

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

10 hours, 0 minutes

Progress:

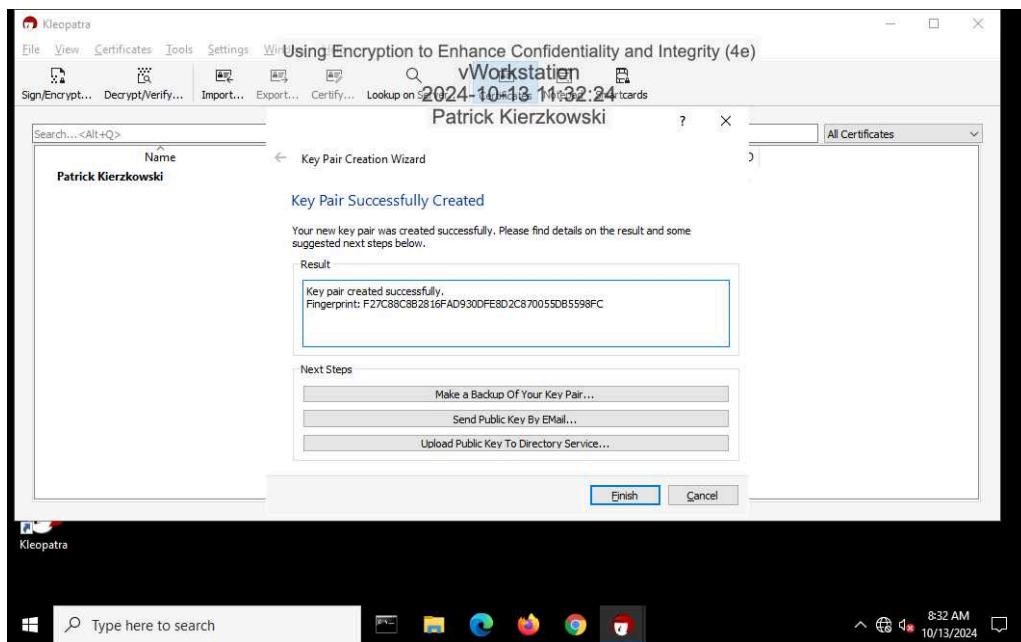
100%

Report Generated: Monday, July 7, 2025 at 9:50 PM

Section 1: Hands-On Demonstration

Part 1: Create and Exchange Asymmetric Encryption Keys

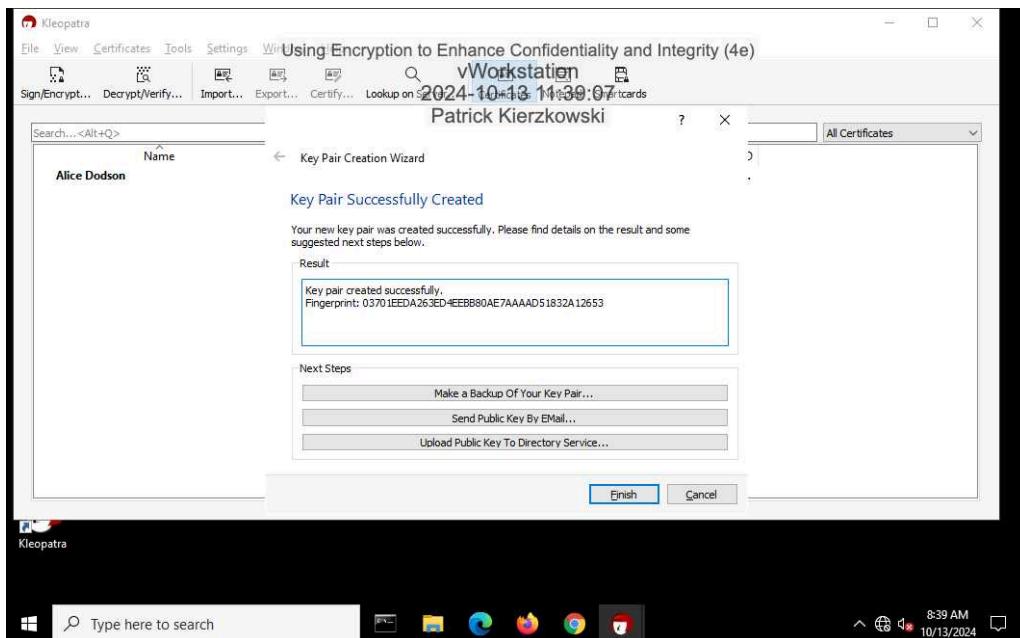
9. Make a screen capture showing the **fingerprint** for your key pair.



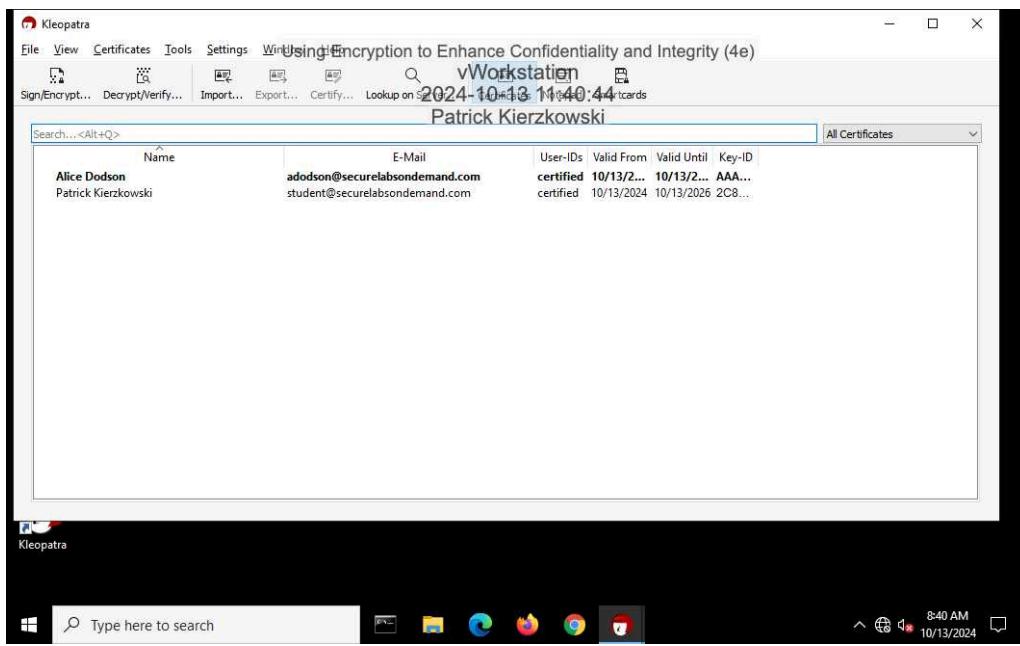
Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



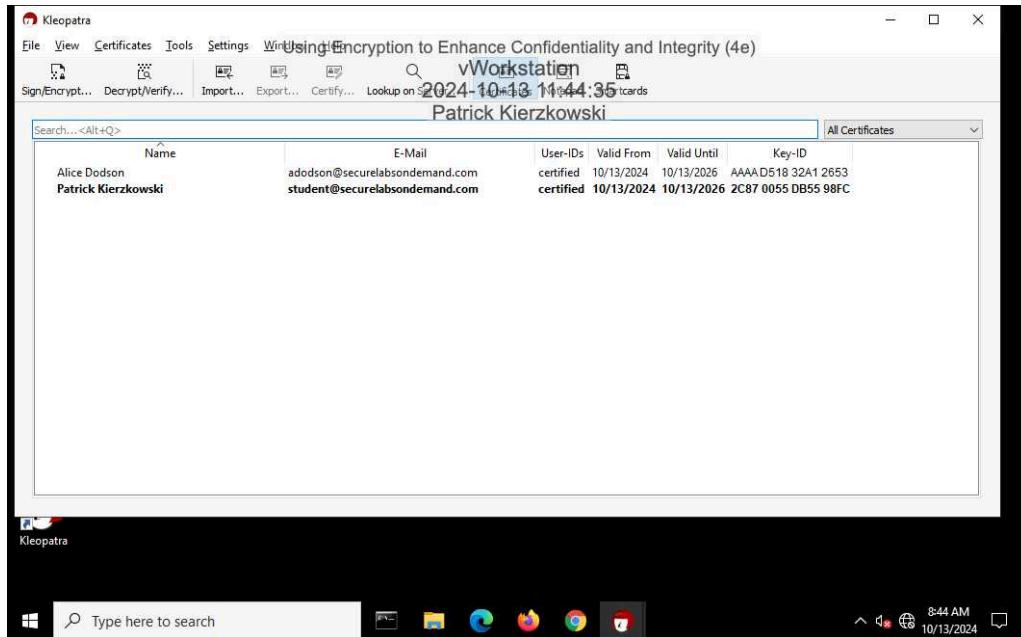
30. Make a screen capture showing your public key in Alice's certificate cache.



Using Encryption to Enhance Confidentiality and Integrity (4e)

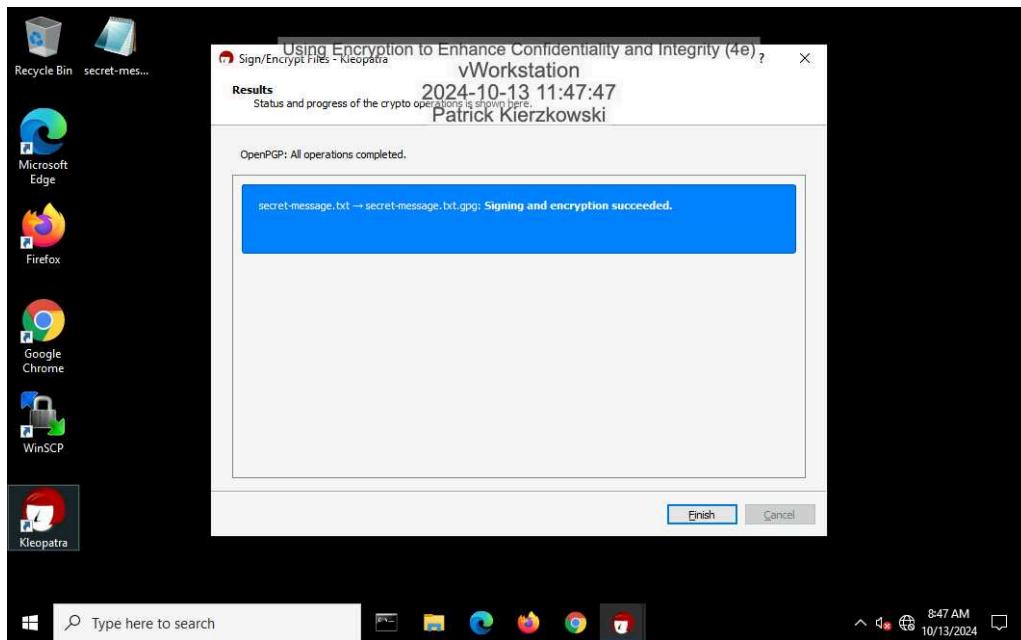
Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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.



Using Encryption to Enhance Confidentiality and Integrity (4e)

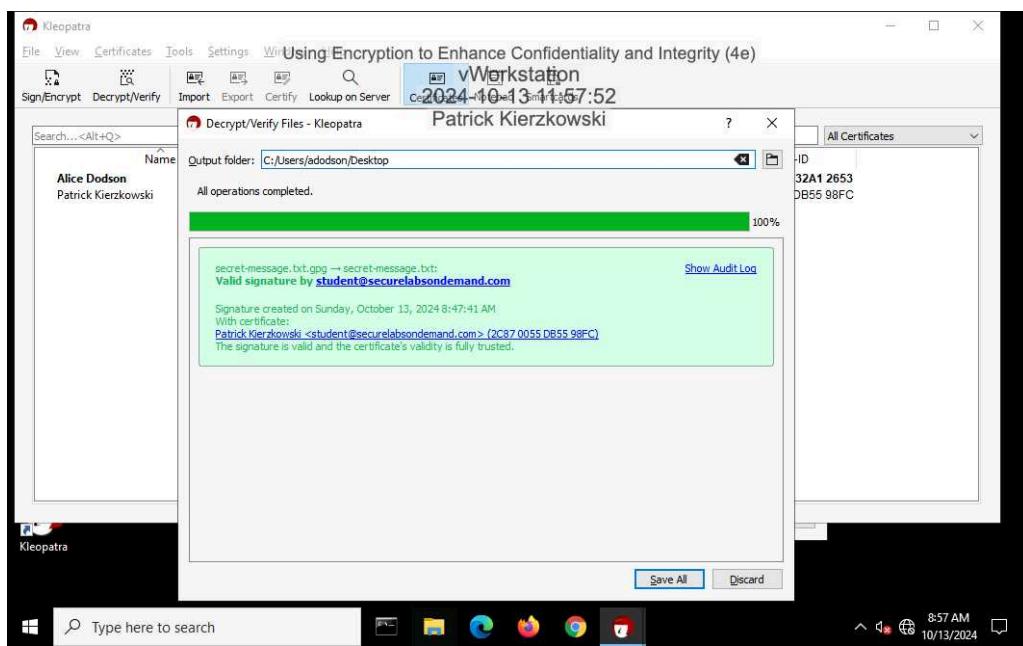
Fundamentals of Information Systems Security, Fourth Edition - Lab 05

12. Make a screen capture showing the ciphertext.



Part 3: Decrypt a File Using Asymmetric Encryption

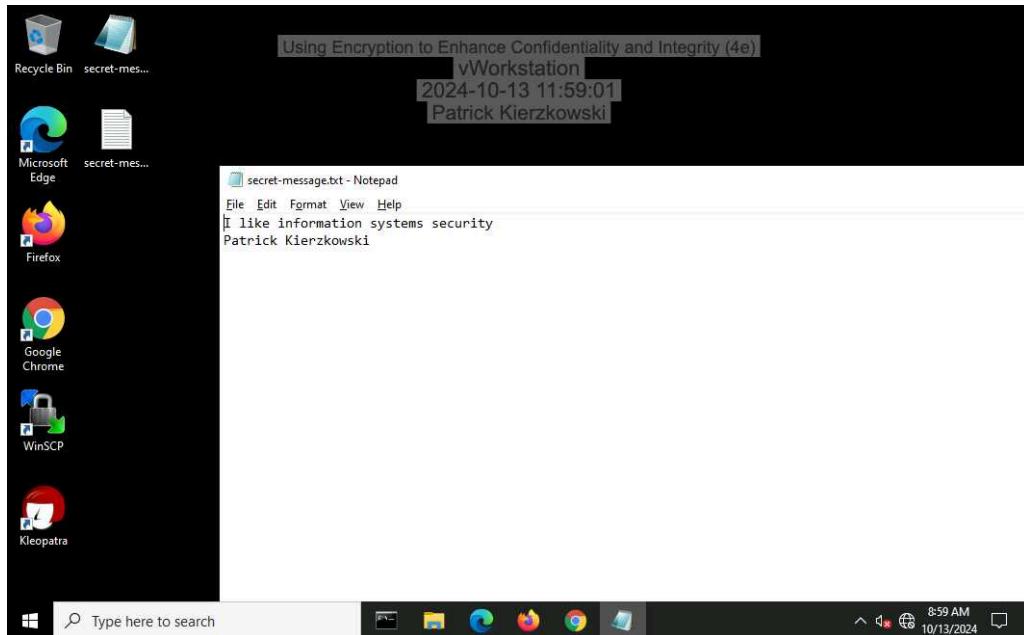
15. Make a screen capture showing the Decrypt/Verify Files window.



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.



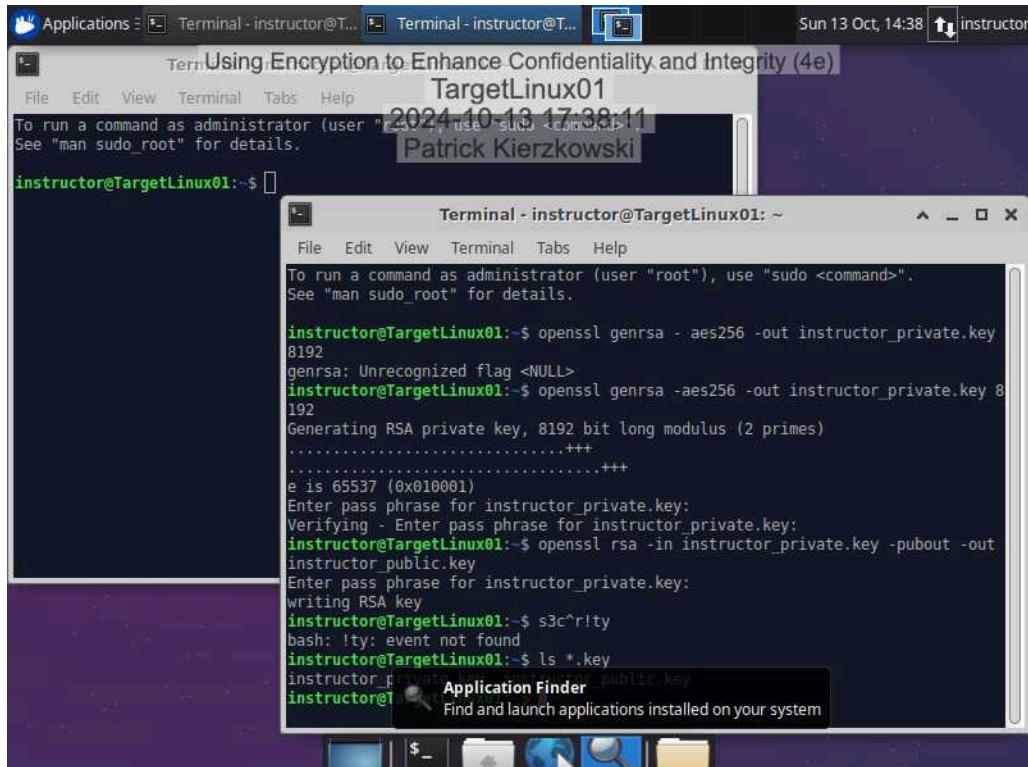
Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

Section 2: Applied Learning

Part 1: Create an Asymmetric Key Pair

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



```
instructor@TargetLinux01:~$ openssl genrsa -aes256 -out instructor_private.key
8192
genrsa: Unrecognized flag <NULL>
instructor@TargetLinux01:~$ openssl genrsa -aes256 -out instructor_private.key 8
192
Generating RSA private key, 8192 bit long modulus (2 primes)
.....+++
.....+++
e is 65537 (0x10001)
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:~$ s3c^rity
bash: !ty: event not found
instructor@TargetLinux01:~$ ls *.key
instructor_private.key  instructor_public.key
```

Part 2: Encrypt a File Using Symmetric Encryption

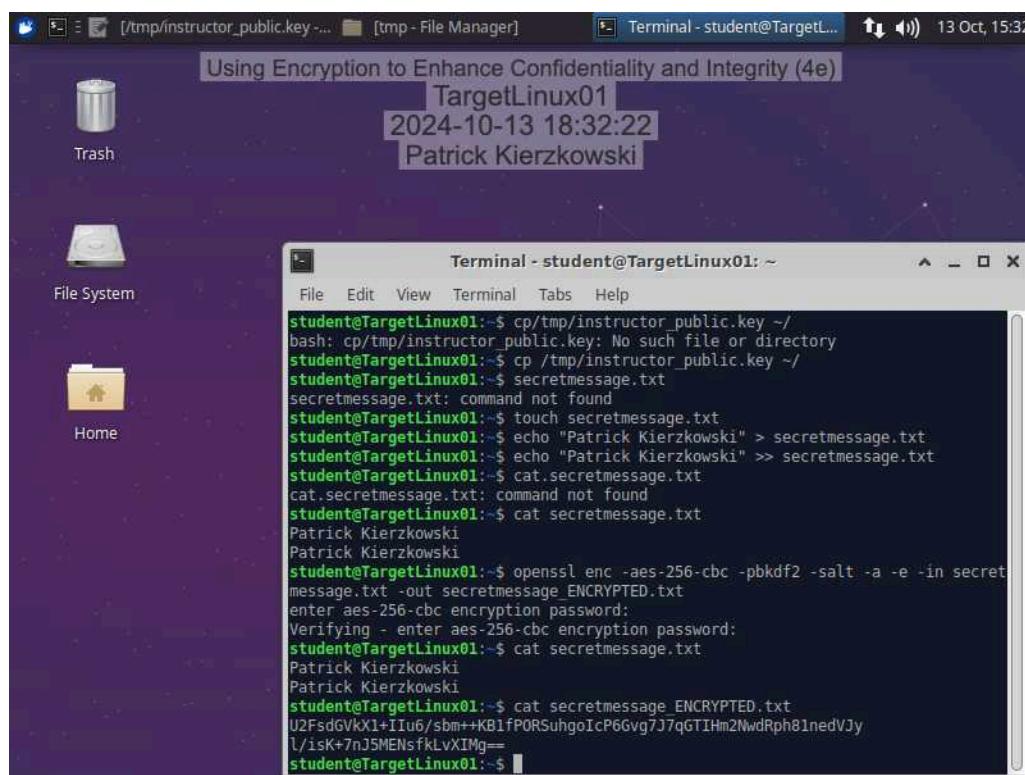
11. Document the password you used to symmetrically encrypt the file.

yourownpassword

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



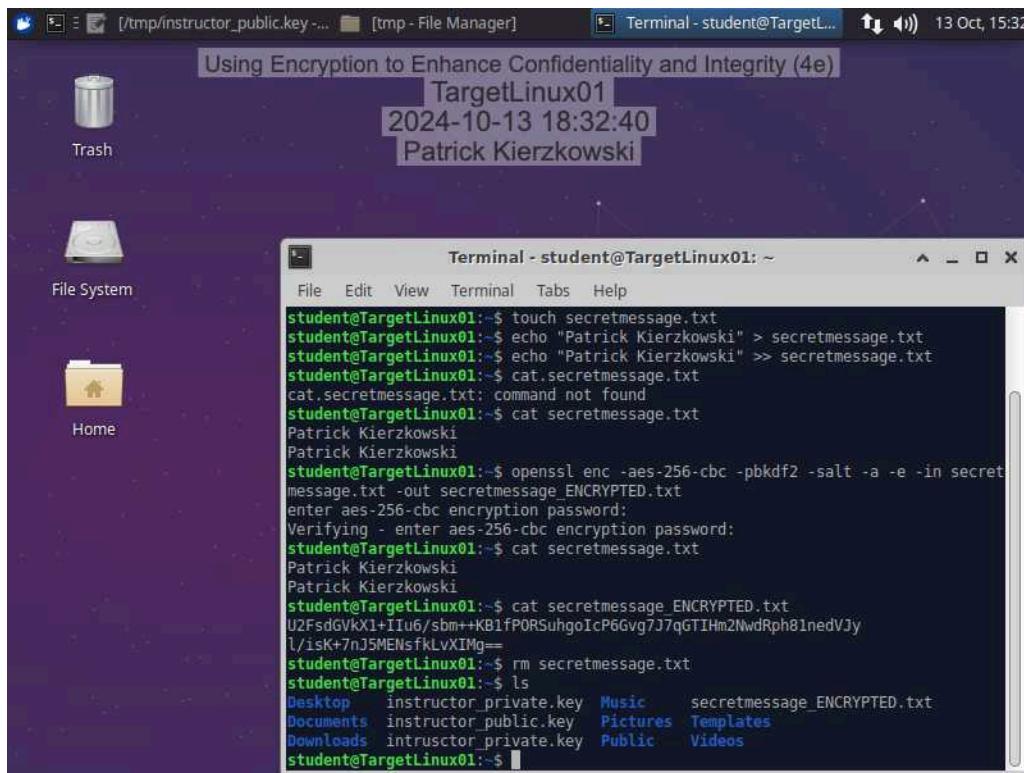
The screenshot shows a Linux desktop environment with a purple theme. A terminal window titled "Terminal - student@TargetLinux01: ~" is open, displaying the following command-line session:

```
student@TargetLinux01:~$ cp /tmp/instructor_public.key ~/
bash: cp /tmp/instructor_public.key: No such file or directory
student@TargetLinux01:~$ cp /tmp/instructor_public.key ~/
student@TargetLinux01:~$ secretemail.txt
secretemail.txt: command not found
student@TargetLinux01:~$ touch secretemail.txt
student@TargetLinux01:~$ echo "Patrick Kierzkowski" > secretemail.txt
student@TargetLinux01:~$ echo "Patrick Kierzkowski" >> secretemail.txt
student@TargetLinux01:~$ cat secretemail.txt
cat.secretemail.txt: command not found
student@TargetLinux01:~$ cat secretemail.txt
Patrick Kierzkowski
Patrick Kierzkowski
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secretemail.txt -out secretemail.ENCRYPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat secretemail.txt
Patrick Kierzkowski
Patrick Kierzkowski
student@TargetLinux01:~$ cat secretemail.ENCRYPTED.txt
U2FsdGVkX1+IIu6/sbm+KB1fPOR5uhgoIcP6Gvg7J7qGTIHm2NwdRph81nedVJy
l/isK+7nJ5MENsfkLvXIMg==
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.



The screenshot shows a Linux desktop environment with a purple theme. A terminal window titled "Terminal - student@TargetLinux01: ~" is open, displaying the following command-line session:

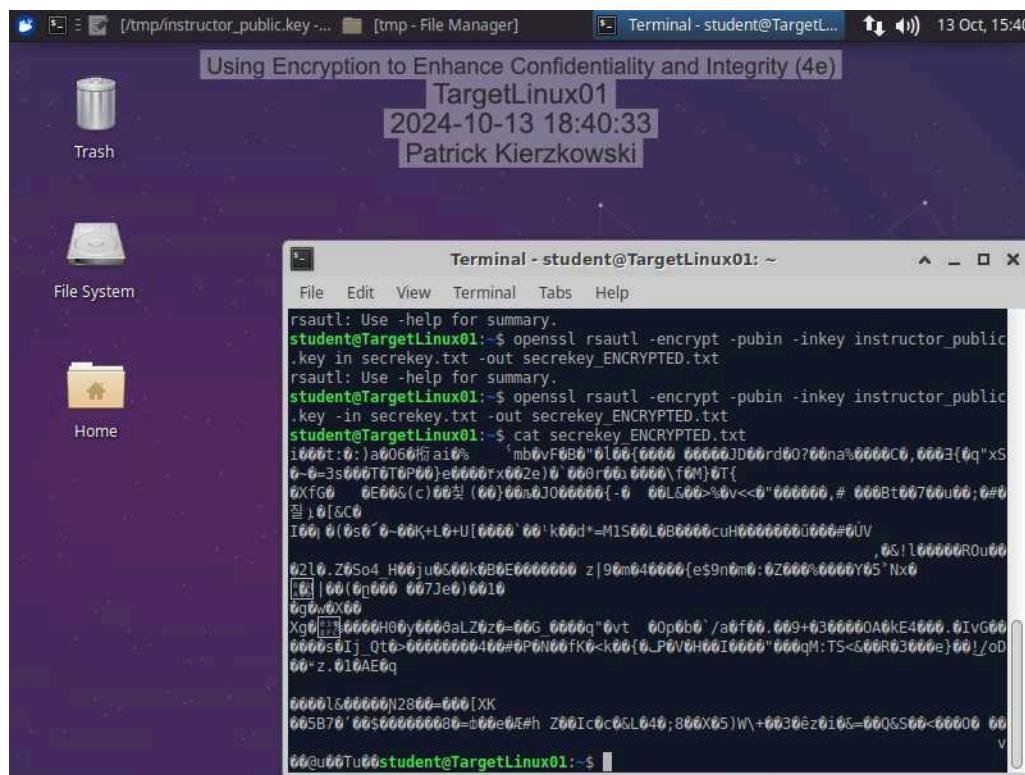
```
student@TargetLinux01:~$ touch secretmessage.txt
student@TargetLinux01:~$ echo "Patrick Kierzkowski" > secretmessage.txt
student@TargetLinux01:~$ echo "Patrick Kierzkowski" >> secretmessage.txt
student@TargetLinux01:~$ cat secretmessage.txt
cat.secretmessage.txt: command not found
student@TargetLinux01:~$ cat secretmessage.txt
Patrick Kierzkowski
Patrick Kierzkowski
student@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -e -in secretmessage.txt -out secretmessage.ENCRIPTED.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@TargetLinux01:~$ cat secretmessage.ENCRIPTED.txt
U2FsdGVkX1+IIu6/sbm++KB1fPORsuhgoIcpGGvg7J7qGTIHm2NwdRph81nedVjy
l/ikK+7nJ5MENsfklvXIMg==
student@TargetLinux01:~$ rm secretmessage.txt
student@TargetLinux01:~$ ls
Desktop  instructor_private.key  Music      secretmessage.ENCRIPTED.txt
Documents  instructor_public.key  Pictures   Templates
Downloads  intrusctor_private.key  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.



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.

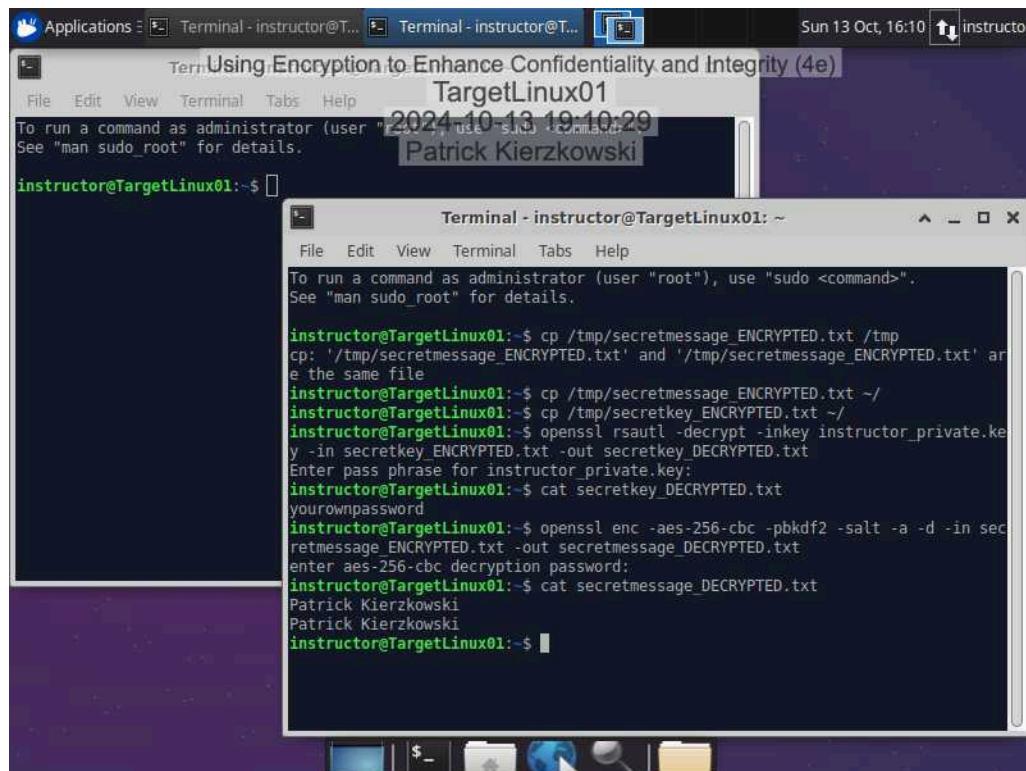
```
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-10-13 19:08:56
See "man sudo_root" for details.
Patrick Kierzkowski

instructor@TargetLinux01:~$ cp /tmp/secretmessage_ENCRYPTED.txt /tmp
cp: '/tmp/secretmessage_ENCRYPTED.txt' and '/tmp/secretmessage_ENCRYPTED.txt' are
the same file
instructor@TargetLinux01:~$ cp /tmp/secretmessage_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ cp /tmp/secretkey_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ openssl rsa -decrypt -inkey instructor_private.key
-in secretkey_ENCRYPTED.txt -out secretkey_DECRYPTED.txt
Enter pass phrase for instructor_private.key:
instructor@TargetLinux01:~$ cat secretkey_DECRYPTED.txt
yourownpassword
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.



```
instructor@TargetLinux01:~$ cp /tmp/secretmessage_ENCRYPTED.txt /tmp
cp: '/tmp/secretmessage_ENCRYPTED.txt' and '/tmp/secretmessage_ENCRYPTED.txt' are the same file
instructor@TargetLinux01:~$ cp /tmp/secretkey_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ openssl rsa -decrypt -inkey instructor_private.key -in secretkey_ENCRYPTED.txt -out secretkey_DECRYPTED.txt
Enter pass phrase for instructor_private.key:
instructor@TargetLinux01:~$ cat secretkey_DECRYPTED.txt
yourownpassword
instructor@TargetLinux01:~$ openssl enc -aes-256-cbc -pbkdf2 -salt -a -d -in secretmessage_ENCRYPTED.txt -out secretmessage_DECRYPTED.txt
enter aes-256-cbc decryption password:
instructor@TargetLinux01:~$ cat secretmessage_DECRYPTED.txt
Patrick Kierzkowski
Patrick Kierzkowski
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.

```
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-10-13 19:13:29
See "man sudo_root" for details.
Patrick Kierzkowski

instructor@TargetLinux01:~$ 
Terminal - instructor@TargetLinux01: ~
File Edit View Terminal Tabs Help
public and secret key created and signed.

pub rsa3072 2024-10-13 [SC] [expires: 2026-10-13]
    AA5EFCF57F64E1B5A95E781B015E019074A192A
uid                      Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2024-10-13 [E] [expires: 2026-10-13]

instructor@TargetLinux01:~$ gpg --armor --export qcompson@securelabsondemand.com
> ~/keys/PublicKey.txt
instructor@TargetLinux01:~$ gpg --list-keys
gpg: invalid option "--list-keys."
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 2026-10-13
/home/instructor/.gnupg/pubring.kbx

pub rsa3072 2024-10-13 [SC] [expires: 2026-10-13]
    AA5EFCF57F64E1B5A95E781B015E019074A192A
uid          [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2024-10-13 [E] [expires: 2026-10-13]

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.

```
instructor@TargetLinux01:~$ gpg --sign unsignedmessage.txt
gpg: signing failed: 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
This is a test message that will be digitally signed by my own user account uns
gnedmessage.txt
instructor@TargetLinux01:~$ echp "This is a test message that will be digitally signed by my own user account" >> unsignedmessage.txt
Command 'echp' not found, did you mean:
  command 'ecp' from deb ecere-dev (0.44.15-1build3)
  command 'echo' from deb coreutils (8.30-3ubuntu2)
Try: sudo apt install <deb name>
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.

