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

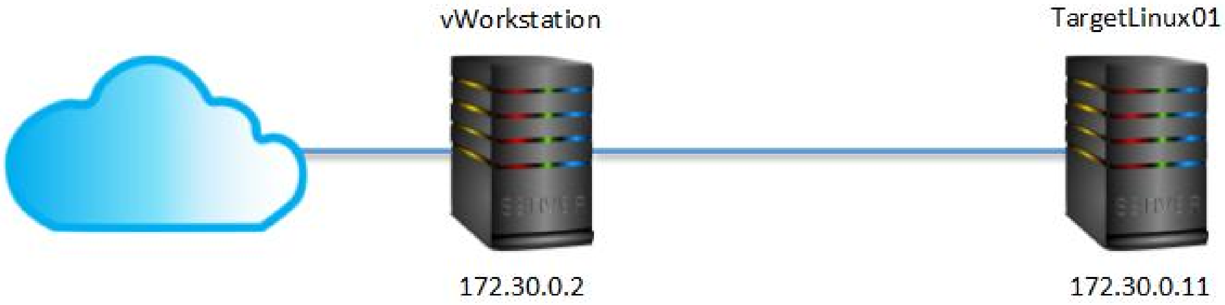
JBL LAB 8: Encrypting and Decrypting Files with PKI

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)

Section 3: Challenge and Analysis

Part 1: Analysis and Discussion

Sharing a private k Sharing a private key, especially in RSA encryption, is a severe security risk with significant consequences:

1. Confidentiality Loss: Matthew could decrypt data meant only for Nancy, risking unauthorized access to classified information.

2. Data Integrity Risk: Matthew's access to Nancy's private key could result in data tampering before decryption.

3. Identity Impersonation: Matthew could impersonate Nancy, signing messages fraudulently.

4. Trust Erosion: Sharing keys undermines trust, impacting reputation and legal compliance.

5. Legal Concerns: Sharing keys may violate laws and regulations, leading to fines.

6. Insecure Encrypted Communication: Messages relying on Nancy's key become vulnerable.

Part 2: Tools and Commands

Rainbow tables expedite password cracking by matching hash values to plaintext passwords. However, salting disrupts their efficacy.

1. Unique Hashes for Each User: Salting ensures even identical passwords yield different hashes, thwarting simultaneous attacks on multiple hashes.

2. Expanded Hash Space: Salting increases the hash space, making exhaustive rainbow table generation impractical.

3. Resource-Intensive: Creating salted rainbow tables demands more resources and time, slowing down cracking attempts.

4. Limited Reusability: Salted hashes are system-specific, hindering rainbow table reuse across systems.

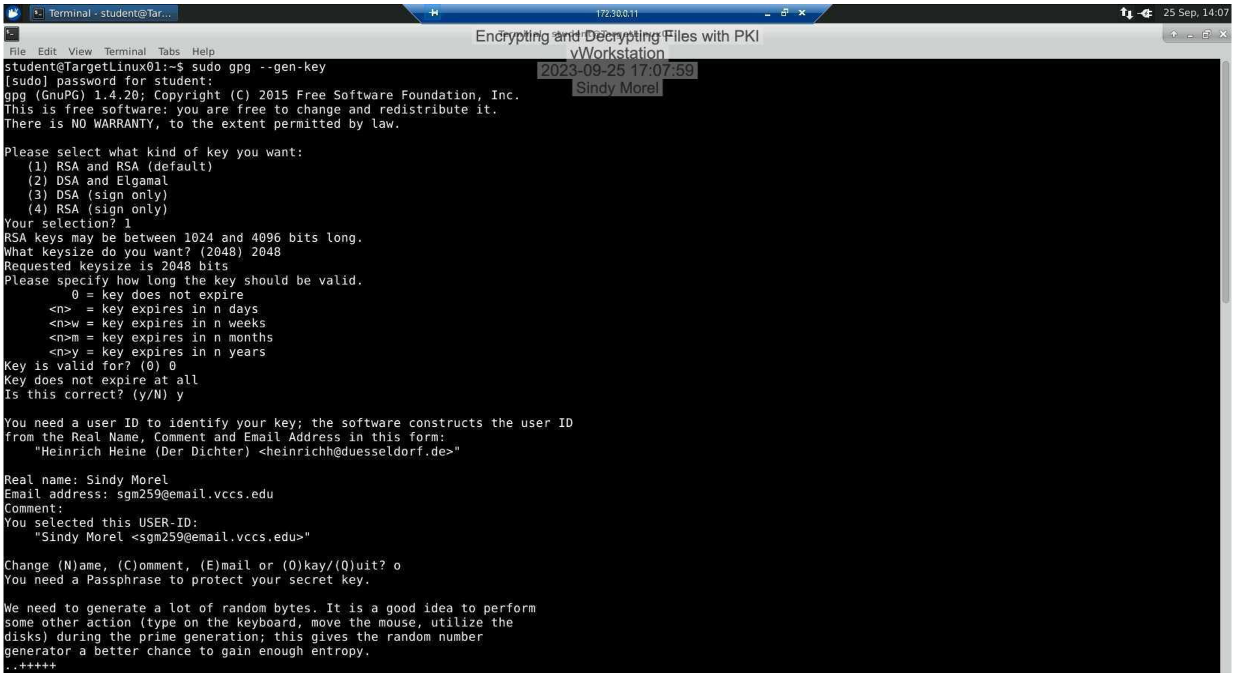
5. No Precomputation: Salting introduces unpredictability, making precomputation of hash tables ineffective.

Salting is a vital security practice, safeguarding hashed passwords by thwarting rainbow tables through uniqueness, complexity, and system specificity.

Part 3: Challenge Exercise

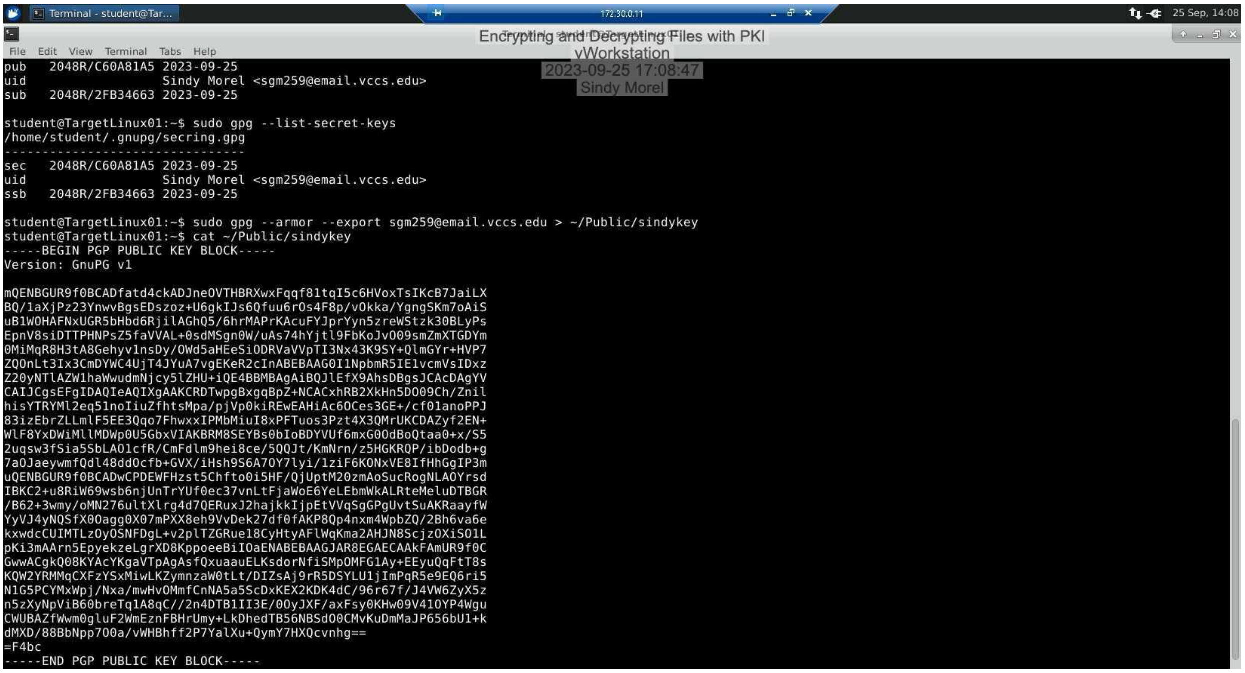
Keys Generated

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


Terminal - student@Tar...
172.30.0.11
25 Sep, 14:07
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-25 17:07:59
Sindy Morel
File Edit View Terminal Tabs Help

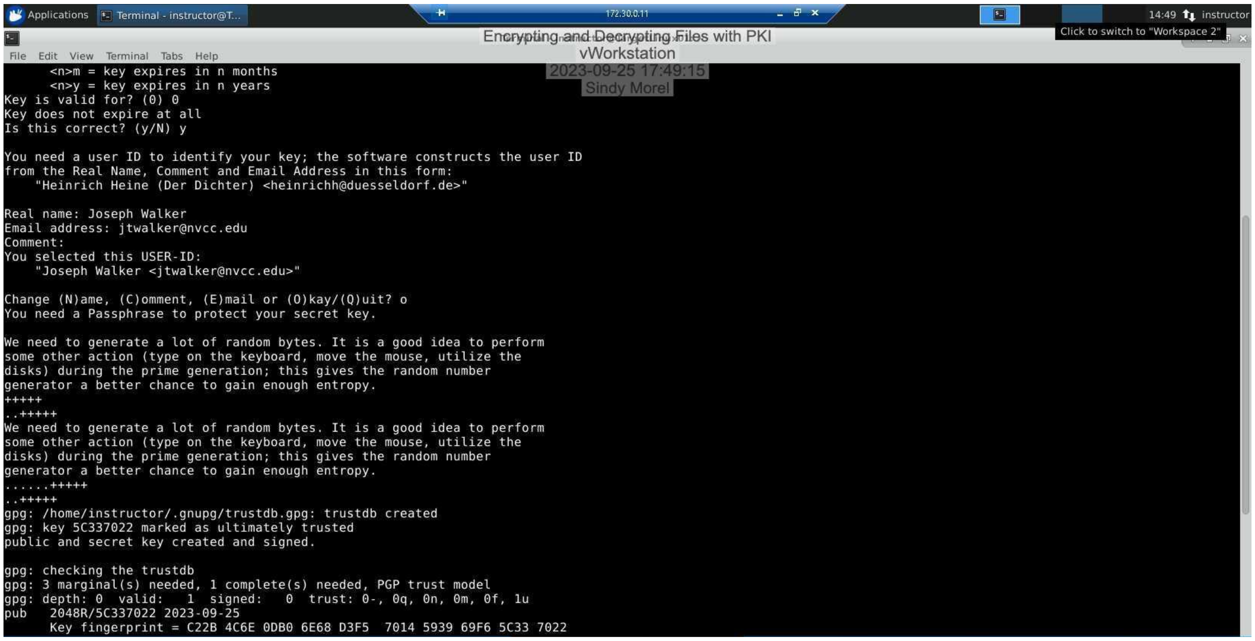
```
student@TargetLinux01:~$ sudo gpg --gen-key
[sudo] password for student:
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Sindy Morel
Email address: sgm259@email.vccs.edu
Comment:
You selected this USER-ID:
    "Sindy Morel <sgm259@email.vccs.edu>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
..+++++
```

Encrypted Keys

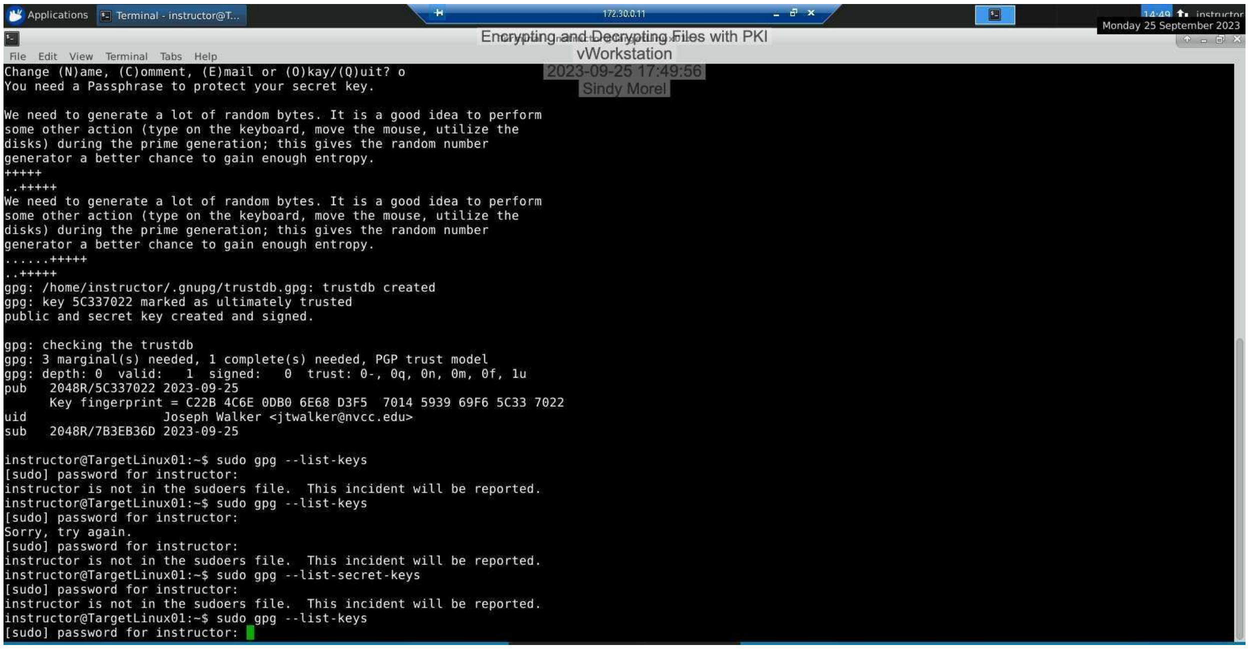

Terminal - student@Tar...
172.30.0.11
25 Sep, 14:08
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-25 17:08:47
Sindy Morel
File Edit View Terminal Tabs Help

```
pub   2048R/C60A81A5 2023-09-25
uid                  Sindy Morel <sgm259@email.vccs.edu>
sub   2048R/2FB34663 2023-09-25

student@TargetLinux01:~$ sudo gpg --list-secret-keys
/home/student/.gnupg/secring.gpg
--------------------------------
sec   2048R/C60A81A5 2023-09-25
uid                  Sindy Morel <sgm259@email.vccs.edu>
ssb   2048R/2FB34663 2023-09-25

student@TargetLinux01:~$ sudo gpg --armor --export sgm259@email.vccs.edu > ~/Public/sindykey
student@TargetLinux01:~$ cat ~/Public/sindykey
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBGUR9f0BCADfatd4ckADJneOVTHBRXwxFqqf81tqI5c6HVoxTsIKcB7JaiLX
BQ/1aXjPz23YnwvBgsEDszoz+U6gkIJs6Qfuu6rOs4F8p/vOkka/YgngSKm7oAiS
uB1WOHAFNxUGR5bHbd6RjilAGhQ5/6hrMAPrKAcuFYJprYyn5zreWStzk30BLyPs
EpnV8siDTTPHNPsZ5faVVAL+0sdMSgn0W/uAs74hYjtl9FbKoJvO09smZmXTGDYm
0MiMqR8H3tA8Gehyv1nsDy/OWd5aHEeSiODRVaVVpTI3Nx43K9SY+QlmGYr+HVP7
ZQOnLt3Ix3CmDYWC4UjT4JYuA7vgEKeR2cInABEBAAG0I1NpbmR5IE1vcmVsIDxz
Z20yNTlAZW1haWwudmNjcy5lZHU+iQE4BBMBAgAiBQJlEfX9AhsDBgsJCAcDAgYV
CAIJCgsEFgIDAQIeAQIXgAAKCRDTwpgBxgqBpZ+NCACxhRB2XkHn5DO09Ch/Znil
hisYTRYMl2eq51noIiuZfhtsMpa/pjVp0kiREwEAHiAc6OCes3GE+/cf01anoPPJ
83izEbrZLLmlF5EE3Qqo7FhwxxIPMbMiuI8xPFTuos3Pzt4X3QMrUKCDAZyf2EN+
WlF8YxDWiMllMDWp0U5GbxVIAKBRM8SEYBs0bIoBDYVUf6mxG0OdBoQtaa0+x/S5
2uqsw3fSia5SbLAO1cfR/CmFdlm9hei8ce/5QQJt/KmNrn/z5HGKRQP/ibDodb+g
7aOJaeywmfQdl48ddOcfb+GVX/iHsh9S6A7OY7lyi/1ziF6KONxVE8IfHhGgIP3m
uQENBGUR9f0BCADwCPDEWFHzst5Chfto0i5HF/QjUptM20zmAoSucRogNLAOYrsd
IBKC2+u8RiW69wsb6njUnTrYUf0ec37vnLtFjaWoE6YeLEbmWkALRteMeluDTBGR
/B62+3wmy/oMN276ultXlrg4d7QERuxJ2hajkkIjpEtVVqSgGPgUvtSuAKRaayfW
YyVJ4yNQSfX0Oagg0X07mPXX8eh9VvDek27df0fAKP8Qp4nxm4WpbZQ/2Bh6va6e
kxwdcCUIMTLzOyOSNFDgL+v2plTZGRue18CyHtyAFlWqKma2AHJN8ScjzOXiSO1L
pKi3mAArn5EpyekzeLgrXD8KppoeeBiIOaENABEBAAGJAR8EGAECAAkFAmUR9f0C
GwwACgkQ08KYAcYKgaVTpAgAsfQxuaauELKsdorNfiSMpOMFG1Ay+EEyuQqFtT8s
KQW2YRMMqCXFzYSxMiwLKZymnzaW0tLt/DIZsAj9rR5DSYLU1jImPqR5e9EQ6ri5
N1G5PCYMxWpj/Nxa/mwHvOMmfCnNA5a5ScDxKEX2KDK4dC/96r67f/J4VW6ZyX5z
n5zXyNpViB60breTq1A8qC//2n4DTB1II3E/0OyJXF/axFsy0KHw09V41OYP4Wgu
CWUBAZfWwm0gluF2WmEznFBHrUmy+LkDhedTB56NBSdO0CMvKuDmMaJP656bU1+k
dMXD/88BbNpp7O0a/vWHBhff2P7YalXu+QymY7HXQcvnhg==
=F4bc
-----END PGP PUBLIC KEY BLOCK-----
```

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

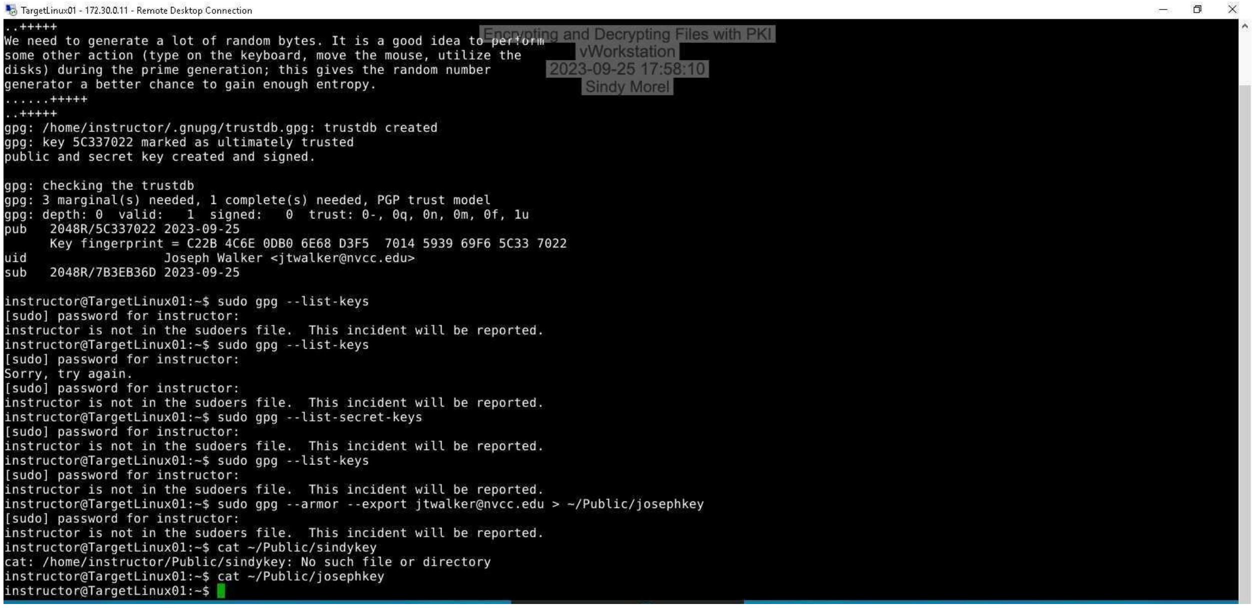


```
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Joseph Walker
Email address: jtwalker@nvcc.edu
Comment:
You selected this USER-ID:
    "Joseph Walker <jtwalker@nvcc.edu>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++
..+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
......+++++
..+++++
gpg: /home/instructor/.gnupg/trustdb.gpg: trustdb created
gpg: key 5C337022 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
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/5C337022 2023-09-25
      Key fingerprint = C22B 4C6E 0DB0 6E68 D3F5  7014 5939 69F6 5C33 7022
```



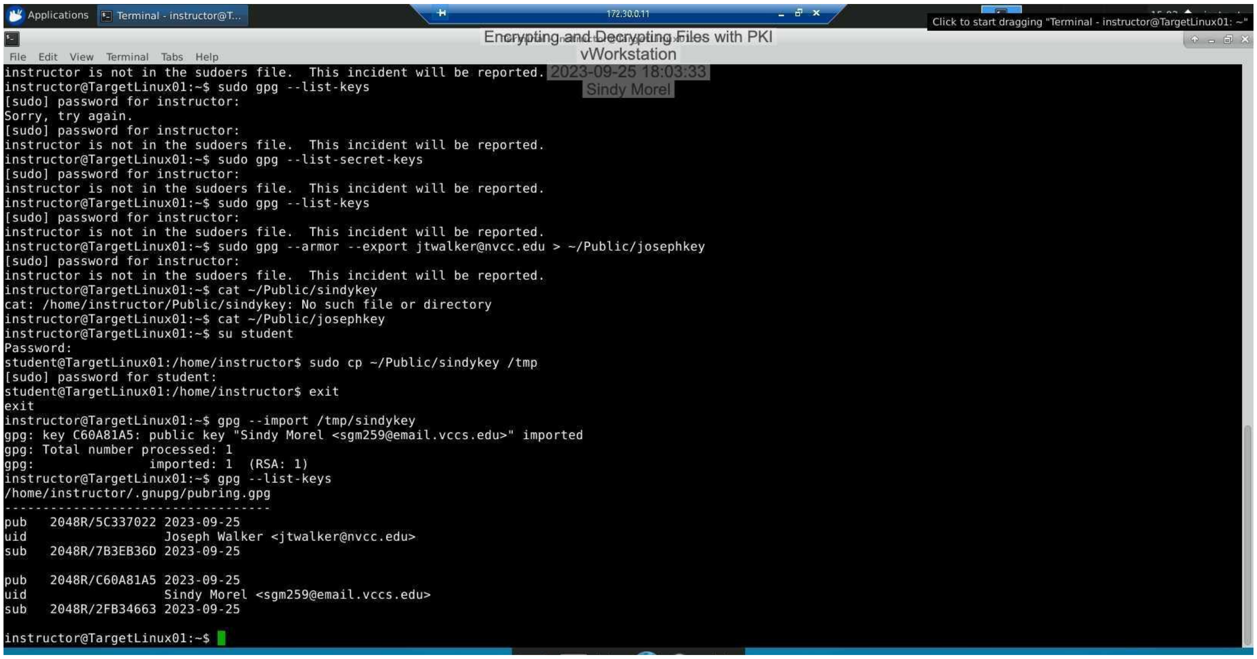
```
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++
..+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
......+++++
..+++++
gpg: /home/instructor/.gnupg/trustdb.gpg: trustdb created
gpg: key 5C337022 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
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/5C337022 2023-09-25
      Key fingerprint = C22B 4C6E 0DB0 6E68 D3F5  7014 5939 69F6 5C33 7022
uid                  Joseph Walker <jtwalker@nvcc.edu>
sub   2048R/7B3EB36D 2023-09-25

instructor@TargetLinux01:~$ sudo gpg --list-keys
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-keys
[sudo] password for instructor:
Sorry, try again.
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-secret-keys
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-keys
[sudo] password for instructor:
```

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


TargetLinux01 - 172.30.0.11 - Remote Desktop Connection
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-25 17:58:10
Sindy Morel

```
..+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
......+++++
..+++++
gpg: /home/instructor/.gnupg/trustdb.gpg: trustdb created
gpg: key 5C337022 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
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/5C337022 2023-09-25
      Key fingerprint = C22B 4C6E 0DB0 6E68 D3F5  7014 5939 69F6 5C33 7022
uid                  Joseph Walker <jtwalker@nvcc.edu>
sub   2048R/7B3EB36D 2023-09-25

instructor@TargetLinux01:~$ sudo gpg --list-keys
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-keys
[sudo] password for instructor:
Sorry, try again.
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-secret-keys
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-keys
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --armor --export jtwalker@nvcc.edu > ~/Public/josephkey
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ cat ~/Public/sindykey
cat: /home/instructor/Public/sindykey: No such file or directory
instructor@TargetLinux01:~$ cat ~/Public/josephkey
instructor@TargetLinux01:~$ 
```

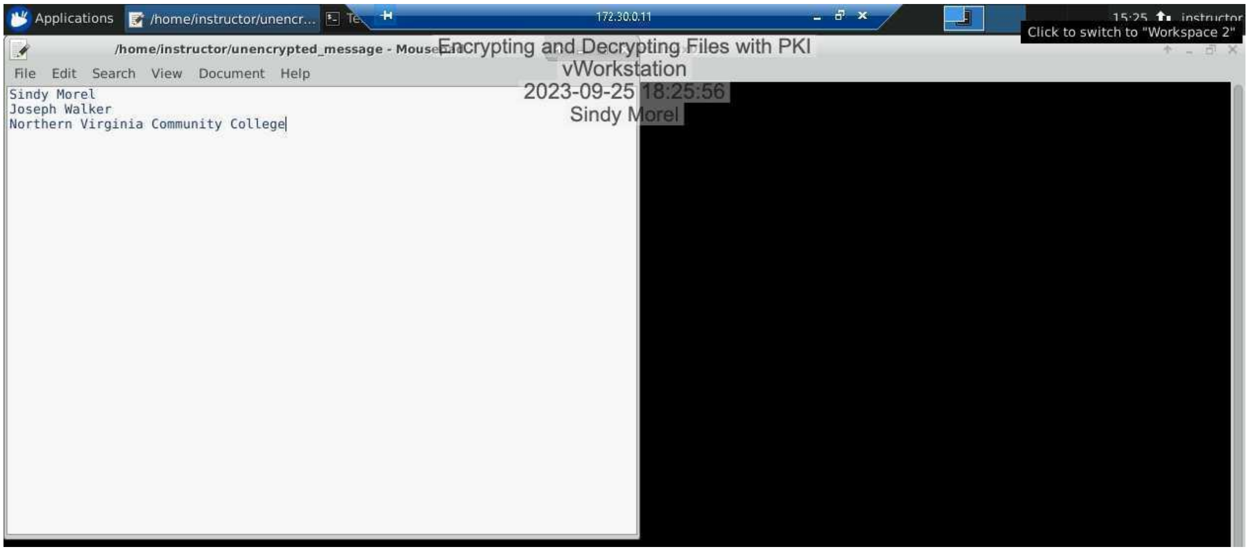
Student & Instructor Keys


Applications
Terminal - instructor@T...
172.30.0.11
Click to start dragging "Terminal - instructor@TargetLinux01: ~"
File
Edit
View
Terminal
Tabs
Help
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-25 18:03:33
Sindy Morel

```
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-keys
[sudo] password for instructor:
Sorry, try again.
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-secret-keys
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --list-keys
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ sudo gpg --armor --export jtwalker@nvcc.edu > ~/Public/josephkey
[sudo] password for instructor:
instructor is not in the sudoers file.  This incident will be reported.
instructor@TargetLinux01:~$ cat ~/Public/sindykey
cat: /home/instructor/Public/sindykey: No such file or directory
instructor@TargetLinux01:~$ cat ~/Public/josephkey
instructor@TargetLinux01:~$ su student
Password:
student@TargetLinux01:/home/instructor$ sudo cp ~/Public/sindykey /tmp
[sudo] password for student:
student@TargetLinux01:/home/instructor$ exit
exit
instructor@TargetLinux01:~$ gpg --import /tmp/sindykey
gpg: key C60A81A5: public key "Sindy Morel <sgm259@email.vccs.edu>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
instructor@TargetLinux01:~$ gpg --list-keys
/home/instructor/.gnupg/pubring.gpg
-----------------------------------
pub   2048R/5C337022 2023-09-25
uid                  Joseph Walker <jtwalker@nvcc.edu>
sub   2048R/7B3EB36D 2023-09-25

pub   2048R/C60A81A5 2023-09-25
uid                  Sindy Morel <sgm259@email.vccs.edu>
sub   2048R/2FB34663 2023-09-25

instructor@TargetLinux01:~$ 
```

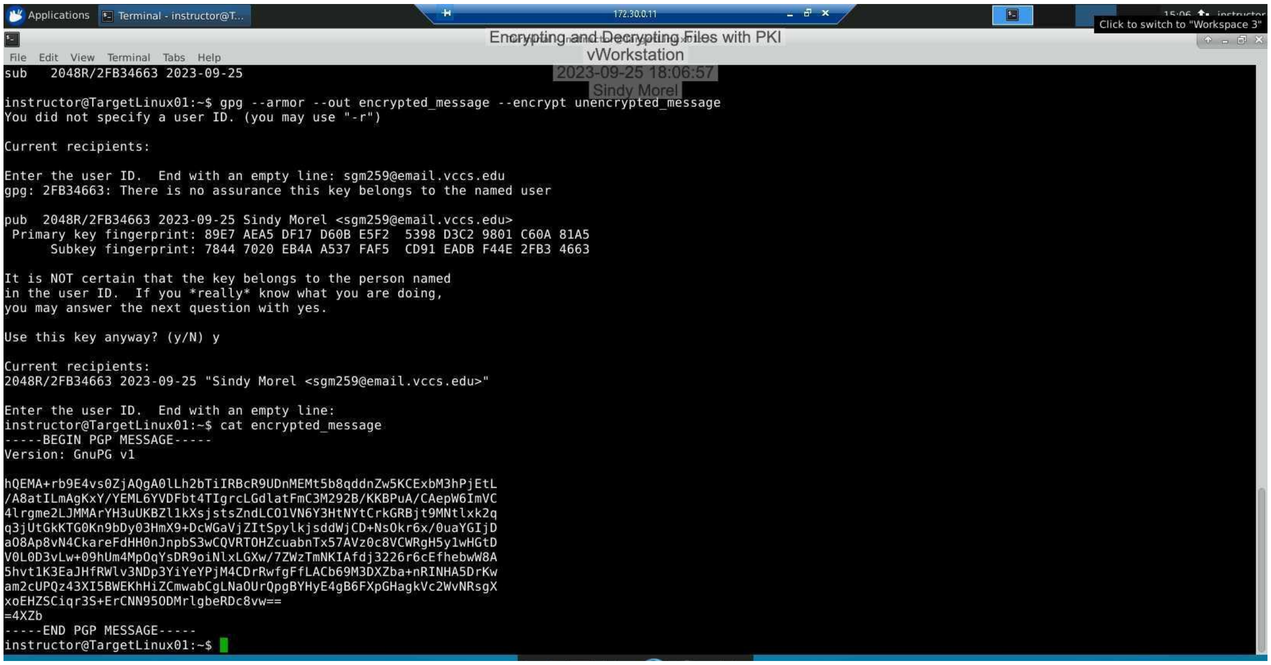
Sindy Morel	JBL LAB8: Encrypting and Decrypting Files with PKI	September 23, 2023

Unencrypted Text


Applications
/home/instructor/unencr...
172.30.0.11
15:25 instructor
Click to switch to "Workspace 2"
/home/instructor/unencrypted_message - Mouse
File Edit Search View Document Help
Encrypting and Decrypting Files with PKI
vWorkstation
2023-09-25 18:25:56
Sindy Morel

```
Sindy Morel
Joseph Walker
Northern Virginia Community College
```

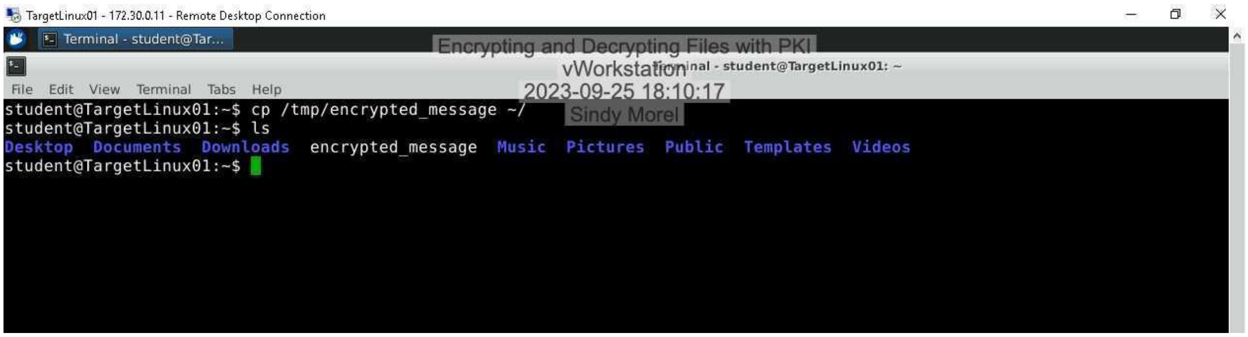
Encrypted Message


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
2023-09-25 18:06:57
Sindy Morel

```
sub   2048R/2FB34663 2023-09-25

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: sgm259@email.vccs.edu
gpg: 2FB34663: There is no assurance this key belongs to the named user

pub  2048R/2FB34663 2023-09-25 Sindy Morel <sgm259@email.vccs.edu>
 Primary key fingerprint: 89E7 AEA5 DF17 D60B E5F2  5398 D3C2 9801 C60A 81A5
      Subkey fingerprint: 7844 7020 EB4A A537 FAF5  CD91 EADB F44E 2FB3 4663

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/2FB34663 2023-09-25 "Sindy Morel <sgm259@email.vccs.edu>"

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

hQEMA+rb9E4vs0ZjAQgA0lLh2bTiIRBcR9UDnMEMt5b8qddnZw5KCExbM3hPjEtL
/A8atILmAgKxY/YEML6YVDFbt4TIgrcLGdlatFmC3M292B/KKBPuA/CAepW6ImVC
4lrgme2LJMMArYH3uUKBZl1kXsjstsZndLCO1VN6Y3HtNYtCrkGRBjt9MNtlxk2q
q3jUtGkKTG0Kn9bDy03HmX9+DcWGaVjZItSpylkjsddWjCD+NsOkr6x/0uaYGIjD
aO8Ap8vN4CkareFdHH0nJnpbS3wCQVRTOHZcuabnTx57AVz0c8VCWRgH5y1wHGtD
V0L0D3vLw+09hUm4MpOqYsDR9oiNlxLGXw/7ZWzTmNKIAfdj3226r6cEfhebwW8A
5hvt1K3EaJHfRWlv3NDp3YiYeYPjM4CDrRwfgFfLACb69M3DXZba+nRINHA5DrKw
am2cUPQz43XI5BWEKhHiZCmwabCgLNaOUrQpgBYHyE4gB6FXpGHagkVc2WvNRsgX
xoEHZSCiqr3S+ErCNN95ODMrlgbeRDc8vw==
=4XZb
-----END PGP MESSAGE-----
instructor@TargetLinux01:~$
```

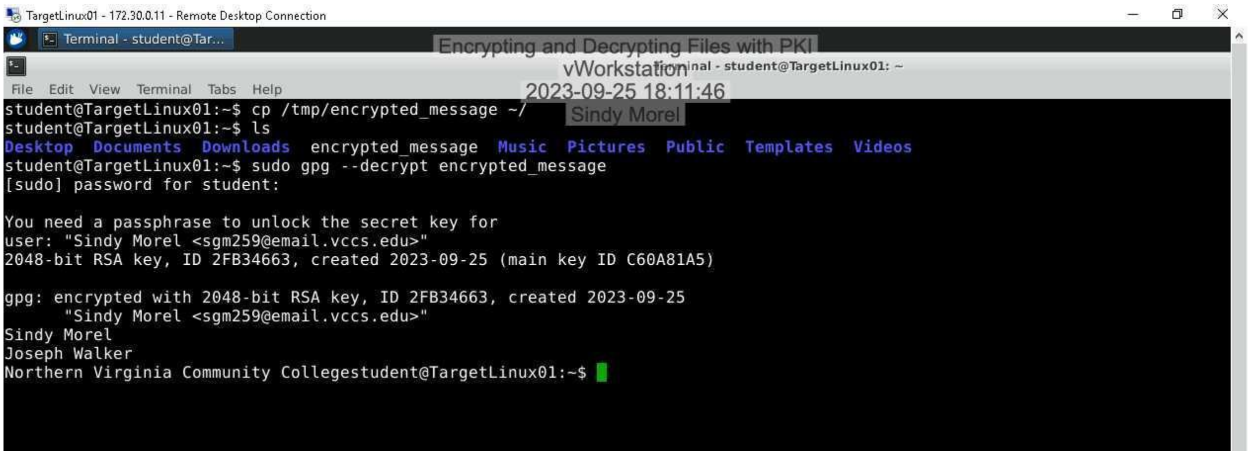
Sindy Morel	JBL LAB8: Encrypting and Decrypting Files with PKI	September 23, 2023

Listed file in directory


TargetLinux01 - 172.30.0.11 - Remote Desktop Connection
Terminal - student@Tar...
Encrypting and Decrypting Files with PKI
vWorkstation
Terminal - student@TargetLinux01: ~
2023-09-25 18:10:17
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:~$ 
```

Unencrypted Message


TargetLinux01 - 172.30.0.11 - Remote Desktop Connection
Terminal - student@Tar...
Encrypting and Decrypting Files with PKI
vWorkstation
Terminal - student@TargetLinux01: ~
2023-09-25 18:11:46
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: "Sindy Morel <sgm259@email.vccs.edu>"
2048-bit RSA key, ID 2FB34663, created 2023-09-25 (main key ID C60A81A5)

gpg: encrypted with 2048-bit RSA key, ID 2FB34663, created 2023-09-25
      "Sindy Morel <sgm259@email.vccs.edu>"
Sindy Morel
Joseph Walker
Northern Virginia Community Collegestudent@TargetLinux01:~$ 
```