F20CN – Computer Network Security.

Coursework 1.

By Daniyar Nazarbayev (H00204990).

Table of Contents

1.Introduction.

I used a virtual machine to run linux. Specifically, VMware and latest version of CentOS. My openssl version was 1.0.2k-fips and I used emacs for hexadecimal editing.

2. Part 1

My first action was to just take the letter frequencies of the cipher, and match them to the real letter frequencies of english language. That of course did not work, otherwise it would be too easy. I did the same with bigram and trigram letter frequencies, only using the top 10 from the list and matching them to their corresponding letters (which I got from wikipedia). But no meaningful result came. I have came to realize that different texts have different letter frequencies, and just trying to match letters as is would not always work. There will always be a few letters in the wrong position.

I did notice though that letters “ytn” looked a lot like “the” though. That left me with 23 more letters, but everything else was gibberish. Considering the complexity of 23 factorial, I decided not to bother and looked for an alternative. Considering how old this crypto method is, there is probably a de facto way of solving this. That is how I stumbled on this.

https://www.ti89.com/cryptotut/mono_crack.htm

It gave me a step by step tutorial on how to crack the cipher. It said that you first have to look for “the”, the most frequent three-letter word in english language, and then start from there. Once you know the “the”, you can easily find words like there, this, than, thus, that. With each new letter you uncover, the words in the text will become more clearer, to the point where you just have to feel the gap (which gives you a new letter). It sort of felt like solving a sudoku puzzle, and just like sudoku, if you make a mistake, you have to backtrack.

Encryption Table.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C	F	M	Y	P	V	B	R	L	Q	X	W	I	E	J	D	S	G	K	H	N	A	Z	O	T	U

3. Part 2

I picked AES, RC5 and Blowfish ciphers for this part. Each of them running in CBC, OFB and CFB modes. I checked the wikipedia page for the key size and block size (for IV) lengths. I also used a hexadecimal random generator site to create the data for me.

1. AES CBC

openssl enc -aes-128-cbc -base64 -e -in plain.txt -out cipher1.txt -K 00112233445566778889aabbccddeeff -iv 2af543a44e839a4e2dcca19553df062b

```
il/1BNNNcBP/z01MrGQDGQOsOmdzEAe7sZBk6+vOFXw=
```

2. AES CFB

openssl enc -aes-128-cfb -base64 -e -in plain.txt -out cipher2.txt -K 6c3c15acfc4cbef389754fc31a0a06f6 -iv 9f5a0adc2122040629d99e5601c96364

```
ERoG7KQYhqTZFMD3OmNPAyZamWe+0g==
```

3. AES OFB

openssl enc -aes-128-ofb -base64 -e -in plain.txt -out cipher3.txt -K 3c214f905e025ae2116cd42d1bb63c55 -iv 0fe756eaa21b95794585533f0a67bc9d

```
4CeKBIzQ8yqbsAT7mjNZSG48tsTESQ==
```

4. RC5 OFB

openssl enc -rc5-ofb -base64 -e -in plain.txt -out cipher4.txt -K e44770db9e8ecd5f7ec879f1551d53a6 -iv 231db96643f869a5d1566d3d159aa3a5

```
n+7TcM/wgNdJxormKLtQz3QwQcGbXQ==
```

5. RC5 CBC

openssl enc -rc5-cbc -base64 -e -in plain.txt -out cipher5.txt -K 9b4b4c4517f3f6b0fb2108fba2db761e -iv 3a645c14a2c24c8958f7a699f8d8294b

```
LTB0nRz/7VcKU9jdJl7jlGLGLnZKURrW
```

6. RC5 CFB

openssl enc -rc5-cfb -base64 -e -in plain.txt -out cipher6.txt -K 8204d3d2dc1dc3bc4214d132b8e9ad37 -iv 8d27ce06eb3e8db0b2c9c2b6b46b8669

```
V9oJPQhMtwczp7+Mz/tHa207SeC6zg==
```

7. BF CBC

openssl enc -bf-cbc -base64 -e -in plain.txt -out cipher7.txt -K ac7c93b390258f7d3a718e70134ccb54 -iv 1065d5bbb630aee4

```
2UfDr6yFBbNASpUlz0iTy/L+cILvphf0
```

8. BF CFB

openssl enc -bf-cfb -base64 -e -in plain.txt -out cipher8.txt -K 17c9e1f7c316cc3daeec2e8978ef84d8 -iv 2bdaadf0464602f7

```
csnzJxoY4ZJj7WNMd81EJzokVuVgLQ==
```

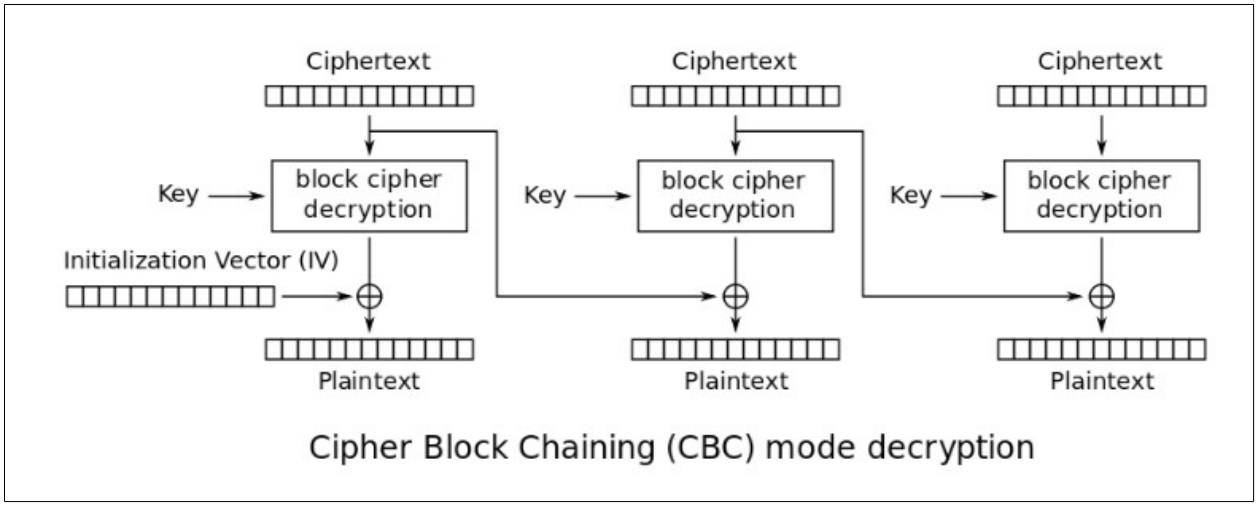
9. BF OFB

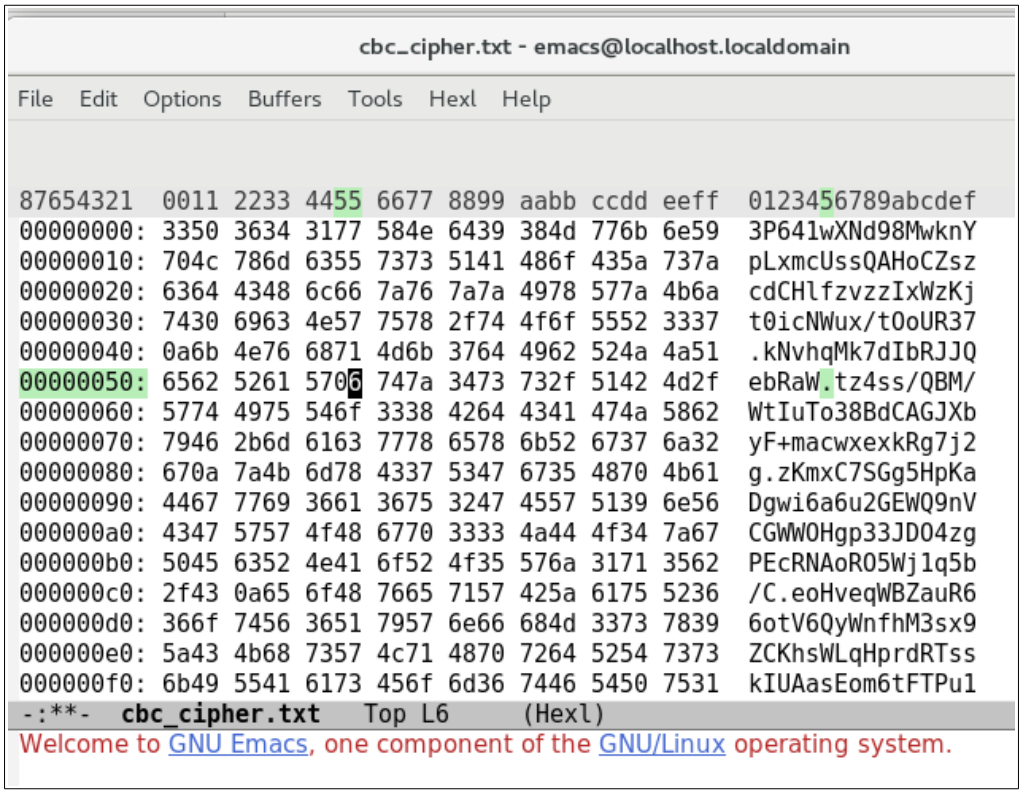
openssl enc -bf-ofb -base64 -e -in plain.txt -out cipher9.txt -K 17c9e1f7c316cc3daeec2e8978ef84d8 -iv 270d8bc234a259a4

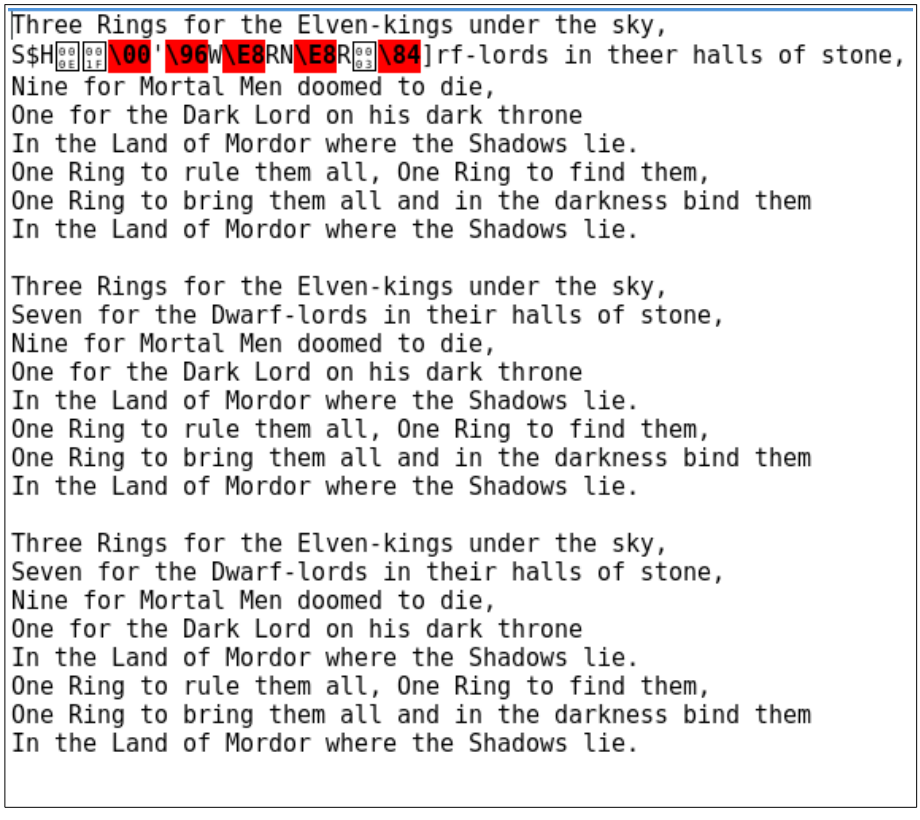
```
IPzp11QIK1UC7TtQSHWUaeyoYTMc2A==
```

4. Task 3

1. CBC
According to the diagram I found in wikipedia, I assumed that 2 blocks are going to get corrupted. The ciphertext block where we change the bit, and the block following it, because the ciphertext value is XORed with the next block, and since it is flawed, it will give inaccurate results.

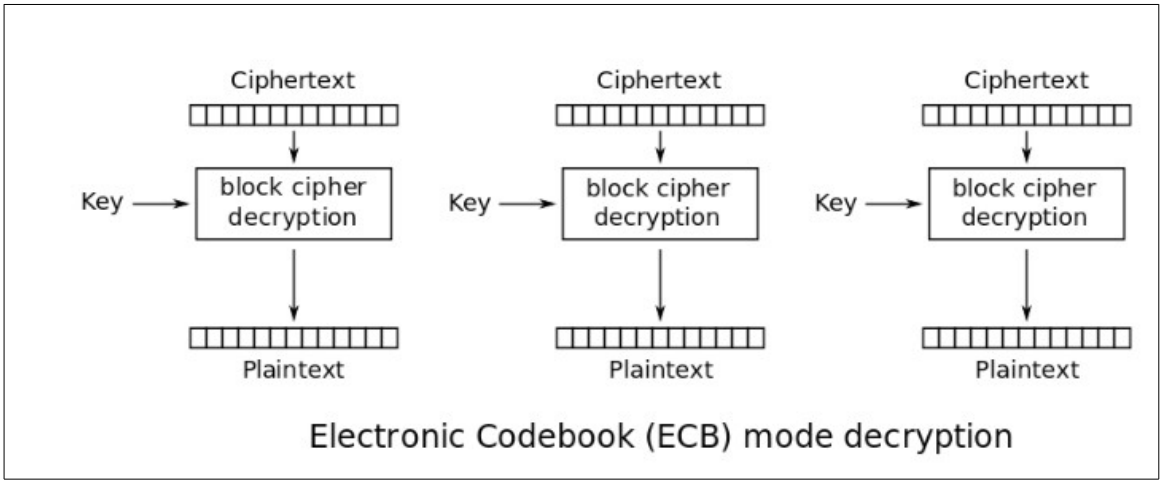



cbc_cipher.txt - emacs@localhost.localdomain
File Edit Options Buffers Tools Hexl Help
87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
00000000: 3350 3634 3177 584e 6439 384d 776b 6e59 3P641wXNd98MwknY
00000010: 704c 786d 6355 7373 5141 486f 435a 737a pLxmcUssQAHoCZsz
00000020: 6364 4348 6c66 7a76 7a7a 4978 577a 4b6a cdCHlfzvzzIxWzKj
00000030: 7430 6963 4e57 7578 2f74 4f6f 5552 3337 t0icNWux/tOoUR37
00000040: 0a6b 4e76 6871 4d6b 3764 4962 524a 4a51 .kNvhqMk7dIbRJJQ
00000050: 6562 5261 5706 747a 3473 732f 5142 4d2f ebRaW.tz4ss/QBM/
00000060: 5774 4975 546f 3338 4264 4341 474a 5862 WtIuTo38BdCAGJXb
00000070: 7946 2b6d 6163 7778 6578 6b52 6737 6a32 yF+macwxexkRg7j2
00000080: 670a 7a4b 6d78 4337 5347 6735 4870 4b61 g.zKmxC7SGg5HpKa
00000090: 4467 7769 3661 3675 3247 4557 5139 6e56 Dgwi6a6u2GEWQ9nV
000000a0: 4347 5757 4f48 6770 3333 4a44 4f34 7a67 CGWWOHgp33JDO4zg
000000b0: 5045 6352 4e41 6f52 4f35 576a 3171 3562 PEcRNAoRO5Wj1q5b
000000c0: 2f43 0a65 6f48 7665 7157 425a 6175 5236 /C.eoHveqWBZauR6
000000d0: 366f 7456 3651 7957 6e66 684d 3373 7839 6otV6QyWnfhM3sx9
000000e0: 5a43 4b68 7357 4c71 4870 7264 5254 7373 ZCKhsWLqHprdRTss
000000f0: 6b49 5541 6173 456f 6d36 7446 5450 7531 kIUAasEom6tFTPu1
-:**- cbc_cipher.txt Top L6 (Hexl)
Welcome to GNU Emacs, one component of the GNU/Linux operating system.


Three Rings for the Elven-kings under the sky,
S$H\00'\96w\E8RN\E8R\84]rf-lords in theer halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.
Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.
Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

2. ECB

Again, according to the diagram, it looks like only 1 block will get corrupted.

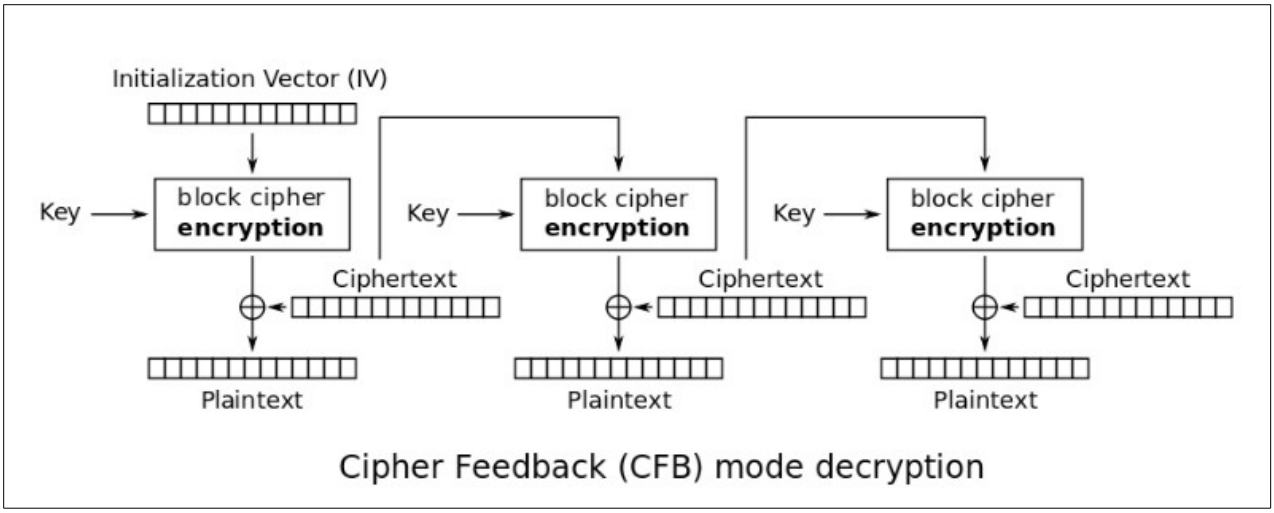



```
87654321  0011 2233 4455 6677 8899 aabb ccdd eeff  0123456789abcdef
00000000: 2f42 7856 6565 6e4d 4d59 4242 7048 4245  /BxVeenMMYBBpHBE
00000010: 5575 7955 7347 6358 4e35 315a 3268 3538  UuyUsGcXN51Z2h58
00000020: 366d 5471 4565 4844 6f59 2f68 2f2b 5341  6mTqEeHDoY/h/+SA
00000030: 3547 445a 5a56 7049 2f49 6e54 6541 7364  5GDZZVpI/InTeAsd
00000040: 0a75 7450 6134 6235 536a 3038 3755 4c64  .utPa4b5Sj087ULd
00000050: 6a4c 3677 326b 7865 387a 4e63 3475 736b  jL6w2kxe8zNc4usk
00000060: 6338 497a 656f 444c 4859 5838 3572 3467  c8IzeoDLHYX85r4g
00000070: 3074 7638 346d 596c 6761 6373 5074 7a39  0tv84mYlgacsPtz9
00000080: 380a 6930 3970 314f 6379 4773 4832 2f55  8.i09p1OcyGsH2/U
00000090: 6774 6679 3557 6a68 3779 2f6b 4952 7751  gtfy5Wjh7y/kIRwQ
000000a0: 5064 686c 6c73 4868 656c 416d 5146 7349  PdhllsHhelAmQFsI
000000b0: 4552 6b64 4f71 4866 646e 4570 624f 7765  ERkdOqHfdnEpbOwe
000000c0: 4d64 0a66 5279 4173 674f 5a4f 6e5a 6a72  Md.fRyAsgOZOnZjr
000000d0: 325a 3458 792b 2b79 6b56 3847 4241 5256  2Z4Xy++ykV8GBARV
000000e0: 6556 3656 4856 7048 557a 6249 6843 436b  eV6VHVpHUzbIhCCk
-:---  ecb_cipher.txt   Top L6     (Hexl)
Welcome to GNU Emacs, one component of the GNU/Linux operating system.
To follow a link, click Mouse-1 on it, or move to it and type RET.
To quit a partially entered command, type Control-g.

Important Help menu items:
Emacs Tutorial          Learn basic Emacs keystroke commands
Read the Emacs Manual   View the Emacs manual using Info
```

```
Three Rings for the Elven-kings under the sky,
S
|ãËP>_l@Ö$Árf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.
```

3. CFB

I think that 2 blocks will get corrupted. One because of the first XOR, and the second one that goes in the block cipher and XORed with the next cipher block (which is correct). That said, the issues stop there.

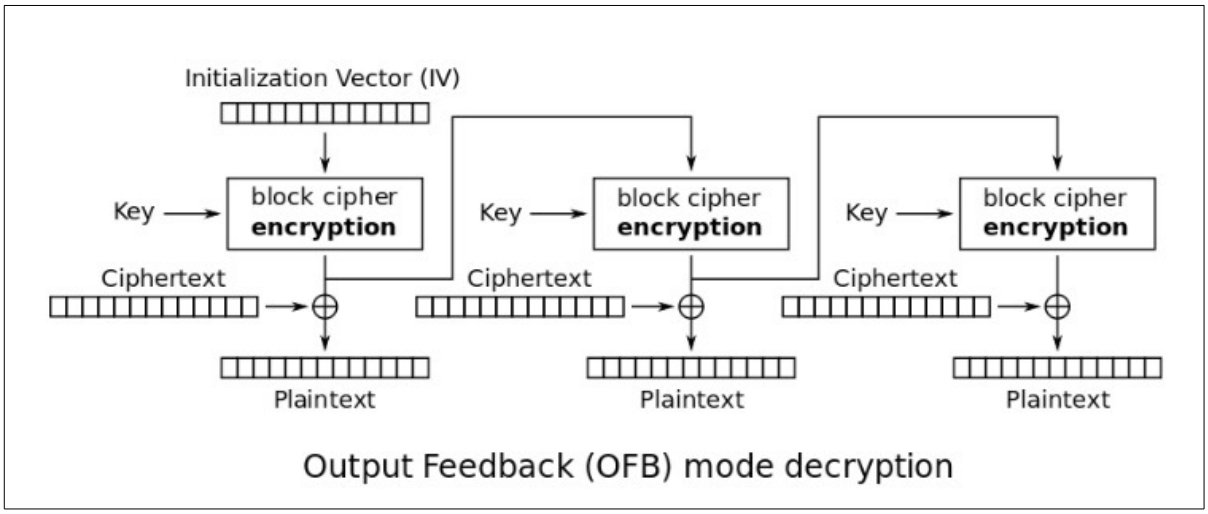


```
Three Rings for the Elven-kings under the sky,
Seven for the Dwq□□bÕ□□©□□€□□i□□É□□□□þð1r halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.
```

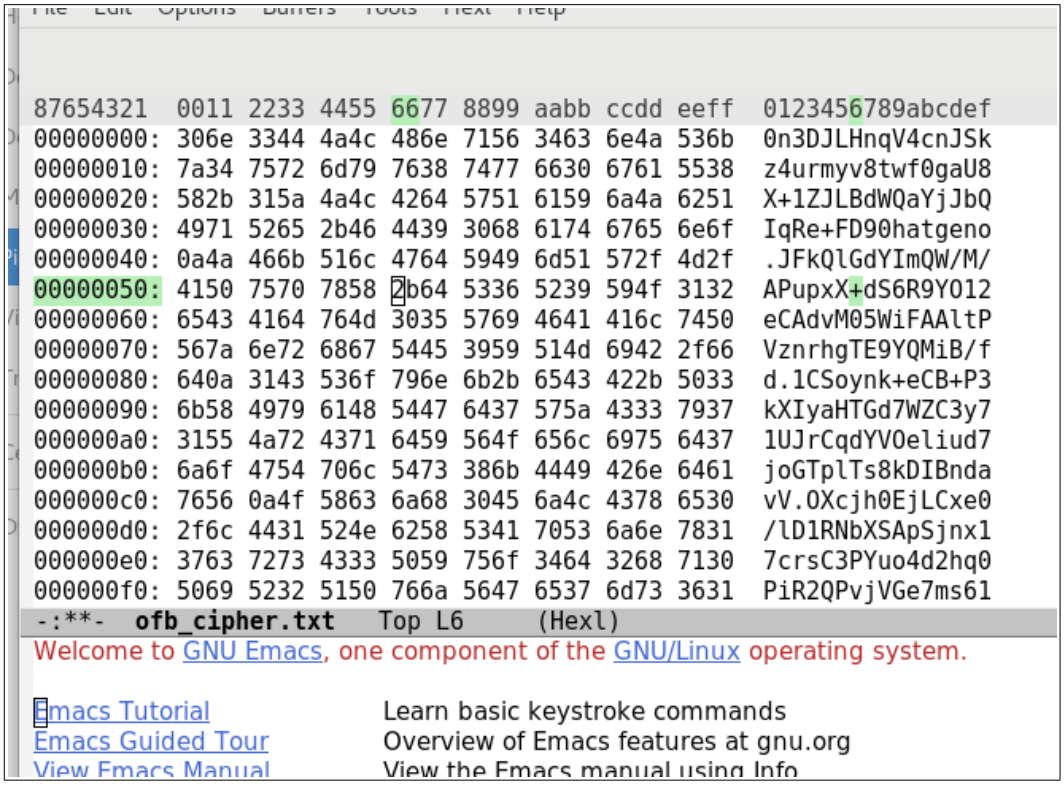
```
87654321  0011 2233 4455 6677 8899 aabb ccdd eeff  0123456789abcdef
00000000: 7559 326a 7430 342f 6464 774b 4674 3643  uY2jt04/ddwKFt6C
00000010: 6970 6632 6c33 3039 3767 2f39 6231 4a4e  ipf2l3097g/9b1JN
00000020: 6364 4543 6738 6f53 2f49 6578 4233 6c6d  cdECg8oS/IexB3lm
00000030: 3063 5951 4476 5964 5059 4851 2f30 6b64  0cYQDvYdPYHQ/0kd
00000040: 0a4a 6978 3739 3945 2f7a 436a 4b61 6433  .Jix799E/zCjKad3
00000050: 4d73 3565 5039 4634 3775 6672 2b51 6d71  Ms5eP9F47ufr+Qmq
00000060: 3464 4875 774b 4e46 4d46 5a79 6142 6953  4dHuwKNFMFZyaBiS
00000070: 3356 4974 6541 514e 7850 442f 3936 3831  3VIteAQNxPD/9681
00000080: 580a 2b33 3143 716f 586f 4530 3943 7165  X.+31CqoXoE09Cqe
00000090: 7439 4c73 4b37 4e71 6956 3958 7852 7831  t9LsK7NqiV9XxRx1
000000a0: 5063 3549 524a 3873 6375 4171 5838 5958  Pc5IRJ8scuAqX8YX
000000b0: 6556 6e43 7533 454b 6370 6b42 4b7a 5133  eVnCu3EKcpkBKzQ3
000000c0: 6835 0a58 7369 7178 4748 6238 7a79 7054  h5.XsiqxGHb8zypT
000000d0: 6135 4777 7955 5435 7543 6d46 3067 6b70  a5GwyUT5uCmF0gkp
000000e0: 6b75 5031 6b57 364e 6339 6930 5373 3142  kuP1kW6Nc9i0Ss1B
000000f0: 6a53 535a 4352 3149 6459 5870 7549 2f32  jSSZCR1IdYXpuI/2
-:---  cfb_cipher.txt   Top L6     (Hexl)
Welcome to GNU Emacs, one component of the GNU/Linux operating system.

Emacs Tutorial          Learn basic keystroke commands
Emacs Guided Tour       Overview of Emacs features at gnu.org
View Emacs Manual       View the Emacs manual using Info
```

4. OFB

It looks like only 1 block will get corrupted. IV and key are used to create the keysteam, in complete isolation of the ciphertext (where one of the blocks is corrupted), and when the keystream is XORed to the ciphertext, only that corrupted block will stay corrupted. Actually, since we only changed 1 bit overall, there should be only 1 character that is different, which appears to be the case (Dwarf to Dwerf).




```
Three Rings for the Elven-kings under the sky,
Seven for the Dwerf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.
```



5. Task 4

This task was pretty straight forward. 2 ciphers are using the same IV, and we have the plaintext of 1 of the ciphers. By knowing the ciphertext and the plaintext, we can find the keystream of that cipher (by XORing), and then we can XOR the keystream with the ciphertext to get plaintext of the second cipher.

What I found weird was that the XOR just worked. That means that both the IV and the key were the same, and I highly doubt that would be so in a real world situation. The only possibility is that the user only used a key when encrypting, meaning that the IV was derived from the key.

Also, I actually read about the purpose of IVs one sites like stack.overflow and crypto.stackexchange, and people over there said that IVs are there to allow people to reuse the same key, so honestly, having the same IV and key kind of defeats the point.

keystream – f001d8b622a8b99907b6353e2d2356c1d67e2ce356c3a478

message – Order: Launch a missile!

6. Task 5

It took me some time to do it, but in the end I did it.

But first of all, I would like to dedicate a paragraph to bash. I do not think I ever had programmed in a language as backward as bash. It is by far the worst language I programmed in. Typically, I would reserve that place for PHP, but the syntax in bash really takes the cake. You need to have your equal sign between the variable and the value to assign something (ex: x=1; x = 1 is invalid). The same rule applies about brackets in if and while statements, where you have to have a space before and after the square brackets. There are no curly brackets, but instead start and end keywords for things like if clauses or loops (ex: if fi and while do done). You have to use the "let" keyword to do arithmetic operations. Conditions like less than are written as "-lt" rather than "<". Plus, you have to use the $ sign to call variables. Finally, I do not think you can reference to a memory address, and you can not check for a null terminator.

Now, onto the task itself. My idea was to copy the dictionary words, by using the cat command, and putting them into a variable. Then splitting them into an array (which can be done by putting the variable in round brackets), and then checking for the key one by one, via an openssl command. Originally, I made checksum of the plaintext, and used the words to decrypt the ciphertext. The match was supposed to have the same checksum, but no luck though. I spent hours looking for the bug, and I found plenty (related to bash syntax), but I did not find that specific bug. I then decided to do the reverse, making a checksum of the ciphertext and encrypting the plaintext with dictionary words. I was hoping that it would make a difference, and while it did not, it did reveal the issue with my code. When encrypting the plaintext, I noticed that the output has a "Salted__" prefix next to it. After a few minutes of searching, I found out about parameters such as -p and -nosalt. The former (-p) prints the key, iv and salt, while the latter (-nosalt) disables salting. It appears to be that salting is enabled by default, and is randomly generated if not specified. The IV seems to be generated from the key itself.

My ciphertext was number 28, and the key was Letitia.

7. Appendix

Part 1 – text.

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

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 PRICE 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

Part 3 – text.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.

Part 5 – source code.

```
#!/usr/bin/env bash


Contents=$(cat words\(3\).txt)
array=( $Contents );

size=${#array[@]};
x=0;

echo $size;

while [ $x -lt $size ]
do
#echo ${array[$x]};
let "x=x+1";
done

x=0;

checksum1=$(cat cipher-28.txt | md5sum)
echo $checksum1;

while [ $x -lt $size ]
do

        echo "${array[$x]}";


        openssl enc -aes-128-cbc -e -nosalt -in plain.txt -out original_task5_b.txt -k "${array[$x]}"

        #wait

        checksum2=$(cat original_task5_b.txt | md5sum)

        echo $checksum2;

        if [ "$checksum1" == "$checksum2" ]
        then
                echo "correct output";
                echo "key is ${array[$x]}";
                echo "key $x out of $size";
                break;
        else
                echo "fail";
        fi
```

```
        let "x=x+1";
        echo "key $x out of $size";

done
```