BUBT | BANGLADESH UNIVERSITY OF BUSINESS AND TECHNOLOGY

Committed to Academic Excellence

Lab Work 4

Course Title: Cyber Security and Digital Forensic Lab

Course Code: CSE 414

Submitted By:	**Submitted To:**
Hasan Al Mahmud	**Dr. Shekh Abdullah-Al-Musa Ahmed**
ID: 18192103239	**Lecturer**
Intake: 41	**Department of CSE,BUBT**
Section: 07	

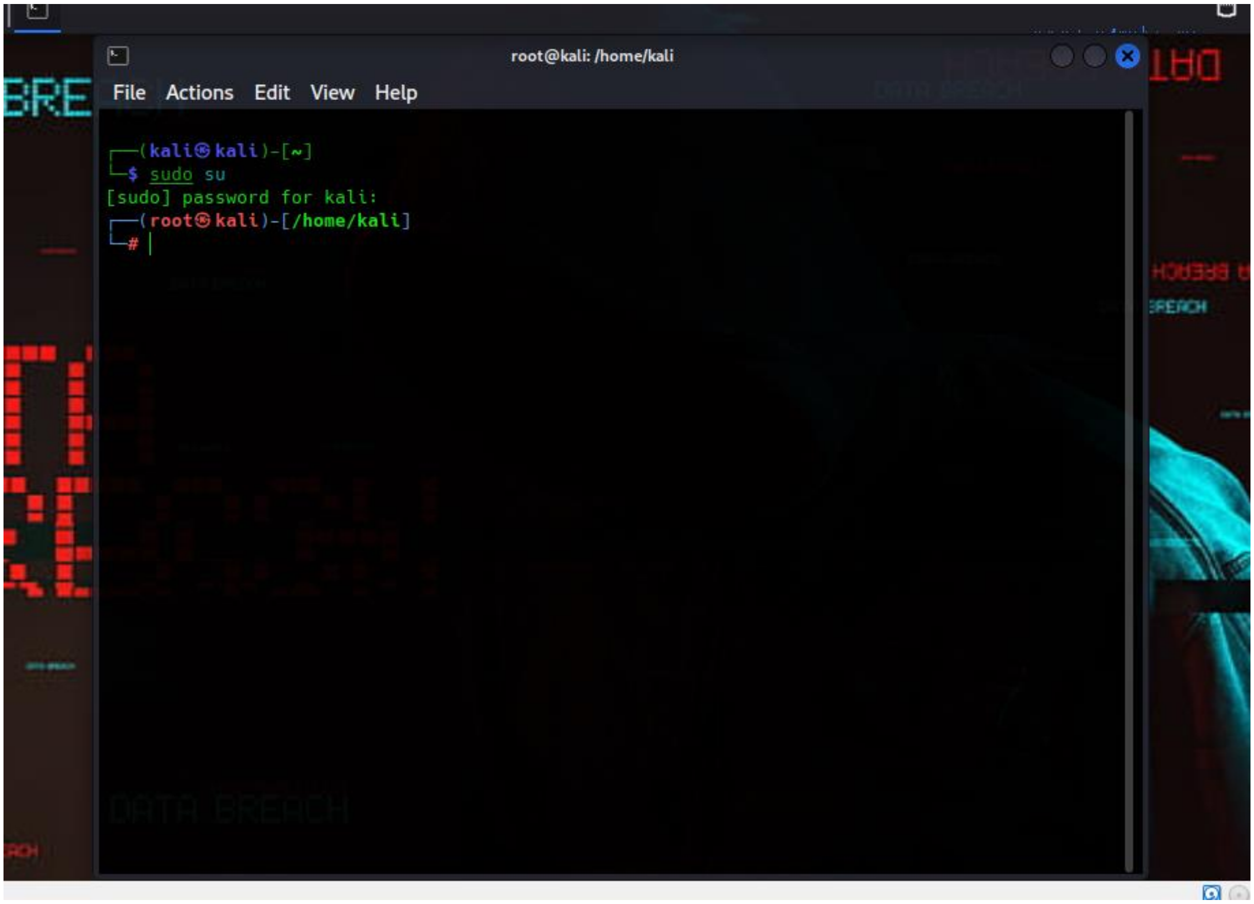
Introduction

RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.

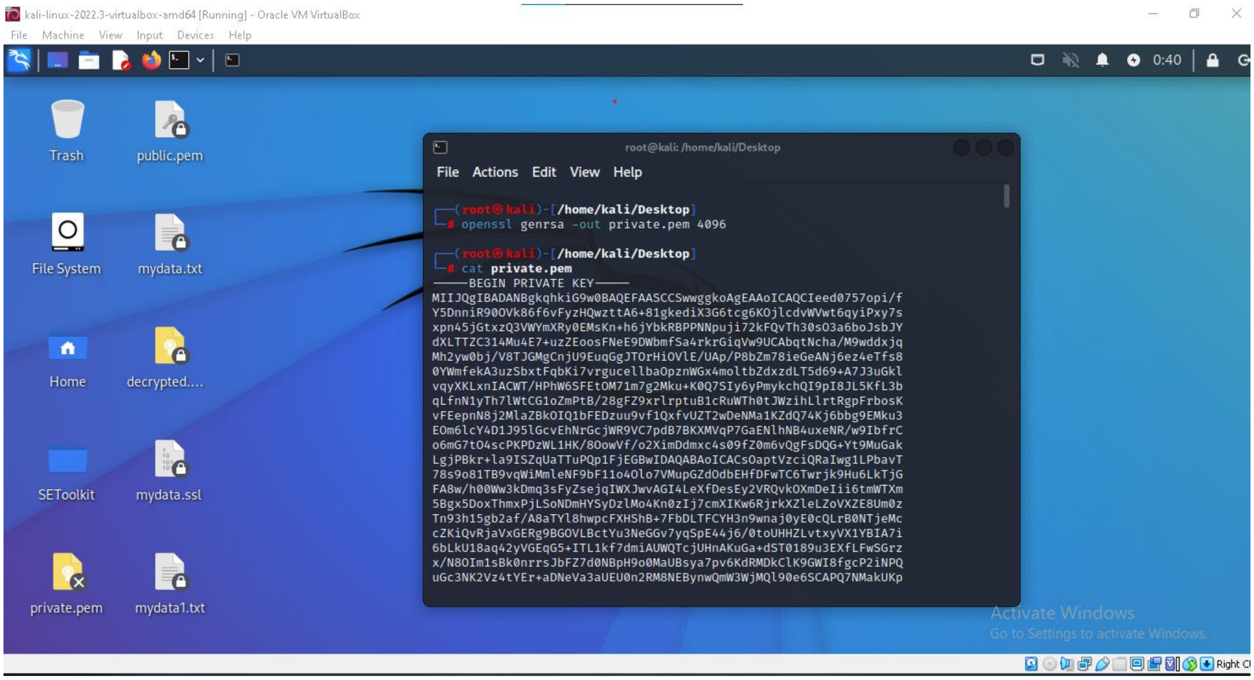
Now, let see the process of Encryption and Decryption:

Step 1: At first open the terminal in linux.



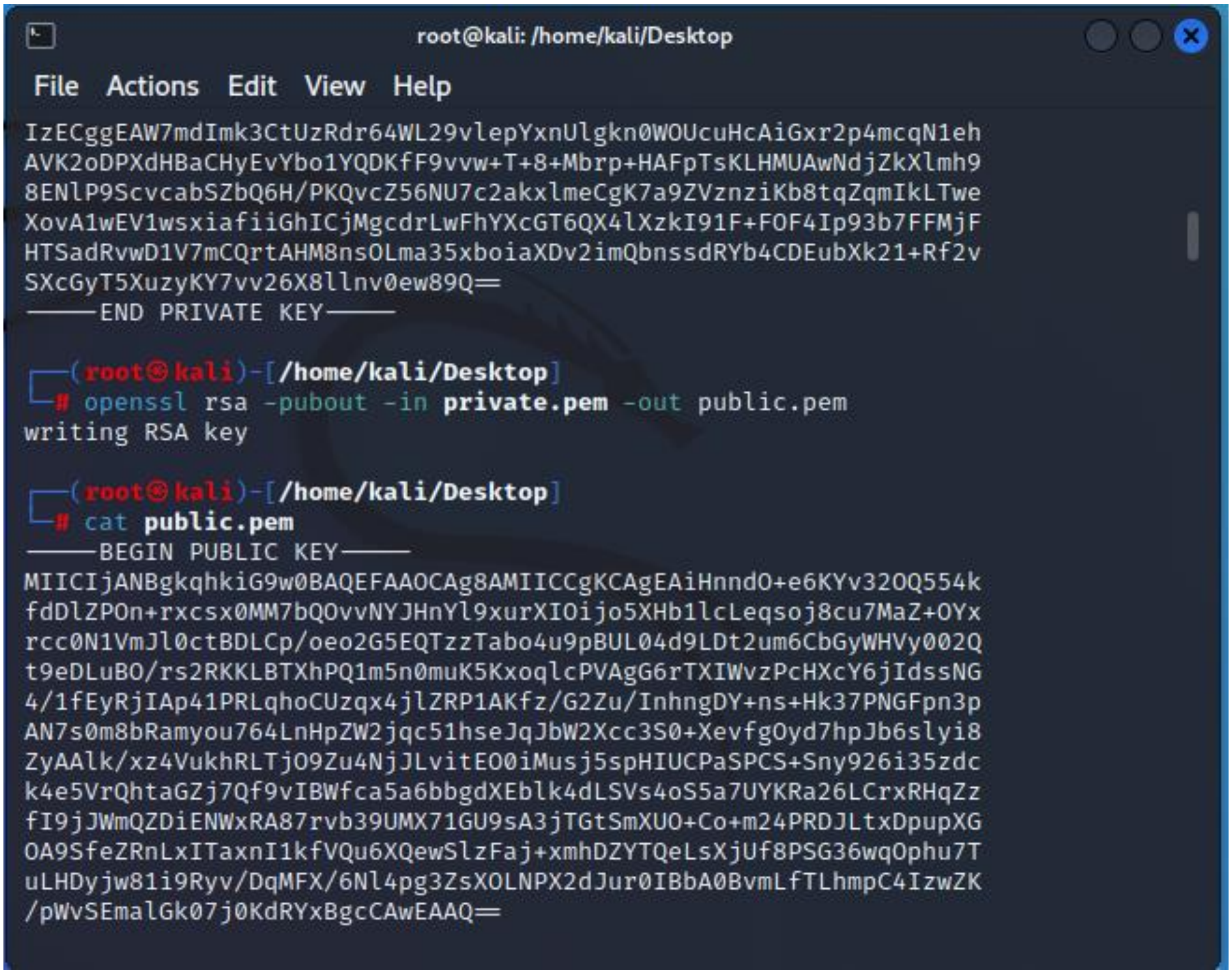
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# 
```

Step 2: Create a private.pem forlder.


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
0:40
Trash
public.pem
File System
mydata.txt
Home
decrypted....
SEToolkit
mydata.ssl
private.pem
mydata1.txt
root@kali: /home/kali/Desktop
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right C

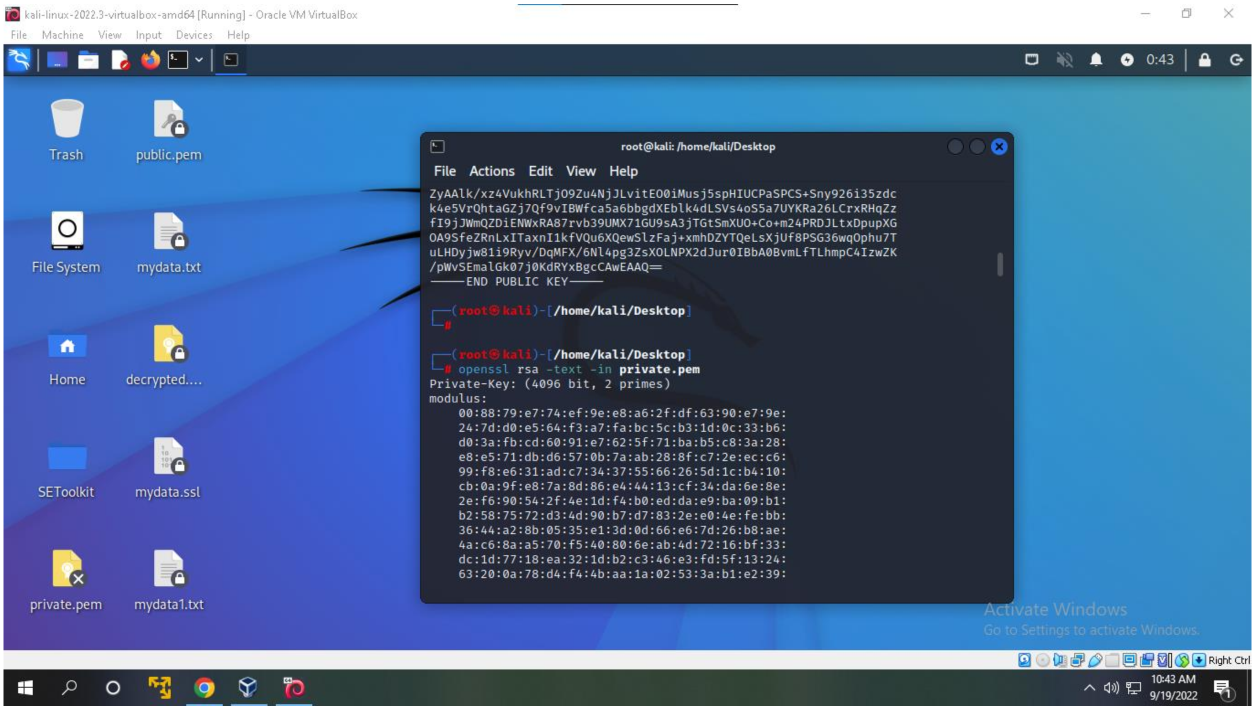
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# openssl genrsa -out private.pem 4096

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat private.pem
-----BEGIN PRIVATE KEY-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQCIeed0757opi/f
Y5DnniR90OVk86f6vFyzHQwzttA6+81gkediX3G6tcg6KOjlcdvWVwt6qyiPxy7s
xpn45jGtxzQ3VWYmXRy0EMsKn+h6jYbkRBPPNNpuji72kFQvTh30sO3a6boJsbJY
dXLTTZC314Mu4E7+uzZEoosFNeE9DWbmfSa4rkrGiqVw9UCAbqtNcha/M9wddxjq
Mh2yw0bj/V8TJGMgCnjU9EuqGgJTOrHiOVlE/UAp/P8bZm78ieGeANj6ez4eTfs8
0YWmfekA3uzSbxtFqbKi7vrgucellbaOpznWGx4moltbZdxzdLT5d69+A7J3uGkl
vqyXKLxnIACWT/HPhW6SFEtOM71m7g2Mku+K0Q7SIy6yPmykchQI9pI8JL5KfL3b
qLfnN1yTh7lWtCG1oZmPtB/28gFZ9xrlrptuB1cRuWTh0tJWzihLlrtRgpFrbosK
vFEepnN8j2MlaZBkOIQ1bFEDzuu9vf1QxfvUZT2wDeNMa1KZdQ74Kj6bbg9EMku3
EOm6lcY4D1J95lGcvEhNrGcjWR9VC7pdB7BKXMVqP7GaENlhNB4uxeNR/w9IbfrC
o6mG7tO4scPKPDzWL1HK/8OowVf/o2XimDdmxc4s09fZ0m6vQgFsDQG+Yt9MuGak
LgjPBkr+la9ISZqUaTTuPQp1FjEGBwIDAQABAoICACsOaptVzciQRaIwg1LPbavT
78s9o81TB9vqWiMmleNF9bF11o4Olo7VMupGZdOdbEHfDFwTC6Twrjk9Hu6LkTjG
FA8w/h00Ww3kDmq3sFyZsejqIWXJwvAGI4LeXfDesEy2VRQvkOXmDeIii6tmWTXm
5Bgx5DoxThmxPjLSoNDmHYSyDzlMo4Kn0zIj7cmXIKw6RjrkXZleLZoVXZE8Um0z
Tn93h15gb2af/A8aTYl8hwpcFXHShB+7FbDLTFCYH3n9wnaj0yE0cQLrB0NTjeMc
cZKiQvRjaVxGERg9BGOVLBctYu3NeGGv7yqSpE44j6/0toUHHZLvtxyVX1YBIA7i
6bLkU18aq42yVGEqG5+ITL1kf7dmiAUWQTcjUHnAKuGa+dST0189u3EXfLFwSGrz
x/N8OIm1sBk0nrrsJbFZ7d0NBpH9o0MaUBsya7pv6KdRMDkClK9GWI8fgcP2iNPQ
uGc3NK2Vz4tYEr+aDNeVa3aUEU0n2RM8NEBynwQmW3WjMQl90e6SCAPQ7NMakUKp
```

Step 3: Then open the folder in your terminal.



```
IzECggEAW7mdImk3CtUzRdr64WL29vlepYxnUlgkn0WOUcuHcAiGxr2p4mcqN1eh
AVK2oDPXdHBaCHyEvYbo1YQDKfF9vvw+T+8+Mbrp+HAFpTsKLHMUAwNdjZkXlmh9
8ENlP9ScvcabSZbQ6H/PKQvcZ56NU7c2akxlmeCgK7a9ZVznziKb8tqZqmIkLTwe
XovA1wEV1wsxiafiiGhICjMgcdrLwFhYXcGT6QX4lXzkI91F+FOF4Ip93b7FFMjF
HTSadRvwD1V7mCQrtAHM8nsOLma35xboiaXDv2imQbnssdRYb4CDEubXk21+Rf2v
SXcGyT5XuzyKY7vv26X8llnv0ew89Q==
-----END PRIVATE KEY-----

┌──(root㉿kali)-[/home/kali/Desktop]
└─# openssl rsa -pubout -in private.pem -out public.pem
writing RSA key

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat public.pem
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAiHnndO+e6KYv32OQ554k
fdDlZPOn+rxcsx0MM7bQOvvNYJHnYl9xurXIOijo5XHb1lcLeqsoj8cu7MaZ+OYx
rcc0N1VmJl0ctBDLCp/oeo2G5EQTzzTabo4u9pBUL04d9LDt2um6CbGyWHVy002Q
t9eDLuBO/rs2RKKLBTXhPQ1m5n0muK5KxoqlcPVAgG6rTXIWvzPcHXcY6jIdssNG
4/1fEyRjIAp41PRLqhoCUzqx4jlZRP1AKfz/G2Zu/InhngDY+ns+Hk37PNGFpn3p
AN7s0m8bRamyou764LnHpZW2jqc51hseJqJbW2Xcc3S0+XevfgOyd7hpJb6slyi8
ZyAAlk/xz4VukhRLTjO9Zu4NjJLvitEO0iMusj5spHIUCPaSPCS+Sny926i35zdc
k4e5VrQhtaGZj7Qf9vIBWfca5a6bbgdXEblk4dLSVs4oS5a7UYKRa26LCrxRHqZz
fI9jJWmQZDiENWxRA87rvb39UMX71GU9sA3jTGtSmXUO+Co+m24PRDJLtxDpupXG
OA9SfeZRnLxITaxnI1kfVQu6XQewSlzFaj+xmhDZYTQeLsXjUf8PSG36wqOphu7T
uLHDyjw81i9Ryv/DqMFX/6Nl4pg3ZsXOLNPX2dJur0IBbA0BvmLfTLhmpC4IzwZK
/pWvSEmalGk07j0KdRYxBgcCAwEAAQ==
```

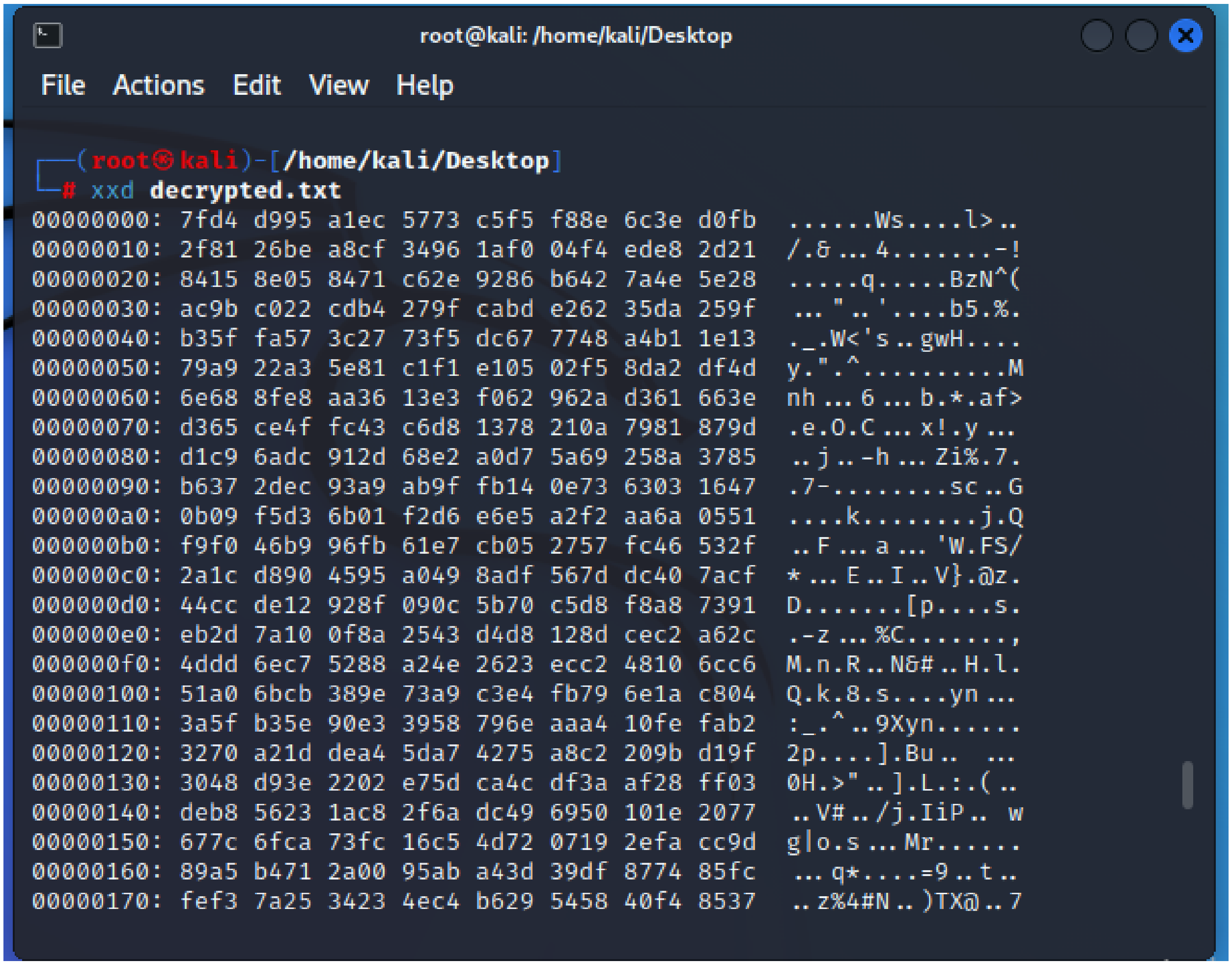
Step 4: The private key is generating.



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
0:43
Trash
public.pem
File System
mydata.txt
Home
decrypted....
SEToolkit
mydata.ssl
private.pem
mydata1.txt
root@kali: /home/kali/Desktop
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
10:43 AM
9/19/2022

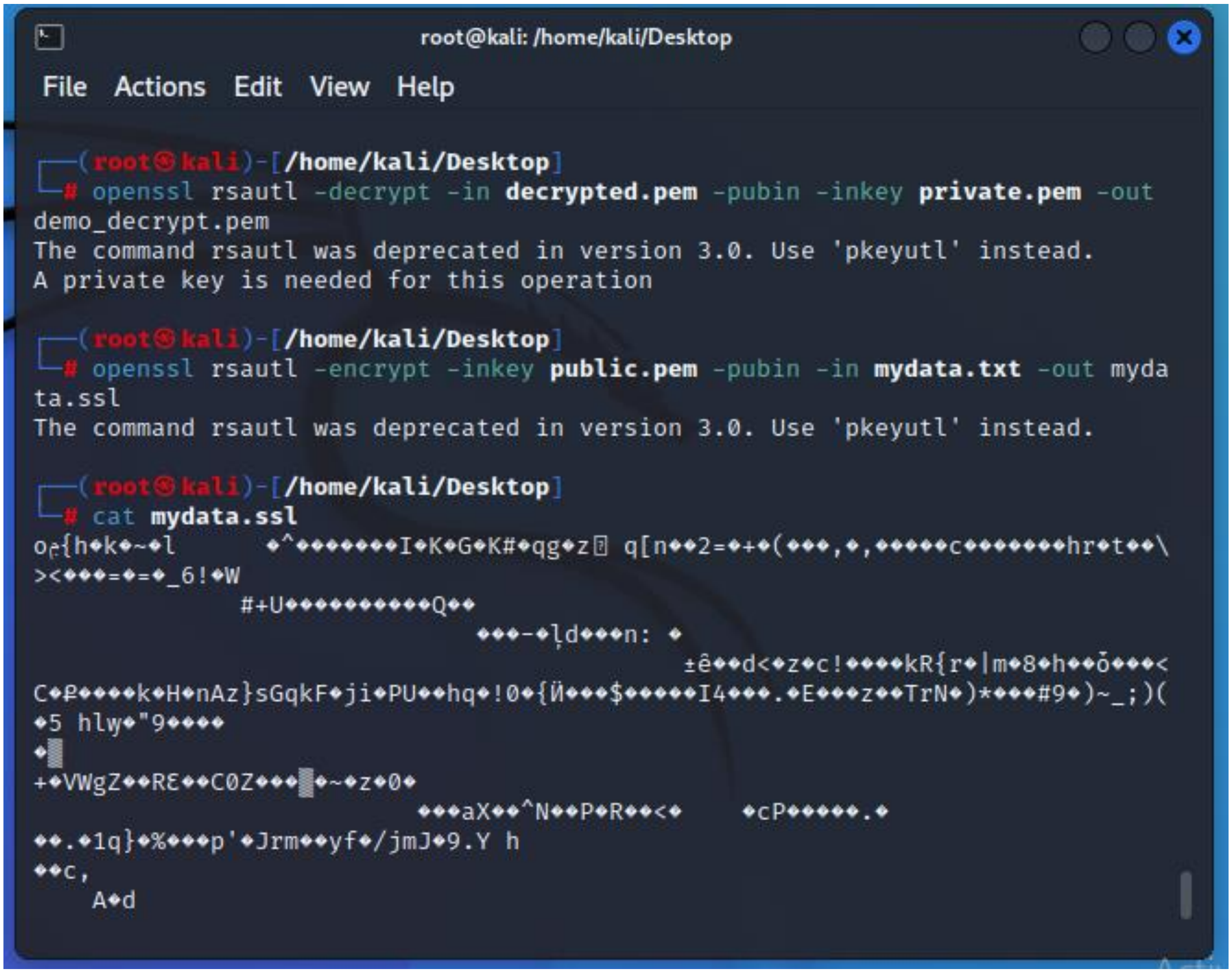
```
ZyAAlk/xz4VukhRLTjO9Zu4NjJLvitEO0iMusj5spHIUCPaSPCS+Sny926i35zdc
k4e5VrQhtaGZj7Qf9vIBWfca5a6bbgdXEblk4dLSVs4oS5a7UYKRa26LCrxRHqZz
fI9jJWmQZDiENWxRA87rvb39UMX71GU9sA3jTGtSmXUO+Co+m24PRDJLtxDpupXG
OA9SfeZRnLxITaxnI1kfVQu6XQewSlzFaj+xmhDZYTQeLsXjUf8PSG36wqOphu7T
uLHDyjw81i9Ryv/DqMFX/6Nl4pg3ZsXOLNPX2dJur0IBbA0BvmLfTLhmpC4IzwZK
/pWvSEmalGk07j0KdRYxBgcCAwEAAQ==
-----END PUBLIC KEY-----

┌──(root㉿kali)-[/home/kali/Desktop]
└─#

┌──(root㉿kali)-[/home/kali/Desktop]
└─# openssl rsa -text -in private.pem
Private-Key: (4096 bit, 2 primes)
modulus:
    00:88:79:e7:74:ef:9e:e8:a6:2f:df:63:90:e7:9e:
    24:7d:d0:e5:64:f3:a7:fa:bc:5c:b3:1d:0c:33:b6:
    d0:3a:fb:cd:60:91:e7:62:5f:71:ba:b5:c8:3a:28:
    e8:e5:71:db:d6:57:0b:7a:ab:28:8f:c7:2e:ec:c6:
    99:f8:e6:31:ad:c7:34:37:55:66:26:5d:1c:b4:10:
    cb:0a:9f:e8:7a:8d:86:e4:44:13:cf:34:da:6e:8e:
    2e:f6:90:54:2f:4e:1d:f4:b0:ed:da:e9:ba:09:b1:
    b2:58:75:72:d3:4d:90:b7:d7:83:2e:e0:4e:fe:bb:
    36:44:a2:8b:05:35:e1:3d:0d:66:e6:7d:26:b8:ae:
    4a:c6:8a:a5:70:f5:40:80:6e:ab:4d:72:16:bf:33:
    dc:1d:77:18:ea:32:1d:b2:c3:46:e3:fd:5f:13:24:
    63:20:0a:78:d4:f4:4b:aa:1a:02:53:3a:b1:e2:39:
```

Step 5: Then generate a private file.



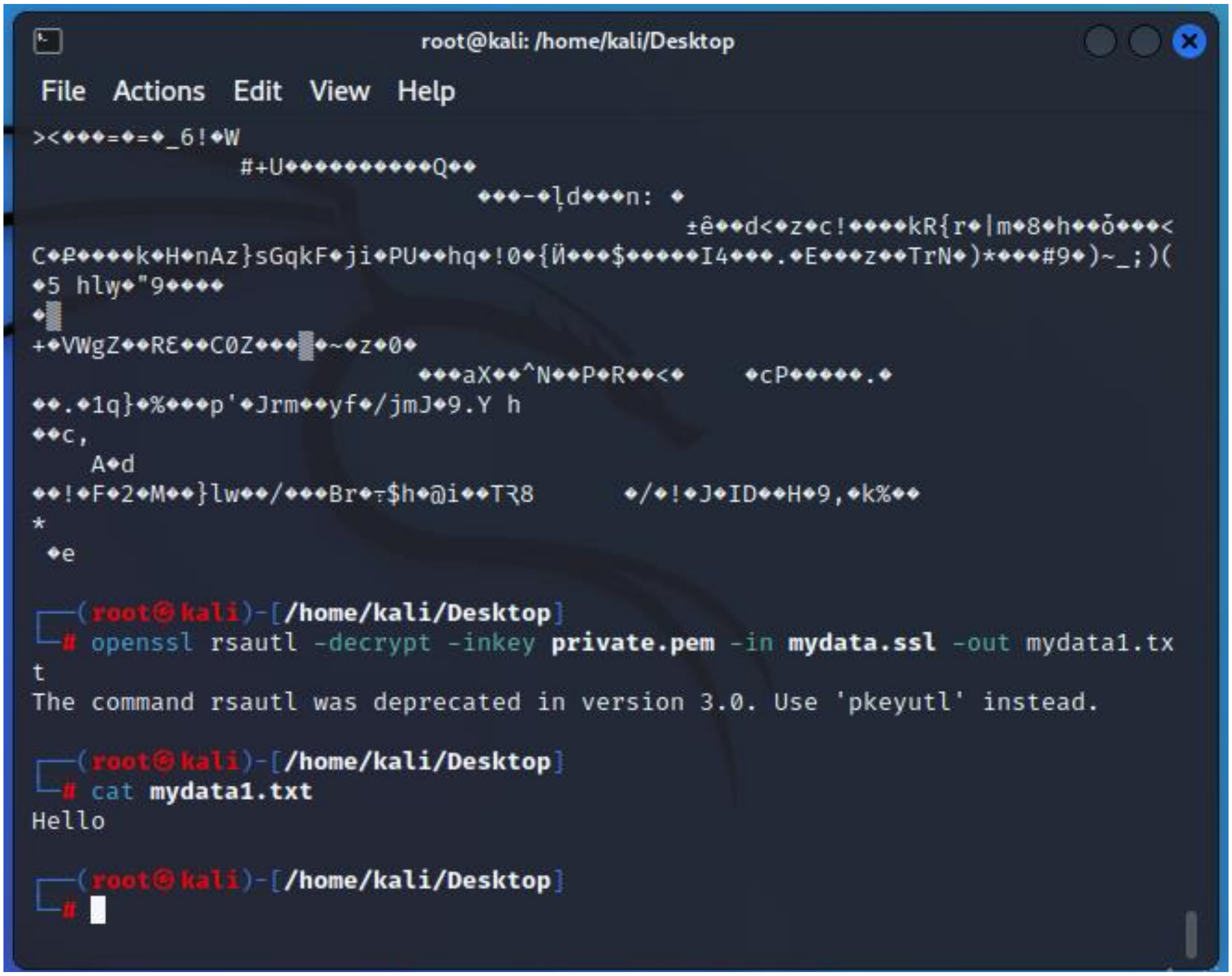
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# xxd decrypted.txt
00000000: 7fd4 d995 a1ec 5773 c5f5 f88e 6c3e d0fb  ......Ws....l>..
00000010: 2f81 26be a8cf 3496 1af0 04f4 ede8 2d21  /.&...4.......-!
00000020: 8415 8e05 8471 c62e 9286 b642 7a4e 5e28  .....q.....BzN^(
00000030: ac9b c022 cdb4 279f cabd e262 35da 259f  ...".'....b5.%.
00000040: b35f fa57 3c27 73f5 dc67 7748 a4b1 1e13  ._.W<'s..gwH....
00000050: 79a9 22a3 5e81 c1f1 e105 02f5 8da2 df4d  y.".^..........M
00000060: 6e68 8fe8 aa36 13e3 f062 962a d361 663e  nh...6...b.*.af>
00000070: d365 ce4f fc43 c6d8 1378 210a 7981 879d  .e.O.C...x!.y...
00000080: d1c9 6adc 912d 68e2 a0d7 5a69 258a 3785  ..j..-h...Zi%.7.
00000090: b637 2dec 93a9 ab9f fb14 0e73 6303 1647  .7-........sc..G
000000a0: 0b09 f5d3 6b01 f2d6 e6e5 a2f2 aa6a 0551  ....k........j.Q
000000b0: f9f0 46b9 96fb 61e7 cb05 2757 fc46 532f  ..F...a...'W.FS/
000000c0: 2a1c d890 4595 a049 8adf 567d dc40 7acf  *...E..I..V}.@z.
000000d0: 44cc de12 928f 090c 5b70 c5d8 f8a8 7391  D.......[p....s.
000000e0: eb2d 7a10 0f8a 2543 d4d8 128d cec2 a62c  .-z...%C.......,
000000f0: 4ddd 6ec7 5288 a24e 2623 ecc2 4810 6cc6  M.n.R..N&#..H.l.
00000100: 51a0 6bcb 389e 73a9 c3e4 fb79 6e1a c804  Q.k.8.s....yn...
00000110: 3a5f b35e 90e3 3958 796e aaa4 10fe fab2  :_.^..9Xyn......
00000120: 3270 a21d dea4 5da7 4275 a8c2 209b d19f  2p....].Bu.. ...
00000130: 3048 d93e 2202 e75d ca4c df3a af28 ff03  0H.>"..].L.:.(..
00000140: deb8 5623 1ac8 2f6a dc49 6950 101e 2077  ..V#../j.IiP.. w
00000150: 677c 6fca 73fc 16c5 4d72 0719 2efa cc9d  g|o.s...Mr......
00000160: 89a5 b471 2a00 95ab a43d 39df 8774 85fc  ...q*....=9..t..
00000170: fef3 7a25 3423 4ec4 b629 5458 40f4 8537  ..z%4#N..)TX@..7
```

Step 6: Then file is decrypted..



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# openssl rsautl -decrypt -in decrypted.pem -pubin -inkey private.pem -out
demo_decrypt.pem
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
A private key is needed for this operation

┌──(root㉿kali)-[/home/kali/Desktop]
└─# openssl rsautl -encrypt -inkey public.pem -pubin -in mydata.txt -out myda
ta.ssl
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat mydata.ssl
o{h◆k◆~◆l       ◆^◆◆◆◆◆◆◆I◆K◆G◆K#◆qg◆z q[n◆◆2=◆+◆(◆◆◆,◆,◆◆◆◆◆c◆◆◆◆◆◆◆◆hr◆t◆◆\
><◆◆◆=◆=◆_6!◆W
              #+U◆◆◆◆◆◆◆◆◆◆◆Q◆◆
                              ◆◆◆-◆ļd◆◆◆n: ◆
                                            ±ê◆◆d<◆z◆c!◆◆◆◆kR{r◆|m◆8◆h◆◆ǒ◆◆◆<
C◆₽◆◆◆◆◆k◆H◆nAz}sGqkF◆ji◆PU◆◆hq◆!0◆{Й◆◆◆$◆◆◆◆◆I4◆◆◆.◆E◆◆◆z◆◆TrN◆)*◆◆◆#9◆)~_;)(
◆5 hlу◆"9◆◆◆◆
◆▒
+◆VWgZ◆◆RƐ◆◆C0Z◆◆◆▒◆~◆z◆0◆
                          ◆◆◆aX◆◆^N◆◆P◆R◆◆<◆    ◆cP◆◆◆◆◆.◆
◆◆.◆1q}◆%◆◆◆p'◆Jrm◆◆yf◆/jmJ◆9.Y h
◆◆c,
    A◆d
```

Step 7: Finally access the file by encrypting.



```
><◆◆◆=◆=◆_6!◆W
              #+U◆◆◆◆◆◆◆◆◆◆◆Q◆◆
                              ◆◆◆-◆ḷd◆◆◆n: ◆
                                            ±ê◆◆d<◆z◆c!◆◆◆◆kR{r◆|m◆8◆h◆◆ŏ◆◆◆<
C◆₽◆◆◆◆k◆H◆nAz}sGqkF◆ji◆PU◆◆hq◆!0◆{Й◆◆◆$◆◆◆◆◆I4◆◆◆.◆E◆◆◆z◆◆TrN◆)*◆◆◆#9◆)~_;)(
◆5 hlу◆"9◆◆◆◆
◆▒
+◆VWgZ◆◆RƐ◆◆C0Z◆◆◆▒◆~◆z◆0◆
                          ◆◆◆aX◆◆^N◆◆P◆R◆◆<◆    ◆cP◆◆◆◆◆.◆
◆◆.◆1q}◆%◆◆◆p'◆Jrm◆◆yf◆/jmJ◆9.Y h
◆◆c,
    A◆d
◆◆!◆F◆2◆M◆◆}lw◆◆/◆◆◆Br◆⍑$h◆@i◆◆Tϡ8      ◆/◆!◆J◆ID◆◆H◆9,◆k%◆◆
*
 ◆e

┌──(root㉿kali)-[/home/kali/Desktop]
└─# openssl rsautl -decrypt -inkey private.pem -in mydata.ssl -out mydata1.tx
t
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat mydata1.txt
Hello

┌──(root㉿kali)-[/home/kali/Desktop]
└─# 
```