## Task 1

[10/02/21]seed@VM:~/lab02$ grep -o a ciphertext.txt |wc -l

81

[10/02/21]seed@VM:~/lab02$ grep -o b ciphertext.txt |wc -l

1

[10/02/21]seed@VM:~/lab02$ grep -o c ciphertext.txt |wc -l

26

[10/02/21]seed@VM:~/lab02$ grep -o d ciphertext.txt |wc -l

7

[10/02/21]seed@VM:~/lab02$ grep -o e ciphertext.txt |wc -l

6

[10/02/21]seed@VM:~/lab02$ grep -o f ciphertext.txt |wc -l

64

[10/02/21]seed@VM:~/lab02$ grep -o g ciphertext.txt |wc -l

30

[10/02/21]seed@VM:~/lab02$ grep -o h ciphertext.txt |wc -l

45

[10/02/21]seed@VM:~/lab02$ grep -o i ciphertext.txt |wc -l

4

[10/02/21]seed@VM:~/lab02$ grep -o j ciphertext.txt |wc -l

16

[10/02/21]seed@VM:~/lab02$ grep -o k ciphertext.txt |wc -l

31

[10/02/21]seed@VM:~/lab02$ grep -o l ciphertext.txt |wc -l

85

[10/02/21]seed@VM:~/lab02$ grep -o m ciphertext.txt |wc -l

1

[10/02/21]seed@VM:~/lab02$ grep -o n ciphertext.txt |wc -l

18

[10/02/21]seed@VM:~/lab02$ grep -o o ciphertext.txt |wc -l

93

[10/02/21]seed@VM:~/lab02$ grep -o p ciphertext.txt |wc -l

116

[10/02/21]seed@VM:~/lab02$ grep -o q ciphertext.txt |wc -l

12

[10/02/21]seed@VM:~/lab02$ grep -o r ciphertext.txt |wc -l

0

[10/02/21]seed@VM:~/lab02$ grep -o s ciphertext.txt |wc -l

41

[10/02/21]seed@VM:~/lab02$ grep -o t ciphertext.txt |wc -l

0

[10/02/21]seed@VM:~/lab02$ grep -o u ciphertext.txt |wc -l

15

[10/02/21]seed@VM:~/lab02$ grep -o v ciphertext.txt |wc -l

26

[10/02/21]seed@VM:~/lab02$ grep -o w ciphertext.txt |wc -l

61

[10/02/21]seed@VM:~/lab02$ grep -o x ciphertext.txt |wc -l

35

[10/02/21]seed@VM:~/lab02$ grep -o y ciphertext.txt |wc -l

68

[10/02/21]seed@VM:~/lab02$ grep -o z ciphertext.txt |wc -l

79

[10/02/21]seed@VM:~/lab02$ grep -o ya ciphertext.txt |wc -l

7

[10/02/21]seed@VM:~/lab02$

[10/02/21]seed@VM:~/lab02$ grep -o "zls" ciphertext.txt |wc -l

10

[10/02/21]seed@VM:~/lab02$ grep -o "szj" ciphertext.txt |wc -l

1

[10/02/21]seed@VM:~/lab02$ grep -o "nxs" ciphertext.txt |wc -l

1

[10/02/21]seed@VM:~/lab02$ grep -o "qfl" ciphertext.txt |wc -l

1

[10/02/21]seed@VM:~/lab02$ grep -o "oxp" ciphertext.txt |wc -l

11

[10/02/21]seed@VM:~/lab02$ grep -o "hzl" ciphertext.txt |wc -l

2

[10/02/21]seed@VM:~/lab02$ grep -o "ya" ciphertext.txt |wc -l

7

[10/02/21]seed@VM:~/lab02$ grep -o "lpq" ciphertext.txt |wc -l

1

[10/02/21]seed@VM:~/lab02$ grep -o "fu" ciphertext.txt |wc -l

8

[10/02/21]seed@VM:~/lab02$ grep -o "ipj" ciphertext.txt |wc -l

1

[10/02/21]seed@VM:~/lab02$ grep -o "of" ciphertext.txt |wc -l

3

[10/02/21]seed@VM:~/lab02$ grep -o "za" ciphertext.txt |wc -l

10

[10/02/21]seed@VM:~/lab02$ grep -o "nxs" ciphertext.txt |wc -l

1

[10/02/21]seed@VM:~/lab02$ grep -o "fkw" ciphertext.txt |wc -l

4

[10/02/21]seed@VM:~/lab02$ grep -o "zo" ciphertext.txt |wc -l

16

[10/02/21]seed@VM:~/lab02$ grep -o "yl" ciphertext.txt |wc -l

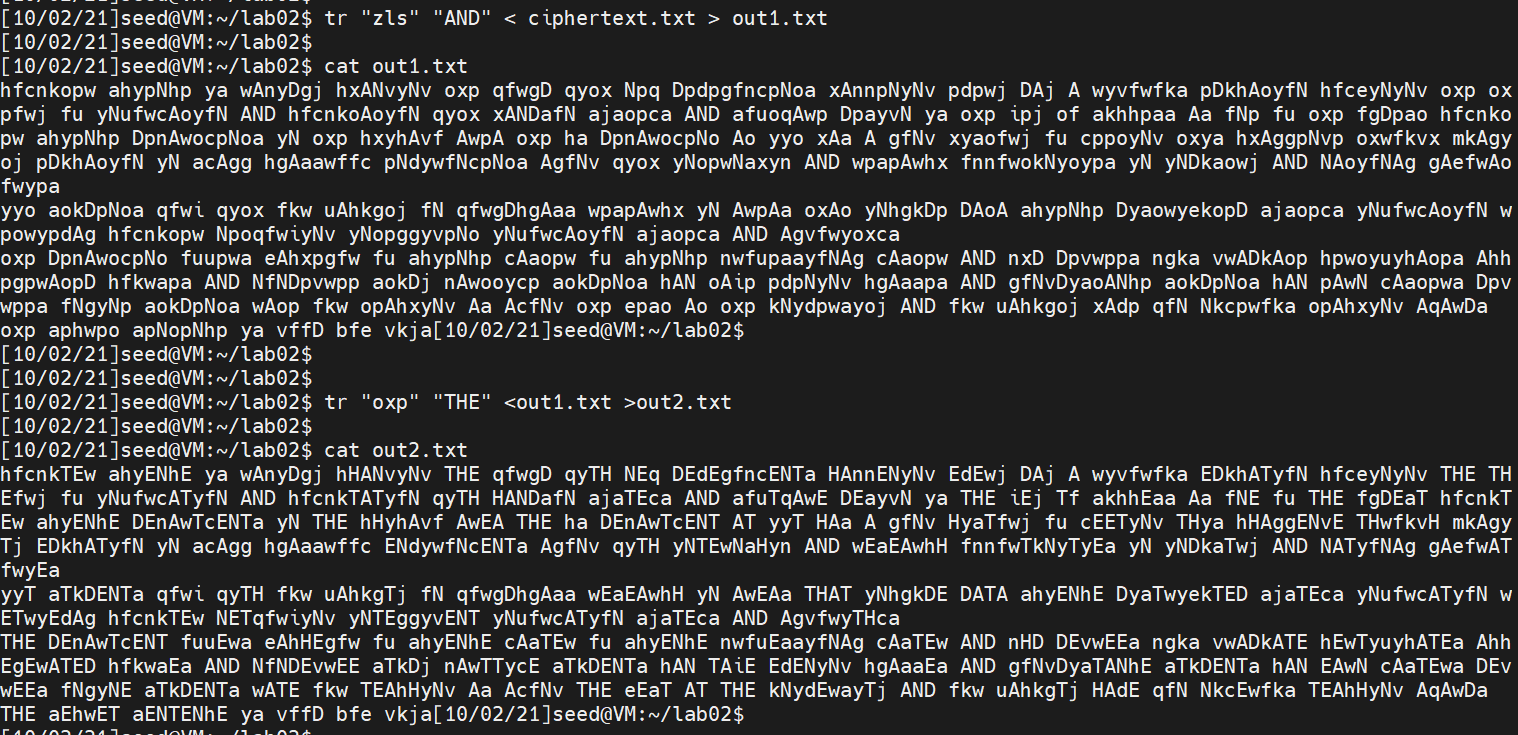
21

[10/02/21]seed@VM:~/lab02$ grep -o "bfe" ciphertext.txt |wc -l

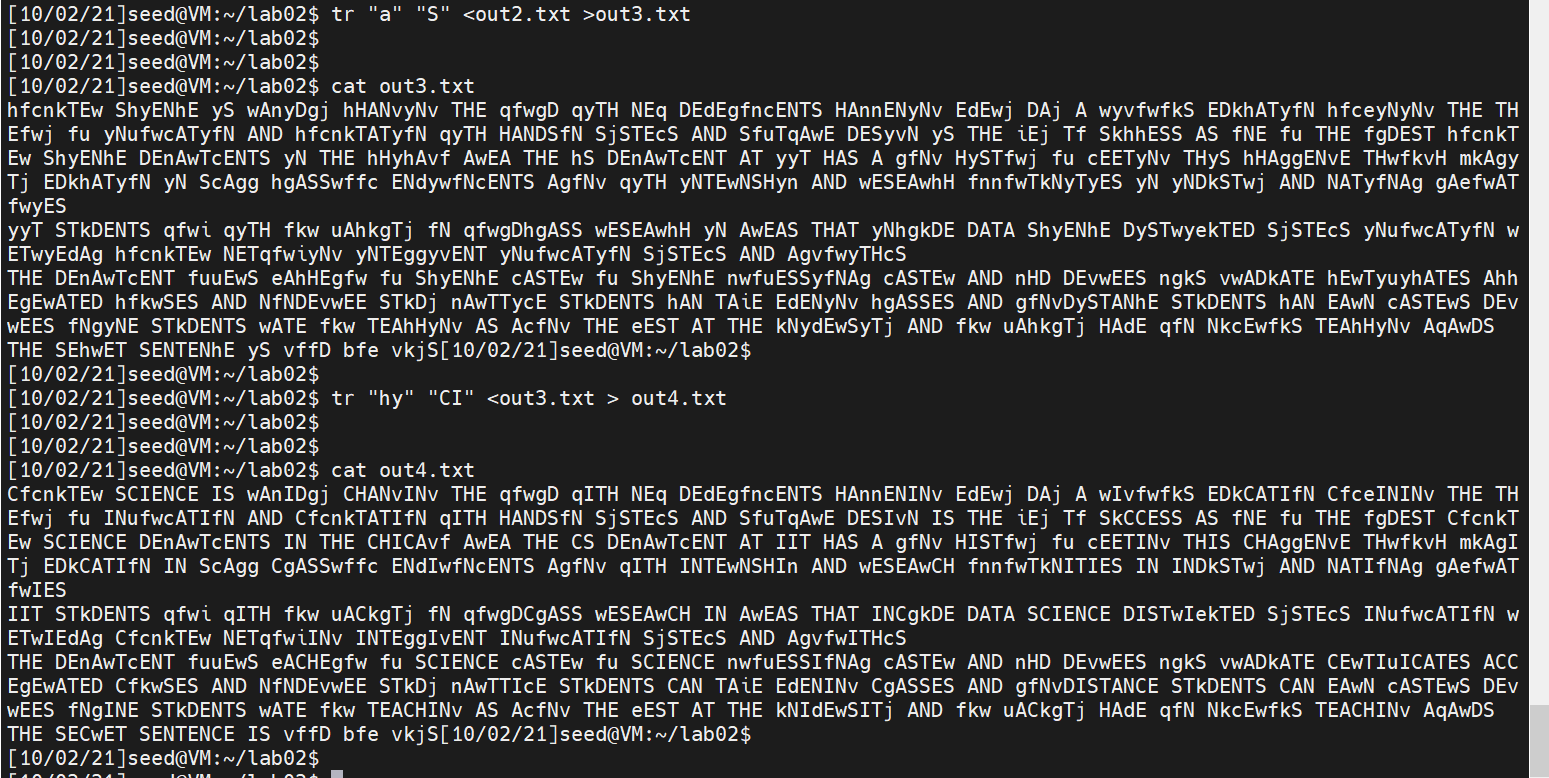
1

In the ciphertext.txt, 只有‘z’ appears 作为一个单词单独出现了，且以z打头的三个字母的单词”zls”出现了10次，以z打头的2个字母的单词“za” 出现了10次，”zo”出现了16次。猜测“z”原文为”a”,”zls” 为“and”.

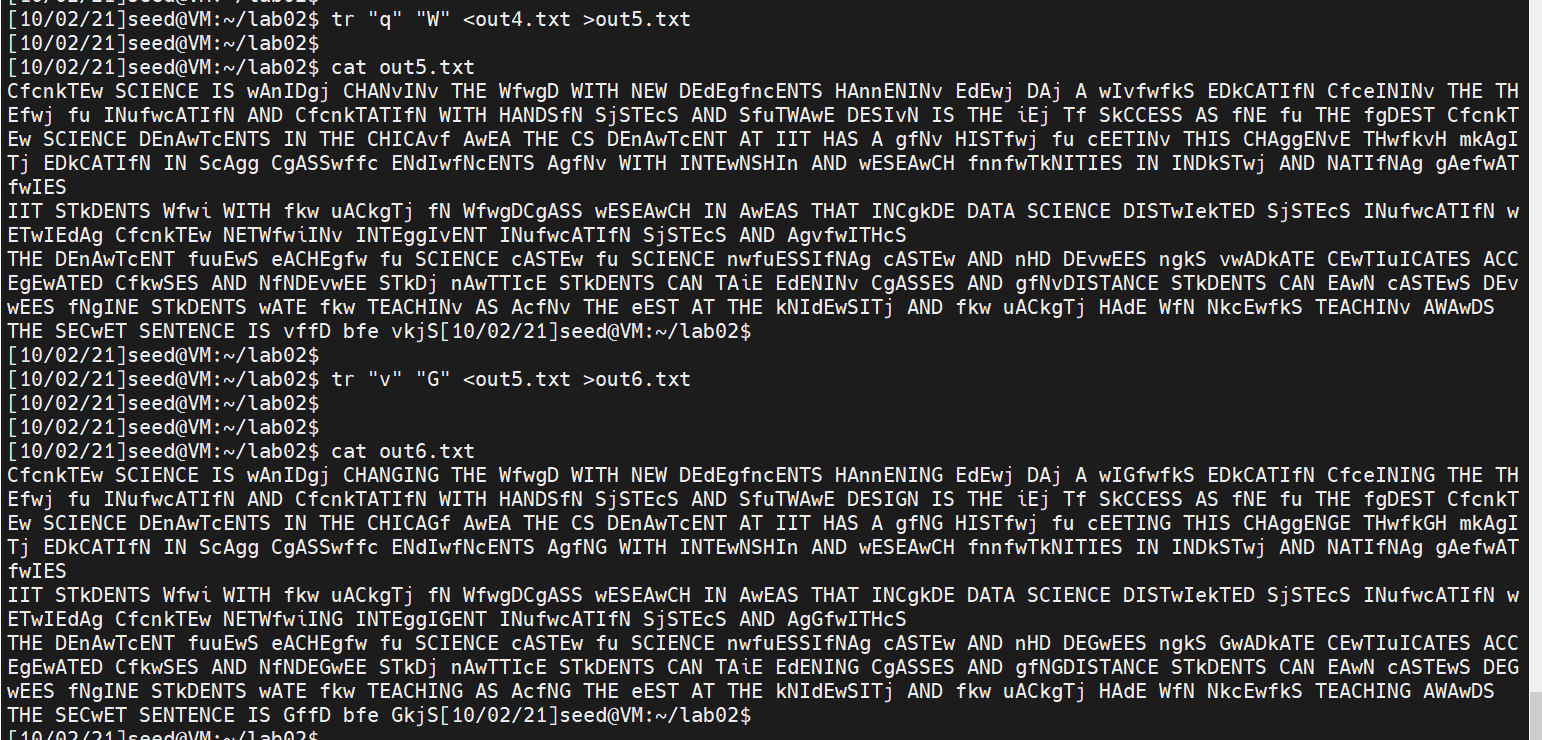
“oxp” 作为3个字母的单词出现的次数最多，因此猜测为 the



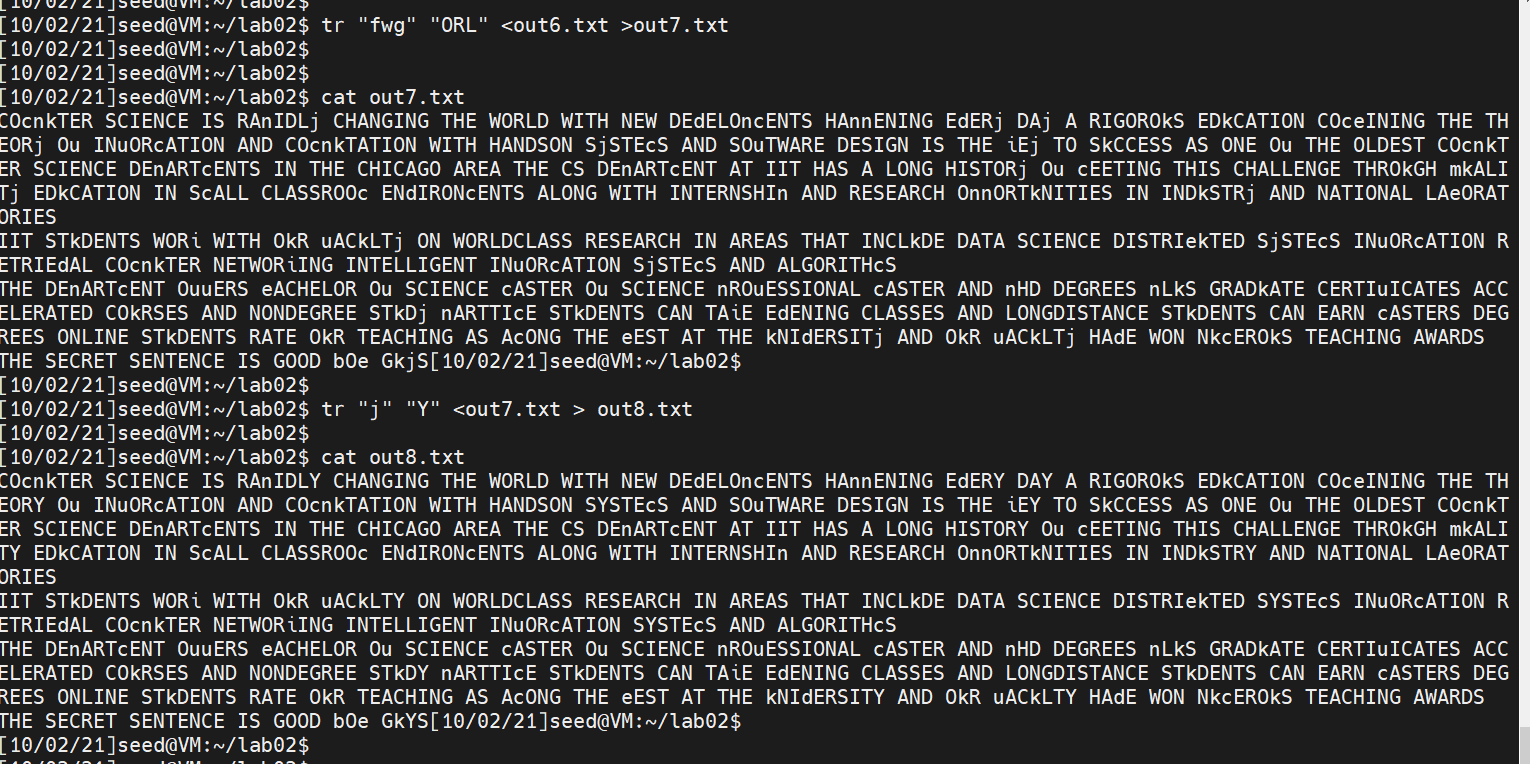
then， “ya“ 和”Aa” 作为两个字母的单词出现频率分别是7次和10次，并且根据单词“HAa”， 以及相邻DATA的单词“ahyENhE” 猜测为 DATA SCIENCE，可以比较明确a 的原文为”S”



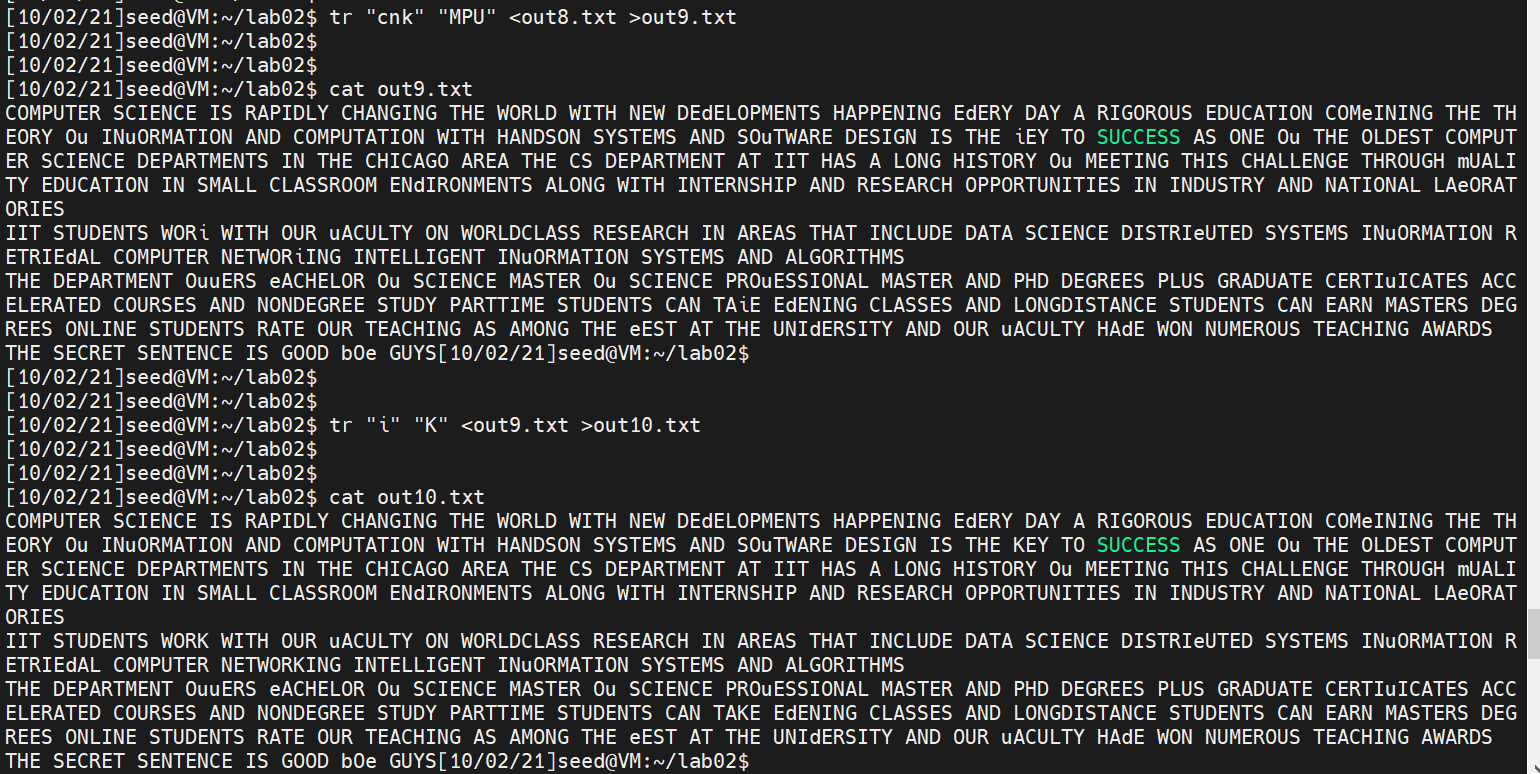
此时，原文已经有大部分字母被翻译出来，经过结合语境和上下文，根据单词“qITH”, 可以猜测 “q” 为”W“, 根据”CHANvINv” 猜测v 为“G”

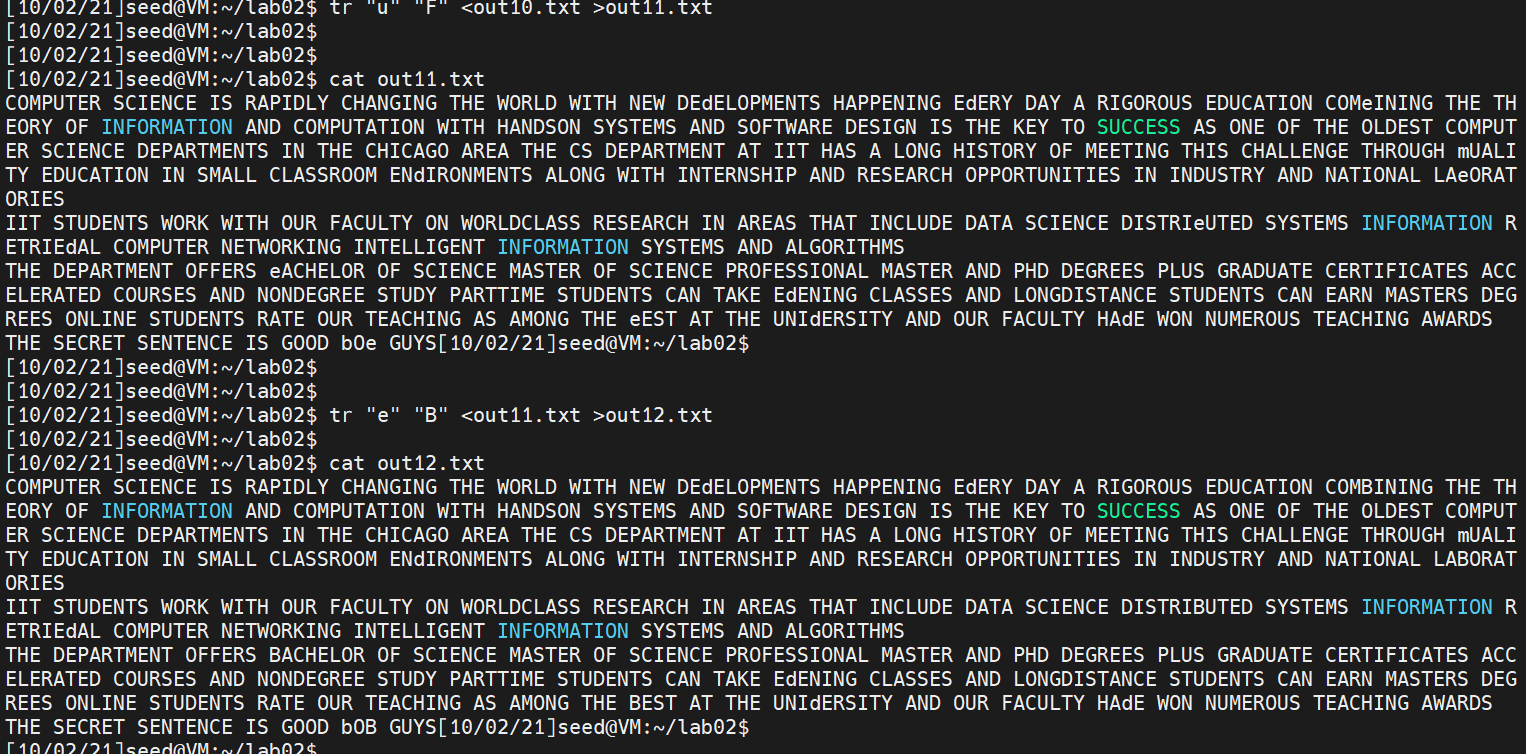


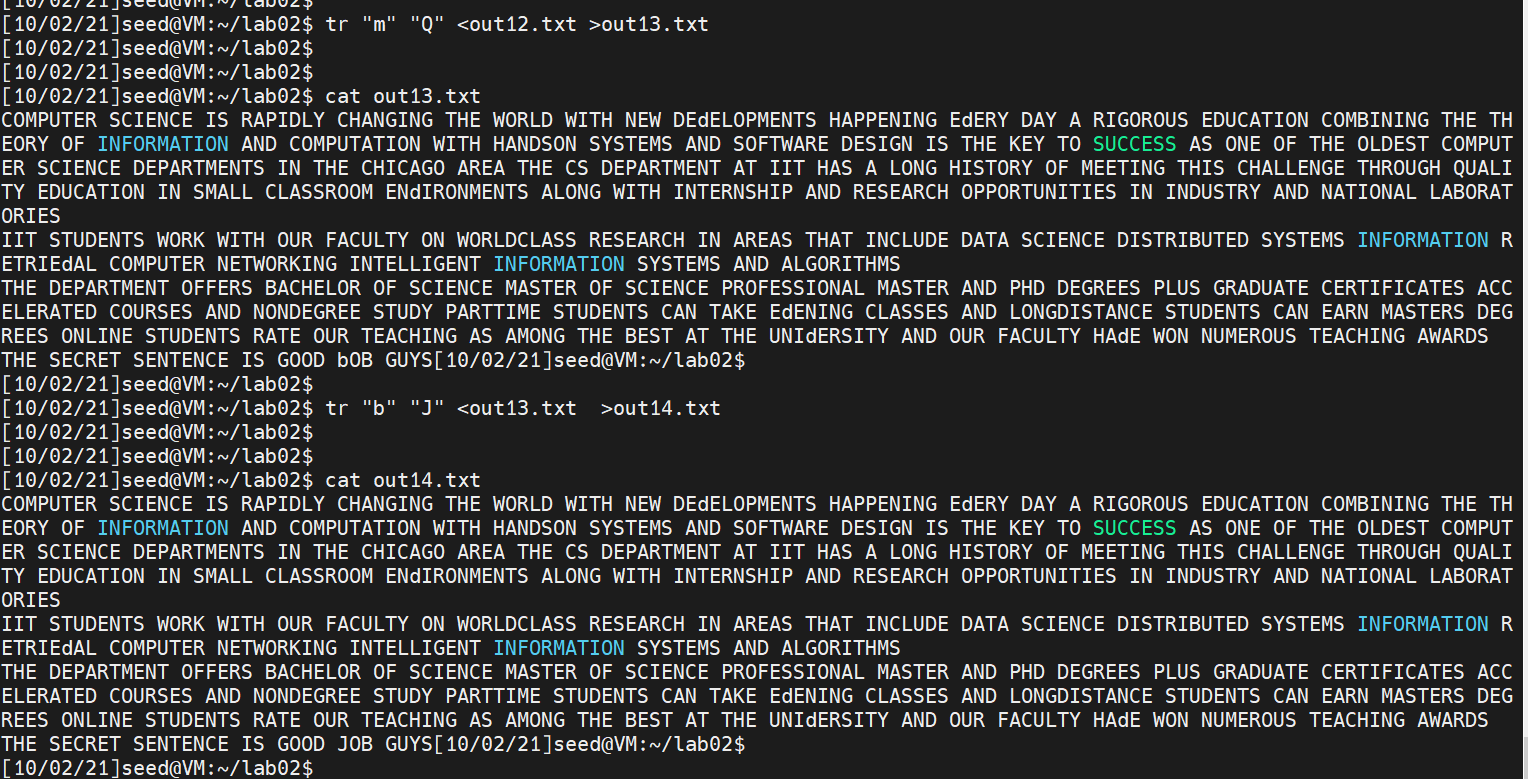
根据“WfwgD” 猜测 为“WORLD” DAj 猜测为DAY

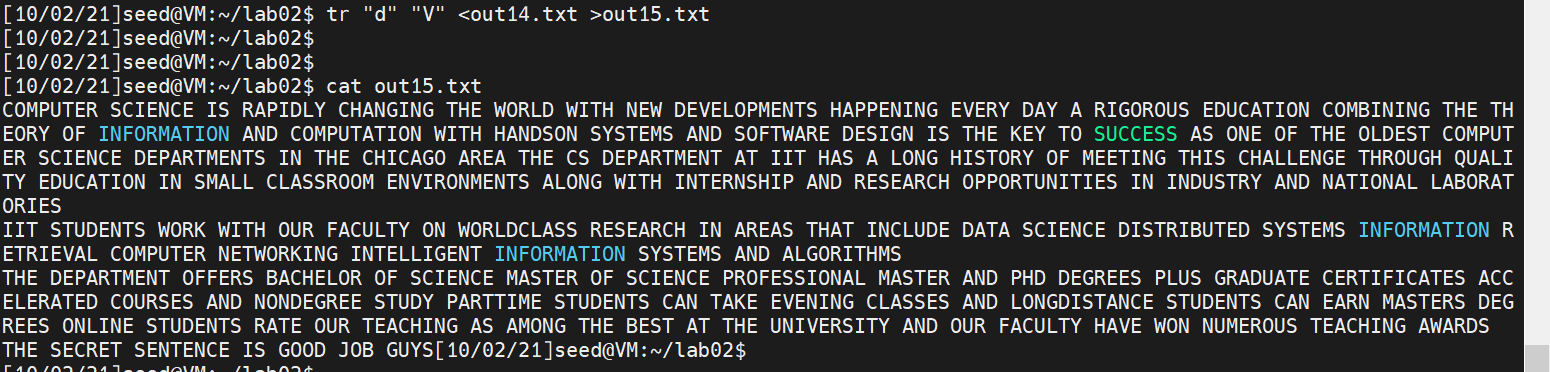


根据上下文，“COcnkTER SCIENCE” 猜测 cnk 为MPU, 后面同理根据上下文进行猜测









COMPUTER SCIENCE IS RAPIDLY CHANGING THE WORLD WITH NEW DEVELOPMENTS HAPPENING EVERY DAY A RIGOROUS EDUCATION COMBINING THE THEORY OF INFORMATION AND COMPUTATION WITH HANDSON SYSTEMS AND SOFTWARE DESIGN IS THE KEY TO SUCCESS AS ONE OF THE OLDEST COMPUTER SCIENCE DEPARTMENTS IN THE CHICAGO AREA THE CS DEPARTMENT AT IIT HAS A LONG HISTORY OF MEETING THIS CHALLENGE THROUGH QUALITY EDUCATION IN SMALL CLASSROOM ENVIRONMENTS ALONG WITH INTERNSHIP AND RESEARCH OPPORTUNITIES IN INDUSTRY AND NATIONAL LABORATORIES

IIT STUDENTS WORK WITH OUR FACULTY ON WORLDCLASS RESEARCH IN AREAS THAT INCLUDE DATA SCIENCE DISTRIBUTED SYSTEMS INFORMATION RETRIEVAL COMPUTER NETWORKING INTELLIGENT INFORMATION SYSTEMS AND ALGORITHMS

THE DEPARTMENT OFFERS BACHELOR OF SCIENCE MASTER OF SCIENCE PROFESSIONAL MASTER AND PHD DEGREES PLUS GRADUATE CERTIFICATES ACCELERATED COURSES AND NONDEGREE STUDY PARTTIME STUDENTS CAN TAKE EVENING CLASSES AND LONGDISTANCE STUDENTS CAN EARN MASTERS DEGREES ONLINE STUDENTS RATE OUR TEACHING AS AMONG THE BEST AT THE UNIVERSITY AND OUR FACULTY HAVE WON NUMEROUS TEACHING AWARDS

THE SECRET SENTENCE IS GOOD JOB GUYS

## TASK 2

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$ openssl enc -aes-128-cbc -e -in plain.txt -out cipher.bin -K 00010203040506070809aabbccddeeff -iv 0a0b0c0d0e0f010203040506070809

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$ xxd cipher.bin

00000000: e11f 1c04 5fb6 0146 b22f 3a51 e2f7 f491 ....\_..F./:Q....

00000010: b895 bf2a 001f e24a ce1a 31f2 48e1 4ed9 ...\*...J..1.H.N.

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$ openssl enc -aes-128-cfb -e -in plain.txt -out cipher.bin -K 00010203040506070809aabbccddeeff -iv 0a0b0c0d0e0f010203040506070809

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$ xxd cipher.bin

00000000: a4d9 ea90 48ea 2077 3773 2e40 7ca1 e99a ....H. w7s.@|...

00000010: 4784 920e eab6 45ee 2b78 5d G.....E.+x]

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$ openssl enc -bf-cbc -e -in plain.txt -out cipher.bin -K 00010203040506070809aabbccddeeff -iv 0a0b0c0d0e0f010203040506070809

[**10/02/21**]seed@VM:~/lab02$

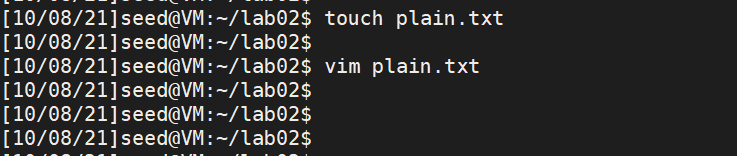
[**10/02/21**]seed@VM:~/lab02$ xxd cipher.bin

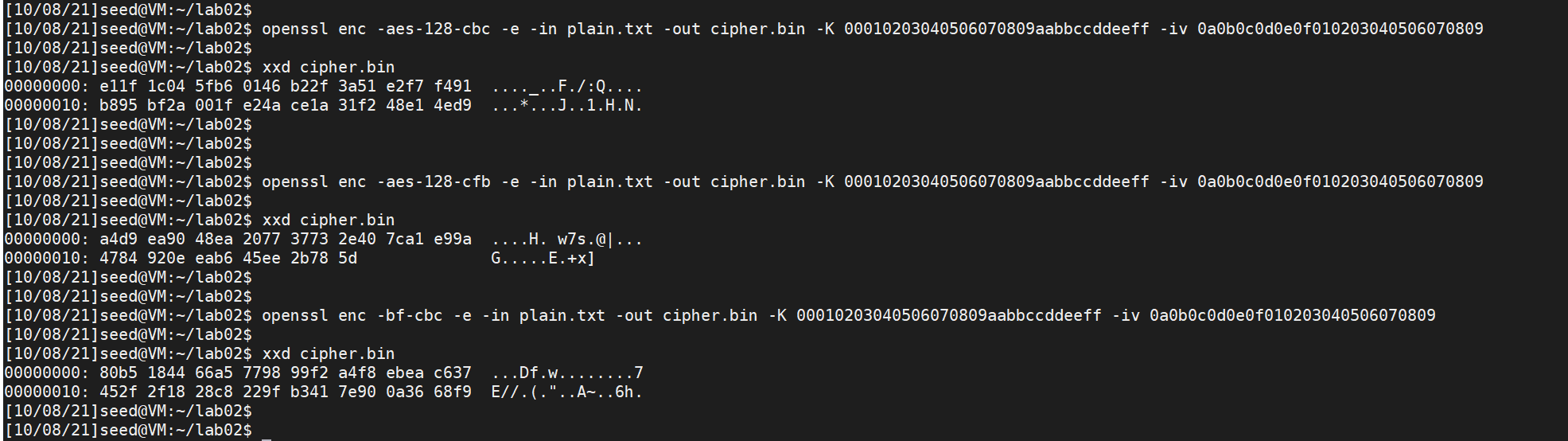
00000000: 80b5 1844 66a5 7798 99f2 a4f8 ebea c637 ...Df.w........7

00000010: 452f 2f18 28c8 229f b341 7e90 0a36 68f9 E//.(."..A~..6h.

[**10/02/21**]seed@VM:~/lab02$

[**10/02/21**]seed@VM:~/lab02$

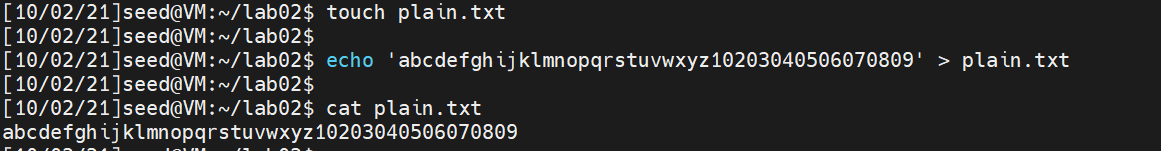




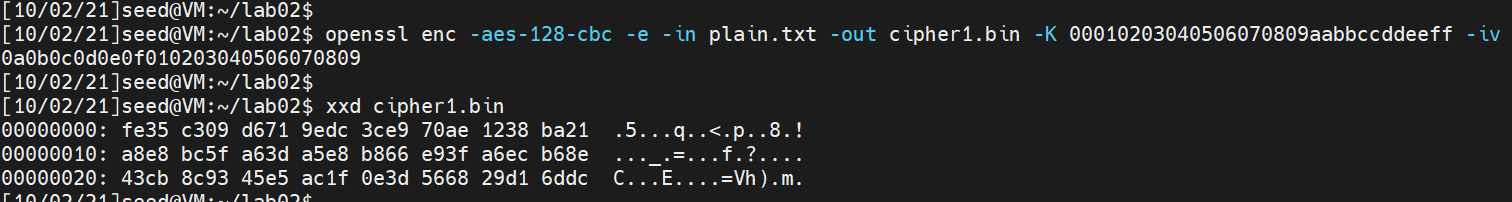
=====================上面的不要了==

use three different cipher type, such as -aes-128-cbc , -aes-128-cfb , -bf-cbc ,

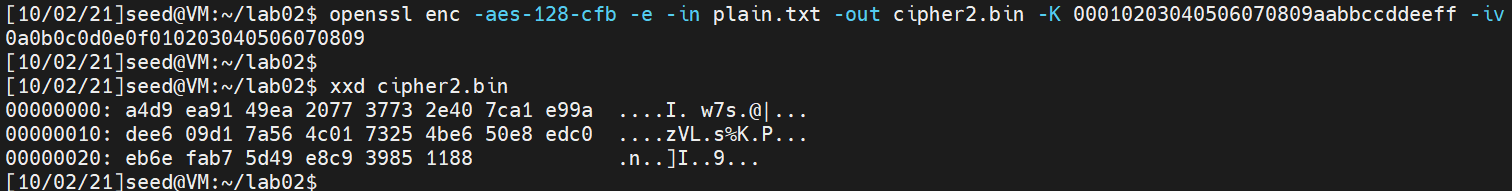
etc. In this task, you should try at least 3 di\_erent ciphers and three di\_erent mode



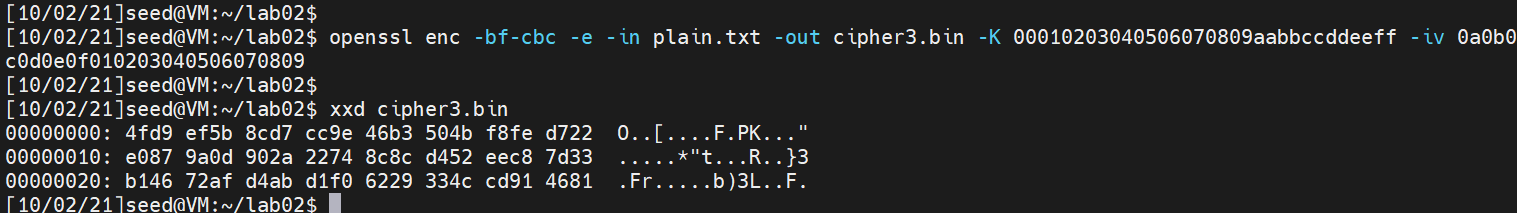
$ openssl enc -aes-128-cbc -e -in plain.txt -out cipher1.bin -K 00010203040506070809aabbccddeeff -iv 0a0b0c0d0e0f010203040506070809



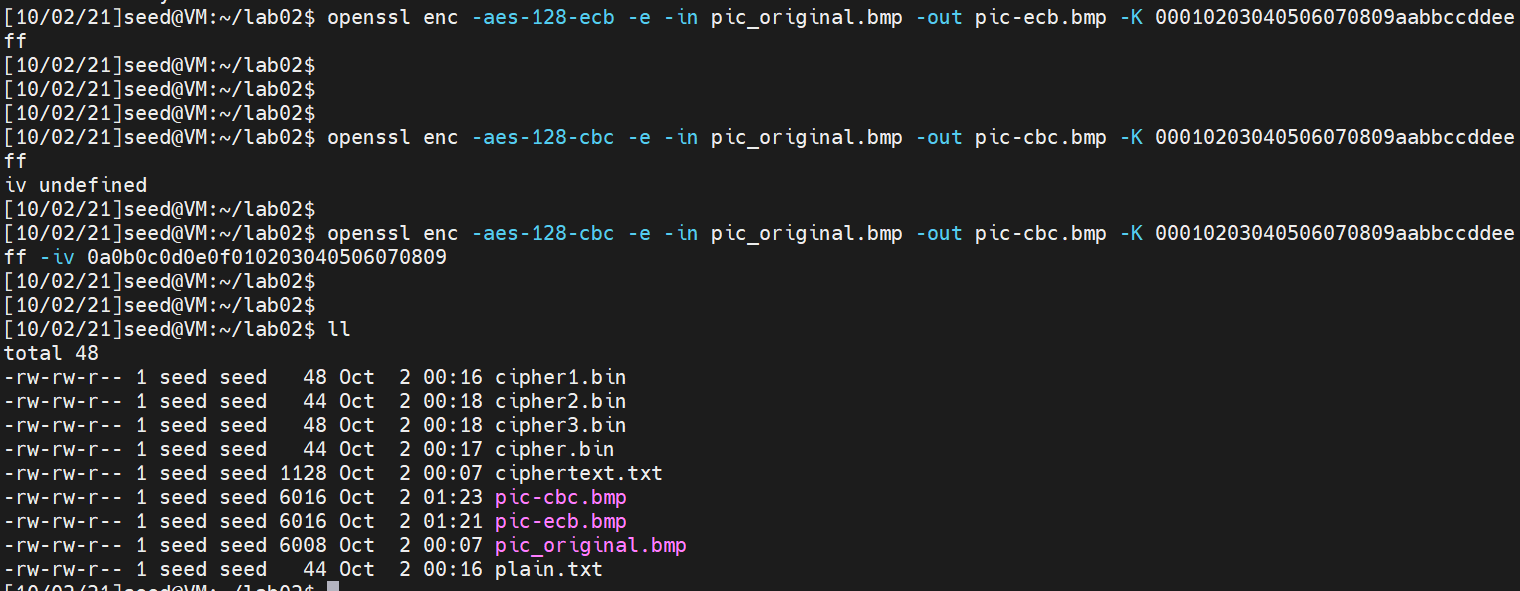
$ openssl enc -aes-128-cfb -e -in plain.txt -out cipher2.bin -K 00010203040506070809aabbccddeeff -iv 0a0b0c0d0e0f010203040506070809

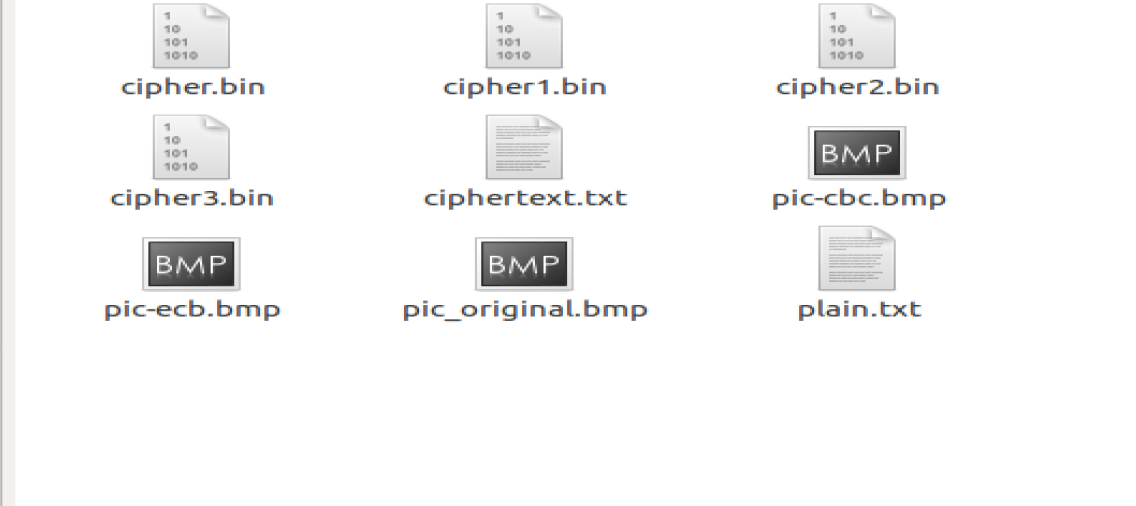


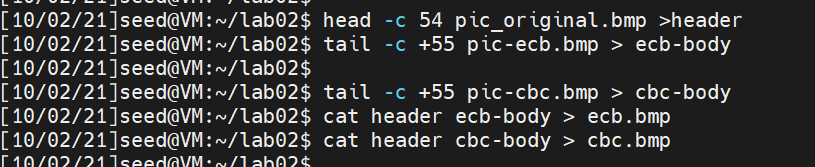
$ openssl enc -bf-cbc -e -in plain.txt -out cipher3.bin -K 00010203040506070809aabbccddeeff -iv 0a0b0c0d0e0f010203040506070809

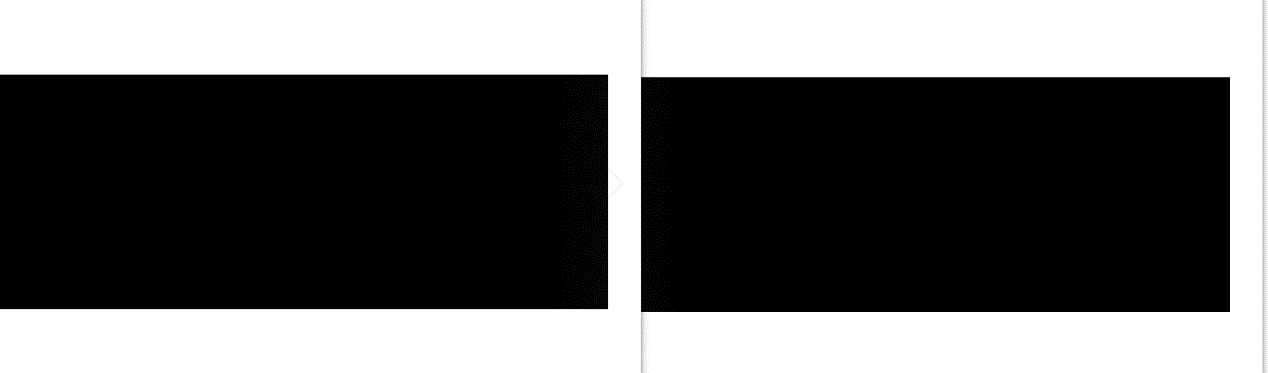


## TASK 3



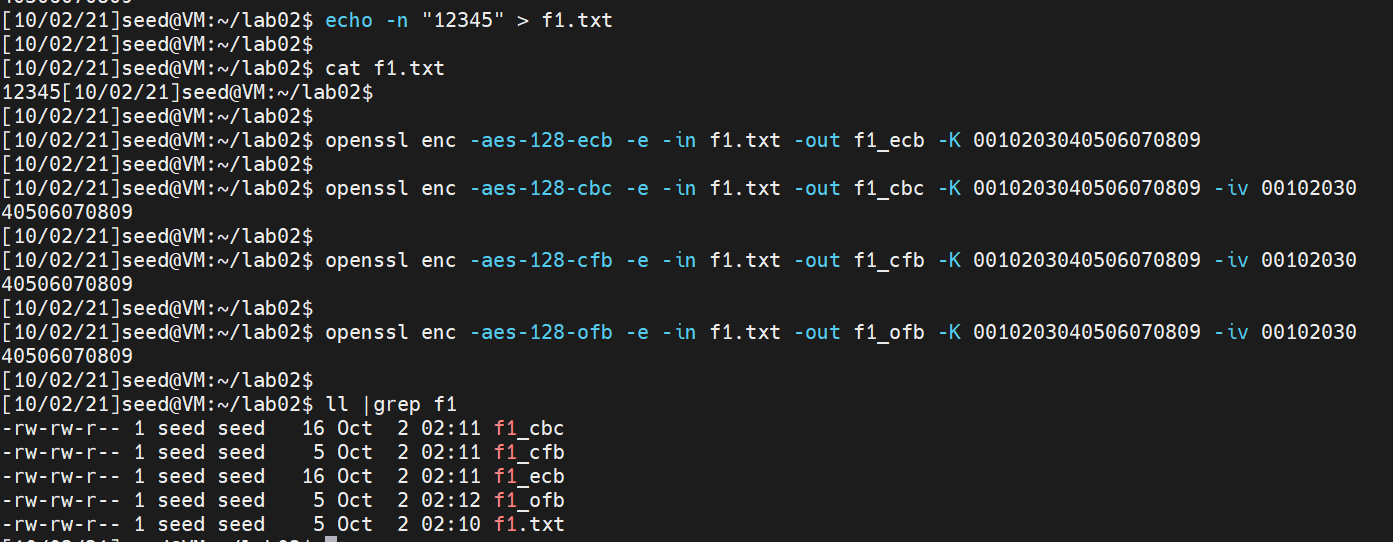






## TASK 4

.1. Use ECB, CBC, CFB, and OFB modes to encrypt a file (you can pick any cipher). Please report which modes have paddings and which ones do not. For those that do not need paddings, please explain why.



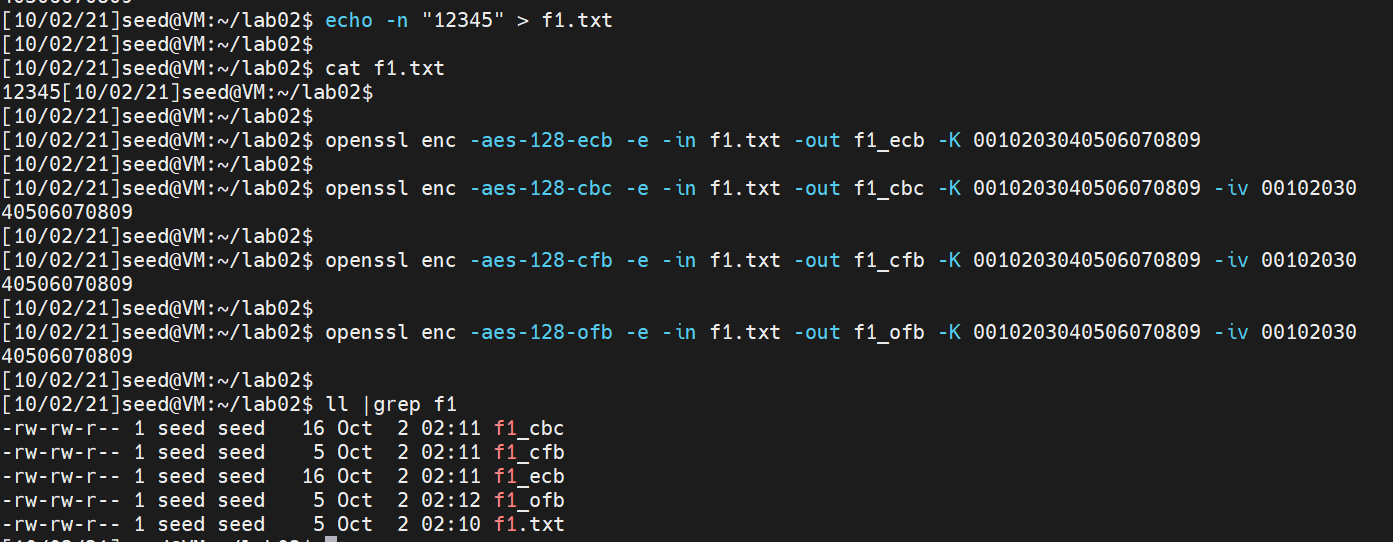
The size of f1\_cbc and f1\_ecb is 16 and others are 5 which is same as the original file f1.txt

So the encrypt mode CBC and ECB have paddings

And the encrypt mode CFB, OFB don’t have paddings.

2. Let us create three files, which contain 5 bytes, 10 bytes, and 16 bytes, respectively. We can use the following echo -n command to create such files.

(1) 5 bytes file.

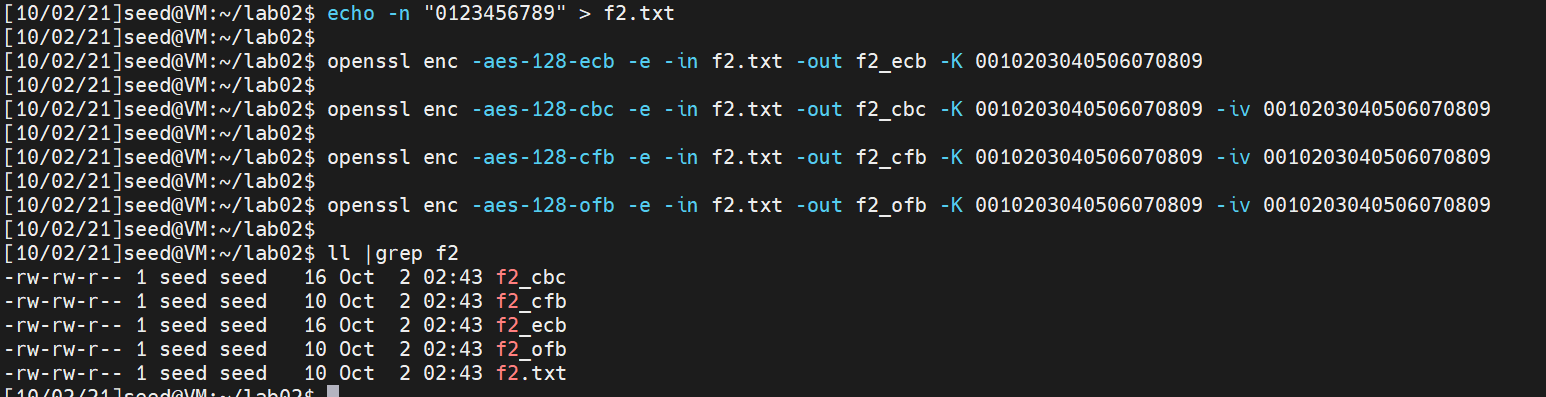


The size of f1\_cbc and f1\_ecb is 16 and others are 5 which is same as the original file f1.txt

So the encrypt mode CBC and ECB have paddings

And the encrypt mode CFB, OFB don’t have paddings.

(2) 10 bytes file

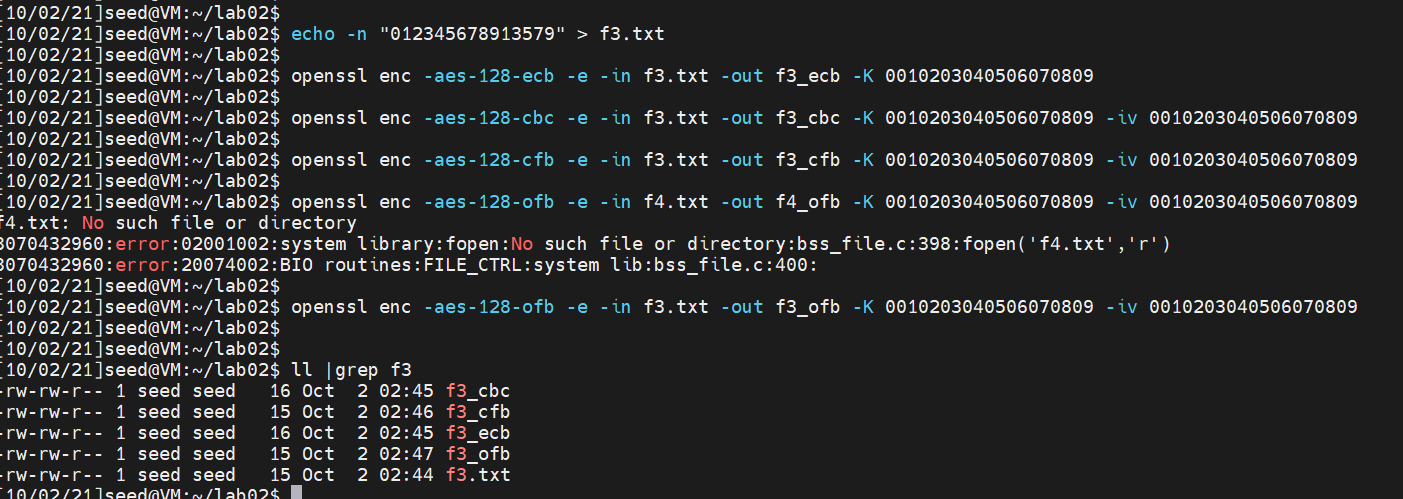


The size of f2\_cbc and f2\_ecb is 16 and others are 10 which is same as the original file f2.txt

So the encrypt mode CBC and ECB have paddings

And the encrypt mode CFB, OFB don’t have paddings.

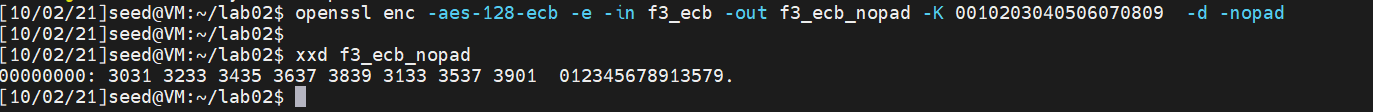
(3) 15 bytes file

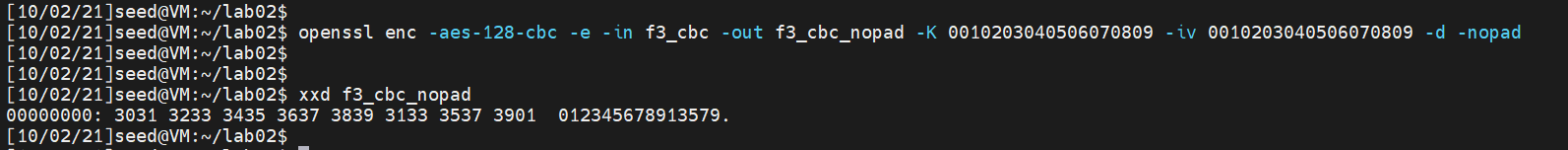


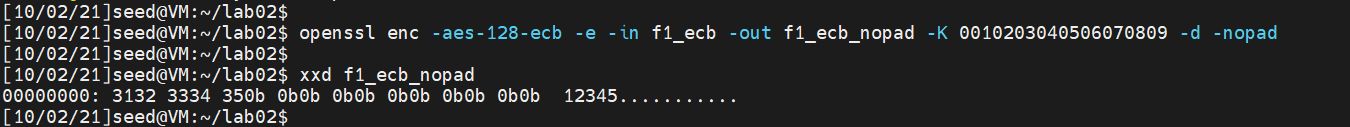
The size of f3\_cbc and f3\_ecb is 16 and others are 15 which is same as the original file f3.txt

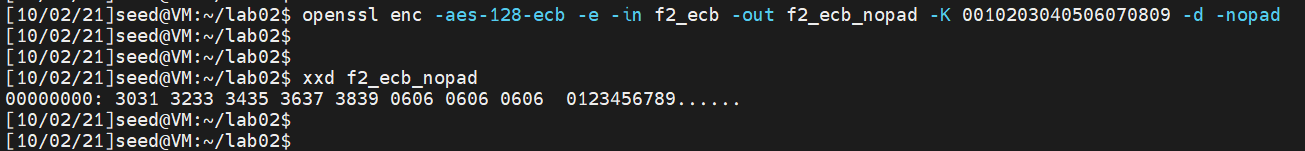
So the encrypt mode CBC and ECB have paddings

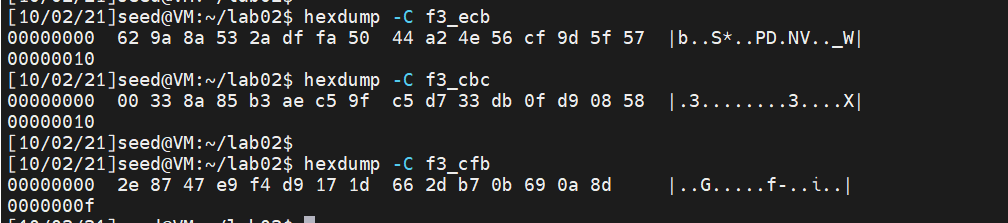
And the encrypt mode CFB, OFB don’t have paddings.





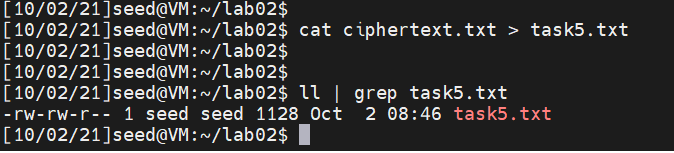




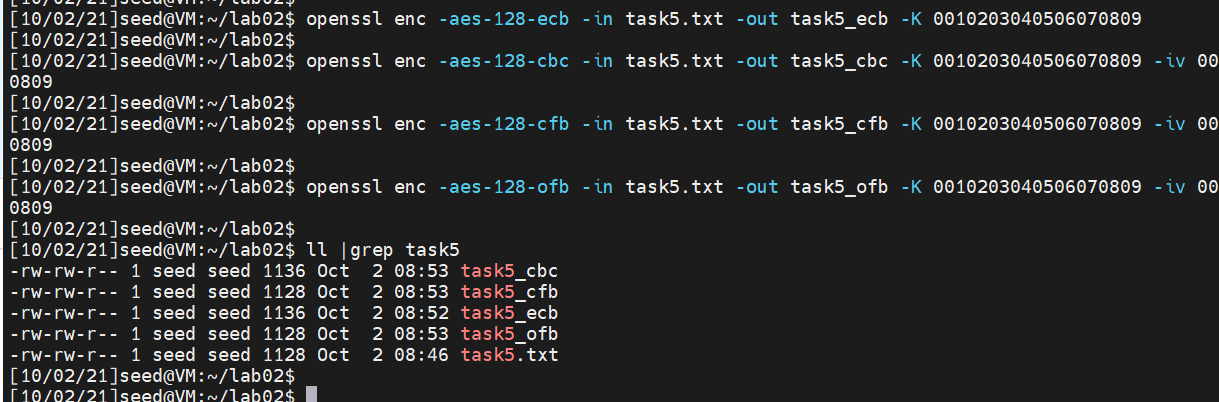


TASK 5

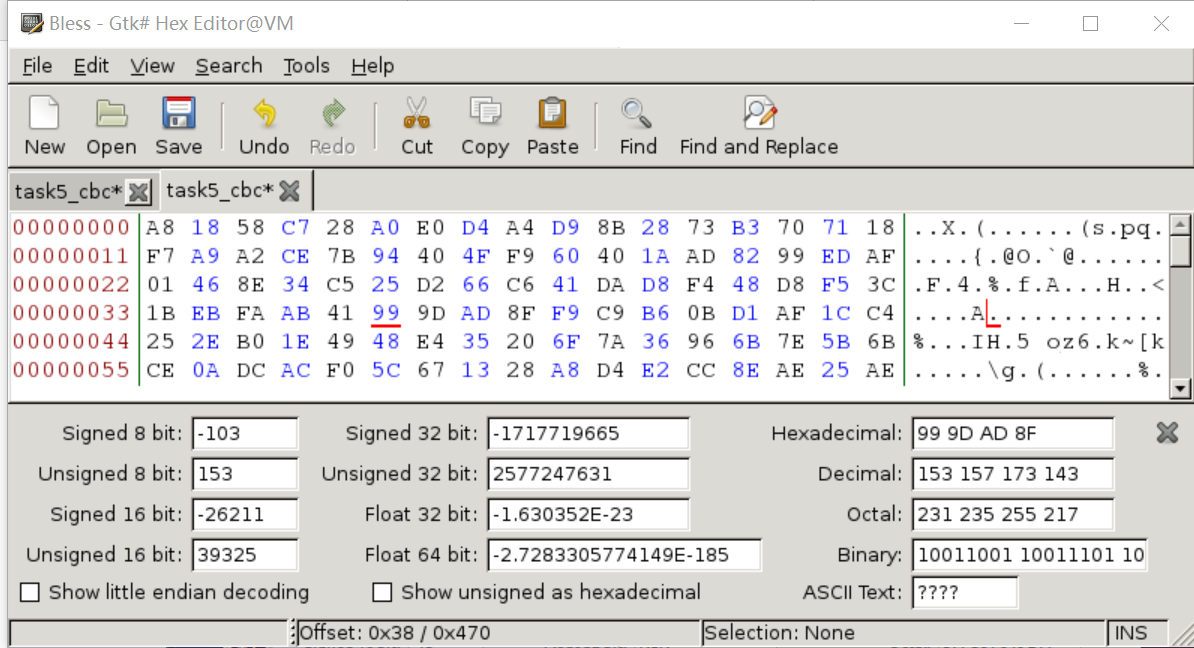
Using ciphertext content into task5.txt, the size is 1128, it’s more than 1000 bytes.

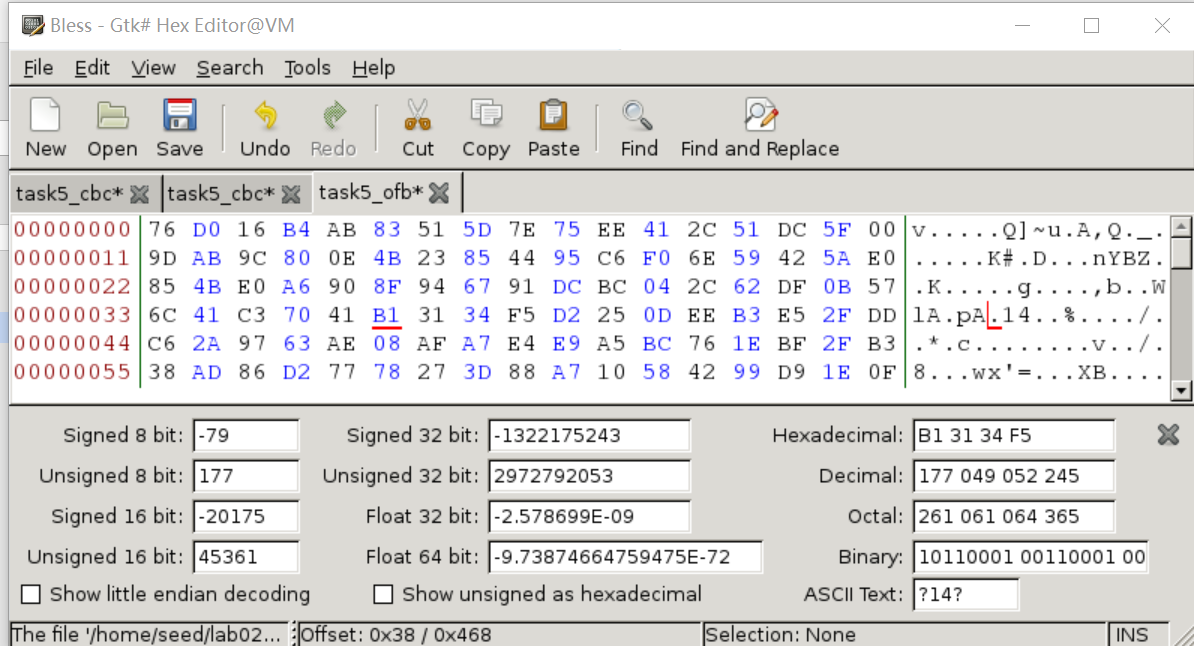


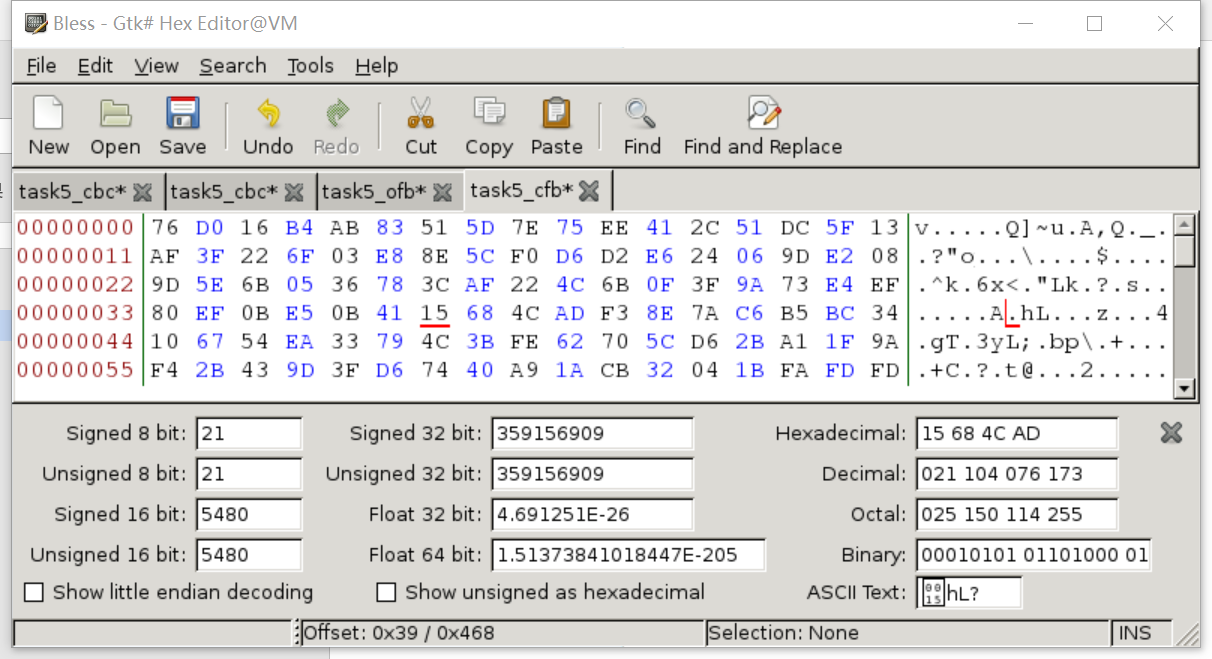
Use ecb, cbc, cfb, ofb encrypt file task5.txt

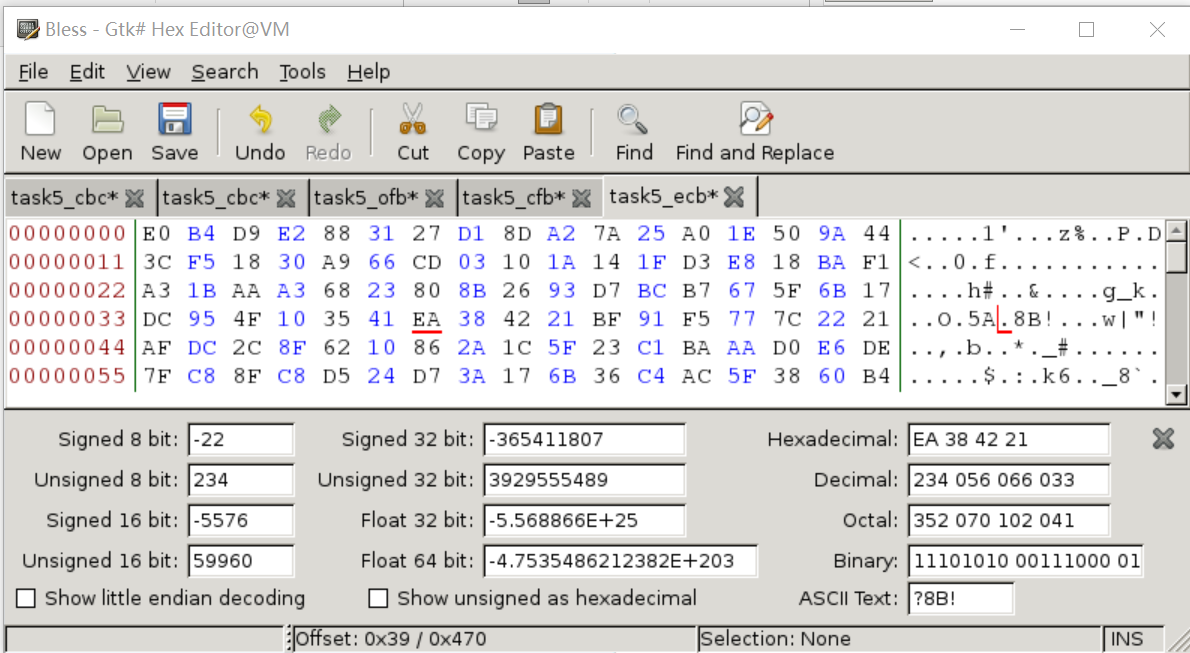


Using the bless hex editor, a single bit of the 55th byte in the encrypted file got corrupted. It becomes “A”

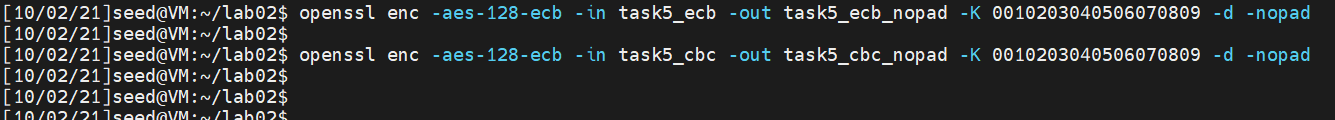


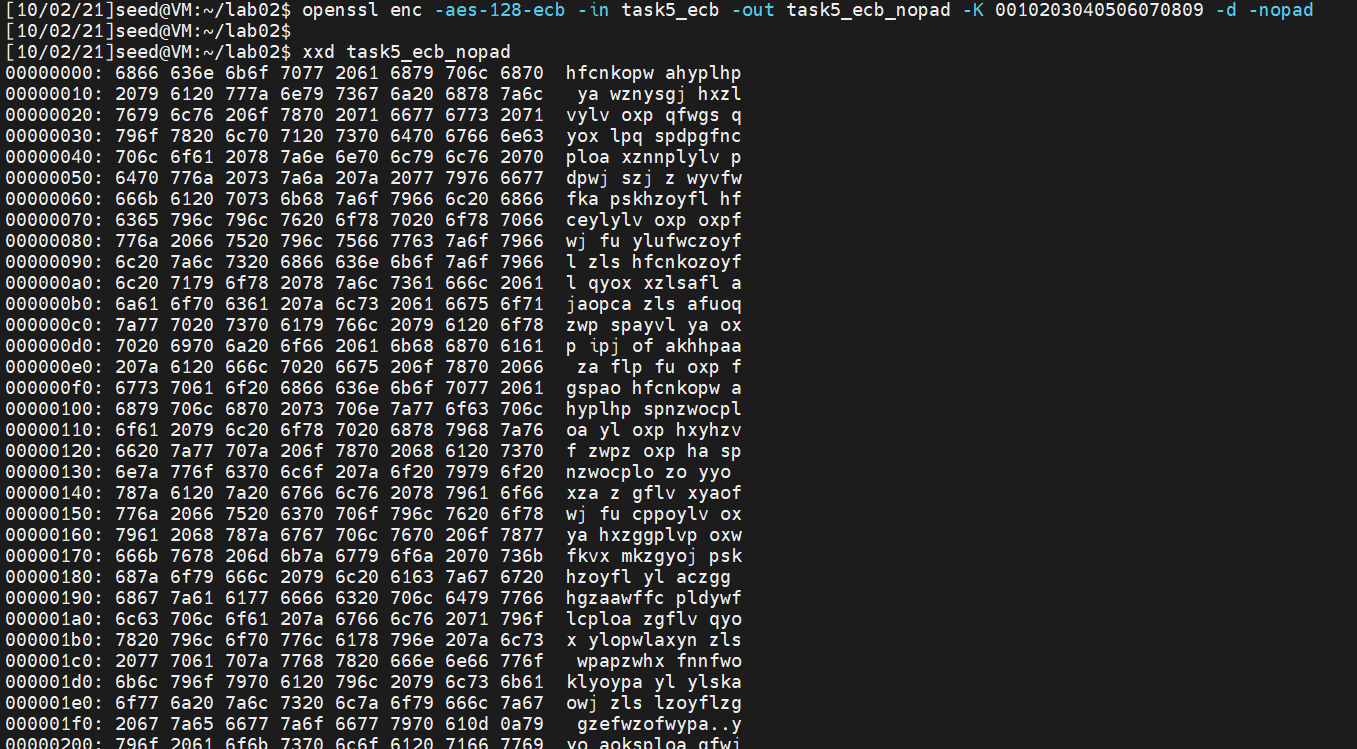






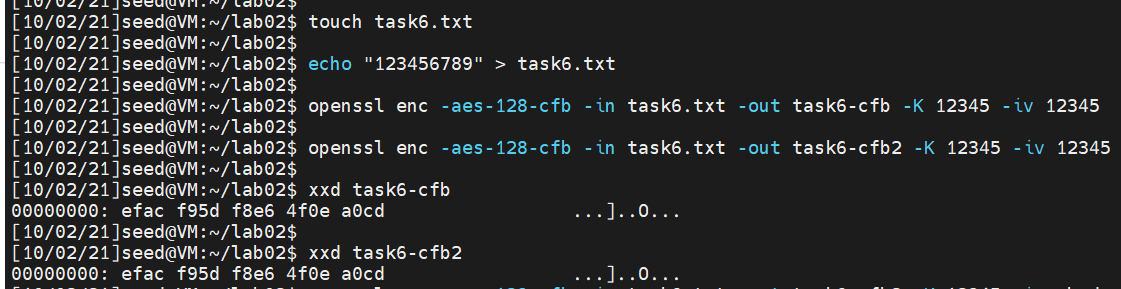
Decrypt the corrupted ciphertext file using the correct key and IV





## TASK 6

Using same ivs, get the same encrypt result.



Using different iv, then get different encrypt result.

