

JBL LAB8: Encrypting and
Decrypting Files with PKI

JBL LAB8: Encrypting and Decrypting Files with PKI

Tools and Software..... 2

Section 2: Applied Learning..... 2

 Part 1: Encrypt a File with Symmetric Encryption.....3

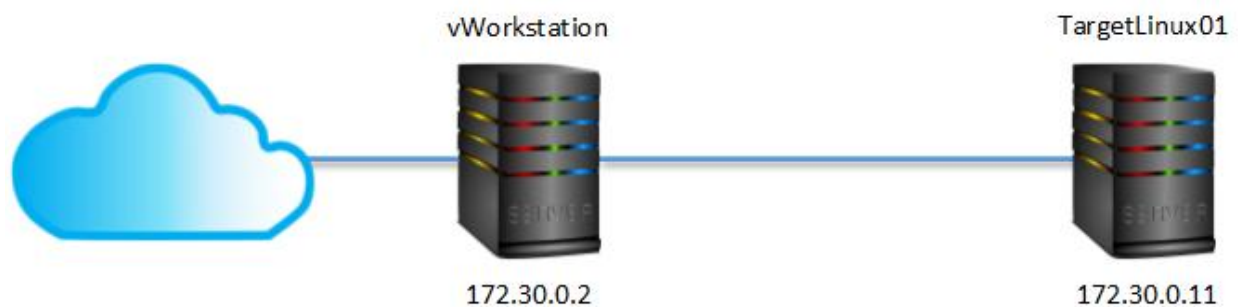
 Part 2: Encrypt a File with Asymmetric Encryption.....4

JBL LAB8: Encrypting and Decrypting Files with PKI

Topology

This lab contains the following virtual devices. Please refer to the network topology diagram below.

- vWorkstation (Windows Server 2016)
- TargetLinux01 (Xubuntu Linux)



Tools and Software

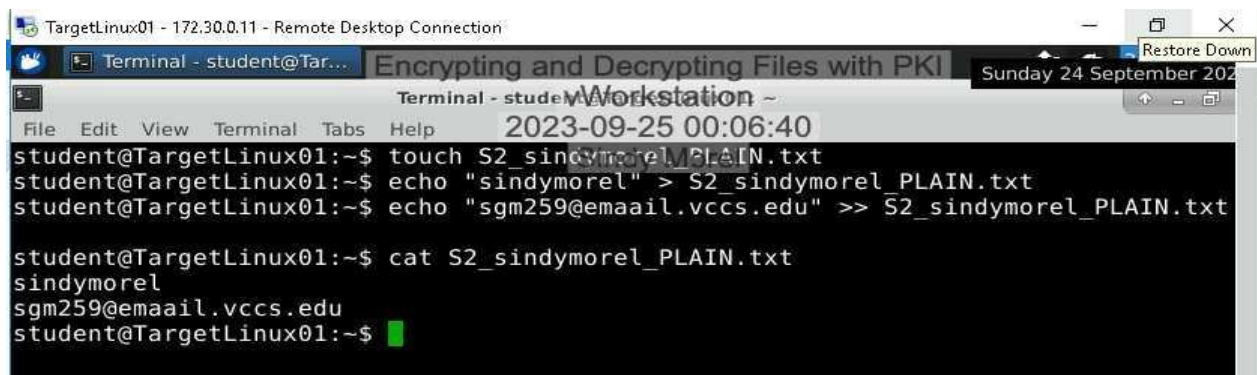
The following software and/or utilities are required to complete this lab. You are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- GNU Privacy Guard (GnuPG or GPG)

JBL LAB8: Encrypting and
Decrypting Files with PKI

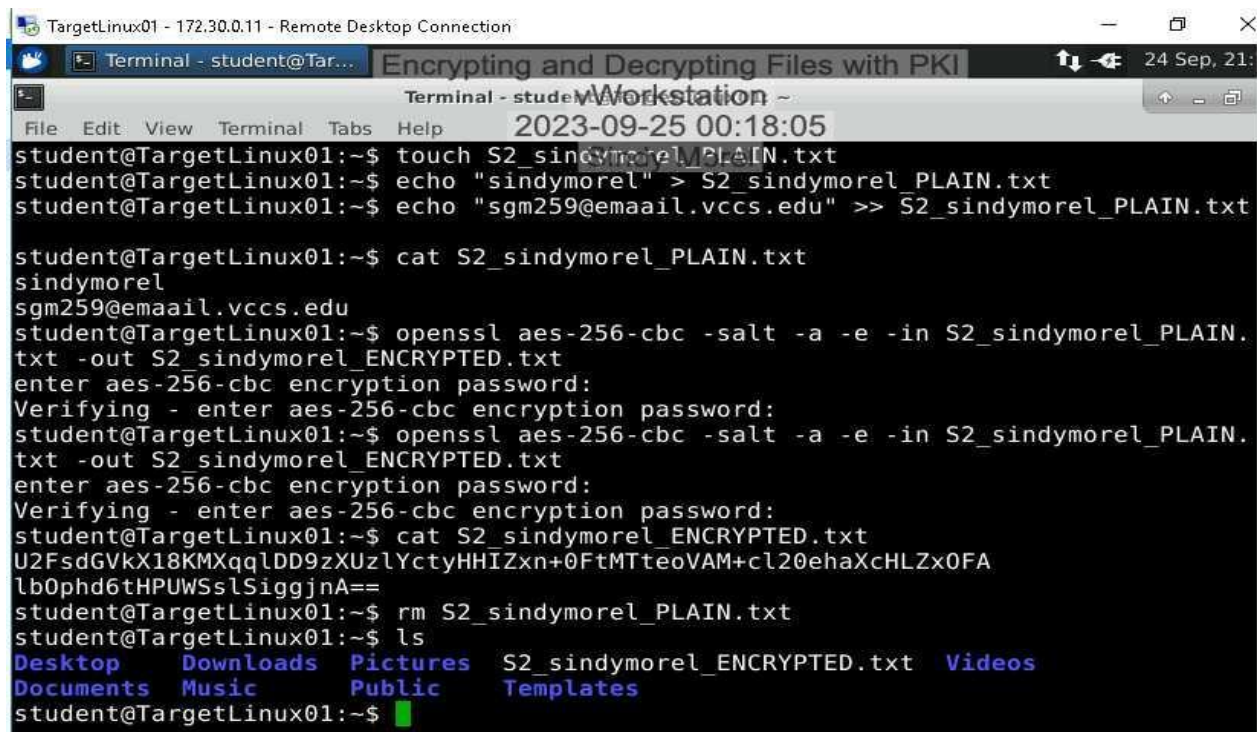
Section 2: Applied Learning

Part 1: Encrypt a File with Symmetric Encryption

A terminal window titled 'Terminal - student@Tar...' with a menu bar (File, Edit, View, Terminal, Tabs, Help) and a timestamp '2023-09-25 00:06:40'. The window shows the creation of a file named 'S2_sindymorel_PLAIN.txt' using 'touch', followed by two 'echo' commands to write 'sindymorel' and 'sgm259@emaail.vccs.edu' to the file. Finally, 'cat' is used to display the file's contents.

```
student@TargetLinux01:~$ touch S2_sindymorel_PLAIN.txt
student@TargetLinux01:~$ echo "sindymorel" > S2_sindymorel_PLAIN.txt
student@TargetLinux01:~$ echo "sgm259@emaail.vccs.edu" >> S2_sindymorel_PLAIN.txt

student@TargetLinux01:~$ cat S2_sindymorel_PLAIN.txt
sindymorel
sgm259@emaail.vccs.edu
student@TargetLinux01:~$
```

A terminal window titled 'Terminal - student@Tar...' with a menu bar (File, Edit, View, Terminal, Tabs, Help) and a timestamp '2023-09-25 00:18:05'. It continues from the previous screenshot, showing the encryption of 'S2_sindymorel_PLAIN.txt' to 'S2_sindymorel_ENCRYPTED.txt' using 'openssl aes-256-cbc'. It prompts for an encryption password, which is entered and verified. The encrypted file is then displayed with 'cat'. Finally, the original file is removed with 'rm' and the directory is listed with 'ls', showing the encrypted file and standard Linux directories.

```
student@TargetLinux01:~$ touch S2_sindymorel_PLAIN.txt
student@TargetLinux01:~$ echo "sindymorel" > S2_sindymorel_PLAIN.txt
student@TargetLinux01:~$ echo "sgm259@emaail.vccs.edu" >> S2_sindymorel_PLAIN.txt

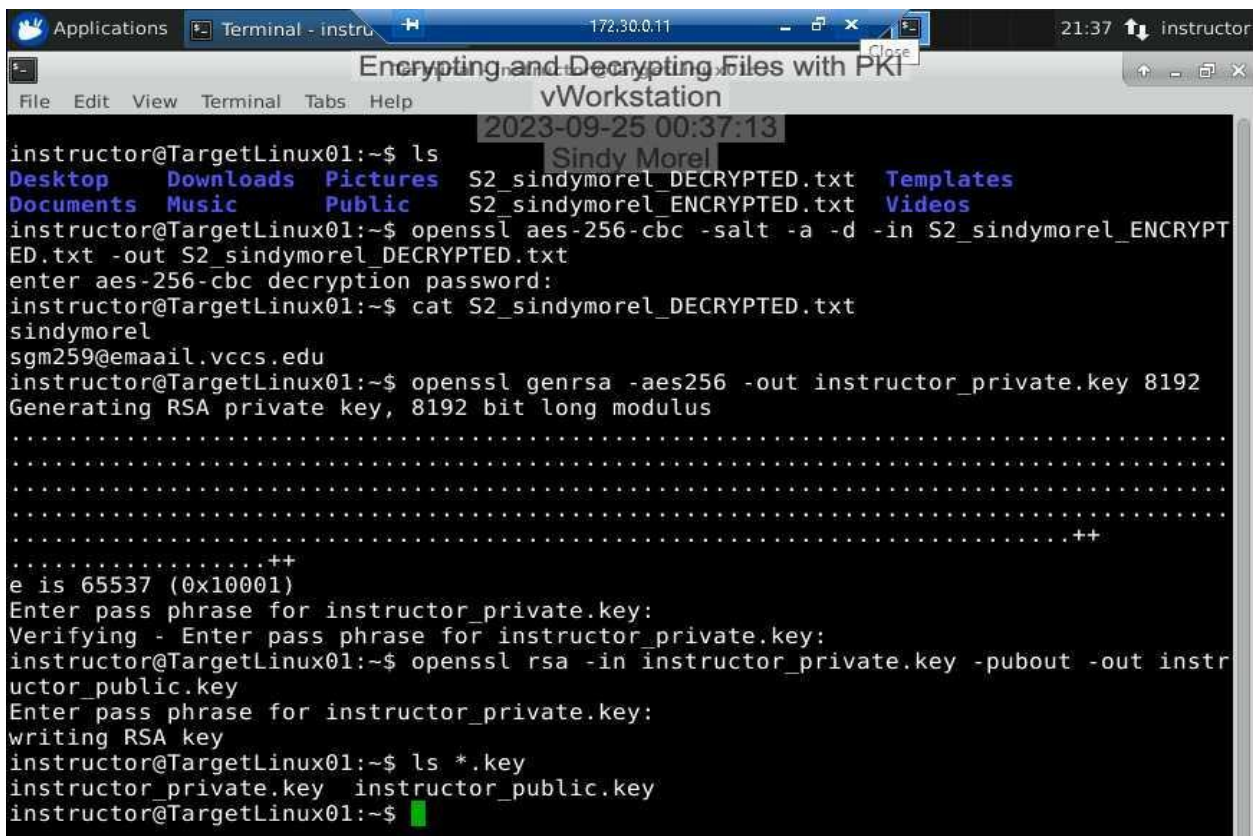
student@TargetLinux01:~$ cat S2_sindymorel_PLAIN.txt
sindymorel
sgm259@emaail.vccs.edu
student@TargetLinux01:~$ openssl aes-256-cbc -salt -a -e -in S2_sindymorel_PLAIN.
txt -out S2_sindymorel_ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ openssl aes-256-cbc -salt -a -e -in S2_sindymorel_PLAIN.
txt -out S2_sindymorel_ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat S2_sindymorel_ENCRYPTED.txt
U2FsdGVkX18KMXqqlDD9zXUzlYctyHHIZxn+0FtMTteoVAM+cl20ehaXcHLZx0FA
lb0phd6tHPUWSslSiggjnA==
student@TargetLinux01:~$ rm S2_sindymorel_PLAIN.txt
student@TargetLinux01:~$ ls
Desktop  Downloads  Pictures  S2_sindymorel_ENCRYPTED.txt  Videos
Documents  Music      Public    Templates
student@TargetLinux01:~$
```

Password: R@1ny D@y!

JBL LAB8: Encrypting and
Decrypting Files with PKI

A screenshot of a terminal window titled "Encrypting and Decrypting Files with PKI" within a vWorkstation environment. The terminal shows a user named "instructor" at "TargetLinux01" performing a series of commands to decrypt a file. The window's title bar includes "Applications", "Terminal - instru", the IP address "172.30.0.11", and the time "21:31". The terminal output is as follows:

```
instructor@TargetLinux01:~$ ls
Desktop  Downloads  Pictures  S2_sindymorel_DECRYPTED.txt  Templates
Documents Music      Public    S2_sindymorel_ENCRYPTED.txt  Videos
instructor@TargetLinux01:~$ openssl aes-256-cbc -salt -a -d -in S2_sindymorel_ENCRYPTED.txt -out S2_sindymorel_DECRYPTED.txt
enter aes-256-cbc decryption password:
instructor@TargetLinux01:~$ cat S2_sindymorel_DECRYPTED.txt
sindymorel
sgm259@emaail.vccs.edu
instructor@TargetLinux01:~$
```



A second screenshot of the same terminal window, showing the generation of an RSA private key. The window title bar now shows the time "21:37". The terminal output continues from the previous state:

```
instructor@TargetLinux01:~$ ls
Desktop  Downloads  Pictures  S2_sindymorel_DECRYPTED.txt  Templates
Documents Music      Public    S2_sindymorel_ENCRYPTED.txt  Videos
instructor@TargetLinux01:~$ openssl aes-256-cbc -salt -a -d -in S2_sindymorel_ENCRYPTED.txt -out S2_sindymorel_DECRYPTED.txt
enter aes-256-cbc decryption password:
instructor@TargetLinux01:~$ cat S2_sindymorel_DECRYPTED.txt
sindymorel
sgm259@emaail.vccs.edu
instructor@TargetLinux01:~$ openssl genrsa -aes256 -out instructor_private.key 8192
Generating RSA private key, 8192 bit long modulus
.....
.....
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for instructor_private.key:
Verifying - Enter pass phrase for instructor_private.key:
instructor@TargetLinux01:~$ openssl rsa -in instructor_private.key -pubout -out instructor_public.key
Enter pass phrase for instructor_private.key:
writing RSA key
instructor@TargetLinux01:~$ ls *.key
instructor_private.key  instructor_public.key
instructor@TargetLinux01:~$
```


Part 2: Encrypt a File with Asymmetric Encryption



```
Applications Terminal - instru 172.30.0.11 Sunday 24 September 2023
Encrypting and Decrypting Files with PKI vWorkstation
File Edit View Terminal Tabs Help
instructor@TargetLinux01:~$ cp /tmp/S2_sindymorel_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ ls
Desktop          instructor_public.key  S2_sindymorel_DECRYPTED.txt
Documents        Music                 S2_sindymorel_ENCRYPTED.txt
Downloads        Pictures              Templates
instructor_private.key  Public               Videos
instructor@TargetLinux01:~$ openssl aes-256-cbc -salt -a -d -in S2_sindymorel_ENCRYPTED.txt -out S2_sindymorel_DECRYPTED.txt
enter aes-256-cbc decryption password:
instructor@TargetLinux01:~$ cat S2_sindymorel_DECRYPTED.txt
sindymorel
sgm259@emaail.vccs.edu
instructor@TargetLinux01:~$
```

JBL LAB8: Encrypting and Decrypting Files with PKI

```
Applications Terminal - instru 172.30.0.11 22:08 instructor@TargetLinux01: ~  
vWorkstation  
File Edit View Terminal Tabs Help  
instructor@TargetLinux01:~$ cp /tmp/S2_sindymorel_ENCRYPTED.txt ~/Sindy Morel  
instructor@TargetLinux01:~$ ls  
Desktop instructor_public.key S2_sindymorel_DECRYPTED.txt  
Documents Music S2_sindymorel_ENCRYPTED.txt  
Downloads Pictures Templates  
Public Videos  
instructor_private.key  
instructor@TargetLinux01:~$ openssl aes-256-cbc -salt -a -d -in S2_sindymorel_ENCRYPTED.txt -out S2_sindymorel_DECRYPTED.txt  
enter aes-256-cbc decryption password:  
instructor@TargetLinux01:~$ cat S2_sindymorel_DECRYPTED.txt  
sindymorel  
sgm259@emaail.vccs.edu  
instructor@TargetLinux01:~$ openssl genrsa -aes256 -out instructor_private.key 8192  
Generating RSA private key, 8192 bit long modulus  
.....++  
e is 65537 (0x10001)  
Enter pass phrase for instructor_private.key:  
Verifying - Enter pass phrase for instructor_private.key:  
Verify failure  
User interface error  
140407817119384:error:0906906F:PEM routines:PEM_ASN1_write_bio:read key:pem_lib.c:379:  
instructor@TargetLinux01:~$ openssl rsa -in instructor_private.key -pubout -out instructor_public.key  
unable to load Private Key  
140211035715224:error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_lib.c:701:  
Expecting: ANY PRIVATE KEY  
instructor@TargetLinux01:~$ ls *.key  
instructor_private.key instructor_public.key  
instructor@TargetLinux01:~$
```

```
Terminal - student@Tar... 172.30.11 24 Sep, 22:15
```

```
Encrypting and Decrypting Files with PKI
vWorkstation
```

```
student@TargetLinux01:~$ cp /tmp/instructor_public.key ~/
student@TargetLinux01:~$ touch S2_sindymorel_newfile.txt
student@TargetLinux01:~$ echo "sindymorel" > S2_sindymorel_new
student@TargetLinux01:~$ echo "Encrypted Message for Instructor" >> S2_sindymorel_new
file.txt
student@TargetLinux01:~$ openssl rsautl -encrypt -pubin -inkey instructor_public.key
-in S2_sindymorel_newfile.txt -out S2_sindymorel_newfile.ENC.txt
student@TargetLinux01:~$ cat S2_sindymorel_newfile.ENC.txt
U00000000p100000000+0SL0(00000000.00070000E=0Cc0pw0)0<UN[0
00n-
0q 0000003MM0000
<00000000@-*5000000000000000Kk0000#800S000zh000 00Z00`000000u000500j000@-0\9m00000Jq
\0Ga00 :C00000 00p)00000l0i00HV00dK00
p000007F+04vL50f00;05t0[0 >0000=0)i0000
:00RN00GT0N0N0n`0010<!000S.~000000@F00~0!cm0000100<n00e0K5T;0N.,i00000s00007 000E0
NEK000tv000k0000F0000000j;0N000>00U0000#r03q00f000s0000h00p00DgV0?8000p000v00000070sE0+^
0C.'0veA0r00H00000m063E0000003700>0[00000?0h000000Amy0K0000+000000g00?000002901000000
J06Z090000000000000p0~00op000bt0000k0000L00FS2~000Sq0z.00000y0S_00evJ0000~00000000007
:äv.0000000000D,^zn00(00x0000008N0000-w)00]-000
3= 04I
+00)000c%0000.\000N 0^9I
0r000000HF00X500000
Y0tq00>0000
0<駄M00+0 Vim040D0P000LFC00007
000d000060 00`JM0f0000N0000Ge0 y0/001>000B-Ä00+s00q000WB004kK00dq0e0n00-000K00
r0y
000:00+D~700000000VkeWa
```


JBL LAB8: Encrypting and
Decrypting Files with PKI

The screenshot shows a terminal window titled "vWorkstation" with a menu bar (File, Edit, View, Terminal, Tabs, Help) and a title bar (Applications, Terminal - instru, 172.30.0.11, Current workspace: "Workspace 1"). The terminal content is as follows:

```
instructor@TargetLinux01:~$ cp S2_sindymorel_newfile.ENC.txt ~/
cp: 'S2_sindymorel_newfile.ENC.txt' and '/home/instructor/S2_sindymorel_newfile.ENC.t
xt' are the same file
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_private.key -in
S2_sindymorel_newfile.ENC.txt -out S2_sindymorel_newfile_DECRYPTED.txt
unable to load Private Key
140174789625496:error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_lib.c:701:
Expecting: ANY PRIVATE KEY
instructor@TargetLinux01:~$ cat S2_sindymorel_newfile_DECRYPTED.txt
cat: S2_sindymorel_newfile_DECRYPTED.txt: No such file or directory
instructor@TargetLinux01:~$ cat S2_sindymorel_DECRYPTED.txt
sindymorel
sgm259@emaail.vccs.edu
instructor@TargetLinux01:~$
```