

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

Student:

Mustafa Shah

Email:

ho3168@wayne.edu

Time on Task:

2 hours, 23 minutes

Progress:

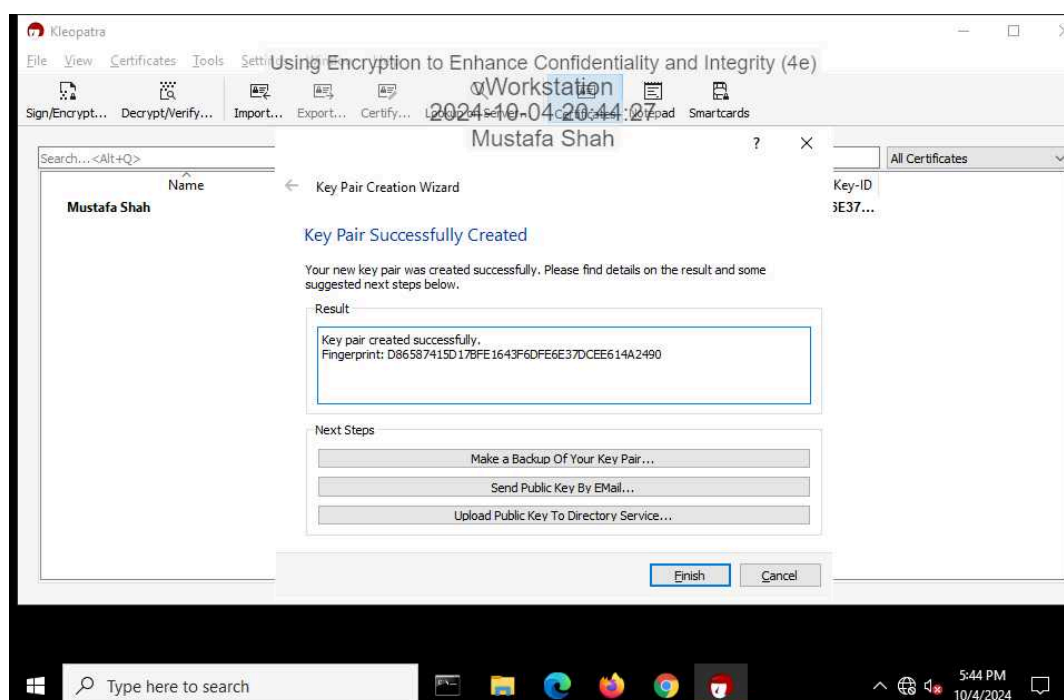
100%

Report Generated: Friday, October 4, 2024 at 10:58 PM

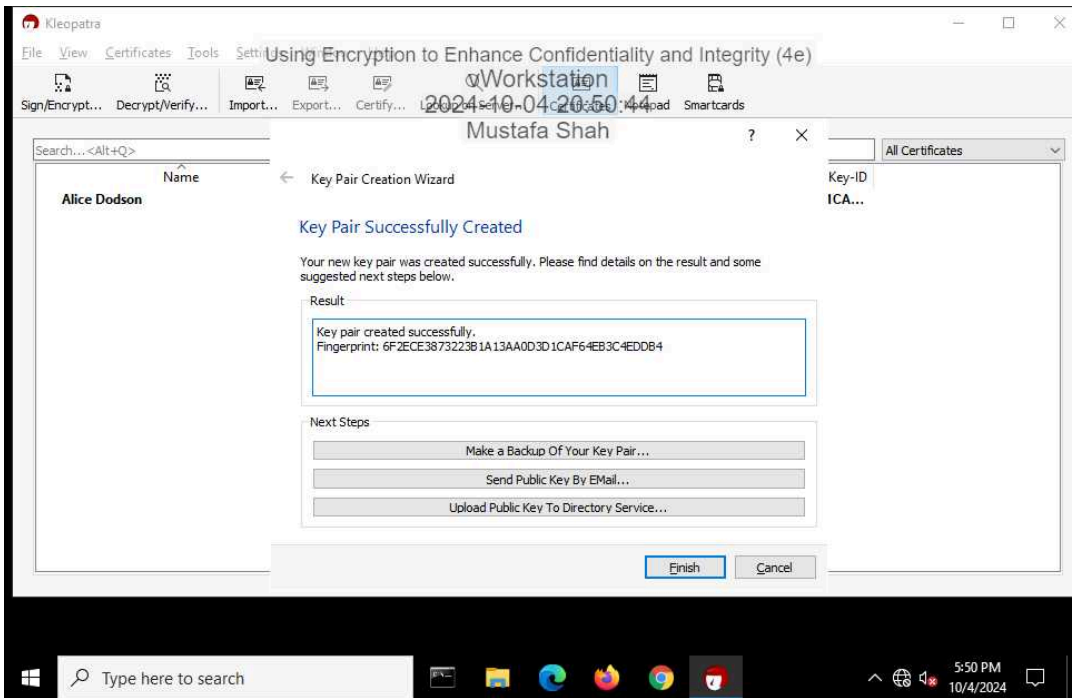
## Section 1: Hands-On Demonstration

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

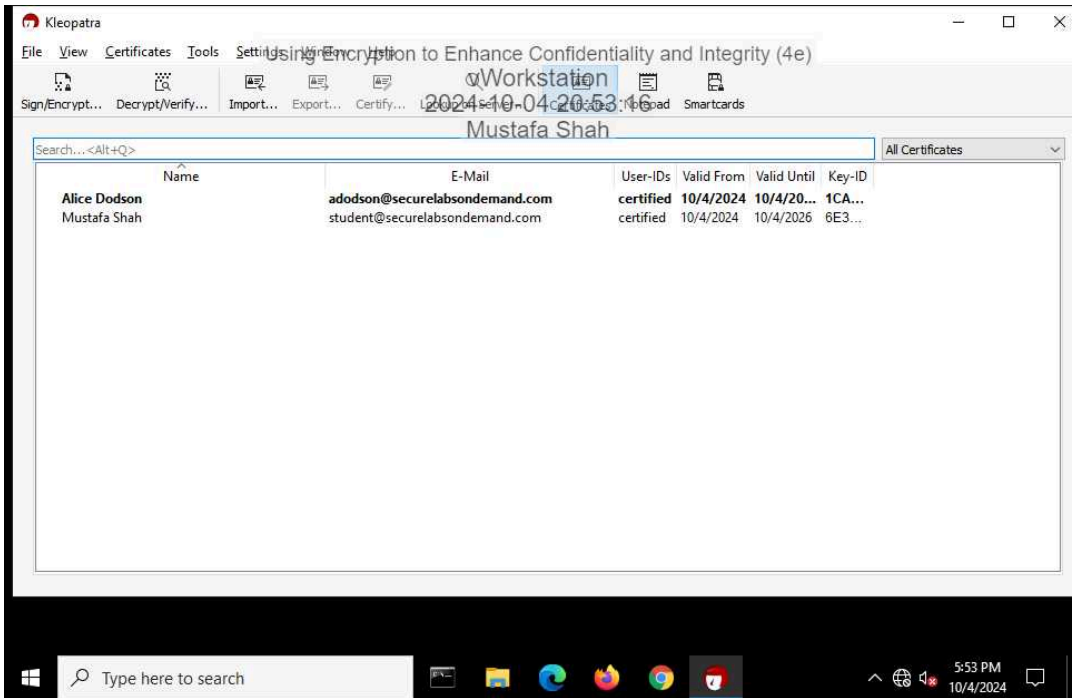
9. Make a screen capture showing the **fingerprint** for your key pair.



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



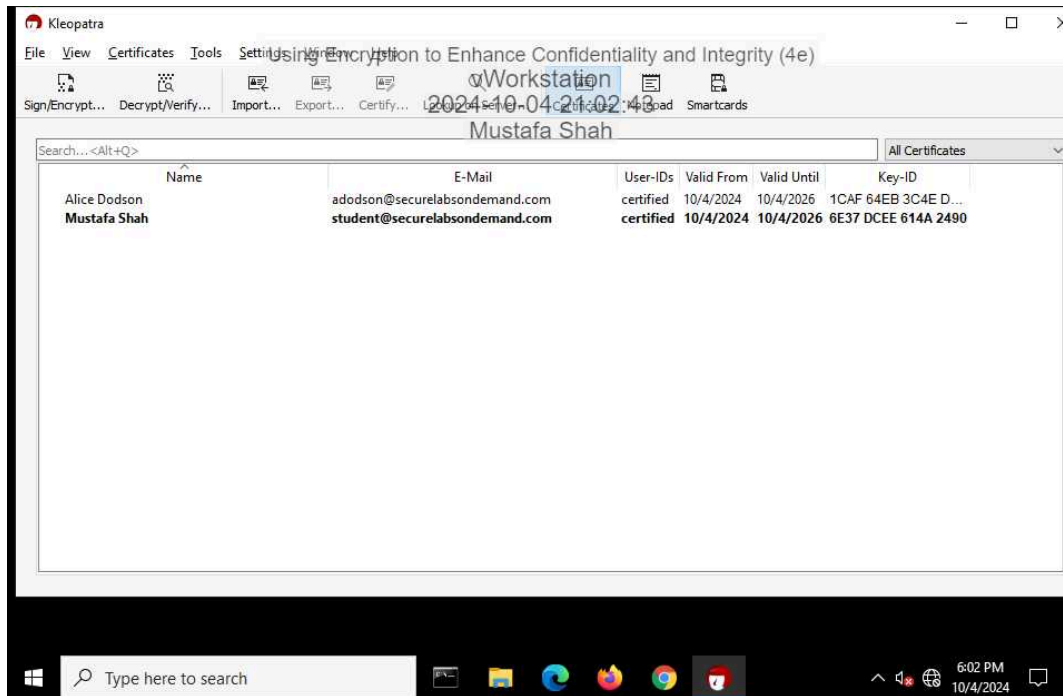
30. Make a screen capture showing your public key in Alice’s certificate cache.



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

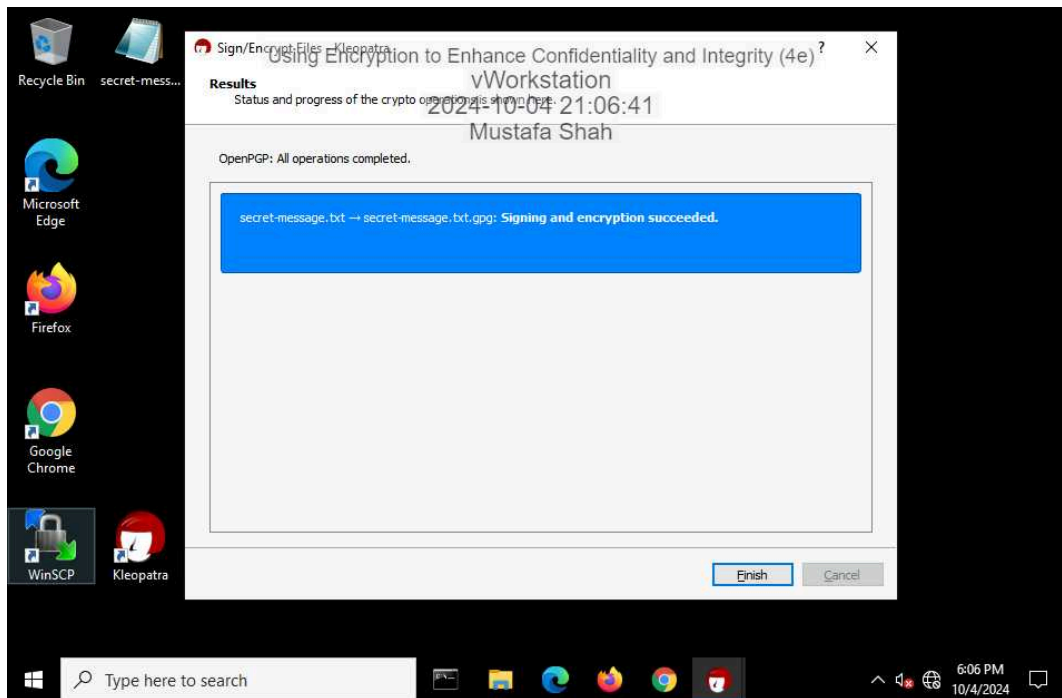
Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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

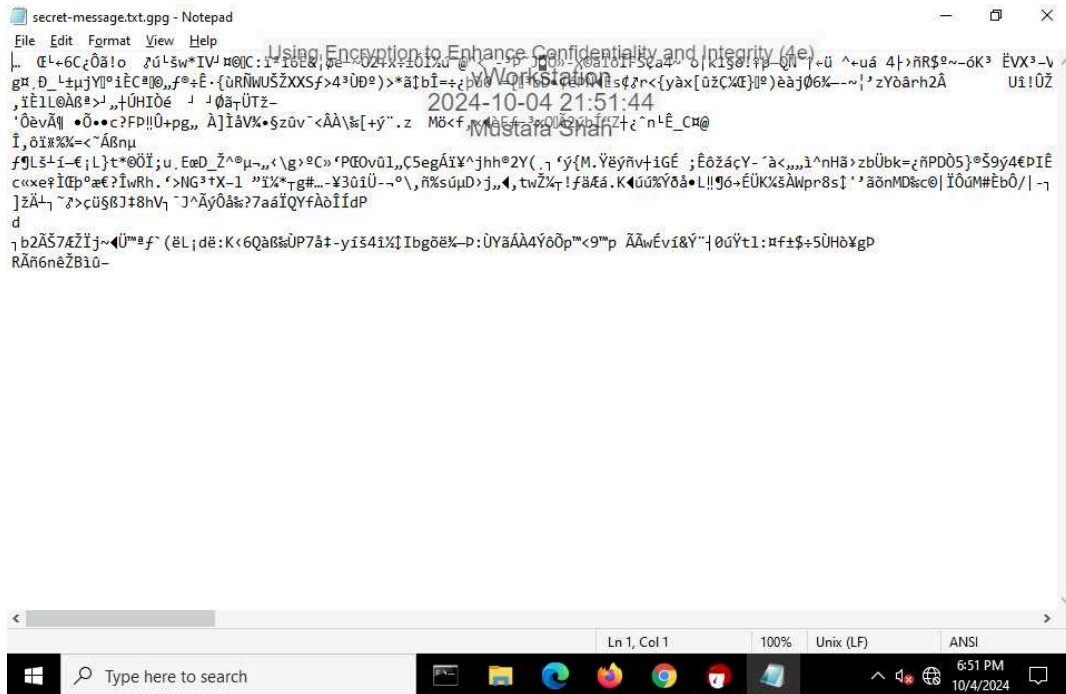


## Part 2: Encrypt a File Using Asymmetric Encryption

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

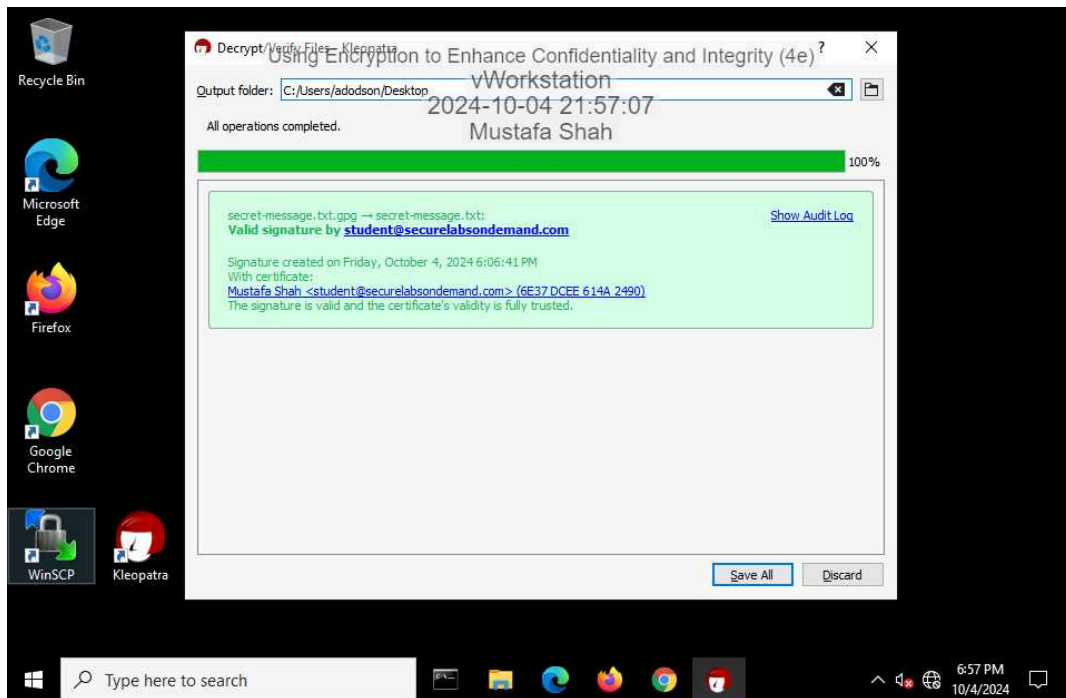


### 12. Make a screen capture showing the ciphertext.



## Part 3: Decrypt a File Using Asymmetric Encryption

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

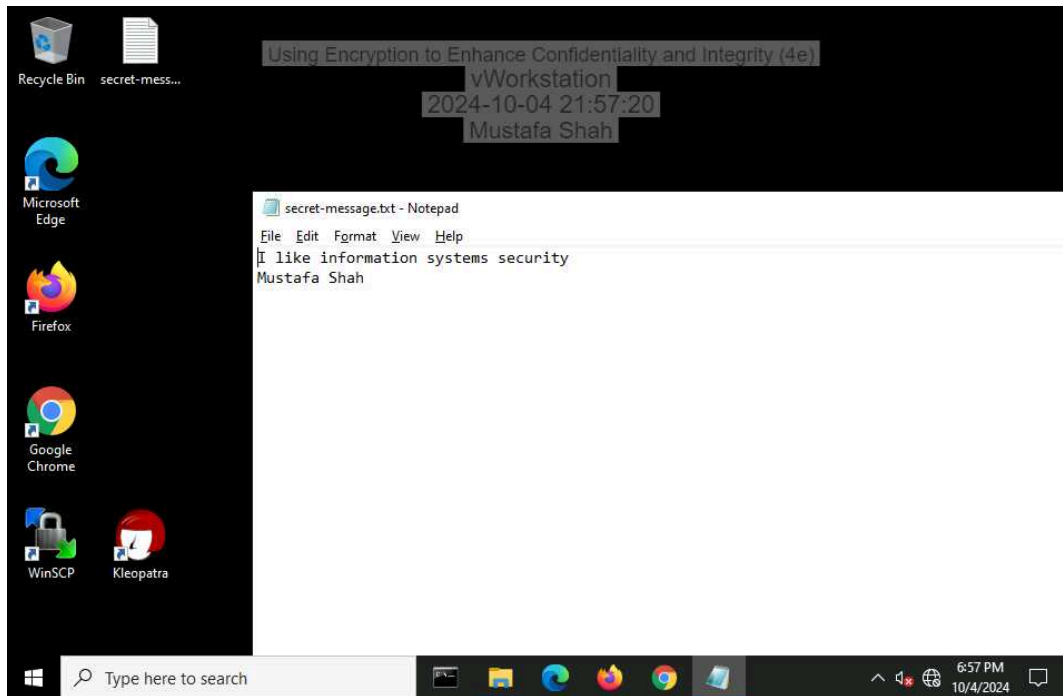


## Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

---

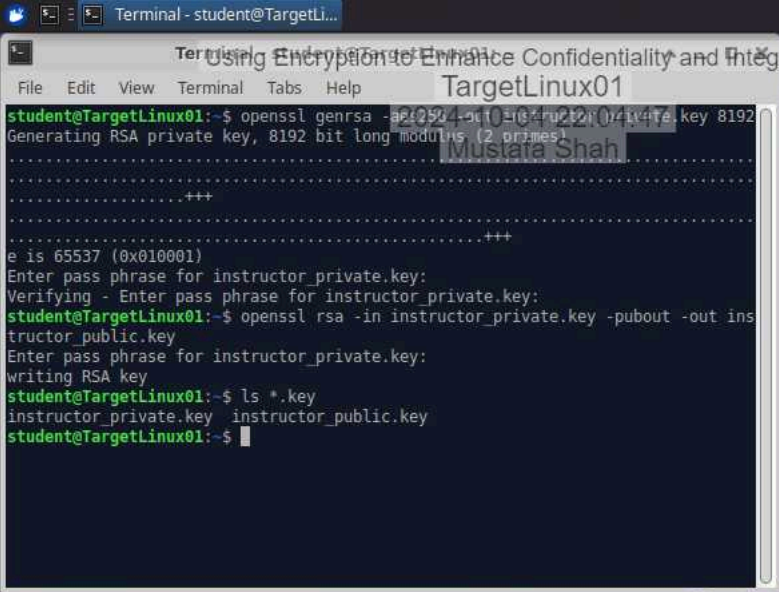
18. Make a screen capture showing the **decrypted secret-message.txt** file in Notepad.



## Section 2: Applied Learning

### Part 1: Create an Asymmetric Key Pair

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



A terminal window titled "Terminal - student@TargetLinux01" is shown. The terminal output is as follows:

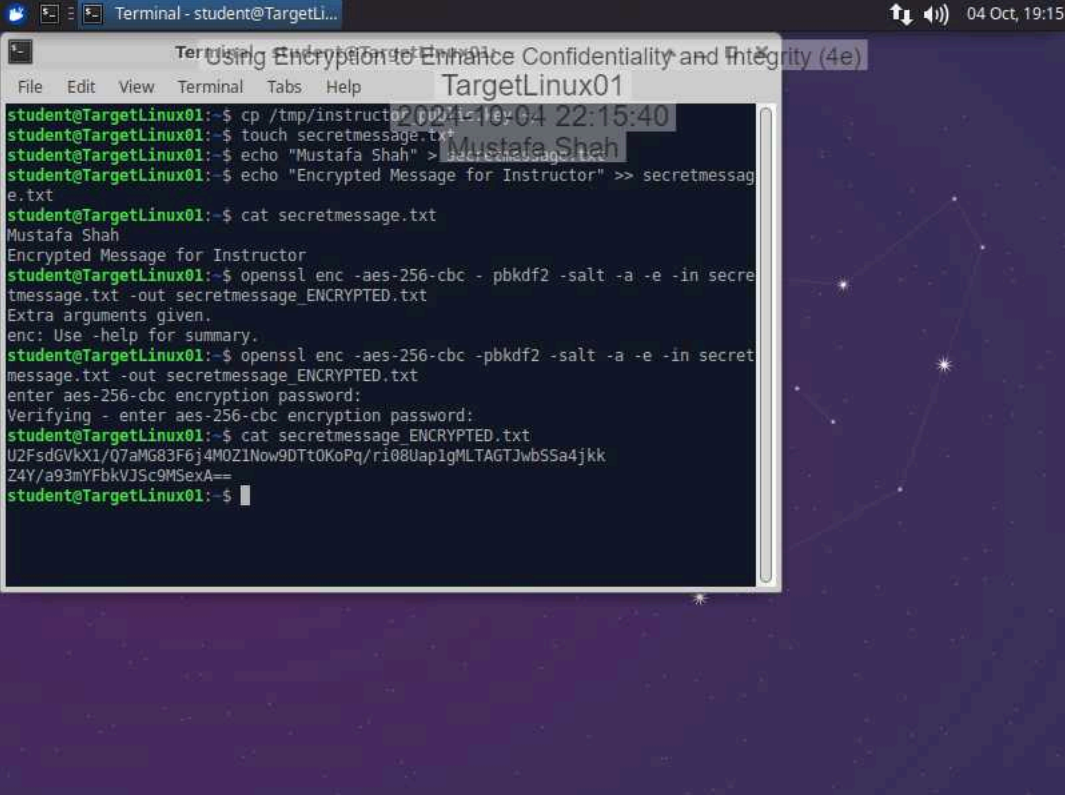
```
student@TargetLinux01:~$ openssl genrsa -a256 -out instructor_private.key 8192
Generating RSA private key, 8192 bit long modulus (2 primes)
.....+++
.....+++
e is 65537 (0x010001)
Enter pass phrase for instructor_private.key:
Verifying - Enter pass phrase for instructor_private.key:
student@TargetLinux01:~$ openssl rsa -in instructor_private.key -pubout -out instructor_public.key
Enter pass phrase for instructor_private.key:
writing RSA key
student@TargetLinux01:~$ ls *.key
instructor_private.key  instructor_public.key
student@TargetLinux01:~$
```

### Part 2: Encrypt a File Using Symmetric Encryption

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

P@ssw0rd!

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:

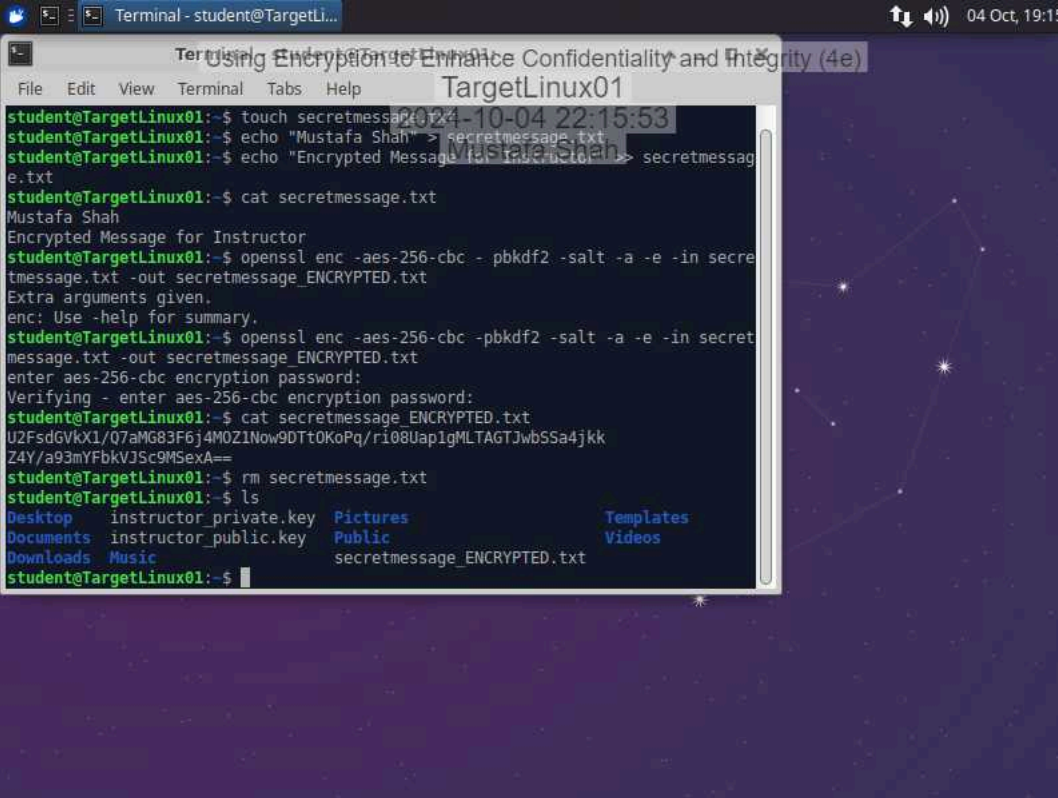
```
student@TargetLinux01:~$ cp /tmp/instructor01/secretmessage.txt .
student@TargetLinux01:~$ touch secretmessage.txt
student@TargetLinux01:~$ echo "Mustafa Shah" > secretmessage.txt
student@TargetLinux01:~$ echo "Encrypted Message for Instructor" >> secretmessage.txt
student@TargetLinux01:~$ cat secretmessage.txt
Mustafa Shah
Encrypted Message for Instructor
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secretmessage.txt -out secretmessage_ENCRYPTED.txt
Extra arguments given.
enc: Use -help for summary.
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
U2FsdGVkX1/07aMG83F6j4MQZ1Now9DTtOKoPq/ri08UapigMLTAGTJwbSSa4jkk
Z4Y/a93mYFbkVJSc9MSeA==
student@TargetLinux01:~$
```



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

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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

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

```
student@TargetLinux01:~$ touch secretmessage.txt
student@TargetLinux01:~$ echo "Mustafa Shah" > secretmessage.txt
student@TargetLinux01:~$ echo "Encrypted Message for Instructor" > secretmessage.txt
student@TargetLinux01:~$ cat secretmessage.txt
Mustafa Shah
Encrypted Message for Instructor
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secretmessage.txt -out secretmessage_ENCRYPTED.txt
Extra arguments given.
enc: Use -help for summary.
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
U2FsdGVkX1/Q7aMG83F6j4MOZINow9DTt0KoPq/r108Uap1gMLTAGTJwbSSa4jkk
Z4Y/a93mYFbkVJSc9MSeX==
student@TargetLinux01:~$ rm secretmessage.txt
student@TargetLinux01:~$ ls
Desktop  instructor_private.key  Pictures  Templates
Documents  instructor_public.key  Public    Videos
Downloads  Music                  secretmessage_ENCRYPTED.txt
```

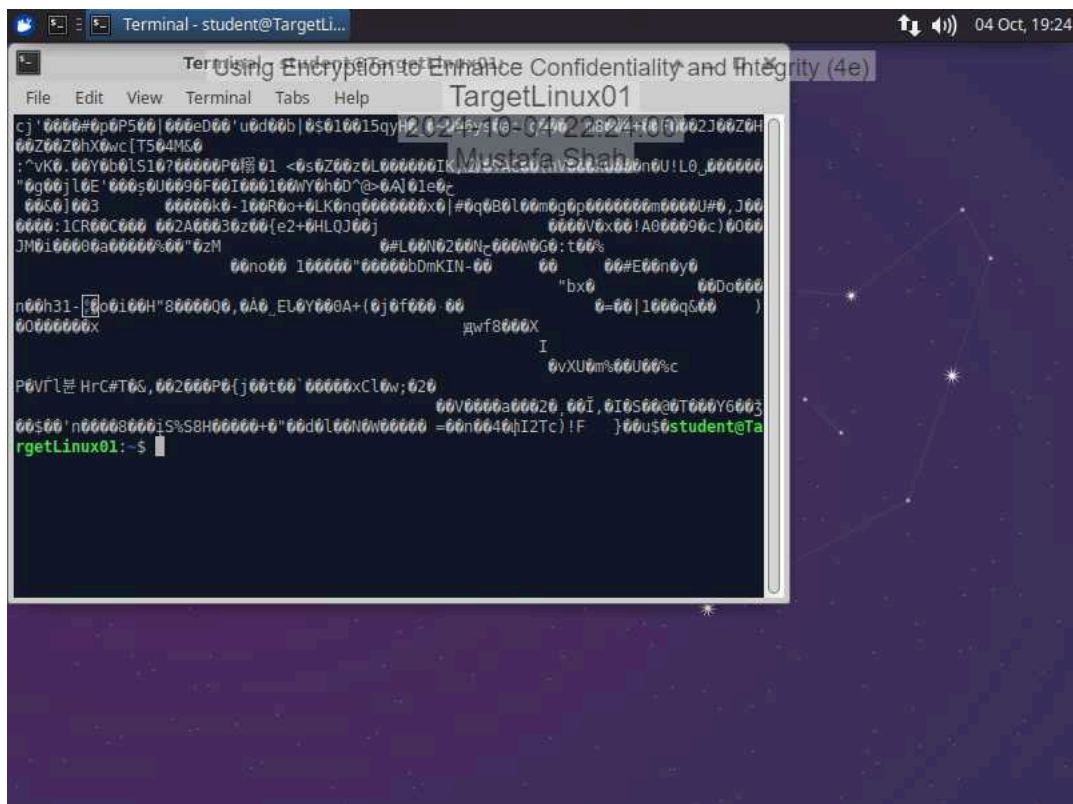
### Part 3: Transfer and Decrypt a File Using Hybrid Cryptography



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

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

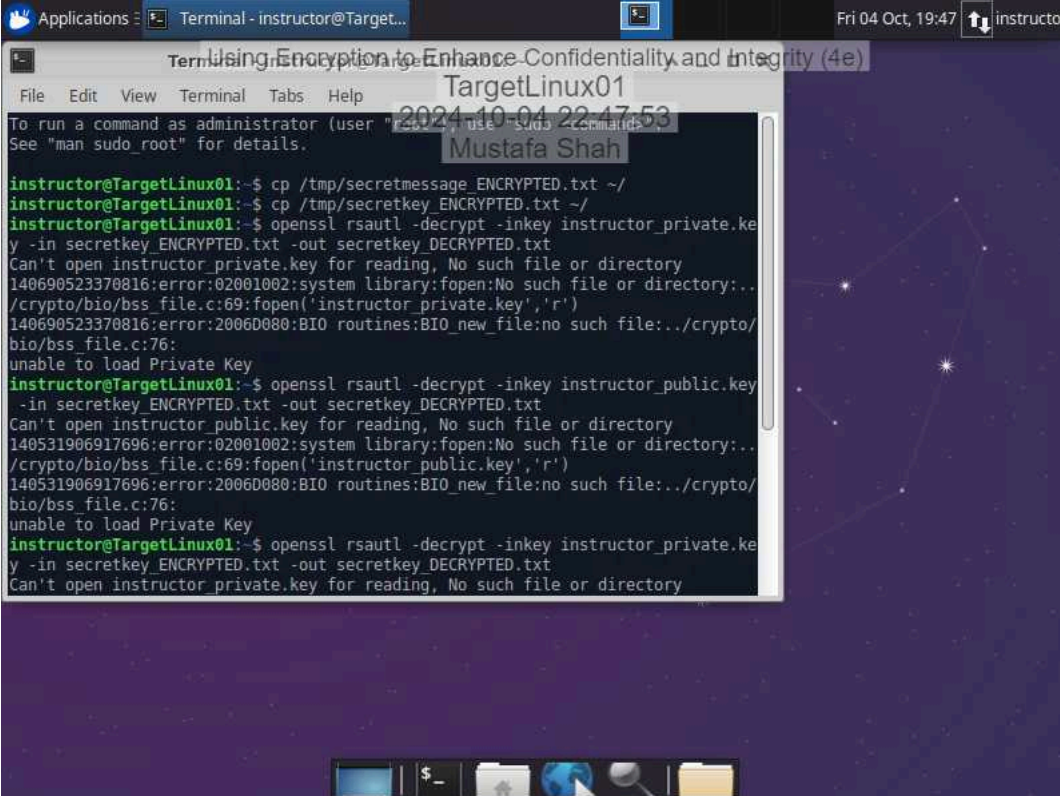
6. Make a screen capture showing the encrypted contents of the `secretkey_ENCRYPTED.txt` file.



## 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.**



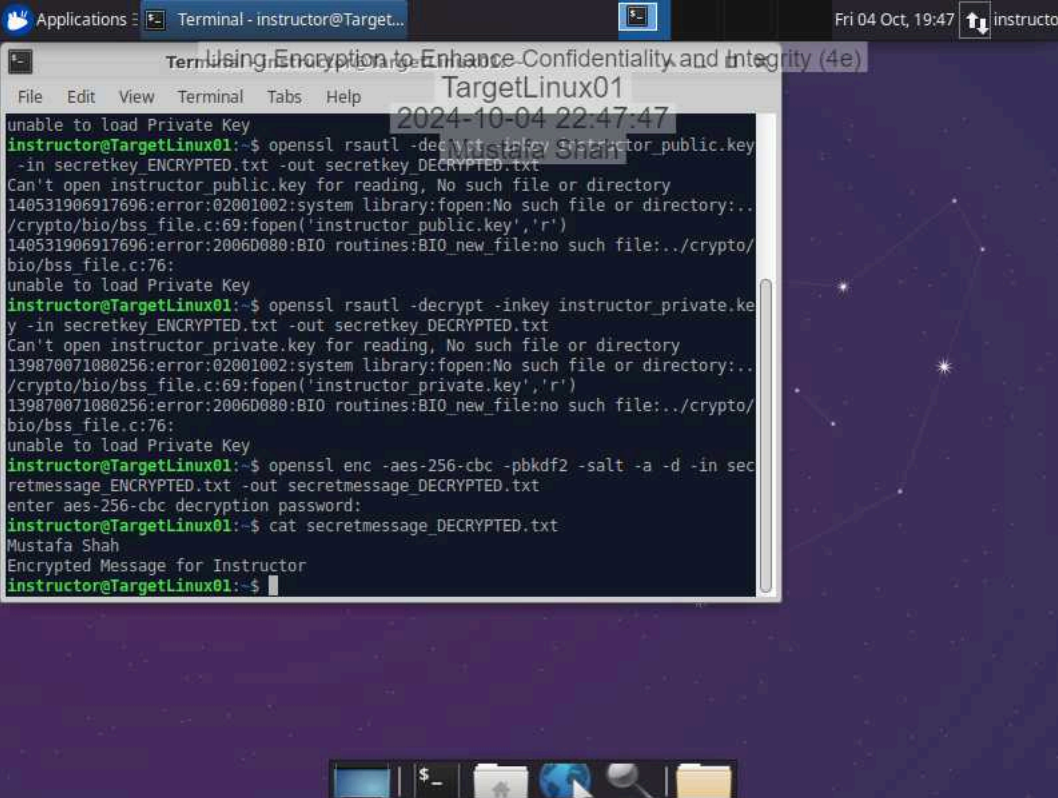
The screenshot shows a terminal window titled "Terminal - instructor@Target..." with a dark background and light-colored text. The terminal output shows the user "instructor@TargetLinux01" performing several commands to decrypt a file. The first command is `cp /tmp/secretmessage. ENCRYPTED.txt ~/`. The second is `cp /tmp/secretkey ENCRYPTED.txt ~/`. The third is `openssl rsautl -decrypt -inkey instructor_private.key -in secretkey ENCRYPTED.txt -out secretkey_DECRYPTED.txt`. This command fails with the error: "Can't open instructor\_private.key for reading, No such file or directory". The fourth command is `openssl rsautl -decrypt -inkey instructor_public.key -in secretkey ENCRYPTED.txt -out secretkey_DECRYPTED.txt`. This command also fails with the error: "Can't open instructor\_public.key for reading, No such file or directory". The fifth command is `openssl rsautl -decrypt -inkey instructor_private.ke` (truncated). This command also fails with the error: "Can't open instructor\_private.key for reading, No such file or directory". The terminal window has a title bar with "Applications", "Terminal - instructor@Target...", and a system clock showing "Fri 04 Oct, 19:47". The background of the terminal window is a dark blue space with a constellation of stars.

```
instructor@TargetLinux01:~$ cp /tmp/secretmessage. ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ cp /tmp/secretkey ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_private.key
Can't open instructor_private.key for reading, No such file or directory
140690523370816:error:02001002:system library:fopen:No such file or directory:..
/crypto/bio/bss_file.c:69:fopen('instructor_private.key','r')
140690523370816:error:2006D080:BIIO routines:BIIO_new_file:no such file:../crypto/
bio/bss_file.c:76:
unable to load Private Key
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_public.key
Can't open instructor_public.key for reading, No such file or directory
140531906917696:error:02001002:system library:fopen:No such file or directory:..
/crypto/bio/bss_file.c:69:fopen('instructor_public.key','r')
140531906917696:error:2006D080:BIIO routines:BIIO_new_file:no such file:../crypto/
bio/bss_file.c:76:
unable to load Private Key
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_private.ke
Can't open instructor_private.key for reading, No such file or directory
```

## 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.

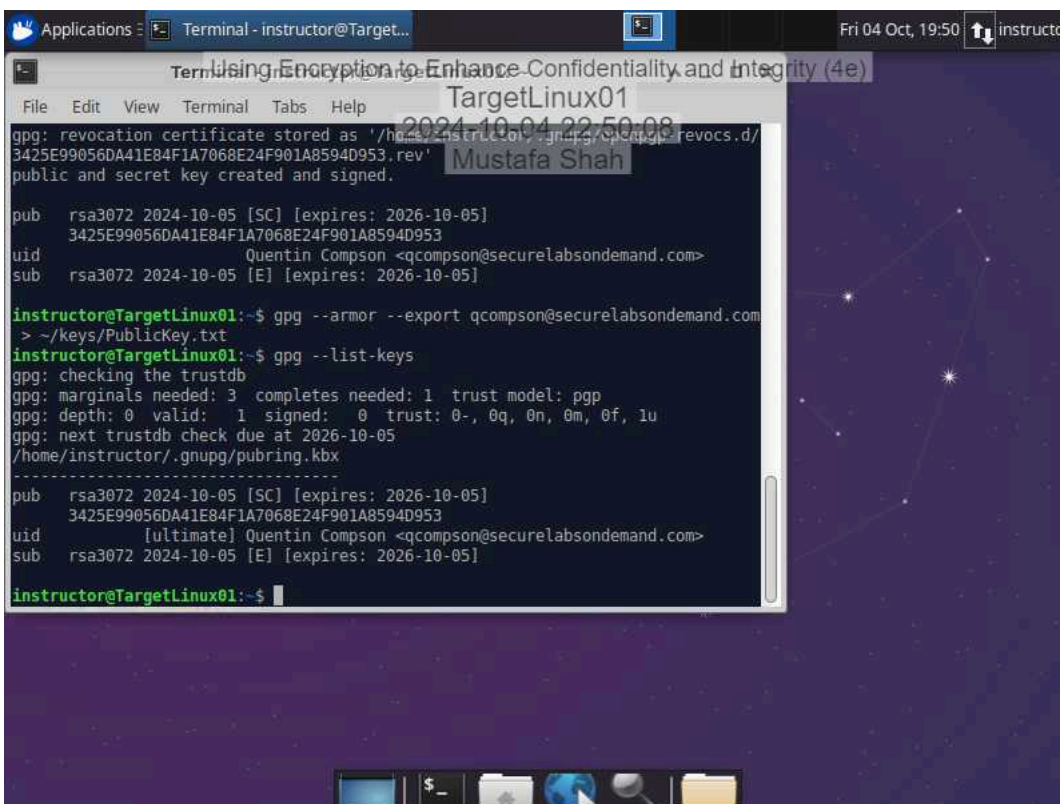


```
Applications ▢ Terminal - instructor@Target... Fri 04 Oct, 19:47 instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-10-04 22:47:47
Mustafa Shah
unable to load Private Key
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_public.key
-in secretkey_ENCRYPTED.txt -out secretkey_DECRYPTED.txt
Can't open instructor_public.key for reading, No such file or directory
140531906917696:error:02001002:system library:fopen:No such file or directory:../
/crypto/bio/bss_file.c:69:fopen('instructor_public.key','r')
140531906917696:error:2006D080:BIIO routines:BIIO_new_file:no such file:../crypto/
bio/bss_file.c:76:
unable to load Private Key
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_private.ke
y -in secretkey_ENCRYPTED.txt -out secretkey_DECRYPTED.txt
Can't open instructor_private.key for reading, No such file or directory
139870071080256:error:02001002:system library:fopen:No such file or directory:../
/crypto/bio/bss_file.c:69:fopen('instructor_private.key','r')
139870071080256:error:2006D080:BIIO routines:BIIO_new_file:no such file:../crypto/
bio/bss_file.c:76:
unable to load Private Key
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
Mustafa Shah
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.

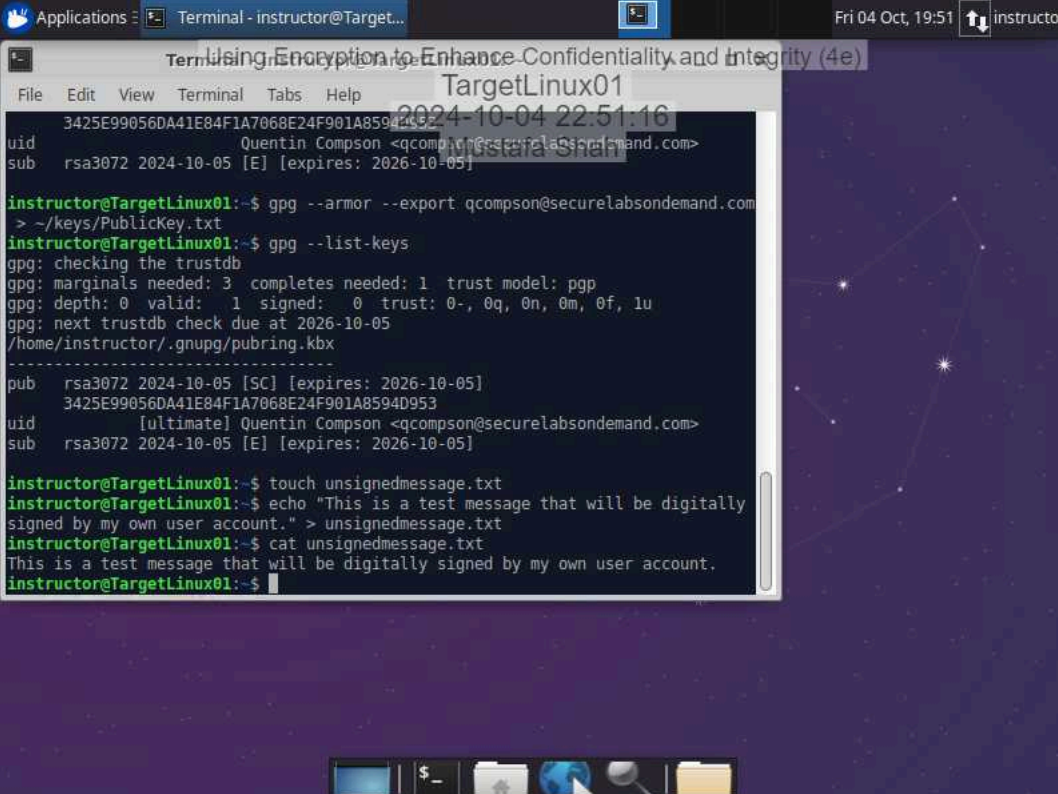


```
gpg: revocation certificate stored as '/home/instructor/.gnupg/openpgp-revocs.d/3425E99056DA41E84F1A7068E24F901A8594D953.rev'  
public and secret key created and signed.  
  
pub  rsa3072 2024-10-05 [SC] [expires: 2026-10-05]  
     3425E99056DA41E84F1A7068E24F901A8594D953  
uid          Quentin Compson <qcompson@securelabsondemand.com>  
sub  rsa3072 2024-10-05 [E] [expires: 2026-10-05]  
  
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 2026-10-05  
/home/instructor/.gnupg/pubring.kbx  
-----  
pub  rsa3072 2024-10-05 [SC] [expires: 2026-10-05]  
     3425E99056DA41E84F1A7068E24F901A8594D953  
uid          [ultimate] Quentin Compson <qcompson@securelabsondemand.com>  
sub  rsa3072 2024-10-05 [E] [expires: 2026-10-05]  
  
instructor@TargetLinux01:~$
```

## 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.



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:

```
3425E99056DA41E84F1A7068E24F901A8594D953
uid      Quentin Compson <qcompson@securelabsondemand.com>
sub      rsa3072 2024-10-05 [E] [expires: 2026-10-05]

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 2026-10-05
/home/instructor/.gnupg/pubring.kbx
-----
pub      rsa3072 2024-10-05 [SC] [expires: 2026-10-05]
         3425E99056DA41E84F1A7068E24F901A8594D953
uid      [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub      rsa3072 2024-10-05 [E] [expires: 2026-10-05]

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.

