JBL LAB8: Encrypting and Decrypting Files with PKI

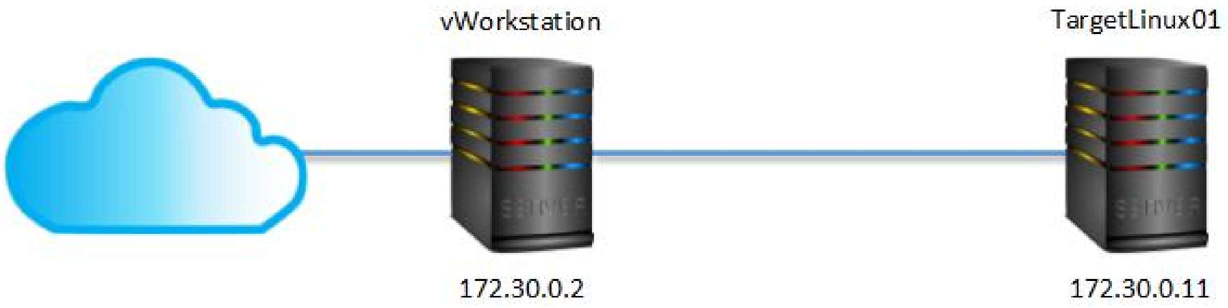
Sindy Morel September 23, 2023

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.

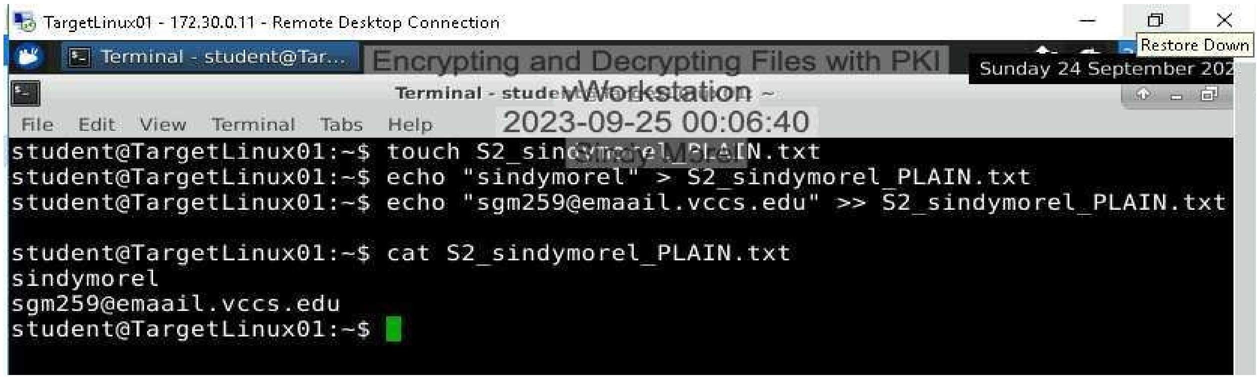
- GNU Privacy Guard (GnuPG or GPG)

Sindy Morel September 23, 2023

JBL LAB8: Encrypting and
Decrypting Files with PKI

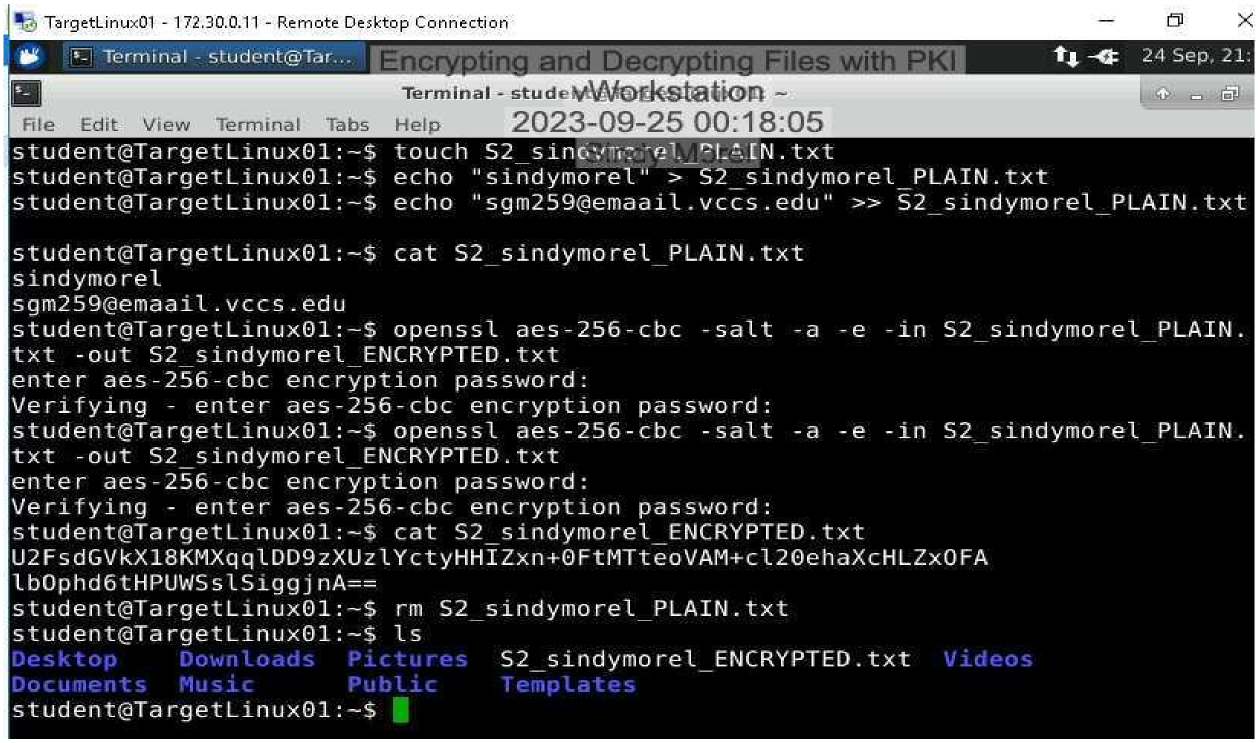
Section 2: Applied Learning

Part 1: Encrypt a File with Symmetric Encryption


TargetLinux01 - 172.30.0.11 - Remote Desktop Connection
Restore Down
Terminal - student@Tar...
Encrypting and Decrypting Files with PKI
Sunday 24 September 202
Terminal - student@TargetLinux01: ~
Workstation
File Edit View Terminal Tabs Help
2023-09-25 00:06:40
Sindy Morel

```
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:~$
```


TargetLinux01 - 172.30.0.11 - Remote Desktop Connection
Terminal - student@Tar...
Encrypting and Decrypting Files with PKI
24 Sep, 21:
Terminal - student@TargetLinux01: ~
Workstation
File Edit View Terminal Tabs Help
2023-09-25 00:18:05
Sindy Morel

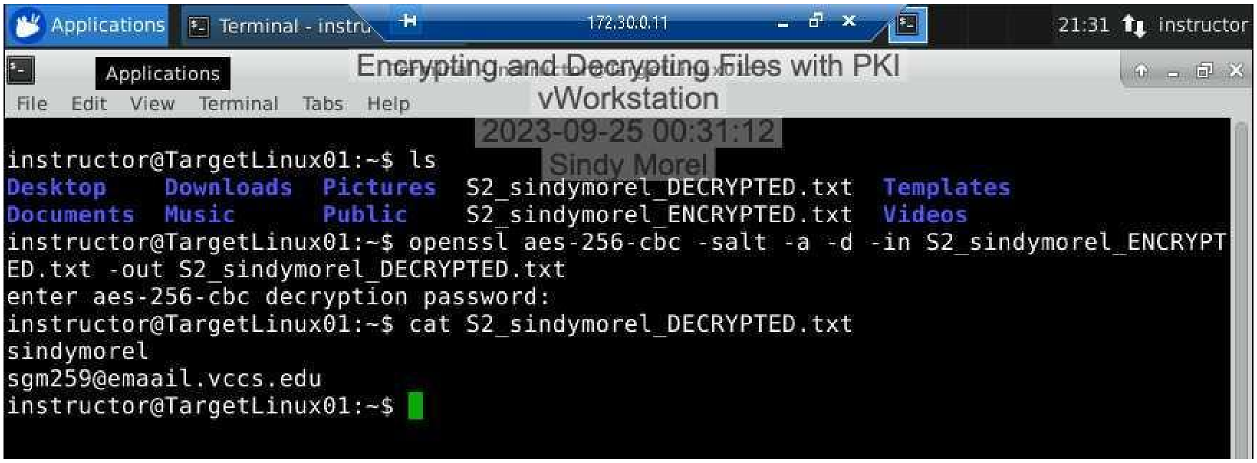
```
student@TargetLinux01:~$ touch S2_sindymorel_PLAIN.txt
student@TargetLinux01:~$ echo "sindymorel" > S2_sindymorel_PLAIN.txt
student@TargetLinux01:~$ echo "sgm259@emaail.vccs.edu" >> S2_sindymorel_PLAIN.txt

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+cl20ehaXcHLZxOFA
lbOphd6tHPUWSslSiggjnA==
student@TargetLinux01:~$ rm S2_sindymorel_PLAIN.txt
student@TargetLinux01:~$ ls
Desktop    Downloads  Pictures  S2_sindymorel_ENCRYPTED.txt  Videos
Documents  Music      Public    Templates
student@TargetLinux01:~$
```

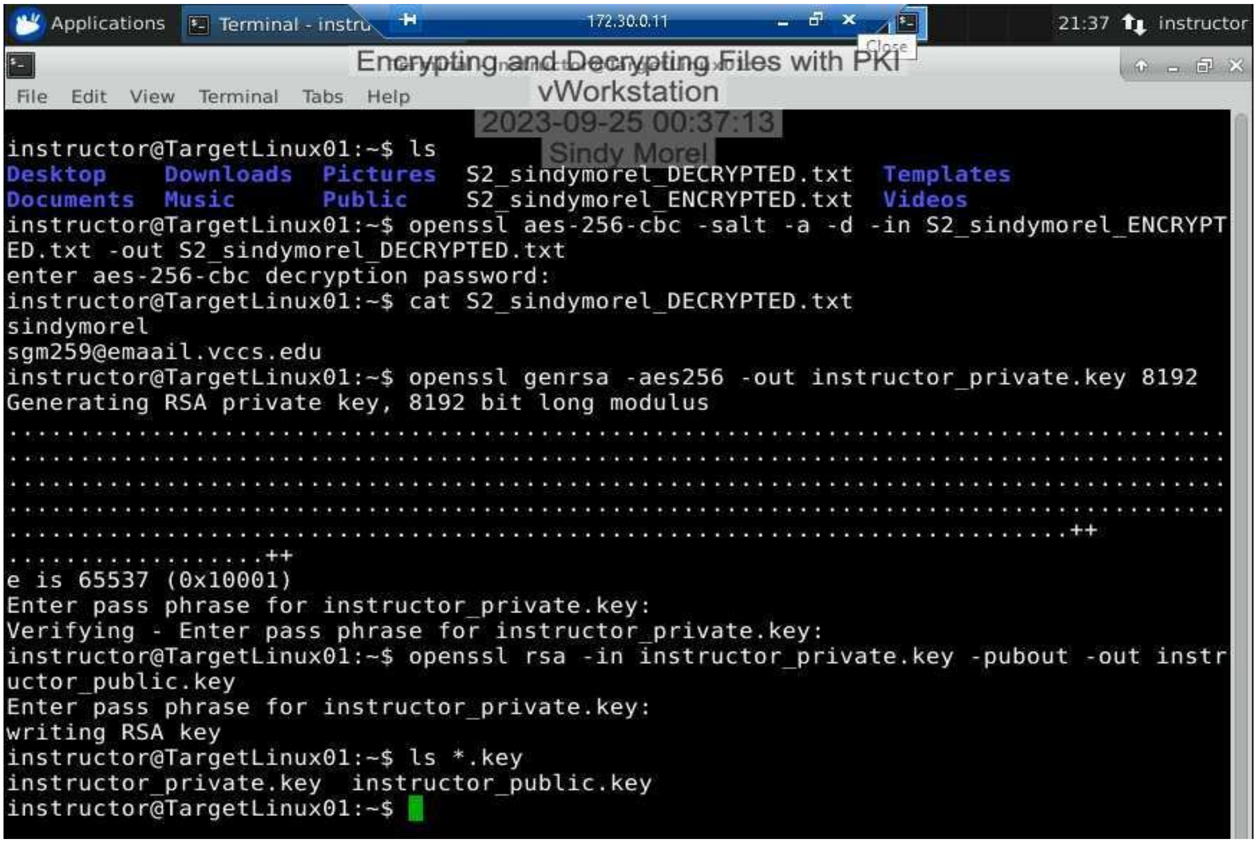
Password: R@1ny D@y!

Sindy Morel September 23, 2023

JBL LAB8: Encrypting and Decrypting Files with PKI



```
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_ENCRYPT
ED.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:~$
```

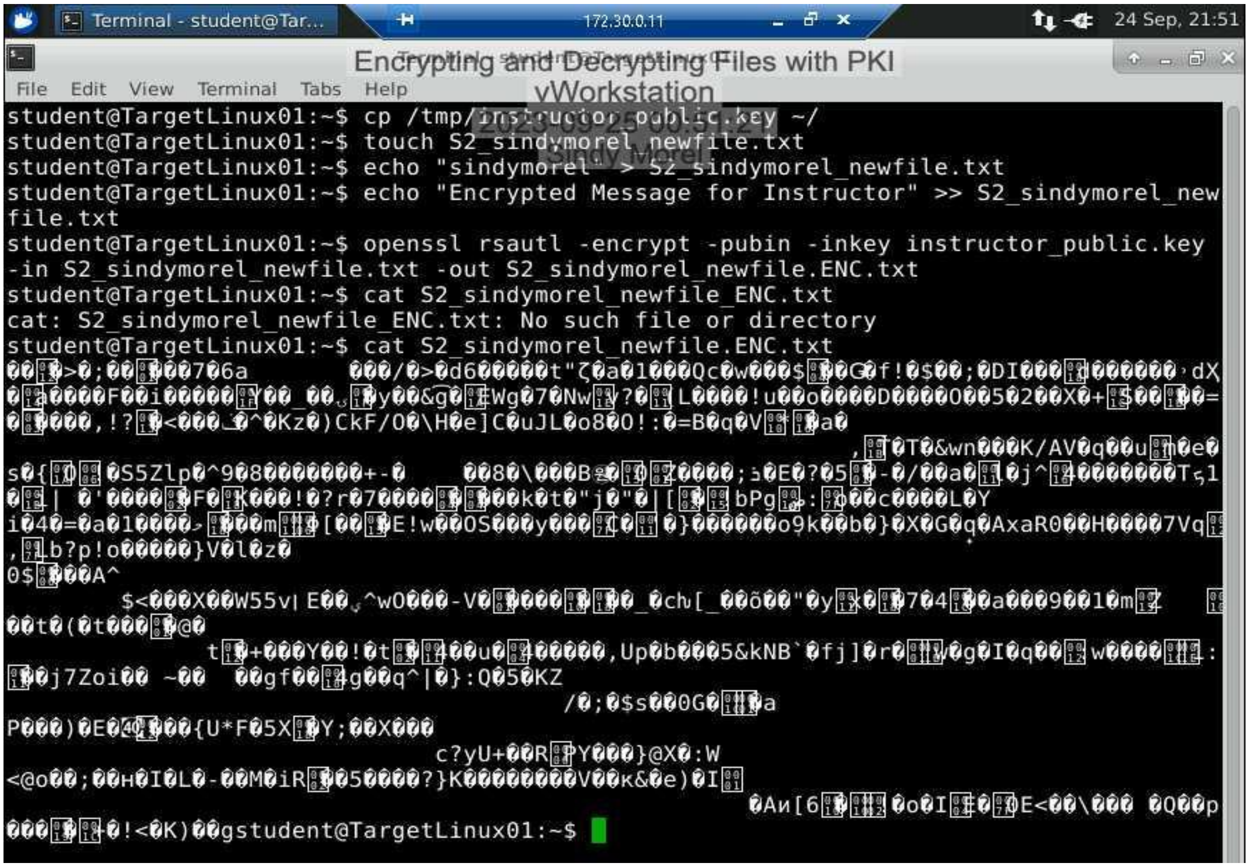


```
instructor@TargetLinux01:~$ ls
Desktop    Downloads  Pictures  S2_sindymorel_DECRYPTED.txt  Templates
Documents  Music      Public    S2_sindymorel_ENCRYPTED.txt  Videos
instructor@TargetLinux01:~$ openssl aes-256-cbc -salt -a -d -in S2_sindymorel_ENCRYPT
ED.txt -out S2_sindymorel_DECRYPTED.txt
enter 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 instr
uctor_public.key
Enter pass phrase for instructor_private.key:
writing RSA key
instructor@TargetLinux01:~$ ls *.key
instructor_private.key  instructor_public.key
instructor@TargetLinux01:~$
```

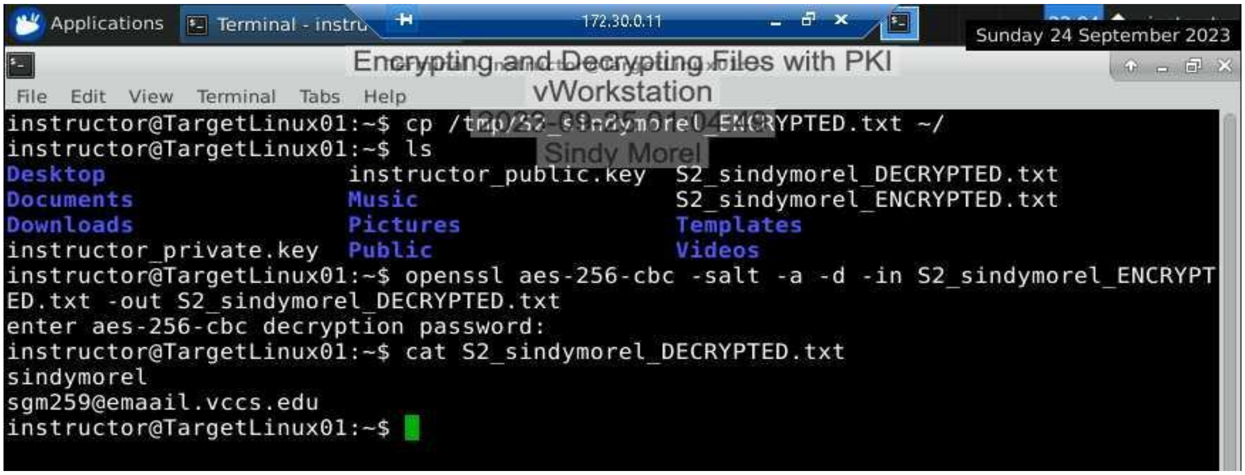
Sindy Morel September 23, 2023

JBL LAB8: Encrypting and
Decrypting Files with PKI

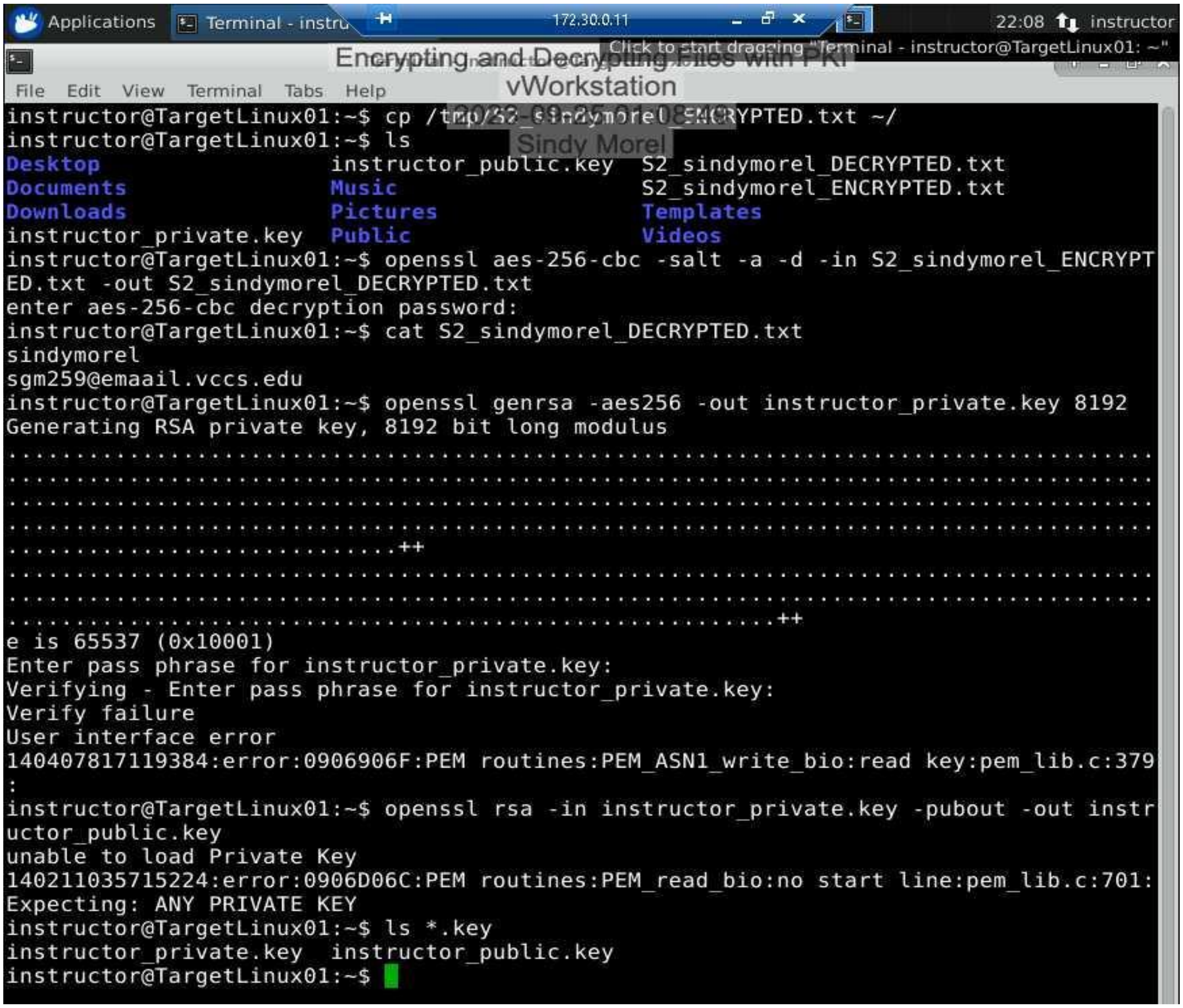
Part 2: Encrypt a File with Asymmetric Encryption



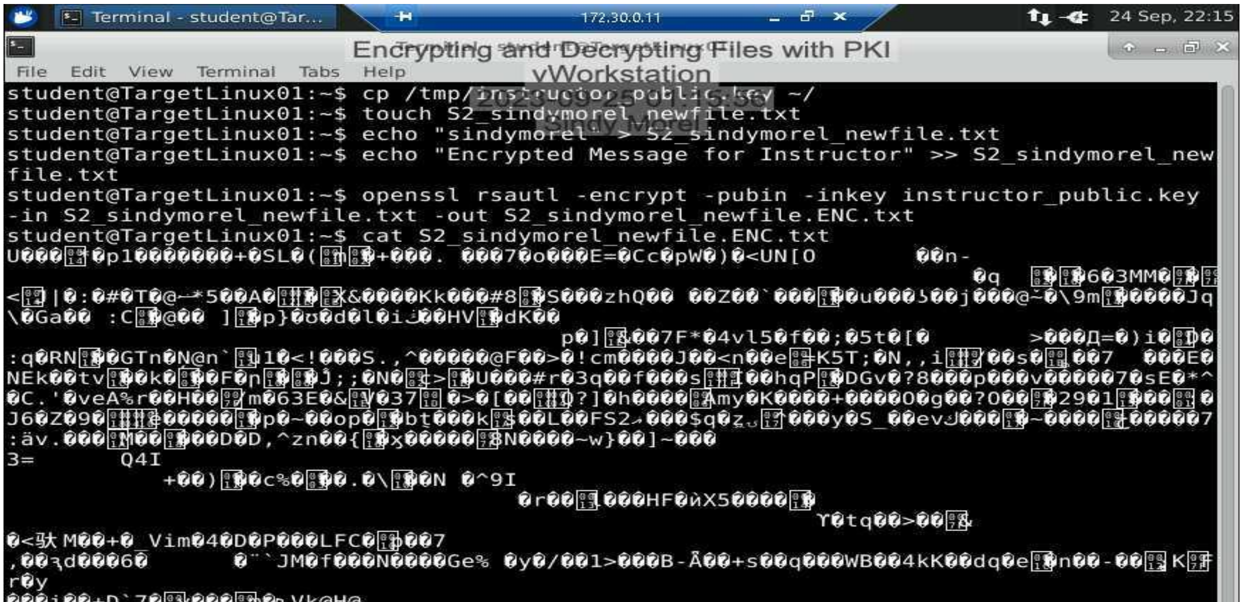
```
student@TargetLinux01:~$ cp /tmp/instructor_public.key ~/
student@TargetLinux01:~$ touch S2_sindymorel_newfile.txt
student@TargetLinux01:~$ echo "sindymorel" > S2_sindymorel_newfile.txt
student@TargetLinux01:~$ echo "Encrypted Message for Instructor" >> S2_sindymorel_new
file.txt
student@TargetLinux01:~$ 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
cat: S2_sindymorel_newfile_ENC.txt: No such file or directory
student@TargetLinux01:~$ cat S2_sindymorel_newfile.ENC.txt
���>�;����7�6a       ���/�>�d6������t"ζ�a�1���Qc�w���$��G�f!�$��;�DI���������dX
��a����F��i�������_��,��y��&g���Wg�7�Nw��?���L����!u��o����D�����O��5�2��X�+��$�����=
������,!?��<���_�^�Kz�)CkF/O�\H�e]C�uJL�o8�O!:�=B�q�V����a�
                                                            ,��T�T�&wn���K/AV�q��u��m�e�
s�{���S5Zlp�^9�8��������+-�     ��8�\���B����Z����;з�E�?�5��-�/��a���j^��4�������T၄1
���| �'�������F���K���!�?r�7������������k�t�"j�"�|[����bPg��:��o��c����L�Y
i�4�=�a�1�����₃����m���[�����E!w��OS���y������C���}������o9k��b�}�X�G�q�AxaR���H����7Vq��
,��b?p!o�����}V�l�z�
0$����A^
        $<���X��W55v| E��,^wO���-V�����������_�cհ[_��õ��"�y��x����7�4����a���9��1�m�Z    ��
��t�(�t������@�
                           t���+���Y��!�t������4��u���4�����,Up�b���5&kNB`�fj]�r�����g�I�q�����w���������:
���j7Zoi�� ~��  ��gf����4g��q^|�}:Q�5�KZ
                                             /�;�$s���G������a
P���)�E�����{U*F�5X���Y;��X���
                                                        c?yU+��R��PY���}@X�:W
<@o��;��H�I�L�-��M�iR����5����?}K��������V��K&�e)�I��
                                                                            �Aи[6�������o�I����E<��\��� �Q��p
����������!<�K)��gstudent@TargetLinux01:~$ 
```



```
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_ENCRYPT
ED.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:~$ 
```



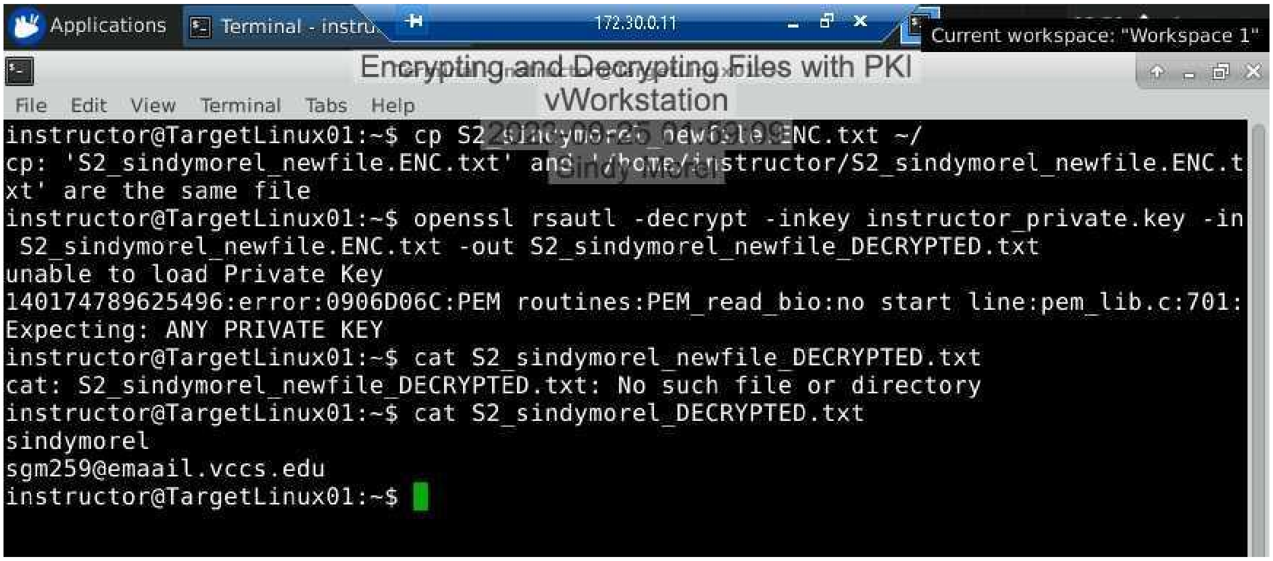
```
instructor@TargetLinux01:~$ cp /tmp/S2_sindymorel_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ ls
Desktop                 instructor_public.key  S2_sindymorel_DECRYPTED.txt
Documents               Music                  S2_sindymorel_ENCRYPTED.txt
Downloads               Pictures               Templates
instructor_private.key  Public                 Videos
instructor@TargetLinux01:~$ openssl aes-256-cbc -salt -a -d -in S2_sindymorel_ENCRYPT
ED.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 instr
uctor_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:~$ 
```



```
student@TargetLinux01:~$ cp /tmp/instructor_public.key ~/
student@TargetLinux01:~$ touch S2_sindymorel_newfile.txt
student@TargetLinux01:~$ echo "sindymorel" > S2_sindymorel_newfile.txt
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
U����p1��������+�SL�(��+���. ���7�o���E=�Cc�pW�)�<UN[O       ��n-
                                                             �q   ���6�3MM���
<�|�:�#�T�@⌐*5��A����X&����Kk���#8��S���zhQ�� ��Z��`�����u���ʖ��j���@~�\9m������Jq
\�Ga�� :C��@�� ]��p}�ʊ�d�l�iر��HV��dK��
                                   p�]��007F*�4vl5�f��;�5t�[�         >���Д=�)i����
:q�RN���GTn�N@n`��1�<!���S.,^�����@F��>�!cm����J��<n��e��K5T;�N,,i���'��s���007  ���E�
NEk��tv���k����F�ɳ����J;;�N��¢>��U���#r�3q��f���s����hqP��DGv�?8���p���v�����7�sE�*^
�C.'�veA%r��H����m�63E�&��V�37���>�[�����?]�h������Amy�K����+�����0g��?O������2901�������
J6�Z�9���������p�~��op��btੑ��k��$��L��FS2ؚ���$q�ẓڼ���y�S_��ev؎�����~�����������7
:äv.�������D�D,^zn��{��ӿ�����N����~w}��]~���
3=       Q4I
          +��)���c%����.�\���N �^9I
                                  �r�������HF�йX5������
                                                      Ƴ�tq��>���&
�<驮M��+�_Vim�4�D�P���LFC����7
,��ʒd����6�       �¨`JM�f���N����Ge% �y�/��1>���B-Ä��+s��q���WB��4kK��dq�e��n��-���K��
r�y
```

Sindy Morel September 23, 2023

JBL LAB8: Encrypting and Decrypting Files with PKI



Applications
Terminal - instru
172.30.0.11
Current workspace: "Workspace 1"
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-25 01:59:09
Sindy Morel
File Edit View Terminal Tabs Help

```
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:~$ 
```