

# Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

Student:

Yengkong Sayaovong

Email:

ysayaovo@asu.edu

Time on Task:

0 hours, 52 minutes

Progress:

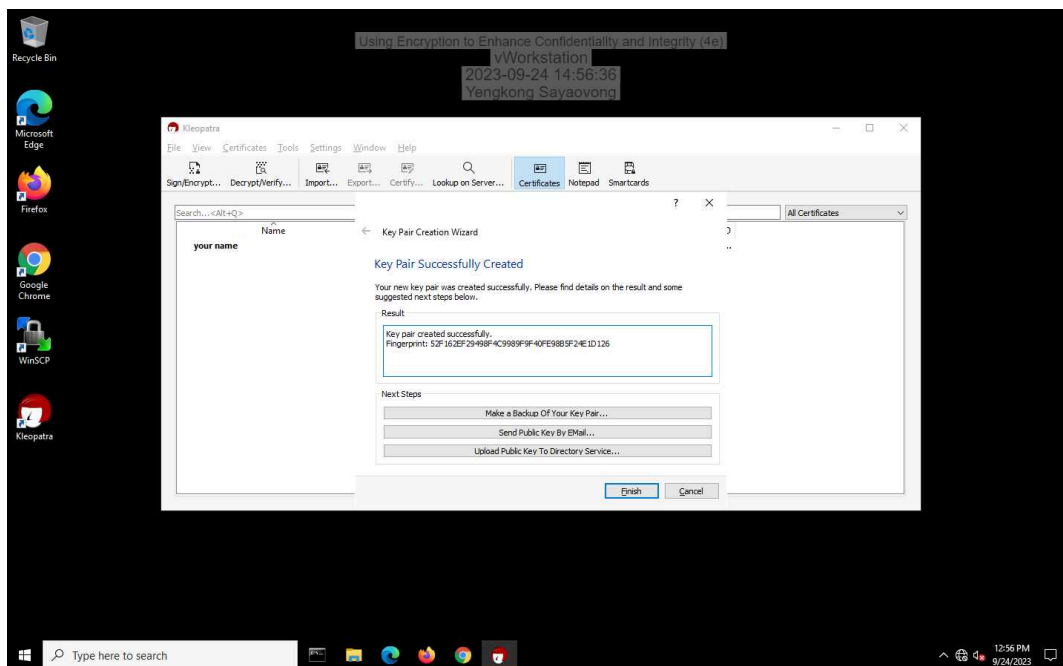
83%

Report Generated: Sunday, September 24, 2023 at 4:40 PM

## Section 1: Hands-On Demonstration

### Part 1: Create and Exchange Asymmetric Encryption Keys

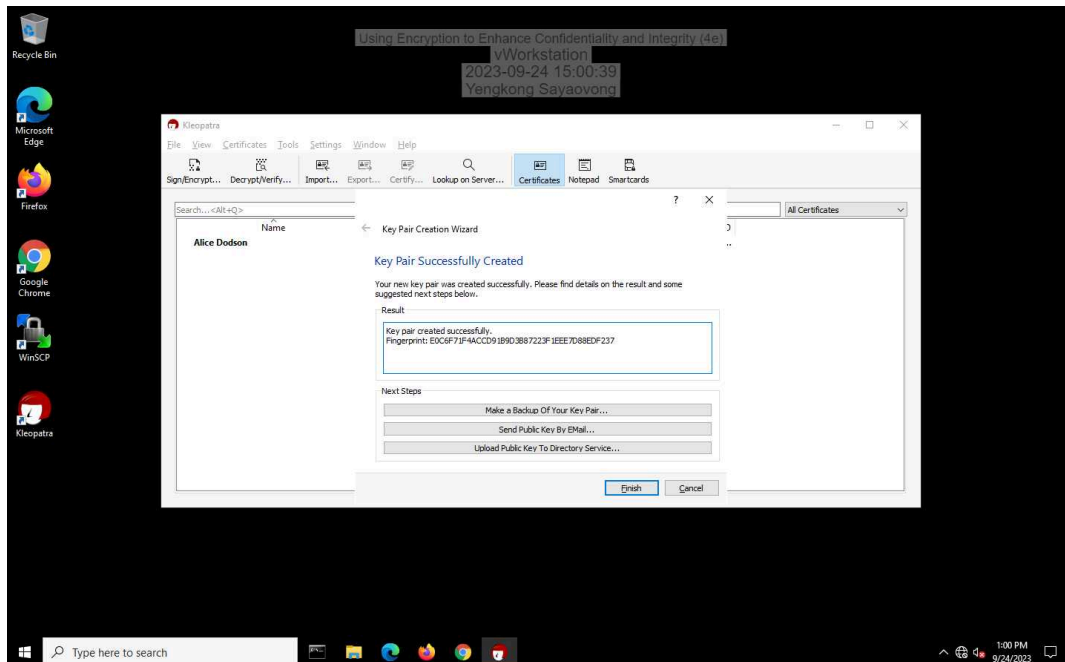
9. Make a screen capture showing the **fingerprint** for your key pair.



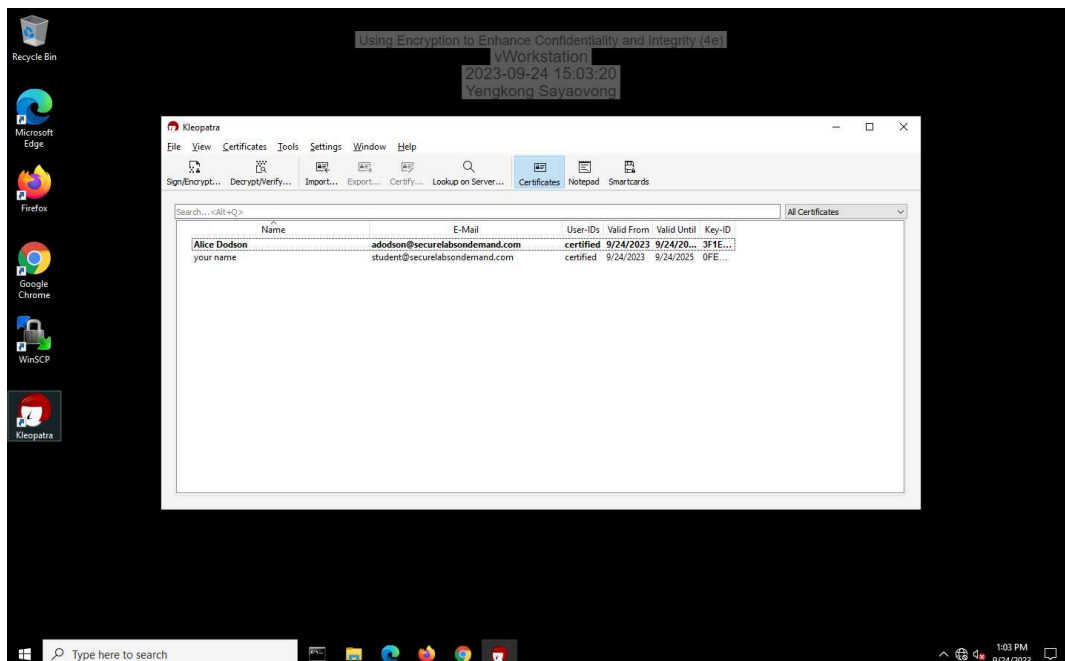
# Using Encryption to Enhance Confidentiality and Integrity (4e)

## Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



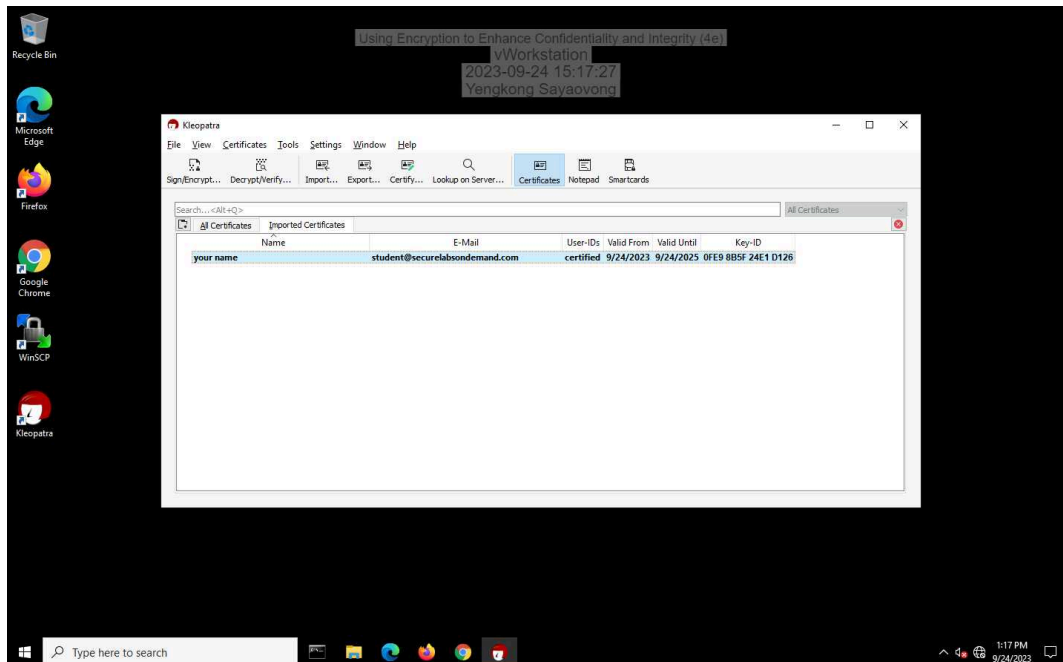
30. Make a screen capture showing your public key in Alice's certificate cache.



# Using Encryption to Enhance Confidentiality and Integrity (4e)

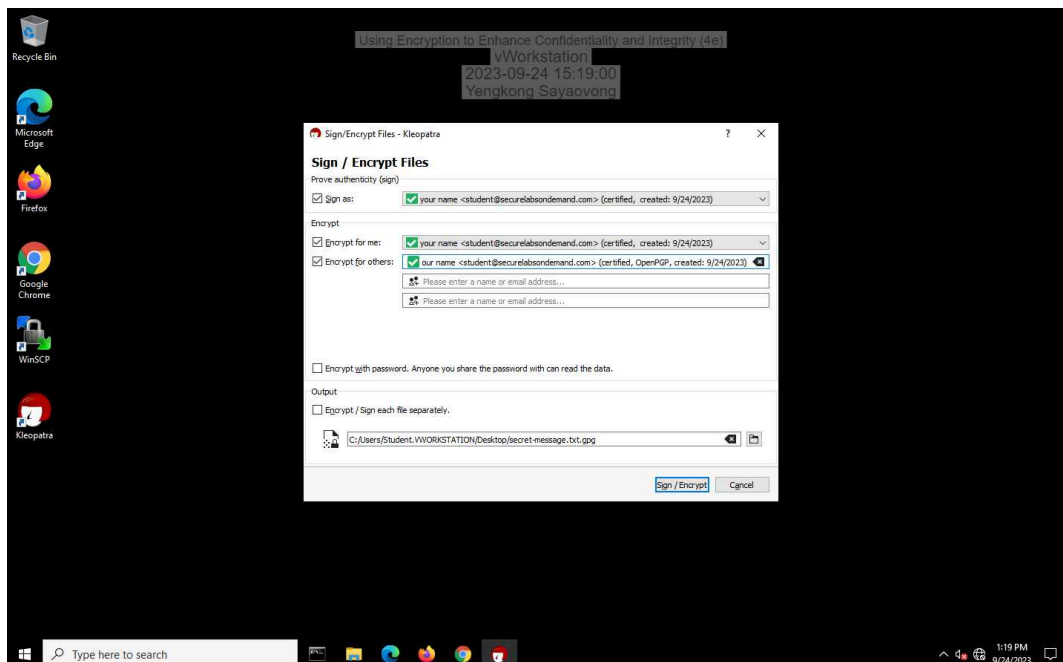
Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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

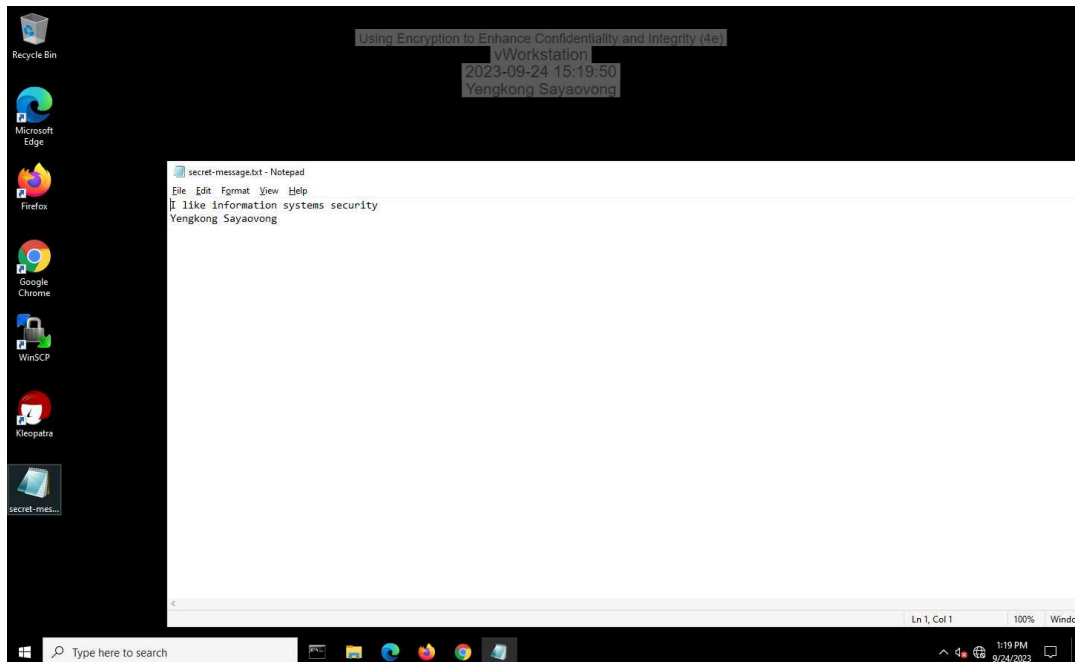


## Part 2: Encrypt a File Using Asymmetric Encryption

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



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.

Incomplete

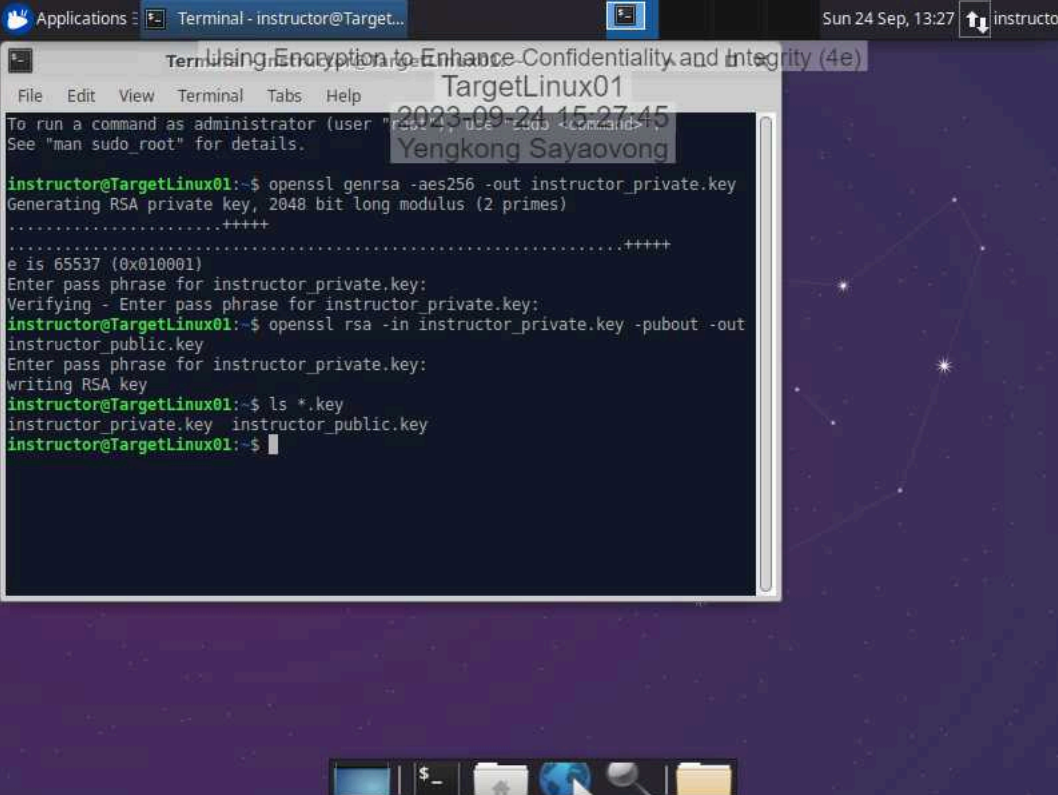
18. Make a screen capture showing the **decrypted secret-message.txt** file in Notepad.

Incomplete

## Section 2: Applied Learning

### Part 1: Create an Asymmetric Key Pair

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



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

```
instructor@TargetLinux01:~$ openssl genrsa -aes256 -out instructor_private.key
Generating RSA private key, 2048 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:~$
```

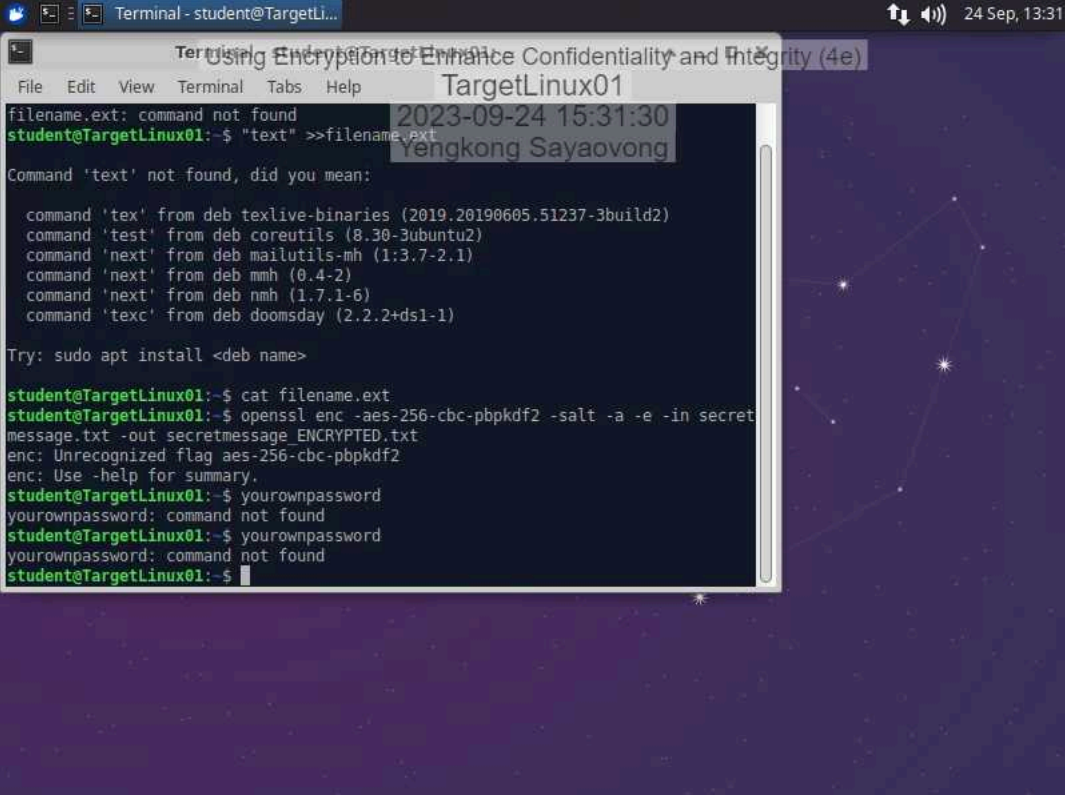
Overlaid on the terminal window is a semi-transparent box containing the text: "TargetLinux01", "2023-09-24 15:27:45", and "Yengkong Sayaovong". The desktop background is a dark purple space-themed wallpaper with a constellation of stars.

### 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.

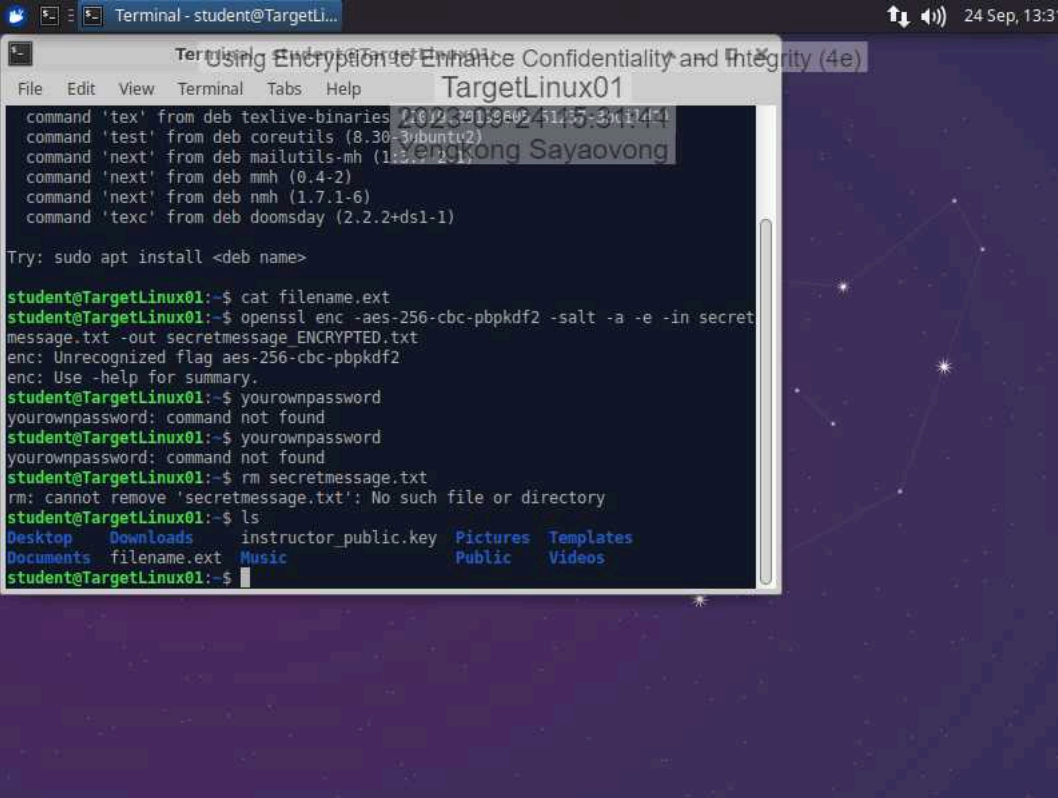


The screenshot shows a terminal window titled "Terminal - student@TargetLinux01" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output is as follows:

```
filename.ext: command not found
student@TargetLinux01:~$ "text" >>filename.ext
Command 'text' not found, did you mean:
  command 'tex' from deb texlive-binaries (2019.20190605.51237-3build2)
  command 'test' from deb coreutils (8.30-3ubuntu2)
  command 'next' from deb mailutils-mh (1:3.7-2.1)
  command 'next' from deb mmh (0.4-2)
  command 'next' from deb nmh (1.7.1-6)
  command 'texc' from deb doomsday (2.2.2+ds1-1)
Try: sudo apt install <deb name>
student@TargetLinux01:~$ cat filename.ext
student@TargetLinux01:~$ openssl enc -aes-256-cbc-pbkdf2 -salt -a -e -in secret
message.txt -out secretmessage_ENCRYPTED.txt
enc: Unrecognized flag aes-256-cbc-pbkdf2
enc: Use -help for summary.
student@TargetLinux01:~$ yourownpassword
yourownpassword: command not found
student@TargetLinux01:~$ yourownpassword
yourownpassword: command not found
student@TargetLinux01:~$
```

Overlaid on the terminal window is a semi-transparent box containing the text "2023-09-24 15:31:30" and "Yengkong Sayaovong". The background of the terminal window is a dark purple space-themed wallpaper with a constellation of stars.

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

A screenshot of a terminal window titled "Terminal - student@TargetLinux01". The window shows a list of installed packages and their versions, followed by a prompt to try the command "sudo apt install <deb name>". The user then runs "cat filename.ext", "openssl enc -aes-256-cbc-pbkdf2 -salt -a -e -in secretmessage.txt -out secretmessage.ENCRYPTED.txt", and "rm secretmessage.txt". The "ls" command is run, showing a directory listing of files and folders. The background of the terminal window is a dark blue space-themed wallpaper with a constellation of stars.

```
command 'tex' from deb texlive-binaries (2023.01-60241.5-3ubuntu4)
command 'test' from deb coreutils (8.30-3ubuntu2)
command 'next' from deb mailutils-mh (1:3.12-1)
command 'next' from deb mmh (0.4-2)
command 'next' from deb nmh (1.7.1-6)
command 'text' from deb doomsday (2.2.2+ds1-1)

Try: sudo apt install <deb name>

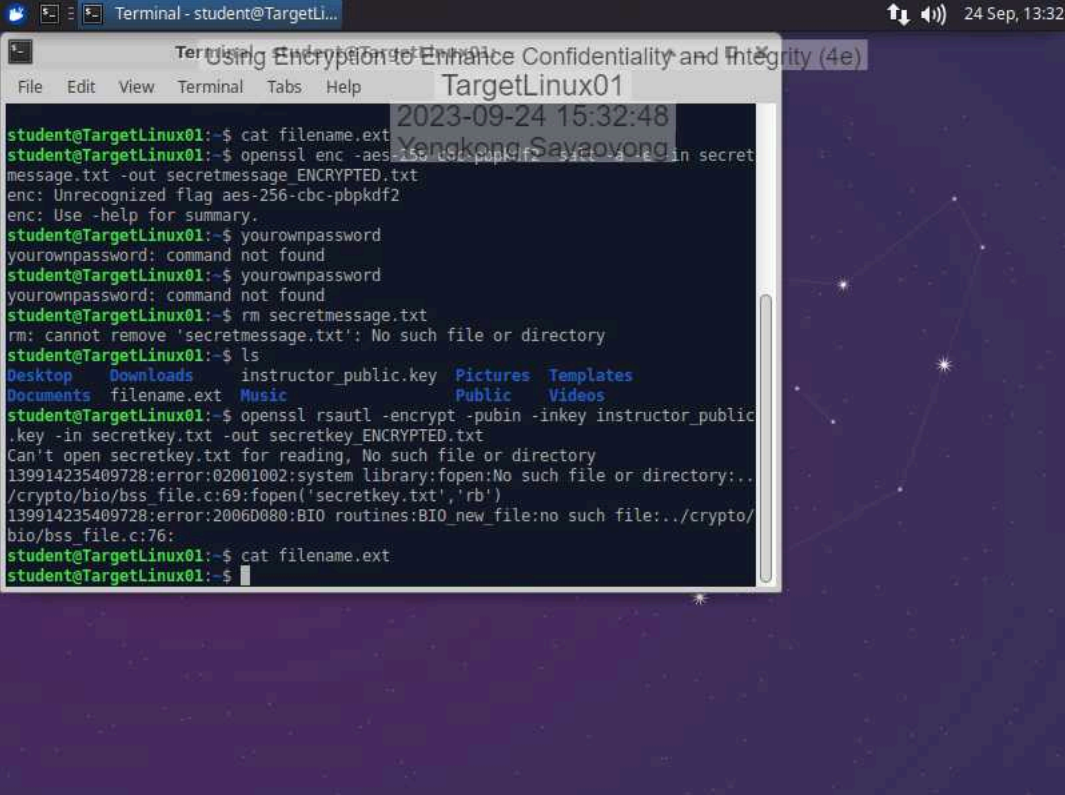
student@TargetLinux01:~$ cat filename.ext
student@TargetLinux01:~$ openssl enc -aes-256-cbc-pbkdf2 -salt -a -e -in secret
message.txt -out secretmessage.ENCRYPTED.txt
enc: Unrecognized flag aes-256-cbc-pbkdf2
enc: Use -help for summary.
student@TargetLinux01:~$ yourownpassword
yourownpassword: command not found
student@TargetLinux01:~$ yourownpassword
yourownpassword: command not found
student@TargetLinux01:~$ rm secretmessage.txt
rm: cannot remove 'secretmessage.txt': No such file or directory
student@TargetLinux01:~$ ls
Desktop  Downloads  instructor_public.key  Pictures  Templates
Documents  filename.ext  Music  Public  Videos
student@TargetLinux01:~$
```

### 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.



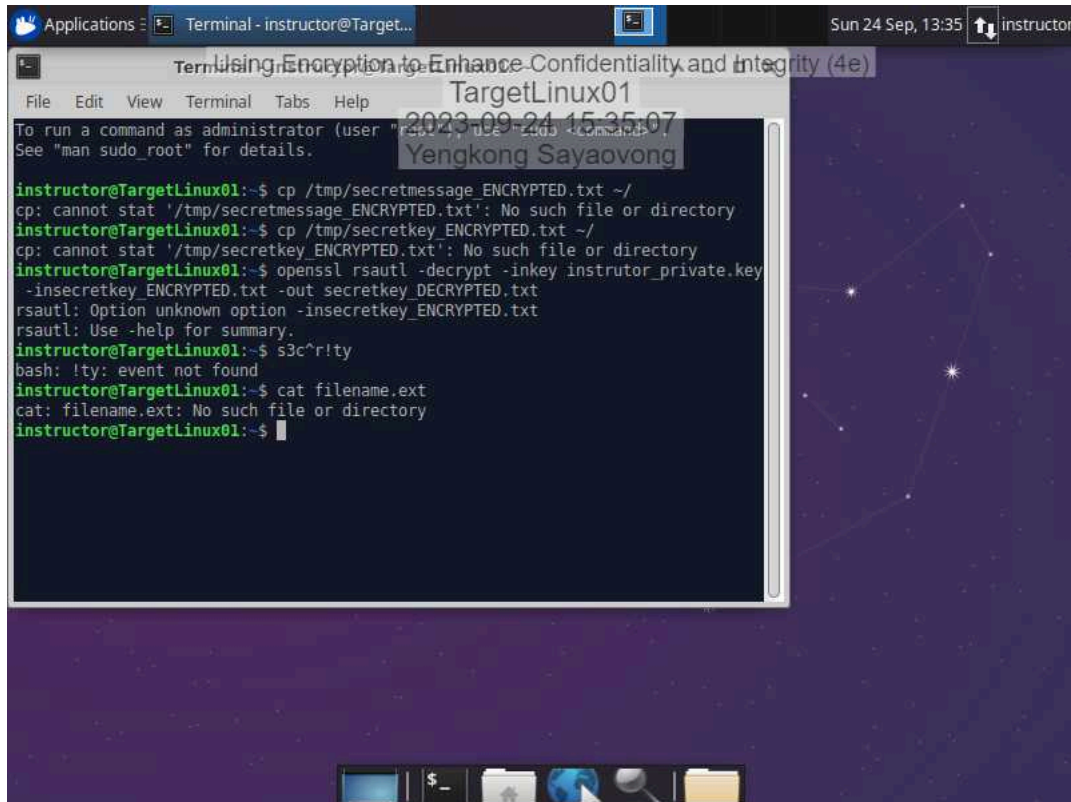
```
Terminal - student@TargetLinux01
2023-09-24 15:32:48
student@TargetLinux01:~$ cat filename.ext
student@TargetLinux01:~$ openssl enc -aes-128-cbc -pbkdf2 -iter 10000 -salt -in secretmessage.txt -out secretmessage_ENCRYPTED.txt
enc: Unrecognized flag aes-256-cbc-pbkdf2
enc: Use -help for summary.
student@TargetLinux01:~$ yourownpassword
yourownpassword: command not found
student@TargetLinux01:~$ yourownpassword
yourownpassword: command not found
student@TargetLinux01:~$ rm secretmessage.txt
rm: cannot remove 'secretmessage.txt': No such file or directory
student@TargetLinux01:~$ ls
Desktop  Downloads  instructor_public.key  Pictures  Templates
Documents  filename.ext  Music  Public  Videos
student@TargetLinux01:~$ openssl rsautl -encrypt -pubin -inkey instructor_public.key -in secretkey.txt -out secretkey_ENCRYPTED.txt
Can't open secretkey.txt for reading, No such file or directory
139914235409728:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('secretkey.txt','rb')
139914235409728:error:2006D080:BIIO routines:BIIO_new_file:no such file:../crypto/bio/bss_file.c:76:
student@TargetLinux01:~$ cat filename.ext
student@TargetLinux01:~$
```



## Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

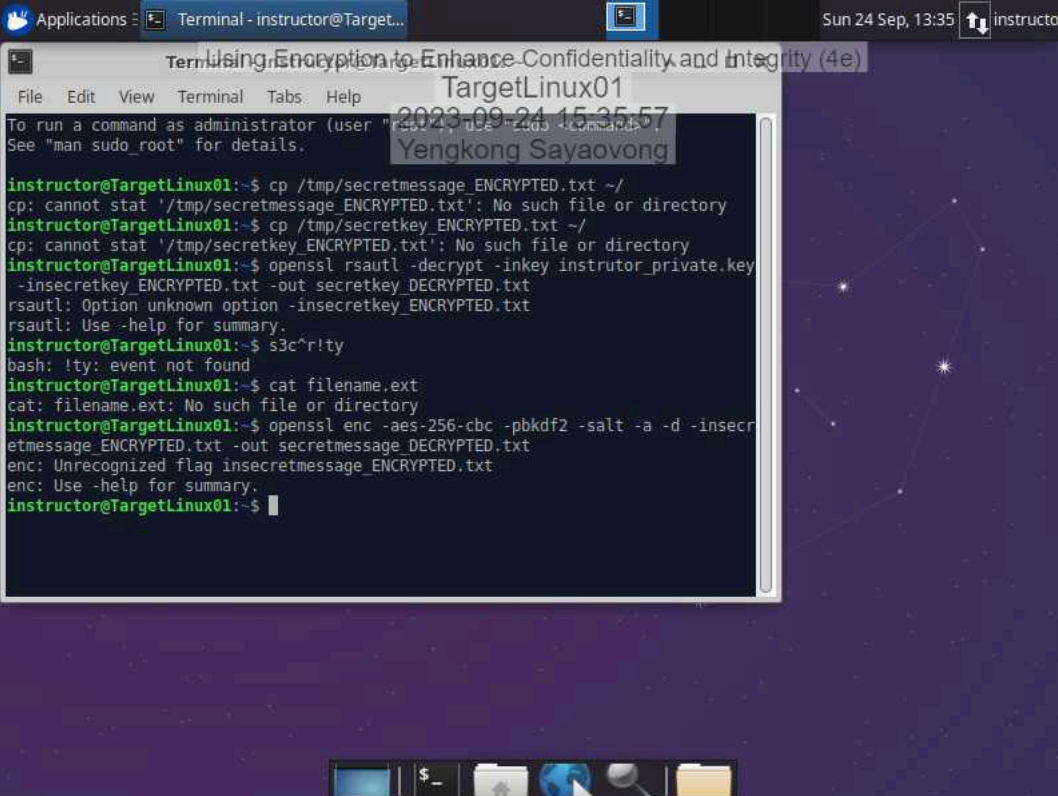
17. **Make a screen capture** showing the **decrypted contents of the secretkey\_DECRYPTED.txt file**.



## 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 dark background and light-colored text. The terminal output shows the following commands and their results:

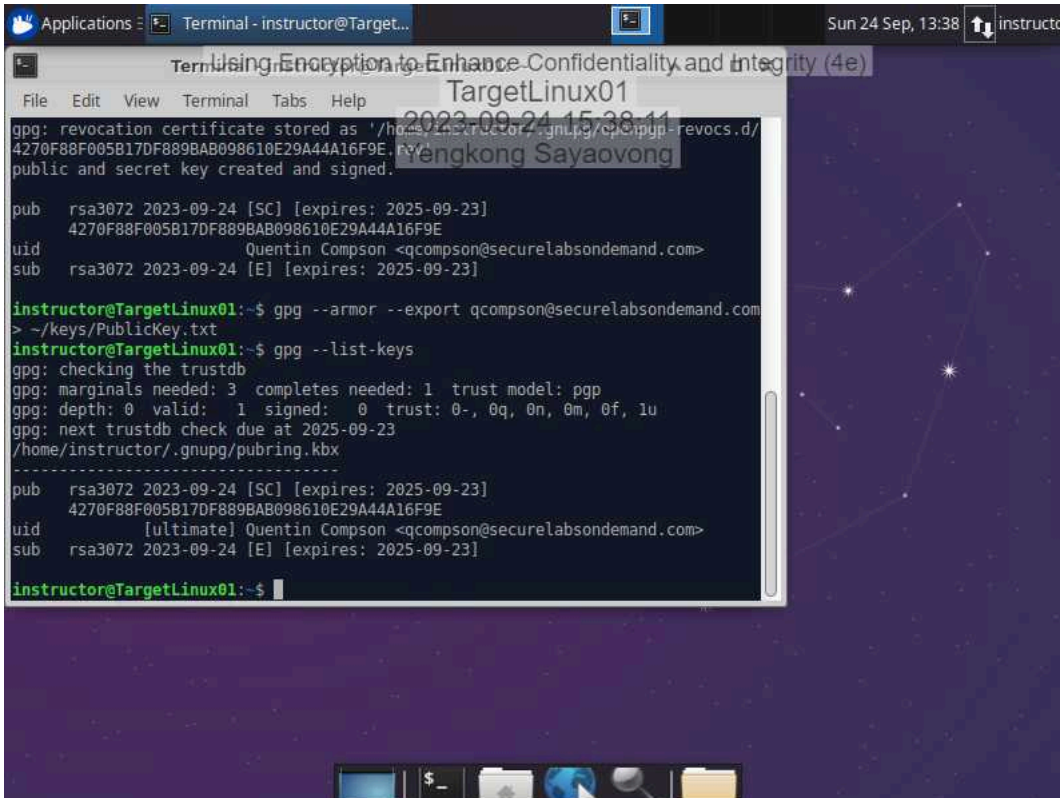
```
instructor@TargetLinux01:~$ cp /tmp/secretmessage_ENCRYPTED.txt ~/
cp: cannot stat '/tmp/secretmessage_ENCRYPTED.txt': No such file or directory
instructor@TargetLinux01:~$ cp /tmp/secretkey_ENCRYPTED.txt ~/
cp: cannot stat '/tmp/secretkey_ENCRYPTED.txt': No such file or directory
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_private.key
-insecretkey_ENCRYPTED.txt -out secretkey_DECRYPTED.txt
rsautl: Option unknown option -insecretkey_ENCRYPTED.txt
rsautl: Use -help for summary.
instructor@TargetLinux01:~$ s3c^r!ty
bash: !ty: event not found
instructor@TargetLinux01:~$ cat filename.ext
cat: filename.ext: No such file or directory
instructor@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -d -insecr
etmessage_ENCRYPTED.txt -out secretmessage_DECRYPTED.txt
enc: Unrecognized flag insecretmessage_ENCRYPTED.txt
enc: Use -help for summary.
instructor@TargetLinux01:~$
```

The terminal window is overlaid on a desktop background featuring a starry night sky with constellations. The desktop environment includes a top bar with the date "Sun 24 Sep, 13:35" and the username "instructor". A bottom taskbar shows icons for a terminal, a file manager, a web browser, and a search icon.

## 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/cmpgpg-revocs.d/4270F88F005B17DF889BAB098610E29A44A16F9E.rev'
public and secret key created and signed.

pub  rsa3072 2023-09-24 [SC] [expires: 2025-09-23]
     4270F88F005B17DF889BAB098610E29A44A16F9E
uid          Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2023-09-24 [E] [expires: 2025-09-23]

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 2025-09-23
/home/instructor/.gnupg/pubring.kbx
-----
pub  rsa3072 2023-09-24 [SC] [expires: 2025-09-23]
     4270F88F005B17DF889BAB098610E29A44A16F9E
uid          [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2023-09-24 [E] [expires: 2025-09-23]

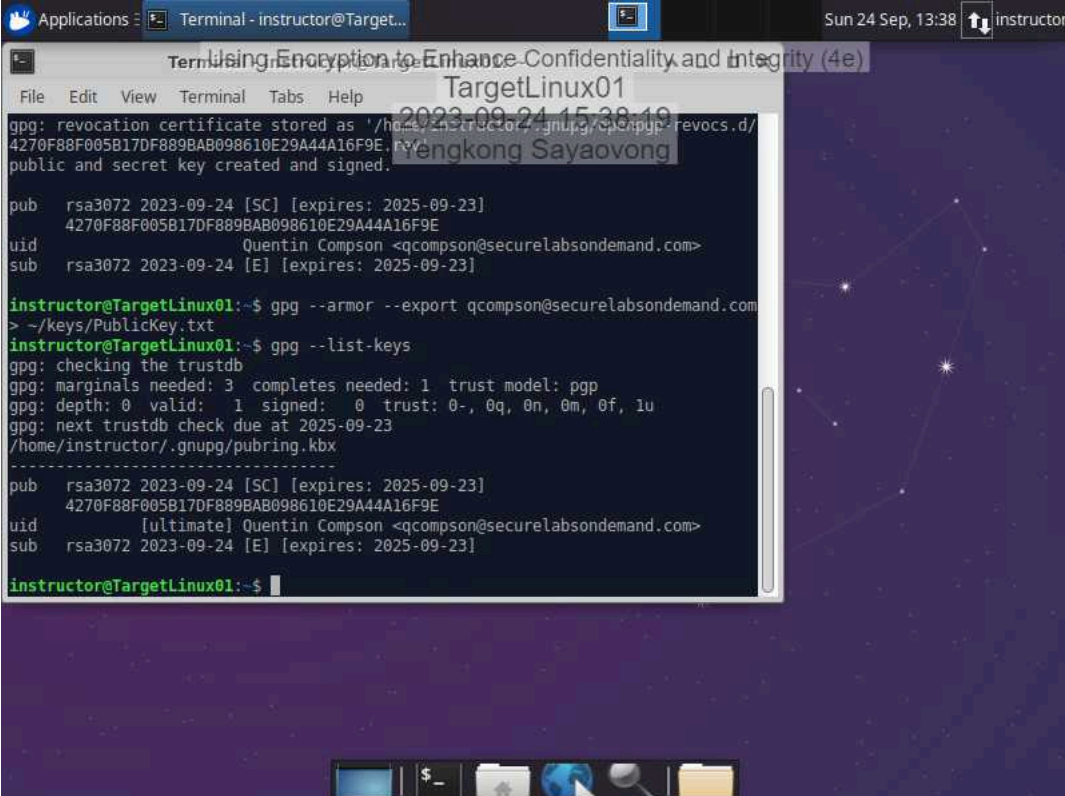
instructor@TargetLinux01:~$
```

Overlaid on the terminal output is a semi-transparent box containing the text: "TargetLinux01", "2023-09-24 15:38:11", and "Pengkong Sayaovong". The desktop background is a dark purple space-themed wallpaper with a constellation of stars. The system tray at the bottom shows icons for a terminal, a file manager, a globe, a magnifying glass, and a folder.

## 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 | Sun 24 Sep, 13:38 | instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2023-09-24 15:38:19
Yengkong Sayaovong

gpg: revocation certificate stored as '/home/instructor/.gnupg/openpgp-revocs.d/
4270F88F005B17DF889BAB098610E29A44A16F9E.rev'
public and secret key created and signed.

pub  rsa3072 2023-09-24 [SC] [expires: 2025-09-23]
     4270F88F005B17DF889BAB098610E29A44A16F9E
uid          Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2023-09-24 [E] [expires: 2025-09-23]

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 2025-09-23
/home/instructor/.gnupg/pubring.kbx
-----
pub  rsa3072 2023-09-24 [SC] [expires: 2025-09-23]
     4270F88F005B17DF889BAB098610E29A44A16F9E
uid          [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2023-09-24 [E] [expires: 2025-09-23]

instructor@TargetLinux01:~$
```

## Part 2: Verify the Digital Signature Using Kleopatra

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

Incomplete