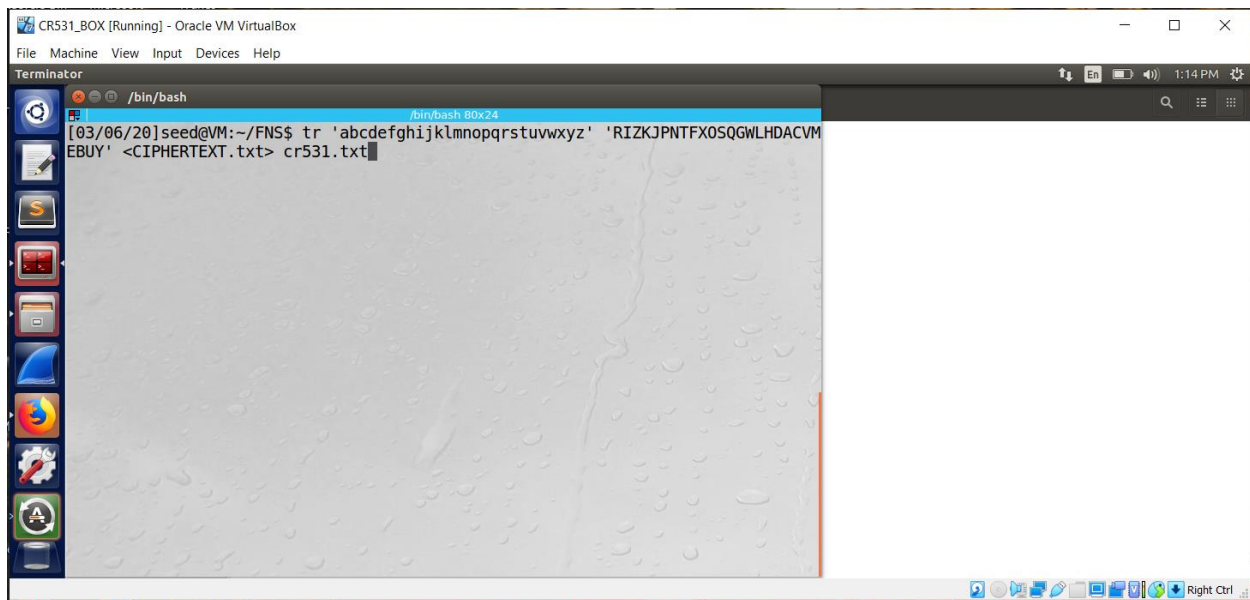


# Foundations of Network Security

Chakradhar Reddy Donuri

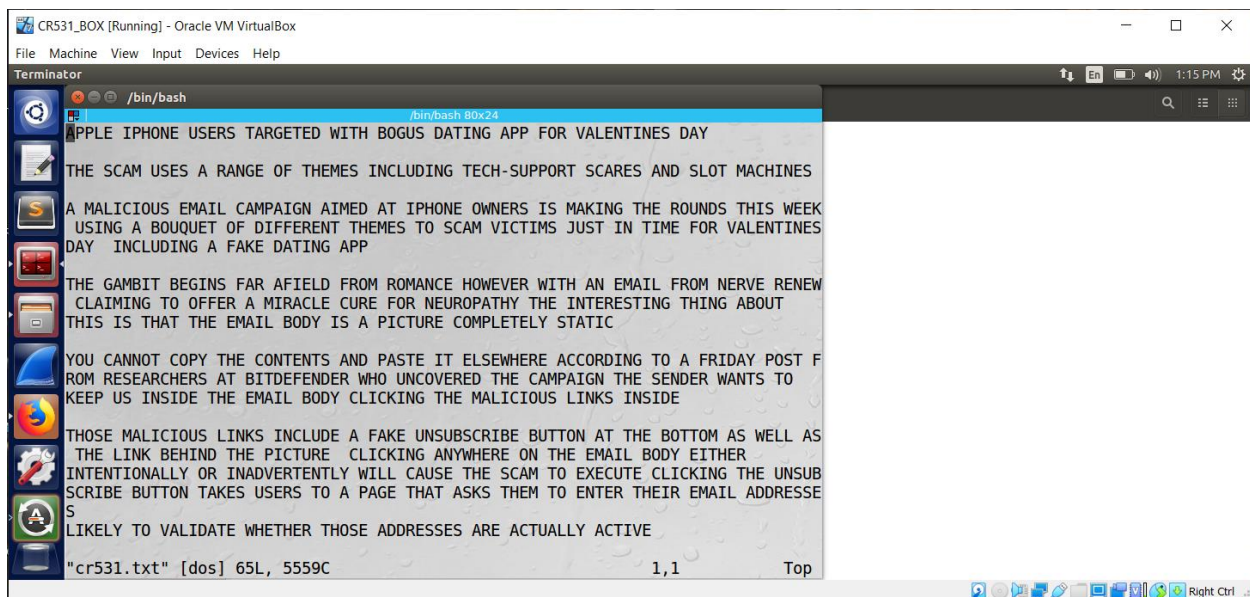
E949F496

## Task-1



The screenshot shows a VirtualBox window titled "CR531\_BOX [Running] - Oracle VM VirtualBox". Inside the window is a Linux desktop environment with a terminal window open. The terminal prompt is "seed@VM:~/FNS\$". The command entered is "tr 'abcdefghijklmnopqrstuvwxyz' 'RIZKJPNTFXOSQWLHDACVMEBUY' <CIPHERTEXT.txt> cr531.txt". The terminal background has a light blue and white pattern.

Below shown is the decrypted text.



The screenshot shows the same VirtualBox window as before, but the terminal now displays the decrypted text. The text is as follows:

```
APPLE IPHONE USERS TARGETED WITH BOGUS DATING APP FOR VALENTINES DAY  
THE SCAM USES A RANGE OF THEMES INCLUDING TECH-SUPPORT SCARES AND SLOT MACHINES  
A MALICIOUS EMAIL CAMPAIGN AIMED AT IPHONE OWNERS IS MAKING THE ROUNDS THIS WEEK  
USING A BOUQUET OF DIFFERENT THEMES TO SCAM VICTIMS JUST IN TIME FOR VALENTINES  
DAY INCLUDING A FAKE DATING APP  
THE GAMBIT BEGINS FAR AFIELD FROM ROMANCE HOWEVER WITH AN EMAIL FROM NERVE RENEW  
CLAIMING TO OFFER A MIRACLE CURE FOR NEUROPATHY THE INTERESTING THING ABOUT  
THIS IS THAT THE EMAIL BODY IS A PICTURE COMPLETELY STATIC  
YOU CANNOT COPY THE CONTENTS AND PASTE IT ELSEWHERE ACCORDING TO A FRIDAY POST F  
ROM RESEARCHERS AT BITDEFENDER WHO UNCOVERED THE CAMPAIGN THE SENDER WANTS TO  
KEEP US INSIDE THE EMAIL BODY CLICKING THE MALICIOUS LINKS INSIDE  
THOSE MALICIOUS LINKS INCLUDE A FAKE UNSUBSCRIBE BUTTON AT THE BOTTOM AS WELL AS  
THE LINK BEHIND THE PICTURE CLICKING ANYWHERE ON THE EMAIL BODY EITHER  
INTENTIONALLY OR INADVERTENTLY WILL CAUSE THE SCAM TO EXECUTE CLICKING THE UNSUB  
SCRIBE BUTTON TAKES USERS TO A PAGE THAT ASKS THEM TO ENTER THEIR EMAIL ADDRESSE  
S  
LIKELY TO VALIDATE WHETHER THOSE ADDRESSES ARE ACTUALLY ACTIVE  
"cr531.txt" [dos] 65L, 5559C 1,1 Top
```

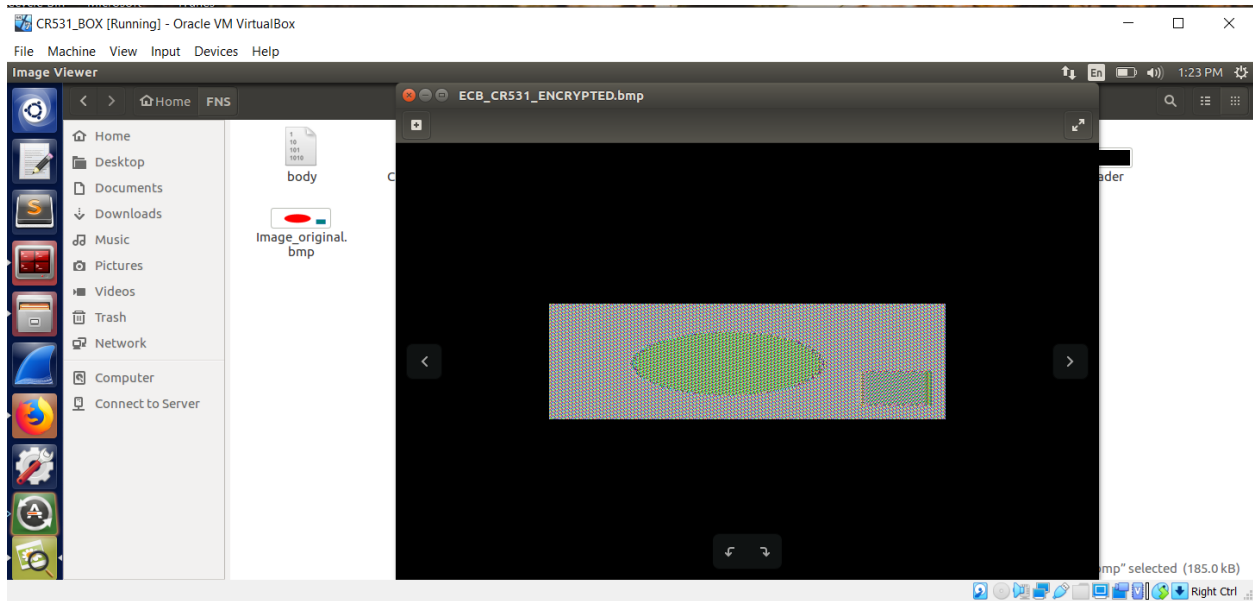
Below shown is the Key:

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

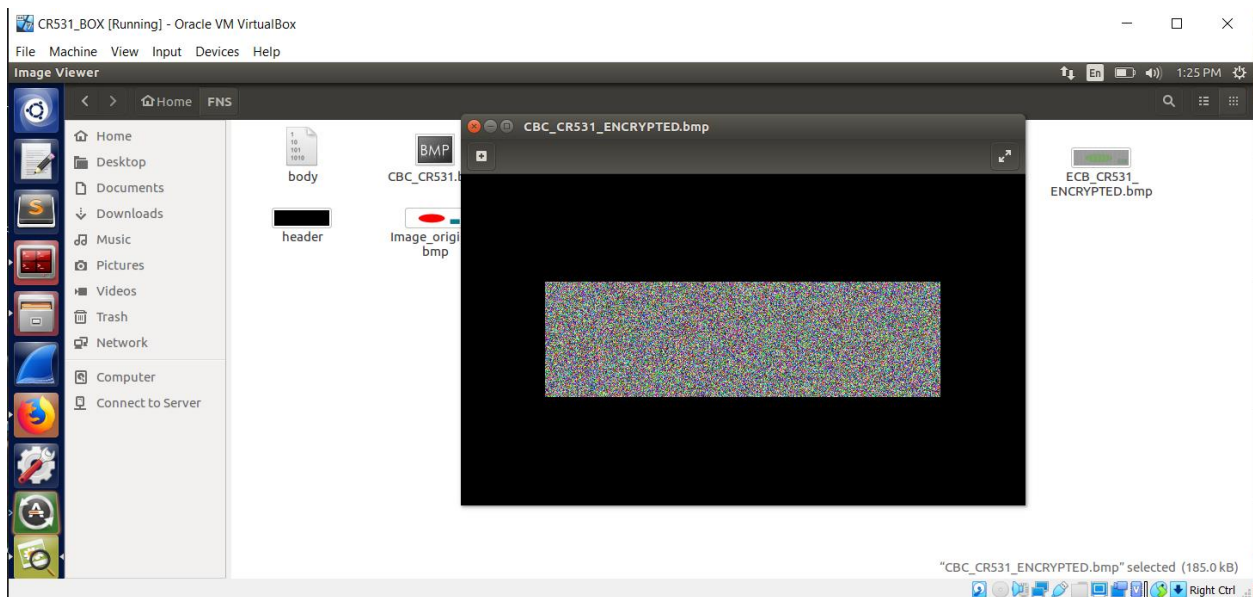
Substitution Key : RIZKJPNTFXOSQGWLHDACVMEBUY

## Task-2:

ECB Encrypted Image.



CBC Encrypted Image



There are some traces of Original image in the above shown ECB Encrypted image and there is no such trace we can find in CBC Encrypted image i.e. we are not able to depict anything from CBC Encrypted image.

### Task-3:

In ECB, a particular block of cipher text has an error in transmission, when the whole cipher text is decrypted then the block that contains error is decrypted incorrectly.

Where as in CBC, a particular block of cipher text has an error in transmission, when the whole cipher text is decrypted then the block that contains error and the block which is next to it is decrypted incorrectly.

Below is the Original Text File.



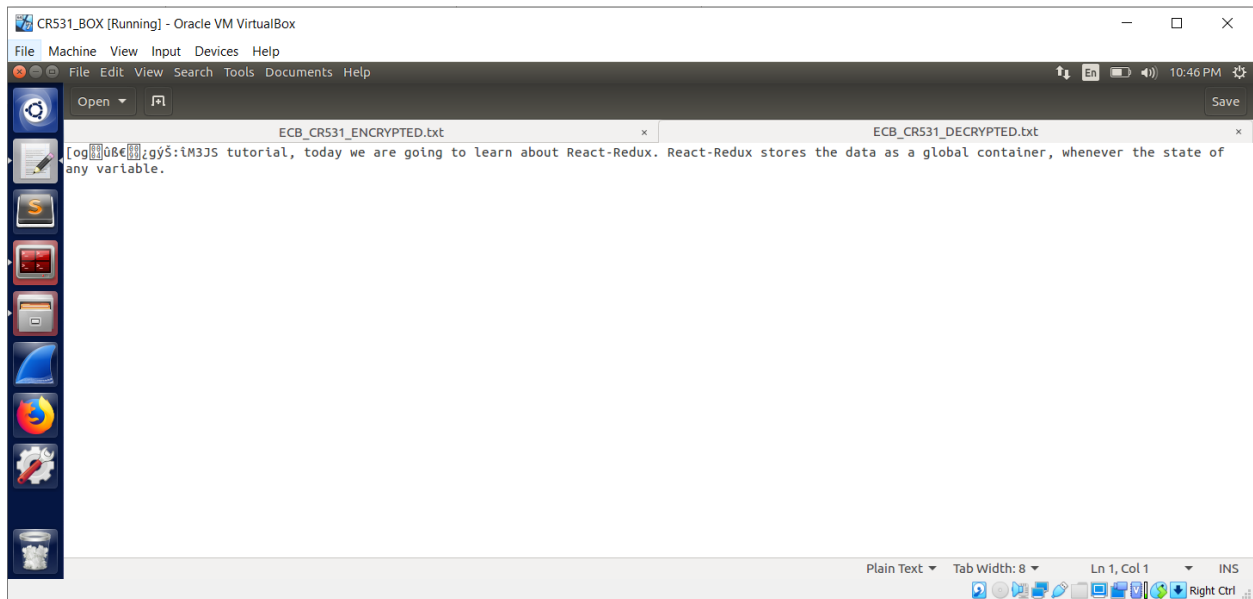
Below is the ECB Encrypted File



Below is the Corrupted ECB Encrypted file



Below is the Decrypted File of the Corrupted ECB encrypted file.



The screenshot shows a VirtualBox window titled "CR531\_BOX [Running] - Oracle VM VirtualBox". Inside the VM, a file manager window is open with two tabs: "ECB\_CR531\_ENCRYPTED.txt" and "ECB\_CR531\_DECRYPTED.txt". The "ECB\_CR531\_DECRYPTED.txt" tab is active, displaying the following text: "log[0]8[0]zgy5:IM3JS tutorial, today we are going to learn about React-Redux. React-Redux stores the data as a global container, whenever the state of any variable." The status bar at the bottom indicates "Plain Text", "Tab Width: 8", "Ln 1, Col 1", and "INS".

Below is the CBC Encrypted File



The screenshot shows a VirtualBox window titled "CR531\_BOX [Running] - Oracle VM VirtualBox". Inside the VM, a file manager window is open with a tab titled "CBC\_CR531\_ENCRYPTED.txt (~/.FNS) - gedit". The file contains several lines of encrypted text, including "Salted\_\_y6p-«G[0]zv/[0]0[0]\*E[0]6iUa\0[0]I7[0]U0[0]#0[0]>#6[0]0[0]0[0]0[0]·[0]0[0]N~2\$ [0]0[0]a[0]0[0]e)°f.ô;çB9[0]z[0]", "z[0]", "[0]0[0]s[0]b[0]8[0]ç[0]M[0]i[0]0[0]0[0]1", "w0à[0]e[0]I[0]uà[0]0[0]0[0]", and "Cn:0[0]0[0]0[0]A0[0]Nv[0]S[0]x[0]0[0]é[0]ù[0]à[0]k[0]z[0]F[0]0[0]ù[0]D[0]x[0]g[0]é[0]Z[0](Ró[0]>:N[0]0[0]A[0]-D[0])ô[0]0[0]z[0][0]?I[0]0[0]e[0]y[0]|'X0yt@0rVúI07|w[0] t0p". The status bar at the bottom indicates "Plain Text", "Tab Width: 8", "Ln 1, Col 1", and "INS".

Below is the Corrupted CBC Encrypted File.



Below is the Decrypted file of Corrupted CBC Encrypted File.



From the above screenshots attached, it is clearly depicted that our information about ECB, CBC about the error propagation was shown practically and was true.