

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

Student:

Marc Corona

Email:

coronami@calpoly.edu

Time on Task:

4 hours, 46 minutes

Progress:

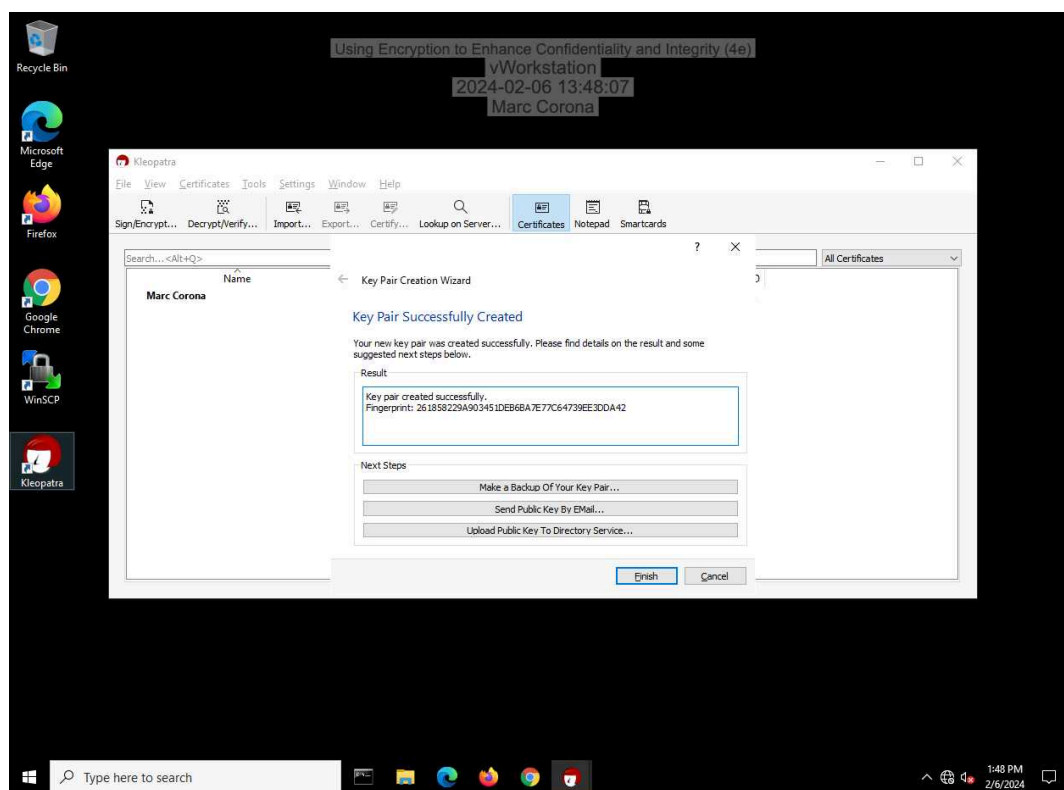
100%

Report Generated: Tuesday, February 13, 2024 at 1:07 AM

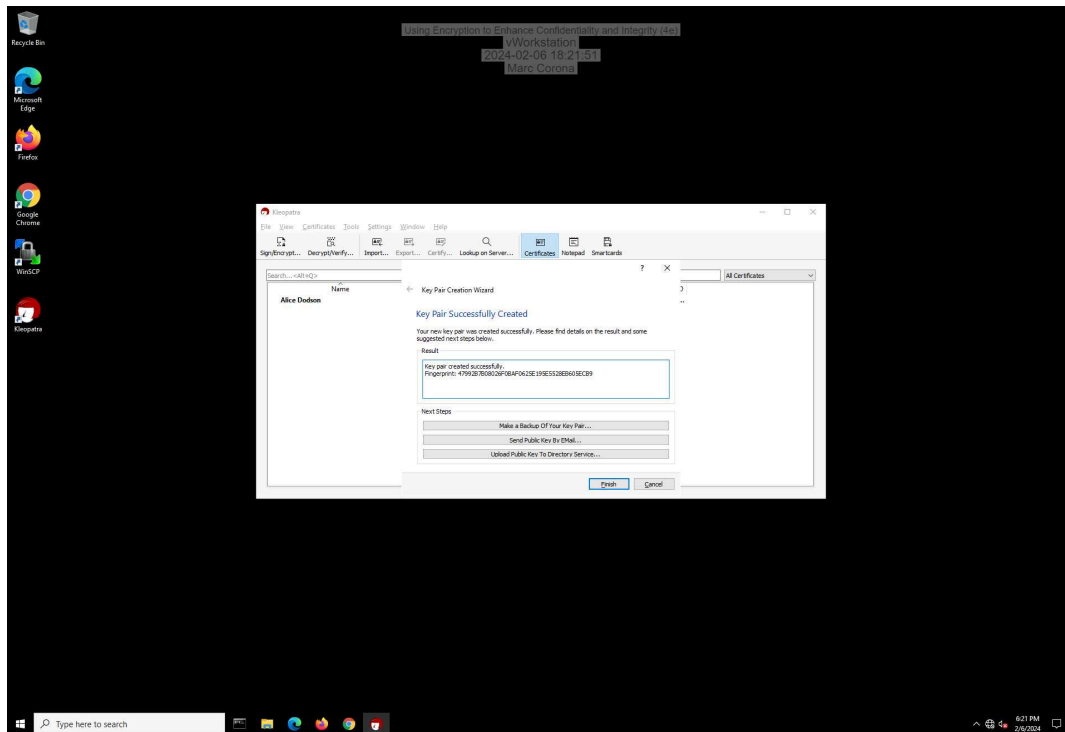
Section 1: Hands-On Demonstration

Part 1: Create and Exchange Asymmetric Encryption Keys

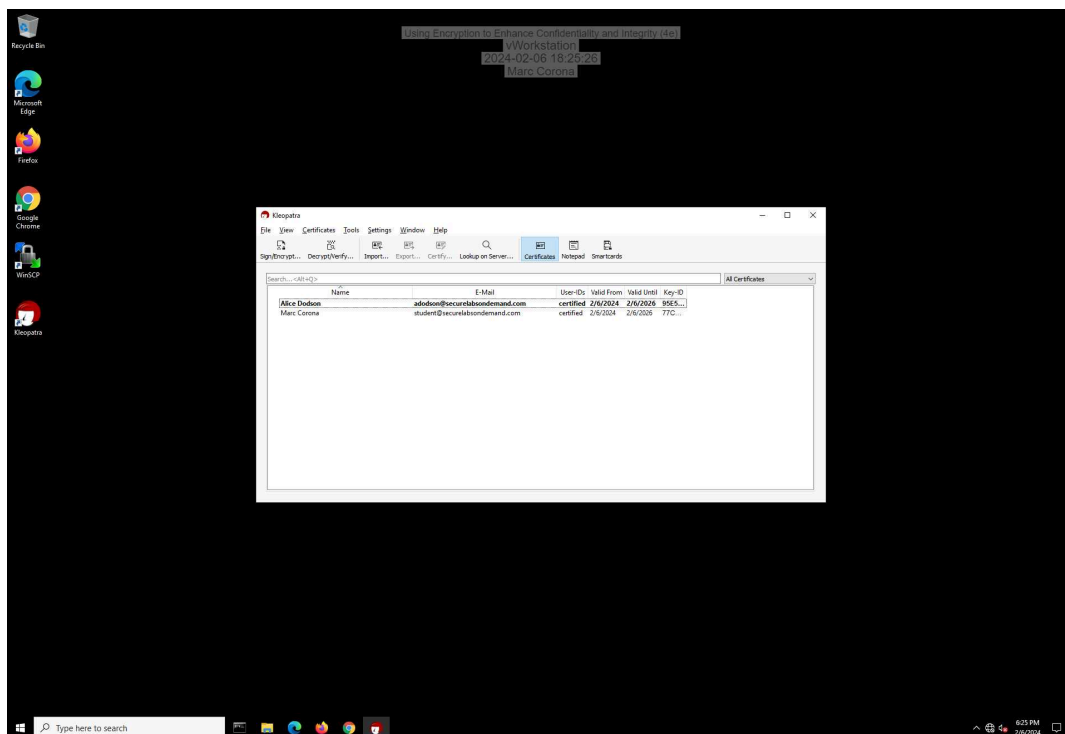
9. Make a screen capture showing the **fingerprint** for your key pair.



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



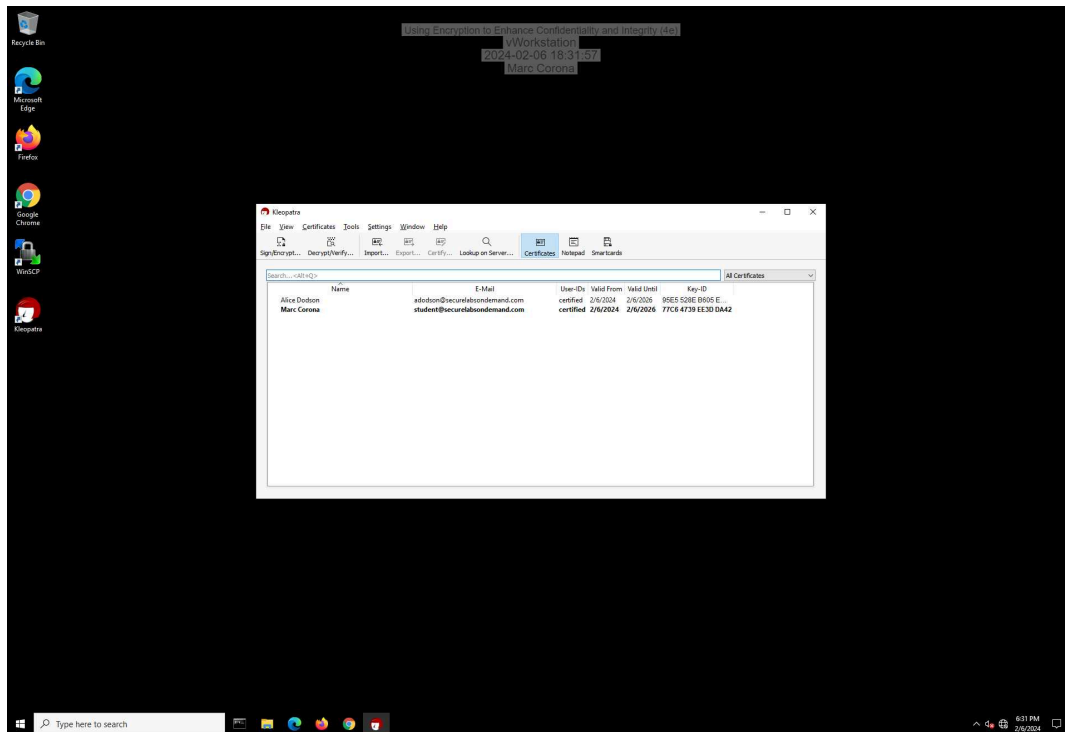
30. Make a screen capture showing your public key in Alice's certificate cache.



Using Encryption to Enhance Confidentiality and Integrity (4e)

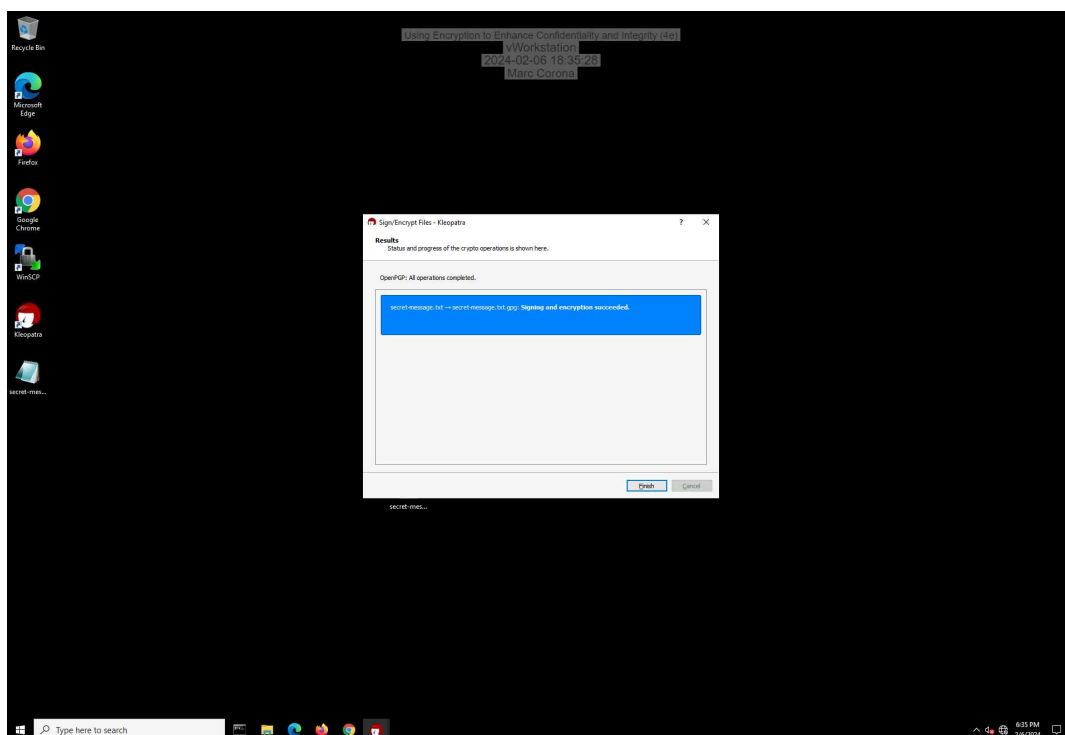
Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



Part 2: Encrypt a File Using Asymmetric Encryption

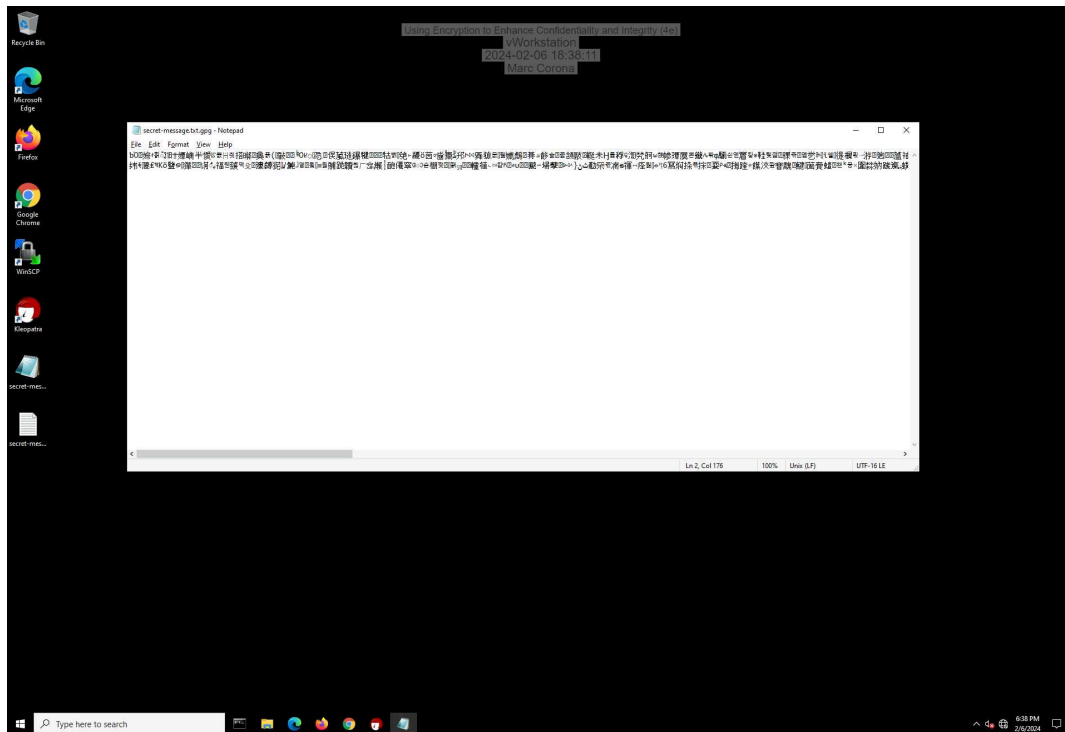
9. Make a screen capture showing the successful signing and encryption message.



Using Encryption to Enhance Confidentiality and Integrity (4e)

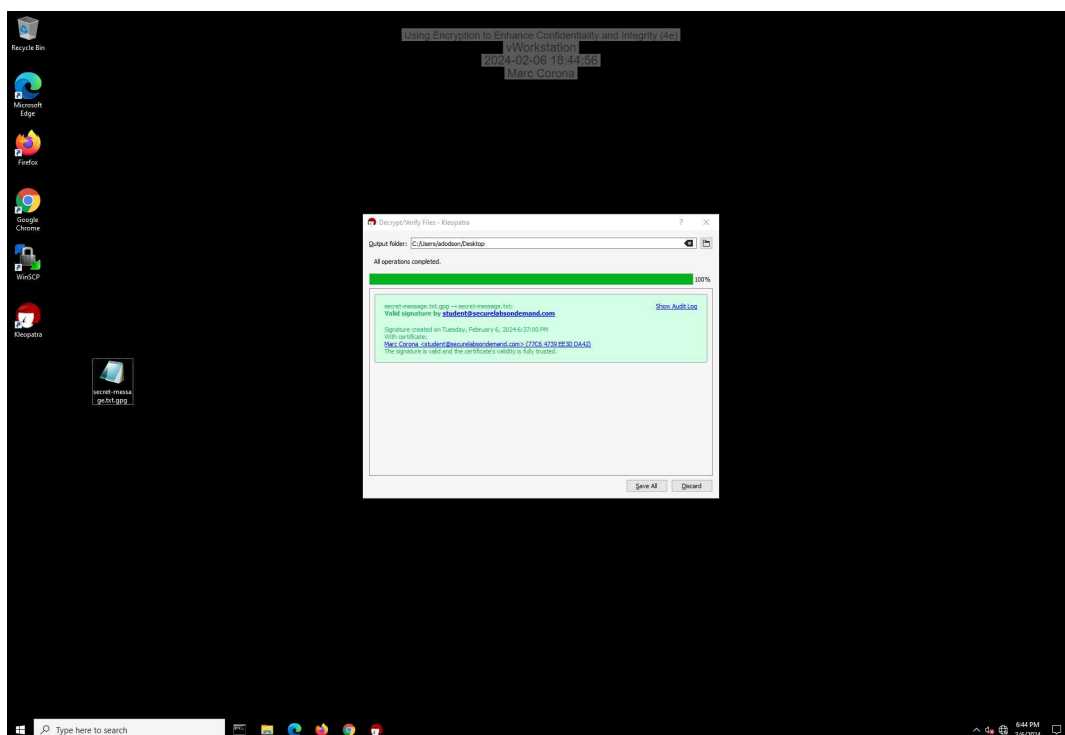
Fundamentals of Information Systems Security, Fourth Edition - Lab 05

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



Part 3: Decrypt a File Using Asymmetric Encryption

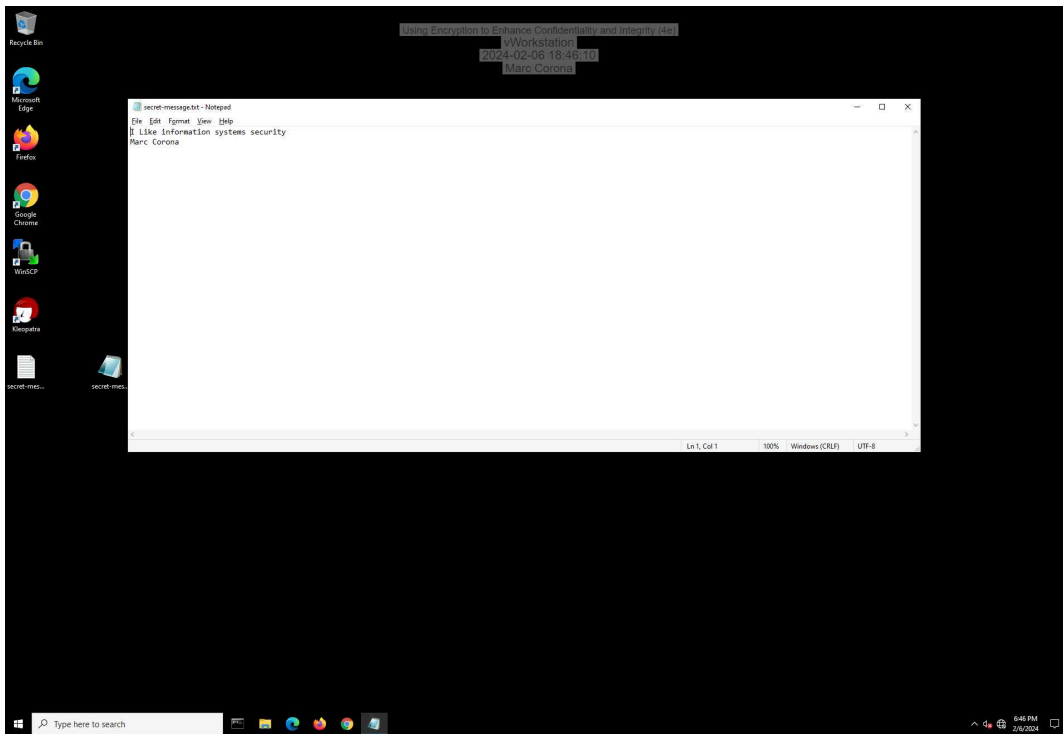
15. Make a screen capture showing the **Decrypt/Verify Files** window.



Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

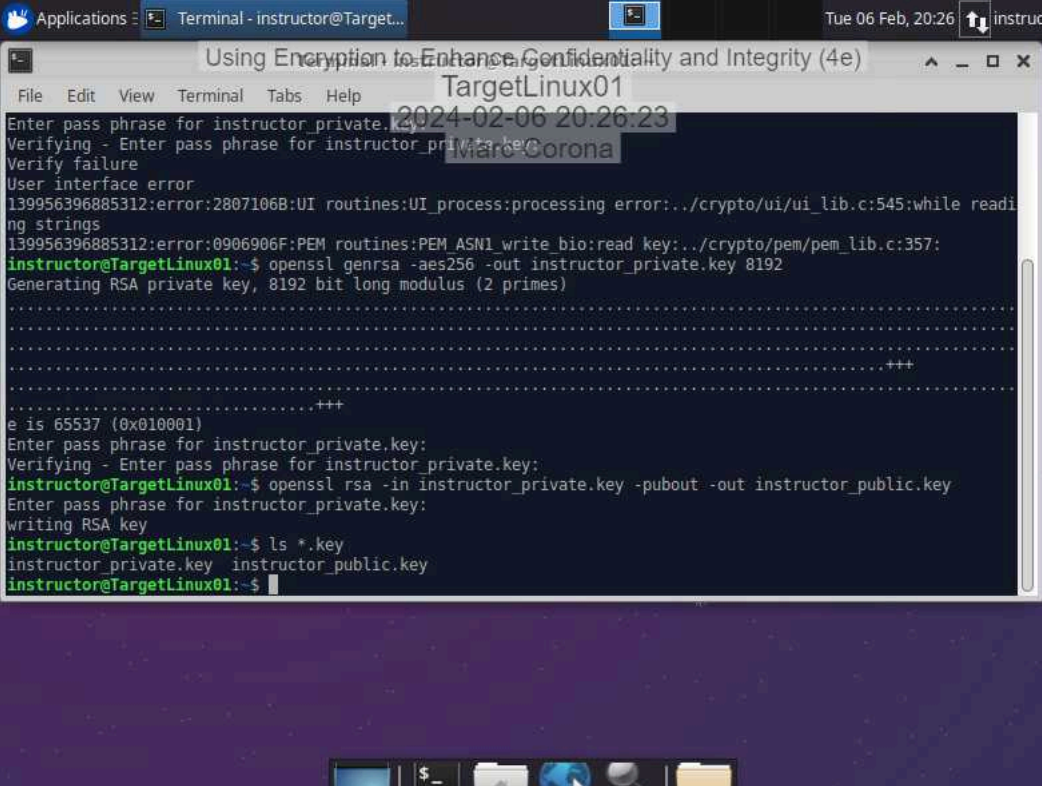
18. Make a screen capture showing the **decrypted secret-message.txt** file in Notepad.



Section 2: Applied Learning

Part 1: Create an Asymmetric Key Pair

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



```
Applications ▢ Terminal - instructor@Target... Tue 06 Feb, 20:26 instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-06 20:26:23
Enter pass phrase for instructor_private.key:
Verifying - Enter pass phrase for instructor_private.key:
Verify failure
User interface error
139956396885312:error:2807106B:UI routines:UI_process:processing error:../crypto/ui/ui_lib.c:545:while reading strings
139956396885312:error:0906906F:PEM routines:PEM_ASN1_write_bio:read key:../crypto/pem/pem_lib.c:357:
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:~$
```

Part 2: Encrypt a File Using Symmetric Encryption

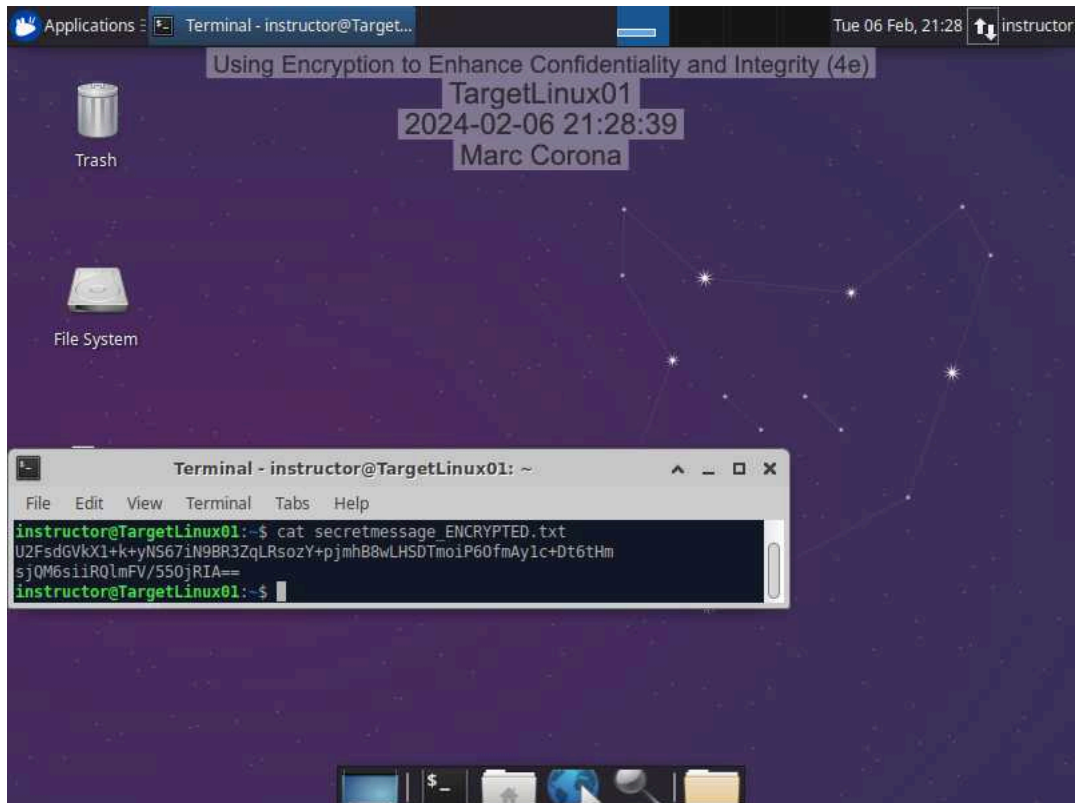
11. Document the password you used to symmetrically encrypt the file.

L!^erp00l!

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

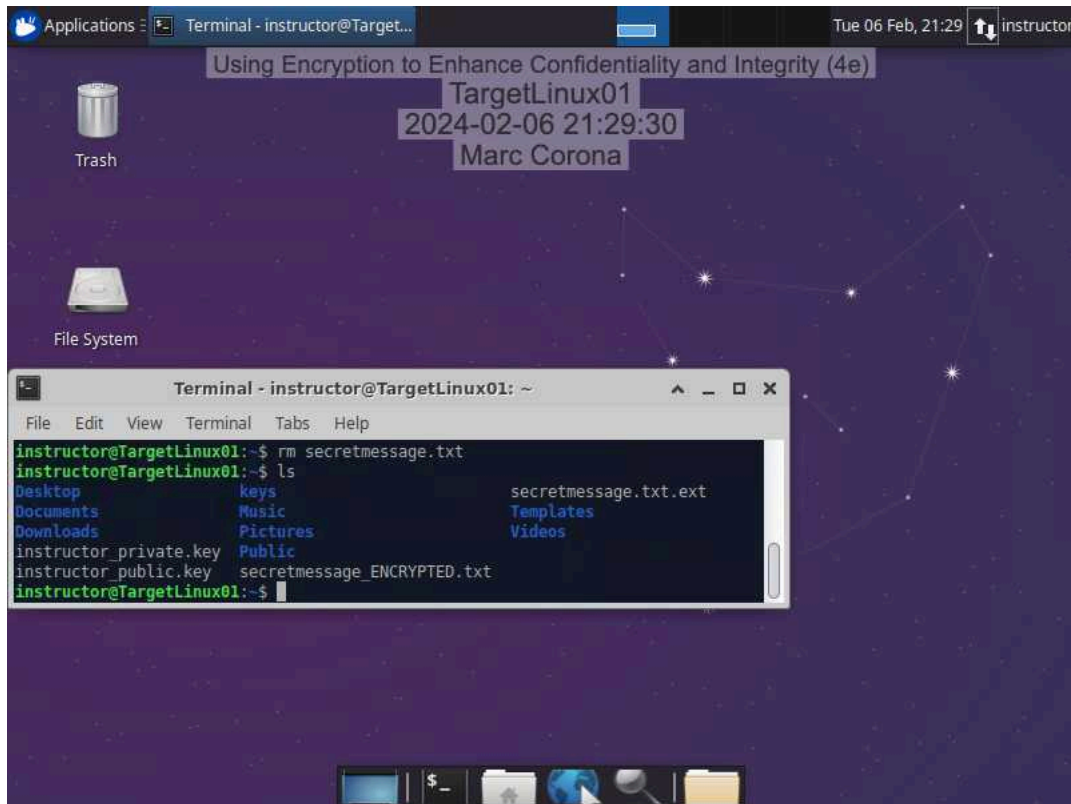
13. **Make a screen capture** showing the **ciphertext** in the **secretmessage_ENCRYPTED.txt** file.



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**.

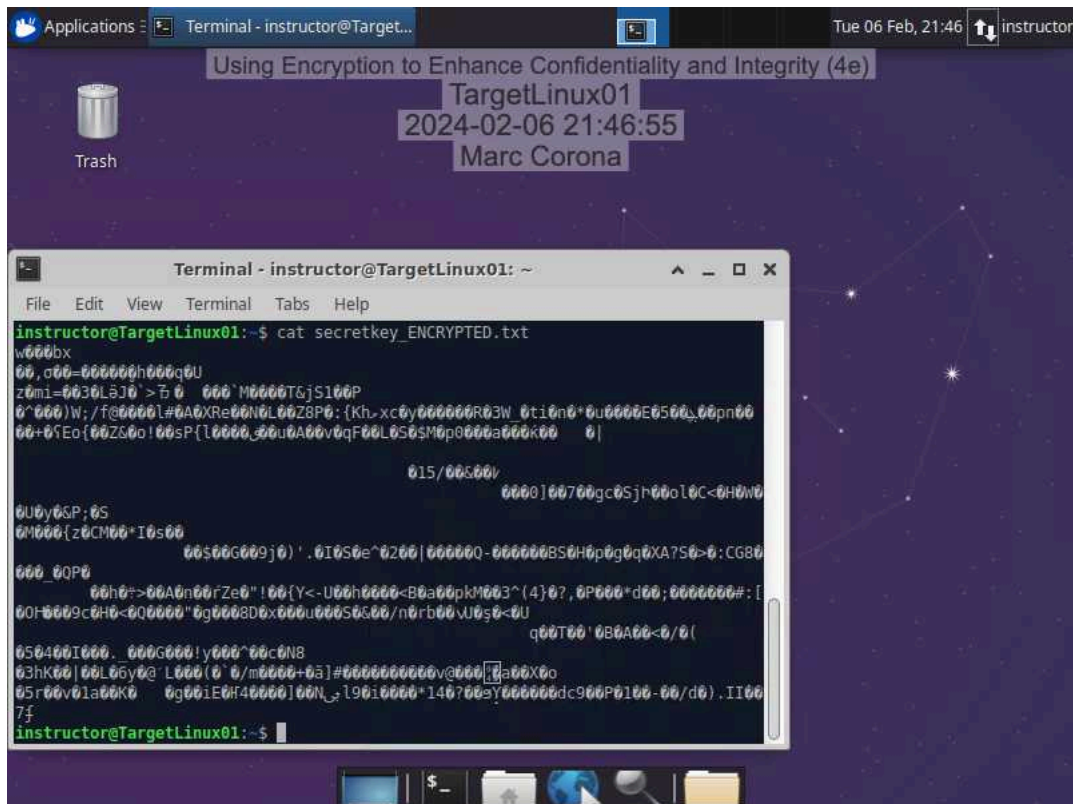


Part 3: Transfer and Decrypt a File Using Hybrid Cryptography

Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

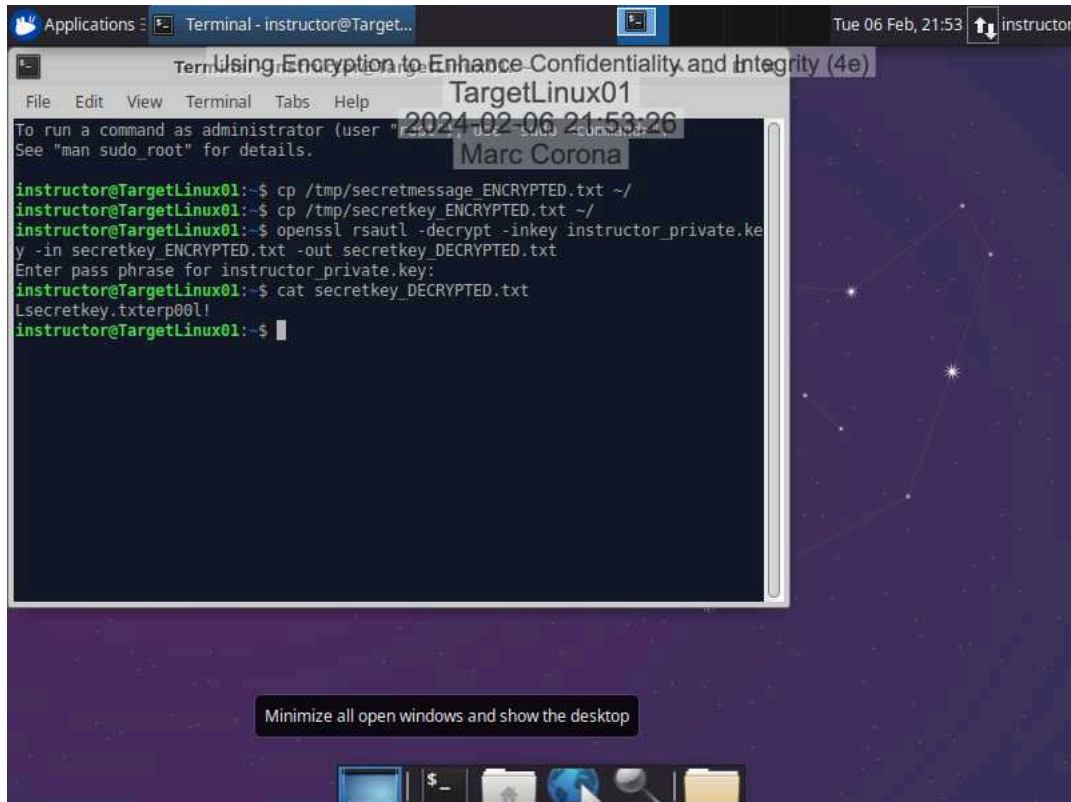
6. Make a screen capture showing the encrypted contents of the `secretkey_ENCRYPTED.txt` file.



Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

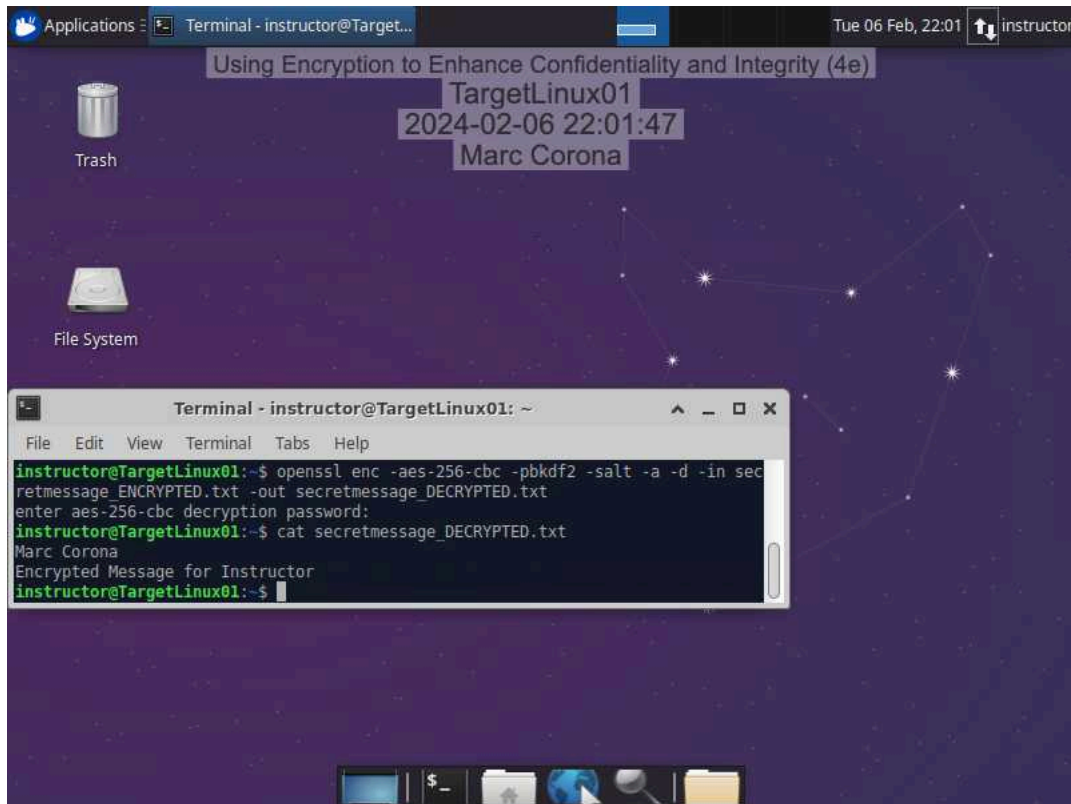
17. **Make a screen capture** showing the **decrypted contents of the secretkey_DECRYPTED.txt file.**



Using Encryption to Enhance Confidentiality and Integrity (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 05

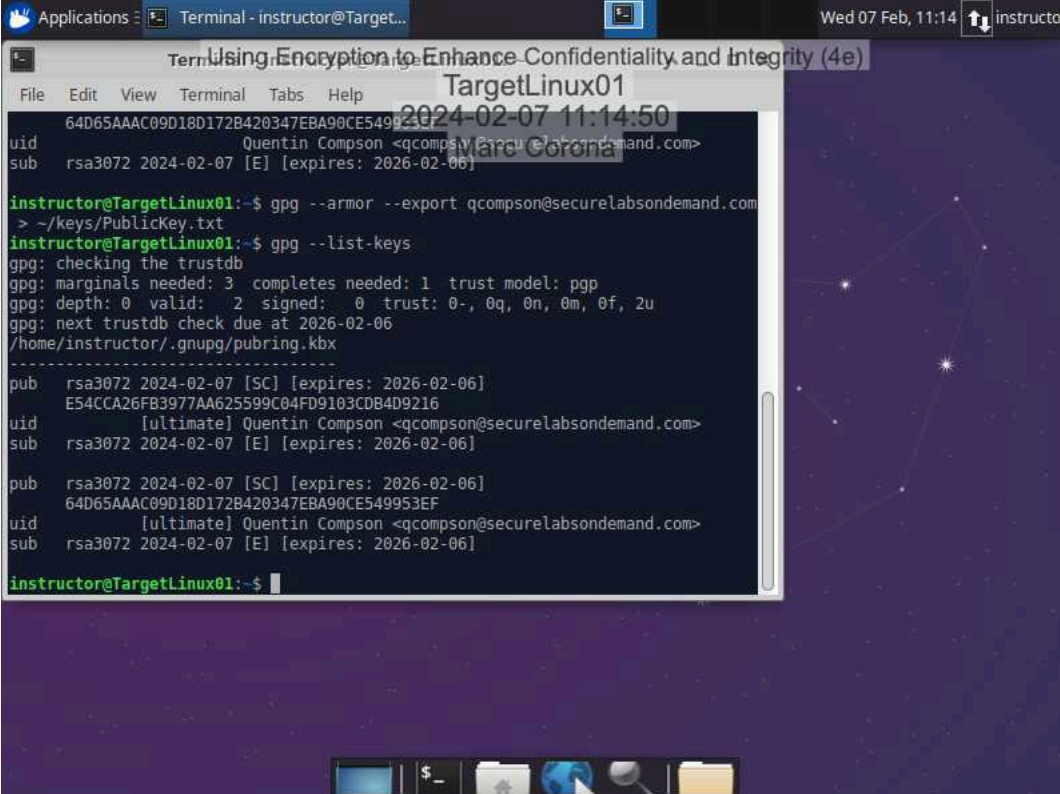
21. Make a screen capture showing the **contents of the secretmessage_DECRYPTED** file.



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.



```
Applications ▢ Terminal - instructor@Target... Wed 07 Feb, 11:14 instructor
Using Encryption to Enhance Confidentiality and Integrity (4e)
TargetLinux01
2024-02-07 11:14:50
64D65AAAC09D18D172B420347EBA90CE54992307
uid      Quentin Compson <qcompson@securelabsondemand.com>
sub      rsa3072 2024-02-07 [E] [expires: 2026-02-06]

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: 2 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2026-02-06
/home/instructor/.gnupg/pubring.kbx
-----
pub      rsa3072 2024-02-07 [SC] [expires: 2026-02-06]
         E54CCA26FB3977AA625599C04FD9103CDB4D9216
uid      [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub      rsa3072 2024-02-07 [E] [expires: 2026-02-06]

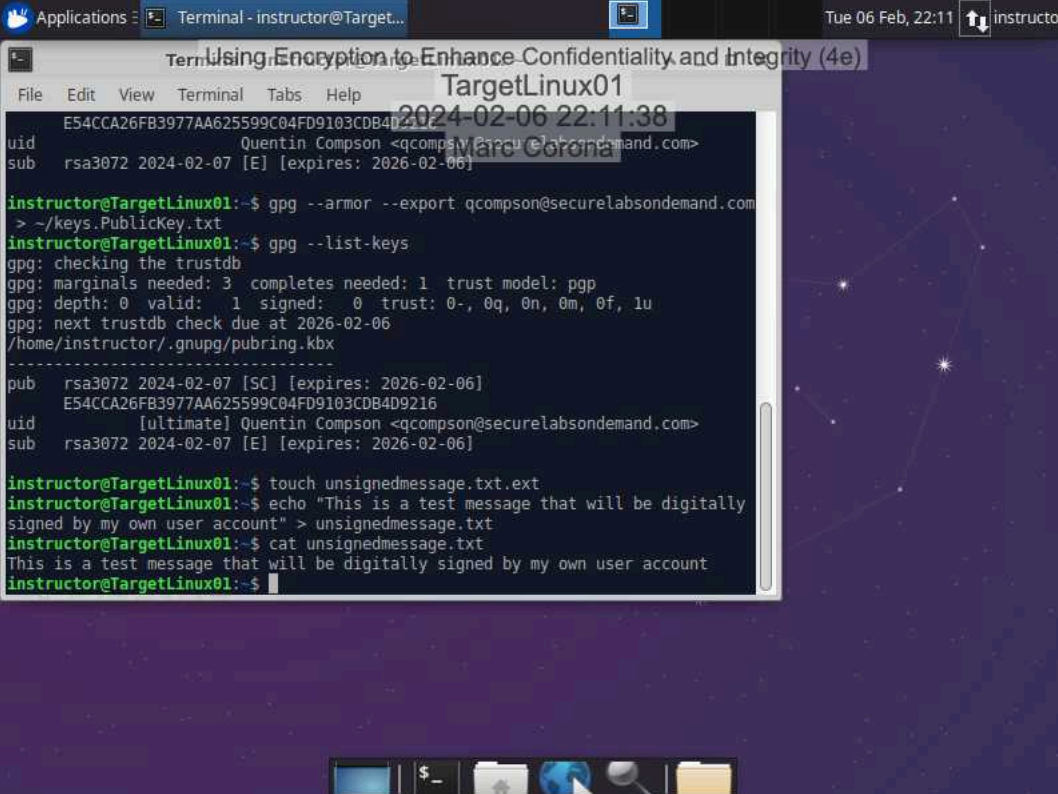
pub      rsa3072 2024-02-07 [SC] [expires: 2026-02-06]
         64D65AAAC09D18D172B420347EBA90CE549953EF
uid      [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub      rsa3072 2024-02-07 [E] [expires: 2026-02-06]

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@Target..." with a dark background and light text. The terminal output is as follows:

```
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 2026-02-06
/home/instructor/.gnupg/pubring.kbx
-----
pub  rsa3072 2024-02-07 [SC] [expires: 2026-02-06]
     E54CCA26FB3977AA625599C04FD9103CDB4D9216
uid  [ultimate] Quentin Compson <qcompson@securelabsondemand.com>
sub  rsa3072 2024-02-07 [E] [expires: 2026-02-06]

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:~$
```

The terminal window is part of a desktop environment with a dark purple background featuring a constellation pattern. The top of the window shows the title bar with "Applications", "Terminal - instructor@Target...", and system icons for network, volume, and battery. The top right corner of the desktop shows the date and time: "Tue 06 Feb, 22:11" and the username "instructor".

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.

