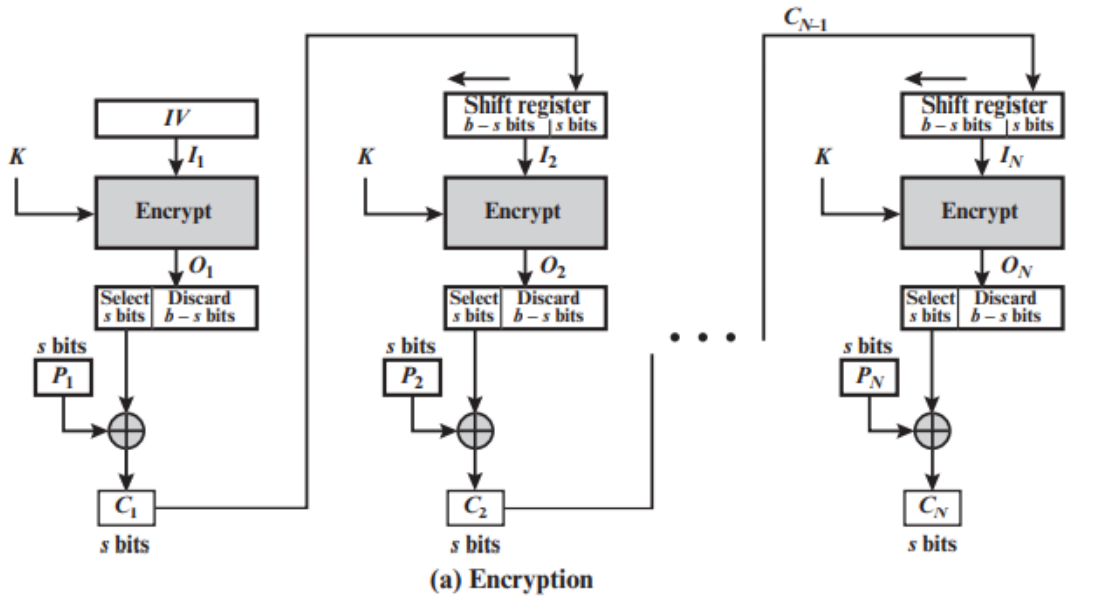
```
ubuntu@ubuntu:~$ python3 sample_code.py "This is a known message!" \
> a469b1c502c1cab966965e50425438e1bb1b5f9037a4c159 \
> bf73bcd3509299d566c35b5d450337e1bb175f903fafc159
Order: Launch a missile!
ubuntu@ubuntu:~$
```

(*) sample_code.py :

```
from sys import argv
_, first, second, third = argv
p1 = bytearray(first, encoding = 'utf-8')
c1 = bytearray.fromhex(second)
c2 = bytearray.fromhex(third)
p2 = bytearray(x^y^z for x,y,z in zip(p1,c1,c2))
print(p2.decode('utf-8'))
```

Câu hỏi:Nếu chúng ta thay thế OFB trong thử nghiệm này bằng CFB (Phản hồi mật mã), bao nhiêu P2 có thể được tiết lộ?

Trả lời: Em không biết



(a) Encryption

6.3 Common Mistake: Use a Predictable IV

Em chưa biết làm