Using Encryption to Enhance Data Confidentiality and Encryption

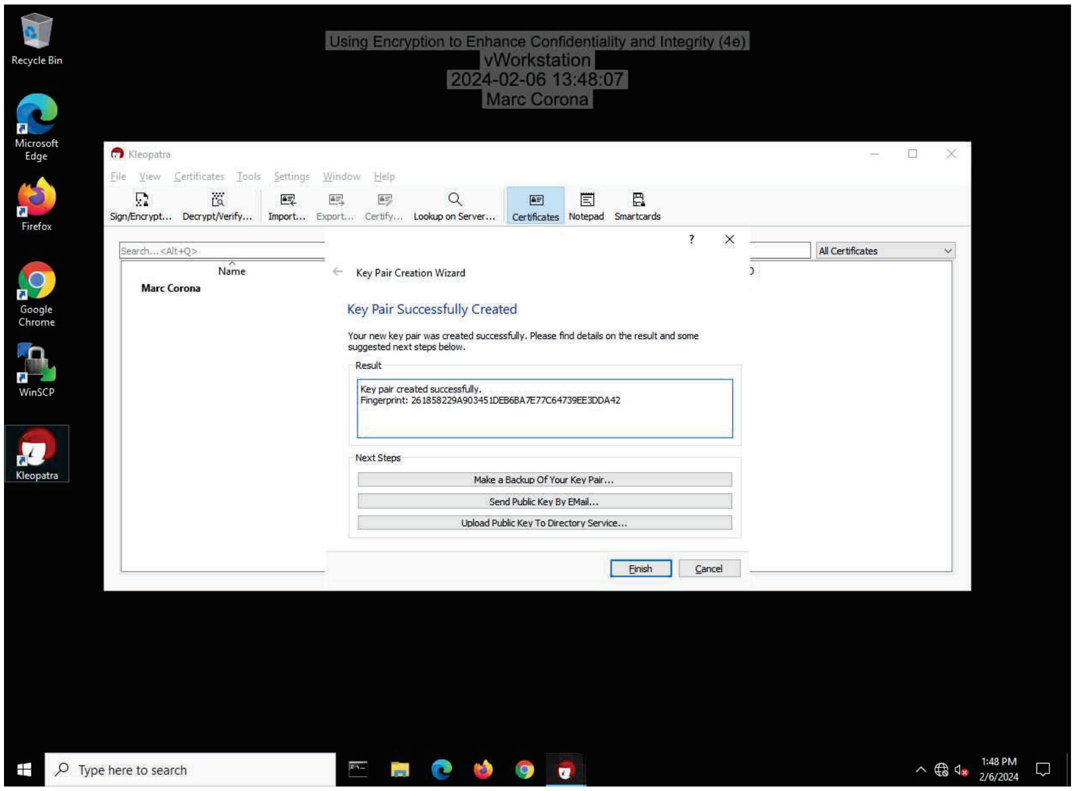
Student:

Marc Corona Mireles

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.**


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-06 13:48:07
Marc Corona
Kleopatra
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.

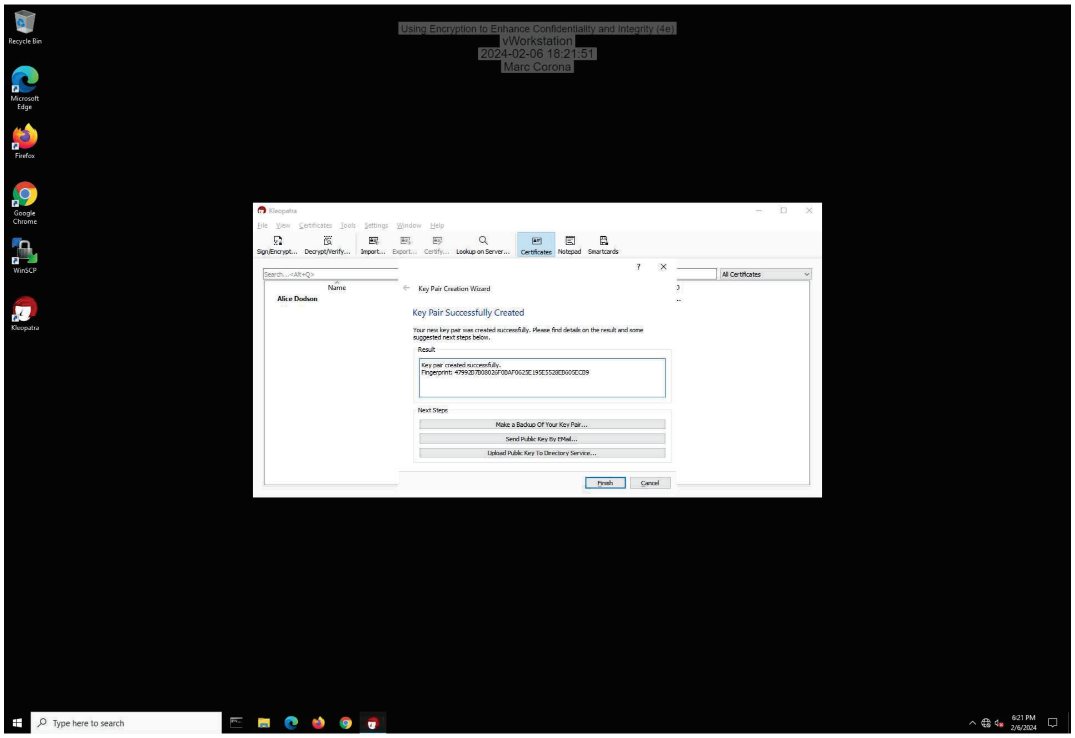
Result

```
Key pair created successfully.
Fingerprint: 261858229A903451DEB6BA7E77C64739EE3DDA42
```

Next Steps

Make a Backup Of Your Key Pair...
Send Public Key By EMail...
Upload Public Key To Directory Service...
Finish
Cancel

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


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-06 18:21:51
Marc Corona
Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Name
Alice Dodson
Key Pair Creation Wizard
Make a Backup Of Your Key Pair...
Send Public Key By EMail...
Upload Public Key To Directory Service...
Finish
Cancel

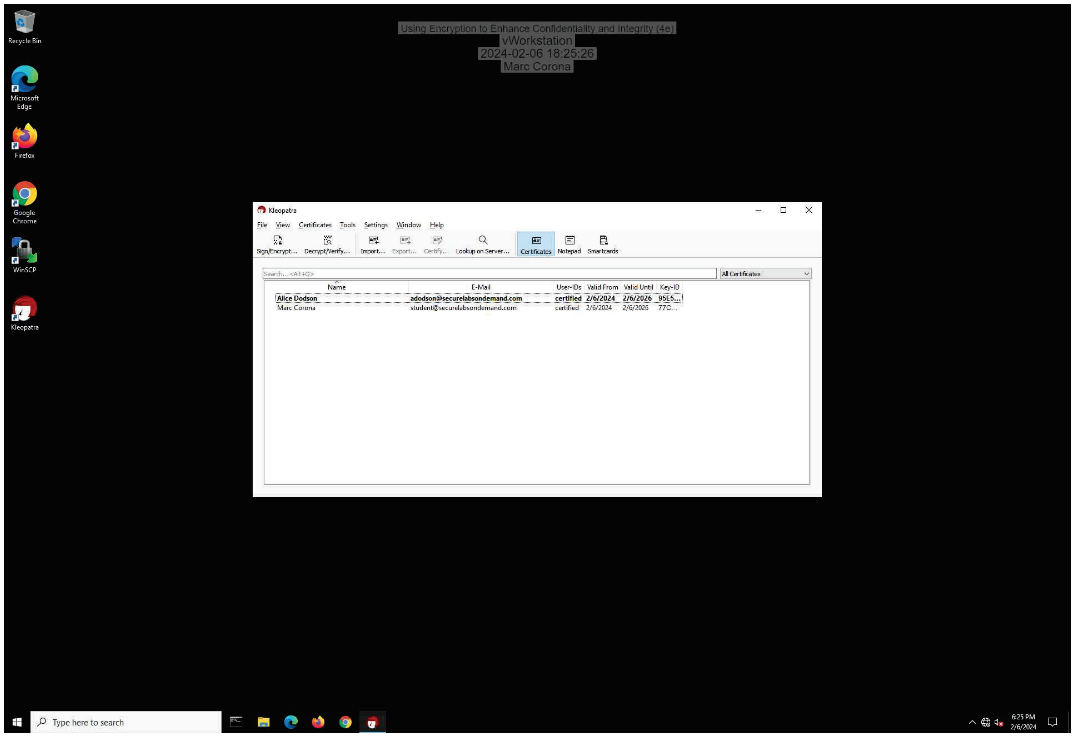
Key Pair Successfully Created

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

Result

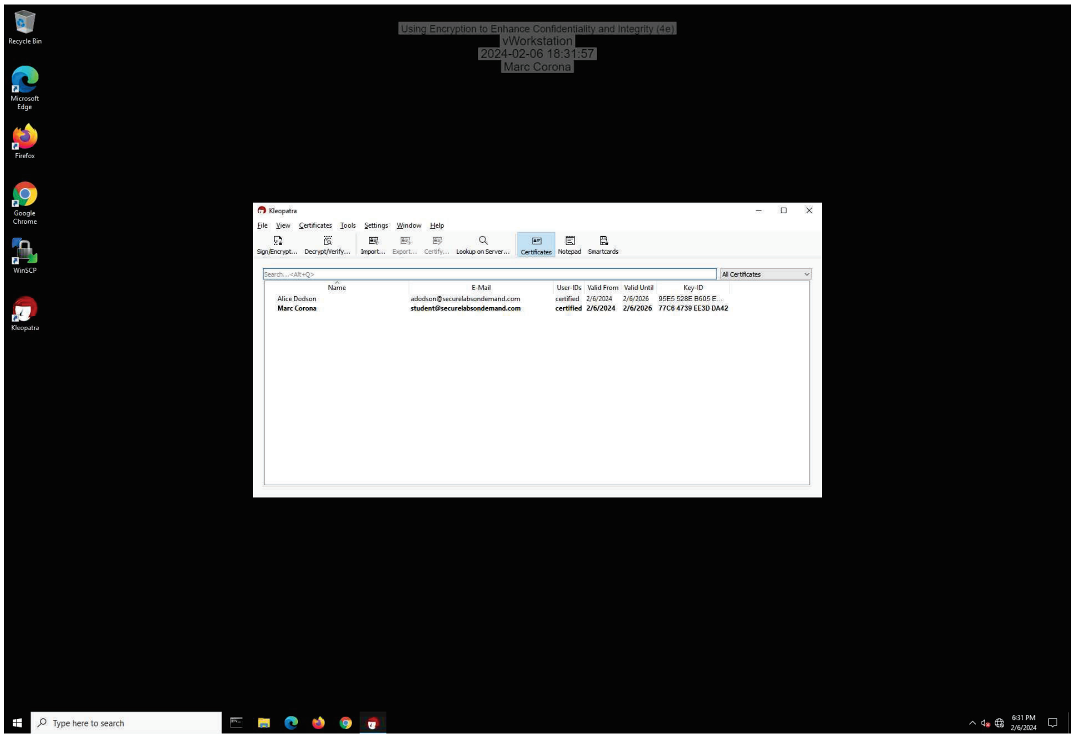
```
Key pair created successfully.
Fingerprint: 47992B7B08026F0BAF0625E195E5528EB605ECB9
```

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


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-06 18:25:26
Marc Corona
Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
All Certificates

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Alice Dodson	**adodson@securelabsondemand.com**	**certified**	**2/6/2024**	**2/6/2026**	**95E5...**
Marc Corona	student@securelabsondemand.com	certified	2/6/2024	2/6/2026	77C...

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


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-06 18:31:57
Marc Corona

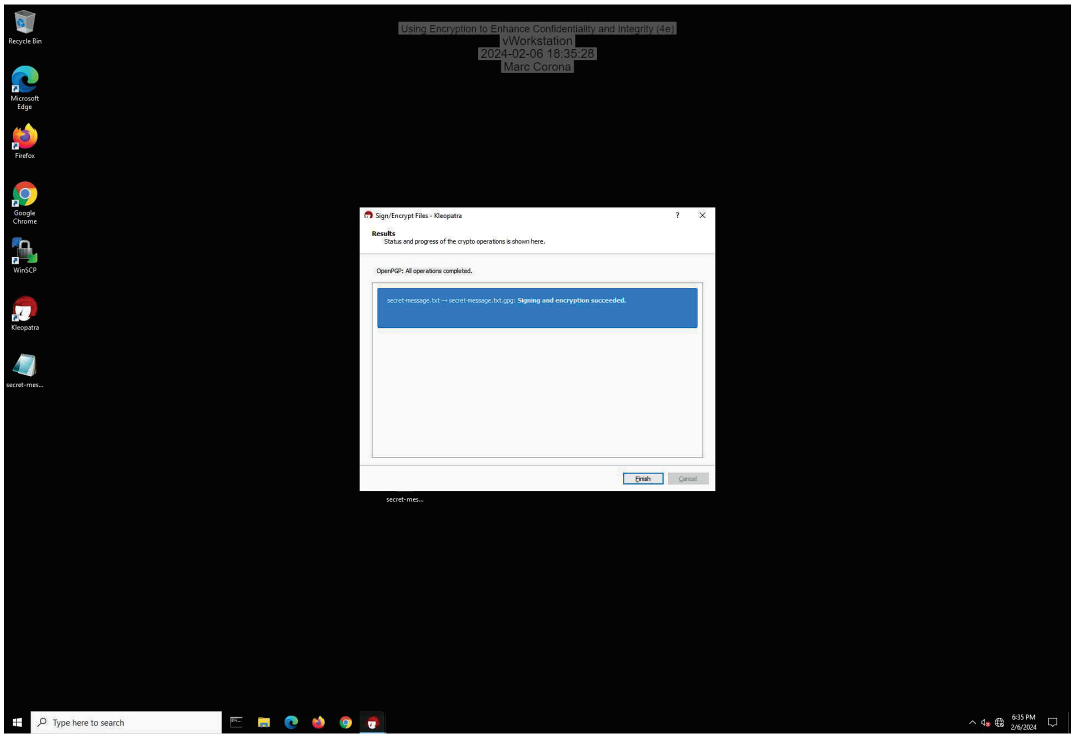
Kleopatra

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Alice Dodson	adodson@securelabsondemand.com	certified	2/6/2024	2/6/2026	95E5 528E B605 E...
Marc Corona	**student@securelabsondemand.com**	**certified**	**2/6/2024**	**2/6/2026**	**77C6 4739 EE3D DA42**

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
Type here to search
6:31 PM
2/6/2024

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
2024-02-06 18:35:28
Marc Corona

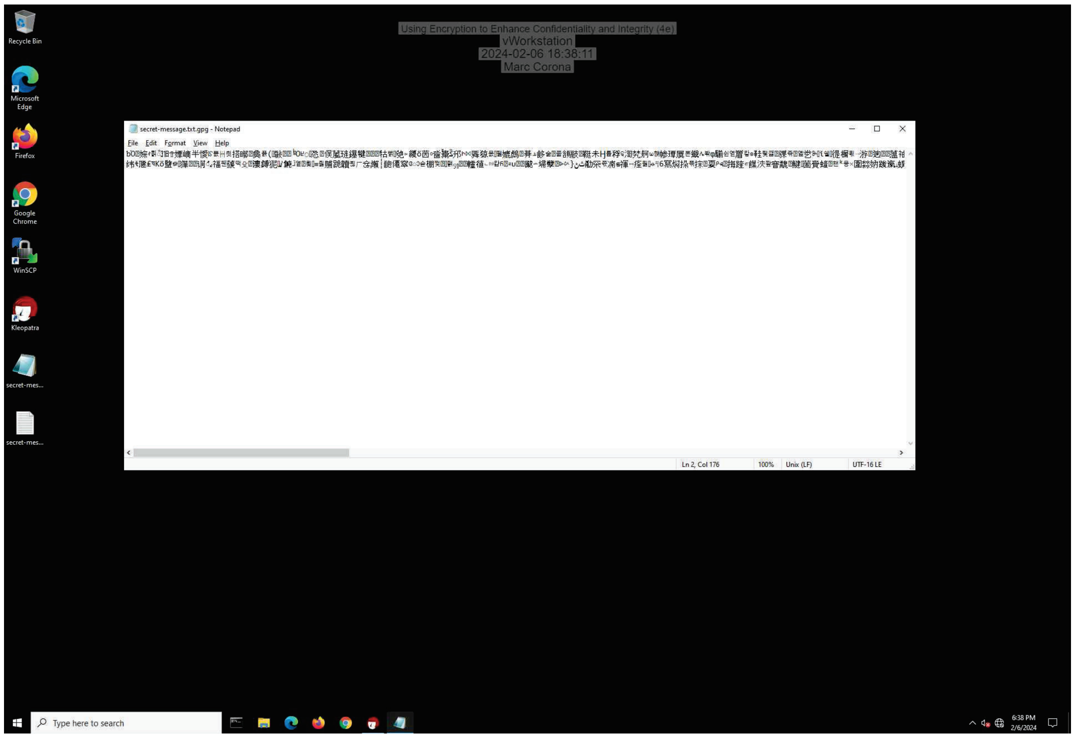
Sign/Encrypt Files - Kleopatra

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**.


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-06 18:38:11
Marc Corona

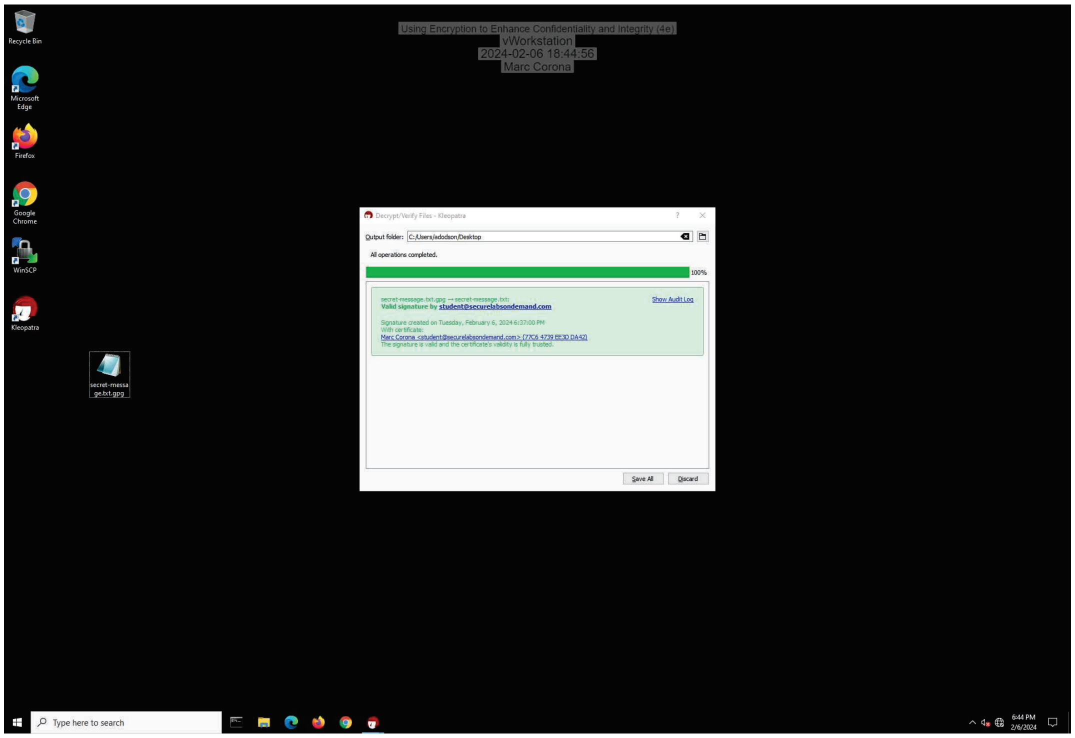
secret-message.txt.gpg - Notepad

```
[illegible]
```

Ln 2, Col 176 100% Unix (LF) UTF-16 LE

Part 3: Decrypt a File Using Asymmetric Encryption

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


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-06 18:44:56
Marc Corona

Decrypt/Verify Files - Kleopatra

Output folder: C:/Users/adodson/Desktop

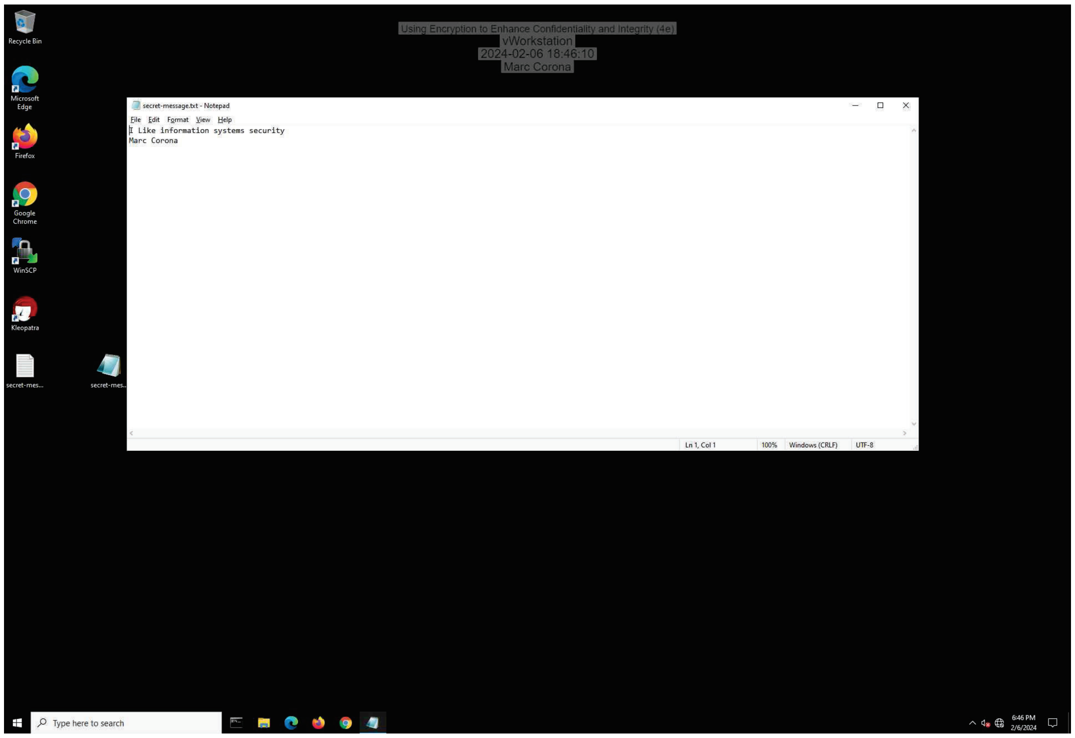
All operations completed.

100%

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

Signature created on Tuesday, February 6, 2024 6:37:00 PM
With certificate:
Marc Corona <student@securelabsondemand.com> (77C6 4739 EE3D DA42)
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**.



Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-06 18:46:10
Marc Corona

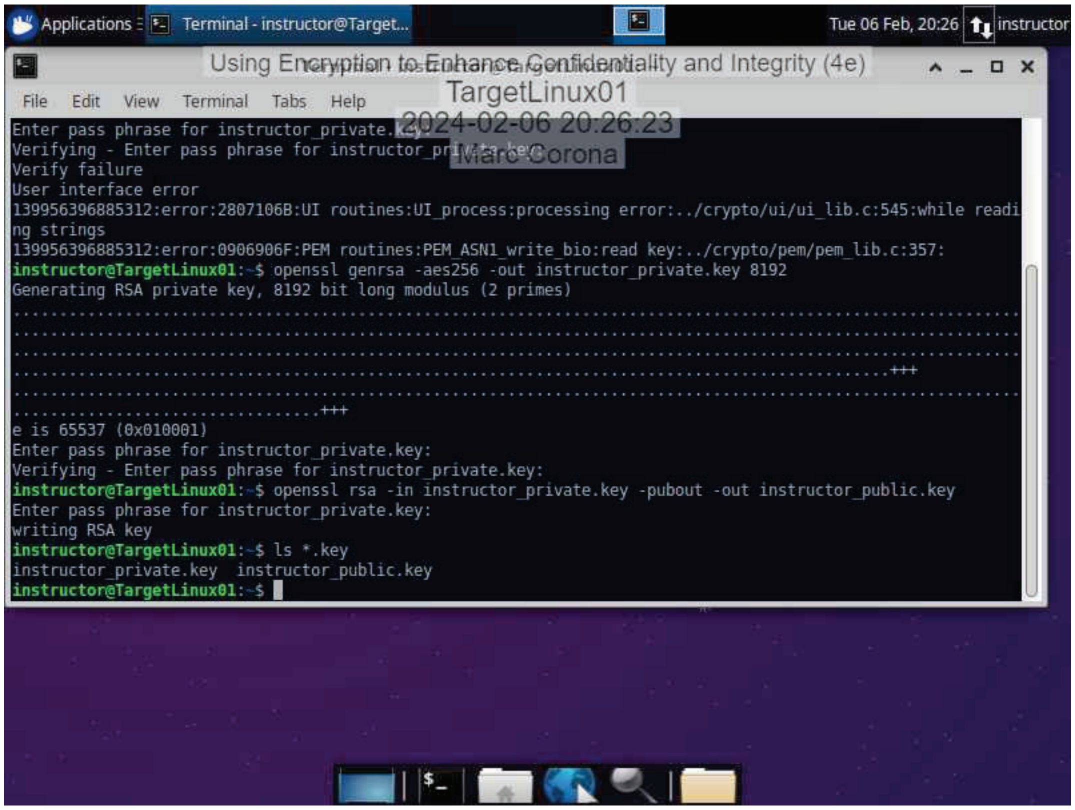
secret-message.txt - Notepad

```
I Like information systems security
Marc Corona
```

Section 2: Applied Learning

Part 1: Create an Asymmetric Key Pair

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


Applications
Terminal - instructor@Target...
Tue 06 Feb, 20:26
instructor
File Edit View Terminal Tabs Help

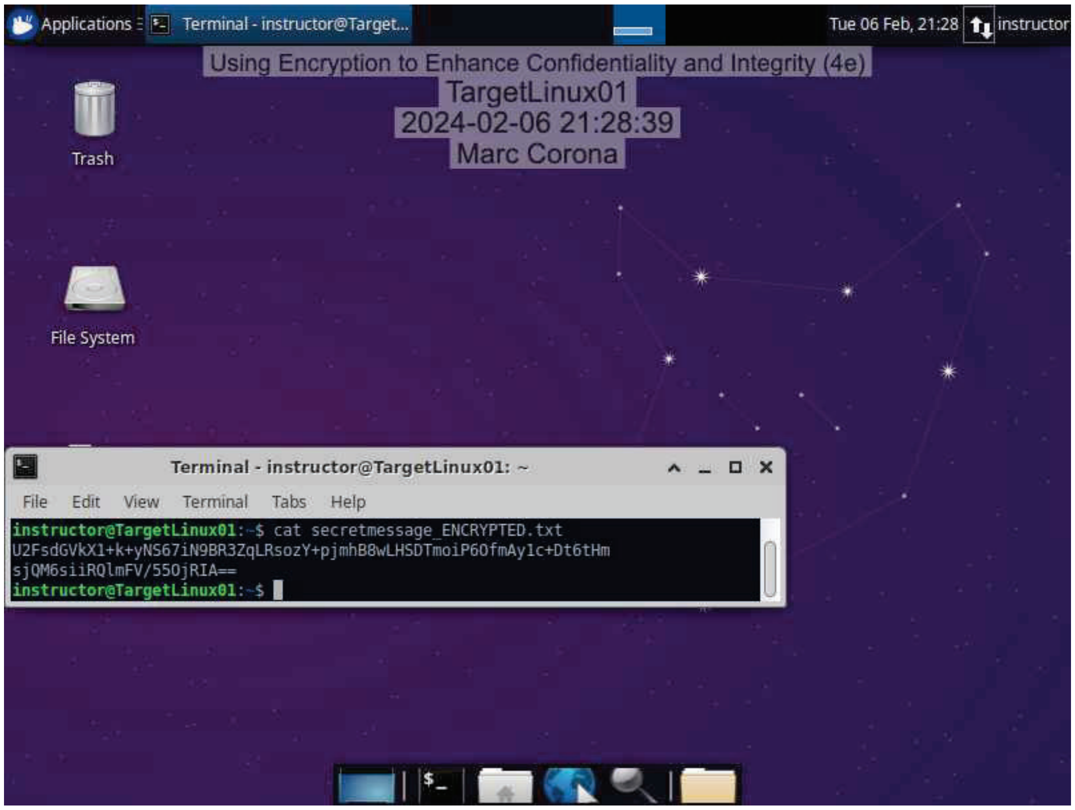
```
Enter pass phrase for instructor_private.key:
Verifying - Enter pass phrase for instructor_private.key:
Verify failure
User interface error
139956396885312:error:2807106B:UI routines:UI_process:processing error:../crypto/ui/ui_lib.c:545:while readi
ng strings
139956396885312:error:0906906F:PEM routines:PEM_ASN1_write_bio:read key:../crypto/pem/pem_lib.c:357:
instructor@TargetLinux01:~$ openssl genrsa -aes256 -out instructor_private.key 8192
Generating RSA private key, 8192 bit long modulus (2 primes)
..........................................................................................................
..........................................................................................................
..........................................................................................................
.............................................................................................+++
..........................................................................................................
...................................+++
e is 65537 (0x010001)
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 Using Symmetric Encryption

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

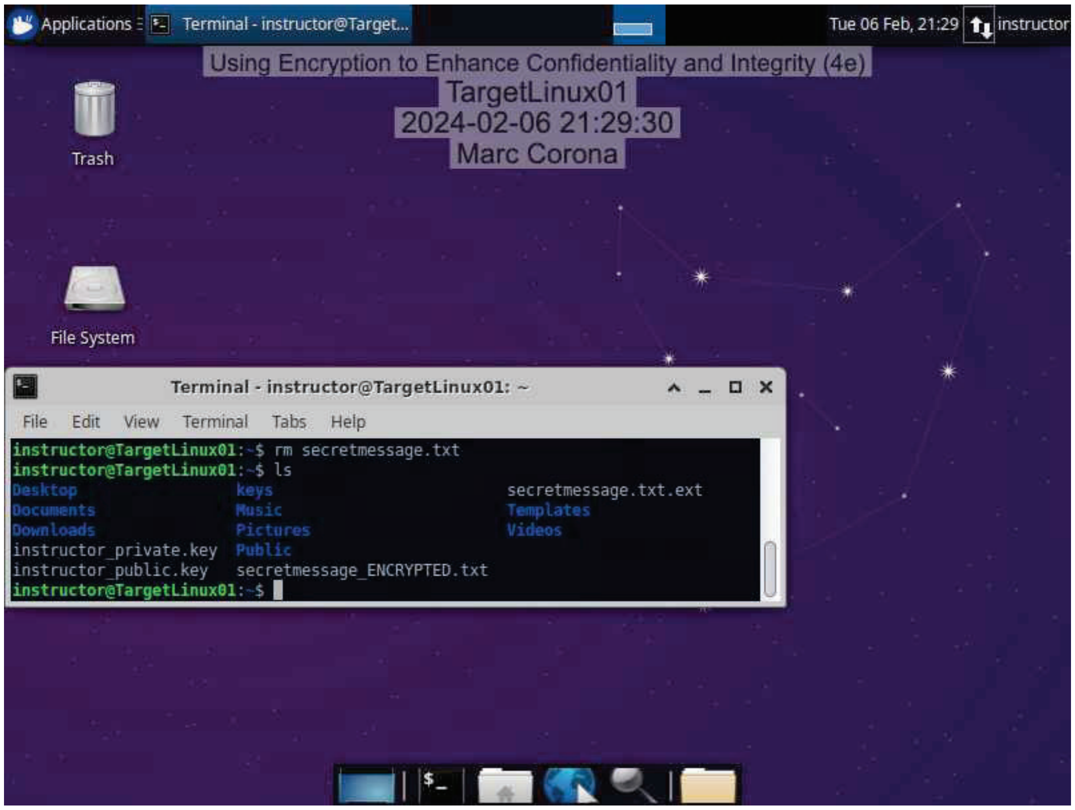
L!^erp00l!

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


Applications
Terminal - instructor@Target...
Tue 06 Feb, 21:28
instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-06 21:28:39
Marc Corona
Trash
File System
Terminal - instructor@TargetLinux01: ~
File
Edit
View
Terminal
Tabs
Help

```
instructor@TargetLinux01:~$ cat secretmessage_ENCRYPTED.txt
U2FsdGVkX1+k+yNS67iN9BR3ZqLRsozY+pjmhB8wLHSDTmoiP6OfmAy1c+Dt6tHm
sjQM6siiRQlmFV/55OjRIA==
instructor@TargetLinux01:~$
```

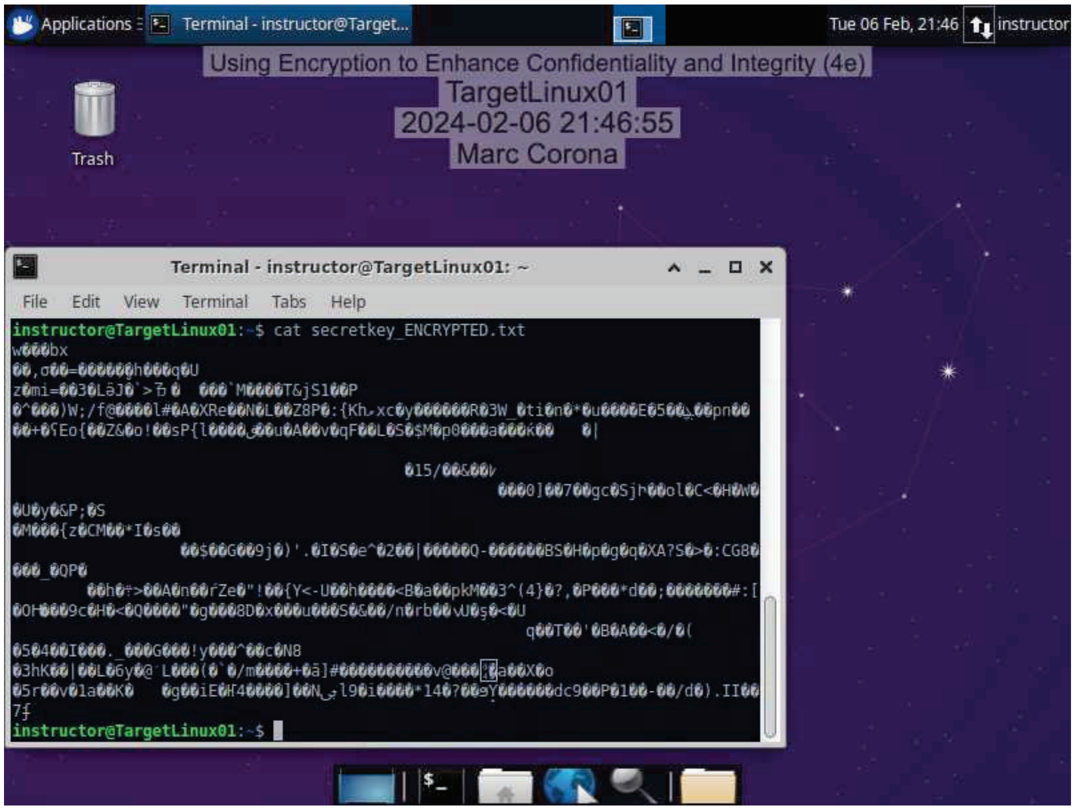
16. **Make a screen capture** showing the **output of the ls command**.


Applications
Terminal - instructor@Target...
Tue 06 Feb, 21:29
instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-06 21:29:30
Marc Corona
Trash
File System
Terminal - instructor@TargetLinux01: ~
File Edit View Terminal Tabs Help

```
instructor@TargetLinux01:~$ rm secretmessage.txt
instructor@TargetLinux01:~$ ls
Desktop               keys                           secretmessage.txt.ext
Documents             Music                          Templates
Downloads             Pictures                       Videos
instructor_private.key  Public
instructor_public.key   secretmessage_ENCRYPTED.txt
instructor@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**.

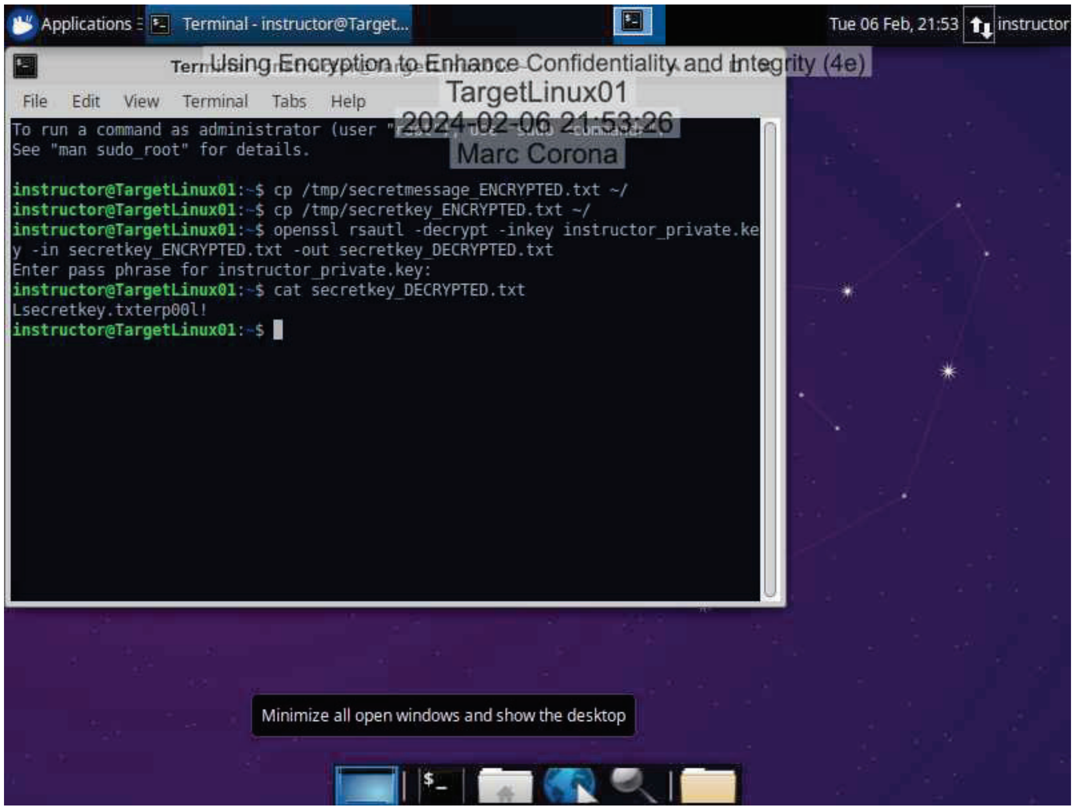


Applications
Terminal - instructor@Target...
Tue 06 Feb, 21:46
instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-06 21:46:55
Marc Corona
Trash
Terminal - instructor@TargetLinux01: ~
File
Edit
View
Terminal
Tabs
Help

```
instructor@TargetLinux01:~$ cat secretkey_ENCRYPTED.txt
w���bx
��,σ��=������h���q�U
z�mi=��3�LǝJ�`>ㄋ�  ���`M����T&jS1��P
�^���)W;/f@����l#�A�XRe��N�L��Z8P�:{Kh⌐xc�y������R�3W_�ti�n�*�u����E�5��,��pn��
��+�ʕEo{��Z&�o!��sP{l����,��u�A��v�qF��L�S�$M�p����a���K��   �|

                                        �15/��&��ᵥ
                                                 ���0]��7��gc�Sjʰ��ol�C<�H�W�
�U�y�&P;�S
�M���{z�CM��*I�s��
                 ��$��G��9j�)'.�I�S�e^�2��|�����Q-������BS�H�p�g�q�XA?S�>�:CG8�
���_�QP�
        ��h�∓>��A�n��ŕZe�"!��{Y<-U��h����<B�a��pkM��3^(4}�?,�P���*d��;�������#:[
�OH���9c�H�<�Q����"�g���8D�x���u���S�&��/n�rb��ᴠU�ş�<�U
                                                    q��T��'�B�A��<�/�(
�5�4��I���._���G���!y���^��c�N8
�3hK��|��L�6y�@`L���(�`�/m����+�ā]#����������v@���ʖ�a��X�o
�5r��v�1a��K�   �g��iE�H4����]��N,ب l9�i����*14�?��ɘY������dc9��P�1��-��/d�).II��
7ʄ
instructor@TargetLinux01:~$ 
```

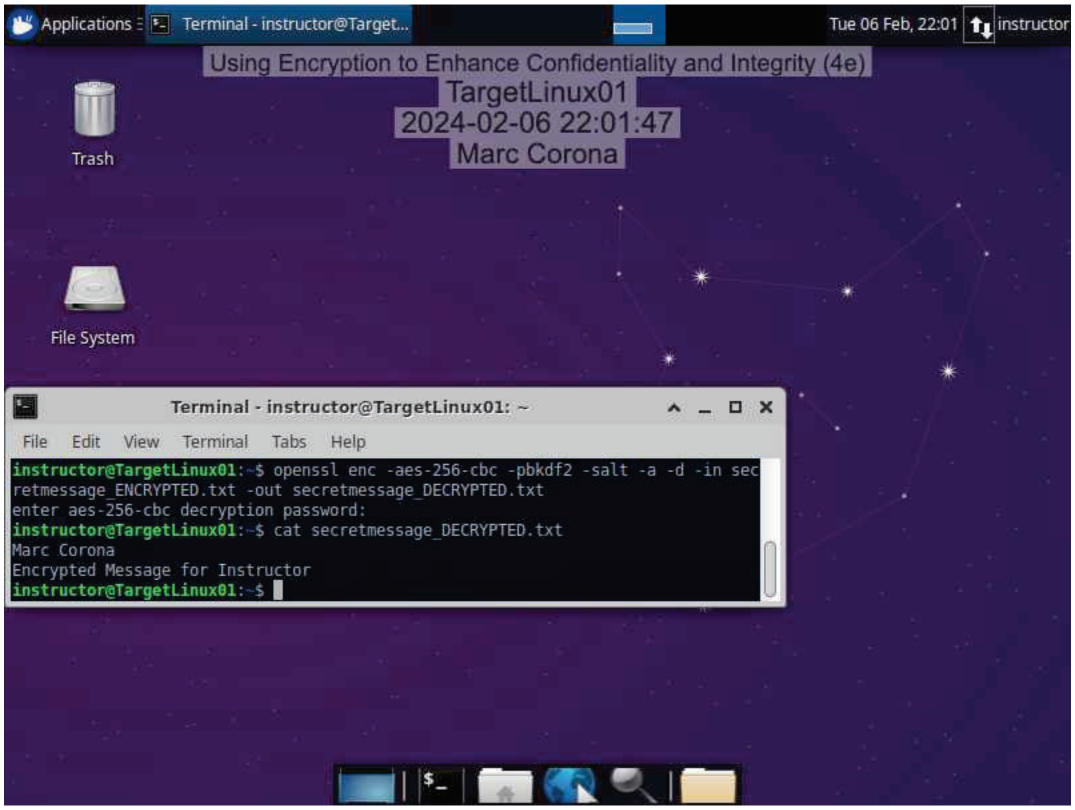
17. **Make a screen capture** showing the **decrypted contents of the secretkey_DECRYPTED.txt file**.


Applications
Terminal - instructor@Target...
Tue 06 Feb, 21:53
instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-06 21:53:26
Marc Corona
File Edit View Terminal Tabs Help
Minimize all open windows and show the desktop

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

instructor@TargetLinux01:~$ cp /tmp/secretmessage_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ cp /tmp/secretkey_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_private.ke
y -in secretkey_ENCRYPTED.txt -out secretkey_DECRYPTED.txt
Enter pass phrase for instructor_private.key:
instructor@TargetLinux01:~$ cat secretkey_DECRYPTED.txt
Lsecretkey.txterp00l!
instructor@TargetLinux01:~$
```

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

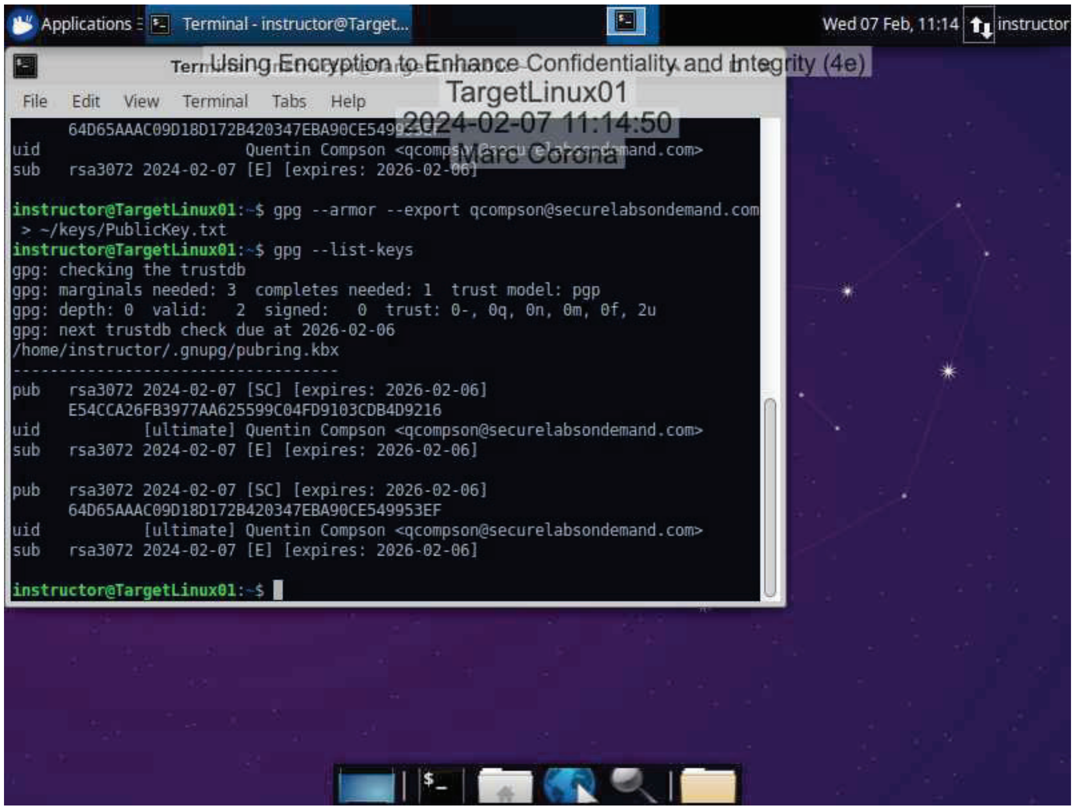

Applications
Terminal - instructor@Target...
Tue 06 Feb, 22:01
instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-06 22:01:47
Marc Corona
Trash
File System
Terminal - instructor@TargetLinux01: ~
File Edit View Terminal Tabs Help

```
instructor@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -d -in sec
retmessage_ENCRYPTED.txt -out secretmessage_DECRYPTED.txt
enter aes-256-cbc decryption password:
instructor@TargetLinux01:~$ cat secretmessage_DECRYPTED.txt
Marc Corona
Encrypted Message for Instructor
instructor@TargetLinux01:~$
```

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**.



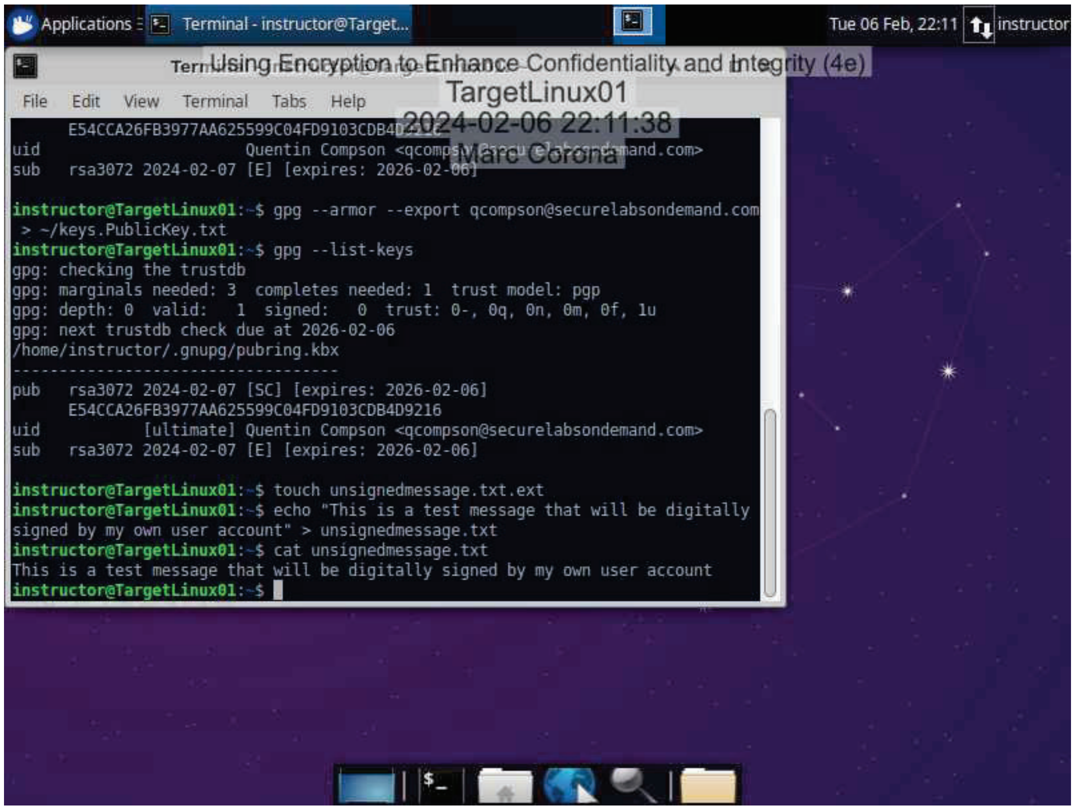
```
      64D65AAAC09D18D172B420347EBA90CE549953EF
uid                      Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-07 [E] [expires: 2026-02-06]

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:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2026-02-06
/home/instructor/.gnupg/pubring.kbx
-----------------------------------
pub   rsa3072 2024-02-07 [SC] [expires: 2026-02-06]
      E54CCA26FB3977AA625599C04FD9103CDB4D9216
uid           [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-07 [E] [expires: 2026-02-06]

pub   rsa3072 2024-02-07 [SC] [expires: 2026-02-06]
      64D65AAAC09D18D172B420347EBA90CE549953EF
uid           [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-07 [E] [expires: 2026-02-06]

instructor@TargetLinux01:~$
```

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


Applications
Terminal - instructor@Target...
Tue 06 Feb, 22:11
instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-06 22:11:38
Marc Corona
File Edit View Terminal Tabs Help

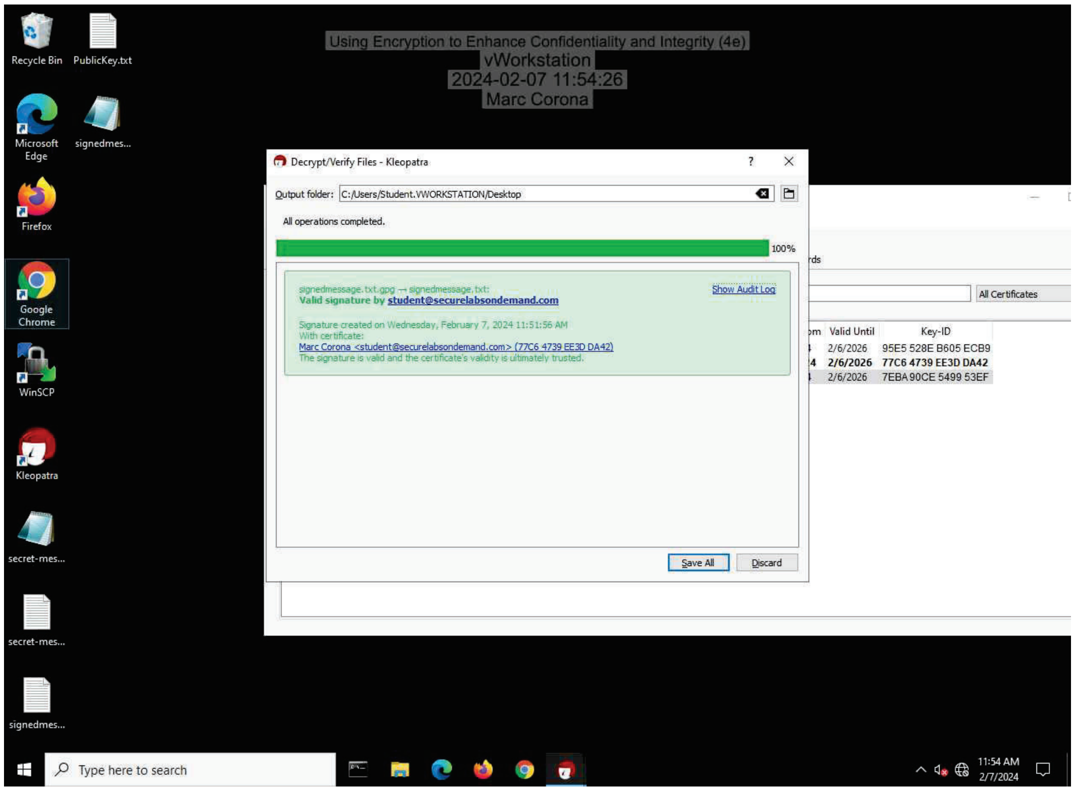
```
      E54CCA26FB3977AA625599C04FD9103CDB4D9216
uid                      Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-07 [E] [expires: 2026-02-06]

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 2026-02-06
/home/instructor/.gnupg/pubring.kbx
-----------------------------------
pub   rsa3072 2024-02-07 [SC] [expires: 2026-02-06]
      E54CCA26FB3977AA625599C04FD9103CDB4D9216
uid           [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-07 [E] [expires: 2026-02-06]

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

Part 2: Verify the Digital Signature Using Kleopatra

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



Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-07 11:54:26
Marc Corona

Decrypt/Verify Files - Kleopatra

Output folder: C:/Users/Student.VWORKSTATION/Desktop

All operations completed.

100%

signedmessage.txt.gpg → signedmessage.txt:
Valid signature by student@securelabsondemand.com

Signature created on Wednesday, February 7, 2024 11:51:56 AM
With certificate:
Marc Corona <student@securelabsondemand.com> (77C6 4739 EE3D DA42)
The signature is valid and the certificate's validity is ultimately trusted.

Valid Until	Key-ID
2/6/2026	95E5 528E B605 ECB9
2/6/2026	**77C6 4739 EE3D DA42**
2/6/2026	7EBA 90CE 5499 53EF