Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

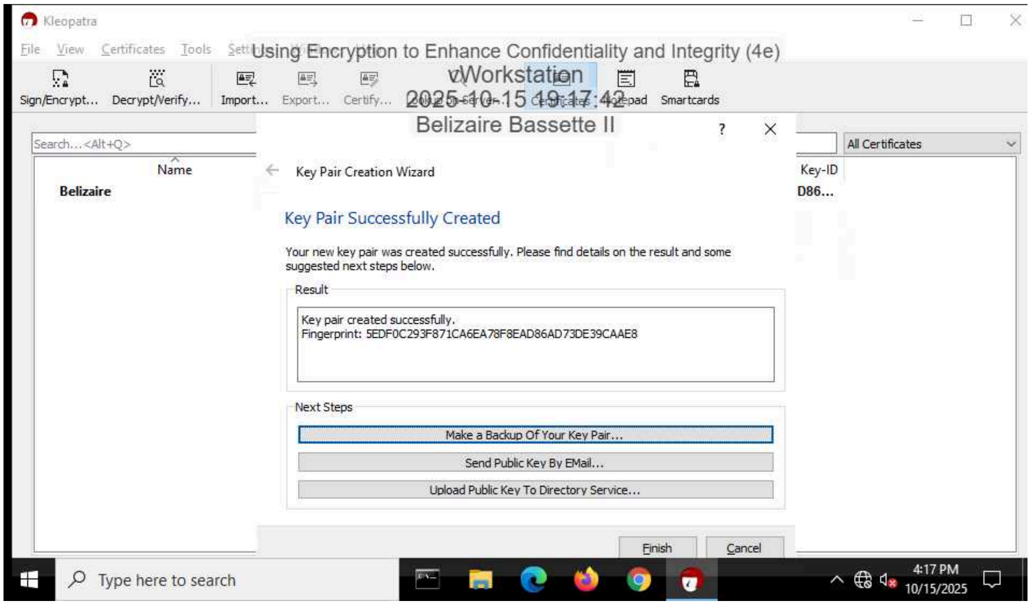
Student: Belizaire Bassette II	Email: bebasset@syr.edu
Time on Task: 25 hours, 14 minutes	Progress: 100%

Report Generated: Thursday, October 16, 2025 at 8:34 PM

Section 1: Hands-On Demonstration

Part 1: Create and Exchange Asymmetric Encryption Keys

9. **Make a screen capture** showing the **fingerprint for your key pair.**


Kleopatra
File View Certificates Tools Setti
Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2025-10-15 19:17:42
Belizaire Bassette II
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Smartcards
Search...<Alt+Q>
All Certificates
Name
Belizaire
Key-ID
D86...
Key Pair Creation Wizard

Key Pair Successfully Created

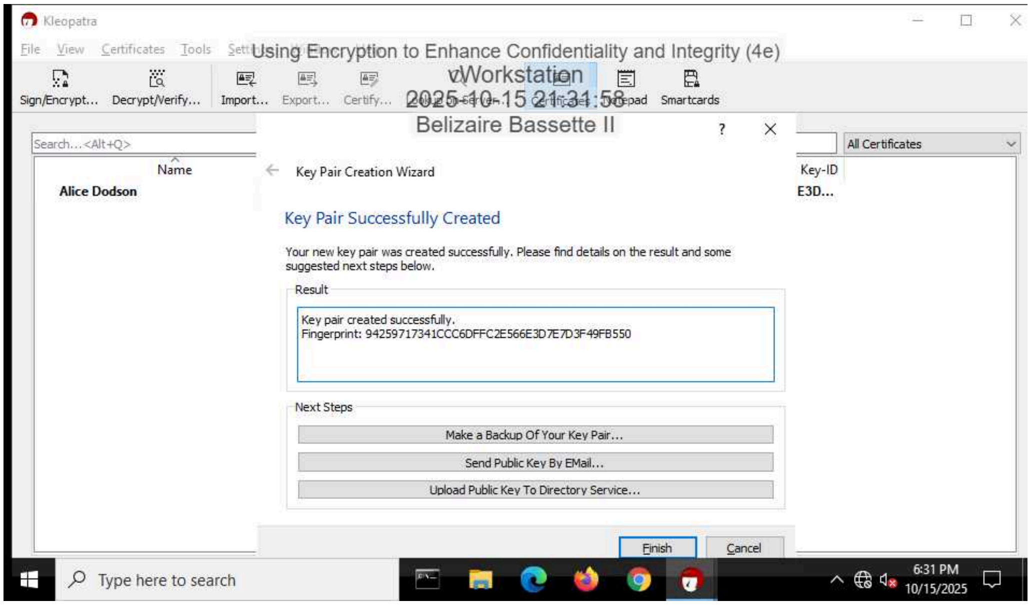
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result

```
Key pair created successfully.
Fingerprint: 5EDF0C293F871CA6EA78F8EAD86AD73DE39CAAE8
```

Next Steps
Make a Backup Of Your Key Pair...
Send Public Key By EMail...
Upload Public Key To Directory Service...
Finish
Cancel
Type here to search
4:17 PM
10/15/2025

22. **Make a screen capture** showing the **fingerprint for Alice's key pair**.



Key Pair Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result

Key pair created successfully.
Fingerprint: 94259717341CCC6DFFC2E566E3D7E7D3F49FB550

Next Steps

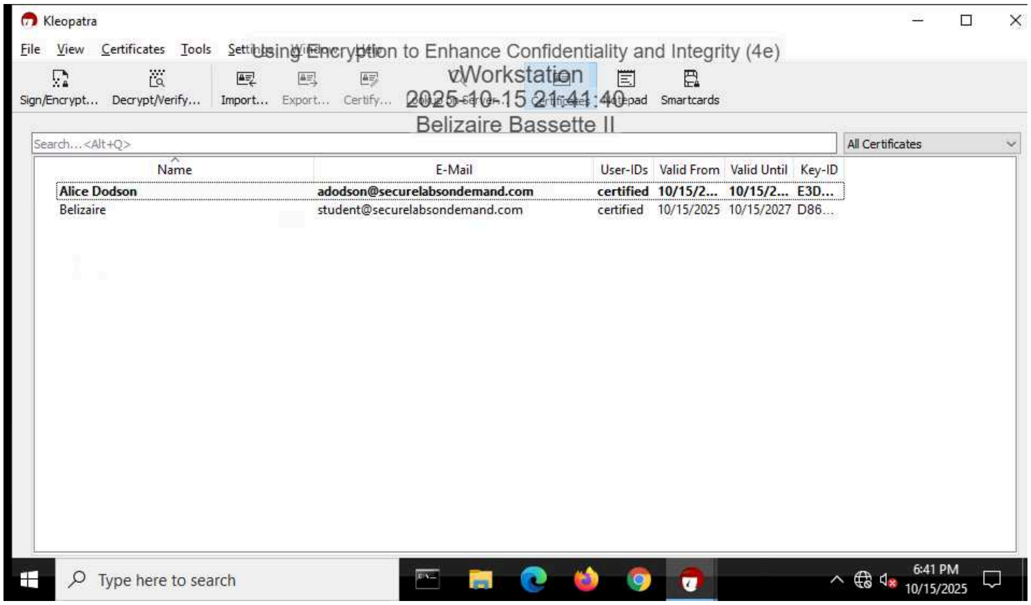
Make a Backup Of Your Key Pair...

Send Public Key By EMail...

Upload Public Key To Directory Service...

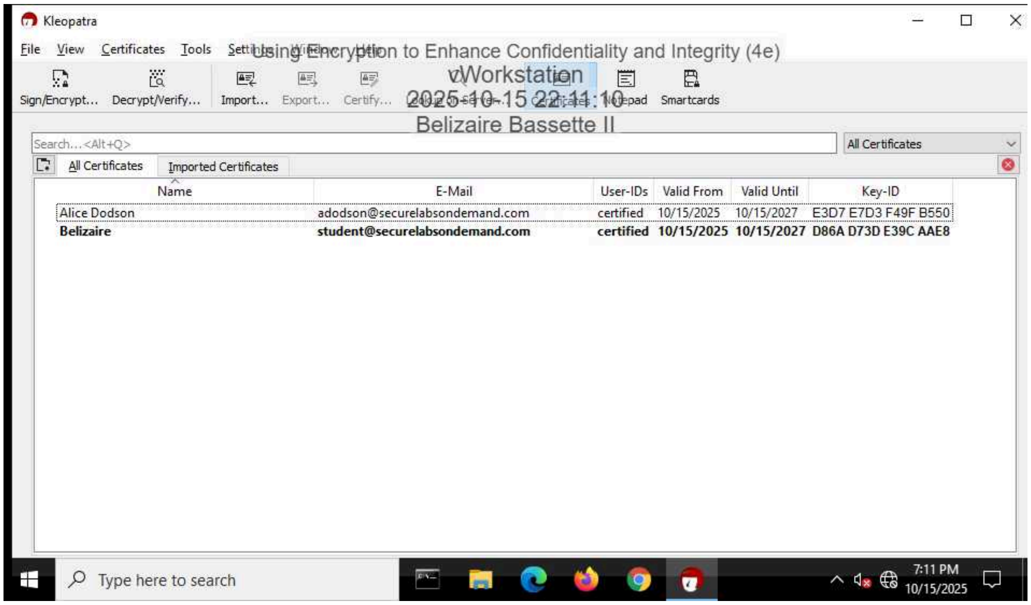
Finish Cancel

30. **Make a screen capture** showing **your public key in Alice's certificate cache**.



Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Alice Dodson	**adodson@securelabsondemand.com**	**certified**	**10/15/2...**	**10/15/2...**	**E3D...**
Belizaire	student@securelabsondemand.com	certified	10/15/2025	10/15/2027	D86...

35. **Make a screen capture** showing **Alice's public key in your certificate cache**.



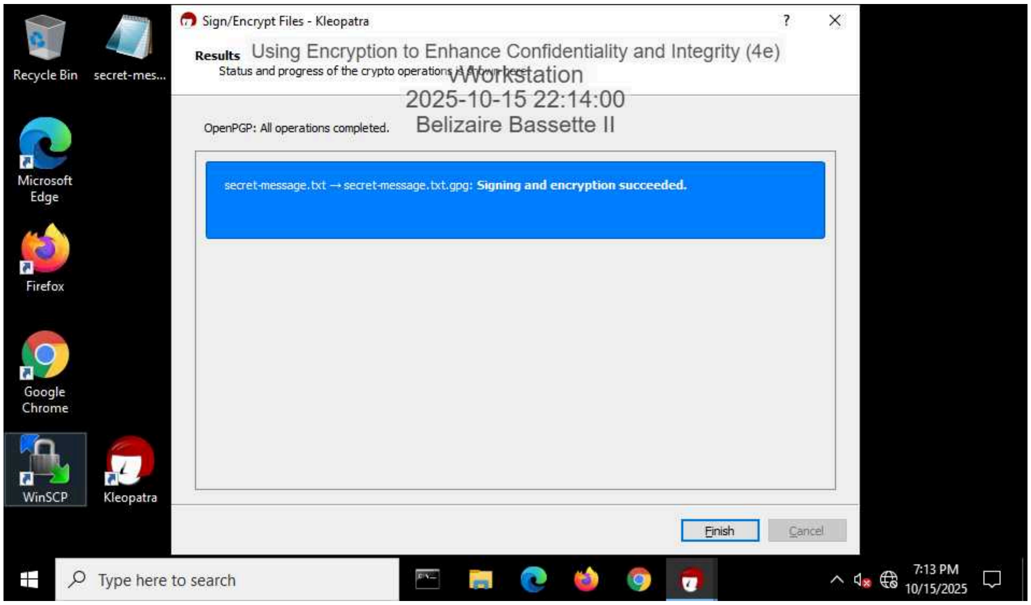
Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2025-10-15 22:11:10
Belizaire Bassette II

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Alice Dodson	adodson@securelabsondemand.com	certified	10/15/2025	10/15/2027	E3D7 E7D3 F49F B550
Belizaire	**student@securelabsondemand.com**	**certified**	**10/15/2025**	**10/15/2027**	**D86A D73D E39C AAE8**

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Search...<Alt+Q>
All Certificates
All Certificates
Imported Certificates
Type here to search
7:11 PM
10/15/2025

Part 2: Encrypt a File Using Asymmetric Encryption

9. **Make a screen capture** showing the **successful signing and encryption message**.



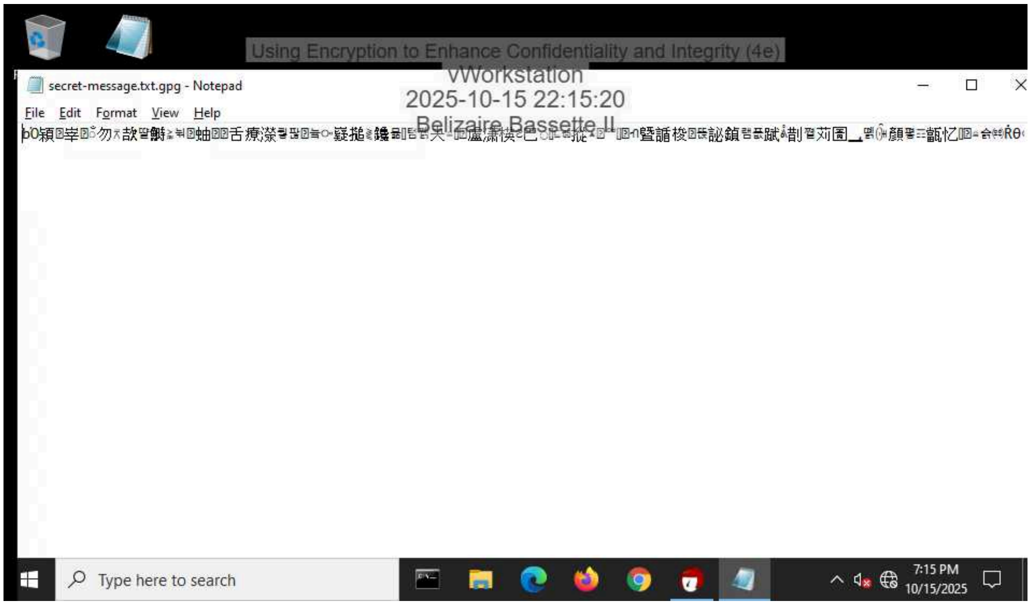
Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2025-10-15 22:14:00
Belizaire Bassette II

Results
Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

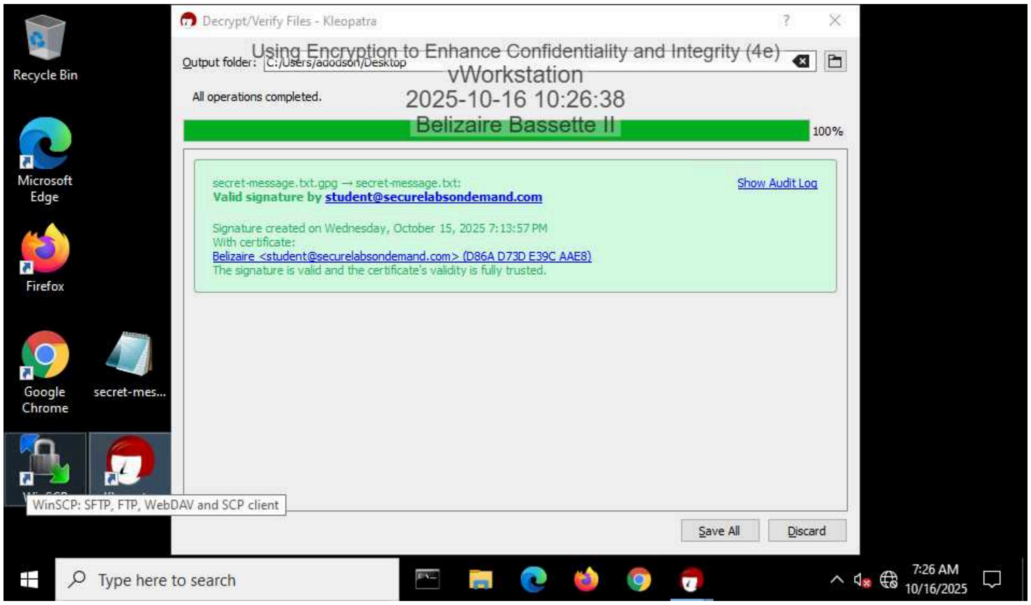
secret-message.txt → secret-message.txt.gpg: **Signing and encryption succeeded.**

12. **Make a screen capture** showing the **ciphertext**.



Part 3: Decrypt a File Using Asymmetric Encryption

15. **Make a screen capture** showing the **Decrypt/Verify Files window**.



Output folder: C:/Users/adodson/Desktop

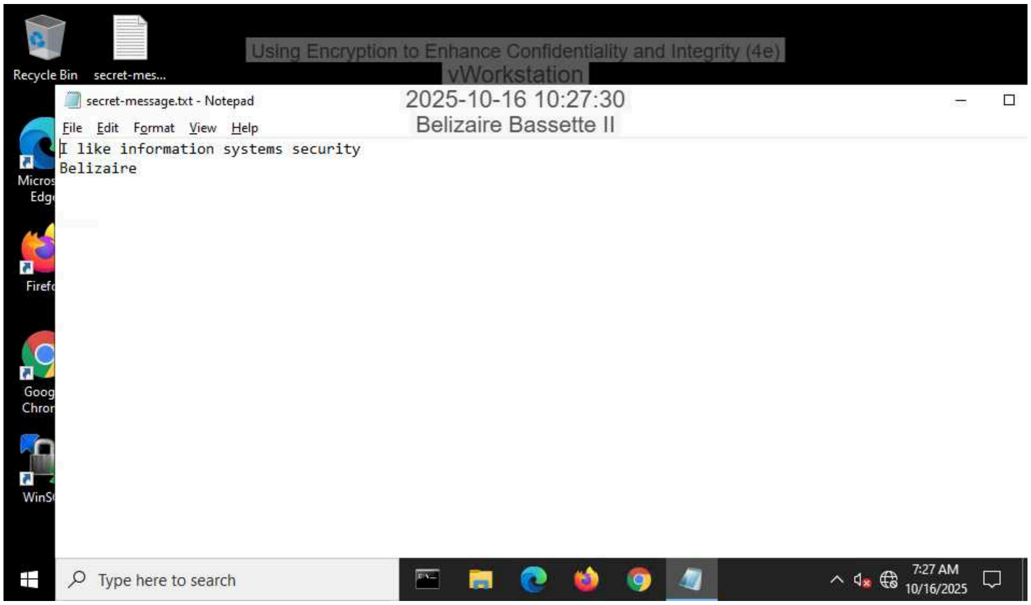
All operations completed.

100%

secret-message.txt.gpg → secret-message.txt:
Valid signature by student@securelabsondemand.com

Signature created on Wednesday, October 15, 2025 7:13:57 PM
With certificate:
Belizaire <student@securelabsondemand.com> (D86A D73D E39C AAE8)
The signature is valid and the certificate's validity is fully trusted.

18. **Make a screen capture** showing the **decrypted secret-message.txt file in Notepad**.



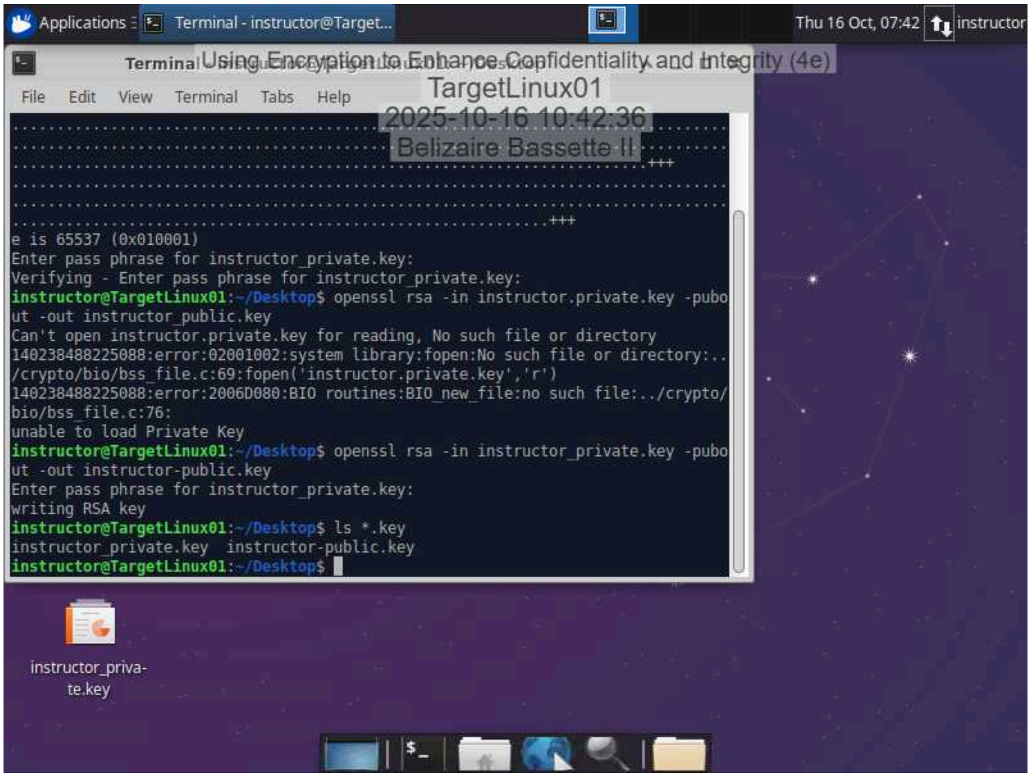
Recycle Bin
secret-mes...
Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
secret-message.txt - Notepad
2025-10-16 10:27:30
Belizaire Bassette II
File Edit Format View Help
Type here to search
7:27 AM
10/16/2025

```
I like information systems security
Belizaire
```

Section 2: Applied Learning

Part 1: Create an Asymmetric Key Pair

10. **Make a screen capture** showing the **instructor's key pair files**.



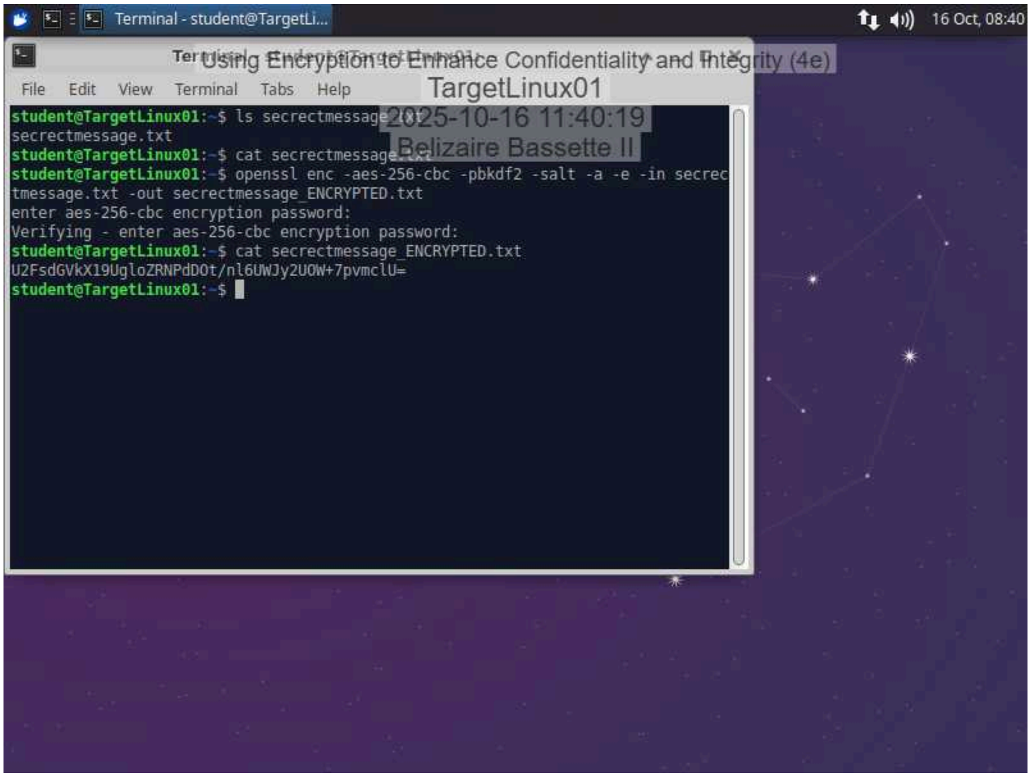
```
.........................................................................
.........................................................................
.................................................................+++
.........................................................................
.........................................................................
.......................................................+++
e is 65537 (0x010001)
Enter pass phrase for instructor_private.key:
Verifying - Enter pass phrase for instructor_private.key:
instructor@TargetLinux01:~/Desktop$ openssl rsa -in instructor.private.key -pubo
ut -out instructor_public.key
Can't open instructor.private.key for reading, No such file or directory
140238488225088:error:02001002:system library:fopen:No such file or directory:..
/crypto/bio/bss_file.c:69:fopen('instructor.private.key','r')
140238488225088:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/
bio/bss_file.c:76:
unable to load Private Key
instructor@TargetLinux01:~/Desktop$ openssl rsa -in instructor_private.key -pubo
ut -out instructor-public.key
Enter pass phrase for instructor_private.key:
writing RSA key
instructor@TargetLinux01:~/Desktop$ ls *.key
instructor_private.key  instructor-public.key
instructor@TargetLinux01:~/Desktop$ 
```

Part 2: Encrypt a File Using Symmetric Encryption

11. **Document** the password you used to symmetrically encrypt the file.

yourownpassword

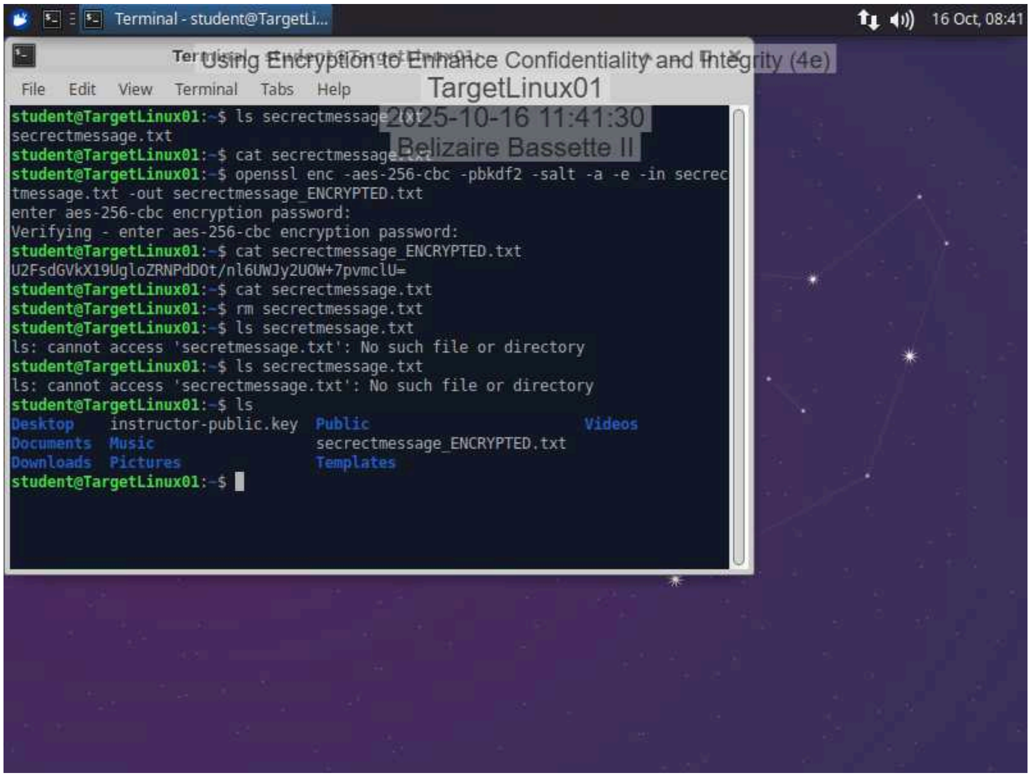
13. **Make a screen capture** showing the **ciphertext in the secretmessage_ENCRYPTED.txt file**.



Terminal - student@TargetLi...
16 Oct, 08:40
File Edit View Terminal Tabs Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2025-10-16 11:40:19
Belizaire Bassette II

```
student@TargetLinux01:~$ ls secrectmessage.txt
secrectmessage.txt
student@TargetLinux01:~$ cat secrectmessage.txt
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secrec
tmessage.txt -out secrectmessage_ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat secrectmessage_ENCRYPTED.txt
U2FsdGVkX19UgloZRNPdDOt/nl6UWJy2UOW+7pvmclU=
student@TargetLinux01:~$
```

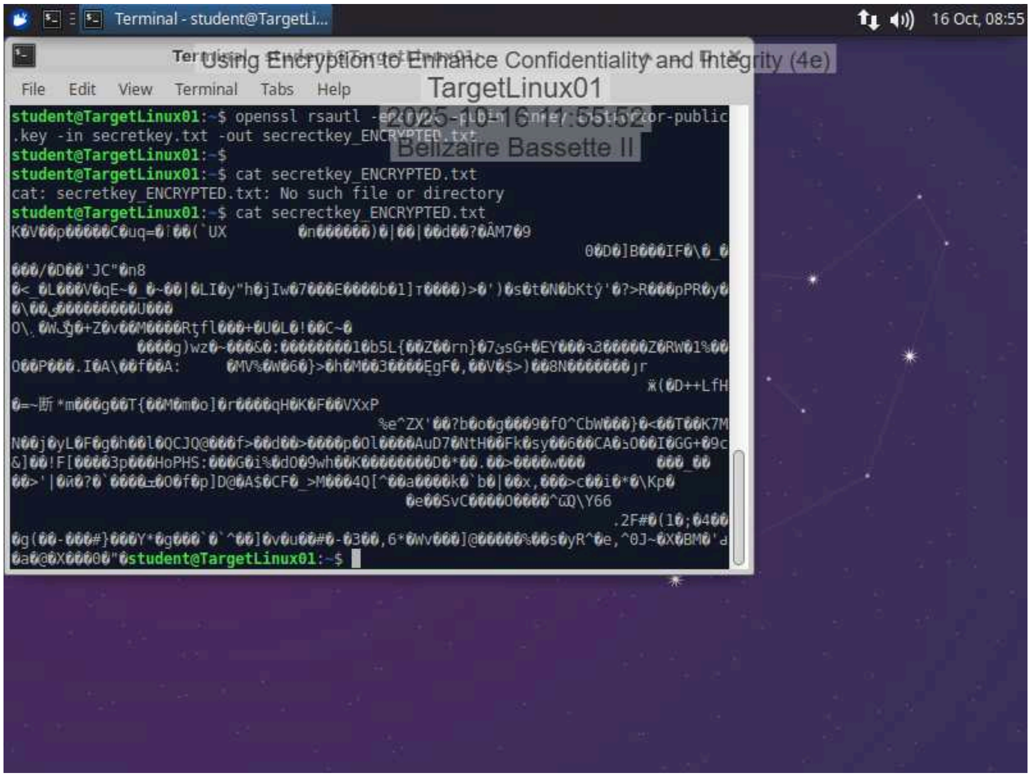
16. **Make a screen capture** showing the **output of the ls command**.


Terminal - student@TargetLi...
16 Oct, 08:41
Terminal - student@TargetLinux01
File
Edit
View
Terminal
Tabs
Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2025-10-16 11:41:30
Belizaire Bassette II

```
student@TargetLinux01:~$ ls secrectmessage.txt
secrectmessage.txt
student@TargetLinux01:~$ cat secrectmessage.txt
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secrec
tmessage.txt -out secrectmessage_ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat secrectmessage_ENCRYPTED.txt
U2FsdGVkX19UgloZRNPdDOt/nl6UWJy2UOW+7pvmclU=
student@TargetLinux01:~$ cat secrectmessage.txt
student@TargetLinux01:~$ rm secrectmessage.txt
student@TargetLinux01:~$ ls secretmessage.txt
ls: cannot access 'secretmessage.txt': No such file or directory
student@TargetLinux01:~$ ls secrectmessage.txt
ls: cannot access 'secrectmessage.txt': No such file or directory
student@TargetLinux01:~$ ls
Desktop    instructor-public.key  Public                        Videos
Documents  Music                  secrectmessage_ENCRYPTED.txt
Downloads  Pictures               Templates
student@TargetLinux01:~$ 
```

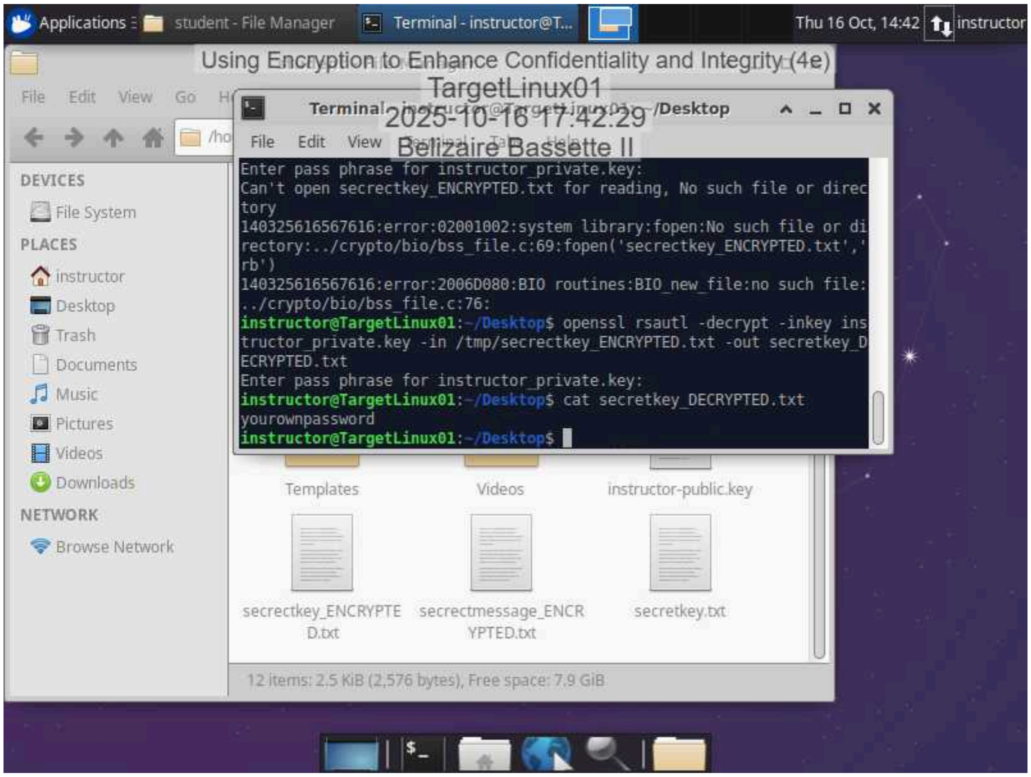
Part 3: Transfer and Decrypt a File Using Hybrid Cryptography

6. **Make a screen capture** showing the **encrypted contents of the secretkey_ENCRYPTED.txt file**.


Terminal - student@TargetLi...
16 Oct, 08:55
Terminal - student@TargetLinux01
File
Edit
View
Terminal
Tabs
Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2025-10-16 11:55:52
Belizaire Bassette II

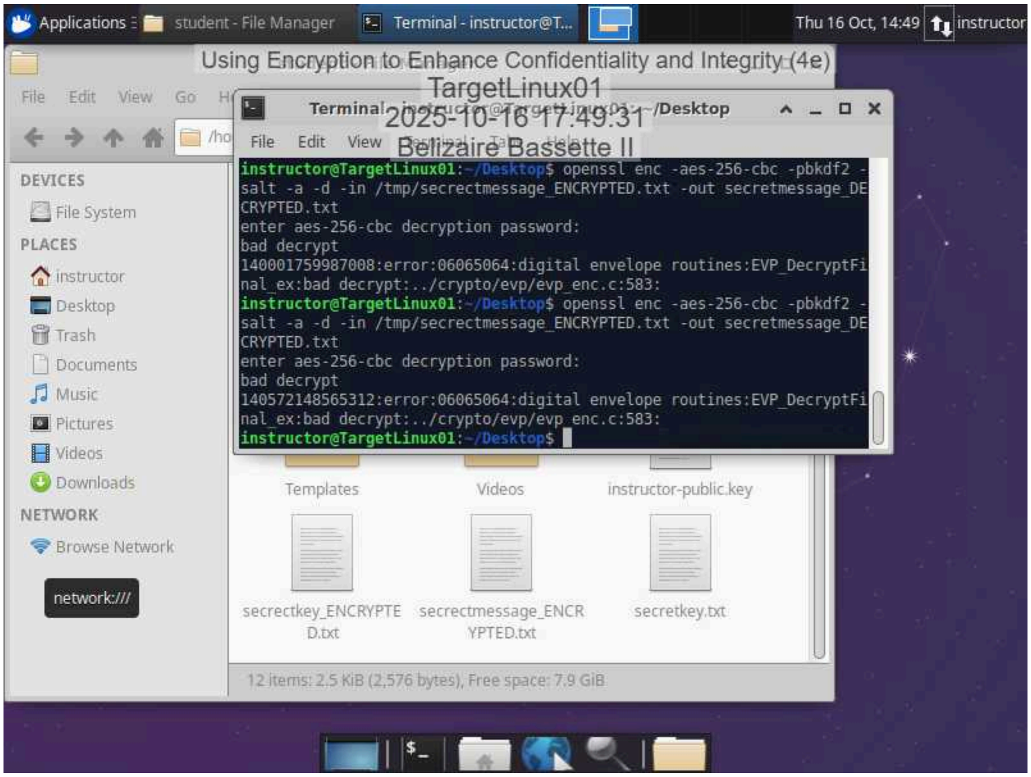
```
student@TargetLinux01:~$ openssl rsautl -encrypt -pubin -inkey ~/instructor-public
.key -in secretkey.txt -out secrectkey_ENCRYPTED.txt
student@TargetLinux01:~$
student@TargetLinux01:~$ cat secretkey_ENCRYPTED.txt
cat: secretkey_ENCRYPTED.txt: No such file or directory
student@TargetLinux01:~$ cat secrectkey_ENCRYPTED.txt
K�V��p�����C�uq=�!��(`UX        �n������)�|��|��d��?�ÂM7�9
                                                         0�D�]B���IF�\�_�
���/�D��'JC"�n8
�<_�L���V�qE~�_�~��|�LI�y"h�jIw�7���E����b�1]т����)>�')�s�t�N�bKtў'�?>R���pPR�y�
�\��ي���������U���
O\. �WJ̌g�+Z�v��M����Rţfl���+�U�L�!��C~�
                �����g)wz�~���&�:���������1�b5L{��Z��rn}�7ڏsG+�EY���ߒ3�����Z�RW�1%��
O��P���.I�A\��f��A:     �MV%�W�6�}>�h�M��3����ĘgF�,��V�$>)��8N�������յr
                                                                   ж(�D++LfH
�=~断*m���g��T{��M�m�o]�r����qH�K�F��VXxP
                                              %e^ZX'��?b�o�g����9�f0^CbW���}�<��T��K7M
N��j�yL�F�g�h��l�QCJQ@���f>��d��>����p�Ol����AuD7�NtH��Fk�sy��6��CA�ѕO��I�GG+�9c
&]��!F[����3p���HoPHS:���G�i%�dO�9wh��K���������D�*��.��>����w���       ���_��
��>'|�й�?�`����ـ�O�f�p]D@�A$�CF�_>M����4Q[^��a����k�`b�|��x,���>c��i�*�\Kp�
                                                      �e��SvC�����O����^ǖQ\Y66
                                                                      .2F#�(1�;�4��
�g(��-���#}���Y*�g���`�`^��]�v�u��#�-�3��,6*�Wv���]@�����%��s�yR^�e,^0J~�X�BM�'a
�a�@�X����O�"�student@TargetLinux01:~$
```

17. **Make a screen capture** showing the **decrypted contents of the secretkey_DECRYPTED.txt file**.



```
Enter pass phrase for instructor_private.key:
Can't open secrectkey_ENCRYPTED.txt for reading, No such file or direc
tory
140325616567616:error:02001002:system library:fopen:No such file or di
rectory:../crypto/bio/bss_file.c:69:fopen('secrectkey_ENCRYPTED.txt','
rb')
140325616567616:error:2006D080:BIO routines:BIO_new_file:no such file:
../crypto/bio/bss_file.c:76:
instructor@TargetLinux01:~/Desktop$ openssl rsautl -decrypt -inkey ins
tructor_private.key -in /tmp/secrectkey_ENCRYPTED.txt -out secretkey_D
ECRYPTED.txt
Enter pass phrase for instructor_private.key:
instructor@TargetLinux01:~/Desktop$ cat secretkey_DECRYPTED.txt
yourownpassword
instructor@TargetLinux01:~/Desktop$
```

21. **Make a screen capture** showing the **contents of the secretmessage_DECRYPTED file.**

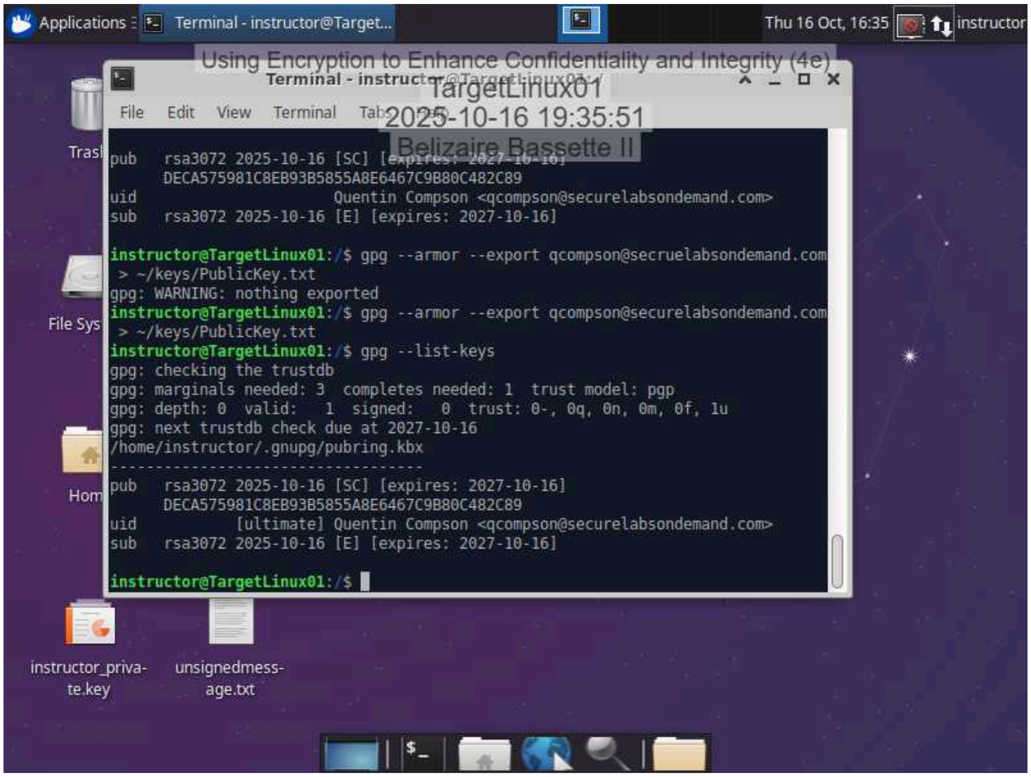


```
instructor@TargetLinux01:~/Desktop$ openssl enc -aes-256-cbc -pbkdf2 -
salt -a -d -in /tmp/secrectmessage_ENCRYPTED.txt -out secretmessage_DE
CRYPTED.txt
enter aes-256-cbc decryption password:
bad decrypt
140001759987008:error:06065064:digital envelope routines:EVP_DecryptFi
nal_ex:bad decrypt:../crypto/evp/evp_enc.c:583:
instructor@TargetLinux01:~/Desktop$ openssl enc -aes-256-cbc -pbkdf2 -
salt -a -d -in /tmp/secrectmessage_ENCRYPTED.txt -out secretmessage_DE
CRYPTED.txt
enter aes-256-cbc decryption password:
bad decrypt
140572148565312:error:06065064:digital envelope routines:EVP_DecryptFi
nal_ex:bad decrypt:../crypto/evp/evp_enc.c:583:
instructor@TargetLinux01:~/Desktop$
```

Section 3: Challenge and Analysis

Part 1: Digitally Sign a Document Using GPG

Make a screen capture showing the **key fingerprint for the key pair you generated in this part of the lab**.

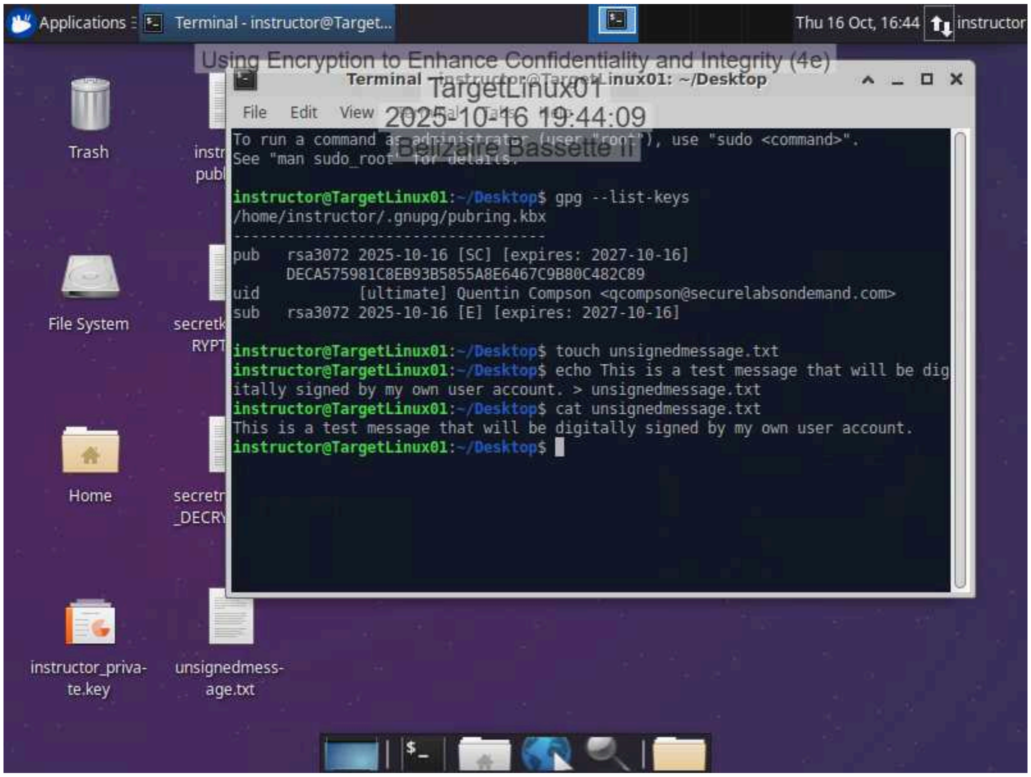


```
pub   rsa3072 2025-10-16 [SC] [expires: 2027-10-16]
      DECA575981C8EB93B5855A8E6467C9B80C482C89
uid                      Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2025-10-16 [E] [expires: 2027-10-16]

instructor@TargetLinux01:/$ gpg --armor --export qcompson@secruelabsondemand.com
 > ~/keys/PublicKey.txt
gpg: WARNING: nothing exported
instructor@TargetLinux01:/$ gpg --armor --export qcompson@securelabsondemand.com
 > ~/keys/PublicKey.txt
instructor@TargetLinux01:/$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2027-10-16
/home/instructor/.gnupg/pubring.kbx
-----------------------------------
pub   rsa3072 2025-10-16 [SC] [expires: 2027-10-16]
      DECA575981C8EB93B5855A8E6467C9B80C482C89
uid           [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2025-10-16 [E] [expires: 2027-10-16]

instructor@TargetLinux01:/$ 
```

Make a screen capture showing the **contents of the unsignedmessage.txt file**.



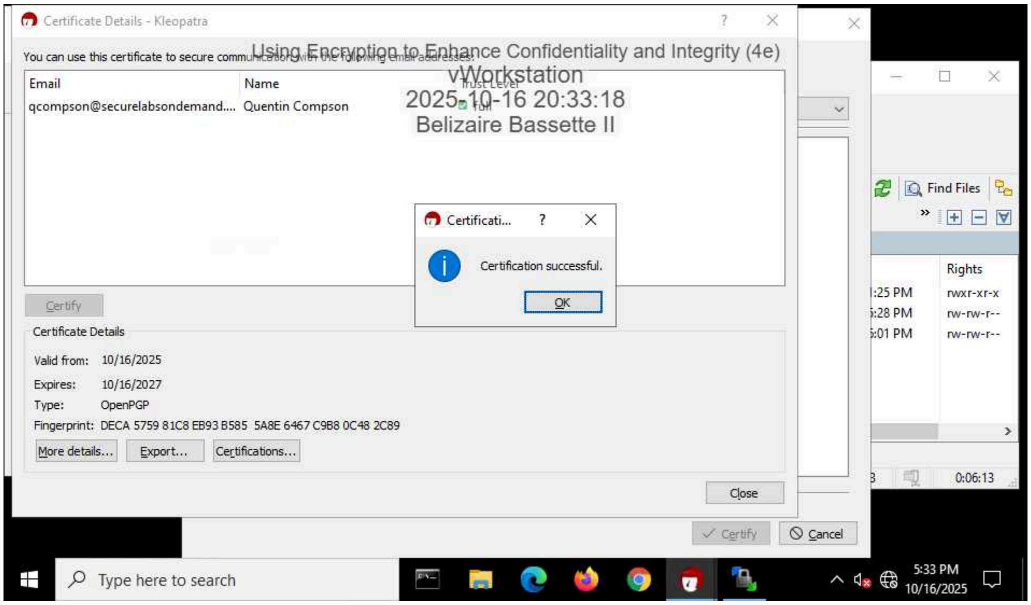
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

instructor@TargetLinux01:~/Desktop$ gpg --list-keys
/home/instructor/.gnupg/pubring.kbx
-----------------------------------
pub   rsa3072 2025-10-16 [SC] [expires: 2027-10-16]
      DECA575981C8EB93B5855A8E6467C9B80C482C89
uid           [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2025-10-16 [E] [expires: 2027-10-16]

instructor@TargetLinux01:~/Desktop$ touch unsignedmessage.txt
instructor@TargetLinux01:~/Desktop$ echo This is a test message that will be dig
itally signed by my own user account. > unsignedmessage.txt
instructor@TargetLinux01:~/Desktop$ cat unsignedmessage.txt
This is a test message that will be digitally signed by my own user account.
instructor@TargetLinux01:~/Desktop$
```

Part 2: Verify the Digital Signature Using Kleopatra

Make a screen capture showing the **successful signature verification on the signed message file.**



Certificate Details - Kleopatra

You can use this certificate to secure communications with the following email addresses:

Email	Name	Trust Level
qcompson@securelabsondemand....	Quentin Compson	Full

Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2025-10-16 20:33:18
Belizaire Bassette II

Certificati...

Certification successful.

Certificate Details

Valid from: 10/16/2025
Expires: 10/16/2027
Type: OpenPGP
Fingerprint: DECA 5759 81C8 EB93 B585 5A8E 6467 C9B8 0C48 2C89