

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

Student:

Sadam Hashi

Email:

smhashi@asu.edu

Time on Task:

10 hours, 52 minutes

Progress:

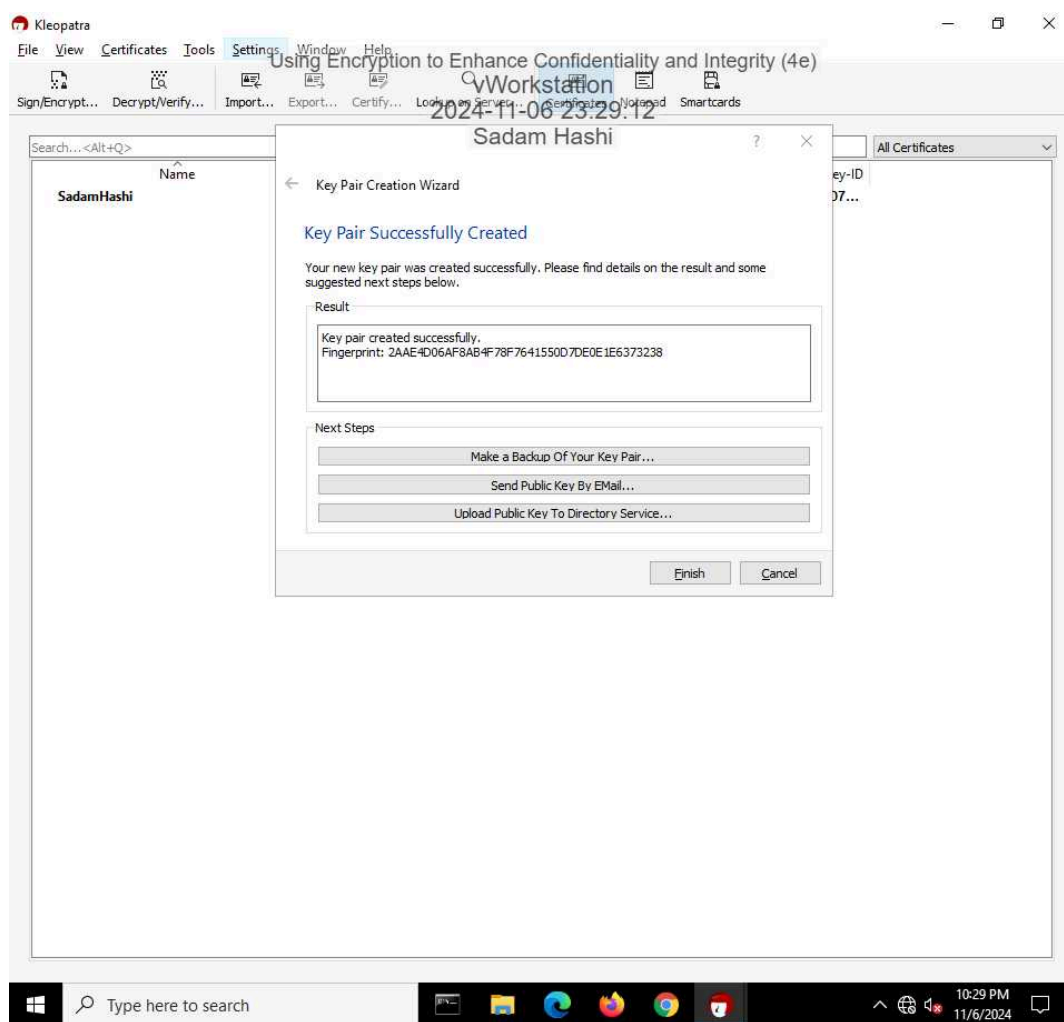
100%

Report Generated: Friday, November 8, 2024 at 5:35 AM

Section 1: Hands-On Demonstration

Part 1: Create and Exchange Asymmetric Encryption Keys

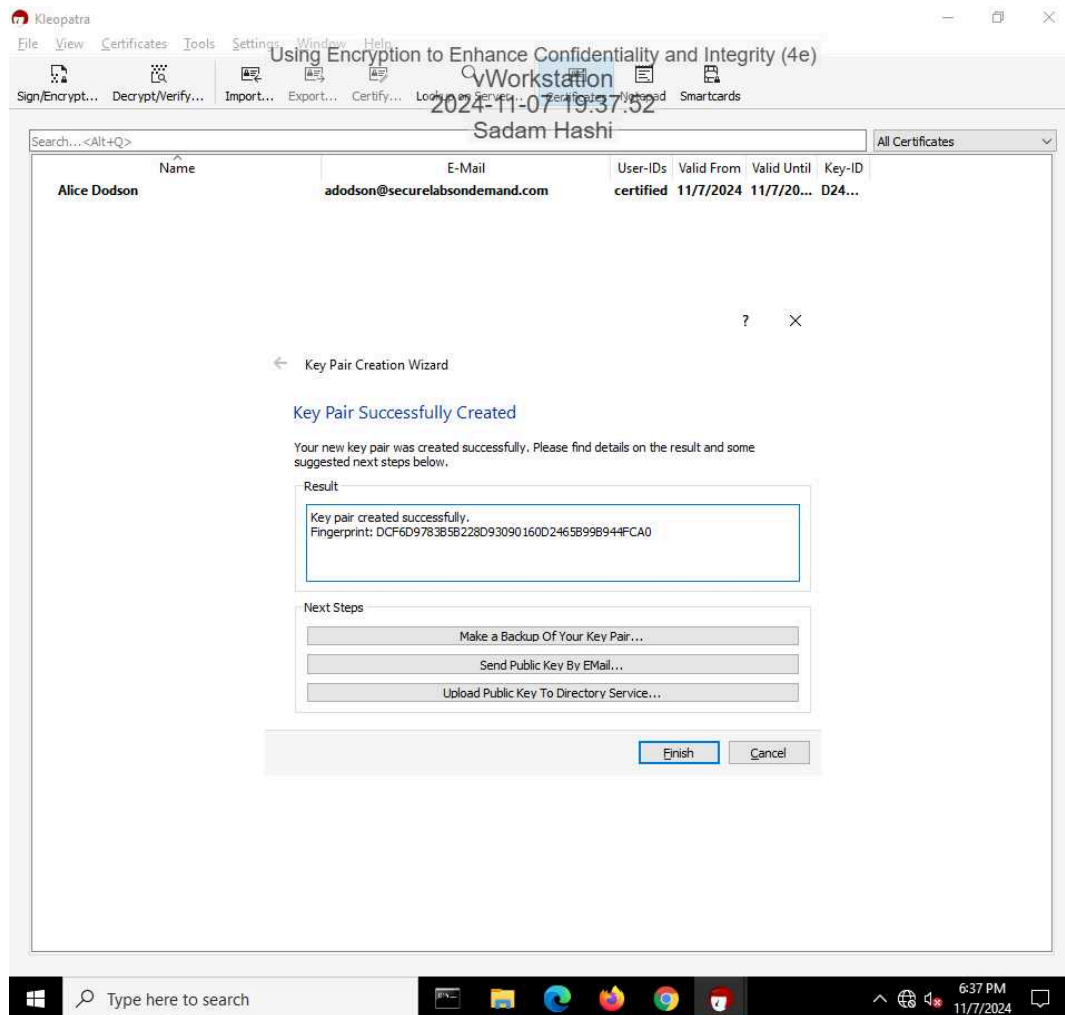
9. Make a screen capture showing the **fingerprint** for your key pair.



Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

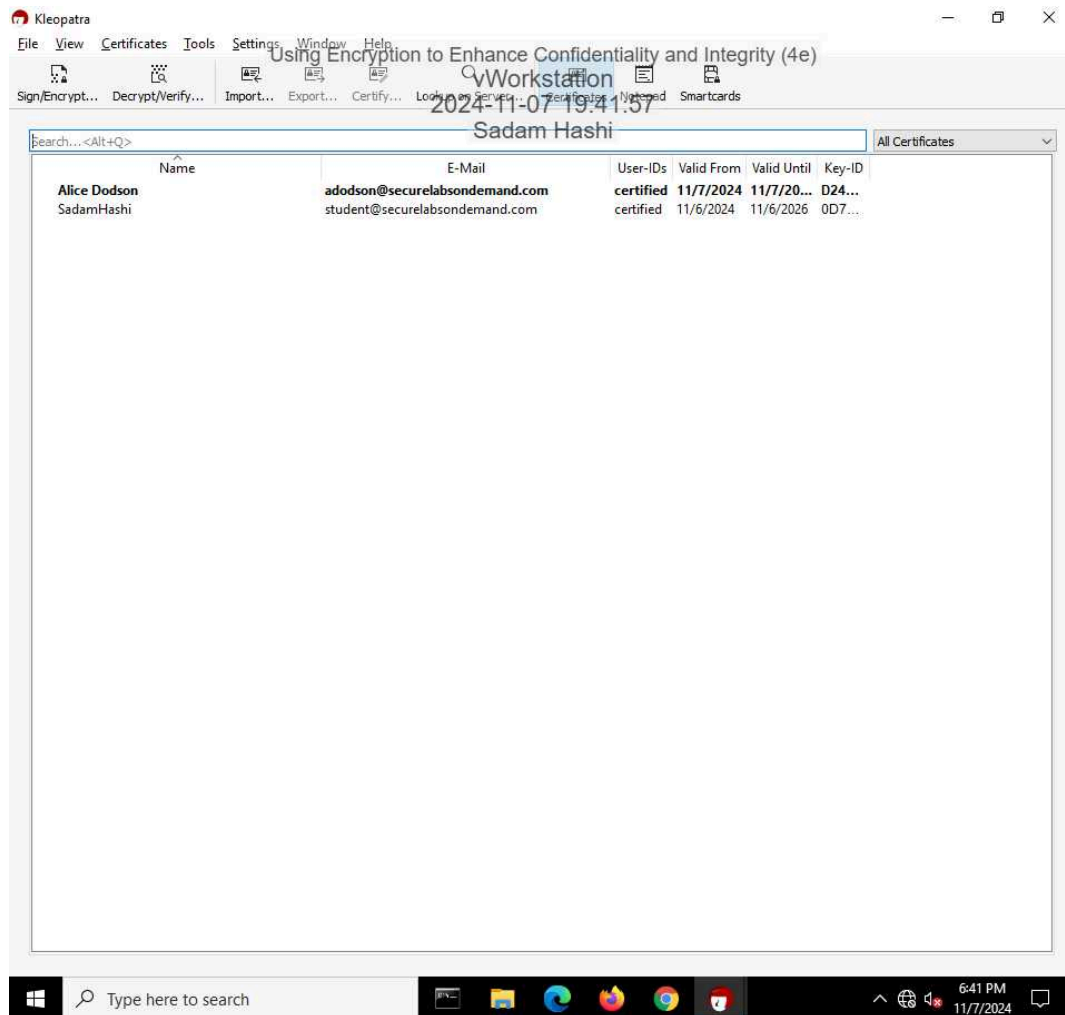
22. Make a screen capture showing the **fingerprint** for Alice's key pair.



Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

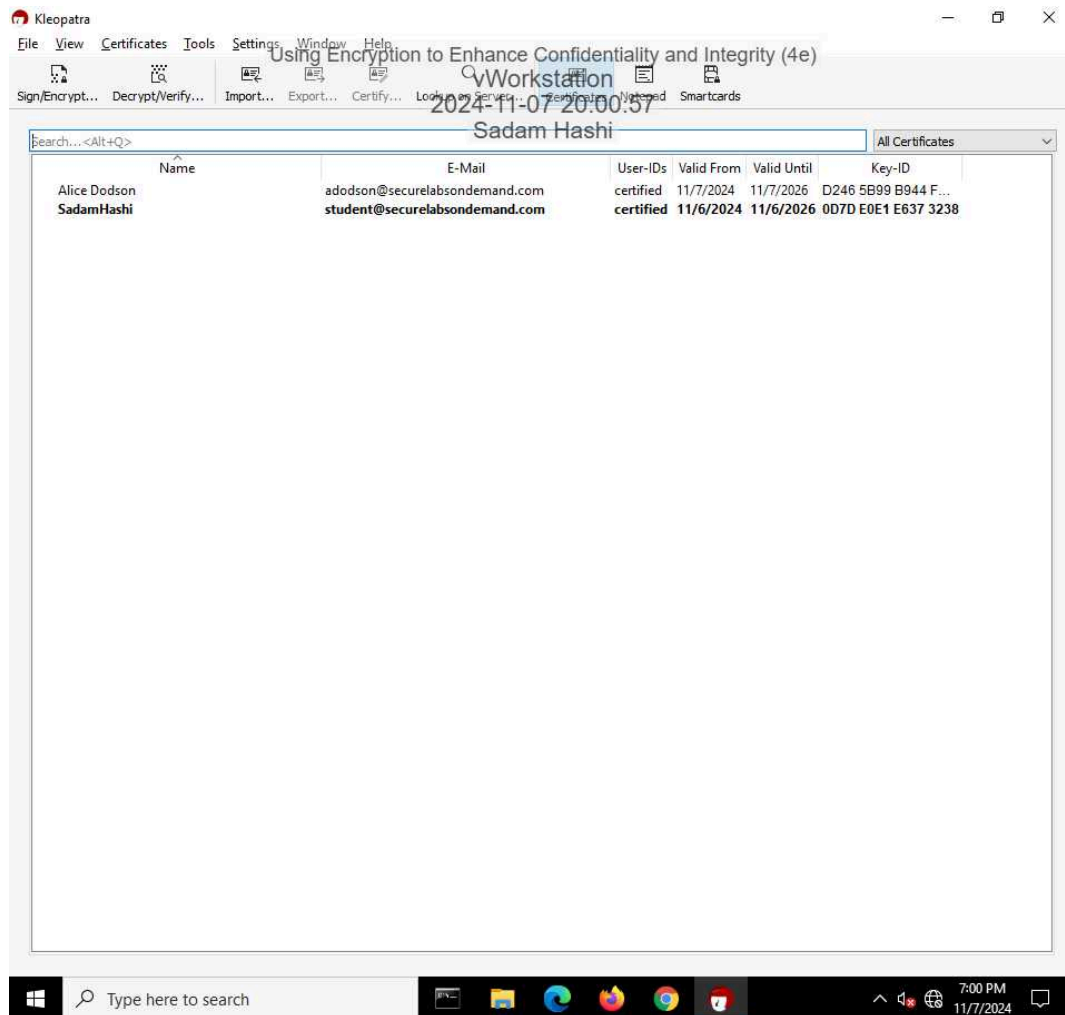
30. Make a screen capture showing your public key in Alice's certificate cache.



Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

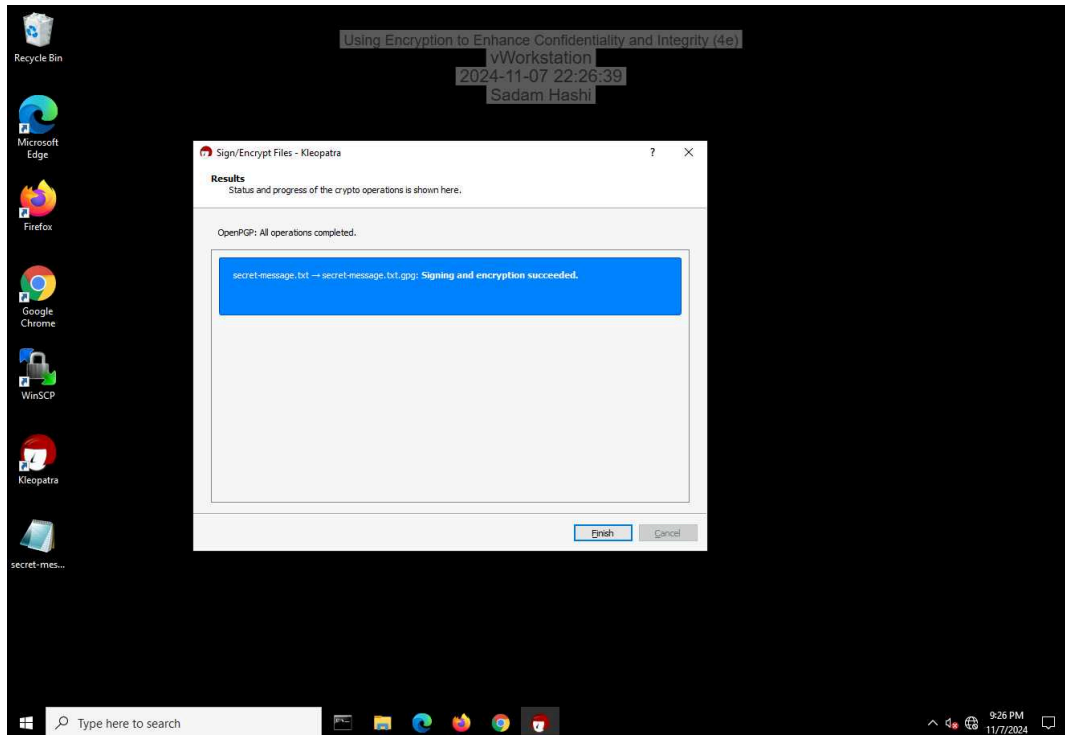
35. Make a screen capture showing Alice's public key in your certificate cache.



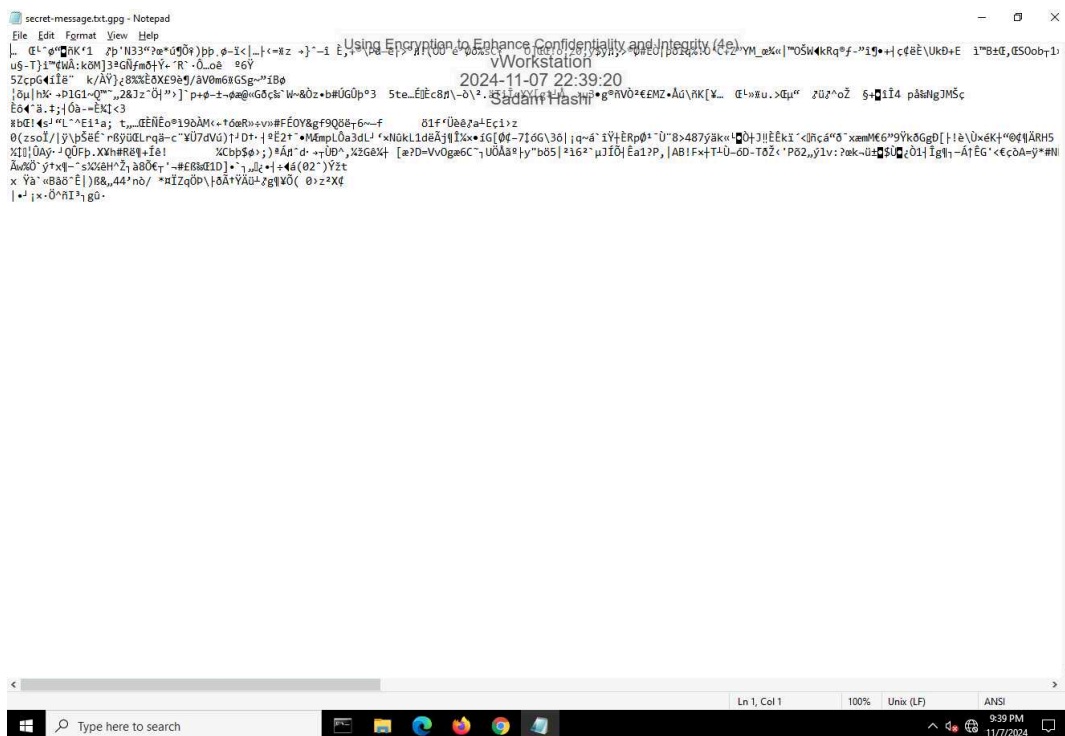
Part 2: Encrypt a File Using Asymmetric Encryption

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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

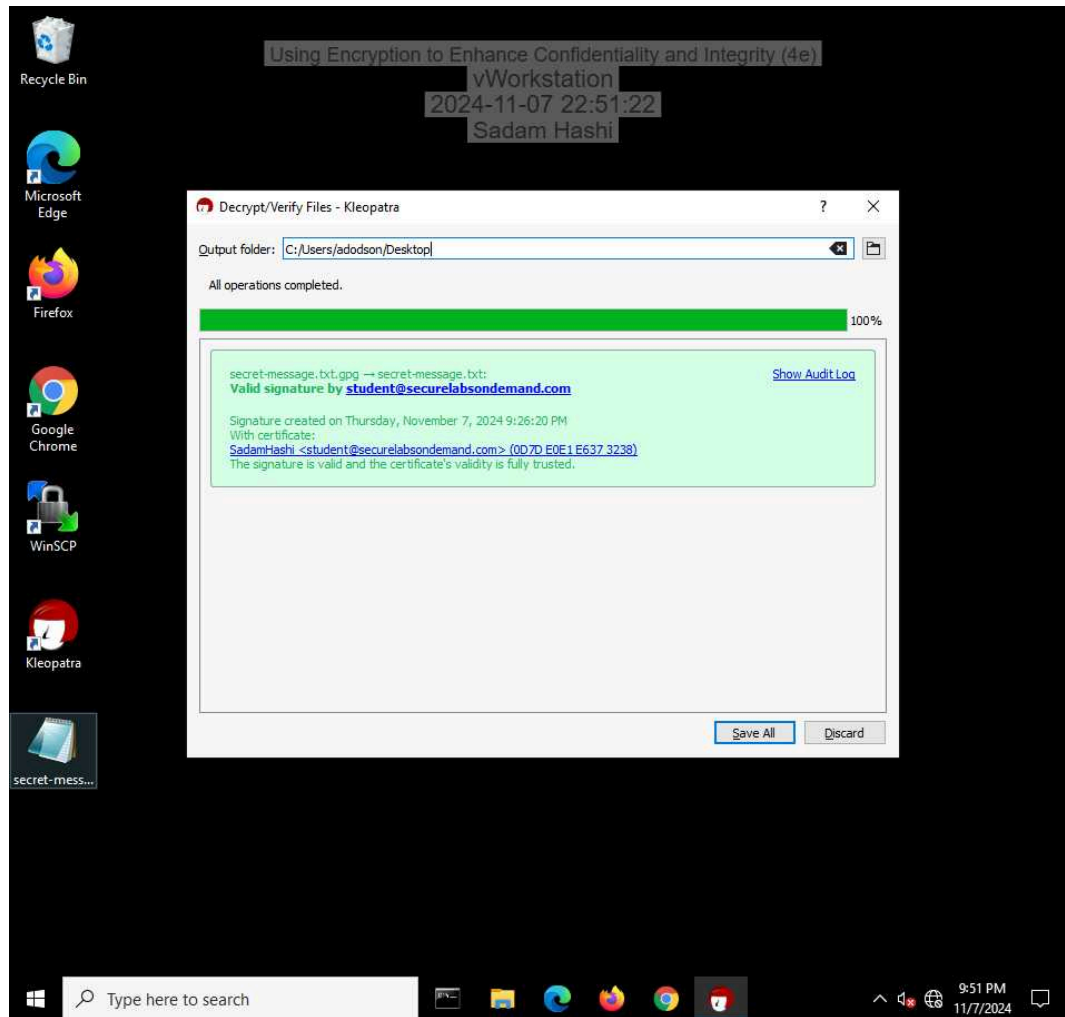


12. **Make a screen capture** showing the **ciphertext**.



Part 3: Decrypt a File Using Asymmetric Encryption

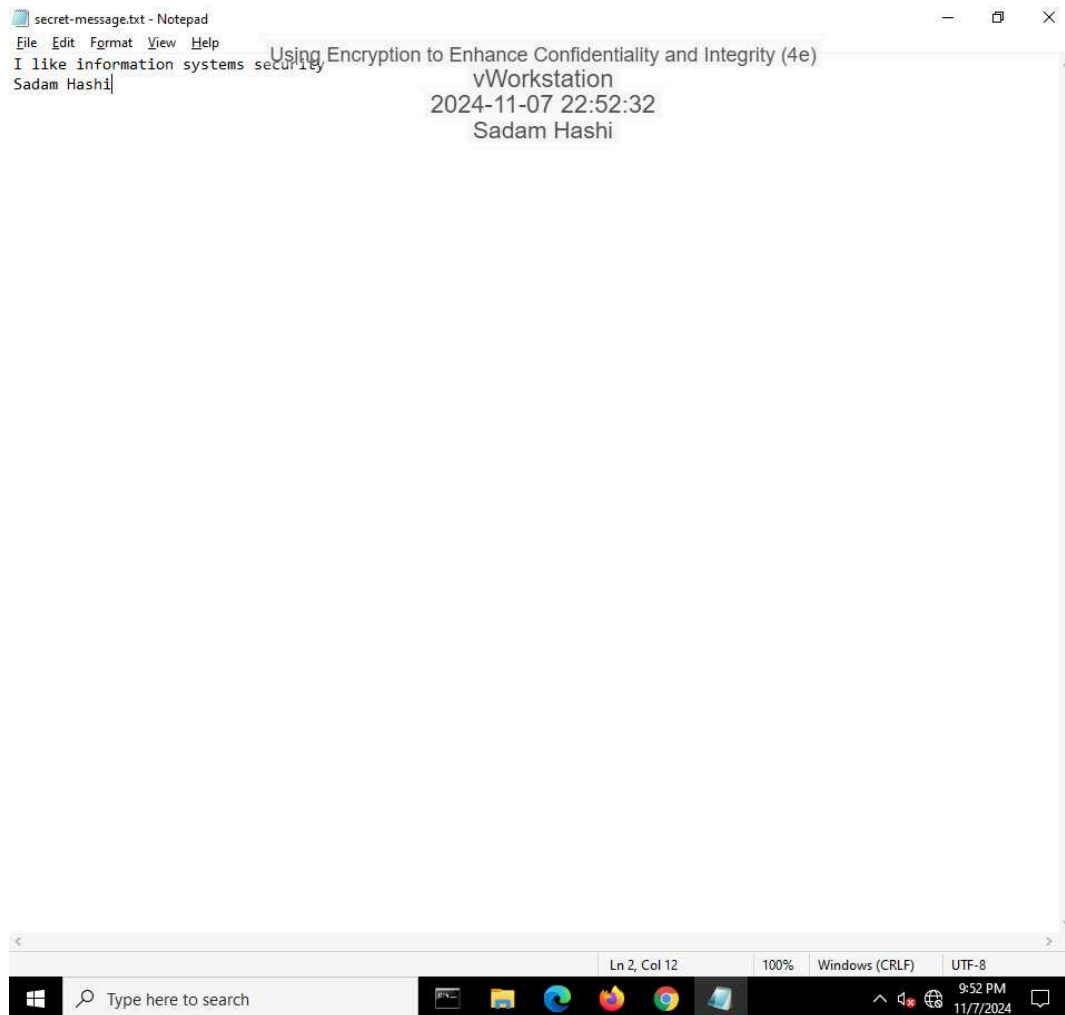
15. Make a screen capture showing the **Decrypt/Verify Files** window.



Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

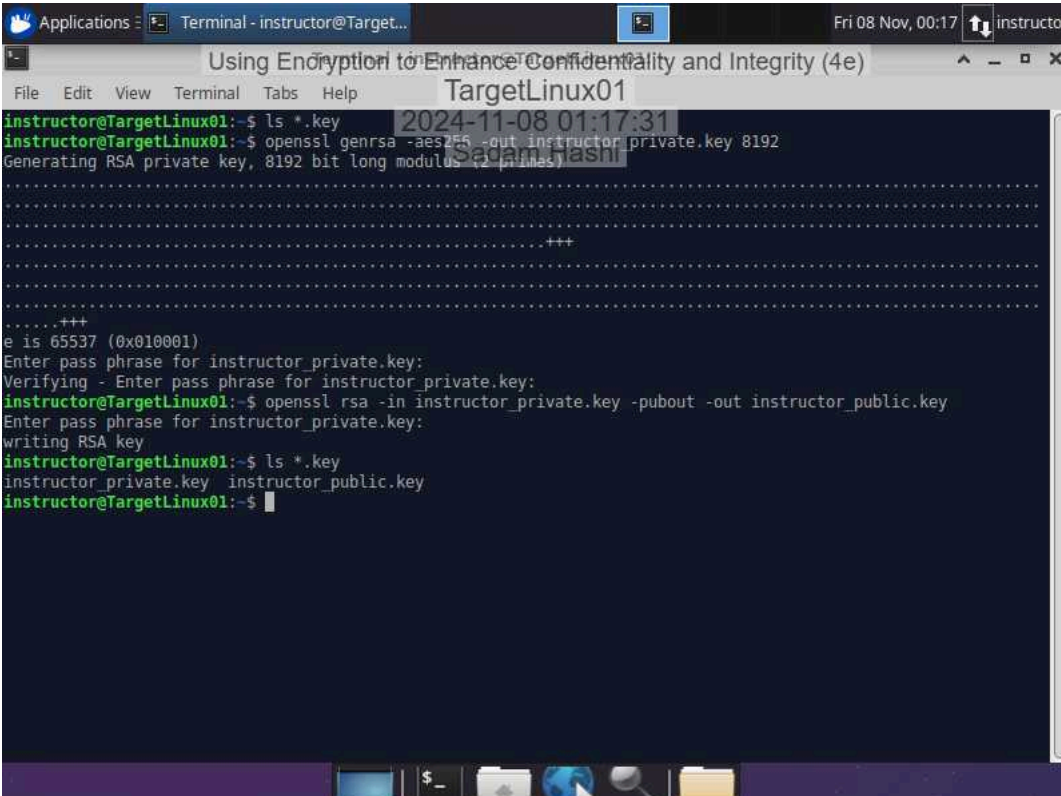
18. **Make a screen capture** showing the **decrypted secret-message.txt** file in Notepad.



Section 2: Applied Learning

Part 1: Create an Asymmetric Key Pair

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



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

```
instructor@TargetLinux01:~$ ls *.key
instructor@TargetLinux01:~$ openssl genrsa -aes256 -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:
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:~$
```

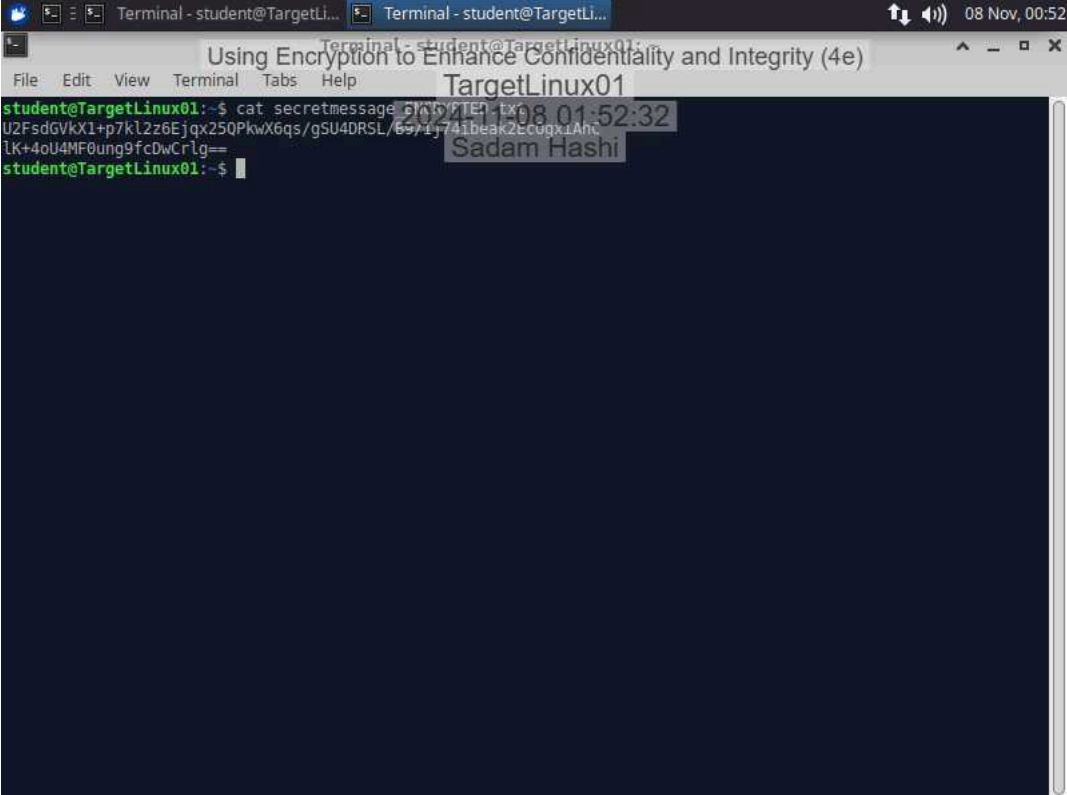
Watermarks for "TargetLinux01", "2024-11-08 01:17:31", and "Sadam Hashi" are visible over the terminal content.

Part 2: Encrypt a File Using Symmetric Encryption

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

sadam

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



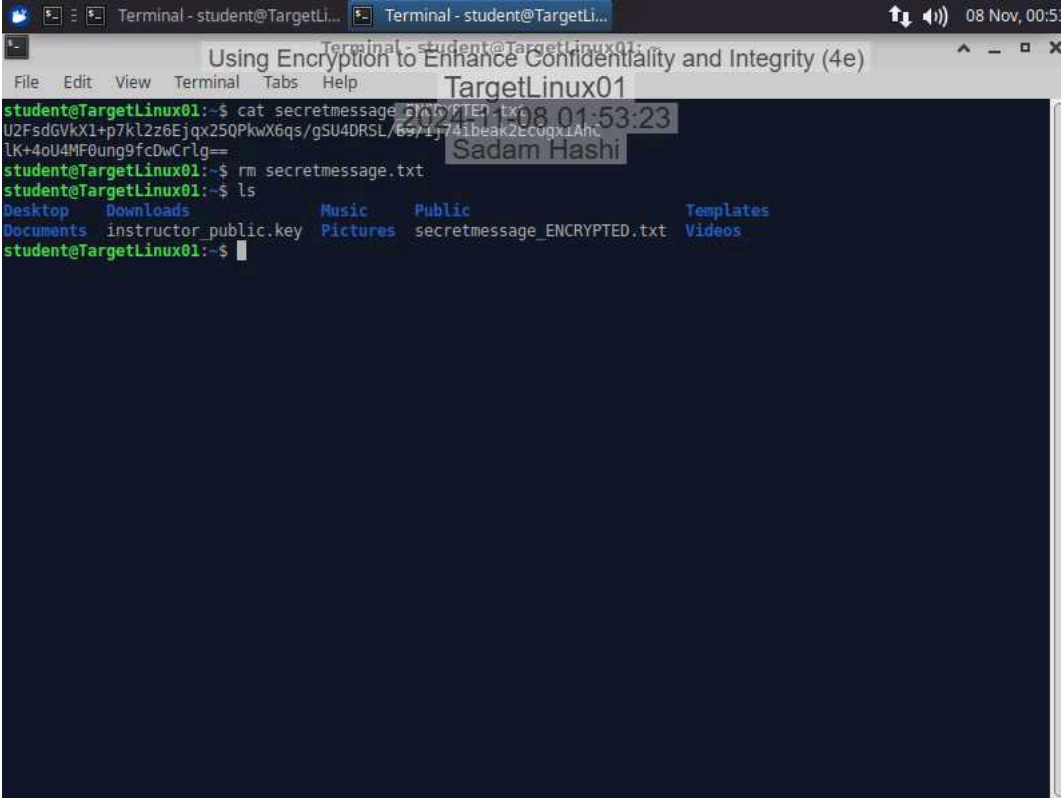
A terminal window titled "Terminal - student@TargetLinux01" displays the command `cat secretmessage_ENCRYPTED.txt` and its output. The output is a long string of ciphertext: `U2FsdGVkX1+p7kl2z6Ejqx250PkwX6qs/gSU4DRSL/6971741beak2Ecogx1AntLK+4oU4MF0ung9fcDwCrlg==`. The terminal window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The title bar shows "TargetLinux01" and the system clock "08 Nov, 00:52".

```
student@TargetLinux01:~$ cat secretmessage_ENCRYPTED.txt
U2FsdGVkX1+p7kl2z6Ejqx250PkwX6qs/gSU4DRSL/6971741beak2Ecogx1AntLK+4oU4MF0ung9fcDwCrlg==
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" is shown. The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content shows the following commands and output:

```
student@TargetLinux01:~$ cat secretmessage_ENCRIPTED.txt
U2FsdGVkX1+p7kl2z6Ejqx25QPkwX6qs/gSU4DR5L/697174ibeak2EcogxzAnc
LK+4oU4MF0ung9fcDwCrlg==
student@TargetLinux01:~$ rm secretmessage.txt
student@TargetLinux01:~$ ls
Desktop  Downloads  Music      Public      Templates
Documents instructor_public.key Pictures    secretmessage_ENCRYPTED.txt Videos
```

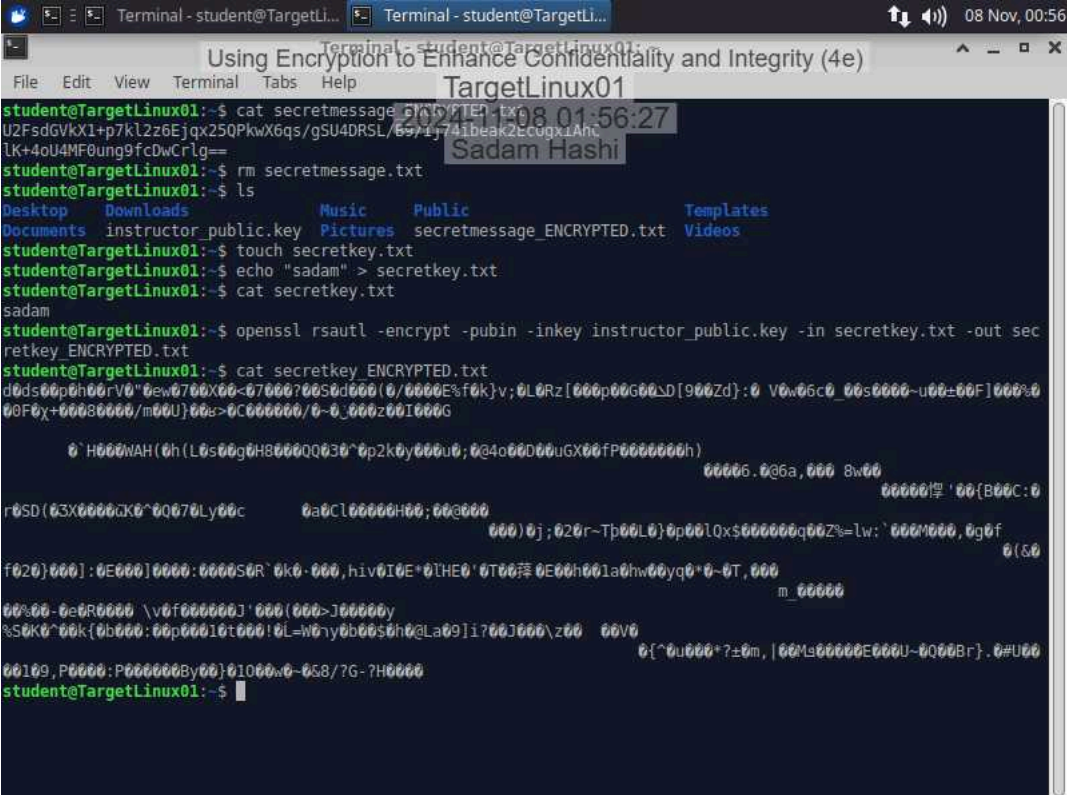
The terminal window also displays a timestamp "08 Nov, 00:53" in the top right corner. There are some redaction boxes over the terminal content, including one over the filename "secretmessage_ENCRIPTED.txt" and another over the output "secretmessage_ENCRYPTED.txt".

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.

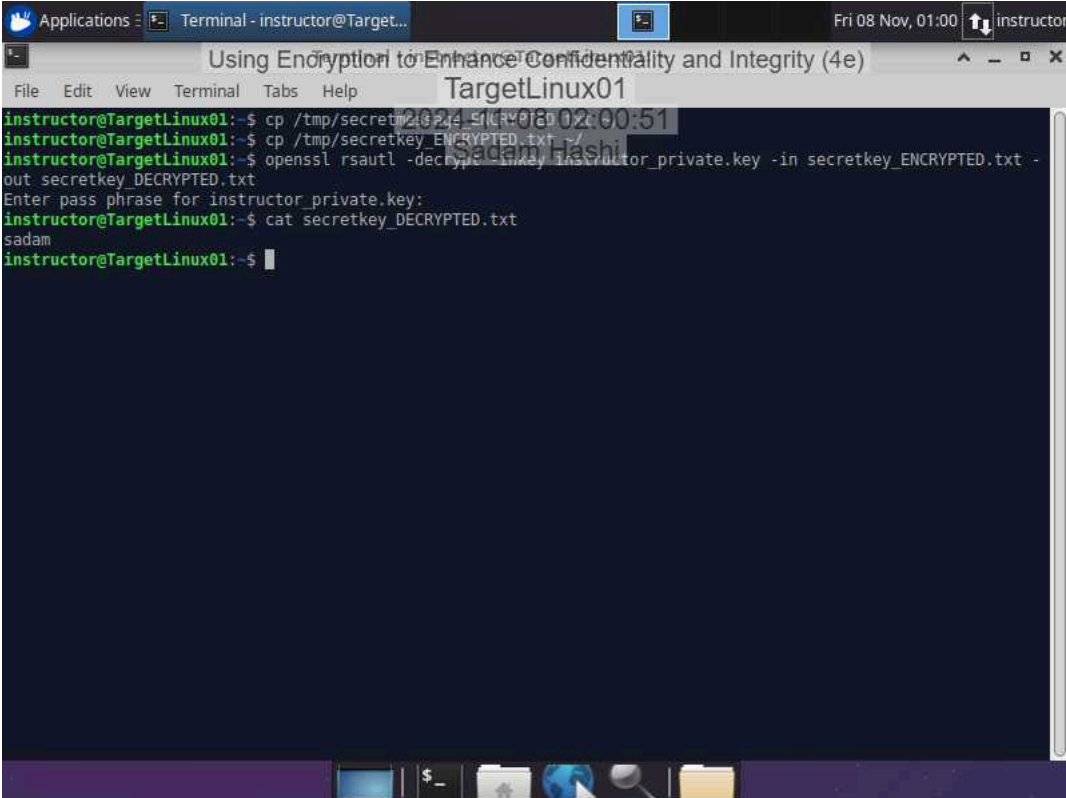


```
Terminal - student@TargetLinux01: ~
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
student@TargetLinux01:~$ cat secretmessage.txt
U2FsdGVkX1+p7kL2z6Ejqx250PkwX6qs/gSU4DRSL/697174ibeaK2Ecugx1Anc
LK+4oU4MF0ung9fcDwCrlg==
student@TargetLinux01:~$ rm secretmessage.txt
student@TargetLinux01:~$ ls
Desktop  Downloads  Music  Public  Templates
Documents  instructor_public.key  Pictures  secretmessage_ENCRYPTED.txt  Videos
student@TargetLinux01:~$ touch secretkey.txt
student@TargetLinux01:~$ echo "sadam" > secretkey.txt
student@TargetLinux01:~$ cat secretkey.txt
sadam
student@TargetLinux01:~$ openssl rsautl -encrypt -pubin -inkey instructor_public.key -in secretkey.txt -out secretkey_ENCRYPTED.txt
student@TargetLinux01:~$ cat secretkey_ENCRYPTED.txt
d0ds00p0h00rV0"0ew0700X00<07000?00S0d000(0/0000E$foK}v;0L0Rz[000p00G00ΔD[900Zd]:0 V0w06c0_00s0000~u00±00F]000%0
00F0x+00080000/m00U}00e>0C000000/0~0_000z00I000G
0`H000WAH(0h(L0s00g0H8000QQ030^0p2k0y000u0;0@4o00D00UGX00fP0000000h)
00006.0@6a,000 8w00
00000!學'00{B00C:0
r0SD(03X0000GK0^0Q070Ly00c 0a0Cl00000H00;00c000
000)0j;020r~Tp00L0}0p00lQx$000000q00Z%=lw:'000M000,0g0f
0(Δ0
f020}000]:0E000]0000:0000S0R`0k0.000,hiv0IE*0THE0'0T00萍0E00h001a0hw00yq0*0~0T,000
m_00000
00%00-0e0R0000 \v0f000000J'000(000>J00000y
%S0K0~00k{0b000:00p00010t000!0L=w0ry0b00$0h0@La09]i700J000\z00 00V0
00109,P0000:P0000008y00}01000w0~058/7G-?H0000
0{~0u000*?±0m,[00M900000E000U~0Q00Br}.0#U00
student@TargetLinux01:~$
```

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.**



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

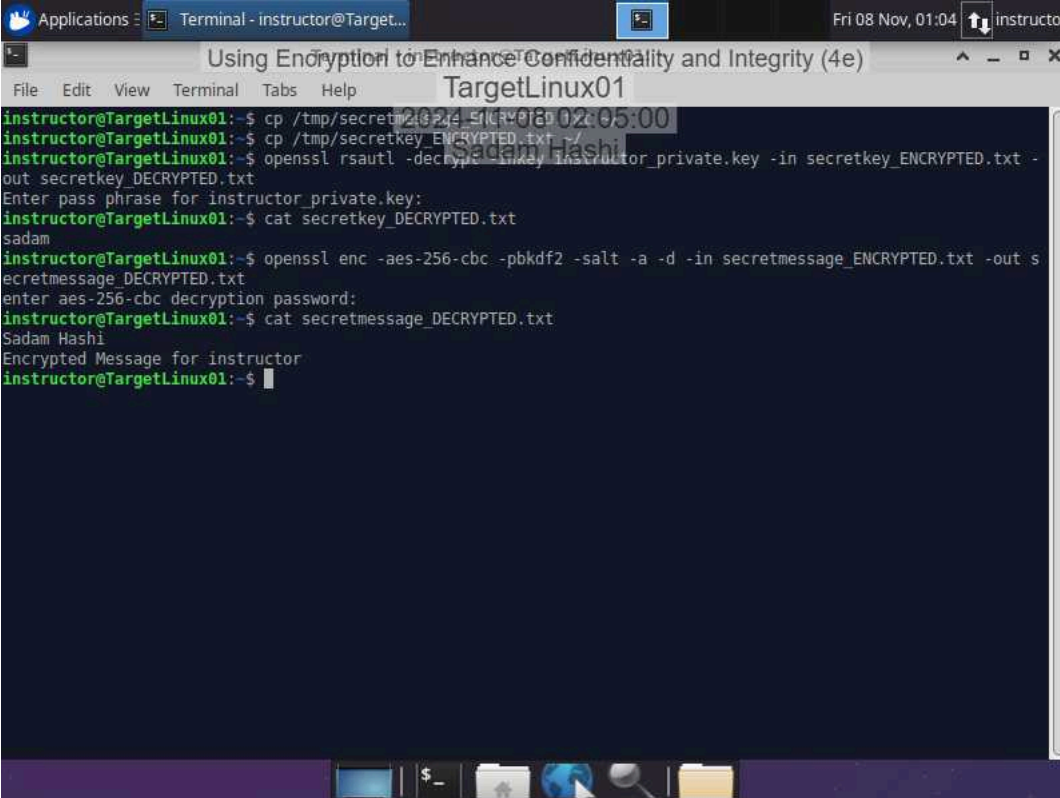
```
instructor@TargetLinux01:~$ cp /tmp/secretkey_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ cp /tmp/secretkey_ENCRYPTED.txt ~/
instructor@TargetLinux01:~$ openssl rsautl -decrypt -inkey instructor_private.key -in secretkey_ENCRYPTED.txt -
out secretkey_DECRYPTED.txt
Enter pass phrase for instructor_private.key:
instructor@TargetLinux01:~$ cat secretkey_DECRYPTED.txt
sadam
instructor@TargetLinux01:~$
```

The terminal window is overlaid on a desktop environment. The desktop background is dark blue. At the top, there is a window title bar with the text "Using Encryption to Enhance Confidentiality and Integrity (4e)". The desktop also shows a taskbar at the bottom with icons for a terminal, a file manager, a web browser, and a search icon. The system clock in the top right corner shows "Fri 08 Nov, 01:00".

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.

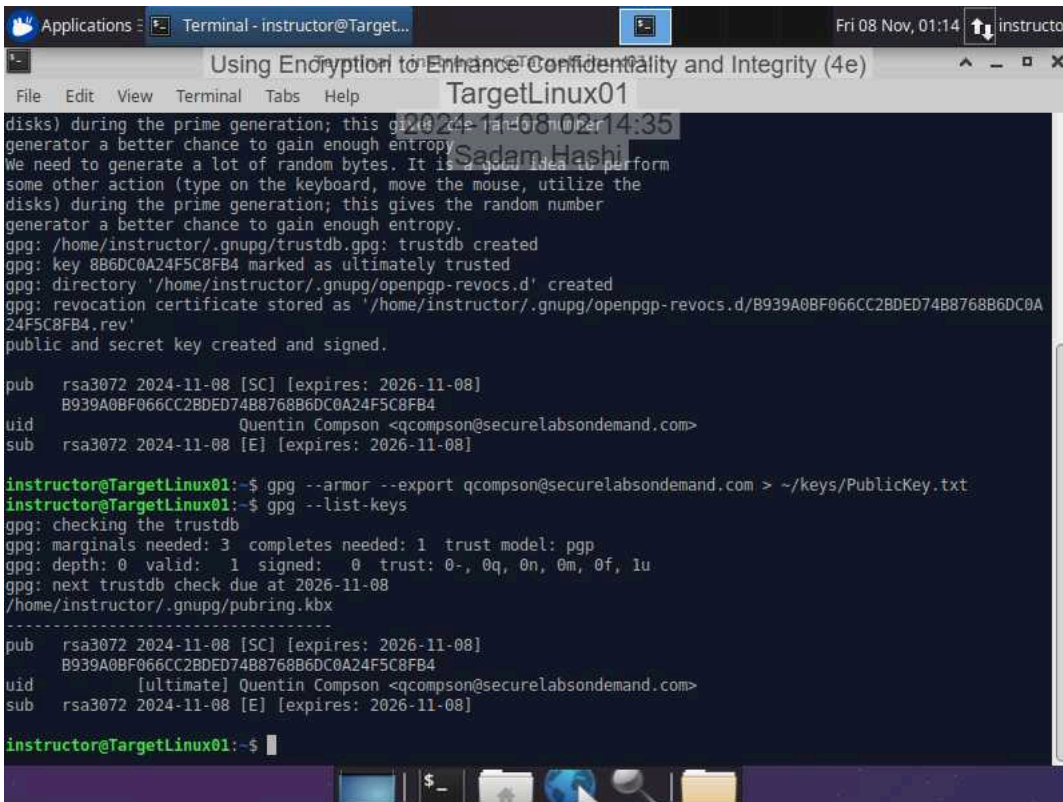
A screenshot of a terminal window titled "Terminal - instructor@TargetLinux01" with a timestamp of "Fri 08 Nov, 01:04". The window shows a series of commands and their outputs. The commands include copying files, using openssl to decrypt a key, and then using openssl to encrypt a message. The final output shows the decrypted message "Sadam Hashi" and "Encrypted Message for instructor".

```
instructor@TargetLinux01:~$ cp /tmp/secretmessage.txt ./
instructor@TargetLinux01:~$ cp /tmp/secretkey_ENCRYPTED.txt ./
instructor@TargetLinux01:~$ openssl rsautl -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
sadam
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
Sadam Hashi
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.



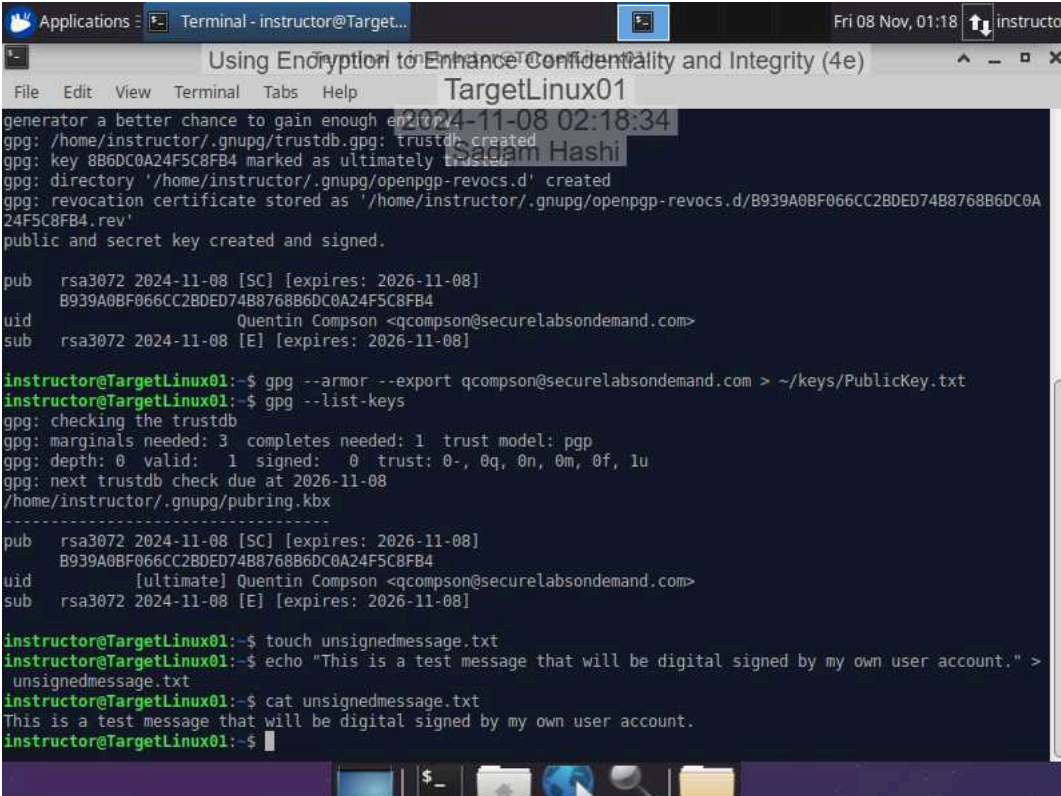
The screenshot shows a terminal window titled "Terminal - instructor@TargetLinux01" with a timestamp of "Fri 08 Nov, 01:14". The window displays the output of GPG commands. It starts with a message about entropy generation. Then, it shows the creation of a trust database, a key pair (rsa3072 2024-11-08 [SC] [expires: 2026-11-08]), and a revocation certificate. The key fingerprint is displayed as B939A0BF066CC2BDED74B8768B6DC0A24F5C8FB4. The user is identified as Quentin Compson <qcompson@securelabsondemand.com>. Finally, the key is exported to ~/keys/PublicKey.txt and listed using gpg --list-keys.

```
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 2026-11-08
/home/instructor/.gnupg/pubring.kbx
-----
pub   rsa3072 2024-11-08 [SC] [expires: 2026-11-08]
      B939A0BF066CC2BDED74B8768B6DC0A24F5C8FB4
uid   [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub   rsa3072 2024-11-08 [E] [expires: 2026-11-08]
```

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 | Fri 08 Nov, 01:18 | instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
generator a better chance to gain enough entropy
2024-11-08 02:18:34
gpg: /home/instructor/.gnupg/trustdb.gpg: trustdb created
gpg: key 8B6DC0A24F5C8FB4 marked as ultimately trusted
gpg: directory '/home/instructor/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/instructor/.gnupg/openpgp-revocs.d/B939A0BF066CC2BDED7488768B6DC0A24F5C8FB4.rev'
public and secret key created and signed.

pub   rsa3072 2024-11-08 [SC] [expires: 2026-11-08]
       B939A0BF066CC2BDED7488768B6DC0A24F5C8FB4
uid    Quentin Compson <qcompson@securelabsondemand.com>
sub    rsa3072 2024-11-08 [E] [expires: 2026-11-08]

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 2026-11-08
/home/instructor/.gnupg/pubring.kbx
-----
pub   rsa3072 2024-11-08 [SC] [expires: 2026-11-08]
       B939A0BF066CC2BDED7488768B6DC0A24F5C8FB4
uid    [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub    rsa3072 2024-11-08 [E] [expires: 2026-11-08]

instructor@TargetLinux01:~$ touch unsignedmessage.txt
instructor@TargetLinux01:~$ echo "This is a test message that will be digital signed by my own user account." > unsignedmessage.txt
instructor@TargetLinux01:~$ cat unsignedmessage.txt
This is a test message that will be digital 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.

