

SYSTEM AND NETWORK SECURITY

FALL 2024 – Symmetric Key Encryption

Due: 1st September, 2024

Task 1: Frequency Analysis

- Below is an image of the frequency analysis for a typical English plaintext. (Source: https://en.wikipedia.org/wiki/Frequency_analysis)

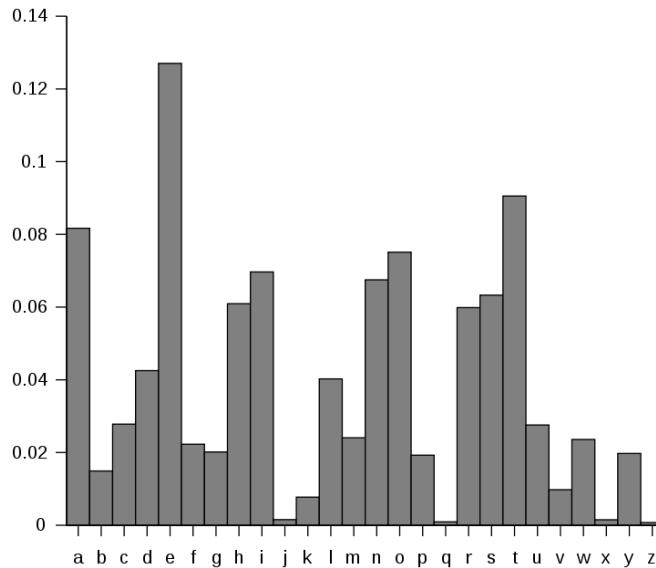


Figure 1

- Using the freq.py Python program, we can find the statistics for n-grams, including the single-letter frequencies, bigram frequencies (2-letter sequence), and trigram frequencies (3-letter sequence), etc.

A screenshot of a terminal window titled 'Terminal'. The command entered is [08/24/24] seed@VM:.../Files\$./freq.py ciphertext.txt. The output shows the frequency analysis of the ciphertext:

```
Aug 24 15:36 •
seed@VM: .../Files
[08/24/24] seed@VM:.../Files$ ./freq.py ciphertext.txt
-----
1-gram (top 20):
n: 488
y: 373
v: 348
x: 291
u: 280
q: 276
m: 264
h: 235
t: 183
i: 166
p: 156
a: 116
c: 104
z: 95
l: 90
g: 83
b: 83
r: 82
e: 76
d: 59
-----
2-gram (top 20):
yt: 115
tn: 89
mu: 74
nh: 58
vh: 57
hn: 57
vu: 56
```

Figure 2

- After getting the above frequencies in the cipher text, we check the frequencies and match them corresponding to Figure 1.
- Using Figure 1 and Figure 2, we replace the letters using the `tr` command. You can use the '`tr`' command to do this.
- Let us replace 'n' with 'E' and 'y' with 'T' as these are the most occurred letters.

```
[08/24/24]seed@VM:.../Files$ tr 'ny' 'ET' < ciphertext.txt > task1.txt
[08/24/24]seed@VM:.../Files$ cat task1.txt
TtE xqavhq Tzhu xu qzupvd ltmat qEEcq vgxzT hmrtT vbTEh Ttmq ixur qThvurE
vlvhpq Thme TtE gyrrEh bEEiq imsE v uxuvrEuvhmvu Txx

TtE vlvhpq hvaE lvq gxxsEupgd TtE pEcmsgE xb tvhfhEd lEmuqTEmu vT mTq xzTqET
vup TtE veevhEuT mceixqmxu xb tmq bmic axcevd vT TtE Eup vup mT lvq qtveEp gd
TtE EcEhrEuaE xb cETxx TmcEq ze givasrxlu eximTmaq vhacavupd vaTmfmcg vup
v uvTmxuvi axufEhvqTmxu vg ghmEb vup cvp vq v bEfEh phEvc vgxzT ltETTtEh TtEhE
xzrT T Tx gE v ehEqmpEut mhuhbEd TtE qEvqvu pmpuT ozqT qEEec EKThv ixur mT lvq
EkThv ixur gEavzqE TtE xqavhq lEhE cxfEp Tx TtE bmhqt LEEsEup mu cvhat Tx
vfxmp axubimaTmru lmTt TtE aixqmur aEhEcxd xb TtE lmuTEh xidcemaq Ttvusq
edExuratvur

xuE gmr jzEqTmxu qzhhxzupmur Ttmq dEvhq vavpEcd vlvhpq mq txl xh mb TtE
aEhEcxd lmii vpphEqq cETxx EqeEamviid vbTEh TtE rxipEu rixgEq ltmat gEavcE
v ozgmiuT axcmurxzT evhTd bxh TmcEq ze TtE cxfEcEut qeEvhtEvpEp gd
exlEhbzi txiidlxp lxcEu ltx tEieEp hvmpqE cmiimxuq xb pxivhq Tx bmrtT qEkzvi
tvhvqqcEuT vhxzup TtE axzuThd

qmrurimur TtEmh qzeexhT rxipEu rixgEq vTTEupEEq qlvTtEp TtEcqEifEq mu givas
qexhTEp ieeEi emuq vup qzxupEp xbb vgxzT qEkmqT exlEh mcgvivuaEq bhxc TtE hEp
avheET vup TtE qTvrE xu TtE vmh E lvq aviiEp xzT vgxzT evd muEjzmTd vbTEh
mTq bxhchEh vuatxh avT qvpih jzmt xuaE qtE iEvhuEp TtvT qtE lvq cvsmur bvH
iEqq Ttvu v cviE axtxqT vup pzhmur TtE aEhEcxd uvTvime exhTcvu Txss v gizuT
vup qvTmqbdmur pmr vT TtE viicvIE hxqTEh xb uxcmuvTEp pmhEaTxhq txl axzip
TtvT gE TxeEp

vq mT Tzhuq xzT vT iEvqT mu TEhcq xb TtE xqavhq mT ehxvgvid lxuT gE

lxcEu mufxifEp mu TmcEq ze qvmp TtvT viTtxzrt TtE rixgEq qmrumbmEp TtE
mumTmvTmfEq ivzuaT TtEd uEfEh muTEupEp mT Tx gE ozqT vu vlvhpq qEvqiu
```

- We can start guessing the letters now. 't', 'x', 'v' can be replaced by 'H', 'O' and 'A'.

```
[08/24/24]seed@VM:.../Files$ tr 'nytxv' 'ETHOA' < ciphertext.txt > task1.txt
[08/24/24]seed@VM:.../Files$ cat task1.txt
THE OqaAhq Tzhu Ou qzupAd lHmaH qEEcq Ag0zT hmrtHT AbTEh THmq iour qThAurE
AlAhpq Thme THE gArrEh bEEiq imsE A u0uArUaHmAu T00

THE AlAhpq hAaE lAq g00sEupEp gd THE pEcmsgE Ob HAHfEd lEmuqTEmu AT mTq OzTqET
Aup THE AeeAhEuT mce10qm0u Ob Hmq bmic aOceAud AT THE Eup Aup mT lAq qHAEep gd
THE EcEhrEuaE Ob cET00 TmcEq ze giAsr0lu oImTmaq AhcaAupd AaTmfmcg Aup
A uATm0uAi a0ufEhqATm0u Aq ghmEb Aup cAp Aq bEfEh phEAc Ag0zT lHETHEN THeHE
OzrHT T0 gE A ehEqmpEut mhuhbEd THE qEAq0u pmpuT ozqT qEEec EKThA iour mT lAq
EkThA iour gEaAzqE THE OqaAhq lEhE c0fEp T0 THE bmhqt LEEsEup mu cAhA T0
Af0mp a0ubimaTmru lmTH THE ai0qmur aEhEcoud Ob THE lmuTEh Oidcemaq THAusq
edEOuraHaur

OuE gmr jzEqTm0u qzhhxzupmur THmq dEahq AaApEcd AlAhpq mq H0l Oh mb THE
aEhEcoud lmii ApphEqq cET00 EqeEamAiid AbTEh THE r0ipEu ri0gEq lHmaH gEaAcE
A ozgmiAuT a0cmur0zT eAhTd b0h TmcEq ze THE c0fEcEut qeEahHEApEp gd
e0lEhbzi H0iidl00p l0cEu lH0 HEieEp hAmqE cmiim0uq Ob p0iiAhq T0 bmrtT qEkzAi
HAhAqqcEuT Ah0zup THE a0zuThd

qmrurimur THEmh qzeexhT r0ipEu ri0gEq ATTEupEEq qlATHEp THEEcqEifEq mu gias
qe0hTEp iAeEi emuq Aup q0zupEp obb Ag0zT qEkmqT e0lEh mcgaiauAeq bh0c THE hEp
aAheET Aup qTArE THE Amh E lAq aAiiEp 0zT Ag0zT eAd muEjzmTd AbTEh
mTq b0hcEh Auah0h aATT qAphih jzmt OuAe qHE iEahuEp THAT qHE lAq cAsmru bAh
iEqq THAu A cAiE a0HOQt Aup pzhmur THE aEhEcoud uATAimE e0hTcAu T00s A gizuT
Aup qATmqbdmur pmr AT THE AiicAiE h0qTEh Ob u0cmuATEp pmhEaT0h0q H0l a0zip
THAT gE T0eeEp

Aq mT Tzhuq OzT AT iEAqT mu TEhcq Ob THE OqaAhq mT eh0gAgid l0uT gE

l0cEu muf0ifEp mu TmcEq ze qAmp THAT A1TH0zrH THE ri0gEq qmrumbmEp THE
mumTmvTmfEq iAzuaH THEd uEfEh muTEupEp mT T0 qE ozqT Au AlAhpq qEaQ0u
```

- We can't be sure but we can slightly guess that 'z' might be 'U', 'r' might be 'G', 'i' might be 'L' and 'g' might be 'B'. Let's try that and see if it works.

```

Activities Terminal Aug 24 15:57 • seed@VM:.../Files
[08/24/24]seed@VM:.../Files$ tr 'nytxvzrgi' 'ETHOAUGBL' < ciphertext.txt > task1.txt
[08/24/24]seed@VM:.../Files$ cat task1.txt
THE OqaAhq TUhu Ou qUpAd lHmaH qEEcq ABOUT hmGHT AbTEh THmq LOuG qThAuGE
AlAhpq Thme THE BAGGEh bEELq LmsE A uOuAGEuAhmAu TOO

THE AlAhpq hAaE lAq BOOsEupEp Bd THE pEcMqE Ob HAhfEd lEmuqTEMu AT mTq OUTqET
Aup THE AeeAhEuT mceLOqmOU Ob Hmq bmlC aOceAud AT THE Eup Aup mT lAq qHAeEp Bd
THE EcHGeuaE Ob cETO0 TmcEq Ue BLAasGolu eOLmTmaq AhcaAupd AaTmfmcq Aup
A uATmOuAL a0ufEhqATmOu Aq BhmEb Aup cAp Aq A bEfEh phEc ABOUT lHTHEH THEhE
OUGHT TO BE A ehEqmpEUT lmubhEd THE qEAqOU pmpuT ouqT qEEc EkThA LOuG mT lAq
EkThA LOuG BEaAUqE THE OqaAhq lEhE c0fEp TO THE bmhqt LEESEup mu cAhaH TO
Afomp a0ubLmaTmuG lmTH THE aLOqmUG aEfEcOud Ob THE lmuTEh OLdcemaq THAusq
edEOuGaHAuG

OuE BmG jUEqTmOu qUhh0UupmuG THmq dEAhQ AaApEcD AlAhpq mq H0l Oh mb THE
aHhEcOud lmLL ApphEqq cETO0 EqeEamALLd AbTEh THE GOLpEu GLOBE Eq lHmaH BEaAcE
A oUBmLauT a0cmuGOUT eAhTd b0h TmcEq Ue THE c0fEcEuT qeEAhHEApEp Bd
eOLEhbUL HOLLdL00p l0cE LHO HELeEp hAmqE cmLLmOuq Ob pOLLAhQ TO bmGHT qEkUAL
HAhAqqcEuT Ah0Uup THE a0uUuT

qmGuALmuG THEmh qUeeOhT GOLpEu GLOBE Eq ATTEmuG qLATHEp THEEcqELfEq mu BLAas
qe0hTEp LAeEL emuq Aup qUupEp Obb ABOUT qEkmqT e0lEh mcBALAuAeq bh0c THE hEp
aAheET Aup THE qTAGE Ou THE Amh E lAq aALLEp OUT ABOUT eAd muEjUmTd AbTEh
mTq b0hcEh AuAH0h aATT qApLEh jUmt OuAE qHE LEAhUep THAT qHE lAq cAsmuG bAh
LEqq THAu A cALE aOHQQT Aup pUhmuG THE aHhEcOud uATAlmE e0hTcAu TOO A BLUuT
Aup qATmqbdmuG pG AT THE ALLcALE h0qTEh Ob uOcmuATEp pmhEaTOhQ H0l a0ULp
THAT BE TOeeEp

Aq mT TUhuq OUT AT LEAQt mu TEhcq Ob THE OqaAhq mT ehOBABLd l0uT BE

l0cEu muF0LfEp mu TmcEq Ue qAmp THAT ALTHOUGH THE GLOBE Eq qmGumbmEp THE
muTmATmfEq LAUuAH THEd uEfEh muTEupEp mT TO BE ouqT Au AlAhpq qEAqOU

```

- So we can guess 'a' to be 'C' and 'm' to be 'I'. Also 'b' as 'F', 'l' as 'W' and 'q' as 'S'. If we apply all these, we get the below:

```

Activities Terminal Aug 24 16:11 • seed@VM:.../Files
[08/24/24]seed@VM:.../Files$ tr 'nytxvzrgiambql' 'ETHOAUGBLCIFSW' < ciphertext.txt > task1.txt
[08/24/24]seed@VM:.../Files$ cat task1.txt
THE OSCAhS TUhu Ou SuupAd WHICH SEEcs ABOUT hIGHT AFTEh THIS LOuG SThAuGE
AWAhps ThIE THE BAGGEh FEELS LiSE A uOuAGEuAhIAU TOO

THE AWAhps hACE WAS BOOsEupEp Bd THE pEcISE OF HAhfEd WEIuSTEIu AT ITS OUTSET
Aup THE AeeAhEuT IceLOSIoU OF HIS FILC CoceAud AT THE Eup Aup IT WAS SHAEp Bd
THE EcHGeUEC OF cETO0 TicEs Ue BLACsGOWu eOLITICS AhcAupd ACTIfISC Aup
A uATIouAL C0ufEhsATIou AS BHIEF Aup cAp AS A FEFeh phEc ABOUT WHEThEh THEhE
OUGHT TO BE A ehESIpEut WIuFhEd THE SEASoU pIpuT ouST SEEc EkThA LOuG IT WAS
EkThA LOuG BECAUSE THE OSCAhS WEHE c0fEp TO THE FiHST WEEsEup Iu cAnCH TO
AfOp COuFLICtiG WITH THE CLOSiUg CEhEcOud OF THE WIuTEh OLdcEiCS THAus
edEOuGChAuG

OuE BIG jUESTIoU SUhh0UupIuG THIS dEAhS ACAPEcD AWAhps IS HOW Oh IF THE
CEhEcOud WILL ApphESS cETO0 ESeECIALld AFTEh THE GOLpEu GLOBEs WHICH BECAcE
A oUBILAuT C0ciuGOUT eAhTd FOH TicEs Ue THE c0fEcEuT SeAhHEApEp Bd
e0WehFUL HOLLdW00p W0cEu WHO HELeEp hAISE cILLIOuS OF pOLLAhs TO FIGHT SEKUAL
HAhASScEuT Ah0Uup THE COUuThd

SIGuALIuG THEh SUEeOhT GOLpEu GLOBEs ATTEmuG SWATEp THEcSELfES Iu BLACs
Se0hTEp LAeEL eIuS Aup SOUupEp OFF ABOUT SEKIST e0WEh IcBALAuCES Fh0c THE hEp
CAhET Aup THE STAGE Ou THE AIh E WAS CALLeP OUT ABOUT eAd IuEjUITD AFTEh
ITS FOhcEh AuCH0h CATT SApLEh jUit OuCE SHE LEAhUep THAT SHE WAS cAsIuG FAh
LESS THAu A cALE COHOST Aup pUhIuG THE CEhEcOud uATAlIE e0hTcAu TOO A BLUuT
Aup SATISFdIuG pIG AT THE ALLcALE h0STEH OF uOciuATEp piHECTOhs HOW COULP
THAT BE TOeeEp

AS IT TUhuS OUT AT LEAST Iu TEhcS OF THE OSCAhS IT ehOBABLd W0uT BE

W0cEu Iuf0LfEp Iu TiCs Ue SAIp THAT ALTHOUGH THE GLOBEs SIGuIFIcEp THE
IuITIATIfEs LAUuCH THEd uEfEh IuTEupEp IT TO BE ouST Au AWAhps SEASoU

```

- Now it is getting clear that 'h' → 'R', 'u' → 'N', 'c' → 'M', 'p' → 'D', 'd' → 'Y', 'f' → 'V', 'e' → 'P'. Let us apply this and analyze.

```

Activities Terminal Aug 24 16:16 • seed@VM: .../Files
[08/24/24]seed@VM:.../Files$ tr 'nytxvzrgiambqlhucpdfe' 'ETHOAUGBLCIFSWRNMDYVP' < ciphertext.txt > task1.txt
[08/24/24]seed@VM:.../Files$ cat task1.txt
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

```

- Now we have 'o' → 'J', 's' → 'K', 'j' → 'Q', 'k' → 'X'

```

Activities Terminal Aug 24 16:25 • seed@VM: .../Files
[08/24/24]seed@VM:.../Files$ tr 'nytxvzrgiambqlhucpdfeosjk' 'ETHOAUGBLCIFSWRNMDYVPJKQX' < ciphertext.txt > task1.txt
[08/24/24]seed@VM:.../Files$ cat task1.txt
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

```

- Lastly we have 'w' → 'z' as that is the last combination.
- Final Output:

```
[08/24/24]seed@VM:.../Files$ tr 'nytxvzrgiambqlhucpdfeosjk' 'ETHOAUGBLCIFSWRNMDYVPJKQX' < ciphertext.txt > task1.txt
[08/24/24]seed@VM:.../Files$ cat task1.txt
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

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 SECONDPPLACE 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

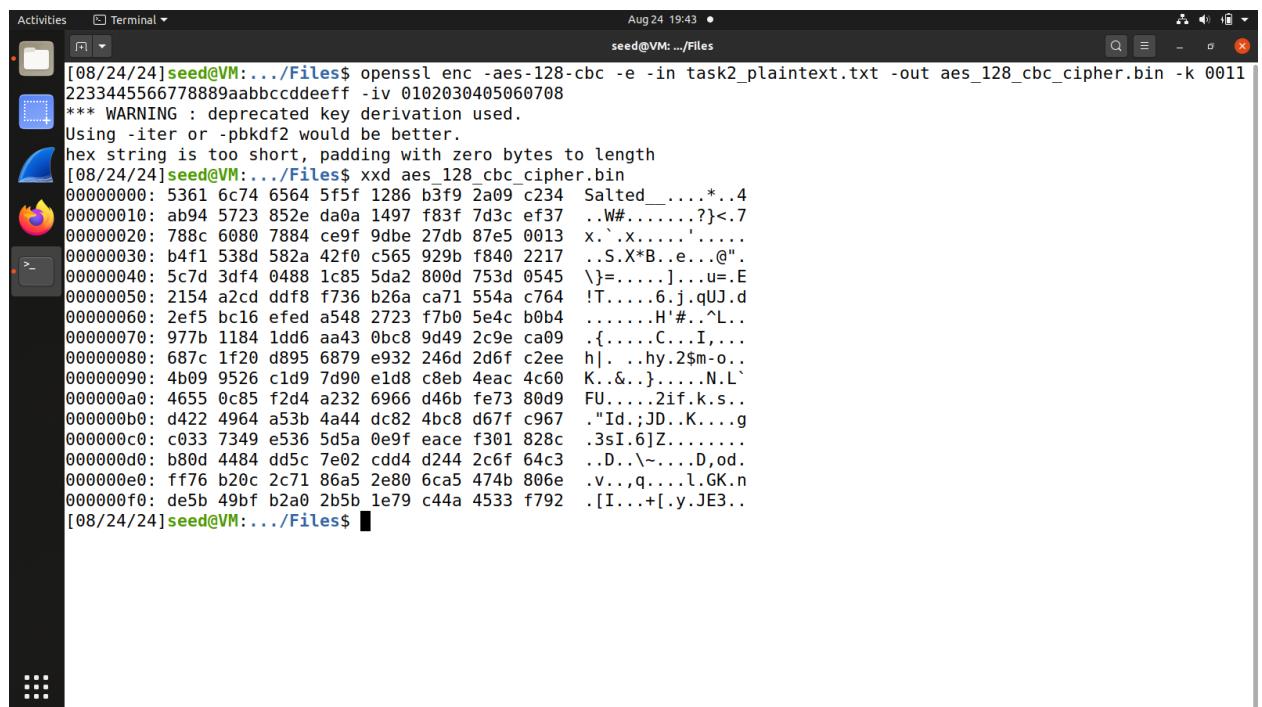
- So we have our final key as below

Cipher text	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
Plain text	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

Task 2: Encryption using Different Ciphers and Modes

- Out of all the cipher types, we will be using 3 different cipher types for this task.
 - aes-128-cbc
 - des-cfb
 - bf-ofb
1. -aes-128-cbc
- Run the command to encrypt the task2_plaintext.txt file using the below command

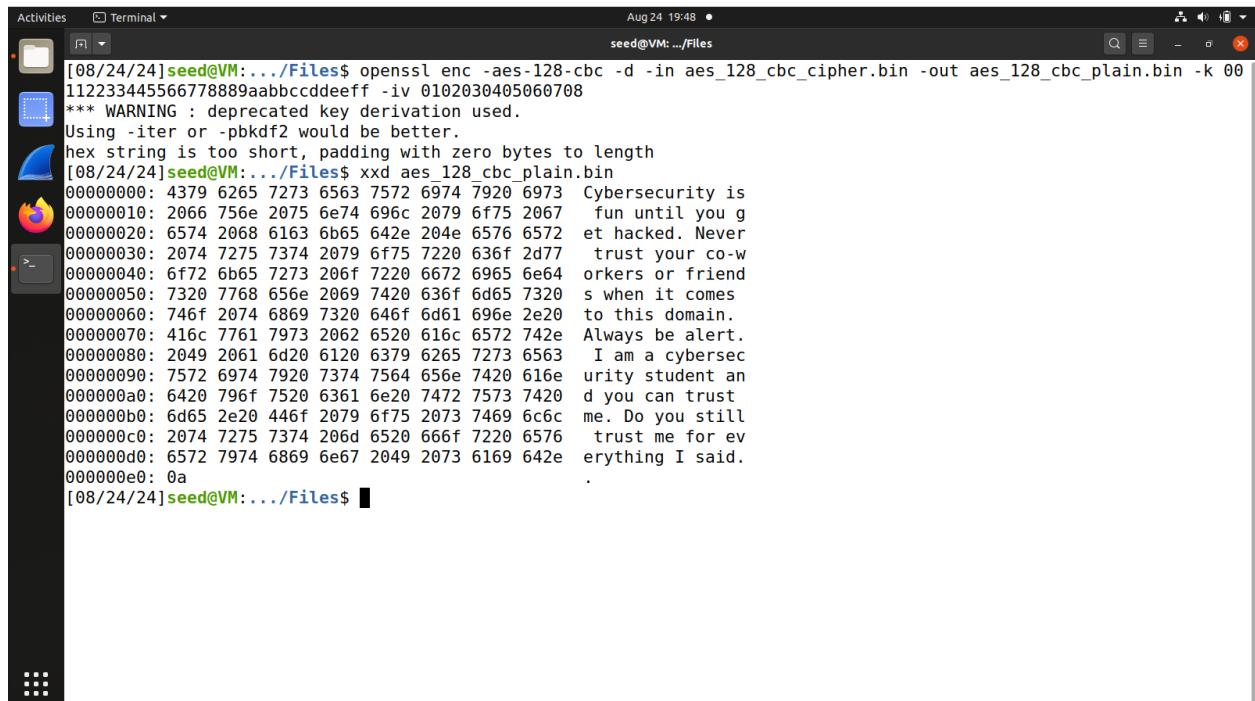
```
$ openssl enc -aes-128-cbc -e -in task2_plaintext.txt -out aes_128_cbc_cipher.bin -k 0011223344556677889aabccddeff -iv 0102030405060708
```
 - We can view the encrypted file using the command `$cat aes_128_cbc_cipher.bin` but to make it more meaningful, run the `$xxd aes_128_cbc_cipher.bin` and we can view in hexadecimal format.



The screenshot shows a terminal window titled "seed@VM:.../Files" running on a Linux desktop environment. The terminal output is as follows:

```
[08/24/24]seed@VM:.../Files$ openssl enc -aes-128-cbc -e -in task2_plaintext.txt -out aes_128_cbc_cipher.bin -k 0011223344556677889aabccddeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/24/24]seed@VM:.../Files$ xxd aes_128_cbc_cipher.bin
00000000: 5361 6c74 6564 5f5f 1286 b3f9 2a09 c234 Salted__....*..4
00000010: ab94 5723 852e da0a 1497 f83f 7d3c ef37 ..W#.....?}<.7
00000020: 788c 6080 7884 ce9f 9dbe 27db 87e5 0013 x..x......
00000030: b4f1 538d 582a 42f0 c565 929b f840 2217 ..S.X*B.e...@".
00000040: 5c7d 3df4 0488 1c85 5da2 800d 753d 0545 \}=....]...u.E
00000050: 2154 a2cd ddf8 f736 b26a c471 554a c764 !T.....6.j.qUJ.d
00000060: 2ef5 bc16 efed a548 2723 f7b0 5e4c b0b4 .....H'#.^L..
00000070: 977b 1184 1dd6 aa43 0bc8 9d49 2c9e ca09 .{....C...I...
00000080: 687c 1f20 d895 6879 e932 246d 2d6f c2ee h|..hy.2$m-o..
00000090: 4b09 9526 c1d9 7d90 e1d8 c8eb 4eac 4c60 K..&..}....N.L` 
000000a0: 4655 0c85 f2d4 a232 6966 d46b fe73 80d9 FU....2if.k.s..
000000b0: d422 4964 a53b 4a44 dc82 4bc8 d67f c967 ."Id.;JD..K....g
000000c0: c033 7349 e536 5d5a 0e9f eace f301 828c .3sI.6jZ.....
000000d0: b80d 4484 dd5c 7e02 cdd4 d244 2c6f 64c3 ..D..`-....D,od.
000000e0: ff76 b20c 2c71 86a5 2e80 6ca5 474b 806e .v.,q...,l.GK.n
000000f0: de5b 49bf b2a0 2b5b 1e79 c44a 4533 f792 .[I...+[.y.JE3..
[08/24/24]seed@VM:.../Files$
```

- For decrypting, use the command `$ openssl enc -aes-128-cbc -d -in aes_128_cbc_cipher.bin -out aes_128_cbc_plain.bin -k 0011223344556677889aabccddeff -iv 0102030405060708`
- For viewing the decrypted content, just use the `cat` or `xxd` command followed by the file name.



```

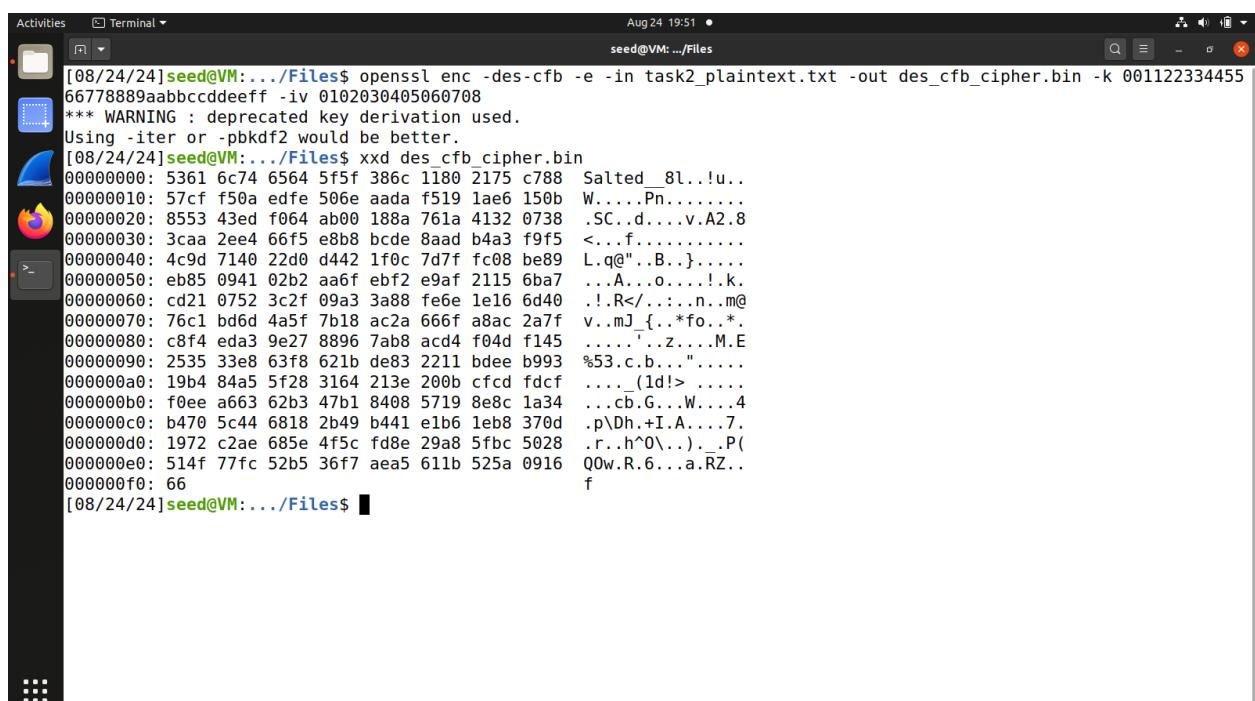
[08/24/24]seed@VM:.../Files$ openssl enc -aes-128-cbc -d -in aes_128_cbc_cipher.bin -out aes_128_cbc_plain.bin -k 00112233445566778889aabbccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/24/24]seed@VM:.../Files$ xxd aes_128_cbc_plain.bin
00000000: 4379 6265 7273 6563 7572 6974 7920 6973 Cybersecurity is
00000010: 2066 756e 2075 6e74 696c 2079 6f75 2067 fun until you g
00000020: 6574 2068 6163 6b65 642e 204e 6576 6572 et hacked. Never
00000030: 2074 7275 7374 2079 6f75 7220 636f 2d77 trust your co-w
00000040: 6f72 6b65 7273 206f 7220 6672 6965 6e64 orkers or friend
00000050: 7320 7768 656e 2069 7420 636f 6d65 7320 s when it comes
00000060: 746f 2074 6869 7320 646f 6d61 696e 2e20 to this domain.
00000070: 416c 7761 7973 2062 6520 616c 6572 742e Always be alert.
00000080: 2049 2061 6d20 6120 6379 6265 7273 6563 I am a cybersec
00000090: 7572 6974 7920 7374 7564 656e 7420 616e urity student an
000000a0: 6420 796f 7520 6361 6e20 7472 7573 7420 d you can trust
000000b0: 6d65 2e20 446f 2079 6f75 2073 7469 6c6c me. Do you still
000000c0: 2074 7275 7374 206d 6520 666f 7220 6576 trust me for ev
000000d0: 6572 7974 6869 6e67 2049 2073 6169 642e erything I said.
000000e0: 0a
[08/24/24]seed@VM:.../Files$ 

```

2. -des-cfb

- Run the command to encrypt the task2_plaintext.txt file using the below command

```
$openssl enc -des-cfb -e -in task2_plaintext.txt -out des_cfb_cipher.bin -k 00112233445566778889aabbccddeeff -iv 0102030405060708
```
- We can view the encrypted file using the command \$cat des_cfb_cipher.bin but to make it more meaningful, run the \$xxd des_cfb_cipher.bin and we can view in hexadecimal format.



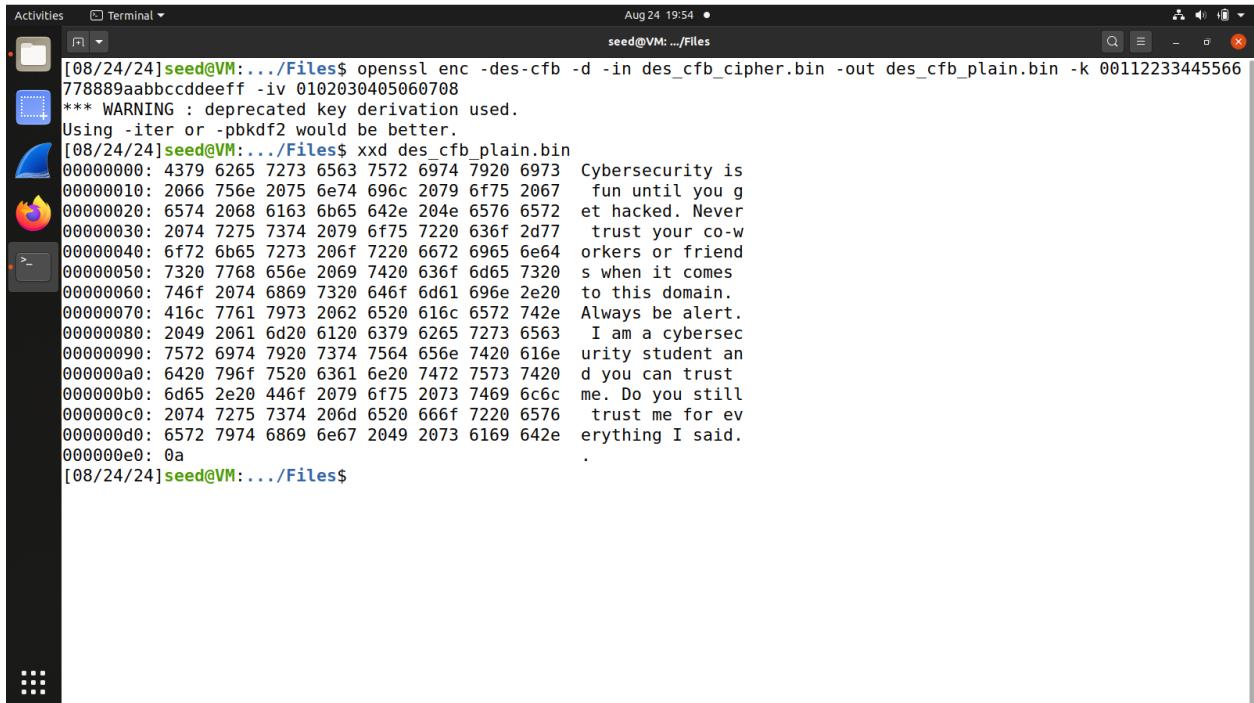
```

[08/24/24]seed@VM:.../Files$ openssl enc -des-cfb -e -in task2_plaintext.txt -out des_cfb_cipher.bin -k 00112233445566778889aabbccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/24/24]seed@VM:.../Files$ xxd des_cfb_cipher.bin
00000000: 5361 6c74 6564 5f5f 386c 1180 2175 c788 Salted_8l..!u..
00000010: 57cf f50a edfe 506e aada f519 lae6 150b W.....Pn.....
00000020: 8553 43ed f064 ab00 188a 761a 4132 0738 .SC..d....v.A2.8
00000030: 3caa 2ee4 66f5 e8b8 bcde 8aad b4a3 f9f5 <...f.....
00000040: 4c9d 7140 22d0 d442 1f0c 7d7f fc08 be89 L.q@"..B..j.....
00000050: eb85 0941 02b2 aa6f ebf2 e9af 2115 6ba7 ..A...o....!k.
00000060: cd21 0752 3c2f 09a3 3a88 fe6e 1e16 6d40 !..R<...:n..m@
00000070: 76c1 bd6d 4a5f 7b18 ac2a 666f a8ac 2a7f v..mJ_{..*fo..*.
00000080: c8f4 eda3 9e27 8896 7ab8 acd4 f04d f145 .....z....M.E
00000090: 2535 33e8 63f8 621b de83 2211 bdee b993 %53.c.b...".....
000000a0: 19b4 84a5 5f28 3164 213e 200b cfcd fdcc ...._(ld!> ....
000000b0: f0ee a663 62b3 47b1 8408 5719 8e8c 1a34 ...cb.G...W....4
000000c0: b470 5c44 6818 2b49 b441 e1b6 1eb8 370d .p\Dh.+I.A....7.
000000d0: 1972 c2ae 685e 4f5c fd8e 29a8 5fbc 5028 .r..h^O...)._P(
000000e0: 514f 77fc 52b5 36f7 aea5 611b 525a 0916 Q0w.R.6...a.RZ..
000000f0: 66 f
[08/24/24]seed@VM:.../Files$ 

```

- For decrypting, use the command \$openssl enc -des-cfb -d -in des_cfb_cipher.bin -out des_cfb_plain.bin -k 00112233445566778889aabbccddeeff -iv 0102030405060708

- For viewing the decrypted content, just use the `cat` or `xxd` command followed by the file name.

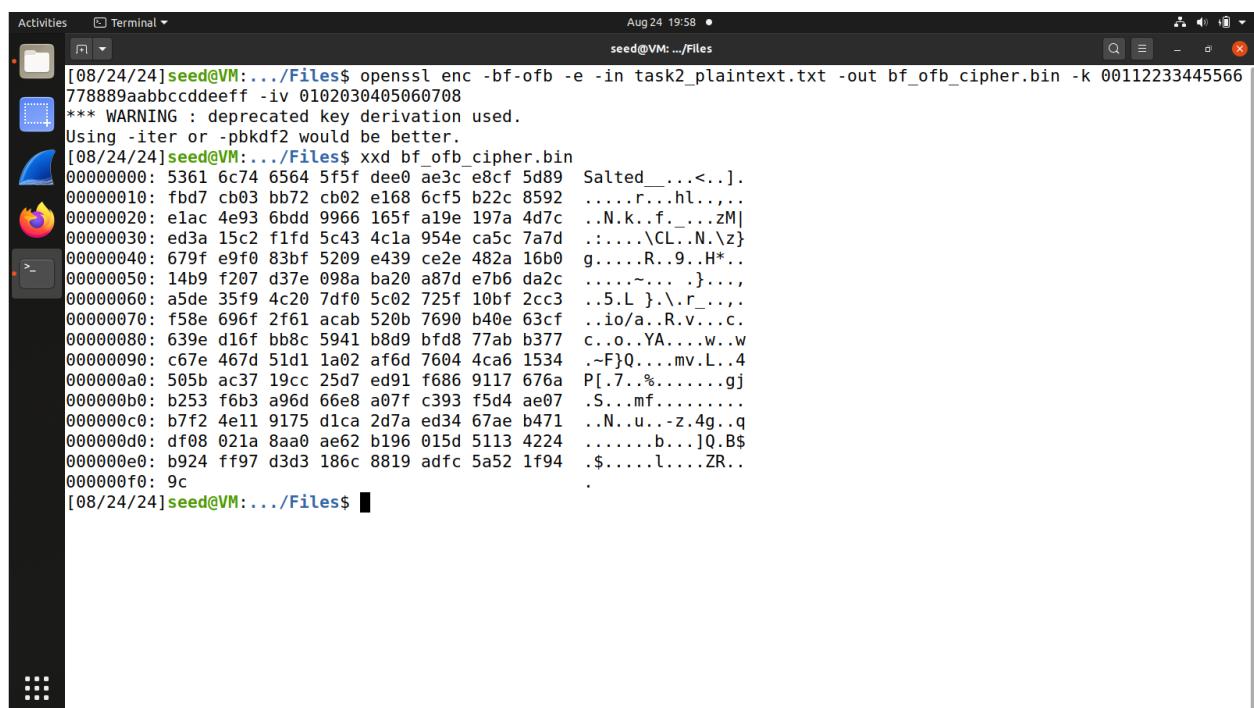


```
[08/24/24]seed@VM:.../Files$ openssl enc -des-cfb -d -in des_cfb_cipher.bin -out des_cfb_plain.bin -k 00112233445566
778889aabbccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/24/24]seed@VM:.../Files$ xxd des_cfb_plain.bin
00000000: 4379 6265 7273 6563 7572 6974 7920 6973 Cybersecurity is
00000010: 2066 756e 2075 6e74 696c 2079 6f75 2067 fun until you g
00000020: 6574 2068 6163 6b65 642e 204e 6576 6572 et hacked. Never
00000030: 2074 7275 7374 2079 6f75 7220 636f 2d77 trust your co-w
00000040: 6f72 6b65 7273 206f 7220 6672 6965 6e64 orkers or friend
00000050: 7320 7768 656e 2069 7420 636f 6d65 7320 s when it comes
00000060: 746f 2074 6869 7320 646f 6d61 696e 2e20 to this domain.
00000070: 416c 7761 7973 2062 6520 616c 6572 742e Always be alert.
00000080: 2049 2061 6d20 6120 6379 6265 7273 6563 I am a cybersec
00000090: 7572 6974 7920 7374 7564 656e 7420 616e urity student an
000000a0: 6420 796f 7520 6361 6e20 7472 7573 7420 d you can trust
000000b0: 6d65 2e20 446f 2079 6f75 2073 7469 6c6c me. Do you still
000000c0: 2074 7275 7374 206d 6520 666f 7220 6576 trust me for ev
000000d0: 6572 7974 6869 6e67 2049 2073 6169 642e erything I said.
000000e0: 0a
[08/24/24]seed@VM:.../Files$
```

3. -bf-ofb

- Run the command to encrypt the `task2_plaintext.txt` file using the below command


```
$ openssl enc -bf-ofb -e -in task2_plaintext.txt -out bf_ofb_cipher.bin -k 0011223344556677889aabbccddeeff -iv 0102030405060708
```
- We can view the encrypted file using the command `$cat bf_ofb_cipher.bin` but to make it more meaningful, run the `$xxd bf_ofb_cipher.bin` and we can view in hexadecimal format.



```
[08/24/24]seed@VM:.../Files$ openssl enc -bf-ofb -e -in task2_plaintext.txt -out bf_ofb_cipher.bin -k 00112233445566
778889aabbccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/24/24]seed@VM:.../Files$ xxd bf_ofb_cipher.bin
00000000: 5361 6c74 6564 5f5f dee0 ae3c e8cf 5d89 Salted_...<...].
00000010: fb7d cb03 bb72 cb02 e168 6cf5 b22c 8592 .....r...hl....
00000020: elac 4e93 6bdd 9966 165f a19e 197a 4d7c ..N.k..f._...zM|
00000030: ed3a 15c2 f1fd 5c43 4c1a 954e ca5c 7a7d :....\CL..N..z}
00000040: 679f e9f0 83bf 5209 e439 ce2e 482a 16b0 g....R..9..H*..
00000050: 14b9 f207 d37e 098a ba20 a87d e7b6 da2c .....~...}.
00000060: a5de 35f9 4c20 7df0 5c02 725f 10bf 2cc3 ..5.L }.\.r....,
00000070: f58e 696f 2f61 acab 520b 7690 b40e 63cf ..io/a..R.V...c.
00000080: 639e d16f bb8c 5941 b8d9 bf8 77ab b377 c..o..YA....w..w
00000090: c67e 467d 51d1 1a02 af6d 7604 4ca6 1534 .~F)Q....mv.L..4
000000a0: 505b ac37 19cc 25d7 ed91 f686 9117 676a P[.7.%.....gj
000000b0: b253 f6b3 a96d 66e8 a07f c393 f5d4 ae07 .S...mf.....
000000c0: b7f2 4e11 9175 d1ca 2d7a ed34 67ae b471 ..N.u..-z.4g..q
000000d0: df08 021a 8aa0 ae62 b196 015d 5113 4224 .....b...]Q.B$
000000e0: b924 ff97 d3d3 186c 8819 adfc 5a52 1f94 $.....l....ZR..
000000f0: 9c
[08/24/24]seed@VM:.../Files$
```

- For decrypting, use the command `$ openssl enc -bf-ofb -d -in bf_ofb_cipher.bin -out bf_ofb_plain.bin -k 00112233445566778889aabbcdddeeff -iv 0102030405060708`
- For viewing the decrypted content, just use the `cat` or `xxd` command followed by the file name.

```
[08/24/24]seed@VM:.../Files$ openssl enc -bf-ofb -d -in bf_ofb_cipher.bin -out bf_ofb_plain.bin -k 00112233445566778889aabbcdddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/24/24]seed@VM:.../Files$ xxd bf_ofb_plain.bin
00000000: 4379 6265 7273 6563 7572 6974 7920 6973 Cybersecurity is
00000010: 2066 756e 2075 6e74 696c 2079 6f75 2067 fun until you g
00000020: 6574 2068 6163 6b65 642e 204e 6576 6577 et hacked. Never
00000030: 2074 7275 7374 2079 6f75 7220 636f 2d77 trust your co-w
00000040: 6f72 6b65 7273 206f 7220 6672 6965 6e64 orkers or friend
00000050: 7320 7768 656e 2069 7420 636f 6d65 7320 s when it comes
00000060: 746f 2074 6869 7320 646f 6d61 696e 2e20 to this domain.
00000070: 416c 7761 7973 2062 6520 616c 6572 742e Always be alert.
00000080: 2049 2061 6d20 6120 6379 6265 7273 6563 I am a cybersec
00000090: 7572 6974 7920 7374 7564 656e 7420 616e urity student an
000000a0: 6420 796f 7520 6361 6e20 7472 7573 7420 d you can trust
000000b0: 6d65 2e20 446f 2079 6f75 2073 7469 6c6c me. Do you still
000000c0: 2074 7275 7374 206d 6520 666f 7220 6576 trust me for ev
000000d0: 6572 7974 6869 6e67 2049 2073 6169 642e erything I said.
000000e0: 0a
[08/24/24]seed@VM:.../Files$
```

Task 3: Encryption Mode – ECB vs. CBC

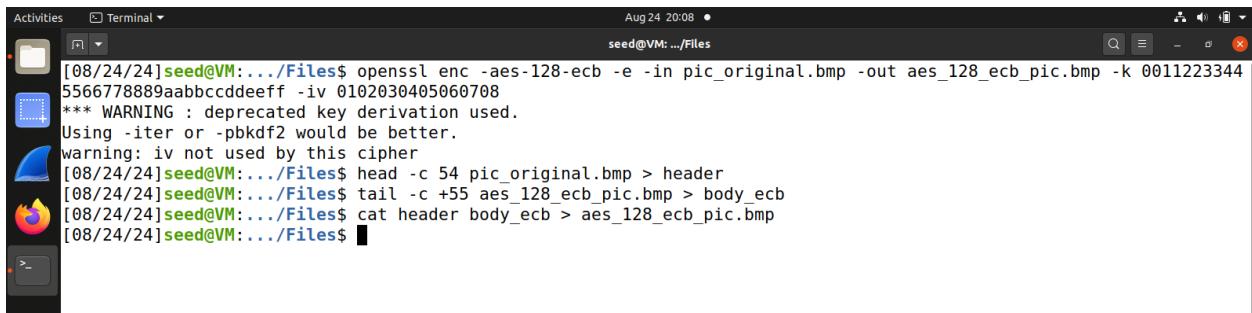
1. Electronic Code Block (ECB)



Figure 4. pic_original.bmp

- Figure 4 is the original image. We encrypt it using the AES-128-ECB cipher type by using the command
`$ openssl enc -aes-128-ecb -e -in pic_original.bmp -out aes_128_ecb_pic.bmp -k 00112233445566778889aabbcdddeeff -iv 0102030405060708`
- NOTE: Once we run this command, we get a warning stating that initial value isn't used by this cipher.

- Using the Bless tool, we can use the following commands
 - \$head -c 54 pic_original.bmp > header
 - \$tail -c +55 aes_128_ecb_pic.bmp > body_ecb
 - \$cat header body_ecb > aes_128_ecb_pic.bmp



```
Activities Terminal Aug 24 20:08
seed@VM:~/Files
[08/24/24]seed@VM:.../Files$ openssl enc -aes-128-ecb -e -in pic_original.bmp -out aes_128_ecb_pic.bmp -k 0011223344556677889aabccddeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
warning: iv not used by this cipher
[08/24/24]seed@VM:.../Files$ head -c 54 pic_original.bmp > header
[08/24/24]seed@VM:.../Files$ tail -c +55 aes_128_ecb_pic.bmp > body_ecb
[08/24/24]seed@VM:.../Files$ cat header body_ecb > aes_128_ecb_pic.bmp
[08/24/24]seed@VM:.../Files$
```

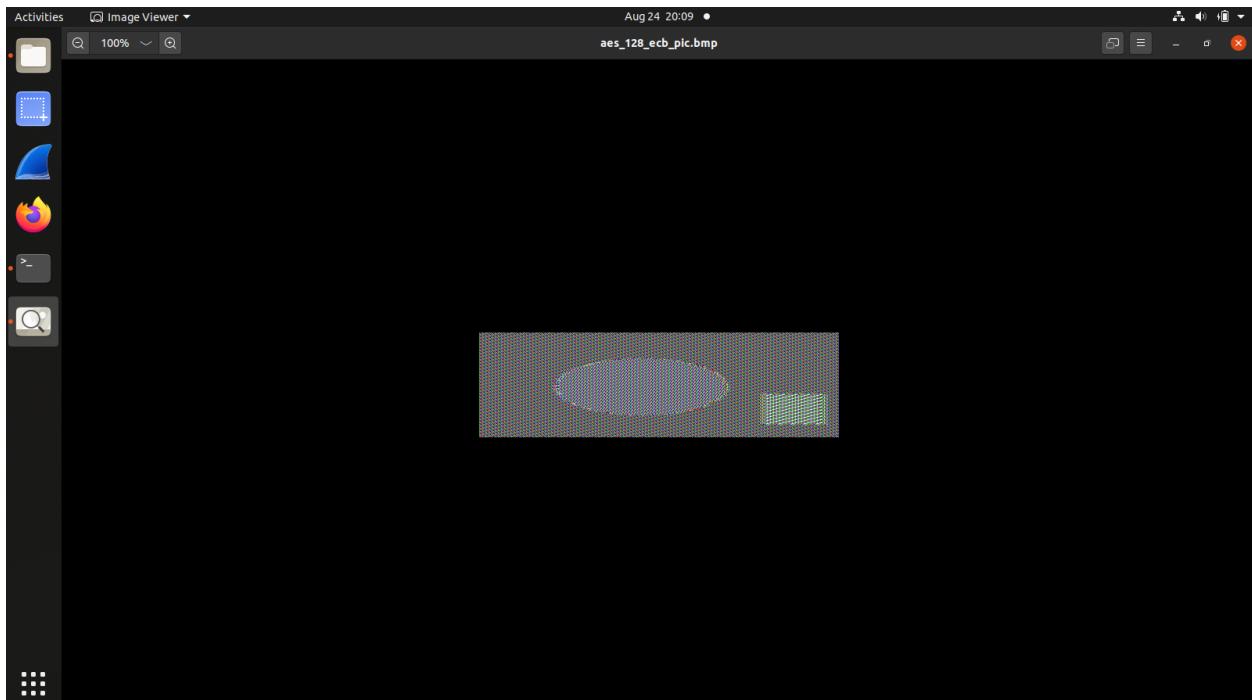


Figure 5. aes_128_ecb_pic.bmp

2. Code Block Cipher (CBC)

- Again we use the same image (Figure 3). This time, we encrypt it using the AES-128-CBC cipher type:


```
$openssl enc -aes-128-cbc -e -in pic_original.bmp -out aes_128_cbc_pic.bmp -k 0011223344556677889aabccddeff -iv 0102030405060708
```
- NOTE: Once we run this command, we get a warning stating that initial value isn't used by this cipher.
 - Using the Bless tool, we can use the following commands. Note here that we didn't run \$head -c 54 pic_original.bmp > header as we already have this header stored and there is no point in running this command again.
 - \$tail -c +55 aes_128_cbc_pic.bmp > body_cbc
 - \$cat header body_cbc > aes_128_cbc_pic.bmp

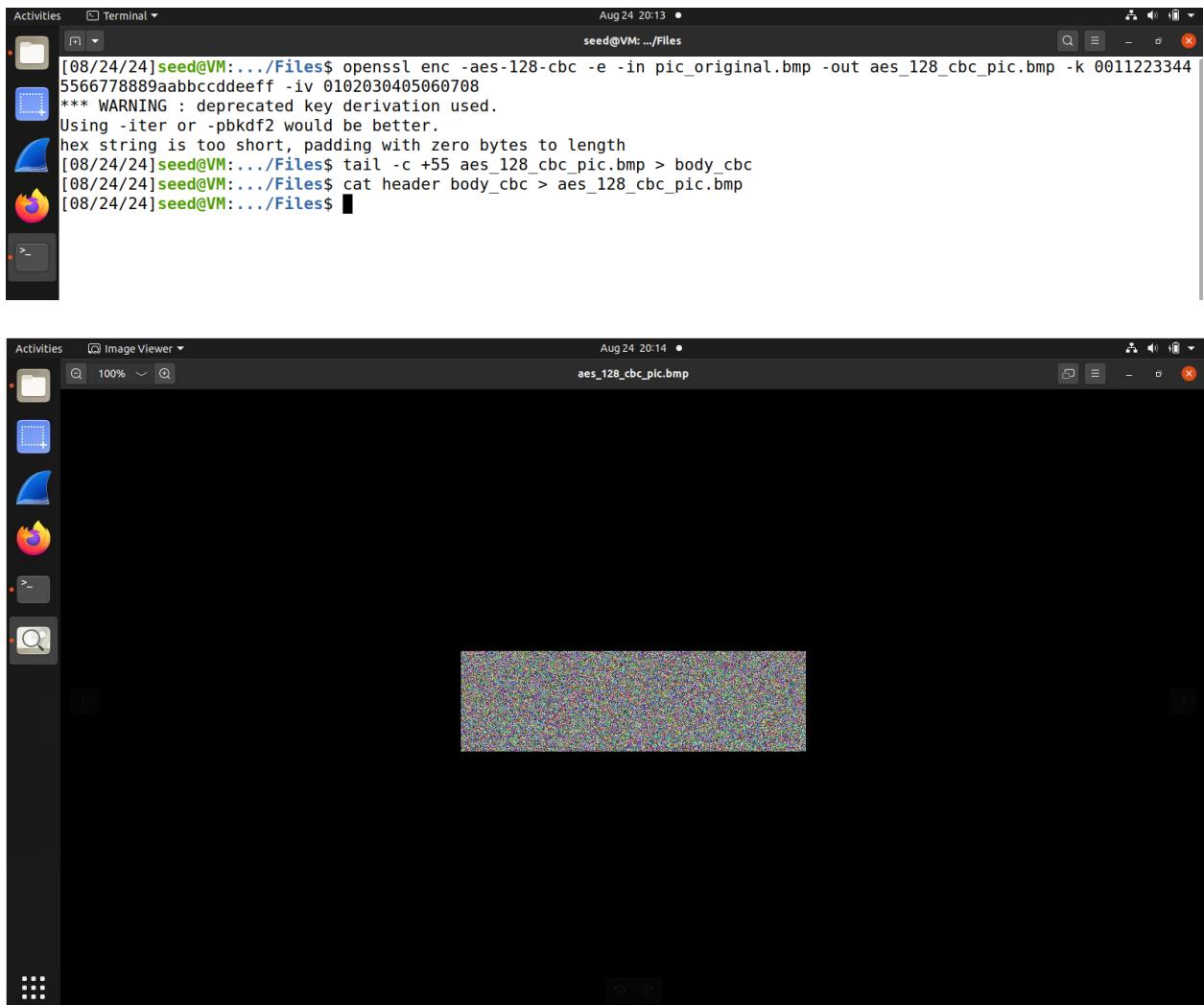


Figure 6. aes_128_cbc_pic.bmp

- Figure 5 and Figure 6 are the resulting encrypted images using EBC and CBC respectively. If we observe, we see that using EBC, we might not be able to identify the actual image perfectly but can easily get an idea of the content present in the image. This is because some contents of the image can still be estimated like the oval shape, the circle and the rectangle. On the other hand, we have the results of the encryption using CBC. There is barely any data or clue that an attacker can extract from Figure 6.

- Now let us examine another image.

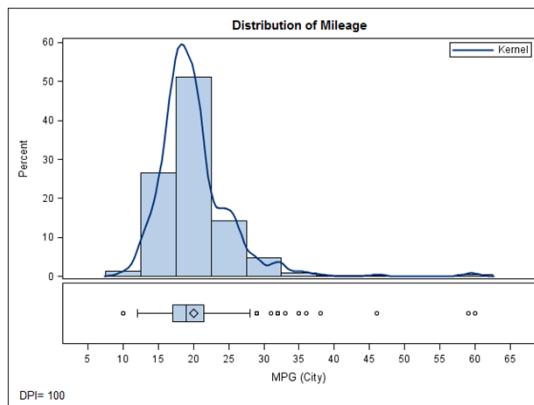
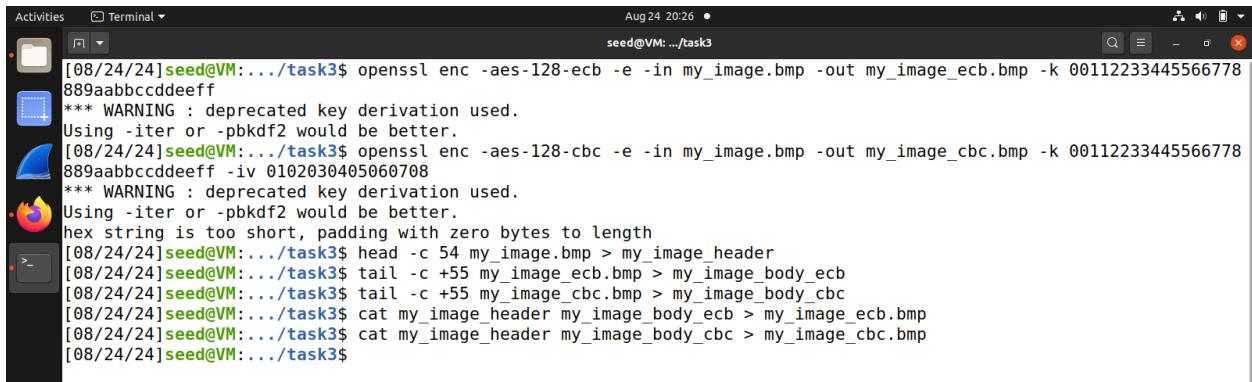


Figure 7. my_image.bmp

- Commands to run.

- \$ openssl enc -aes-128-ecb -e -in my_image.bmp -out my_image_ecb.bmp -k 0011223344556677889aabbcdddeeff
 - \$ openssl enc -aes-128-cbc -e -in my_image.bmp -out my_image_cbc.bmp -k 0011223344556677889aabbcdddeeff -iv 0102030405060708
 - \$head -c 54 my_image.bmp > my_image_header
 - \$tail -c +55 my_image_ecb.bmp > my_image_body_ecb
 - \$tail -c +55 my_image_cbc.bmp > my_image_body_cbc
 - \$cat my_image_header my_image_body_ecb > my_image_ecb.bmp
 - \$cat my_image_header my_image_body_cbc > my_image_cbc.bmp



```

Activities Terminal Aug 24 20:26 •
seed@VM:.../task3
[08/24/24]seed@VM:.../task3$ openssl enc -aes-128-ecb -e -in my_image.bmp -out my_image_ecb.bmp -k 0011223344556677889aabbcdddeeff
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/24/24]seed@VM:.../task3$ openssl enc -aes-128-cbc -e -in my_image.bmp -out my_image_cbc.bmp -k 0011223344556677889aabbcdddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/24/24]seed@VM:.../task3$ head -c 54 my_image.bmp > my_image_header
[08/24/24]seed@VM:.../task3$ tail -c +55 my_image_ecb.bmp > my_image_body_ecb
[08/24/24]seed@VM:.../task3$ tail -c +55 my_image_cbc.bmp > my_image_body_cbc
[08/24/24]seed@VM:.../task3$ cat my_image_header my_image_body_ecb > my_image_ecb.bmp
[08/24/24]seed@VM:.../task3$ cat my_image_header my_image_body_cbc > my_image_cbc.bmp
[08/24/24]seed@VM:.../task3$
```

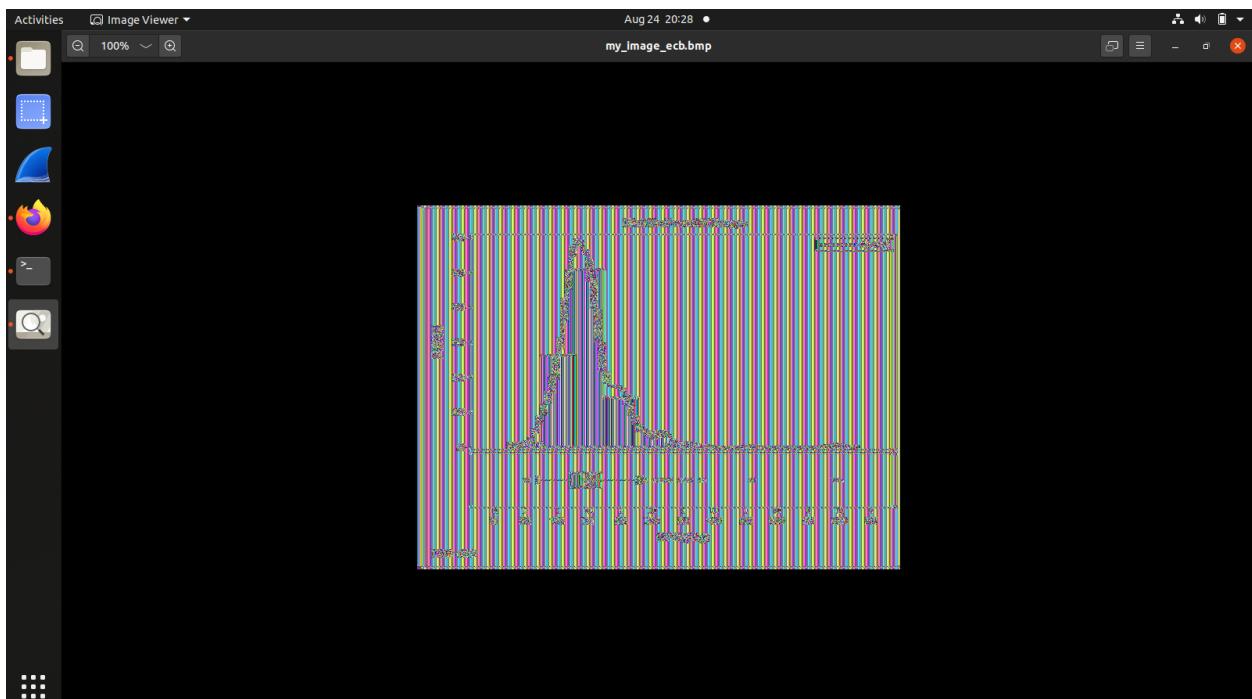


Figure 8. my_image_ecb.bmp

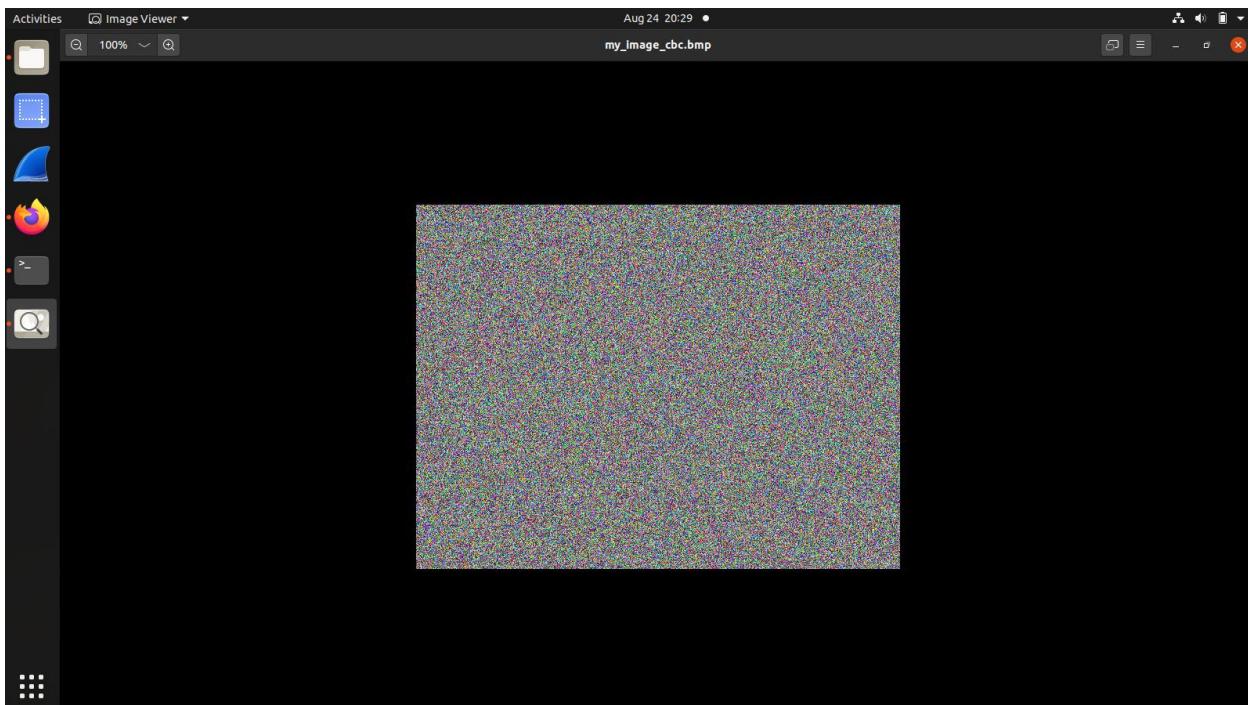


Figure 9. my_image_cbc.bmp

Task 4: Padding

- We will be encrypting 3 files of lengths 5 bytes, 10 bytes and 16 bytes respectively using ECB, CBC, CFB and OFB modes of encrypting a file.
- We will be using the below ciphers
 - **aes-128-ecb** (Block cipher)(Doesn't require IV for encryption)
 - **aes-128-cbc** (Block cipher)
 - **cast5-cfb** (Converts block cipher to stream cipher)
 - **cast5-ofb** (Converts block cipher to stream cipher)
- Similarly for 10 bytes and 16 bytes file.
- Let's create files of sizes 5, 10 and 16 bytes.

```
Activities Terminal Aug 27 16:51 seed@VM: .../task4
[08/27/24]seed@VM:.../task4$ echo -n whyme > 5.txt
[08/27/24]seed@VM:.../task4$ echo -n whymeitsok > 10.txt
[08/27/24]seed@VM:.../task4$ echo -n whymeitsokimfine > 16.txt
[08/27/24]seed@VM:.../task4$ ls -l
total 2
-rwxrwx--- 1 root vboxsf 10 Aug 27 16:49 10.txt
-rwxrwx--- 1 root vboxsf 16 Aug 27 16:51 16.txt
-rwxrwx--- 1 root vboxsf 5 Aug 27 16:49 5.txt
[08/27/24]seed@VM:.../task4$
```

1. 5 bytes file

- ECB

```
Activities Terminal Aug 27 16:57 seed@VM: .../task4
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-ecb -e -in 5.txt -out 5_ecb.bin -k 00112233445566778889aabccddeef
f
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-ecb -d -in 5_ecb.bin -out 5_ecb_decrypt.txt -nopad -k 001122334455
66778889aabccddeeff
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task4$ xxd 5_ecb_decrypt.txt
00000000: 7768 796d 650b 0b0b 0b0b 0b0b 0b0b 0b0b whyme.....
[08/27/24]seed@VM:.../task4$
```

- CBC

```
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-cbc -e -in 5.txt -out 5_cbc.bin -k 00112233445566778889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-cbc -d -in 5_cbc.bin -out 5_cbc_decrypt.txt -nopad -k 00112233445566778889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/27/24]seed@VM:.../task4$ xxd 5_cbc_decrypt.txt
00000000: 7768 796d 650b 0b0b 0b0b 0b0b 0b0b 0b0b whyme.....
[08/27/24]seed@VM:.../task4$
```

- CFB

```
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-cfb -e -in 5.txt -out 5_cfb.bin -k 00112233445566778889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-cfb -d -in 5_cfb.bin -out 5_cfb_decrypt.txt -nopad -k 00112233445566778889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task4$ xxd 5_cfb_decrypt.txt
00000000: 7768 796d 65 0b0b 0b0b 0b0b 0b0b 0b0b whyme
[08/27/24]seed@VM:.../task4$
```

- OFB

```
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-ofb -e -in 5.txt -out 5_ofb.bin -k 00112233445566778889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-ofb -d -in 5_ofb.bin -out 5_ofb_decrypt.txt -nopad -k 00112233445566778889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task4$ xxd 5_ofb_decrypt.txt
00000000: 7768 796d 65 0b0b 0b0b 0b0b 0b0b 0b0b whyme
[08/27/24]seed@VM:.../task4$
```

2. 10 bytes file

- ECB

```
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-ecb -e -in 10.txt -out 10_ecb.bin -k 00112233445566778889aabccddeeff
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-ecb -d -in 10_ecb.bin -out 10_ecb_decrypt.txt -nopad -k 00112233445566778889aabccddeeff
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task4$ xxd 10_ecb_decrypt.txt
00000000: 7768 796d 6569 7473 6f6b 0606 0606 0606 whymeitsok.....
[08/27/24]seed@VM:.../task4$
```

- CBC

```
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-cbc -e -in 10.txt -out 10_cbc.bin -k 00112233445566778889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-cbc -d -in 10_cbc.bin -out 10_cbc_decrypt.txt -nopad -k 00112233445566778889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/27/24]seed@VM:.../task4$ xxd 10_cbc_decrypt.txt
00000000: 7768 796d 6569 7473 6f6b 0606 0606 0606 whymeitsok.....
[08/27/24]seed@VM:.../task4$
```

- CFB

```
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-cfb -e -in 10.txt -out 10_cfb.bin -k 00112233445566778889aabcccddef  
f -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-cfb -d -in 10_cfb.bin -out 10_cfb_decrypt.txt -nopad -k 00112233445566778889aabcccddef  
66778889aabcccddef -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ xxd 10_cfb_decrypt.txt  
00000000: 7768 796d 6569 7473 6f6b whymeitsok  
[08/27/24]seed@VM:.../task4$
```

- OFB

```
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-ofb -e -in 10.txt -out 10_ofb.bin -k 00112233445566778889aabcccddef  
f -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-ofb -d -in 10_ofb.bin -out 10_ofb_decrypt.txt -nopad -k 00112233445566778889aabcccddef  
66778889aabcccddef -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ xxd 10_ofb_decrypt.txt  
00000000: 7768 796d 6569 7473 6f6b whymeitsok  
[08/27/24]seed@VM:.../task4$
```

3. 16 bytes file

- ECB

```
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-ecb -e -in 16.txt -out 16_ecb.bin -k 00112233445566778889aabcccddef  
eff  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-ecb -d -in 16_ecb.bin -out 16_ecb_decrypt.txt -k 00112233445566778889aabcccddef  
889aabcccddef  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ xxd 16_ecb_decrypt.txt  
00000000: 7768 796d 6569 7473 6f6b 696d 6669 6e65 whymeitsokimfine  
[08/27/24]seed@VM:.../task4$
```

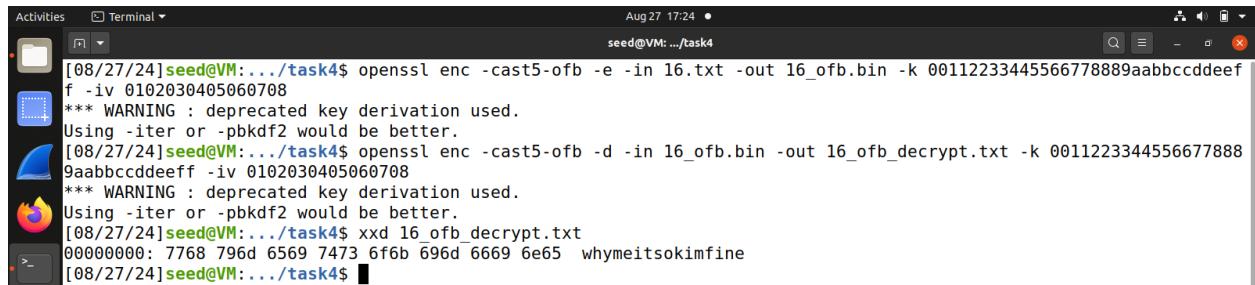
- CBC

```
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-cbc -e -in 16.txt -out 16_cbc.bin -k 00112233445566778889aabcccddef  
eff -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
hex string is too short, padding with zero bytes to length  
[08/27/24]seed@VM:.../task4$ openssl enc -aes-128-cbc -d -in 16_cbc.bin -out 16_cbc_decrypt.txt -nopad -k 00112233445566778889aabcccddef  
5566778889aabcccddef -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
hex string is too short, padding with zero bytes to length  
[08/27/24]seed@VM:.../task4$ xxd 16_cbc_decrypt.txt  
00000000: 7768 796d 6569 7473 6f6b 696d 6669 6e65 whymeitsokimfine  
00000010: 1010 1010 1010 1010 1010 1010 1010 .....  
[08/27/24]seed@VM:.../task4$
```

- CFB

```
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-cfb -e -in 16.txt -out 16_cfb.bin -k 00112233445566778889aabcccddef  
f -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-cfb -d -in 16_cfb.bin -out 16_cfb_decrypt.txt -nopad -k 00112233445566778889aabcccddef  
66778889aabcccddef -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ xxd 16_cfb_decrypt.txt  
00000000: 7768 796d 6569 7473 6f6b 696d 6669 6e65 whymeitsokimfine  
[08/27/24]seed@VM:.../task4$
```

- OFB



```
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-ofb -e -in 16.txt -out 16_ofb.bin -k 0011223344556677889aabcccddef  
f -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ openssl enc -cast5-ofb -d -in 16_ofb.bin -out 16_ofb_decrypt.txt -k 0011223344556677889aabcccddef  
9aabcccddef -iv 0102030405060708  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
[08/27/24]seed@VM:.../task4$ xxd 16_ofb_decrypt.txt  
00000000: 7768 796d 6569 7473 6f6b 696d 6669 6e65 whymeitsokimfine  
[08/27/24]seed@VM:.../task4$
```

- ECB and CBC mode of cipher performs padding to the plaintext while encrypting. The point is that these types of encryption modes require the size of the plaintext to be equal to the block size and hence it pads to the plaintext in order to perform encryption efficiently.
- Unlike the modes aforementioned, CFB and OFB don't perform any padding while encryption. This is because these modes convert the plaintext from blocks to stream cipher.
- For all the files are padded with the data that is based on the sizes of the files. Let's take an example where the size of the file is 5 bytes. For making the length equal to the key size of 128 bits or 16 bytes, we need 11 more bytes. In hexadecimal notation, it is 0x0b. And this is the data padded 11 times at the end of the 5 bytes file. Similarly, for the 10 bytes file, we need 0x06 data repeated for 6 times.

Task 5: Error Propagation – Corrupted Cipher Text

- I'll create a new folder task5 and copied task1.txt file (the decrypted file of task1) in order to keep everything transparent and clear. I'll perform encryption of task1.txt using aes-128-ecb, aes-128-cbc, cast5-cfb and cast5-ofb modes of encryption. Once I encrypt, using bless hex editor, I'll make change to the 1st bit of the 55th byte of the encrypted file and then decrypt it.



```
[08/27/24]seed@VM:.../Files$ mkdir task5  
[08/27/24]seed@VM:.../Files$ cp ./task1/task1.txt ./task5/task1.txt  
[08/27/24]seed@VM:.../Files$ cd task5  
[08/27/24]seed@VM:.../task5$ ls -l  
total 8  
-rwxrwx--- 1 root vboxsf 4759 Aug 27 20:23 task1.txt  
[08/27/24]seed@VM:.../task5$
```

```
[08/27/24]seed@VM:.../task5$ cat task1.txt
THE OSCARS TURN ON SUNDAY WHICH SEEKS 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
```

- **ECB:** Using ECB mode, only the block that has the corrupted cipher byte can't be retrieved and the rest of the file should be good as this mode is independent of other ciphers while decrypting. (Also called parallel encryption/decryption)
- **CBC:** During the decryption process, we first decrypt the cipher block with a correct key and then perform XOR operation with the IV. This will give us a plaintext of the first block. For the next block, we perform the same method but this time we take the previous block's cipher text instead of the IV. While decrypting the 55th byte containing block, we get corrupted plaintext due to the corrupted cipher block and then as we changed one bit in the cipher text, it gets propagated to the next block's plaintext resulting in change of one bit of the block.
- **CFB:** In this case, the bytes in the corrupted block can't be fetched along with the next couple of blocks or may be one or two as we take bits from the plaintext and use them in the shift register for decrypting the next block.
- **OFB:** The decryption of corrupted cipher text would yield us the plaintext except the byte that is corrupted as here we won't be passing the cipher text to the next stream of bits during encryption/decryption; instead we pass the 8 selected bits to the shift register.

1. ECB

- Encryption using aes-128-ecb:

```
[08/27/24]seed@VM:.../task5$ openssl enc -aes-128-ecb -e -in task1.txt -out ecb.txt -k 00112233445566778889aabccdde
eff
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task5$
```

- Actual Cipher Text:

00000000	53	61	6C	74	65	64	5F	5F	9C	F4	D7	BA	23	59	90	CE	61	95	37	22	A7	84	E2	00	2B	76	51	Salted.....#Y..a.7"....+vQ
0000001b	43	CF	DE	C6	36	B9	79	9F	43	9B	DA	09	BC	C6	27	79	69	C2	63	57	95	B4	07	22	08	61	AC	C....6.y.C.....'yi.cW..."a.
00000036	72	9F	D9	EA	14	B3	CA	76	D6	4E	9E	40	AB	8E	17	C6	3D	F6	EA	53	20	8F	00	D7	49	EA	85	r.....v.N.@....=..S...I...
00000051	BA	34	53	F9	03	8A	CC	73	D2	38	44	39	90	21	FE	15	73	50	CF	81	84	13	E2	C3	D5	2E	7E	74S....s.8D9.!..sP.....~

- Corrupted Cipher Text (note the change in 55th byte):

```
/media/sf_CSP_544/Labsetup/Files/task5/ecb.txt * - Bless
File Edit View Search Tools Help
ecb.txt* x
00000000 53 61 6C 74 65 64 5F 5F 9C F4 D7 BA 23 59 90 CE 61 95 37 22 A7 84 E2 00 2B 76 51 | Salted_____#Y..a.7"....+vQ
00000018 43 CF DE C6 36 B9 79 9F 43 9B DA 09 BC C6 27 79 69 C2 63 57 95 B4 07 22 08 61 AC C...6.y.C.....'yi.cW...".a.
00000036 F2 9F D9 EA 14 B3 CA 76 D6 4E 9E 40 AB 8E 17 C6 3D F6 EA 53 20 8F 00 D7 49 EA 85 .....v.N.@....=..S ...I...
00000051 BA 34 53 F9 03 8A CC 73 D2 38 44 39 90 21 FE 15 73 50 CF 81 84 13 E2 C3 D5 2E 7E -4s....s.8D9.!..sP.....~
```

- Decryption of corrupted cipher file:

```
[08/27/24]seed@VM:.../task5$ openssl enc -aes-128-ecb -d -in ecb_corrupt.txt -out ecb_corrupt_plain.txt -k 0011223344556677889aabbccddeeff
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task5$
```

[08/27/24]seed@VM:.../task5\$ cat ecb_corrupt_plain.txt

THE OSCARS TURN ON SUNDAY WHICH6;65p6)=Jp:0HT 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 SPOTTED 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

```
[08/27/24]seed@VM:.../task5$ hexdump -C ecb_corrupt_plain.txt
00000000 54 48 45 20 4f 53 43 41 52 53 20 54 55 52 4e 20 |THE OSCARS TURN |
00000010 20 4f 4e 20 53 55 4e 44 41 59 20 57 48 49 43 48 |ON SUNDAY WHICH|
00000020 36 3b d3 35 ee 70 36 29 3d 4a 70 90 3a 18 e3 fb |6; .5.p6)=Jp:0...|
00000030 48 54 20 41 46 54 45 52 20 54 48 49 53 20 4c 4f |HT AFTER THIS LO|
00000040 4e 47 20 53 54 52 41 4e 47 45 0a 41 57 41 52 44 |NG STRANGE.AWARD|
00000050 53 20 54 52 49 50 20 54 48 45 20 42 41 47 45 |S TRIP THE BAGGE|
00000060 52 20 46 45 45 4c 53 20 4c 49 4b 45 20 41 20 4e |R FEELS LIKE A N|
00000070 4f 4e 41 47 45 4e 41 52 49 41 4e 20 54 4f 0a |ONAGENARIAN TOO.|
00000080 0a 54 48 45 20 41 57 41 52 44 53 20 52 41 43 45 |.THE AWARDS RACE|
00000090 20 57 41 53 20 42 4f 4f 4b 45 4e 44 45 44 20 42 | WAS BOOKENDED B|
000000a0 59 20 54 48 45 20 44 45 4d 49 53 45 20 4f 46 20 |Y THE DEMISE OF |
000000b0 48 41 52 56 45 59 20 57 45 49 4e 53 54 45 49 4e |HARVEY WEINSTEIN|
```

2. CBC

- Encryption using aes-128-cbc:

```
[08/27/24]seed@VM:.../task5$ openssl enc -aes-128-cbc -e -in task1.txt -out cbc.txt -k 0011223344556677889aabbccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/27/24]seed@VM:.../task5$
```

- Actual Cipher

```
/media/sf_CSP_544/Labsetup/Files/task5/cbc.txt - Bless
File Edit View Search Tools Help
cbc.txt x
00000000 53 61 6C 74 65 64 5F 5F 2A 17 33 C4 1F 18 C1 8F C7 A6 04 CC 8E 9F 35 D2 ED 05 0A | Salted_*...5...
0000001b DF C5 A6 50 10 FC E1 99 A2 54 55 40 41 2C E9 82 A3 4F BC BE AD 8B F3 A1 2A C8 A5 ...P....TU@A,...O....*...
00000036 47 59 A8 F9 A0 EC FB 36 BE 89 C7 EF 23 27 9E 99 52 EA 2F D3 78 5A F6 BA F3 C2 CF GY....6...#'.R./.xZ...
00000051 45 C9 1C 03 A8 67 2A CC CA 54 44 1C 11 65 39 64 7F 7C 96 4C B5 5D 1C 3F 69 38 BF E....g*.TD.e9d.|.L.|?i8.
0000006c 51 0B 6D D1 10 F1 33 72 4E 93 86 3B 65 C5 42 24 69 88 0B 22 89 40 38 A3 34 77 1F |Q.m...3rN..;e.B$!..".@8.4w.
```

- Corrupted Cipher Text (note the change in 55th byte):

```
/media/sf_CSP_544/Labsetup/Files/task5/cbc.txt* - Bless
File Edit View Search Tools Help
cbc.txt* x
00000000 53 61 6C 74 65 64 5F 5F 2A 17 33 C4 1F 18 C1 8F C7 A6 04 CC 8E 9F 35 D2 ED 05 0A | Salted_*...5...
0000001b DF C5 A6 50 10 FC E1 99 A2 54 55 40 41 2C E9 82 A3 4F BC BE AD 8B F3 A1 2A C8 A5 ...P....TU@A,...O....*...
00000036 C7 59 A8 F9 A0 EC FB 36 BE 89 C7 EF 23 27 9E 99 52 EA 2F D3 78 5A F6 BA F3 C2 CF .Y....6...#'.R./.xZ...
00000051 45 C9 1C 03 A8 67 2A CC CA 54 44 1C 11 65 39 64 7F 7C 96 4C B5 5D 1C 3F 69 38 BF E....g*.TD.e9d.|.L.|?i8.
0000006c 51 0B 6D D1 10 F1 33 72 4E 93 86 3B 65 C5 42 24 69 88 0B 22 89 40 38 A3 34 77 1F |Q.m...3rN..;e.B$!..".@8.4w.
```

- Decryption of corrupted cipher file:

```
Aug 27 20:50 • seed@VM: .../task5
[08/27/24]seed@VM:.../task5$ openssl enc -aes-128-cbc -d -in cbc_corrupt.txt -out cbc_corrupt_plain.txt -k 0011223344556677889aabccddeef
4556677889aabccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
[08/27/24]seed@VM:.../task5$ cat cbc_corrupt_plain.txt
THE OSCARS TURN ON SUNDAY WHICH t1000000HT AFTOR 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

Aug 27 20:51 • seed@VM: .../task5
[08/27/24]seed@VM:.../task5$ hexdump -C cbc_corrupt_plain.txt
00000000 54 48 45 20 4f 53 43 41 52 53 20 54 55 52 4e 20 |THE OSCARS TURN |
00000010 20 4f 4e 20 53 55 4e 44 41 59 20 57 48 49 43 48 |ON SUNDAY WHICH|
00000020 e6 09 74 7c e8 ef ae c2 0f 92 1e 12 a0 f9 6f 17 |..t|.....o.|
00000030 48 54 20 41 46 54 c5 52 20 54 48 49 53 20 4c 4f |HT AFT.R THIS LO|
00000040 4e 47 20 53 54 52 41 4e 47 45 0a 41 57 41 52 44 |NG STRANGE.AWARD|
00000050 53 20 54 52 49 50 20 54 48 45 20 42 41 47 45 |S TRIP THE BAGGE|
00000060 52 20 46 45 45 c5 20 4c 49 4b 45 20 41 20 4e |R FEELS LIKE A N|
00000070 4f 4e 41 47 45 4e 41 52 49 41 4e 20 54 4f 4f 0a |ONAGENARIAN TOO.|
00000080 0a 54 48 45 20 41 57 41 52 44 53 20 52 41 43 45 |.THE AWARDS RACE|
00000090 20 57 41 53 20 42 4f 4f 4b 45 4e 44 45 44 20 42 | WAS BOOKENDED B|
000000a0 59 20 54 48 45 20 44 45 4d 49 53 45 20 4f 46 20 |Y THE DEMISE OF |
000000b0 48 41 52 56 45 59 20 57 45 49 4e 53 54 45 49 4e |HARVEY WEINSTEIN|
```

3. CFB

- Encryption using cast5-cfb:

```
Aug 27 20:53 • seed@VM: .../tasks
[08/27/24]seed@VM:.../task5$ openssl enc -cast5-cfb -e -in task1.txt -out cfb.txt -k 0011223344556677889aabccddeef
f -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task5$
```

- Actual Cipher Text:

```
/media/sf_CSP_544/Labsetup/Files/task5/cfb.txt - Bless
File Edit View Search Tools Help
cfb.txt x
00000000 53 61 6C 74 65 64 5F 5F D0 6E 9E AA A2 ED DA 0B 36 08 86 70 F9 24 A3 32 5C 3C 77 | Salted_.n.....6..p.$.2\<w
0000001b 75 A8 8A 70 5D 38 4E 3C D6 51 CD A7 F5 F6 66 08 0F 2D 38 3E 9D A0 FC 1D 84 BC 03 u..p]8N<.Q....f..-8>.....
00000036 A8 E4 AC EE C5 94 ED A3 99 5D 57 D5 91 35 03 01 54 13 ED 36 B1 5D 33 AD FE .....]W...c5..T..6.]3...
00000051 EF CF 2E 0F 95 EF C5 4D 56 71 3F 7E 9D CC 75 AB 08 48 F3 6A 7F EA 8D C6 74 EF AB .....MVg?~..u..H.j....t..
0000006c 45 5D 01 D0 31 82 80 5D 51 BC D0 7E 10 30 2A 8C B9 01 B5 FD A8 0C 33 49 6D 4B 3F E]..1..]Q..~.0*.....3ImK?
```

- Corrupted Cipher Text (note the change in 55th byte):

```
/media/sf_CSP_544/Labsetup/Files/task5/cfb_corrupt.txt - Bless
File Edit View Search Tools Help
cfb_corrupt.txt x
00000000| 53 61 6C 74 65 64 5F 5F D0 6E 9E AA A2 ED DA 0B 36 08 86 70 F9 24 A3 32 5C 3C 77| Salted....n.....6..p.$.2\<w
0000001b| 75 A8 8A 70 5D 38 4E 3C D6 51 CD A7 F6 66 08 0F 2D 38 3E 9D A0 FC 1D 84 BC 03 u..p!8N<.Q...f..-8>.....
00000036| A8 E4 AC EE C5 94 ED A3 99 5D 57 D9 D5 91 63 35 03 01 54 13 ED 36 B1 5D 33 AD FE .....]W...c5.T..6.]3...
00000051| 6F CF 2E 0F 95 EF C5 4D 56 71 3F 7E 9D CC 75 AB OB 48 F3 6A 7F EA 8D C6 74 EF AB o.....MVq?~..u..H.j.....
0000006c| 45 5D 01 D0 31 82 80 5D 51 BC D0 7E 10 30 2A 8C B9 01 B5 FD A8 OC 33 49 6D 4B 3F E]..1..]Q..~.0*.....3IMK?
```

- Decryption of corrupted cipher file:

```
[08/27/24]seed@VM:.../task5$ openssl enc -cast5-cfb -d -in cfb_corrupt.txt -out cfb_corrupt_plain.txt -k 0011223344556677889aabcccddeeff
[08/27/24]seed@VM:.../task5$ cat cfb_corrupt_plain.txt
THE OSCARS TURN ON SUNDAY WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO

[08/27/24]seed@VM:.../task5$ hexdump -C cfb_corrupt_plain.txt
00000000 54 48 45 20 4f 53 43 41 52 53 20 54 55 52 4e 20 | THE OSCARS TURN |
00000010 20 4f 4e 20 53 55 4e 44 41 59 20 57 48 49 43 48 | ON SUNDAY WHICH|
00000020 20 53 45 45 4d 53 20 41 42 4f 55 54 20 52 49 47 | SEEMS ABOUT RIG|
00000030 48 54 20 41 46 54 45 52 20 54 48 49 53 20 4c 4f | HT AFTER THIS LO|
00000040 4e c7 20 53 54 52 41 4e c2 8b ad a5 5d dd e4 1e | N. STRAN....]...|
00000050 53 20 54 52 49 50 20 54 48 45 20 42 41 47 45 | S TRIP THE BAGGE|
00000060 52 20 46 45 45 4c 53 20 4c 49 4b 45 20 41 20 4e | R FEELS LIKE A N|
00000070 4f 4e 41 47 45 4e 41 52 49 41 4e 20 54 4f 4f 0a | ONAGENARIAN TOO.|
00000080 0a 54 48 45 20 41 57 41 52 44 53 20 52 41 43 45 | .THE AWARDS RACE|
00000090 20 57 41 53 20 42 4f 4f 4b 45 4e 44 45 44 20 42 | WAS BOOKENDED B|
000000a0 59 20 54 48 45 20 44 45 4d 49 53 45 20 4f 46 20 | Y THE DEMISE OF |
000000b0 48 41 52 56 45 59 20 57 45 49 4e 53 54 45 49 4e | HARVEY WEINSTEIN|
000000c0 20 41 54 20 49 54 53 20 4f 55 54 53 45 54 0a 41 | AT ITS OUTSET.A|
000000d0 4e 44 20 54 48 45 20 41 50 50 41 52 45 4e 54 20 | ND THE APPARENT |
```

4. OFB

- Encryption using cast5-ofb:

```
[08/27/24]seed@VM:.../task5$ openssl enc -cast5-ofb -e -in task1.txt -out ofb.txt -k 0011223344556677889aabcccddeeff
[08/27/24]seed@VM:.../task5$
```

- Actual Cipher Text:

```
/media/sf_CSP_544/Labsetup/Files/task5/ofb.txt - Bless
File Edit View Search Tools Help
ofb.txt x
00000000| 53 61 6C 74 65 64 5F 5F 1E E6 8B 9D 6D 11 66 23 24 B1 B2 02 A5 A8 9D AA 53 09 4C| Salted....m.f#$.....S.L
0000001b| E9 09 3F 3F 71 D1 D0 12 51 B1 B8 B1 4D 27 F3 DF 03 43 B7 88 C5 FF 31 76 1B 53 ..?q...Q...M'....C....lv.S
00000036| EA 8C 7C 0E 73 9C FA C8 4A 50 52 D8 64 58 DE 59 1F 13 3A D5 21 EC D7 6E F6 DB 66 ..|s...JPR.dX.Y...!:!.n..f
00000051| 0E 48 76 4C C9 5F E1 7B DD BF 15 FC 07 94 0D 6E 7A D6 77 54 1E B2 66 CF 8C BD D6 .HvL._.{....nz.wT..f....
0000006c| 93 08 13 5C 2E A9 A5 C8 56 7C 11 33 BB B0 86 7E F7 7F 0C BE A1 A5 8B B6 A5 1A DD ..\..V|.3..~.....
```

- Corrupted Cipher Text (note the change in 55th byte):

```
/media/sf_CSP_544/Labsetup/Files/task5/ofb_corrupt.txt - Bless
File Edit View Search Tools Help
ofb_corrupt.txt x
00000000| 53 61 6C 74 65 64 5F 5F 1E E6 8B 9D 6D 11 66 23 24 B1 B2 02 A5 A8 9D AA 53 09 4C| Salted....m.f#$.....S.L
0000001b| E9 09 3F 3F 71 D1 D0 12 51 B1 B8 B1 4D 27 F3 DF 03 43 B7 88 C5 FF 31 76 1B 53 ..?q...Q...M'....C....lv.S
00000036| EA 8C 7C 0E 73 9C FA C8 4A 50 52 D8 64 58 DE 59 1F 13 3A D5 21 EC D7 6E F6 DB 66 ..|s...JPR.dX.Y...!:!.n..f
00000051| 0E 48 76 4C C9 5F E1 7B DD BF 15 FC 07 94 0D 6E 7A D6 77 54 1E B2 66 CF 8C BD D6 .HvL._.{....nz.wT..f....
0000006c| 93 08 13 5C 2E A9 A5 C8 56 7C 11 33 BB B0 86 7E F7 7F 0C BE A1 A5 8B B6 A5 1A DD ..\..V|.3..~.....
```

- Decryption of corrupted cipher file:

```
[08/27/24]seed@VM:.../task5$ openssl enc -cast5-ofb -d -in ofb_corrupt.txt -out ofb_corrupt_plain.txt -k 001122334455
56677889aabbccddeeff -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[08/27/24]seed@VM:.../task5$ cat ofb_corrupt_plain.txt
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
```

```
[08/27/24]seed@VM:.../task5$ hexdump -C ofb_corrupt_plain.txt
00000000 54 48 45 20 4f 53 43 41 52 53 20 54 55 52 4e 20 |THE OSCARS TURN |
00000010 20 4f 4e 20 53 55 4e 44 41 59 20 57 48 49 43 48 |ON SUNDAY WHICH|
00000020 20 53 45 45 4d 53 20 41 42 4f 55 54 20 52 49 47 |SEEMS ABOUT RIG|
00000030 48 54 20 41 46 45 52 20 54 48 49 53 20 4c 4f |HT AFTER THIS LO|
00000040 4e d7 20 53 54 52 41 4e 47 45 0a 41 57 41 52 44 |N. STRANGE.AWARD|
00000050 53 20 54 52 49 50 20 54 48 45 20 42 41 47 45 |S TRIP THE BAGGE|
00000060 52 20 46 45 45 4c 53 20 4c 49 4b 45 20 41 20 4e |R FEELS LIKE A N|
00000070 4f 4e 41 47 45 4e 41 52 49 41 4e 20 54 4f 4f 0a |ONAGENARIAN TOO.|
00000080 0a 54 48 45 20 41 57 41 52 44 53 20 52 41 43 45 |.THE AWARDS RACE|
00000090 20 57 41 53 20 42 4f 4f 4b 45 4e 44 45 44 20 42 |WAS BOOKENDED B|
000000a0 59 20 54 48 45 20 44 45 4d 49 53 45 20 4f 46 20 |Y THE DEMISE OF|
000000b0 48 41 52 56 45 59 20 57 45 49 4e 53 54 45 49 4e |HARVEY WEINSTEIN|
000000c0 20 41 54 20 49 54 53 20 4f 55 54 53 45 54 0a 41 |AT ITS OUTSET.A|
000000d0 4e 44 20 54 48 45 20 41 50 50 41 52 45 4e 54 20 |ND THE APPARENT|
000000e0 49 4d 50 4c 4f 53 49 4f 4e 20 4f 46 20 48 49 53 |IMPLOSION OF HIS|
000000f0 20 46 49 4c 4d 20 43 4f 4d 50 41 4e 59 20 41 54 |FILM COMPANY AT|
00000100 20 54 48 45 20 45 4e 44 20 41 4e 44 20 49 54 20 |THE END AND IT|
00000110 57 41 53 20 53 48 41 50 45 44 20 42 59 0a 54 48 |WAS SHAPED BY.TH|
00000120 45 20 45 4d 45 52 47 45 4e 43 45 20 4f 46 20 4d |E EMERGENCE OF M|
00000130 45 54 4f 4f 20 54 49 4d 45 53 20 55 50 20 42 4c |ETO0 TIMES UP BL|
00000140 41 43 4b 47 4f 57 4e 20 50 4f 4c 49 54 49 43 53 |ACKGOWN POLITICS|
00000150 20 41 52 4d 43 41 4e 44 59 20 41 43 54 49 56 49 |ARMCANDY ACTIVI|
00000160 53 4d 20 41 4e 44 0a 41 20 4e 41 54 49 4f 4e 41 |SM AND.A NATIONA|
```

Out of the 4 expected observations, 3 are correct. CFB looks wrong; the cause might be the fact that the bits used in the shift register weren't a part of the corrupted byte.

Task 6: Initial Vector (IV) and Common Mistakes

Task 6.1. IV Experiment

We create a file `text.txt` which has the string "Hello, I love Cybersecurity" as input for encryption and the encryption mode here is `aes-128-cbc`. For the first 2 encryptions, I've used different initial vectors and the last command used the same initial vector.

- Output cipher file for 1st encryption using IV1: `enc1.bin`
- Output cipher file for 2nd encryption using IV2: `enc2.bin`
- Output cipher file for 3rd encryption using IV1: `enc3.bin`

Let us compare 1st and 2nd cipher files and then 1st and 3rd cipher files using the `$hexdump -C <file_name>`.

```

[08/29/24]seed@VM:.../task6$ echo -n You are in safe hands > text.txt
[08/29/24]seed@VM:.../task6$ openssl enc -aes-128-cbc -e -in text.txt -out enc1.bin -K 00112233445566778889aabbccdde
eff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[08/29/24]seed@VM:.../task6$ openssl enc -aes-128-cbc -e -in text.txt -out enc2.bin -K 00112233445566778889aabbccdde
eff -iv 1020304050607080
hex string is too short, padding with zero bytes to length
[08/29/24]seed@VM:.../task6$ openssl enc -aes-128-cbc -e -in text.txt -out enc3.bin -K 00112233445566778889aabbccdde
eff -iv 0102030405060708
hex string is too short, padding with zero bytes to length
[08/29/24]seed@VM:.../task6$ hexdump -C enc1.bin
00000000 ba 2d a1 13 62 b4 25 c1 e2 91 c4 8a f6 a2 83 49 |....b.%.....I|
00000010 be fc 74 62 ca 96 77 8e 66 b2 e1 2f 29 0a 67 af |..tb..w.f../).g.|
00000020
[08/29/24]seed@VM:.../task6$ hexdump -C enc2.bin
00000000 a1 cd f7 ab 84 d0 73 04 49 aa 98 23 be 5b 0b 21 |.....s.I..#.!.|
00000010 af 2f fe fb 33 cb 6d ef e5 33 98 05 71 8e 40 ee |./..3.m..3..q.@.|
00000020
[08/29/24]seed@VM:.../task6$ hexdump -C enc3.bin
00000000 ba 2d a1 13 62 b4 25 c1 e2 91 c4 8a f6 a2 83 49 |....b.%.....I|
00000010 be fc 74 62 ca 96 77 8e 66 b2 e1 2f 29 0a 67 af |..tb..w.f../).g.|
00000020
[08/29/24]seed@VM:.../task6$ 

```

- If we observe carefully, we see that using the same IV for a key and encrypt a file; we obtain the same cipher text. This signifies the importance of having unique initial vector. We should be selecting different IV for a key in order to make it difficult for an adversary to predict the plaintext.
- enc1.bin and enc3.bin have the same information stored and enc2.bin is different because of the change in IV while encrypting.

Task 6.2. Common Mistake: Use the Same IV

- For this task, I've developed a script task6_2.py which performs operations similar to sample.py. Below is task6_2.py. The script is self-explanatory for any python developer as it's a basic code that converts ASCII to HEX and then to BYTE ARRAY and finally back from HEX to ASCII.
- This script performs XOR operations to find plaintexts and keys. It starts by defining a function to XOR two byte arrays. The user is prompted to enter the first plaintext (P1) and two cipher texts in hexadecimal format (C1 and C2). The script then converts these inputs into byte arrays. Using XOR, it calculates the key by XOR-ing the plaintext with the first cipher text and prints the key in hexadecimal format. It then calculates the second plaintext by XOR-ing the key with the second cipher text and prints the result both in hexadecimal and ASCII formats.

```

#!/usr/bin/python3

# XOR two bytearrays
def xor(first, second):
    return bytearray(x^y for x,y in zip(first, second))

MSG1 = input("Enter Plaintext (P1): ")
HEX_1 = input("Enter Ciphertext (C1): ")

# Convert ascii string to bytearray
D1 = bytes(MSG1, 'utf-8')
HEX_2 = input("Enter Ciphertext (C2): ")

# Convert hex string to bytearray
D2 = bytearray.fromhex(HEX_1)
D3 = bytearray.fromhex(HEX_2)

r1 = xor(D1, D2)
print("Key = P1 XOR C1 = ",r1.hex())
r2 = xor(r1, D3)
print("P2 = Key XOR C2 = ",r2.hex(),"\nPlaintext P2 in ASCII: ",r2.decode("ASCII"))

```

```

#!/usr/bin/python3

# XOR two bytearrays
def xor(first, second):
    return bytearray(x^y for x,y in zip(first, second))

MSG1 = input("Enter Plaintext (P1): ")
HEX_1 = input("Enter Ciphertext (C1): ")

# Convert ascii string to bytearray
D1 = bytes(MSG1, 'utf-8')
HEX_2 = input("Enter Ciphertext (C2): ")

# Convert hex string to bytearray
D2 = bytearray.fromhex(HEX_1)
D3 = bytearray.fromhex(HEX_2)

r1 = xor(D1, D2)
print("Key = P1 XOR C1 = ", r1.hex())
r2 = xor(r1, D3)
print("P2 = Key XOR C2 = ", r2.hex(), "\nPlaintext P2 in ASCII: ", r2.decode("ASCII"))
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
"task6_2.py" 22L, 558C

```

1,1 All

```

[08/29/24]seed@VM:.../task6$ python3 task6_2.py
Enter Plaintext (P1): This is a known message!
Enter Ciphertext (C1): a469b1c502c1cab966965e50425438e1bb1b5f9037a4c159
Enter Ciphertext (C2): bf73bcd3509299d566c35b5d450337e1bb175f903fafc159
Key = P1 XOR C1 =  f001d8b622a8b99907b6353e2d2356c1d67e2ce356c3a478
P2 = Key XOR C2 =  4f726465723a204c61756e63682061206d697373696c6521
Plaintext P2 in ASCII: Order: Launch a missile!
[08/29/24]seed@VM:.../task6$

```

- If OFB is replaced with CFB, then only the first block can be revealed from the plaintext. If the IV is reused, the whole key stream will be reproduced again, since the keystream is done by successive encryption of the IV, i.e., $K_0 = \text{IV}$, $K_1 = E_k(C_0)$, $K_2 = E_k(C_1)$, ...

Task 6.3. Common Mistake: Use a Predictable IV

- I guess the plaintext ($P1$) to be "Yes". So, I construct $P2$ such that $P2 = P1 \text{ XOR } \text{IV} \text{ XOR } \text{Next_IV}$ where IV is the IV used to generate $C1$ by Bob and Next_IV is the predictable IV used to encrypt the next plaintext input. "Yes" in hex is 596573. I padded it to make sure it is of 16 bytes or 128 bites.
- To perform XOR, I used [xor.pw/#](#).
- $\text{temp} = P1 \text{ XOR } \text{IV}$

- The following Python code looks for the correct key from a list `words.txt`, padding each word to 16 bytes if necessary with a #, and checks if it matches the cipher text when used with AES-128-CBC encryption.
- The code begins by accepting an input in ASCII format, which must be exactly 21 characters in length. If the input length deviates from this requirement, an error is raised. Subsequently, the code requests the ciphertext and Initialization Vector (IV) used for encryption. All inputs are then converted into the appropriate byte array formats.
- The code proceeds to open a file containing a list of potential keys. For each key in the file, the code performs AES-128 encryption in Cipher Block Chaining (CBC) mode using the given IV. It then compares the resulting ciphertext with the provided ciphertext. If a match is found, the key is identified as correct; otherwise, the search continues.
- Before encryption, the code ensures that each key is precisely 16 bytes in length. If a key is shorter than 16 bytes, it is padded with # characters to achieve the required length.

```

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

def main():
    ascii_plaintext = input("Enter plaintext (total 21 characters): ")
    if len(ascii_plaintext) != 21:
        raise ValueError("The plaintext must be exactly 21 characters long.")

    hex_ciphertext = input("Enter ciphertext (in hex format): ")
    hex_iv = input("Enter IV (in hex format): ")
    plaintext = ascii_plaintext.encode('ascii')
    ciphertext = bytes.fromhex(hex_ciphertext)
    iv = bytes.fromhex(hex_iv)

    with open('words.txt') as file:
        words = file.read().splitlines()

    for word in words:
        if len(word) <= 16:
            padded_word = word.ljust(16, '#')
            word_bytes = padded_word.encode('ascii')
            cipher = AES.new(word_bytes, AES.MODE_CBC, iv)
            encrypted_text = cipher.encrypt(pad(plaintext, AES.block_size))
            if encrypted_text == ciphertext:
                # Remove padding from the key
                original_key = padded_word.rstrip('#')
                print(f"Found key: {original_key}")
                return
    print("No matching key found.")

if __name__ == "__main__":
    main()

```

```
Activities Terminal Aug 30 21:36 • seed@VM: .../task7
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad

def main():
    ascii_plaintext = input("Enter plaintext (total 21 characters): ")
    if len(ascii_plaintext) != 21:
        raise ValueError("The plaintext must be exactly 21 characters long.")

    hex_ciphertext = input("Enter ciphertext (in hex format): ")
    hex_iv = input("Enter IV (in hex format): ")
    plaintext = ascii_plaintext.encode('ascii')
    ciphertext = bytes.fromhex(hex_ciphertext)
    iv = bytes.fromhex(hex_iv)

    with open('words.txt') as file:
        words = file.readlines()

    for word in words:
        if len(word) <= 16:
            padded_word = word.ljust(16, '#')
            word_bytes = padded_word.encode('ascii')
            cipher = AES.new(word_bytes, AES.MODE_CBC, iv)
            encrypted_text = cipher.encrypt(pad(plaintext, AES.block_size))
            if encrypted_text == ciphertext:
                # Remove padding from the key
                original_key = padded_word.rstrip('#')
                print(f"Found key: {original_key}")
                return

    print("No matching key found.")

if __name__ == "__main__":
    main()
~
~
~
```

1,22 All

```
Activities Terminal Aug 30 21:38 • seed@VM: .../task7
[08/30/24]seed@VM:.../task7$ ls -l
total 208
-rwxrwx--- 1 root vboxsf 1165 Aug 30 21:29 task7.py
-rwxrwx--- 1 root vboxsf 206662 Aug 23 21:38 words.txt
[08/30/24]seed@VM:.../task7$ python3 task7.py
Enter plaintext (total 21 characters): This is a top secret.
Enter ciphertext (in hex format): 764aa26b55a4da654df6b19e4bce00f4ed05e09346fb0e762583cb7da2ac93a2
Enter IV (in hex format): aabbccddeeff00998877665544332211
Found key: Syracuse
[08/30/24]seed@VM:.../task7$
```