

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

Student:

Andrew Sweeney

Email:

asweene8@depaul.edu

Time on Task:

4 hours, 39 minutes

Progress:

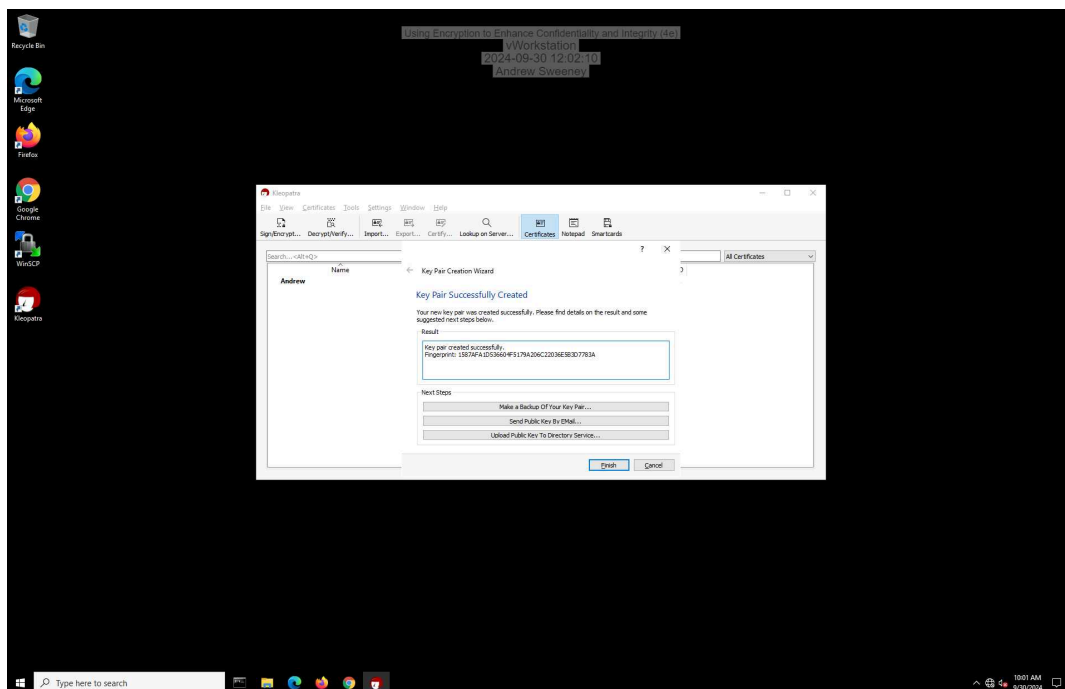
100%

Report Generated: Monday, September 30, 2024 at 3:41 PM

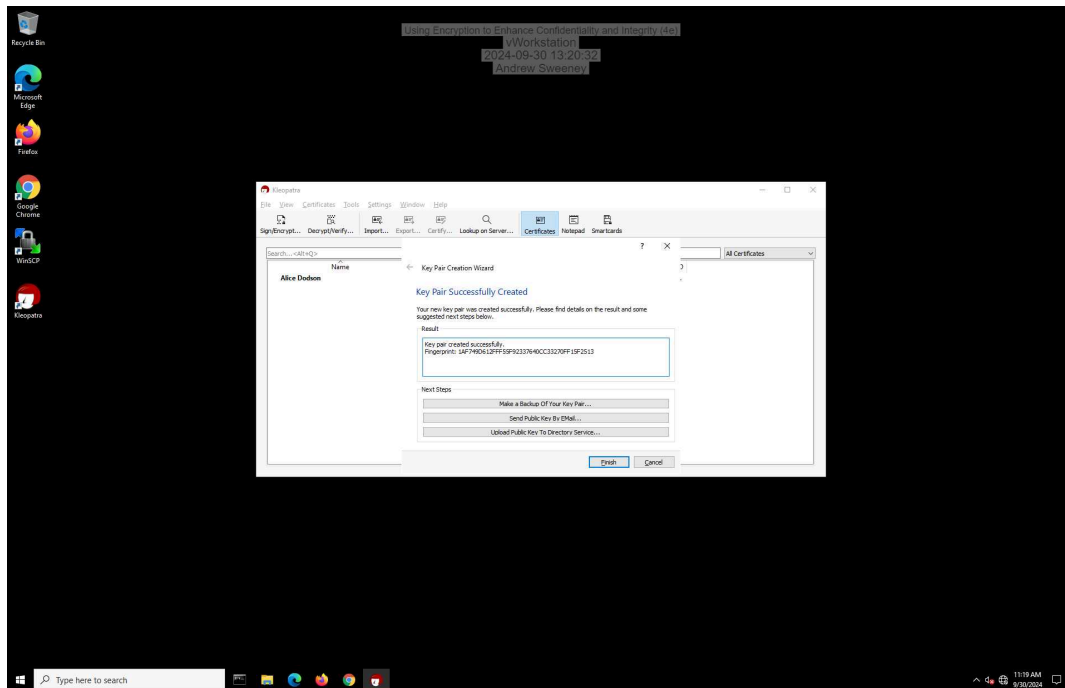
Section 1: Hands-On Demonstration

Part 1: Create and Exchange Asymmetric Encryption Keys

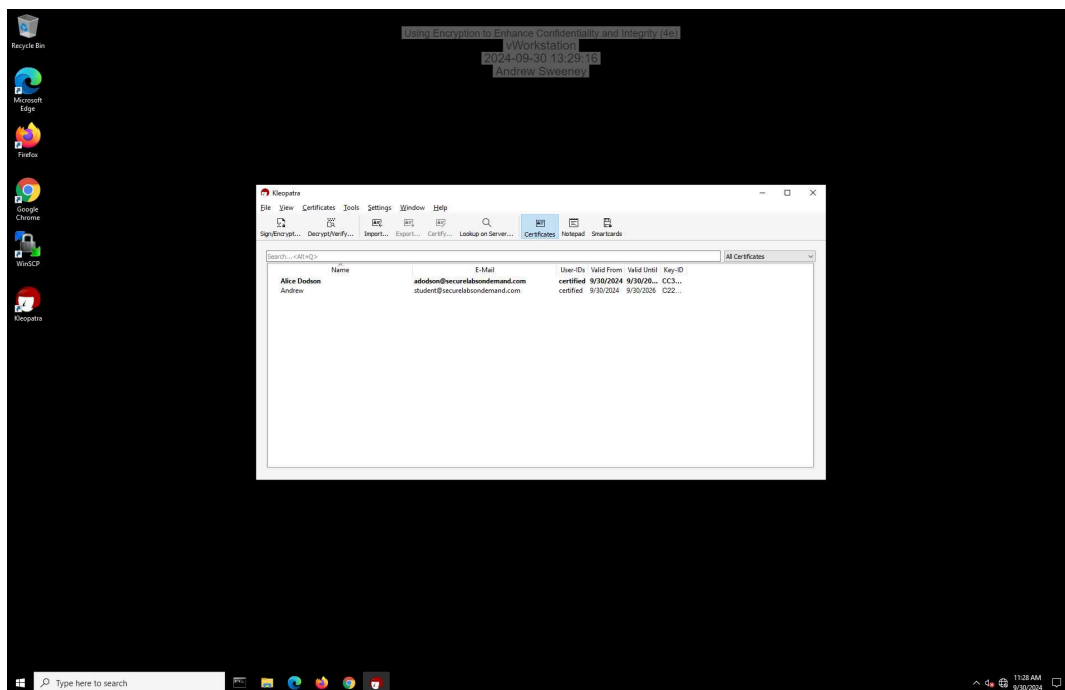
9. Make a screen capture showing the **fingerprint** for your key pair.



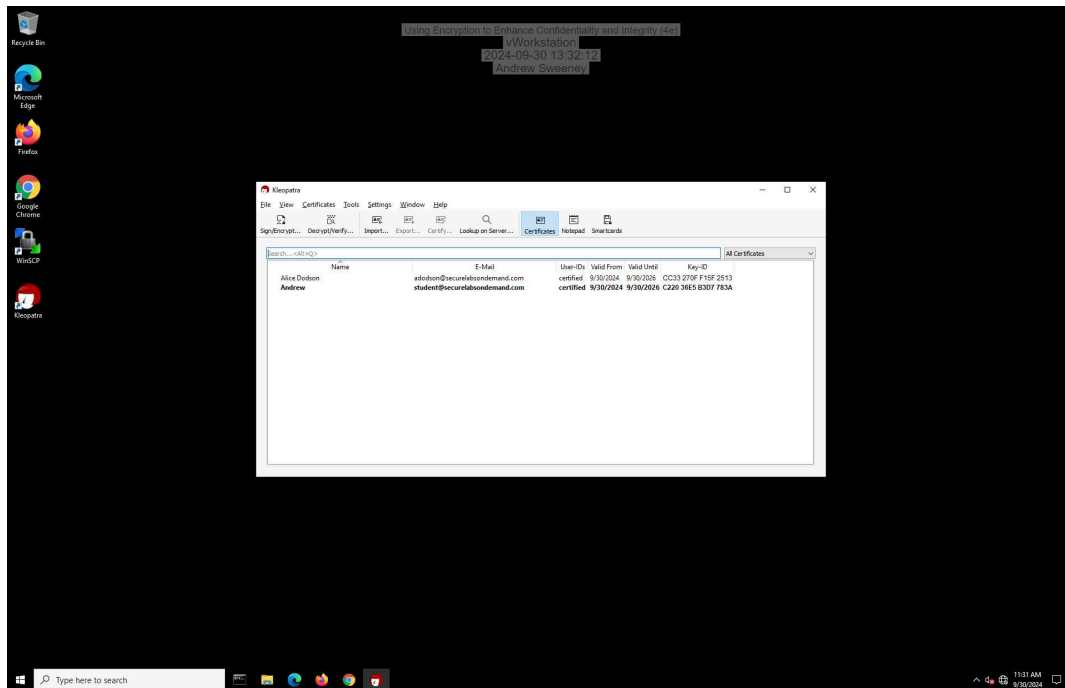
22. Make a screen capture showing the fingerprint for Alice's key pair.



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

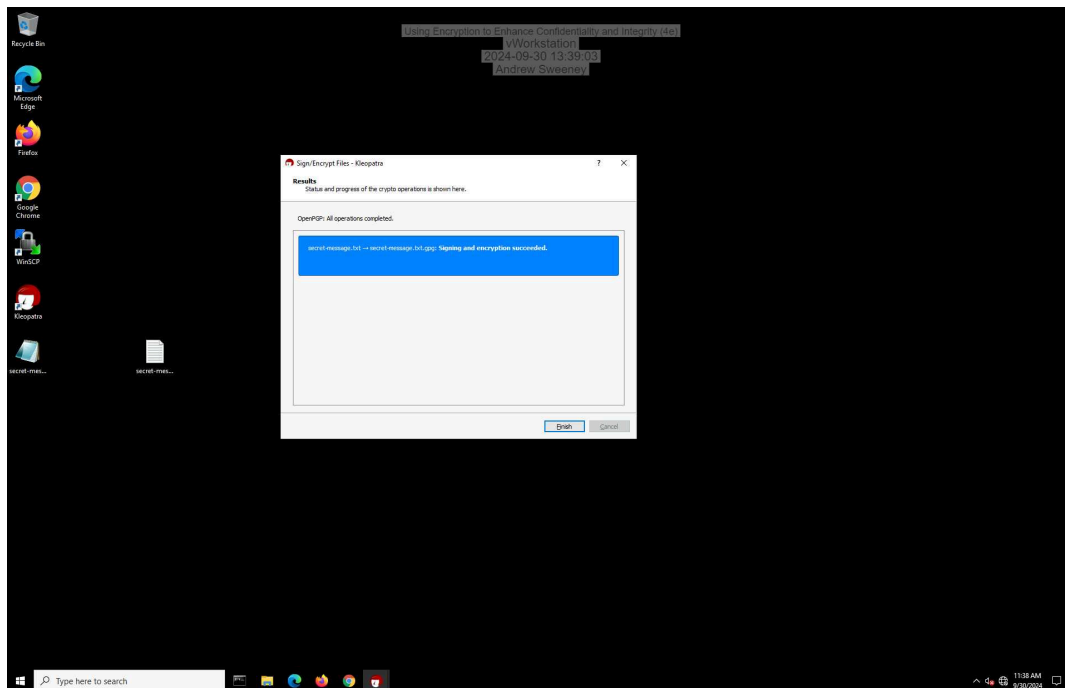


35. Make a screen capture showing Alice's public key in your certificate cache.



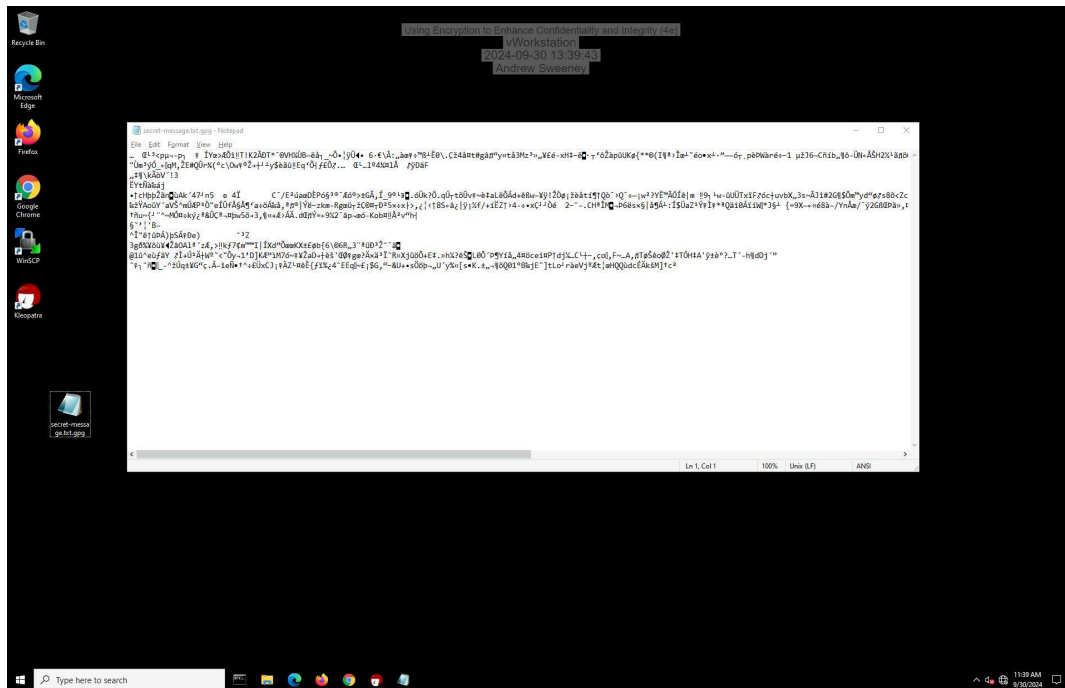
Part 2: Encrypt a File Using Asymmetric Encryption

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



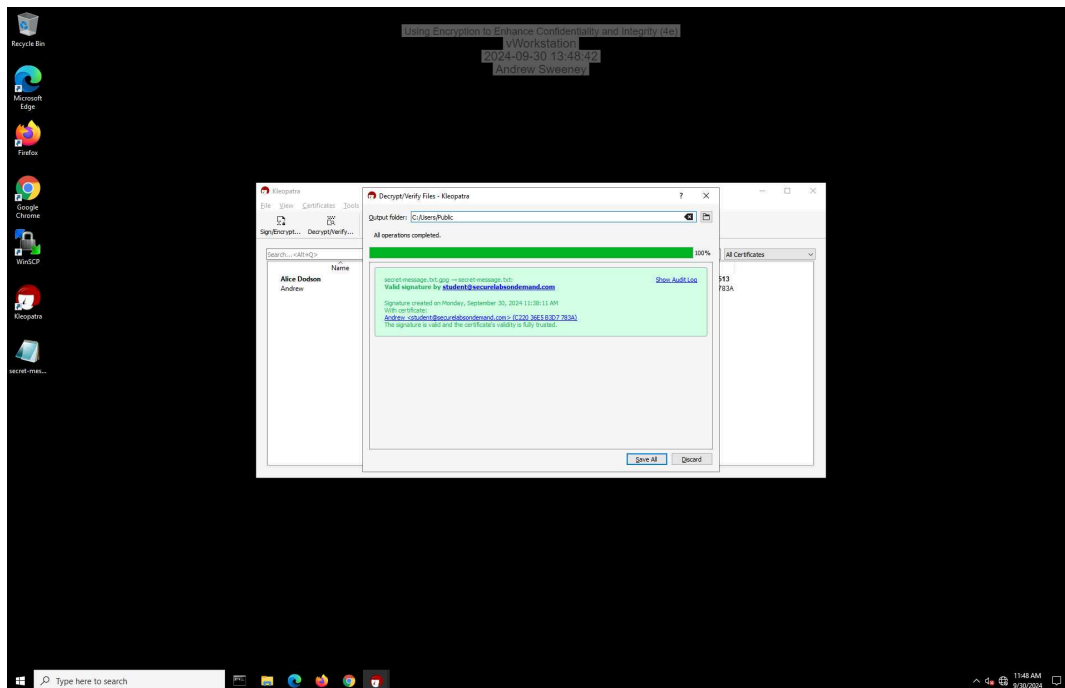
Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



Part 3: Decrypt a File Using Asymmetric Encryption

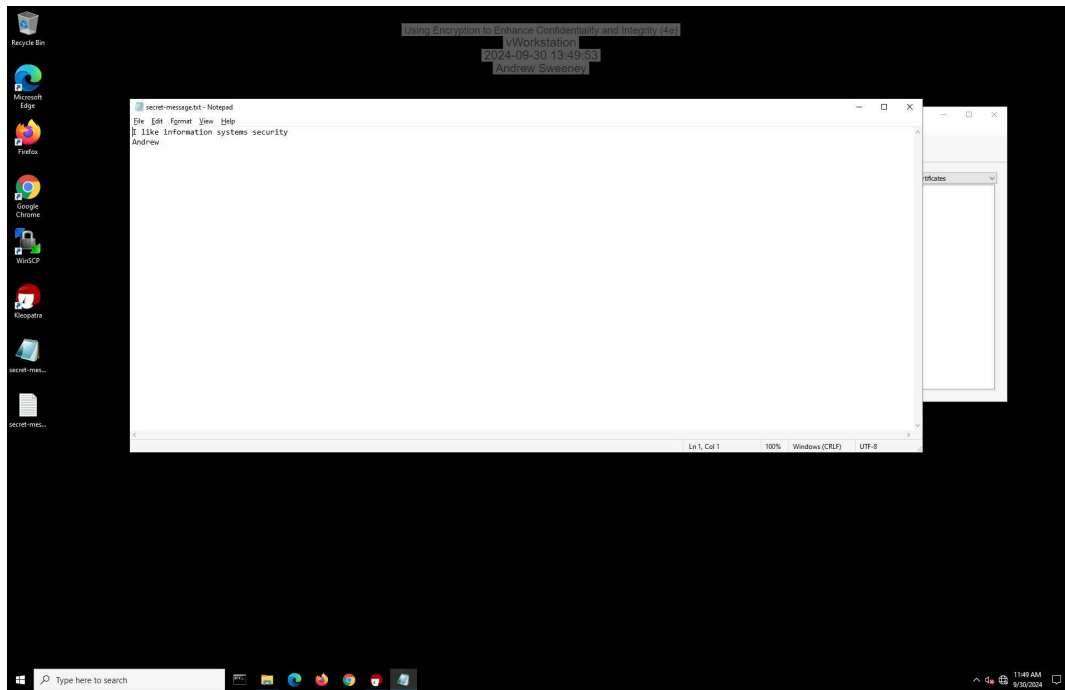
15. **Make a screen capture** showing the **Decrypt/Verify Files** window.



Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

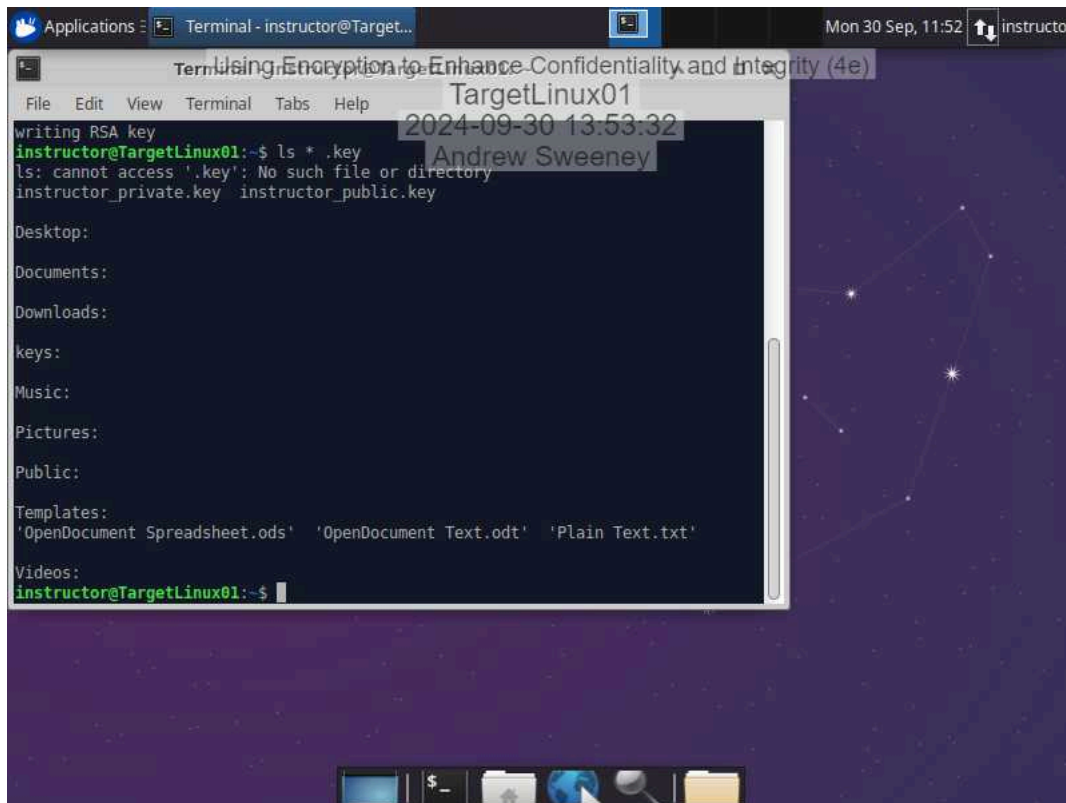
18. Make a screen capture showing the **decrypted secret-message.txt** file in Notepad.



Section 2: Applied Learning

Part 1: Create an Asymmetric Key Pair

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

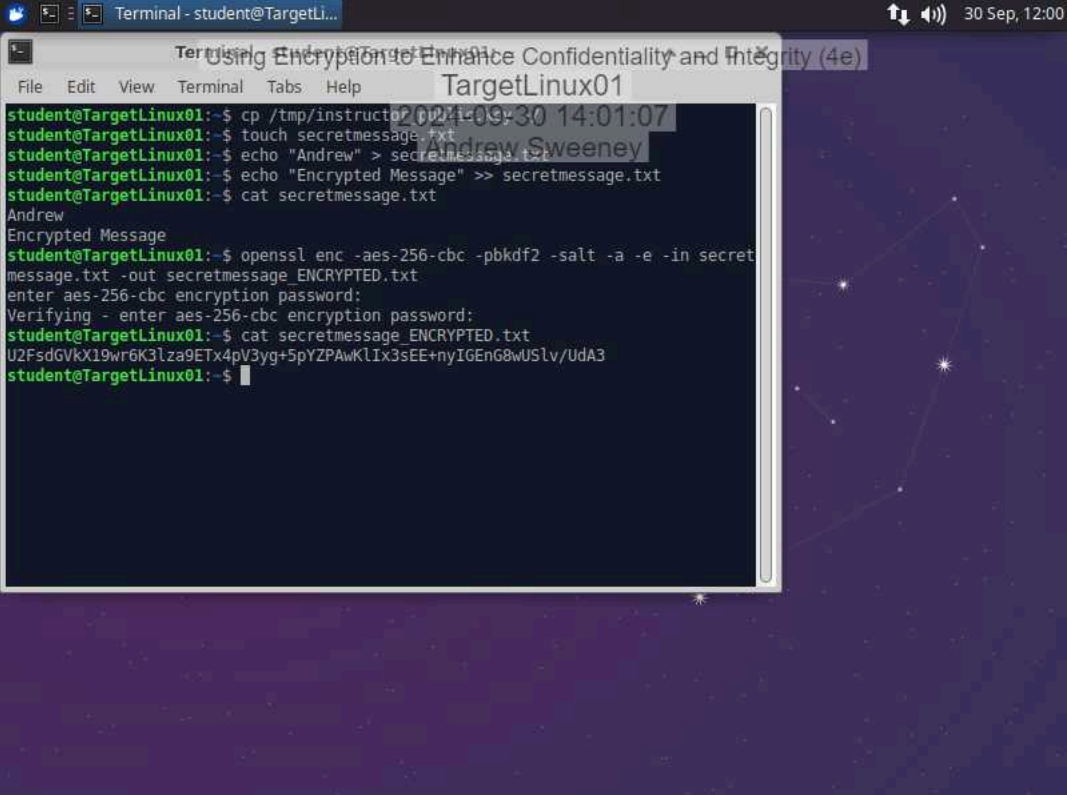


Part 2: Encrypt a File Using Symmetric Encryption

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

Drewdrew3!

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

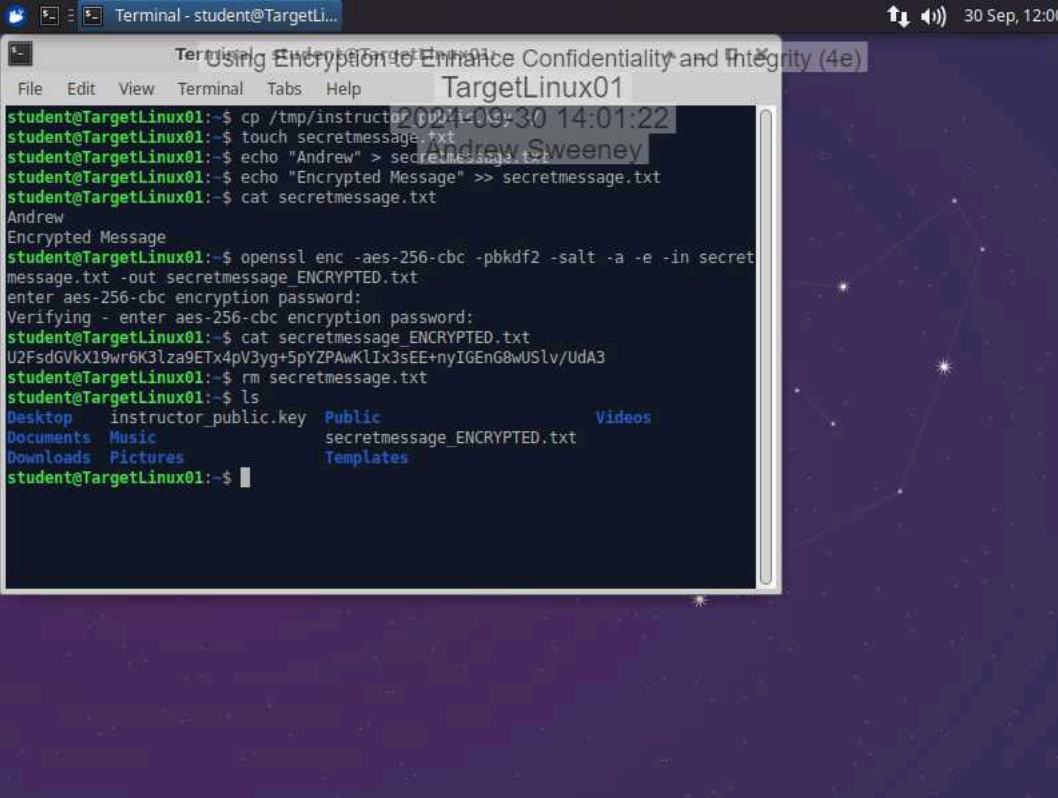


The screenshot shows a terminal window titled "Terminal - student@TargetLinux01" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output is as follows:

```
student@TargetLinux01:~$ cp /tmp/instructor01/secretmessage.txt .
student@TargetLinux01:~$ touch secretmessage.txt
student@TargetLinux01:~$ echo "Andrew" > secretmessage.txt
student@TargetLinux01:~$ echo "Encrypted Message" >> secretmessage.txt
student@TargetLinux01:~$ cat secretmessage.txt
Andrew
Encrypted Message
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secretmessage.txt -out secretmessage_ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat secretmessage_ENCRYPTED.txt
U2FsdGVkX19wr6K3lza9ETx4pV3yg+5pYZPAwKl1x3sEE+nyIGEnG8wUSlv/UdA3
student@TargetLinux01:~$
```

The background of the terminal window features a dark blue space-themed wallpaper with a constellation of stars and a faint outline of a constellation.

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



The screenshot shows a terminal window titled "Terminal - student@TargetLinux01" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output is as follows:

```
student@TargetLinux01:~$ cp /tmp/instructor_public.key .
student@TargetLinux01:~$ touch secretmessage.txt
student@TargetLinux01:~$ echo "Andrew" > secretmessage.txt
student@TargetLinux01:~$ echo "Encrypted Message" >> secretmessage.txt
student@TargetLinux01:~$ cat secretmessage.txt
Andrew
Encrypted Message
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secretmessage.txt -out secretmessage_ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat secretmessage_ENCRYPTED.txt
U2FsdGVkX19wr6K3lza9ETx4pV3yg+5pYZPAwKlIx3sEE+nyIGEnG8wUSlv/UdA3
student@TargetLinux01:~$ rm secretmessage.txt
student@TargetLinux01:~$ ls
Desktop  instructor_public.key  Public  Videos
Documents  Music  secretmessage_ENCRYPTED.txt
Downloads  Pictures  Templates
```

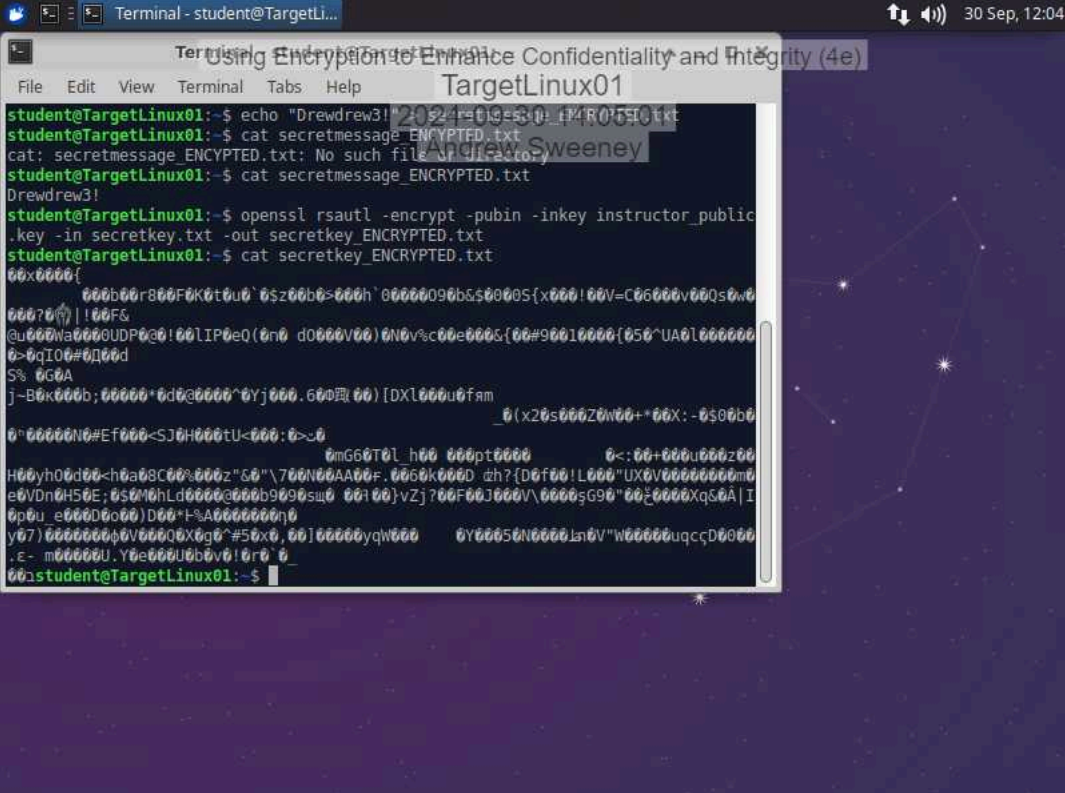
The terminal window is overlaid on a desktop background featuring a constellation of stars on a dark purple sky. A system clock in the top right corner displays "30 Sep, 12:00".

Part 3: Transfer and Decrypt a File Using Hybrid Cryptography

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



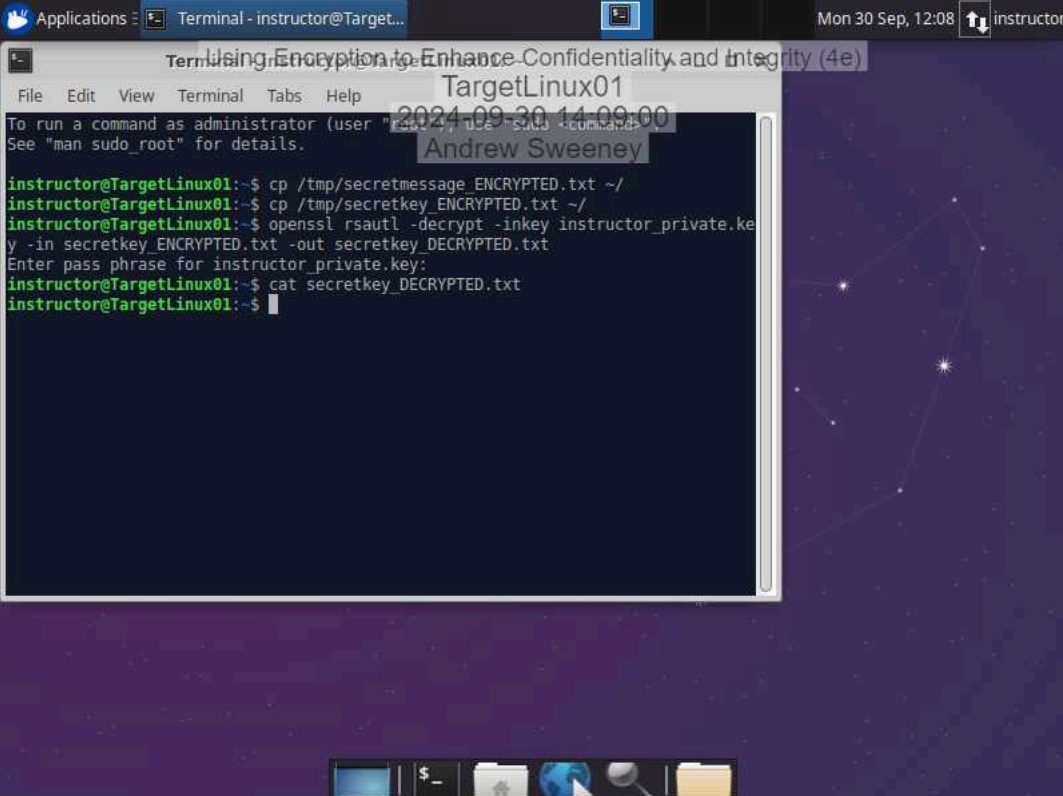
The screenshot shows a terminal window titled "Terminal - student@TargetLinux01" with a menu bar (File, Edit, View, Terminal, Tabs, Help) and a title bar (TargetLinux01). The terminal output is as follows:

```
student@TargetLinux01:~$ echo "Drewdrew3!" > secretmessage.txt
student@TargetLinux01:~$ cat secretmessage_ENCRYPTED.txt
cat: secretmessage_ENCRYPTED.txt: No such file or directory
student@TargetLinux01:~$ cat secretmessage_ENCRYPTED.txt
Drewdrew3!
student@TargetLinux01:~$ openssl rsautl -encrypt -pubin -inkey instructor_public
.key -in secretkey.txt -out secretkey_ENCRYPTED.txt
student@TargetLinux01:~$ cat secretkey_ENCRYPTED.txt
00x0000{
  000b00r800F0K0t0u0'0$z00b0>000h'00000090b0$0000S{x000!00V=C06000v00Qs0w0
  0007000)!00F&
  @u000Wa0000UDP0@0!00IP0e0(0n0 d000V00)0N0v%00e000S{00#90010000{050^UA0l000000
  0>0qIO0#0D00d
  S% 0G0A
  j-B0k000b;00000*0d0@0000^0Yj000.6000(00)[DXl000u0fjam
  0(x20s000Z0n00+*00X:-0$00b0
  0^00000N0#Ef000<SJ0H000tU<000:0>>0
  0mG60T0L_h00 000pt0000 0<:00+000u000z00
  H00yh00d00<h0a08C00%000z"00"\700N00AA00F.0060k000D @h?{D0f00!L000"UX0V00000000m0
  e0VDn0H50E;0$0M0hLd00000000b9000suj0 00100}vZj?00F00J000V\0000$G90"000000XqS0A|I
  0p0u_e000D0o00)D00"F%A0000000n0
  y07)00000000V000Q0X0g0"#50x0,00]00000yqW000 0Y00050N0000Jn0V"W00000uqcqCD0000
  .E- m00000U.Y0e000U0b0v0!0r0`0_
  00student@TargetLinux01:~$
```

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



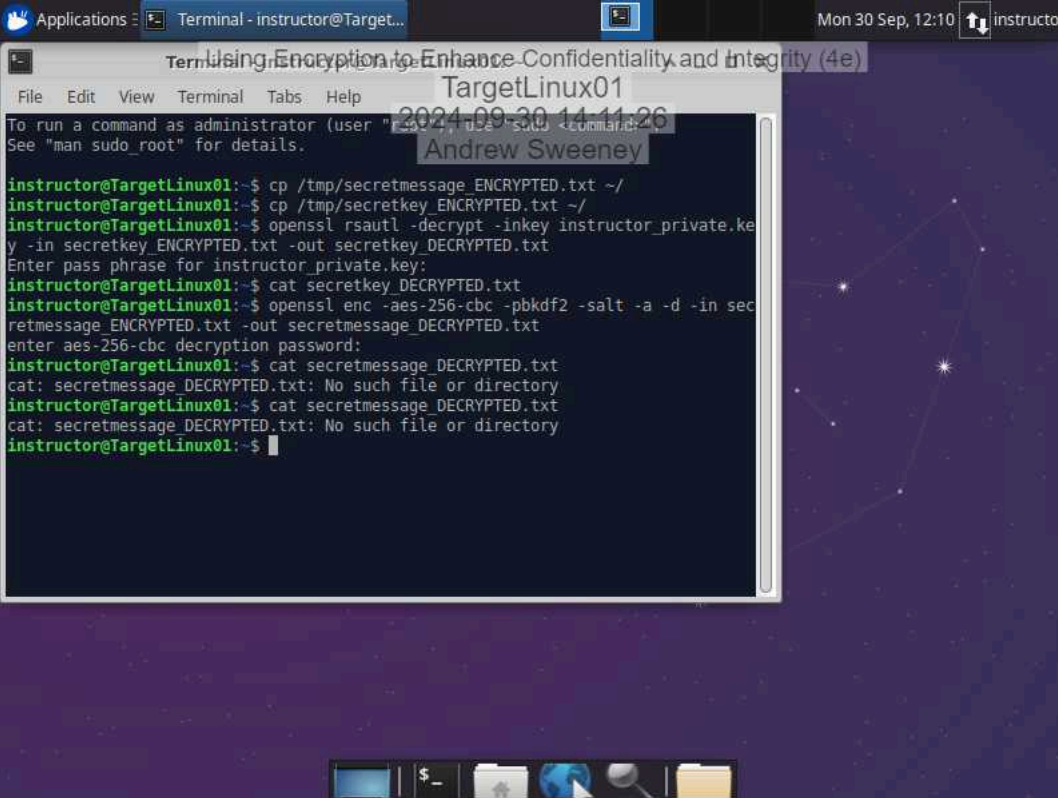
```
Applications ▢ Terminal - instructor@Target... Mon 30 Sep, 12:08 instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-09-30 14:09:00
Andrew Sweeney
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

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
instructor@TargetLinux01:~$
```

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



The screenshot shows a terminal window titled "Terminal - instructor@Target..." with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output shows the following commands and results:

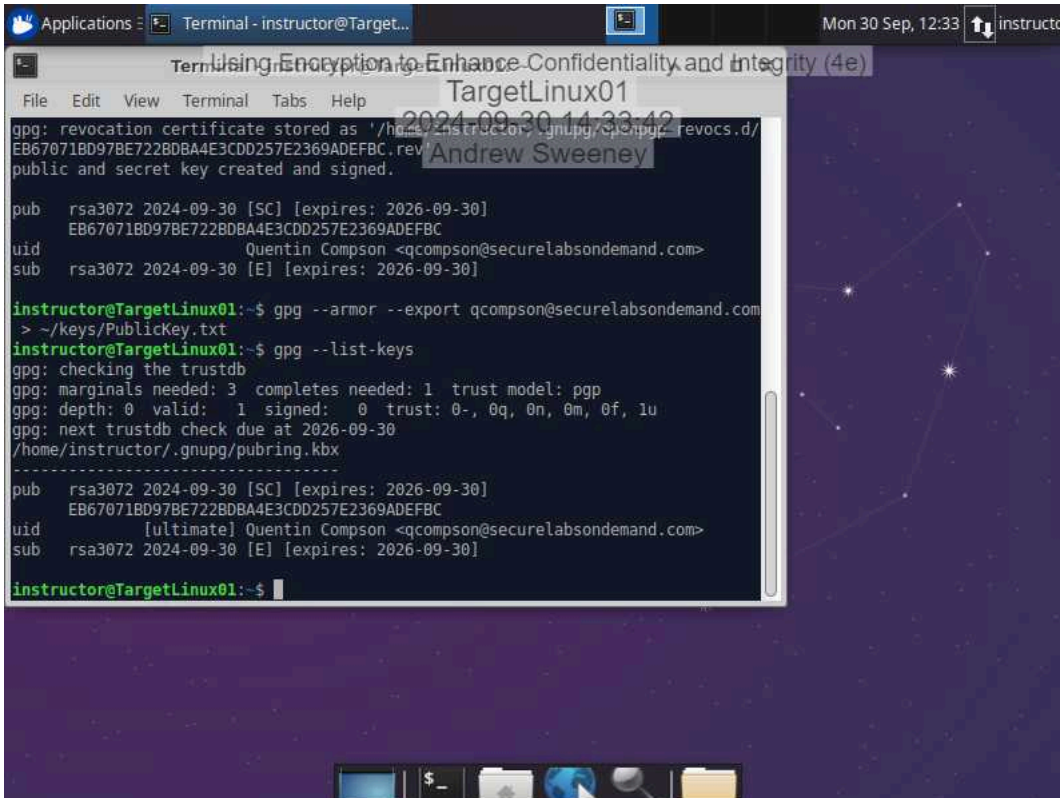
```
instructor@TargetLinux01:~$ cp /tmp/secretmessage_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ cp /tmp/secretkey_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_private.ke
y -in secretkey_ENCRYPTED.txt -out secretkey_DECRYPTED.txt
Enter pass phrase for instructor_private.key:
instructor@TargetLinux01:~$ cat secretkey_DECRYPTED.txt
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
cat: secretmessage_DECRYPTED.txt: No such file or directory
instructor@TargetLinux01:~$ cat secretmessage_DECRYPTED.txt
cat: secretmessage_DECRYPTED.txt: No such file or directory
instructor@TargetLinux01:~$
```

Overlaid on the terminal window is a semi-transparent box containing the text: "Using Encryption to Enhance Confidentiality and Integrity (4e)", "TargetLinux01", "2024-09-30 14:11:26", and "Andrew Sweeney". The desktop background is a dark purple space-themed wallpaper with a constellation. The taskbar at the bottom shows icons for a terminal, file manager, web browser, and other applications.

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.



The screenshot shows a terminal window titled "Terminal - instructor@TargetLinux01" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output shows the following commands and results:

```
gpg: revocation certificate stored as '/home/instructor/.gnupg/openpgp-revocs.d/EB67071B097BE722BD8A4E3CDD257E2369ADEFBC.rev'
public and secret key created and signed.

pub  rsa3072 2024-09-30 [SC] [expires: 2026-09-30]
     EB67071B097BE722BD8A4E3CDD257E2369ADEFBC
uid           Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2024-09-30 [E] [expires: 2026-09-30]

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 2026-09-30
/home/instructor/.gnupg/pubring.kbx
-----
pub  rsa3072 2024-09-30 [SC] [expires: 2026-09-30]
     EB67071B097BE722BD8A4E3CDD257E2369ADEFBC
uid           [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2024-09-30 [E] [expires: 2026-09-30]

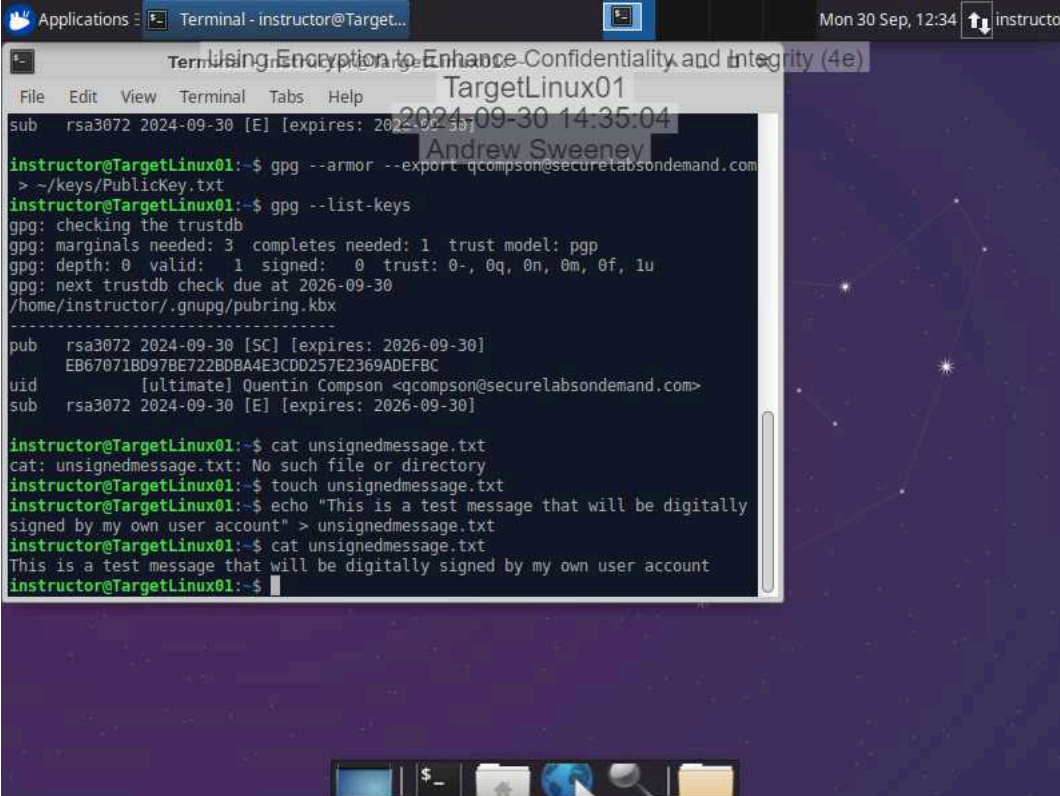
instructor@TargetLinux01:~$
```

Overlaid on the terminal window is a semi-transparent box containing the text: "TargetLinux01", "2024-09-30 14:33:42", and "Andrew Sweeney". The desktop background is a dark purple space-themed wallpaper with a constellation of stars.

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



```
Applications - Terminal - instructor@TargetLinux01
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-09-30 14:35:04
Andrew Sweeney
sub rsa3072 2024-09-30 [E] [expires: 2026-09-30]

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 2026-09-30
/home/instructor/.gnupg/pubring.kbx
-----
pub rsa3072 2024-09-30 [SC] [expires: 2026-09-30]
   EB67071B097BE722BDBA4E3CD0257E2369ADEFBC
uid [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub rsa3072 2024-09-30 [E] [expires: 2026-09-30]

instructor@TargetLinux01:~$ cat unsignedmessage.txt
cat: unsignedmessage.txt: No such file or directory
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

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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

