



## LAB 2

Course name: **Cryptography** - Class code: **NT219.L21.ANTT.1**

Lecturer: **Van Thien Luan**

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

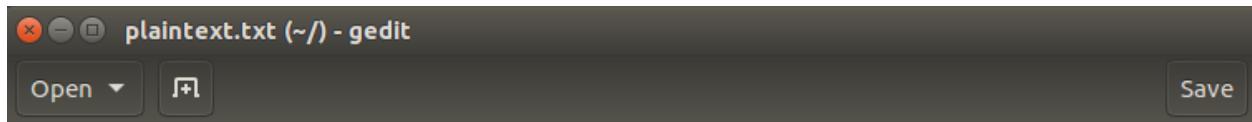
### Task 1:

- 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:

```
● ● ● ubuntu@ubuntu:~  
ubuntu@ubuntu:~$ tr 'ytn' 'THE' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v' 'THE A' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v q my' 'THE A AS IT' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v q my invqy mu' 'THE A AS IT LEAST IN' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v q my invqy mu insn ytnmh lmyt' 'THE A AS IT LEAST IN LIKE THEIR WITH' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v q my invqy mu insn ytnmh lmyt dnhv vlvhpq lnnsup' 'THE A AS IT LEAST IN LIKE THEIR WITH YEAR AWARDS WEEKEND' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v q my invqy mu insn ytnmh lmyt dnhv vlvhpq lnnsup gntmup ltmat cxfnncuy' 'THE A AS IT LEAST IN LIKE THEIR WITH YEAR AWARDS WEEKEND BEHIND WHICH MOVEMENT' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v q my invqy mu insn ytnmh lmyt dnhv vlvhpq lnnsup gntmup ltmat cxfnncuy qzupvd yzhu vgxzy hmrtv bvyhn ixur' 'THE A AS IT LEAST IN LIKE THEIR WITH YEAR AWARDS WEEKEND BEHIND WHICH MOVEMENT SUNDAY TURN ABOUT RIGHT AFTER LONG' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v q my invqy mu insn ytnmh lmyt dnhv vlvhpq lnnsup gntmup ltmat cxfnncuy qzupvd yzhu vgxzy hmrtv bvyhn ixur axcevud nykyhv ehmnw' 'THE A AS IT LEAST IN LIKE THEIR WITH YEAR AWARDS WEEKEND BEHIND WHICH MOVEMENT SUNDAY TURN ABOUT RIGHT AFTER LONG COMPANY EXTRA PRIZE' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ tr 'ytn v q my invqy mu insn ytnmh lmyt dnhv vlvhpq lnnsup gntmup ltmat cxfnncuy qzupvd yzhu vgxzy hmrtv bvyhn ixur axcevud nykyhv ehmnw jznqymxu ozgmivuy' 'THE A AS IT LEAST IN LIKE THEIR WITH YEAR AWARDS WEEKEND BEHIND WHICH MOVEMENT SUNDAY TURN ABOUT RIGHT AFTER LONG COMPANY EXTRA PRIZE QUESTION JUBILANT' <ciphertext.txt> plaintext.txt  
ubuntu@ubuntu:~$ █
```



- 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

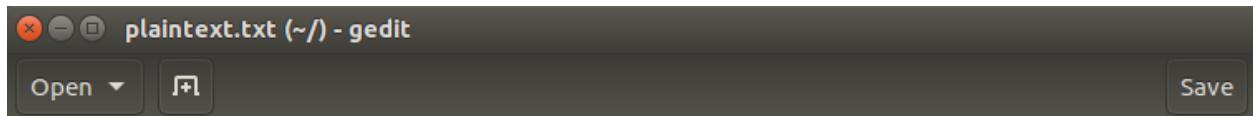
SIGNALING THEIR SUPPORT GOLDEN GLOBES ATTENDEES SWATHED THEMSELVES IN BLACK SPORDED LAPEL PINS AND SOUNDED OFF ABOUT SEXIST POWER IMBALANCES FROM THE RED CARPET AND THE STAGE ON THE AIR E WAS CALLED OUT ABOUT PAY INEQUITY AFTER ITS FORMER ANCHOR CATT SADLER QUIT ONCE SHE LEARNED THAT SHE WAS MAKING FAR 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 00112233445566778889aabbcdddeeff
(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

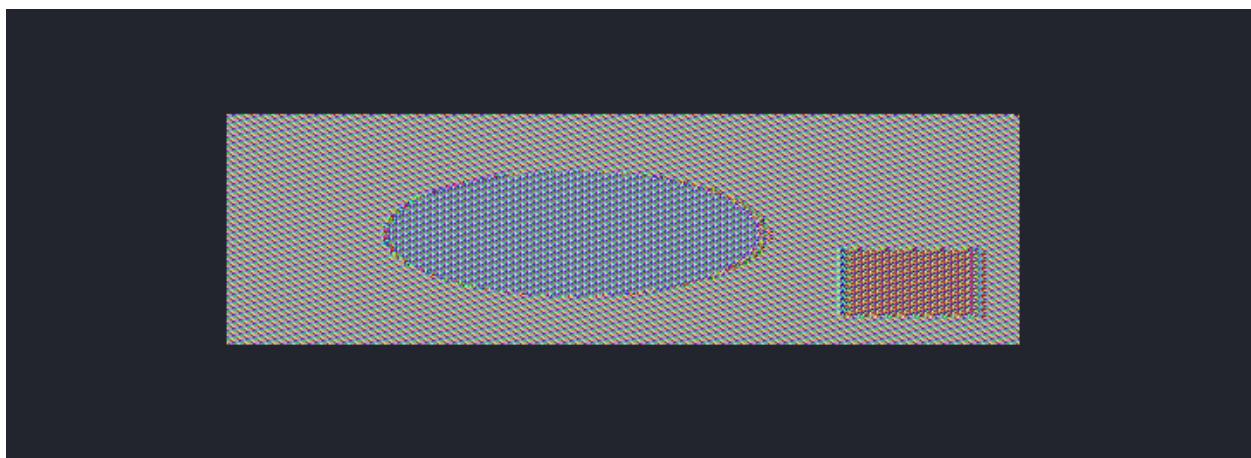


Figure 3: Hình ảnh được mã hóa bởi mode ECB



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

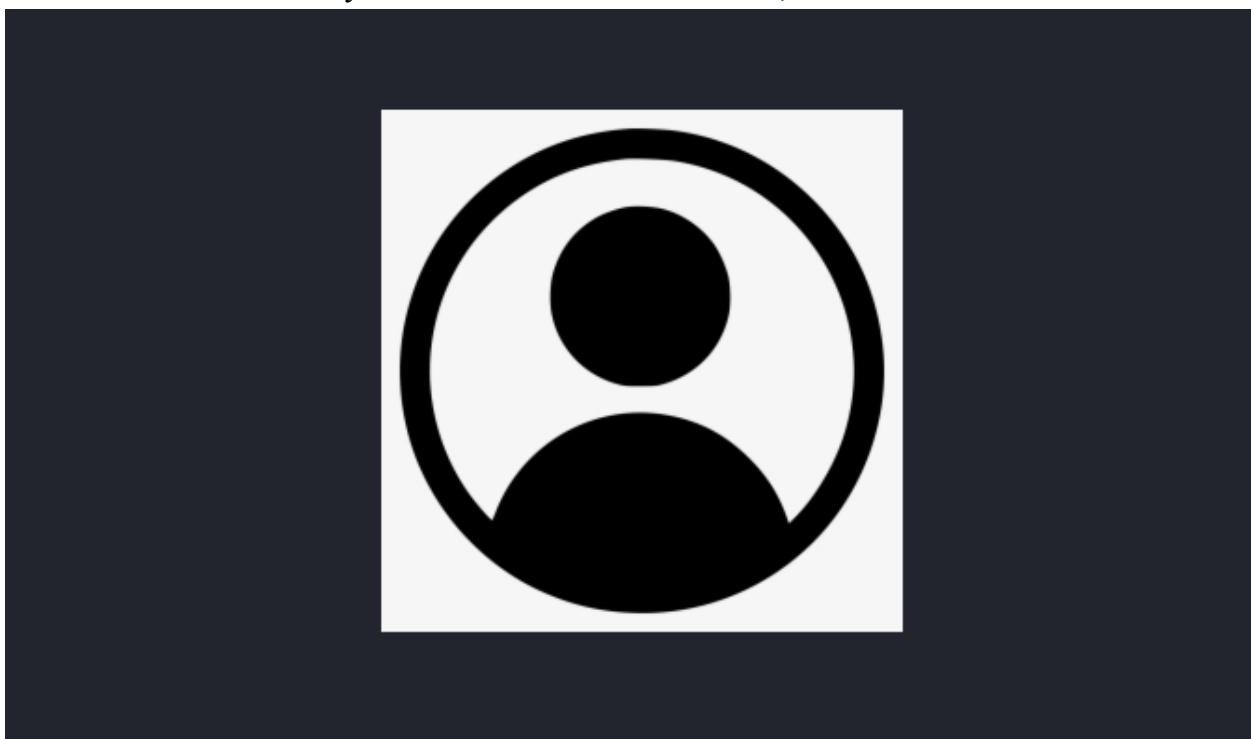


Figure 4: Ảnh gốc trước khi được mã hóa

- Mã hóa hình ảnh bằng mode ECB

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

(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

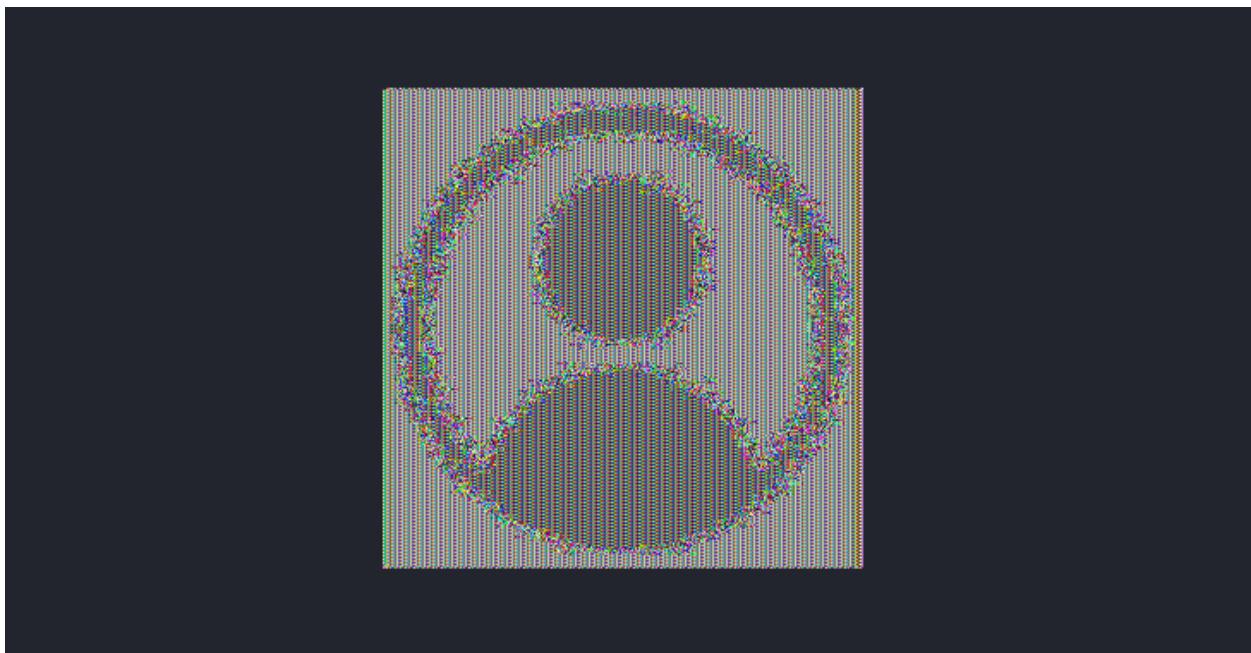


Figure 5: Hình ảnh được mã hóa bởi mode ECB

- Mã hóa hình ảnh bằng CBC

```
(haha@haha) [~]
$ openssl enc -aes-128-cbc -e -in basic.bmp -out cbc4-1.bmp -K 00112233445566778889aabccddeeff -iv 01020304050607088889aabccddeeff
(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:

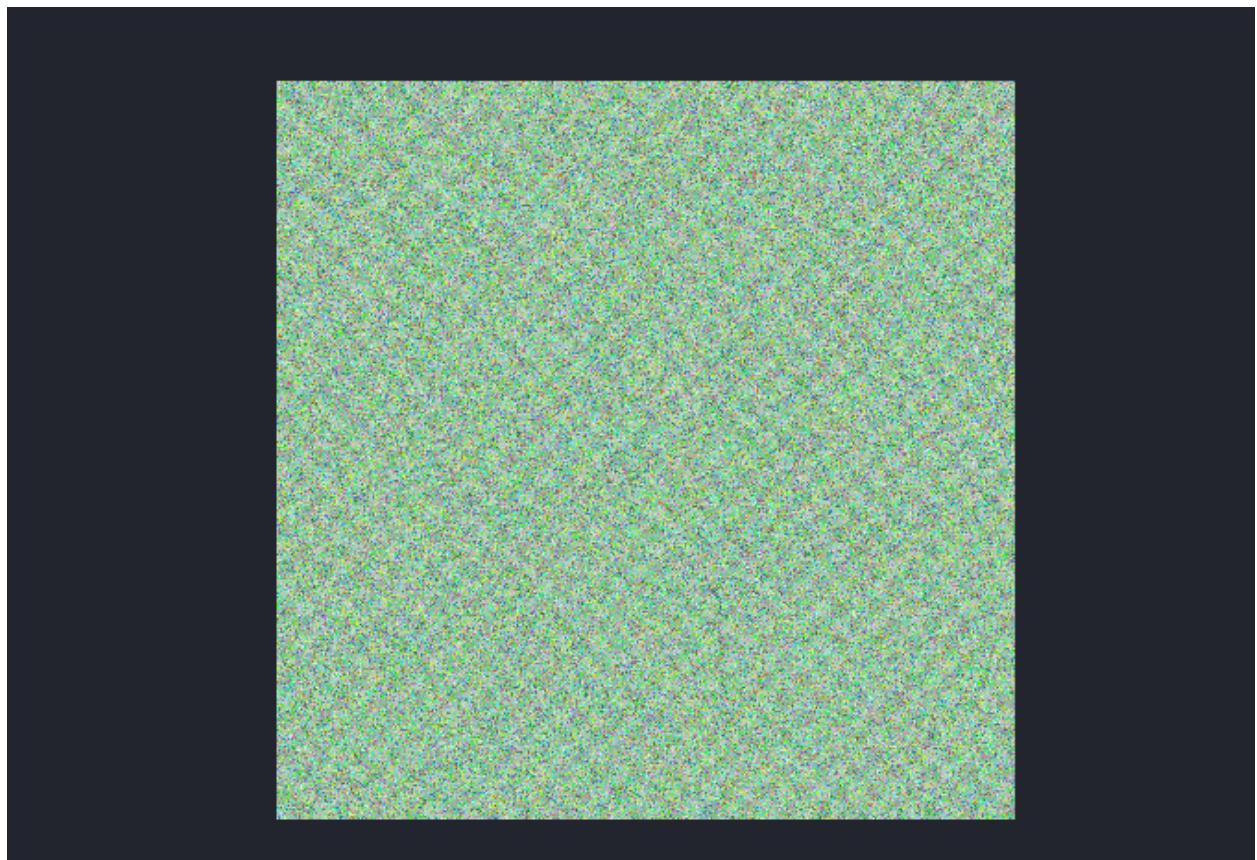


Figure 6: Hình ảnh được mã hóa bởi mode CBC

#### 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 00112233445566778889aabcccddeff -iv 01020304050607088889aabcccddeff
(haha@haha)[~]
$ openssl enc -aes-128-cbc -e -in f2.txt -out 4-f2.bin -K 00112233445566778889aabcccddeff -iv 01020304050607088889aabcccddeff
(haha@haha)[~]
$ openssl enc -aes-128-cbc -e -in f3.txt -out 4-f3.bin -K 00112233445566778889aabcccddeff -iv 01020304050607088889aabcccddeff
SEED Labs - Secret-Key Encryption Lab
```

- 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 -n "12345" > f1.txt
778889aabcccddeff -iv 01020304050607088889aabcccddeff -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 00112233445566778889aabcccddeff -iv 01020304050607088889aabcccddeff -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.....|00000010

(haha@haha)[~]
$ openssl enc -aes-128-cbc -d -in 4-f1.bin -out 4-f1.txt -K 00112233445566778889aabcccddeff -iv 01020304050607088889aabcccddeff -nopad

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

(haha@haha)[~]
$ xxd 4-f1.txt
00000000: 3132 3334 350b 0b0b 0b0b 0b0b 0b0b 0b0b 12345.....|00000010
```

We then use "openssl enc -aes-128-cbc -e" to encrypt these three files using with CBC mode. Please describe the size of the encrypted files.  
We would like to see what is added to the padding during the encryption. To achieve will decrypt these files using "openssl enc -aes-128-cbc -d". Unfortunately by default will automatically remove the padding, making it impossible for us to see. However, the command does have an option called "-nopad", which disables the during the decryption, the command will not remove the padded data. Therefore, by decrypted data, we can see what data are used in the padding. Please use this technique It should be noted that padding data may not be printable, so you need to use a hex tool | The following example shows how to display a file in the hex format:  
\$ hexdump -C p1.txt  
00000000 31 32 33 34 35 36 37 38 39 49 4a 4b 4c 0a |12345678  
\$ xxd p1.txt  
00000000: 3132 3334 3536 3738 3949 4a4b 4c0a |12345678  
7 Task 5: Error Propagation – Corrupted Cipher Text  
In this exercise, we will demonstrate the error propagation property of various encryption modes, we would like to do the following exercise:  
1. Create a text file that is at least 1000 bytes long.



```
(haha@haha)~]$ hexdump -C f1.txt
00000000 31 32 33 34 35
00000005

(haha@haha)~]$ xxd f1.txt
00000000: 3132 3334 35

(haha@haha)~]$ hexdump -C f2.txt
00000000 31 32 33 34 35 36 37 38 39 30
0000000a

(haha@haha)~]$ xxd f2.txt
00000000: 3132 3334 3536 3738 3930

(haha@haha)~]$ hexdump -C f3.txt
00000000 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35
0000000f

(haha@haha)~]$ xxd f3.txt
00000000: 3132 3334 3536 3738 3930 3132 3334 35 123456789012345


```

The screenshot shows a terminal window with four command-line sessions. The first session shows the raw hex dump of file f1.txt. The second session shows the raw hex dump of file f2.txt. The third session shows the raw hex dump of file f3.txt, which includes a 16-byte suffix at the end. To the right of the terminal, there is a file explorer window showing a dark-themed desktop environment with icons for Desktop, Documents, Downloads, Pictures, Public, Templates, Videos, and Music. Several files are visible, including '12345', '1234567890', '123456789012345', '4cbc.bin', '4cbc.txt', '4cfb.bin', '4cfb.txt', '4-f1.bin', and '4-f1.txt'. The file names correspond to the hex dumps shown in the terminal.

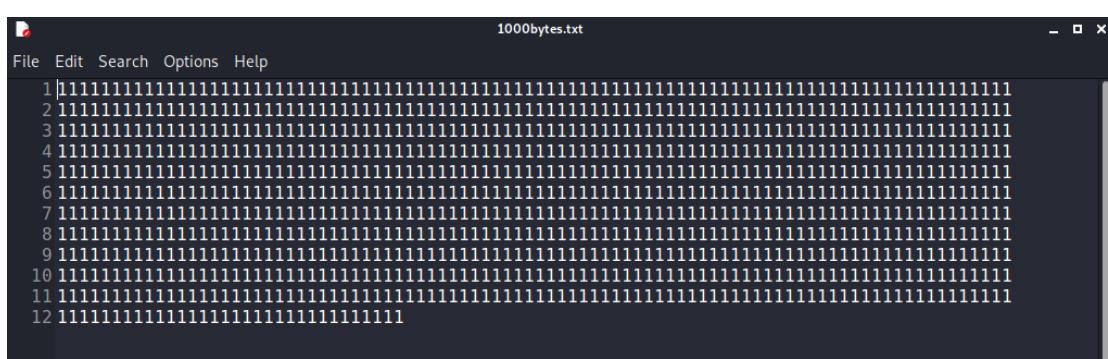
Figure 7: Nội dung file gốc trước khi được mã hóa

### Task 5: Error Propagation – Corrupted Cipher Text

Câu hỏi: Số thông tin có thể tìm 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

```
(haha㉿haha) [~]
$ openssl enc -aes-128-cbc -e -in 1000bytes.txt -out en5cbc.bin -K 00112233445566778899aabccddeeff -iv 01020304050607088889aabccddeeff

(haha㉿haha) [~]
$ bless en5cbc.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"
[...]
```

To understand the exercise:

1. Create a text file.
2. Encrypt the file using the command: `openssl enc -aes-128-cbc -e -in 1000bytes.txt -out en5cbc.bin -K 00112233445566778899aabccddeeff -iv 01020304050607088889aabccddeeff`
3. Unfortunately, the corruption of the byte at offset 55 caused the file to become corrupted.
4. Decrypt the file using the command: `openssl enc -aes-128-cbc -d -in en5cbc.bin -out decrypted.txt -K 00112233445566778899aabccddeeff -iv 01020304050607088889aabccddeeff`

Please answer the question: What is the byte value at offset 55 of the corrupted file, if the encryption mode is ECB, CBC, CFB, or OFB, respectively? Please answer this question before you conduct this task, and then find out whether your answer is correct or wrong after you finish this task.

Offset	Value	Character
0x2a	55	?
0x3ef	55	?

```
(haha㉿haha) [~]
$ openssl enc -aes-128-cbc -e -in 1000bytes.txt -out en5cbc.bin -K 00112233445566778899aabccddeeff -iv 01020304050607088889aabccddeeff

(haha㉿haha) [~]
$ bless en5cbc.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"
[...]
```

To understand the exercise:

1. Create a text file.
2. Encrypt the file using the command: `openssl enc -aes-128-cbc -e -in 1000bytes.txt -out en5cbc.bin -K 00112233445566778899aabccddeeff -iv 01020304050607088889aabccddeeff`
3. Unfortunately, the corruption of the byte at offset 55 caused the file to become corrupted.
4. Decrypt the file using the command: `openssl enc -aes-128-cbc -d -in en5cbc.bin -out decrypted.txt -K 00112233445566778899aabccddeeff -iv 01020304050607088889aabccddeeff`

Please answer the question: What is the byte value at offset 55 of the corrupted file, if the encryption mode is ECB, CBC, CFB, or OFB, respectively? Please answer this question before you conduct this task, and then find out whether your answer is correct or wrong after you finish this task.

Offset	Value	Character
0x2a	55	?
0x3ef	55	?

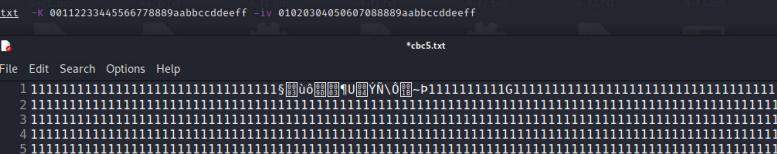


- Cuối cùng, decrypt file encrypt đã được chỉnh sửa và mở ra xem, so sánh với plaintext ban đầu là file 1000bytes.txt thì thấy được có một số byte bị sai.

```
(haha㉿haha) ~]$ openssl enc -aes-128-cbc -e -in 1000bytes.txt -out en5cbc.bin -K 00112233445566778889aabccddeff -iv 01020304050607088889aabccddeff
(haha㉿haha) ~]$ bless en5cbc.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"

(bless:3489): Glib-CRITICAL **: 12:04:46.472: Source ID 571 was not found when attempting to remove it

(haha㉿haha) ~]$ openssl enc -aes-128-cbc -d -in en5cbc.bin -out cbc5.txt -K 00112233445566778889aabccddeff -iv 01020304050607088889aabccddeff
(haha㉿haha) ~]$ cat cbc5.txt
```



The terminal window shows the decrypted file cbc5.txt. The file content is a large binary string consisting of 1s and 0s, arranged in a grid-like pattern. The terminal window has a dark background with light-colored text. The title bar of the window says "cbc5.txt". The file is located in the current directory, as indicated by the command "cat cbc5.txt".

- Với CFB:

```
(haha@haha) [~]
$ openssl enc -aes-128-cfb -e -in 1000bytes.txt -out en5cfb.bin -K 00112233445566778899abbccddeeff -iv 01020304050607088899abbccddeeff
To understand the error propagation property of various encryption modes, we would like to do the following exercise:
(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'. Create a text file named 'export_patterns' in the directory '/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 ~]# ./en5cfb.bin
The Crypto Library
Submission
Acknowledgment

File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
en5cfb.bin x
00000000 EB B7 CC FF 41 86 25 BB 8A E3 15 4A 9A ...A.%...J.
0000000d A5 4B 01 D7 0F AD 85 C6 F8 44 71 F8 9B ...M...Dq...
0000001a 2B 82 48 47 B0 EA 48 CD 03 2F 86 AA 79 ...S.HG..H...y
00000027 F8 04 BE 3B B7 71 EA 90 1D 1C AC 6B 26 ...[.q...k&
00000034 35 6B 93 29 DC 74 6E 74 34 1F C3 3C BF 5h.T.tnt4.<.
00000041 70 A7 19 1A B1 BB 6C 84 C4 81 A1 87 F8 p....l....
0000004e 4E 6B 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 BD 49 O+Zw.p..G1).I
00000075 9A F3 F8 A8 74 1D 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 86 6B AB F8 DC .4..1.b.k...
000000a9 71 D7 3C 37 C9 09 D0 05 46 1E A3 8F C1 q.<7.F....F
```



The screenshot shows a terminal window with the following content:

```
(haha@haha)-[~]
$ openssl enc -aes-128-cfb -d -in en5cfb.bin -out cfb5.txt -K 0011223344556677889aabccddeeff -iv 0102030405060708889aabccddeeff
```

The terminal output shows the file cfb5.txt being decrypted from its binary form (en5cfb.bin) using AES-128-CFB mode. The key and IV used are both the hex string 0011223344556677889aabccddeeff.



- Với OFB: làm các bước tương tự như trên

```

/home/haha/en5ofb.bin* -Bless
File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
en5ofb.bin* x
00000000 EB B7 CC FF 41 86 25 BB 8A E3 15 4A 9A ...A.%....J.
0000000d A5 4D 01 6C 6A AF 2F 7F D5 75 BA E5 C1 .M.lj./..u...
0000001a F4 16 11 40 3D 71 AB BB D4 F4 75 5A 9A ...@q...uz.
00000027 15 41 6B 4E 2A 11 D9 ED 94 F2 E3 F5 74 .AkN%....t.
00000034 41 31 5F C5 D4 91 AF 6D 8E 41 EC EA 51 A1...m.A..Q.
00000041 5B BC 1B 22 A7 0D 00 E7 02 2C 3D B9 18 [...]....=...
0000004e 2C AC BC 94 16 36 72 82 AC E6 18 C0 2B ,....6r....+.
0000005b 36 21 70 58 B7 9A 08 B3 7B A0 E1 C8 C2 6!px....(...
00000068 65 A2 22 6B E4 6D F5 E3 85 25 9C 64 97 e."k.m...%d.
00000075 6E 69 FF 6B 23 C7 61 9F 81 EA F5 60 AB ni.k#....`.
00000082 49 1C B1 86 6F B3 F7 89 BA A2 A9 B3 75 I...o.....u.
0000008f 76 53 B3 80 C1 AF 94 B2 F7 82 D7 8B 3C v$.....<.
0000009c 8A 71 53 4A CF 53 38 B8 22 74 66 C9 CE .qsJS.S8."tf..
000000a9 85 D9 E8 6C B5 71 01 12 5D C1 B0 15 E2 ...l.q].....
Offset: 0x2b / 0x3f2 Selection: None INS
(haha@haha)-[~]
$ openssl enc -aes-128-ofb -e -in 1000bytes.txt -out en5ofb.bin -K 0011233445566778889abbccddeeff -iv 01020304050607088889abbccddeeff
(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"

```

```

/home/haha/en5ofb.bin* -Bless
File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
en5ofb.bin* x
00000000 EB B7 CC FF 41 86 25 BB 8A E3 15 4A 9A ...A.%....J.
0000000d A5 4D 01 6C 6A AF 2F 7F D5 75 BA E5 C1 .M.lj./..u...
0000001a F4 16 11 40 3D 71 AB BB D4 F4 75 5A 9A ...@q...uz.
00000027 15 41 6B 4E 2A 11 D9 ED 94 F2 E3 F5 74 .AkN%....t.
00000034 41 31 5F C5 D4 91 AF 6D 8E 41 EC EA 51 A1...m.A..Q.
00000041 5B BC 1B 22 A7 0D 00 E7 02 2C 3D B9 18 [...]....=...
0000004e 2C AC BC 94 16 36 72 82 AC E6 18 C0 2B ,....6r....+.
0000005b 36 21 70 58 B7 9A 08 B3 7B A0 E1 C8 C2 6!px....(...
00000068 65 A2 22 6B E4 6D F5 E3 85 25 9C 64 97 e."k.m...%d.
00000075 6E 69 FF 6B 23 C7 61 9F 81 EA F5 60 AB ni.k#....`.
00000082 49 1C B1 86 6F B3 F7 89 BA A2 A9 B3 75 I...o.....u.
0000008f 76 53 B3 80 C1 AF 94 B2 F7 82 D7 8B 3C v$.....<.
0000009c 8A 71 53 4A CF 53 38 B8 22 74 66 C9 CE .qsJS.S8."tf..
000000a9 85 D9 E8 6C B5 71 01 12 5D C1 B0 15 E2 ...l.q].....
Offset: 0x2c / 0x3f2 Selection: None INS
(haha@haha)-[~]
$ openssl enc -aes-128-ofb -e -in 1000bytes.txt -out en5ofb.bin -K 0011233445566778889abbccddeeff -iv 01020304050607088889abbccddeeff
(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"

```

- So sánh với plaintext thấy sai một byte



```
(haha@haha) [~]
$ openssl enc -aes-128-ofb -e -in 1000bytes.txt -out en5ofb.bin -K 00112233445566778889aabccddeeff -iv 01020304050607088889aabccddeeff

(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 00112233445566778889aabccddeeff -iv 01020304050607088889aabccddeeff
```

- VỚI ECB:

```
/home/haha/enSecb.bin - Bless
File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
enSecb.bin x
00000000 79 A5 B5 06 C0 37 C7 31 7A FE C8 D8 7B y....7.1z...
0000000d 26 96 3C 79 A5 B5 06 C0 37 C7 31 7A FE &.<y....7.1z.
0000001a C8 D8 7B 26 96 3C 79 A5 B5 06 C0 37 C7 ..&.<y....7.
00000027 31 7A FE C8 D8 7B 26 96 3C 79 A5 B5 06 1z..|..&.<y...
00000034 C0 37 C7 31 7A FE C8 D8 7B 26 96 3C 79 .7.1z...(&.<y...
00000041 A5 B5 06 C0 37 C7 31 7A FE C8 D8 7B 26 ...7.1z...(&.
0000004e 96 3C 4F 09 5A 80 13 2A 72 5E F9 E7 E9 .<0.Z...*r^...
0000005b C0 FB BA 71 37 79 A5 B5 06 C0 37 C7 31 ...q7y....7.1
00000068 7A FE C8 D8 7B 26 96 3C 79 A5 B5 06 C0 z...(&.<y...
00000075 37 C7 31 7A FE C8 D8 7B 26 96 3C 79 A5 7.1z...(&.<y.
00000082 B5 06 C0 37 C7 31 7A FE C8 D8 7B 26 96 ...7.1z...(&.
0000008f 3C 79 A5 B5 06 C0 37 C7 31 7A FE C8 D8 <y....7.1z...
0000009c 7B 26 96 3C 79 A5 B5 06 C0 37 C7 31 7A (&.<y....7.1z
000000a9 FE C8 D8 7B 26 96 3C AA AA CF 79 E1 D4 ...(&.<...y..
Offset: 0x2a / 0x3ff Selection: None INS
[nana@nana ~] $ openssl enc -aes-128-ecb -e -in 1000bytes.txt -out enSecb.bin -K 00112233445566778889aabccddeeff
[nana@nana ~] $ bless enSecb.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"
[nana@nana ~] $
```



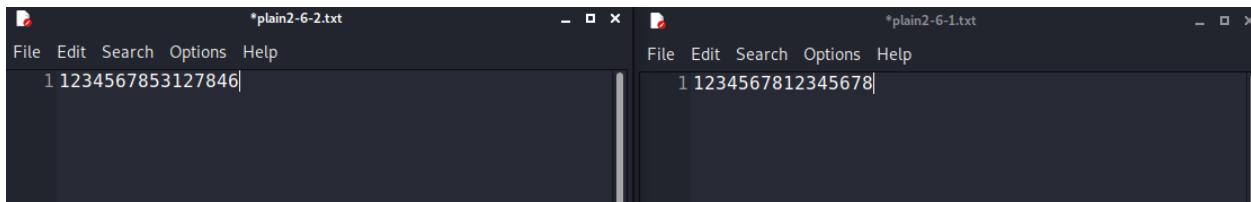
```
File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
en5ecb.bin x
00000000 79 A5 B5 06 C0 37 C7 31 7A FE C8 D8 7B y....7.1z...()
0000000d 26 96 3C 79 A5 B5 06 C0 37 C7 31 7A FE &.<y....7.1z...
0000001a C8 D8 7B 26 96 3C 79 A5 B5 06 C0 37 C7 ..(&.<y....7.
00000027 31 7A FE 38 D8 7B 26 96 3C 79 A5 B5 06 1z.1z.(&.<y...
00000034 C0 37 C7 31 7A FE C8 D8 7B 26 96 3C 79 .7.1z...(&.<y...
00000041 A5 B5 06 C0 37 C7 31 7A FE C8 D8 7B 26 ...7.1z...(&.
00000044 96 3C 4F 09 5A 80 13 CA 72 5E F9 E7 E9 <O.Z...*r^...
0000005b C0 FB BA 71 37 79 A5 B5 06 C0 37 C7 31 ...q7y....7.1
00000068 7A FE C8 D8 7B 26 96 3C 79 A5 B5 06 C0 ...(&.<y....
00000075 37 C7 31 7A FE C8 D8 7B 26 96 3C 79 A5 7.1z...(&.<y...
00000082 B5 06 C0 37 C7 31 7A FE C8 D8 7B 26 96 ...7.1z...(&.
0000008f 3C 79 A5 B5 06 C0 37 C7 31 7A FE C8 D8 ...<y....7.1z...
0000009c 7B 26 96 3C 79 A5 B5 06 C0 37 C7 31 7A ..(&.<y....7.1z...
000000a9 FE C8 D8 7B 26 96 3C AA AA CF 79 E1 D4 ...(&.<y...
Offset: 0x2a / 0x3ff Selection: None INS
nananana`~`$ openssl enc -aes-128-ecb -e -in 1000bytes.txt -out en5ecb.bin -K 0011223344556677889aabccddeeff initial vector (IV) and Common Mistakes
(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"
```

### Task 6:

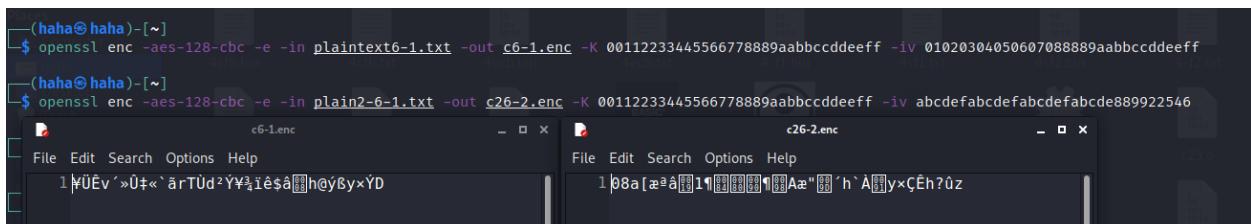


## 6.1 . IV Experiment

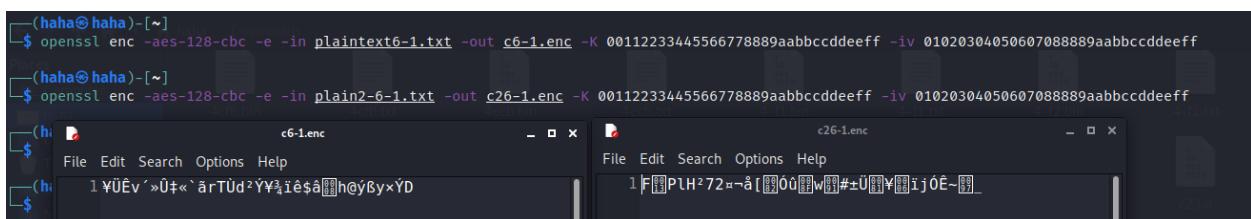
- Tạo hai plaintext có nội dung gần giống nhau



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



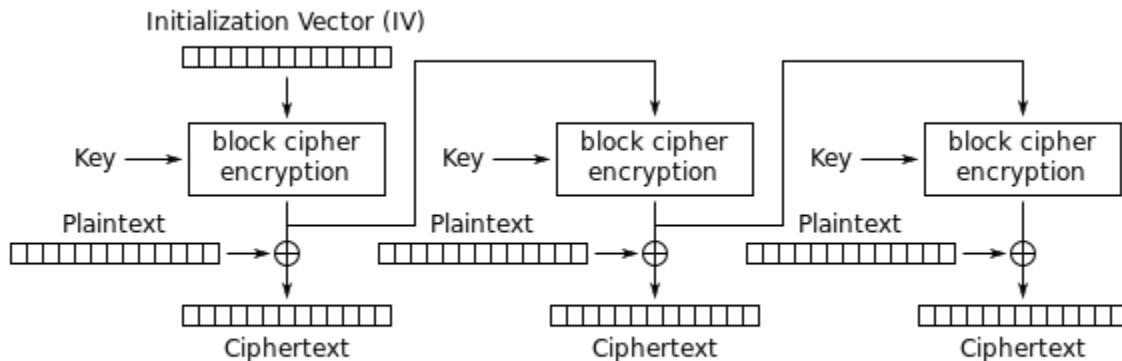
- Mã hóa hai plaintext hai lần với cùng 1 key và 1 IV, có vài điểm giống nhau



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 :

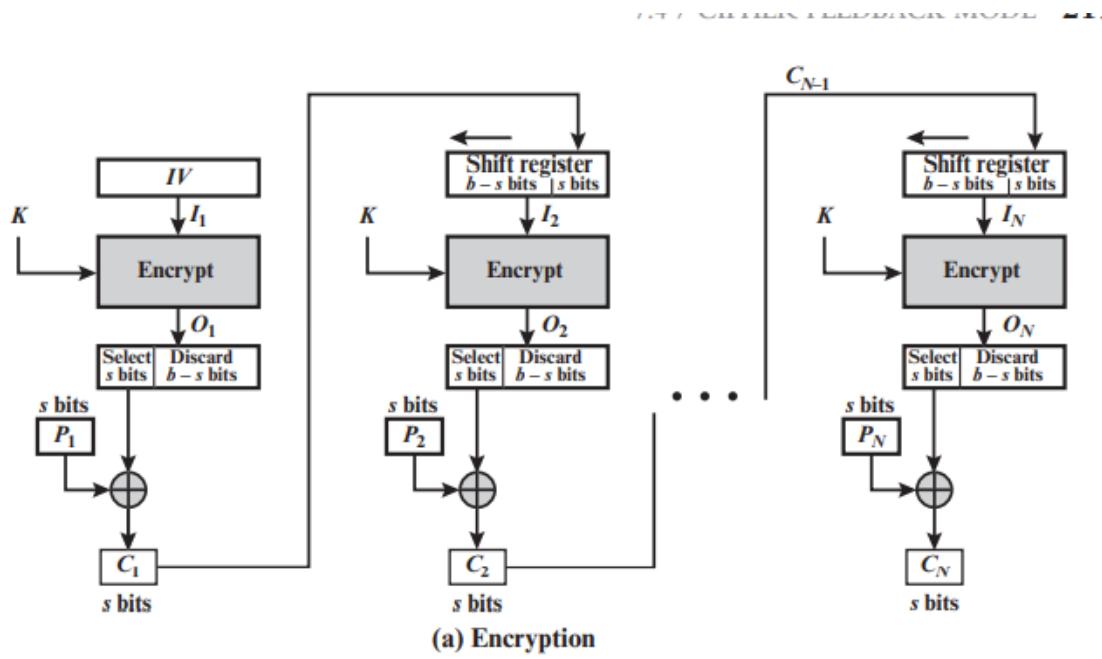
```

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



### 6.3 Common Mistake: Use a Predictable IV

Em chưa biết làm