Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

Student:	Email:
Fernando Parra	fparra1@msudenve.edu

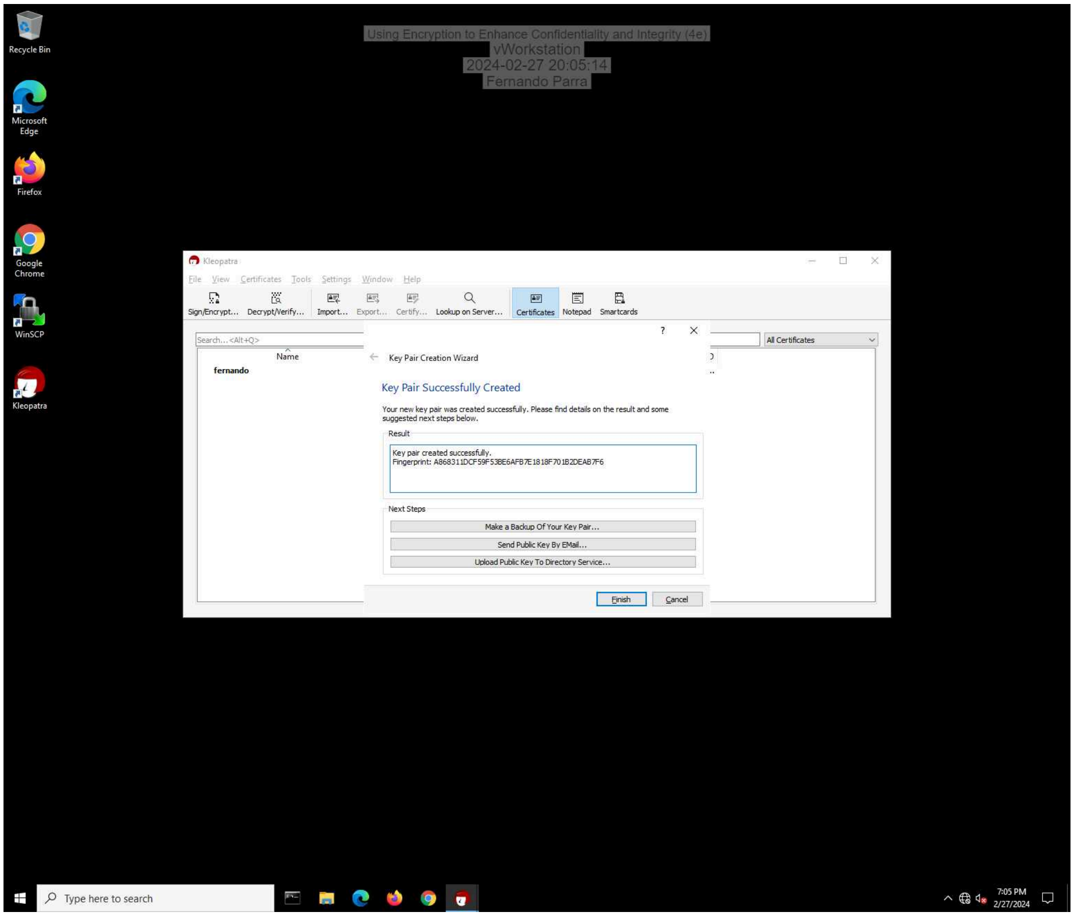
Time on Task:	Progress:
3 hours, 44 minutes	100%

Report Generated: Tuesday, February 27, 2024 at 11:13 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.**



Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-27 20:05:14
Fernando Parra

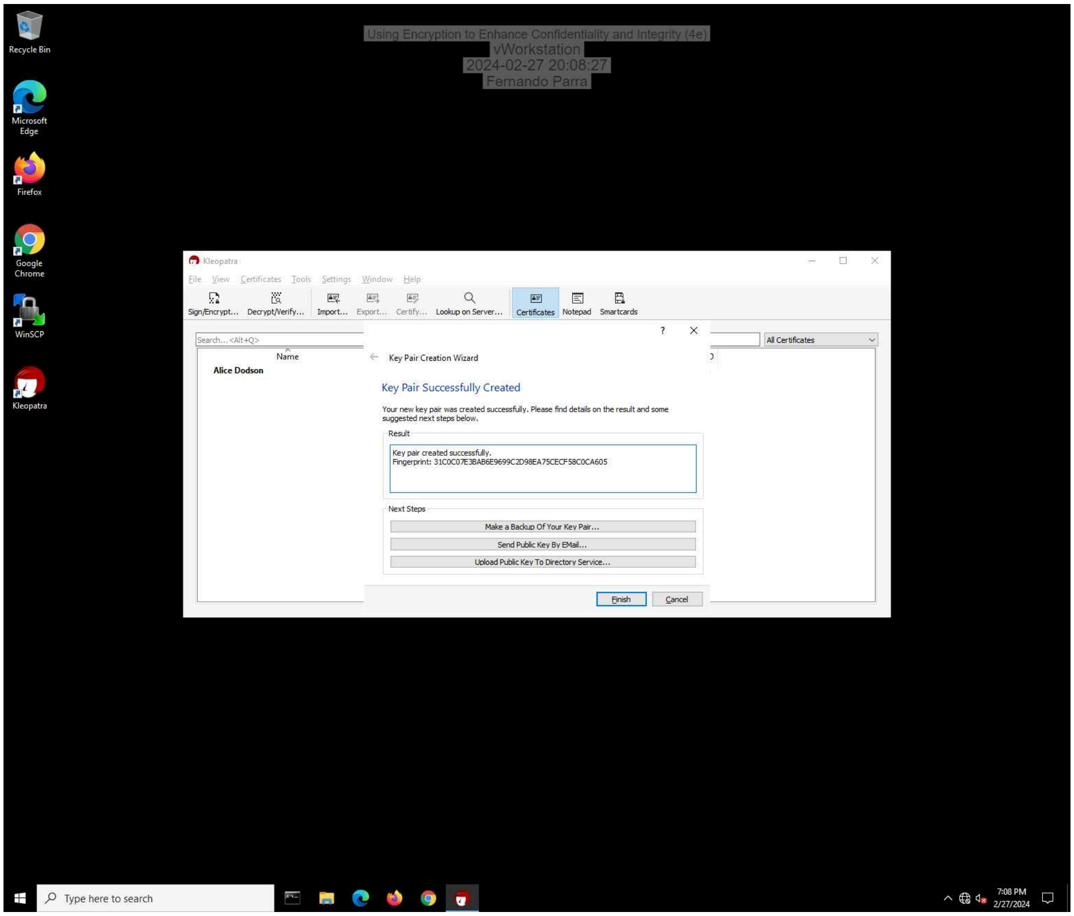
Key Pair Successfully Created

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: A868311DCF59F53BE6AFB7E1818F701B2DEAB7F6
```

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



Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-27 20:08:27
Fernando Parra

Key Pair Creation Wizard

Key Pair Successfully Created

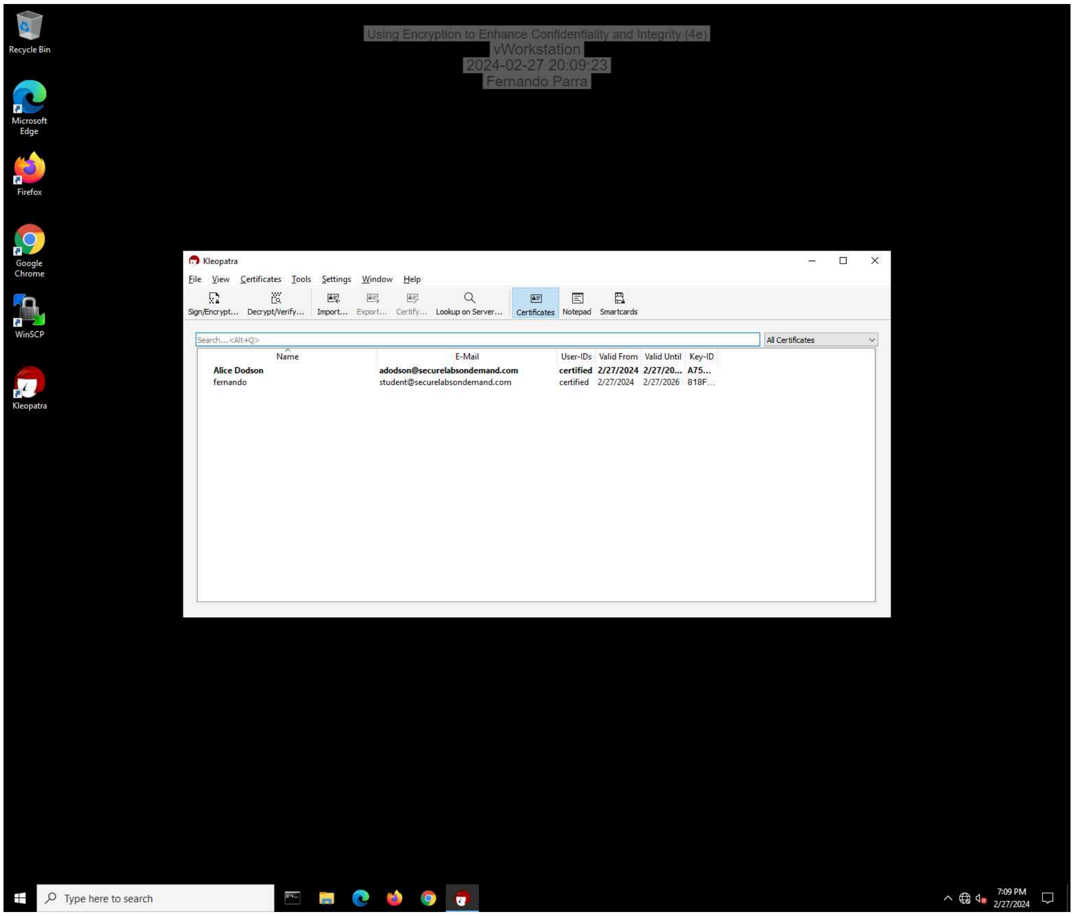
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result

```
Key pair created successfully.
Fingerprint: 31C0C07E3BAB6E9699C2D98EA75CECF58C0CA605
```

Recycle Bin
Microsoft Edge
Firefox
Google Chrome
WinSCP
Kleopatra
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
Name
Alice Dodson
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
7:08 PM
2/27/2024

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

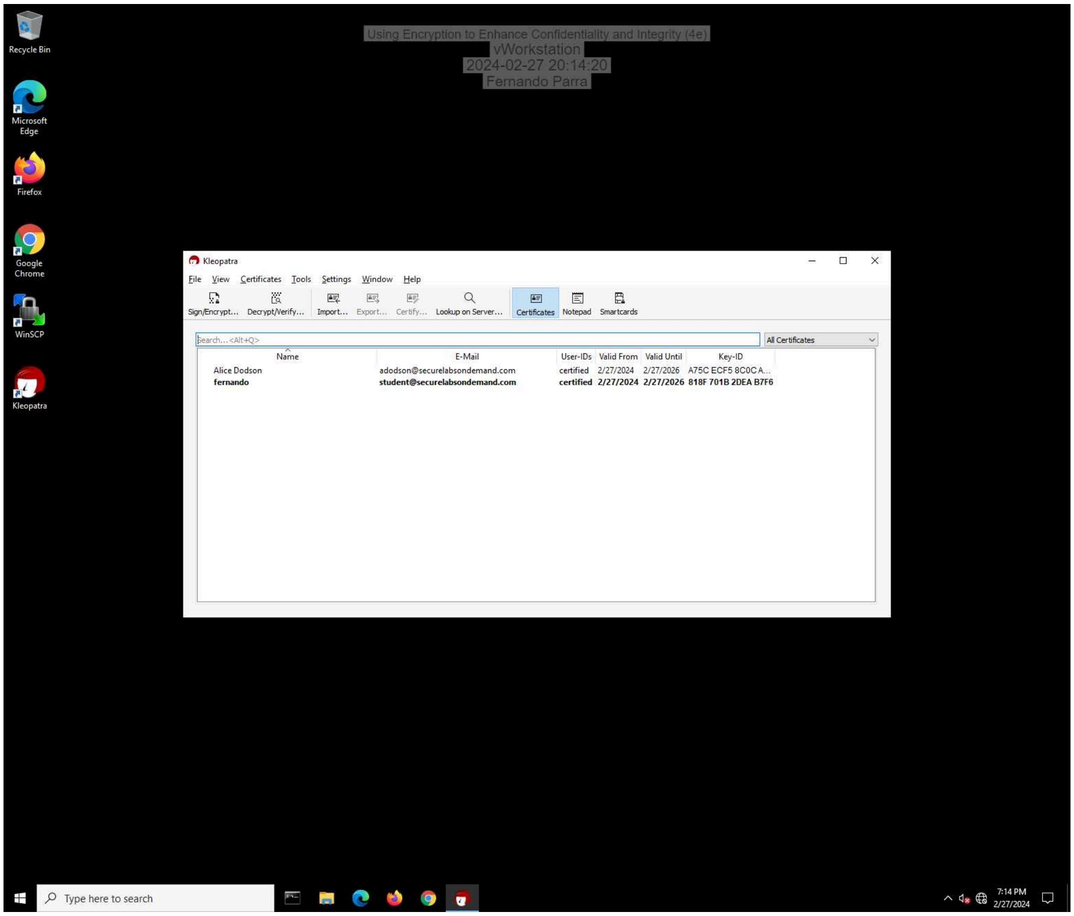


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-27 20:09:23
Fernando Parra

Recycle Bin
Microsoft Edge
Firefox
Google Chrome
WinSCP
Kleopatra
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
Type here to search
7:09 PM
2/27/2024

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Alice Dodson	**adodson@securelabsondemand.com**	**certified**	**2/27/2024**	**2/27/20...**	**A75...**
fernando	student@securelabsondemand.com	certified	2/27/2024	2/27/2026	818F...

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

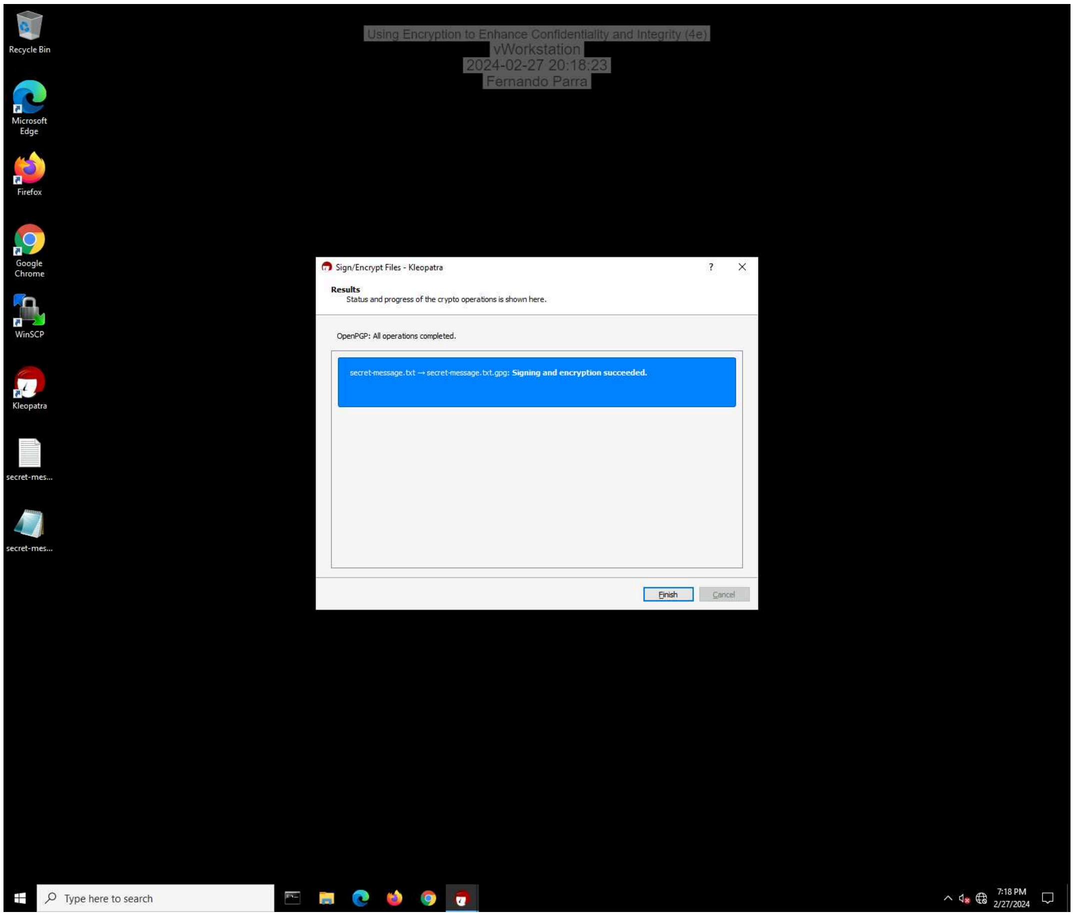


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-27 20:14:20
Fernando Parra

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Alice Dodson	adodson@securelabsondemand.com	certified	2/27/2024	2/27/2026	A75C ECF5 8C0C A...
fernando	**student@securelabsondemand.com**	**certified**	**2/27/2024**	**2/27/2026**	**818F 701B 2DEA B7F6**

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
2024-02-27 20:18:23
Fernando Parra

Sign/Encrypt Files - Kleopatra

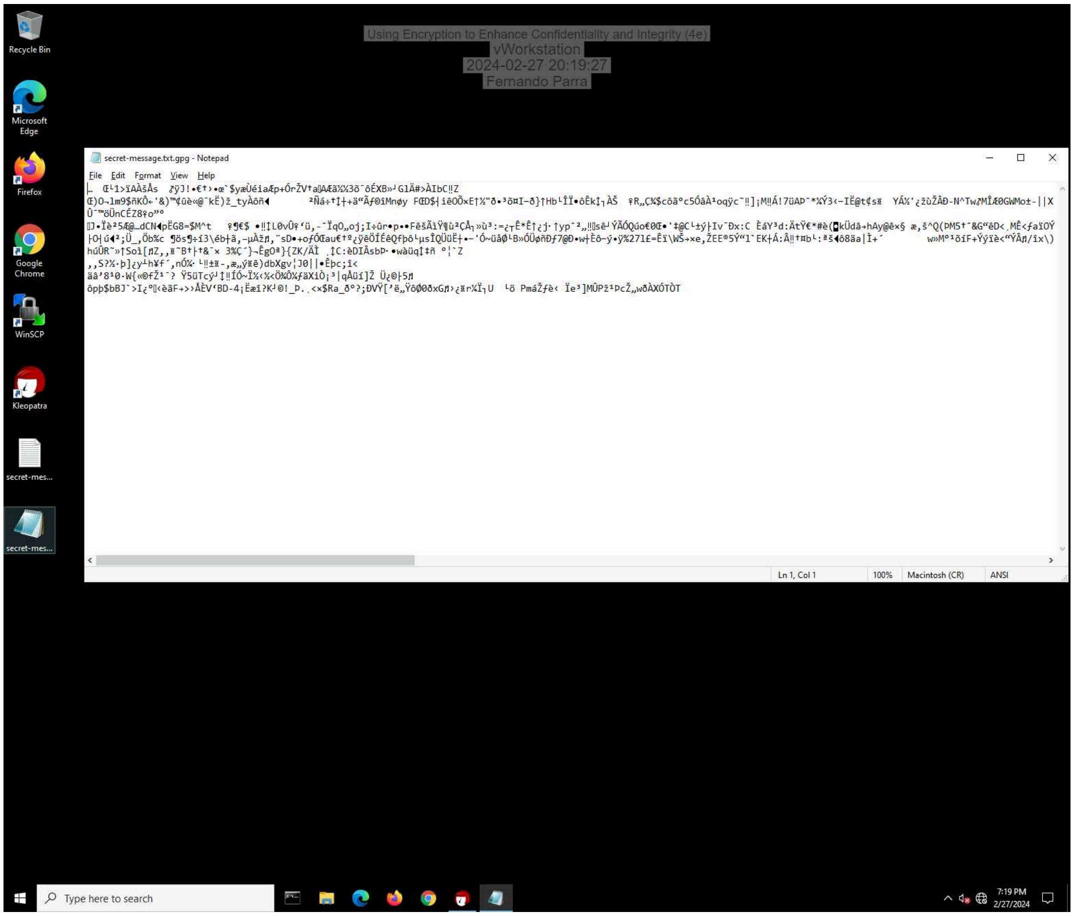
Results

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**.

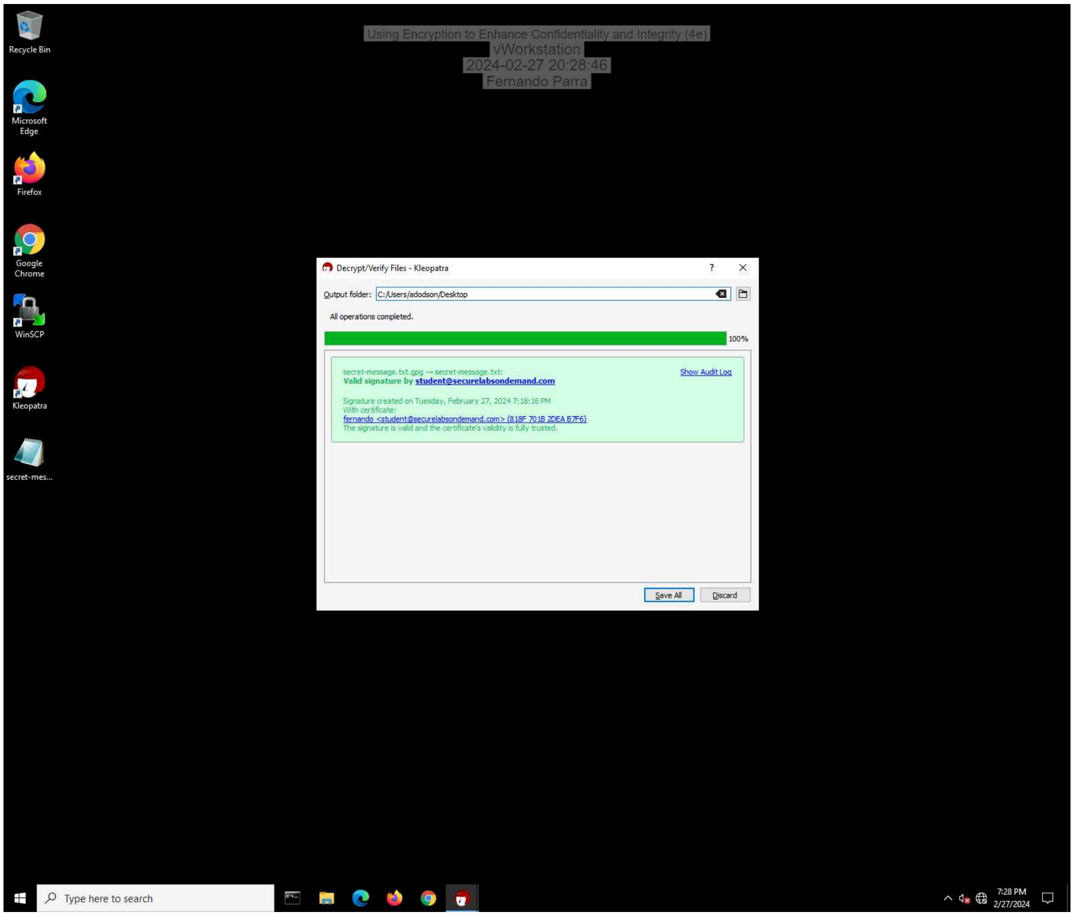


Using Encryption to Enhance Confidentiality and Integrity (4e)
vWorkstation
2024-02-27 20:19:27
Fernando Parra

```
|…  Œ└1>ïAÀšÅs  ♪ÿJ!•€†›•œ`$yæÙéiaÆp+ÓrŽV†a▯AÆã½¼3õ¯ôÉXB»┘GlÄ#>ÀIbC‼Z
Œ)O¬lm9$ñKÔ←'&)™¢ûè«@¯kË)ž_tyÀôñ◄       ²Ñá÷†↨┼+ä“Ãƒ©îMnøy FŒD$┤iêOÕ×E↑½"ð•³õ¤I–ð}↑Hb└ÎÏ•ôÊk↨┐ÀŠ  ♀R„Ç¾$côãºc5ÓâÀ¹oqÿc˜‼]¡M‼Á!7üAÞ^*¼Ý3‹–IË@t¢s※  YÁ½'¿žùŽÂÐ-N^Tw♪MÎÆ0GWMo±-||X
Û¯™öÜnCÉZ8♀o”º
▯J•Ïè²5Æ@…dCN◄pËG8=$M^t   ♀¶€$ •‼↨L0vÛ♀‘ü,-ˆÏqO„oj;I÷ûr•p••FêšÃìŸ¶ù²ÇÅ┐»ù³:=¿┬Ê*Ê↑¿j·↑ypˆ²„‼▯sê┘ÝÃÓQúo€0Œ•'‡@C└±ý├Iv¯Ðx:C ÈáY³d:ÄtŸ€*#è(◘kÜdâ→hAy@ê×§ æ,š^Q(ÞM5†ˆ&G“êD‹.MÊ<ƒaïOÝ
├O┤ú◄²;Ü_,Öb%c ¶ös¶÷í3\éb┼ã,-µÀž♫,¨sD•+oƒÓŒau€†º¿ÿêÖÍÉêQfþô└µsÎQÜüË┼•–'Ó~üåØ└B»ÓÜøñÐƒ7@Ð•w┼Èô–ý•ÿ%271£=Êï\WŠ→×e,ŽEE®5Ý“1`EK┼Á:Â‼†¤b└:ªš◄ô8äa|Ì+´        w»Mº¹õíF+Ýýïè<“ÝÂ♫/îx\)
húÛR˜»↑Soì[♫Z,,※˜B†├†&¯× 3%Ç´}¬ÊgOª}{ZK/ÄÌ .↨C:èDIÂsbÞ·•wàüq↨‡ñ º¦`Z
,,S?½·þ]¿y┴h¥f´,nÓ¼· └‼±※-,æ„ý※ê)dbXgv¦J0||•Êþc;î<
äâ’8¹0·W{«©fŽ¹¯? Ÿ5üTcý┘↨‼ÍÓ~Ï½‹¼<Ö¾Ô¼ƒäXiÒ¡³|qÅüí]Ž Ü¿©├5♫
ôpþ$bBJ`>I¿º▯‹èãF→››ÅÈV‘BD-4¡Ëæî?K┘©!_Þ.¸<×$Ra_ðº?;ÐVŸ['ë„ŸôØ0õxG♫›¿※r¼Ï┐U  └ö PmáŽƒè‹ Ïe³]MÛPž¹ÞcŽ„wðÀXÓTÒT
```

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
2024-02-27 20:28:46
Fernando Parra

Decrypt/Verify Files - Kleopatra

Output folder: C:/Users/adodson/Desktop

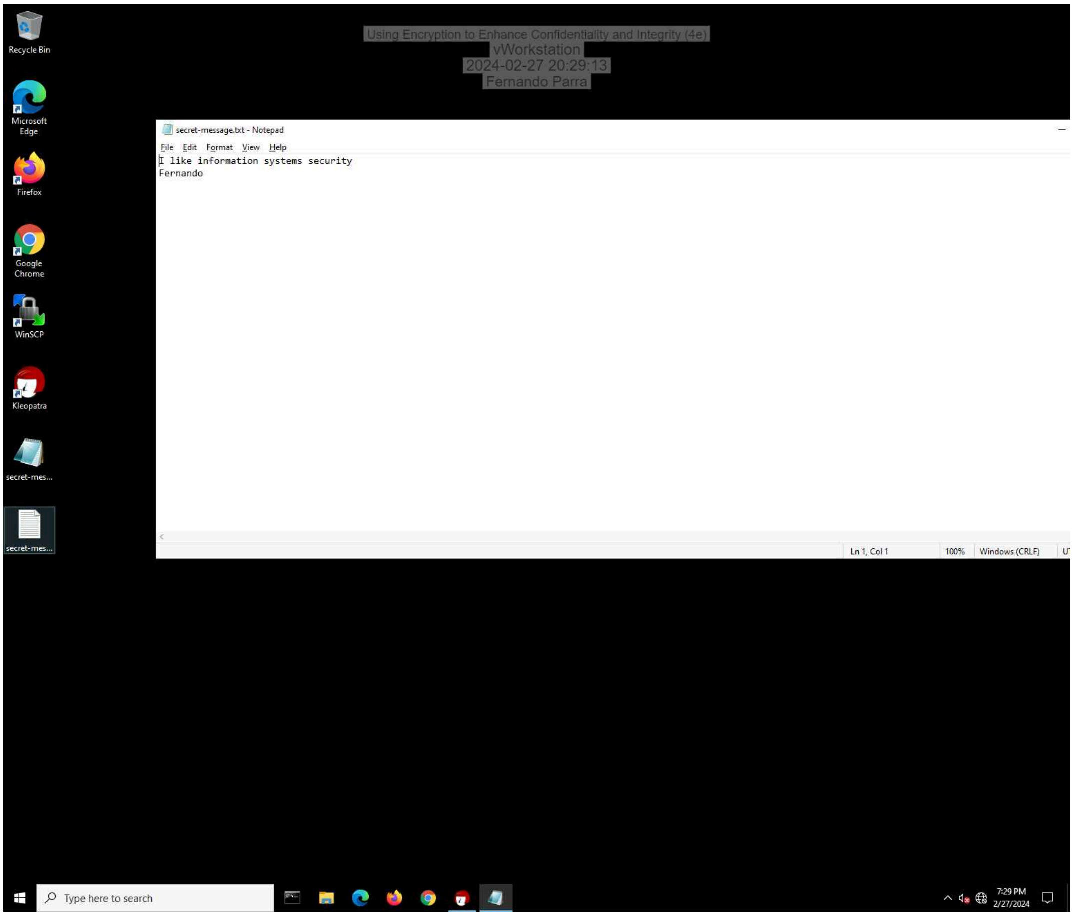
All operations completed.

100%

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

Signature created on Tuesday, February 27, 2024 7:18:16 PM
With certificate:
fernando <student@securelabsondemand.com> (818F 701B 2DEA B7F6)
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
2024-02-27 20:29:13
Fernando Parra

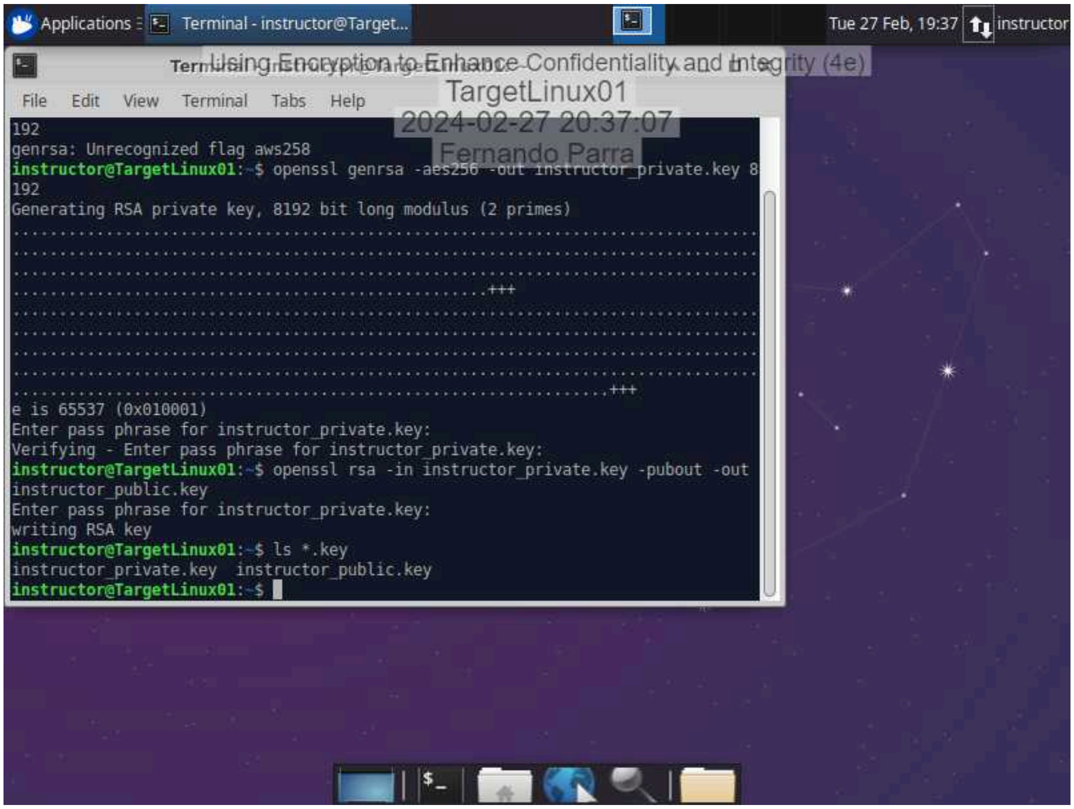
secret-message.txt - Notepad

```
I like information systems security
Fernando
```

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 27 Feb, 19:37
instructor
Terminal - instructor@TargetLinux01: ~
File
Edit
View
Terminal
Tabs
Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-27 20:37:07
Fernando Parra

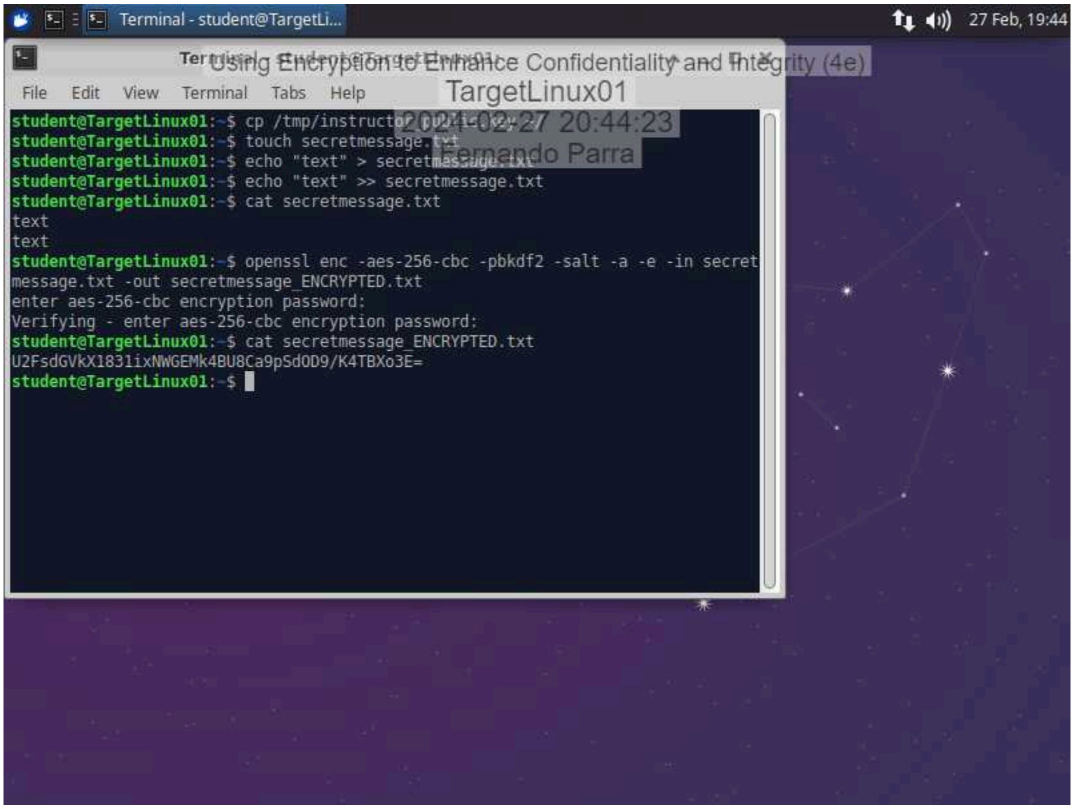
```
192
genrsa: Unrecognized flag aws258
instructor@TargetLinux01:~$ openssl genrsa -aes256 -out instructor_private.key 8
192
Generating RSA private key, 8192 bit long modulus (2 primes)
................................................................................
................................................................................
................................................................................
..................................................+++
................................................................................
................................................................................
................................................................................
................................................................................
..................................................................+++
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.

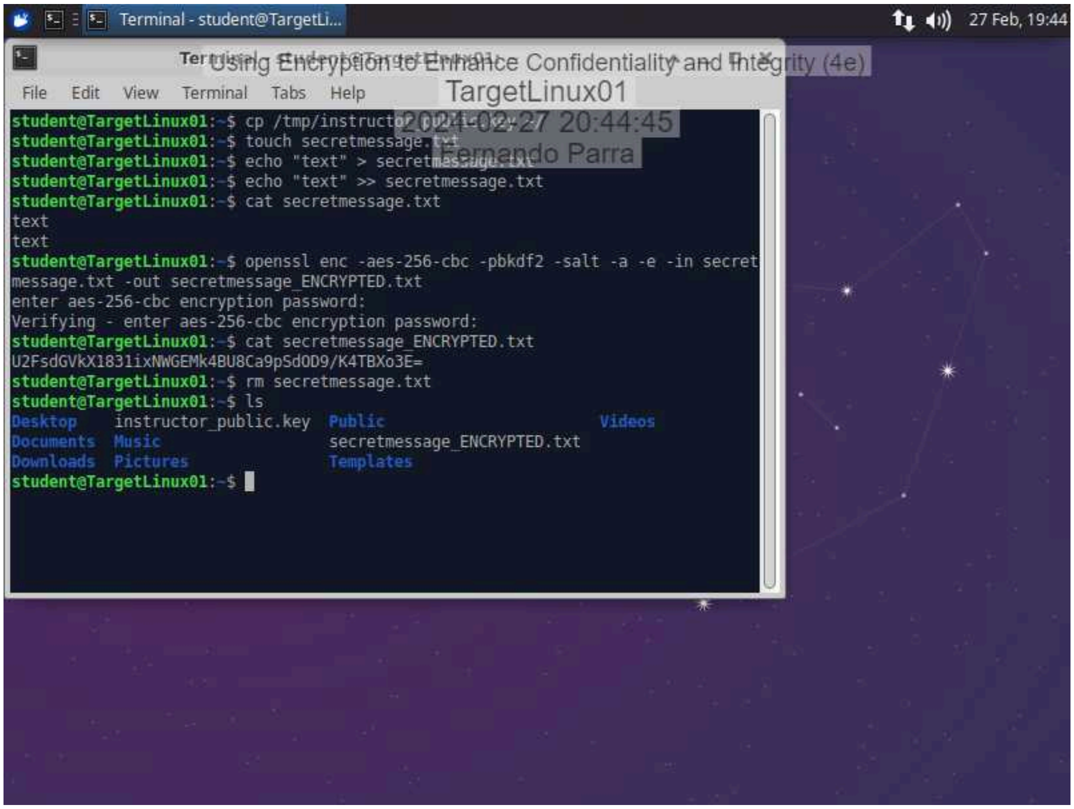
raspberry

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


Terminal - student@TargetLi...
27 Feb, 19:44
Terminal - student@TargetLinux01
File
Edit
View
Terminal
Tabs
Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-27 20:44:23
Fernando Parra

```
student@TargetLinux01:~$ cp /tmp/instructor_public.key ~
student@TargetLinux01:~$ touch secretmessage.txt
student@TargetLinux01:~$ echo "text" > secretmessage.txt
student@TargetLinux01:~$ echo "text" >> secretmessage.txt
student@TargetLinux01:~$ cat secretmessage.txt
text
text
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secret
message.txt -out secretmessage_ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat secretmessage_ENCRYPTED.txt
U2FsdGVkX1831ixNWGEMk4BU8Ca9pSdOD9/K4TBXo3E=
student@TargetLinux01:~$ 
```

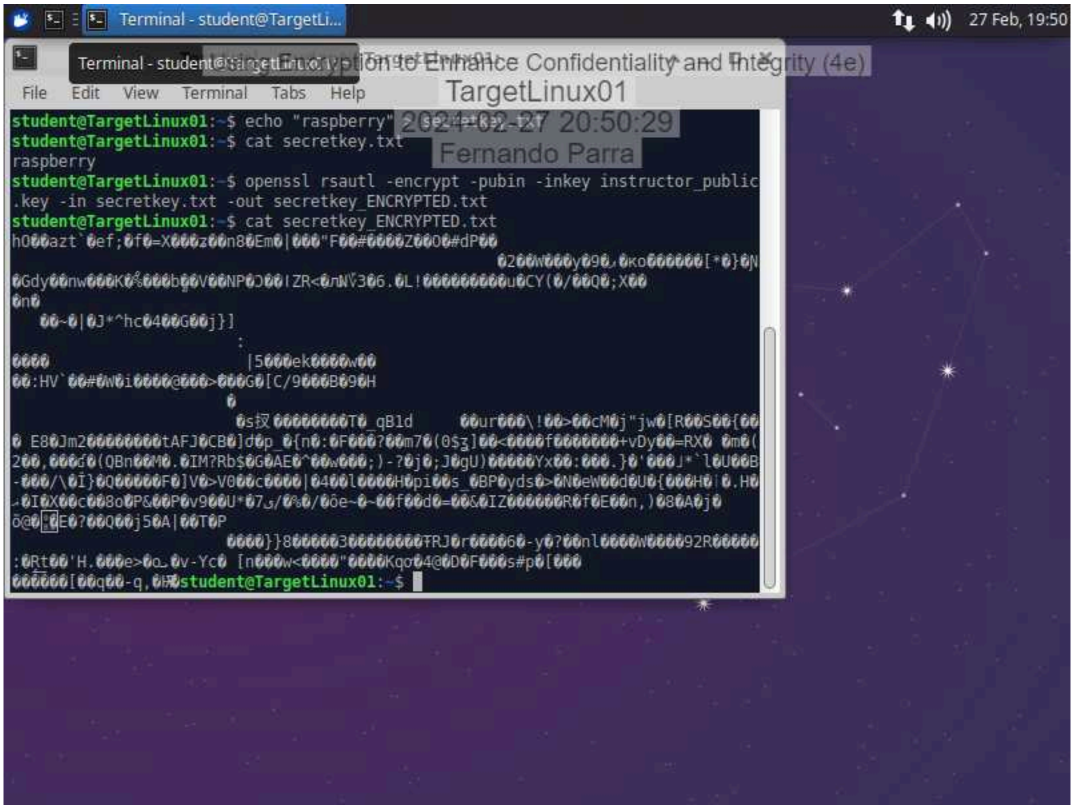
16. **Make a screen capture** showing the **output of the ls command**.


Terminal - student@TargetLi...
27 Feb, 19:44
Terminal - student@TargetLinux01
File
Edit
View
Terminal
Tabs
Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-27 20:44:45
Fernando Parra

```
student@TargetLinux01:~$ cp /tmp/instructor_public.key ~
student@TargetLinux01:~$ touch secretmessage.txt
student@TargetLinux01:~$ echo "text" > secretmessage.txt
student@TargetLinux01:~$ echo "text" >> secretmessage.txt
student@TargetLinux01:~$ cat secretmessage.txt
text
text
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secret
message.txt -out secretmessage_ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat secretmessage_ENCRYPTED.txt
U2FsdGVkX1831ixNWGEMk4BU8Ca9pSdOD9/K4TBXo3E=
student@TargetLinux01:~$ rm secretmessage.txt
student@TargetLinux01:~$ ls
Desktop    instructor_public.key  Public                       Videos
Documents  Music                  secretmessage_ENCRYPTED.txt
Downloads  Pictures               Templates
student@TargetLinux01:~$ 
```

Part 3: Transfer and Decrypt a File Using Hybrid Cryptography

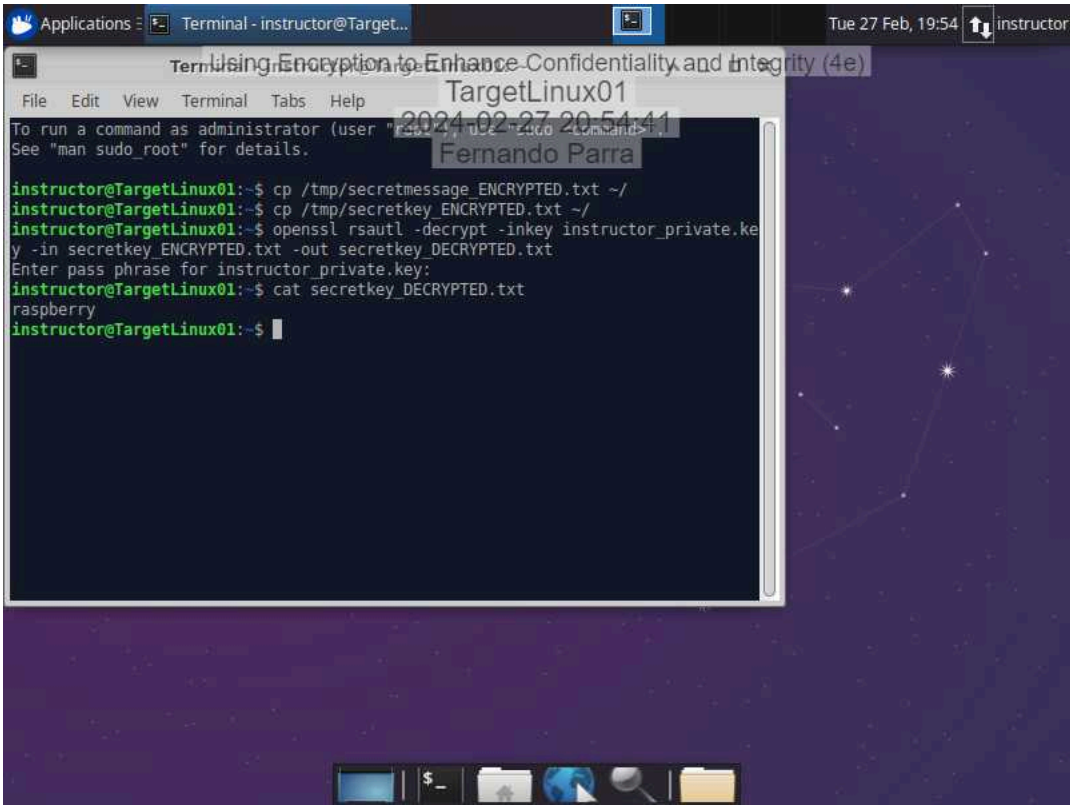
6. **Make a screen capture** showing the **encrypted contents of the secretkey_ENCRYPTED.txt file**.



Terminal - student@TargetLi...
27 Feb, 19:50
Terminal - student@TargetLinux01
File
Edit
View
Terminal
Tabs
Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-27 20:50:29
Fernando Parra

```
student@TargetLinux01:~$ echo "raspberry" > secretkey.txt
student@TargetLinux01:~$ cat secretkey.txt
raspberry
student@TargetLinux01:~$ openssl rsautl -encrypt -pubin -inkey instructor_public
.key -in secretkey.txt -out secretkey_ENCRYPTED.txt
student@TargetLinux01:~$ cat secretkey_ENCRYPTED.txt
hO��azt`�ef;�f�=X���z��n8�Em�|���"F��#����Z��O�#dP��
                                                      �2��W���y�9�,�ко������[*�}�N
�Gdy��nw���K�%���b��V��NP�J��!ZR<�лN√3�6.�L!���������u�CY(�/��Q�;X��
�n�
   ��~�|�J*^hc�4��G��j}]
                         :
����                      |5���ek����w��
��:HV`��#�W�i����@���>���G�[C/9���B�9�H
                        �
                         �s扠��������T�_qB1d     ��ur���\!��>��cM�j"jw�[R��S��{��
� E8�Jm2��������tAFJ�CB�]d�p_�{n�:�F���?��m7�(0$ʒ]��<����f�������+vDy��=RX� �m�(
2��,���d�(QBn��M�.�IM?Rb$�G�AE�^��w���;)-?�j�;J�gU)�����Yx��:���.}�'���J*`l�U��B
-���/\�Ī}�Q�����F�]V�>V0��c����|�4��l����H�pi��s_�BP�yds�>�N�eW��d�U�{���H�|�.H�
˩�I�X��c��8o�P&��P�v9��U*�7ی/�%�/�õe~�~��f��d�=��&�IZ������R�f�E��n,)�8�A�j�
õ@�|�E�?��Q��j5�A|��T�P
                        ����}}8�����3��������TRJ�r�����6�-y�?��nl����W�����92R�����
:�Rt��'H.���e>�ס.�v-Yc� [n���w<����"����Kqσ�4@�D�F���s#p�[���
������[��q��-q,�H�student@TargetLinux01:~$
```

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

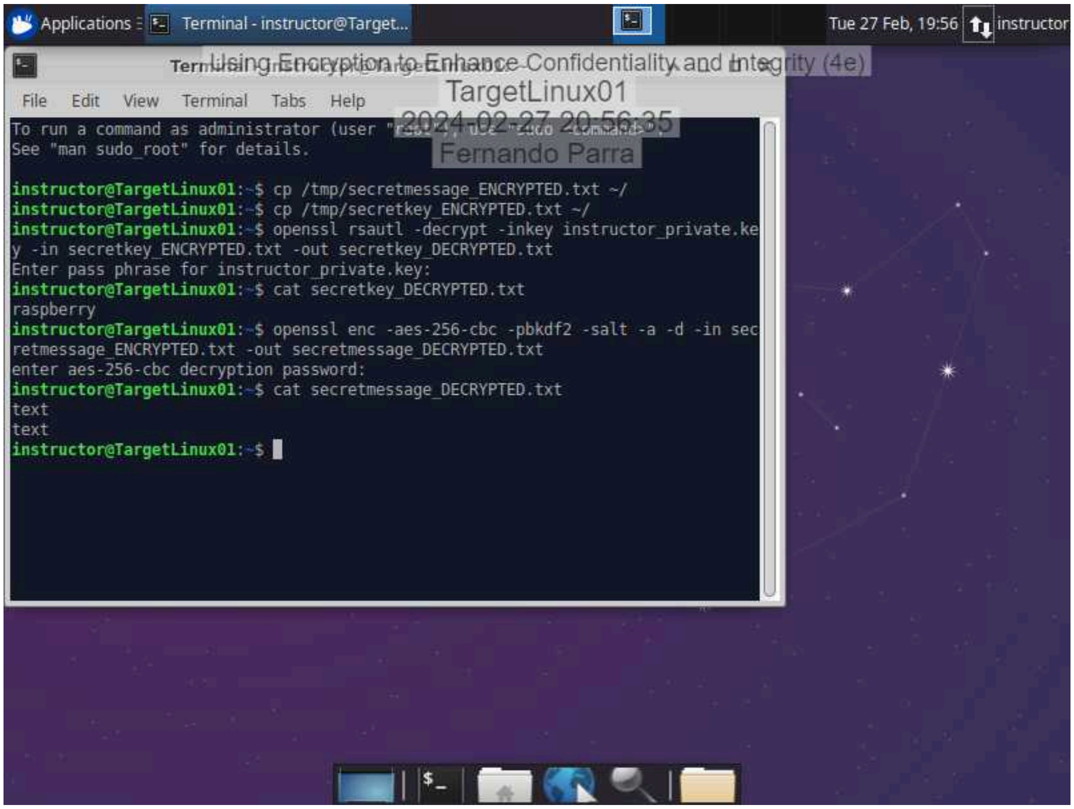

Applications
Terminal - instructor@Target...
Tue 27 Feb, 19:54
instructor
Terminal - instructor@TargetLinux01: ~
File
Edit
View
Terminal
Tabs
Help

Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-27 20:54:41
Fernando Parra

```
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
raspberry
instructor@TargetLinux01:~$ 
```

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



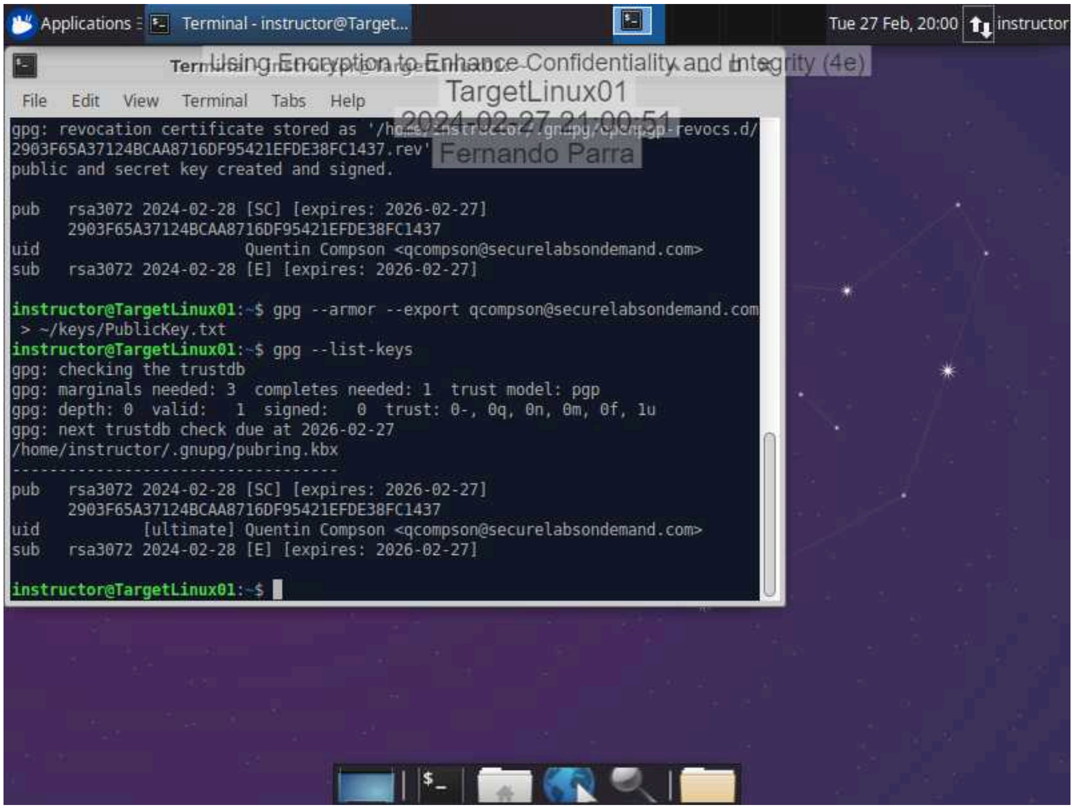
```
To run a command as administrator (user "root", use "sudo <command>".
See "man sudo_root" for details.

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
raspberry
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
text
text
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**.


Applications
Terminal - instructor@Target...
Tue 27 Feb, 20:00
instructor
Terminal - instructor@TargetLinux01: ~
File
Edit
View
Terminal
Tabs
Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-27 21:00:51
Fernando Parra

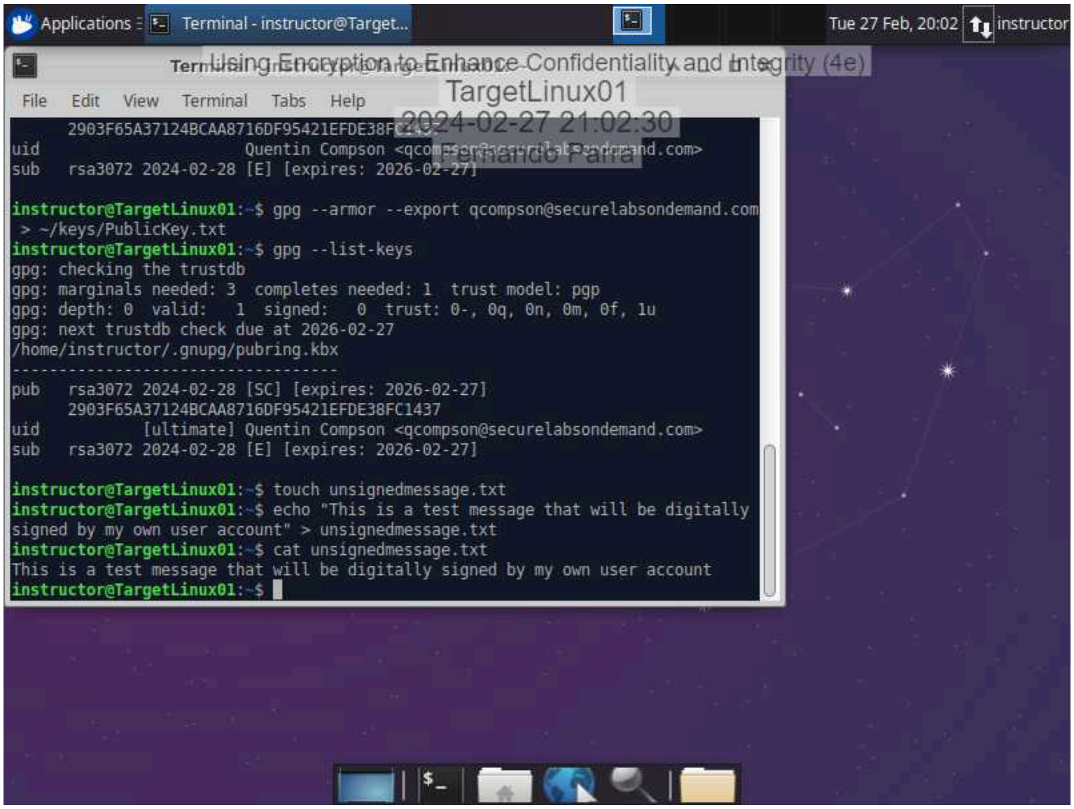
```
gpg: revocation certificate stored as '/home/instructor/.gnupg/openpgp-revocs.d/
2903F65A37124BCAA8716DF95421EFDE38FC1437.rev'
public and secret key created and signed.

pub   rsa3072 2024-02-28 [SC] [expires: 2026-02-27]
      2903F65A37124BCAA8716DF95421EFDE38FC1437
uid                      Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-28 [E] [expires: 2026-02-27]

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 2026-02-27
/home/instructor/.gnupg/pubring.kbx
-----------------------------------
pub   rsa3072 2024-02-28 [SC] [expires: 2026-02-27]
      2903F65A37124BCAA8716DF95421EFDE38FC1437
uid           [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-28 [E] [expires: 2026-02-27]

instructor@TargetLinux01:~$
```

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


Applications
Terminal - instructor@Target...
Tue 27 Feb, 20:02
instructor
Terminal - instructor@TargetLinux01: ~
File
Edit
View
Terminal
Tabs
Help
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-27 21:02:30
Fernando Parra

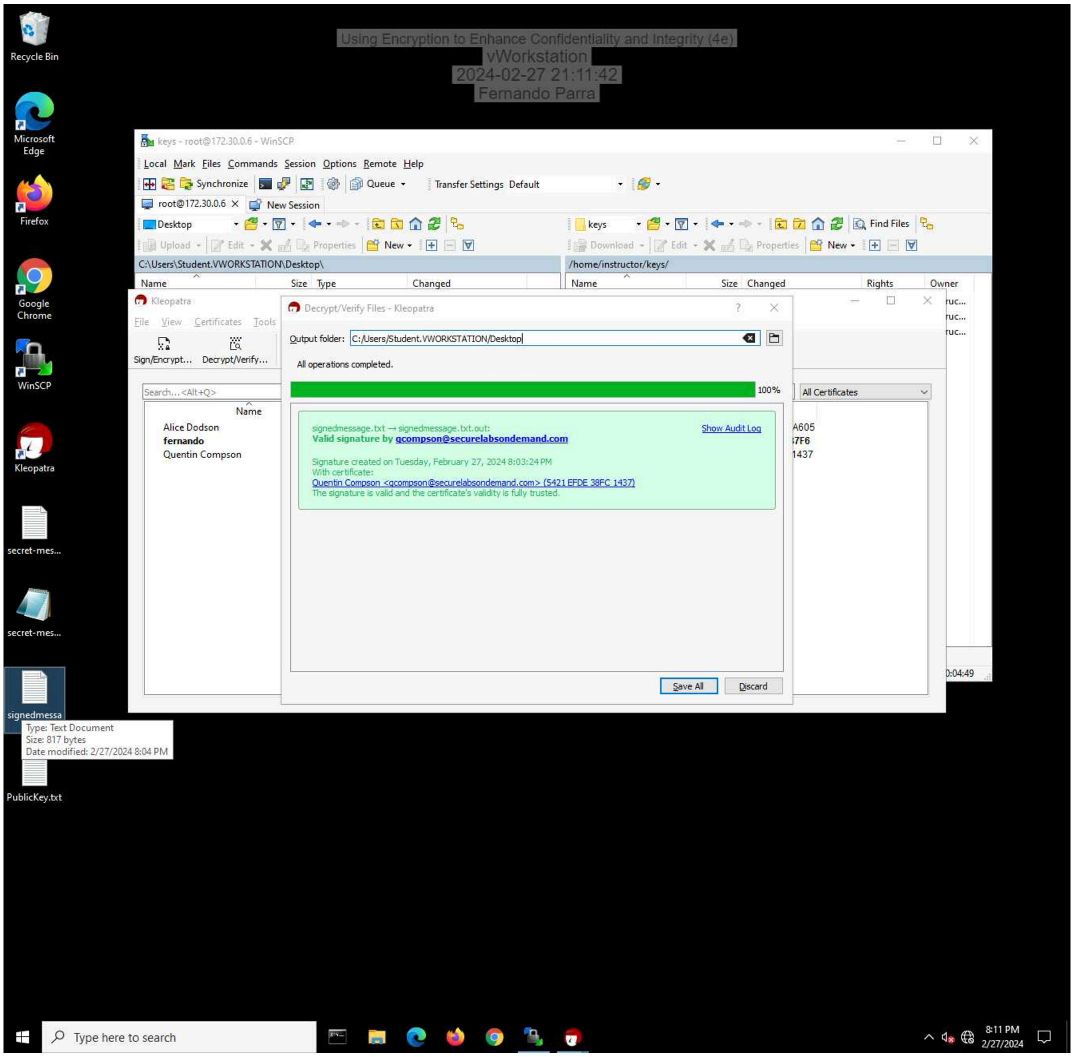
```
      2903F65A37124BCAA8716DF95421EFDE38FC1437
uid                      Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-28 [E] [expires: 2026-02-27]

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 2026-02-27
/home/instructor/.gnupg/pubring.kbx
-----------------------------------
pub   rsa3072 2024-02-28 [SC] [expires: 2026-02-27]
      2903F65A37124BCAA8716DF95421EFDE38FC1437
uid           [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-02-28 [E] [expires: 2026-02-27]

instructor@TargetLinux01:~$ touch unsignedmessage.txt
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
2024-02-27 21:11:42
Fernando Parra

Decrypt/Verify Files - Kleopatra

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

All operations completed.

100%

signedmessage.txt → signedmessage.txt.out:
Valid signature by qcompson@securelabsondemand.com

Signature created on Tuesday, February 27, 2024 8:03:24 PM
With certificate:
Quentin Compson <qcompson@securelabsondemand.com> (5421 EFDE 38FC 1437)
The signature is valid and the certificate's validity is fully trusted.

Type: Text Document
Size: 817 bytes
Date modified: 2/27/2024 8:04 PM