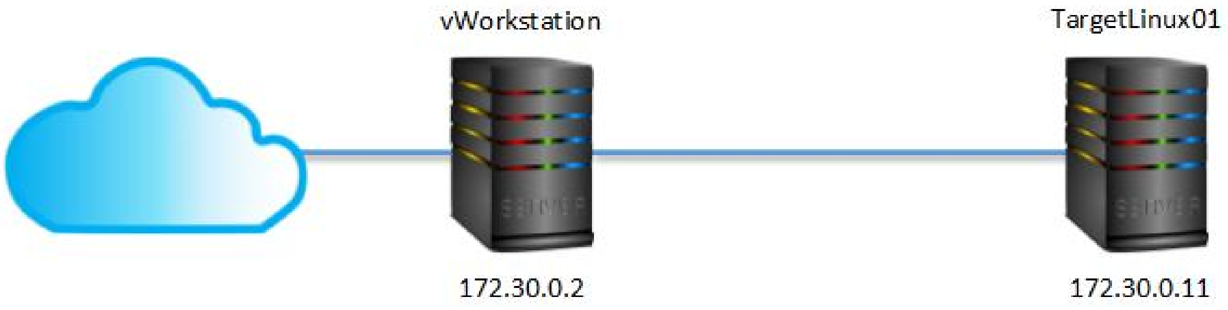
JBL LAB8: Encrypting and Decrypting Files with PKI

Sindy Morel	JBL LAB8: Encrypting and Decrypting Files with PKI	September 23, 2023

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

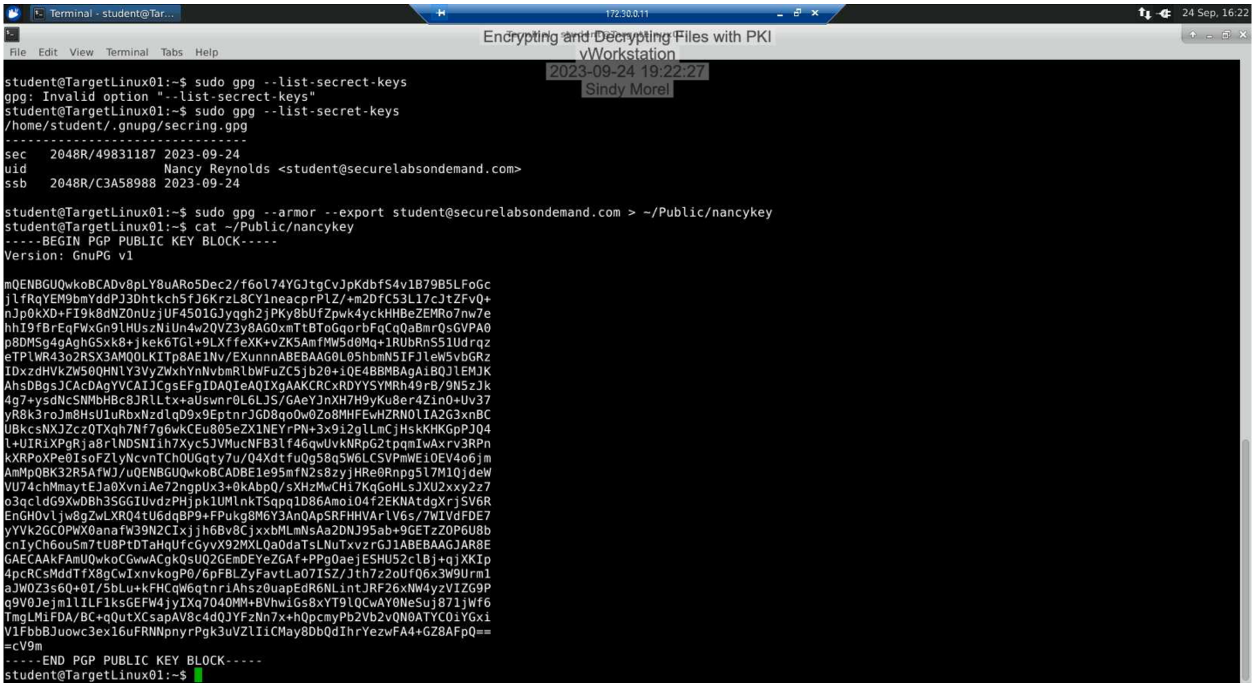
The following software and/or utilities are required to complete this lab. You are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- GNU Privacy Guard (GnuPG or GPG)

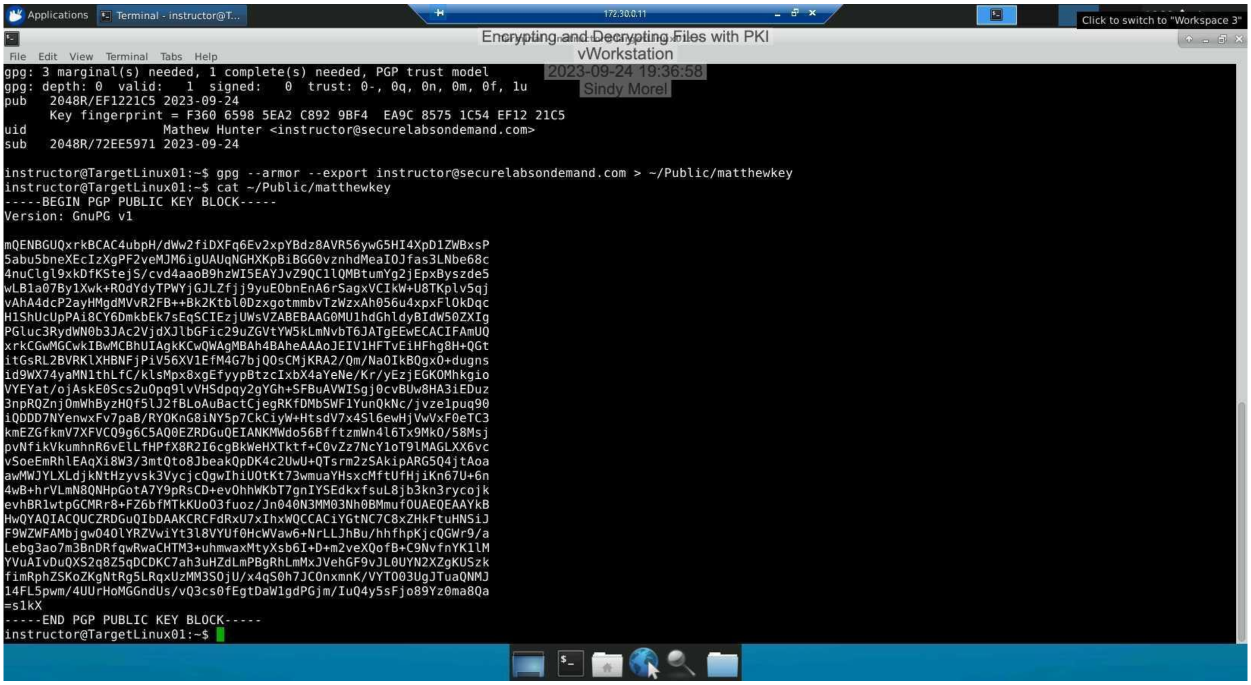
Sindy Morel	JBL LAB8: Encrypting and Decrypting Files with PKI	September 23, 2023

Section 1: Hands-On Demonstration

Part 1: Create Encryption Keys

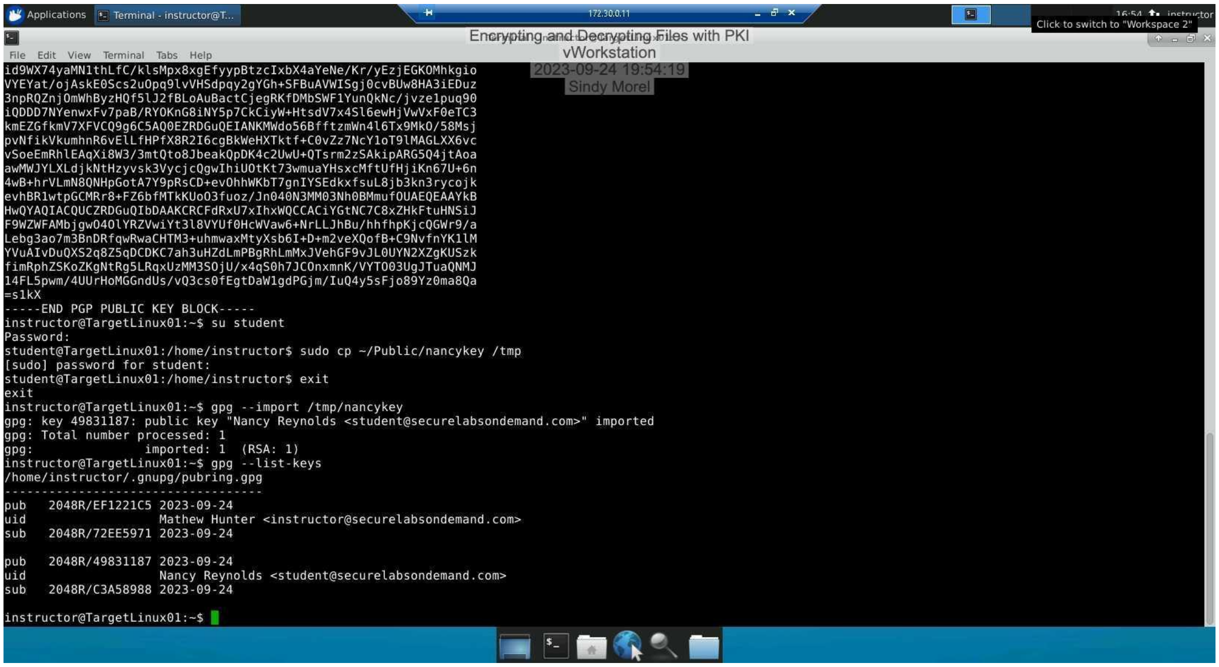

Terminal - student@Tar...
172.30.0.11
24 Sep, 16:22
File Edit View Terminal Tabs Help
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-24 19:22:27
Sindy Morel

```
student@TargetLinux01:~$ sudo gpg --list-secrect-keys
gpg: Invalid option "--list-secrect-keys"
student@TargetLinux01:~$ sudo gpg --list-secret-keys
/home/student/.gnupg/secring.gpg
--------------------------------
sec   2048R/49831187 2023-09-24
uid                  Nancy Reynolds <student@securelabsondemand.com>
ssb   2048R/C3A58988 2023-09-24

student@TargetLinux01:~$ sudo gpg --armor --export student@securelabsondemand.com > ~/Public/nancykey
student@TargetLinux01:~$ cat ~/Public/nancykey
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBGUQwkoBCADv8pLY8uARo5Dec2/f6ol74YGJtgCvJpKdbfS4v1B79B5LFoGc
jlfRqYEM9bmYddPJ3Dhtkch5fJ6KrzL8CY1neacprPlZ/+m2DfC53L17cJtZFvQ+
nJp0kXD+FI9k8dNZOnUzjUF4501GJyqgh2jPKy8bUfZpwk4yckHHBeZEMRo7nw7e
hhI9fBrEqFWxGn9lHUszNiUn4w2QVZ3y8AGOxmTtBToGqorbFqCqQaBmrQsGVPA0
p8DMSg4gAghGSxk8+jkek6TGl+9LXffeXK+vZK5AmfMW5d0Mq+1RUbRnS51Udrqz
eTPlWR43o2RSX3AMQOLKITp8AE1Nv/EXunnnABEBAAG0L05hbmN5IFJleW5vbGRz
IDxzdHVkZW50QHNlY3VyZWxhYnNvbmRlbWFuZC5jb20+iQE4BBMBAgAiBQJlEMJK
AhsDBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRCxRDYYSYMRh49rB/9N5zJk
4g7+ysdNcSNMbHBc8JRlLtx+aUswnr0L6LJS/GAeYJnXH7H9yKu8er4ZinO+Uv37
yR8k3roJm8HsU1uRbxNzdlqD9x9EptnrJGD8qoOw0Zo8MHFEwHZRNOlIA2G3xnBC
UBkcsNXJZczQTXqh7Nf7g6wkCEu805eZX1NEYrPN+3x9i2glLmCjHskKHKGpPJQ4
l+UIRiXPgRja8rlNDSNIih7Xyc5JVMucNFB3lf46qwUvkNRpG2tpqmIwAxrv3RPn
kXRPoXPe0IsoFZlyNcvnTChOUGqty7u/Q4XdtfuQg58q5W6LCSVPmWEiOEV4o6jm
AmMpQBK32R5AfWJ/uQENBGUQwkoBCADBE1e95mfN2s8zyjHRe0Rnpg5l7M1QjdeW
VU74chMmaytEJa0XvniAe72ngpUx3+0kAbpQ/sXHzMwCHi7KqGoHLsJXU2xxy2z7
o3qcldG9XwDBh3SGGIUvdzPHjpk1UMlnkTSqpq1D86AmoiO4f2EKNAtdgXrjSV6R
EnGHOvljw8gZwLXRQ4tU6dqBP9+FPukg8M6Y3AnQApSRFHHVArlV6s/7WIVdFDE7
yYVk2GCOPWX0anafW39N2CIxjjh6Bv8CjxxbMLmNsAa2DNJ95ab+9GETzZOP6U8b
cnIyCh6ouSm7tU8PtDTaHqUfcGyvX92MXLQaOdaTsLNuTxvzrGJ1ABEBAAGJAR8E
GAECAAkFAmUQwkoCGwwACgkQsUQ2GEmDEYeZGAf+PPgOaejESHU52clBj+qjXKIp
4pcRCsMddTfX8gCwIxnvkogP0/6pFBLZyFavtLaO7ISZ/Jth7z2oUfQ6x3W9Urm1
aJWOZ3s6Q+0I/5bLu+kFHCqW6qtnriAhsz0uapEdR6NLintJRF26xNW4yzVIZG9P
q9V0Jejm1lILF1ksGEFW4jyIXq7O4OMM+BVhwiGs8xYT9lQCwAY0NeSuj871jWf6
TmgLMiFDA/BC+qQutXCsapAV8c4dQJYFzNn7x+hQpcmyPb2Vb2vQN0ATYCOiYGxi
V1FbbBJuowc3ex16uFRNNpnyrPgk3uVZlIiCMay8DbQdIhrYezwFA4+GZ8AFpQ==
=cV9m
-----END PGP PUBLIC KEY BLOCK-----
student@TargetLinux01:~$
```

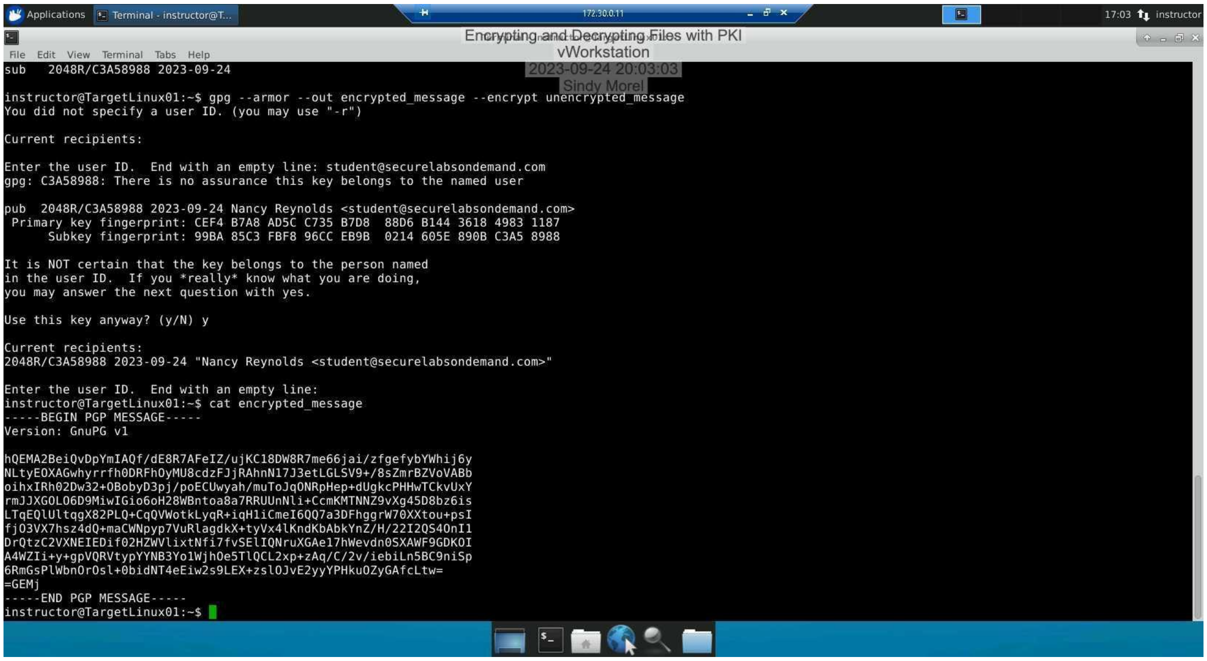

Applications
Terminal - instructor@T...
172.30.0.11
Click to switch to "Workspace 3"
File Edit View Terminal Tabs Help
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-24 19:36:58
Sindy Morel

```
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   2048R/EF1221C5 2023-09-24
      Key fingerprint = F360 6598 5EA2 C892 9BF4  EA9C 8575 1C54 EF12 21C5
uid                  Mathew Hunter <instructor@securelabsondemand.com>
sub   2048R/72EE5971 2023-09-24

instructor@TargetLinux01:~$ gpg --armor --export instructor@securelabsondemand.com > ~/Public/matthewkey
instructor@TargetLinux01:~$ cat ~/Public/matthewkey
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBGUQxrkBCAC4ubpH/dWw2fiDXFq6Ev2xpYBdz8AVR56ywG5HI4XpD1ZWBxsP
5abu5bneXEcIzXgPF2veMJM6igUAUqNGHXKpBiBGG0vznhdMeaIOJfas3LNbe68c
4nuClgl9xkDfKStejS/cvd4aaoB9hzWI5EAYJvZ9QC1lQMBtumYg2jEpxByszde5
wLB1a07By1Xwk+ROdYdyTPWYjGJLZfjj9yuEObnEnA6rSagxVCIkW+U8TKplv5qj
vAhA4dcP2ayHMgdMVvR2FB++Bk2Ktbl0DzxgotmmbvTzWzxAh056u4xpxFlOkDqc
H1ShUcUpPAi8CY6DmkbEk7sEqSCIEzjUWsVZABEBAAG0MU1hdGhldyBIdW50ZXIg
PGluc3RydWN0b3JAc2VjdXJlbGFic29uZGVtYW5kLmNvbT6JATgEEwECACIFAmUQ
xrkCGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEIV1HFTvEiHFhg8H+QGt
itGsRL2BVRKlXHBNFjPiV56XV1EfM4G7bjQOsCMjKRA2/Qm/NaOIkBQgxO+dugns
id9WX74yaMN1thLfC/klsMpx8xgEfyypBtzcIxbX4aYeNe/Kr/yEzjEGKOMhkgio
VYEYat/ojAskE0Scs2uOpq9lvVHSdpqy2gYGh+SFBuAVWISgj0cvBUw8HA3iEDuz
3npRQZnjOmWhByzHQf5lJ2fBLoAuBactCjegRKfDMbSWF1YunQkNc/jvze1puq90
iQDDD7NYenwxFv7paB/RYOKnG8iNY5p7CkCiyW+HtsdV7x4Sl6ewHjVwVxF0eTC3
kmEZGfkmV7XFVCQ9g6C5AQ0EZRDGuQEIANKMWdo56BfftzmWn4l6Tx9MkO/58Msj
pvNfikVkumhnR6vElLfHPfX8R2I6cgBkWeHXTktf+C0vZz7NcY1oT9lMAGLXX6vc
vSoeEmRhlEAqXi8W3/3mtQto8JbeakQpDK4c2UwU+QTsrm2zSAkipARG5Q4jtAoa
awMWJYLXLdjkNtHzyvsk3VycjcQgwIhiUOtKt73wmuaYHsxcMftUfHjiKn67U+6n
4wB+hrVLmN8QNHpGotA7Y9pRsCD+evOhhWKbT7gnIYSEdkxfsuL8jb3kn3rycojk
evhBR1wtpGCMRr8+FZ6bfMTkKUoO3fuoz/Jn04ON3MM03Nh0BMmufOUAEQEAAYkB
HwQYAQIACQUCZRDGuQIbDAAKCRCFdRxU7xIhxWQCCACiYGtNC7C8xZHkFtuHNSiJ
F9WZWFAMbjgwO4OlYRZVwiYt3l8VYUf0HcWVaw6+NrLLJhBu/hhfhpKjcQGWr9/a
Lebg3ao7m3BnDRfqwRwaCHTM3+uhmwaxMtyXsb6I+D+m2veXQofB+C9NvfnYK1lM
YVuAIvDuQXS2q8Z5qDCDKC7ah3uHZdLmPBgRhLmMxJVehGF9vJL0UYN2XZgKUSzk
fimRphZSKoZKgNtRg5LRqxUzMM3SOjU/x4qS0h7JCOnxmnK/VYTO03UgJTuaQNMJ
14FL5pwm/4UUrHoMGGndUs/vQ3cs0fEgtDaW1gdPGjm/IuQ4y5sFjo89Yz0ma8Qa
=s1kX
-----END PGP PUBLIC KEY BLOCK-----
instructor@TargetLinux01:~$
```

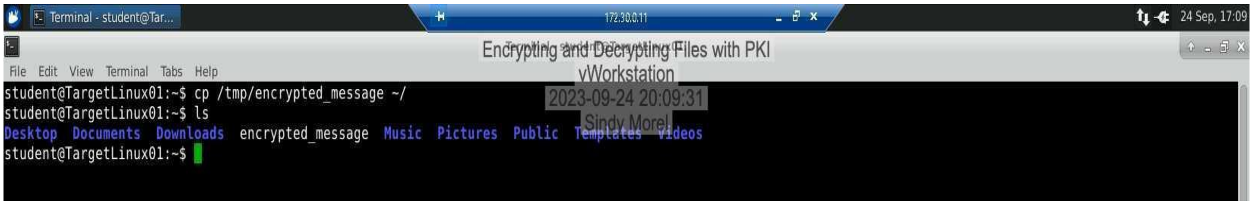
Part 2: Encrypt a File


Applications
Terminal - instructor@T...
172.30.0.11
16:54
instructor
Click to switch to "Workspace 2"
File Edit View Terminal Tabs Help
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-24 19:54:19
Sindy Morel

```
id9WX74yaMN1thLfC/klsMpx8xgEfyypBtzcIxbX4aYeNe/Kr/yEzjEGKOMhkgio
VYEYat/ojAskE0Scs2uOpq9lvVHSdpqy2gYGh+SFBuAVWISgj0cvBUw8HA3iEDuz
3npRQZnjOmWhByzHQf5lJ2fBLoAuBactCjegRKfDMbSWF1YunQkNc/jvze1puq90
iQDDD7NYenwxFv7paB/RYOKnG8iNY5p7CkCiyW+HtsdV7x4Sl6ewHjVwVxF0eTC3
kmEZGfkmV7XFVCQ9g6C5AQ0EZRDGuQEIANKMWdo56BfftzmWn4l6Tx9MkO/58Msj
pvNfikVkumhnR6vElLfHPfX8R2I6cgBkWeHXTktf+C0vZz7NcY1oT9lMAGLXX6vc
vSoeEmRhlEAqXi8W3/3mtQto8JbeakQpDK4c2UwU+QTsrm2zSAkipARG5Q4jtAoa
awMWJYLXLdjkNtHzyvsk3VycjcQgwIhiUOtKt73wmuaYHsxcMftUfHjiKn67U+6n
4wB+hrVLmN8QNHpGotA7Y9pRsCD+evOhhWKbT7gnIYSEdkxfsuL8jb3kn3rycojk
evhBR1wtpGCMRr8+FZ6bfMTkKUoO3fuoz/Jn040N3MM03Nh0BMmufOUAEQEAAYkB
HwQYAQIACQUCZRDGuQIbDAAKCRCFdRxU7xIhxWQCCACiYGtNC7C8xZHkFtuHNSiJ
F9WZWFAMbjgwO4OlYRZVwiYt3l8VYUf0HcWVaw6+NrLLJhBu/hhfhpKjcQGWr9/a
Lebg3ao7m3BnDRfqwRwaCHTM3+uhmwaxMtyXsb6I+D+m2veXQofB+C9NvfnYK1lM
YVuAIvDuQXS2q8Z5qDCDKC7ah3uHZdLmPBgRhLmMxJVehGF9vJL0UYN2XZgKUSzk
fimRphZSKoZKgNtRg5LRqxUzMM3SOjU/x4qS0h7JCOnxmnK/VYTO03UgJTuaQNMJ
14FL5pwm/4UUrHoMGGndUs/vQ3cs0fEgtDaW1gdPGjm/IuQ4y5sFjo89Yz0ma8Qa
=s1kX
-----END PGP PUBLIC KEY BLOCK-----
instructor@TargetLinux01:~$ su student
Password:
student@TargetLinux01:/home/instructor$ sudo cp ~/Public/nancykey /tmp
[sudo] password for student:
student@TargetLinux01:/home/instructor$ exit
exit
instructor@TargetLinux01:~$ gpg --import /tmp/nancykey
gpg: key 49831187: public key "Nancy Reynolds <student@securelabsondemand.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
instructor@TargetLinux01:~$ gpg --list-keys
/home/instructor/.gnupg/pubring.gpg
-----------------------------------
pub   2048R/EF1221C5 2023-09-24
uid                  Mathew Hunter <instructor@securelabsondemand.com>
sub   2048R/72EE5971 2023-09-24

pub   2048R/49831187 2023-09-24
uid                  Nancy Reynolds <student@securelabsondemand.com>
sub   2048R/C3A58988 2023-09-24

instructor@TargetLinux01:~$
```

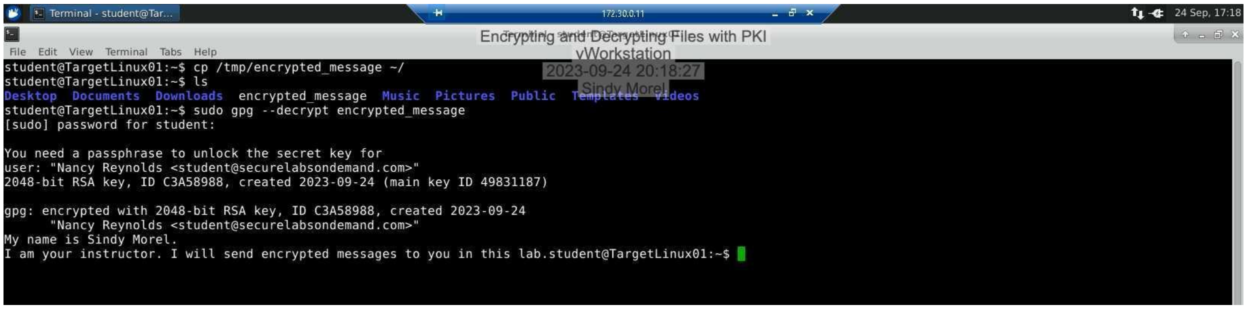

Applications
Terminal - instructor@T...
172.30.0.11
17:03
instructor
File Edit View Terminal Tabs Help
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-24 20:03:03
Sindy Morel

```
sub   2048R/C3A58988 2023-09-24

instructor@TargetLinux01:~$ gpg --armor --out encrypted_message --encrypt unencrypted_message
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID.  End with an empty line: student@securelabsondemand.com
gpg: C3A58988: There is no assurance this key belongs to the named user

pub  2048R/C3A58988 2023-09-24 Nancy Reynolds <student@securelabsondemand.com>
 Primary key fingerprint: CEF4 B7A8 AD5C C735 B7D8  88D6 B144 3618 4983 1187
      Subkey fingerprint: 99BA 85C3 FBF8 96CC EB9B  0214 605E 890B C3A5 8988

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y

Current recipients:
2048R/C3A58988 2023-09-24 "Nancy Reynolds <student@securelabsondemand.com>"

Enter the user ID.  End with an empty line:
instructor@TargetLinux01:~$ cat encrypted_message
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

hQEMA2BeiQvDpYmIAQf/dE8R7AFeIZ/ujKC18DW8R7me66jai/zfgefybYWhij6y
NLtyEOXAGwhyrrfh0DRFhOyMU8cdzFJjRAhnN17J3etLGLSV9+/8sZmrBZVoVABb
oihxIRh02Dw32+OBobyD3pj/poECUwyah/muToJqONRpHep+dUgkcPHHwTCkvUxY
rmJJXGOLO6D9MiwIGio6oH28WBntoa8a7RRUUnNli+CcmKMTNNZ9vXg45D8bz6is
LTqEQlUltqgX82PLQ+CqQVWotkLyqR+iqH1iCmeI6QQ7a3DFhggrW70XXtou+psI
fjO3VX7hsz4dQ+maCWNpyp7VuRlagdkX+tyVx4lKndKbAbkYnZ/H/22I2QS4OnI1
DrQtzC2VXNEIEDif02HZWVlixtNfi7fvSElIQNruXGAe17hWevdn0SXAWF9GDKOI
A4WZIi+y+gpVQRVtypYYNB3Yo1WjhOe5TlQCL2xp+zAq/C/2v/iebiLn5BC9niSp
6RmGsPlWbnOrOsl+0bidNT4eEiw2s9LEX+zslOJvE2yyYPHkuOZyGAfcLtw=
=GEMj
-----END PGP MESSAGE-----
instructor@TargetLinux01:~$
```


Terminal - student@Tar...
172.30.0.11
24 Sep, 17:09
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-24 20:09:31
Sindy Morel
File Edit View Terminal Tabs Help

```
student@TargetLinux01:~$ cp /tmp/encrypted_message ~/
student@TargetLinux01:~$ ls
Desktop  Documents  Downloads  encrypted_message  Music  Pictures  Public  Templates  Videos
student@TargetLinux01:~$
```

Part 3: Decrypting a File


Terminal - student@Tar...
172.30.0.11
24 Sep, 17:18
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-24 20:18:27
Sindy Morel
File Edit View Terminal Tabs Help

```
student@TargetLinux01:~$ cp /tmp/encrypted_message ~/
student@TargetLinux01:~$ ls
Desktop  Documents  Downloads  encrypted_message  Music  Pictures  Public  Templates  Videos
student@TargetLinux01:~$ sudo gpg --decrypt encrypted_message
[sudo] password for student:

You need a passphrase to unlock the secret key for
user: "Nancy Reynolds <student@securelabsondemand.com>"
2048-bit RSA key, ID C3A58988, created 2023-09-24 (main key ID 49831187)

gpg: encrypted with 2048-bit RSA key, ID C3A58988, created 2023-09-24
      "Nancy Reynolds <student@securelabsondemand.com>"
My name is Sindy Morel.
I am your instructor. I will send encrypted messages to you in this lab.student@TargetLinux01:~$
```