Terna Engineering College

Computer Engineering Department

Class: TE **Sem.: VI**

Course: System Security Lab

PART A

(PART A : TO BE REFFERED BY STUDENTS)

Experiment No.13

A.1 Aim: Explore the GPGwin tool and implement email security

A.2 Prerequisite:

1. Basic Knowledge of email, symmetric and asymmetric encryption and decryption

A.3 Outcome:

After successful completion of this experiment students will be able to

To be able to use open source technologies and explore email security and explore various attacks.

A.4 Theory:

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a user name and/or an e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server.

GNU Privacy Guard (GnuPG or GPG) is a free software replacement for Symantec's PGP cryptographic software suite. GnuPG is a hybrid-encryption software program because it uses a combination of conventional symmetric-key cryptography for speed, and public-key cryptography foreaseofsecurekeyexchange,typicallybyusingtherecipient'spublickeytoencryptasessionkey which is only used once. This mode of operation is part of the OpenPGP standard and has been part of PGP from its firstversion.

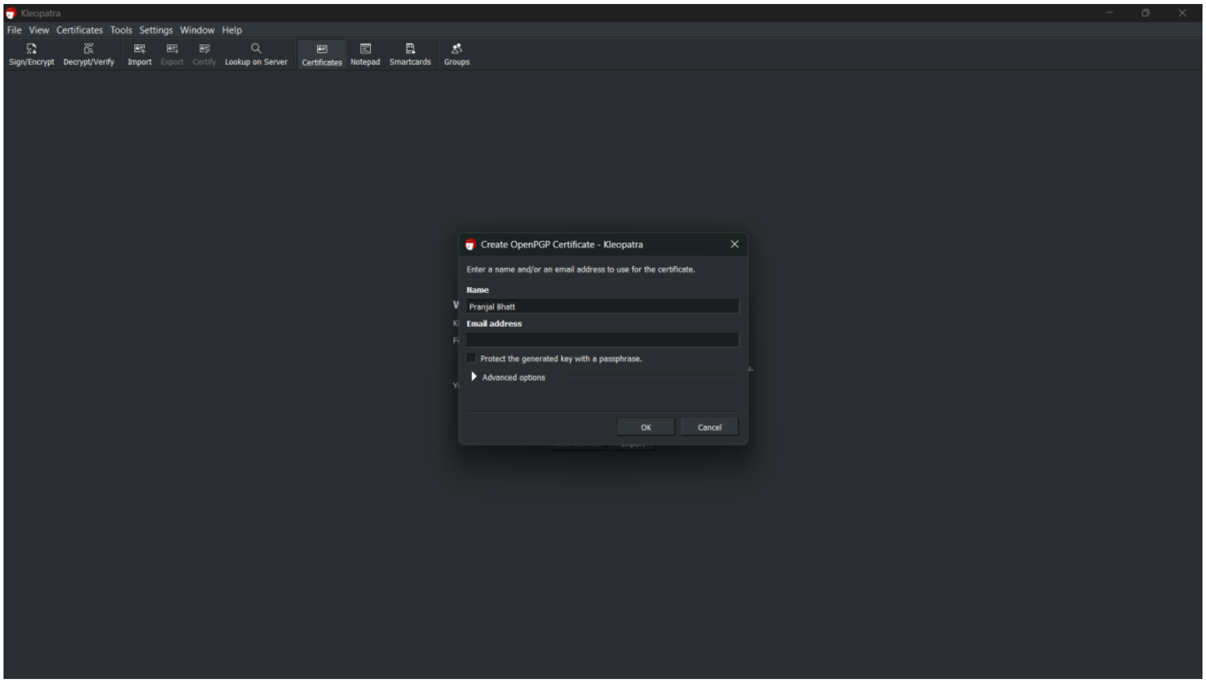
PART B

(PART B : TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)

	Roll No: B30	**Name: Bhatt Pranjal**
	Class : TE COMPS B	**Batch : B2**
	Date of Experiment:	**Date of Submission**
	Grade :	

B.1 Output



Create OpenPGP Certificate - Kleopatra

Enter a name and/or an email address to use for the certificate.

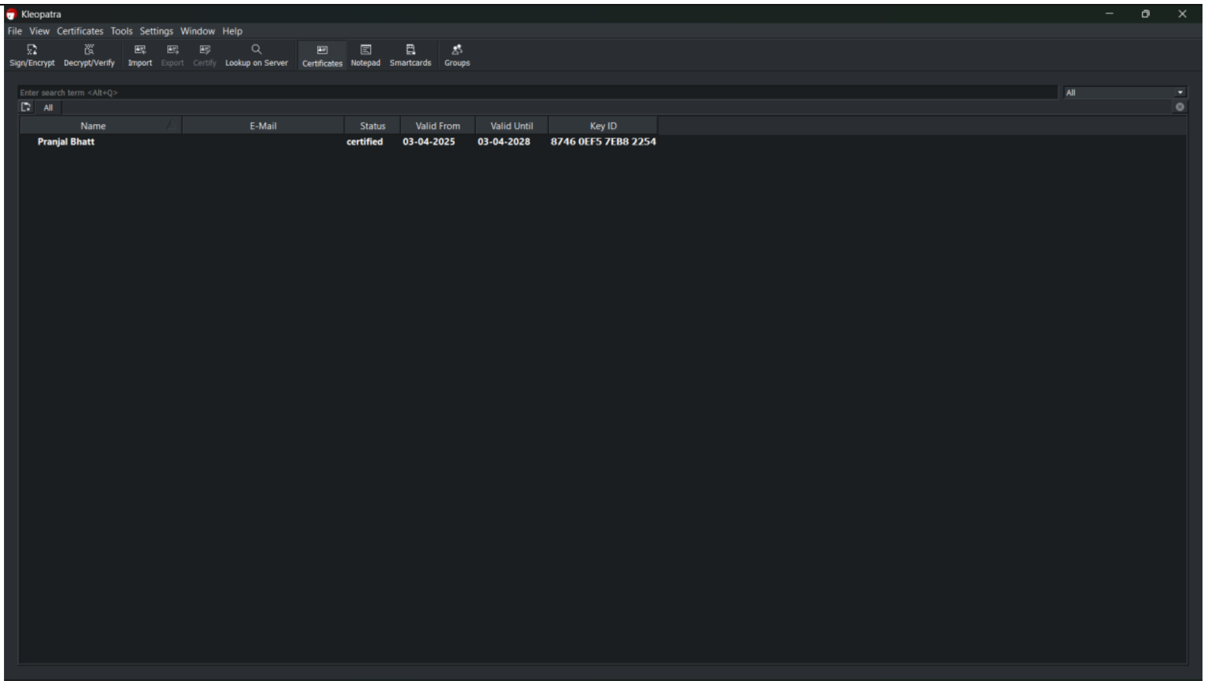
Name

Pranjal Bhatt

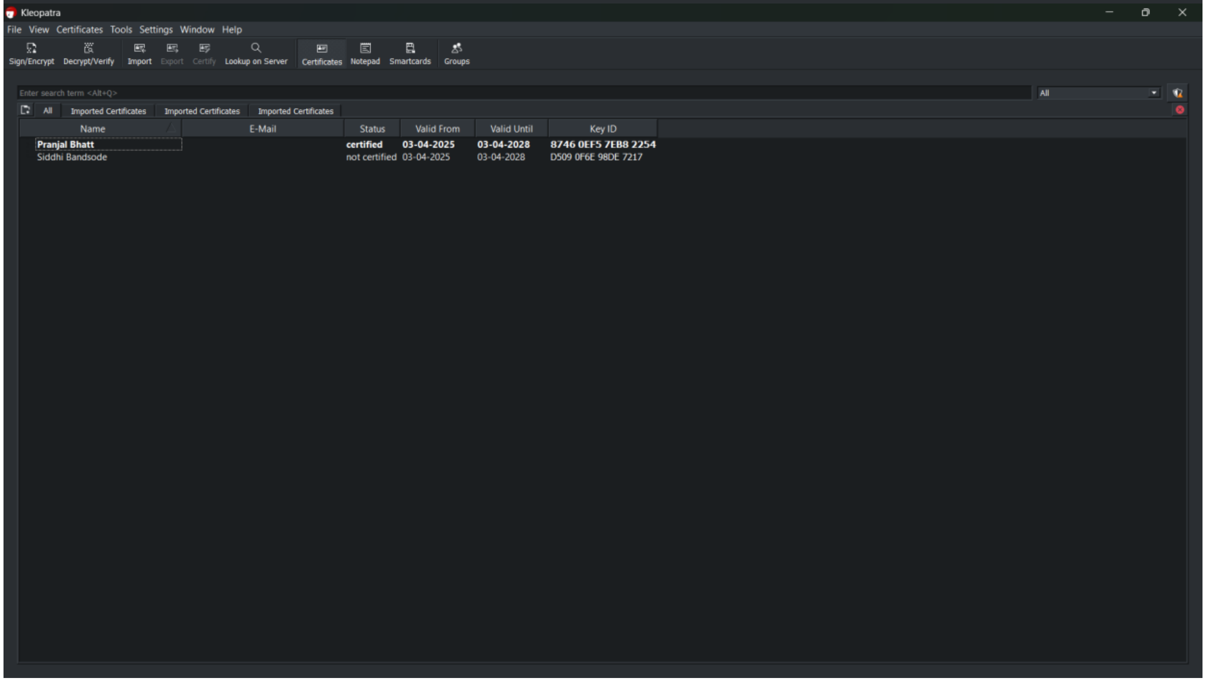
Email address

□ Protect the generated key with a passphrase.

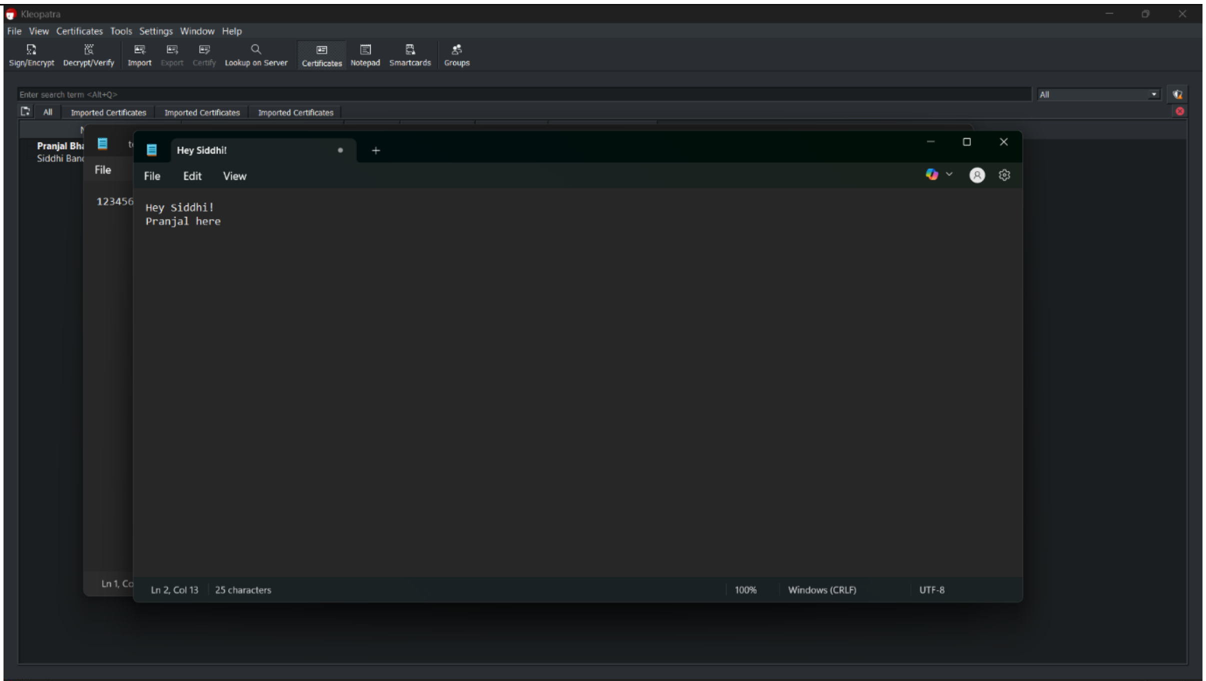
▶ Advanced options



Name	E-Mail	Status	Valid From	Valid Until	Key ID
Pranjal Bhatt		**certified**	**03-04-2025**	**03-04-2028**	**8746 0EF5 7EB8 2254**

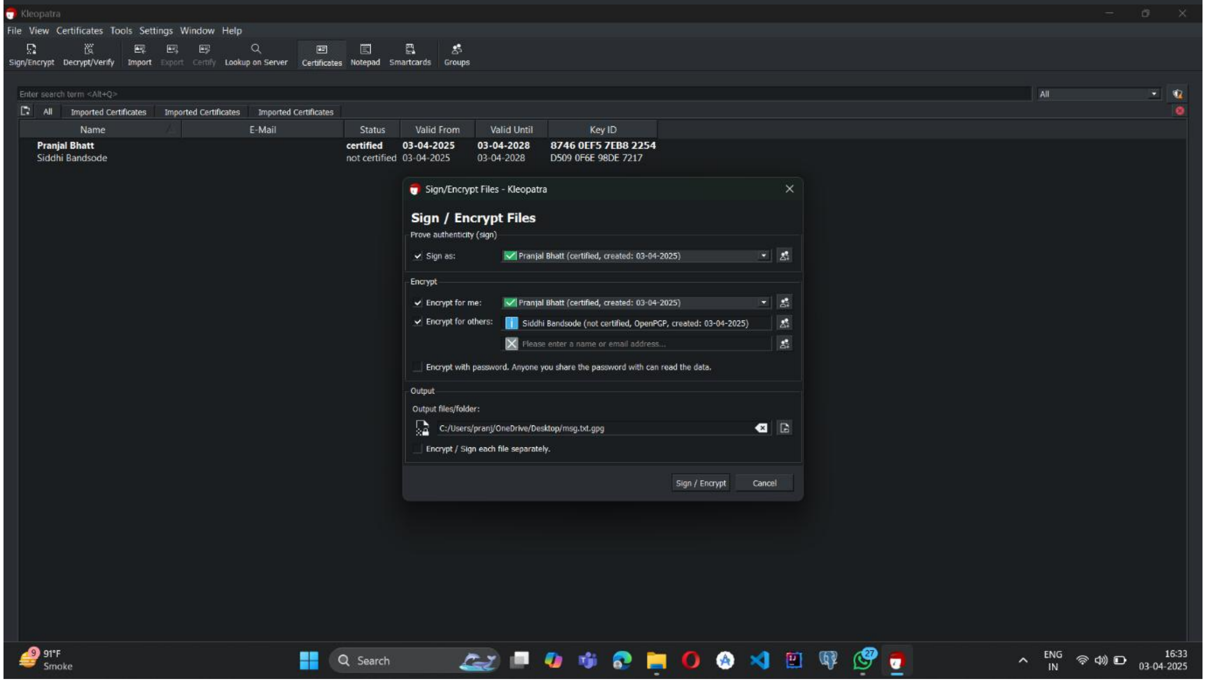


Name	E-Mail	Status	Valid From	Valid Until	Key ID
Pranjal Bhatt		**certified**	**03-04-2025**	**03-04-2028**	**8746 0EF5 7EB8 2254**
Siddhi Bandsode		not certified	03-04-2025	03-04-2028	D509 0F6E 98DE 7217


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards Groups
Enter search term <Alt+Q>
All
All Imported Certificates Imported Certificates Imported Certificates
Pranjal Bha
Siddhi Banc
File
123456
Ln 1, Co
Hey Siddhi!
File Edit View

```
Hey Siddhi!
Pranjal here
```

Ln 2, Col 13
25 characters
100%
Windows (CRLF)
UTF-8


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards Groups
Enter search term <Alt+Q>
All
All Imported Certificates Imported Certificates Imported Certificates

Name	E-Mail	Status	Valid From	Valid Until	Key ID
Pranjal Bhatt		**certified**	**03-04-2025**	**03-04-2028**	**8746 0EF5 7EB8 2254**
Siddhi Bandsode		not certified	03-04-2025	03-04-2028	D509 0F6E 98DE 7217

Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: Pranjal Bhatt (certified, created: 03-04-2025)

Encrypt

☑ Encrypt for me: Pranjal Bhatt (certified, created: 03-04-2025)

☑ Encrypt for others: Siddhi Bandsode (not certified, OpenPGP, created: 03-04-2025)

Please enter a name or email address...

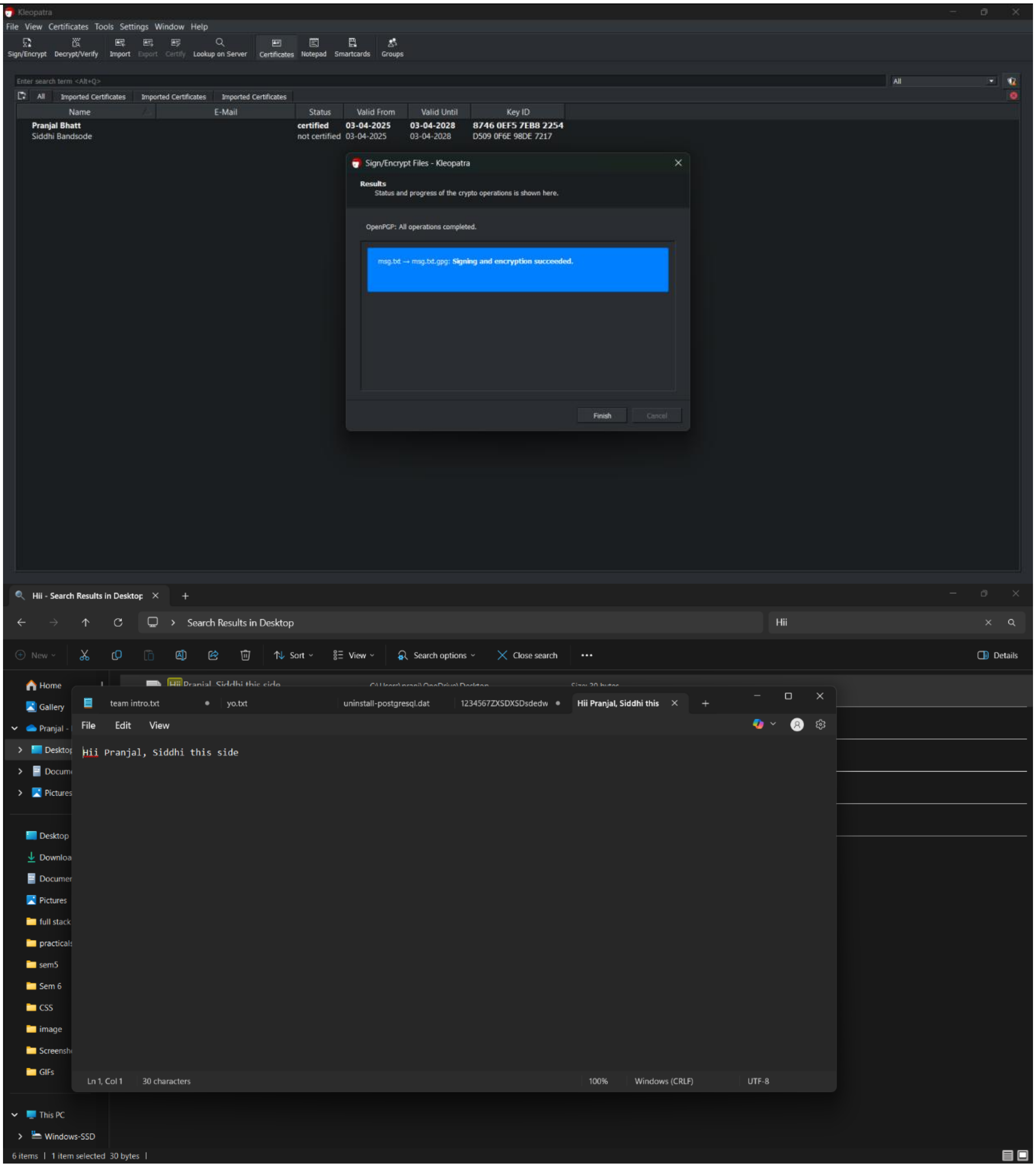
□ Encrypt with password. Anyone you share the password with can read the data.

Output

Output files/folder:

C:/Users/pranj/OneDrive/Desktop/msg.txt.gpg

□ Encrypt / Sign each file separately.



Name	E-Mail	Status	Valid From	Valid Until	Key ID
Pranjal Bhatt		**certified**	**03-04-2025**	**03-04-2028**	**8746 0EF5 7EB8 2254**
Siddhi Bandsode		not certified	03-04-2025	03-04-2028	D509 0F6E 98DE 7217

Sign/Encrypt Files - Kleopatra

Results

Status and progress of the crypto operations is shown here.

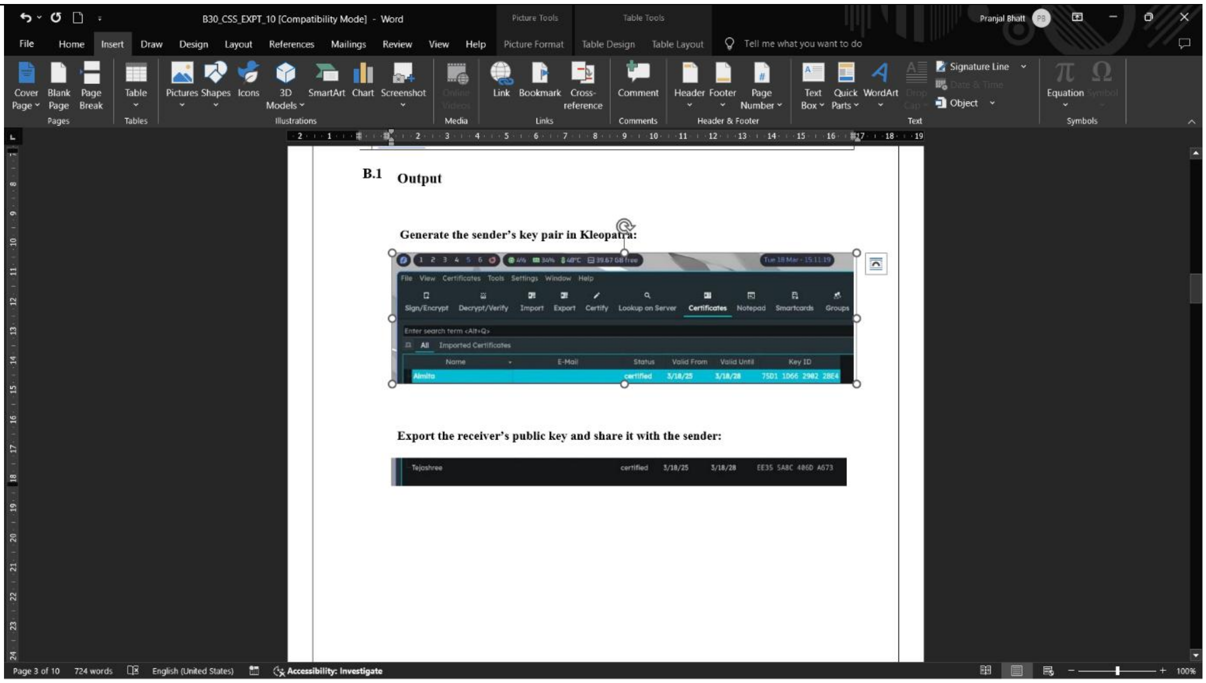
OpenPGP: All operations completed.

msg.txt → msg.txt.gpg: **Signing and encryption succeeded.**

```
Hii Pranjal, Siddhi this side
```

Ln 1, Col 1 | 30 characters | 100% | Windows (CRLF) | UTF-8

6 items | 1 item selected 30 bytes |



B.1 Output

Generate the sender's key pair in Kleopatra:

Name	E-Mail	Status	Valid From	Valid Until	Key ID
Almita		certified	3/18/25	3/18/28	75D1 1D66 2902 28E4

Export the receiver's public key and share it with the sender:

Tejashree		certified	3/18/25	3/18/28	EE35 5A8C 406D A673

B.2. Commands / tools used with syntax:

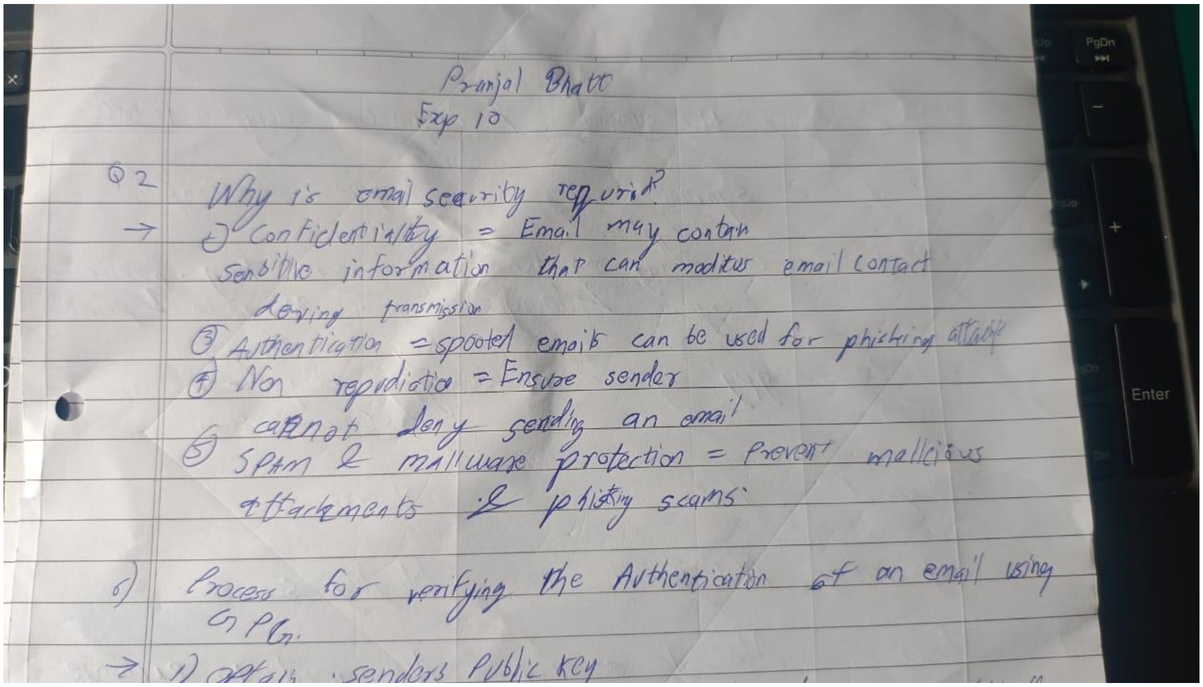
Tool: Kleopatra

B.3 Question of Curiosity: *(Attempt at least 3 questions handwritten)*

1. What is the full form of PGP?

PGP (Pretty Good Privacy) is an encryption program used for securing emails, files, and other forms of data communication through cryptographic techniques.

2. Why email security is required ?



Pranjal Bhatt
Exp 10

Q2 Why is email security requird?

→ 1) Confidentiality = Email may contain sensitive information that can moditus email contact doring transmission

③ Authentication = spooted emails can be used for phishing attack

④ Non repudiation = Ensure sender cannot deny sending an email

⑤ SPAM & mallware protection = Prevent mallicious attachments & phishing scams.

6) Process for verifying the Authentication of an email using GPG.

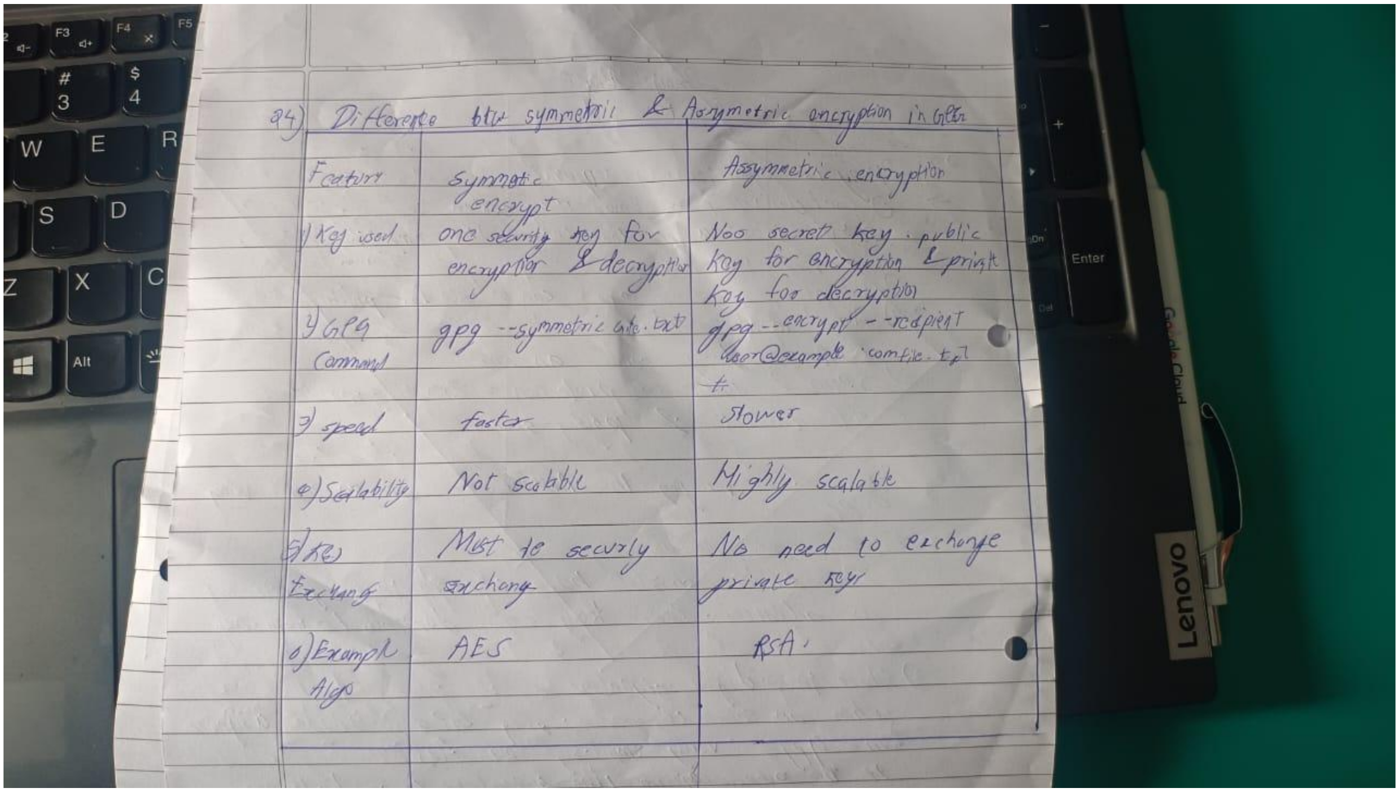
→ 1) obtain senders Public key

3. What is GPG (GNU Privacy Guard) and how does it ensure email security?

GPG (GNU Privacy Guard) is an open-source implementation of PGP encryption, following the OpenPGP standard. It ensures email security by:

- Using asymmetric encryption (public/private key pairs) to encrypt emails.
- Allowing digital signatures to verify the sender's authenticity.
- Providing end-to-end encryption, ensuring that only the recipient can decrypt the message.
- Preventing man-in-the-middle attacks by verifying email integrity.

4. What is the difference between symmetric and asymmetric encryption in the context of GPG?



Q4) Differenco btw symmetric & Asymmetric encryption in GPG

Feature	Symmetric encrypt	Assymmetric encryption
1) Key used	one security key for encryption & decryption	Noo secret key. public key for encryption & privat key for decryption
2) GPG Command	gpg --symmetric file.txt	gpg --encrypt --recipient user@example.com file.txt
3) speed	faster	Slower
4) Scalability	Not scalable	Highly scalable
5) Key Exchang	Must be securly exchang	No need to exchange private keys
6) Example Algo	AES	RSA.

5. What is the role of a public key and private key in email encryption with GPG?

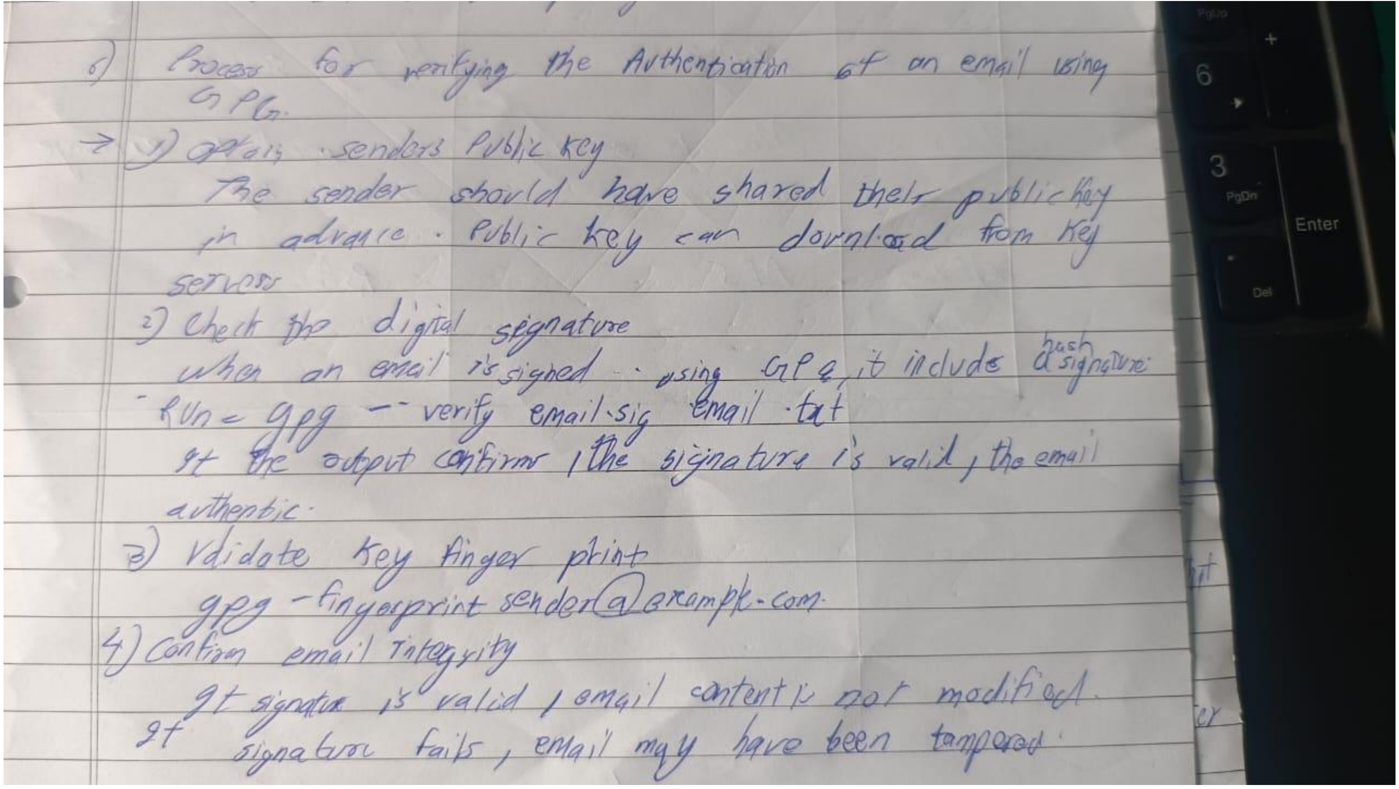
Public Key: Shared openly and used by others to encrypt messages for the recipient.

Private Key: Kept secret by the recipient and used to decrypt messages encrypted with their public key.

This ensures that only the intended recipient can access the message, preventing unauthorized interception.

Digital signatures are also created using the sender’s private key and verified using their public key, ensuring message authenticity.

6. What is the process for verifying the authenticity of an email using GPG?



6) Process for verifying the Authentication of an email using GPG.

→ 1) obtain senders Public key
The sender should have shared their publickey in advance. Public key can download from Key servers

2) Check the digital signature
when an email is signed. using GPG, it include a hash signature.
- Run = gpg --verify email.sig email.txt
If the output confirms, the signature is valid, the email authentic.

3) Vdidate key finger print
gpg -fingerprint sender@example.com.

4) Confirm email Integrity
If signature is valid, email content is not modified.
If signature fails, email may have been tampered.

B.4 Conclusion:

Using Kleopatra, key pairs were generated, the receiver’s public key was imported, and message were encrypted and signed to ensure confidentiality and authenticity. The encrypted message was sent securely, and the recipient decrypted it using their private ate key, verifying its integrity and sender authenticity. This implementation demonstrates how GPG encryption effectively protects email communication from interception, tampering, and impersonation.