

Terna Engineering College

Computer Engineering Department

Class: TE

Sem.: VI

Course: System Security Lab

PART A

(PART A: TO BE REFERRED BY STUDENTS)

Experiment No.10

A.1 Aim:

Explore the GPGwin tool and implement email security.

A.2 Prerequisite:

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

A.3 Outcome:

After the successful completion of this experiment, students will 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 for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is only used once. This mode of operation is part of the OpenPGP standard and has been part of PGP from its first version.

PART B

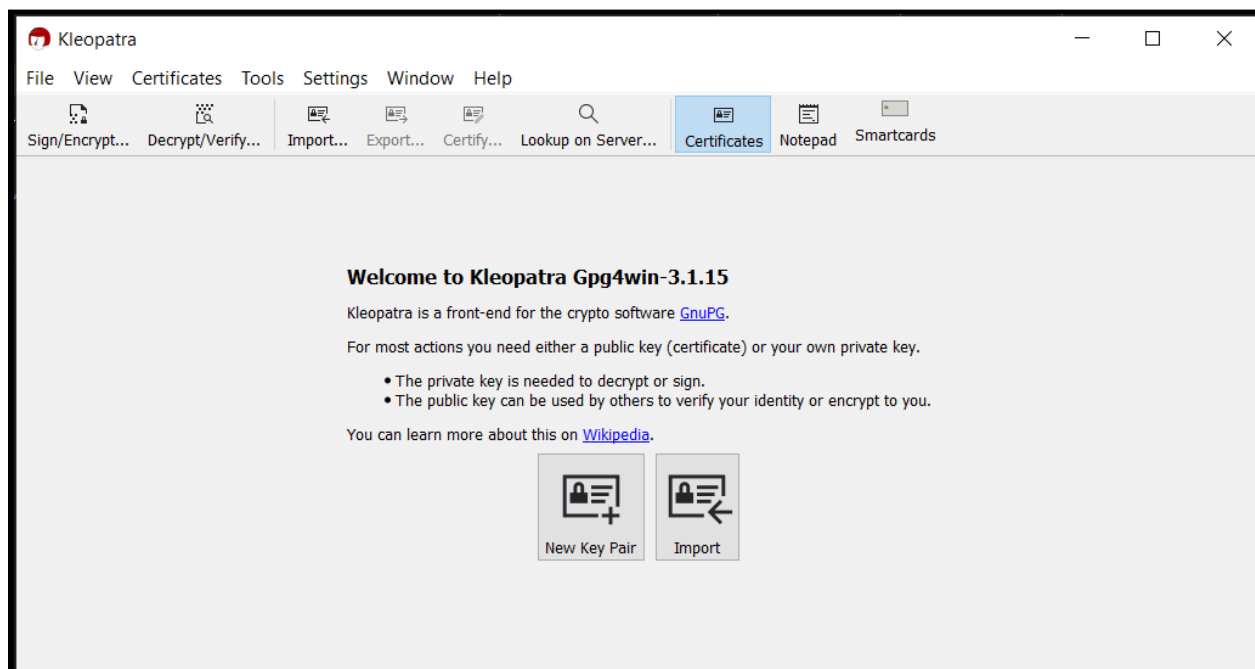
(PART B: TO BE COMPLETED BY STUDENTS)

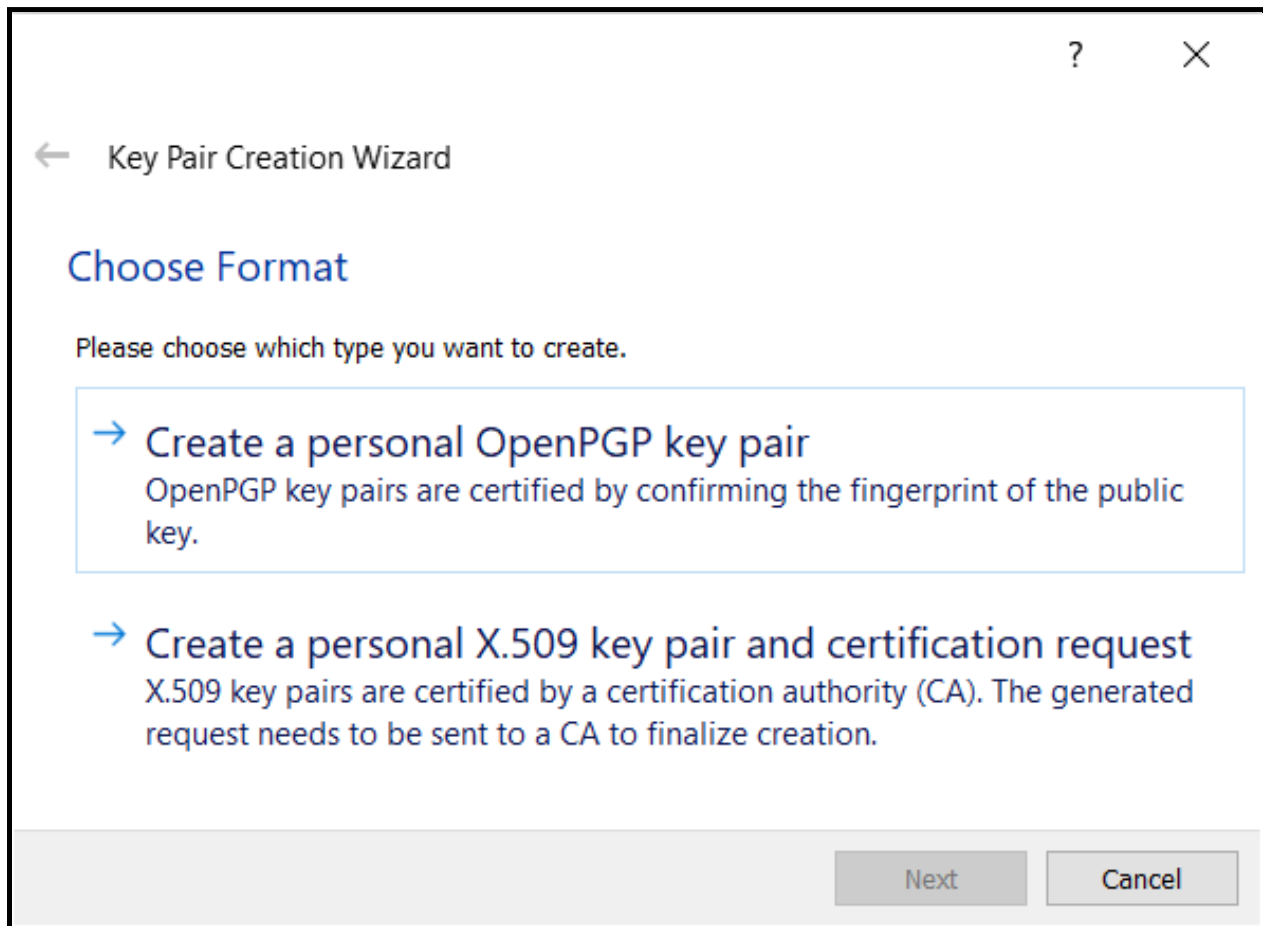
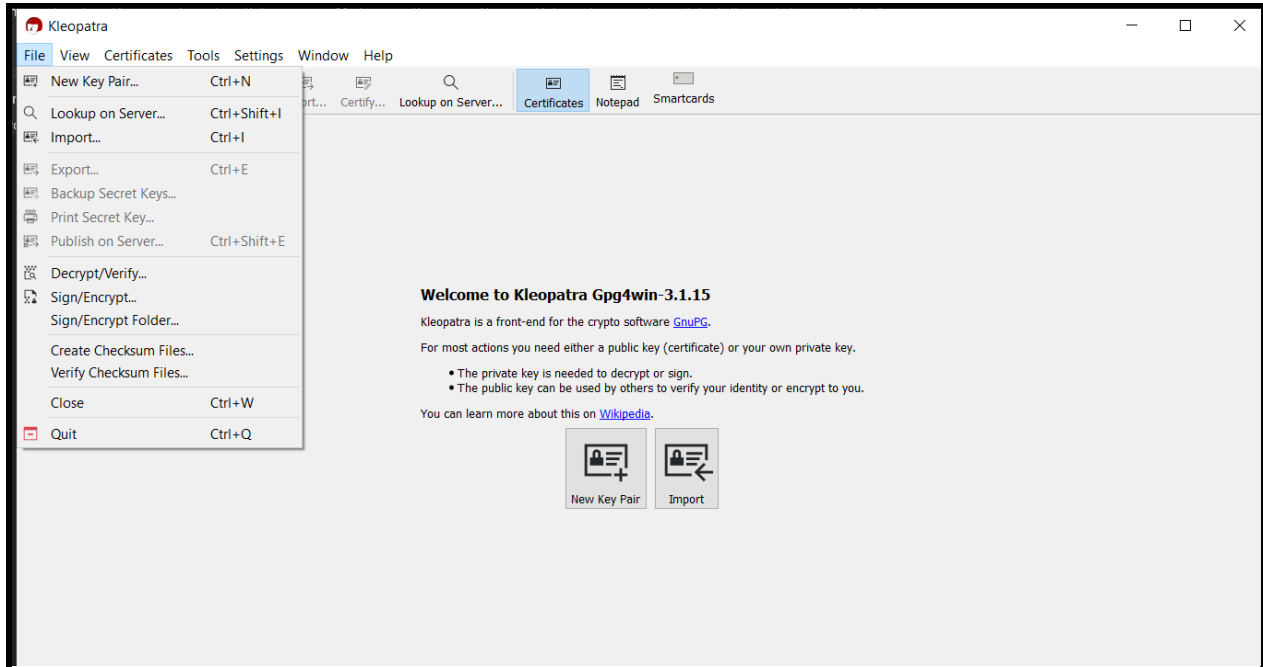
(Students must submit the soft copy as per the following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Blackboard access available)

Roll No. 50	Name: AMEY THAKUR
Class: Comps TE B	Batch: B3
Date of Experiment: 20/04/2021	Date of Submission: 20/04/2021
Grade:	

B.1 Output

(add a snapshot of output)





?

×

← Key Pair Creation Wizard

Enter Details

Please enter your personal details below. If you want more control over the parameters, click on the Advanced Settings button.

Name:

AMEY THAKUR

(optional)

Email:

ameythakur@ternaengg.ac.in

(optional)


☒ Protect the generated key with a passphrase.

AMEY THAKUR <ameythakur@ternaengg.ac.in>

Advanced Settings...


Create

Cancel

 pinentry-qt

—


×



Please enter the passphrase to protect your new key

Passphrase:

●●●●●●●●

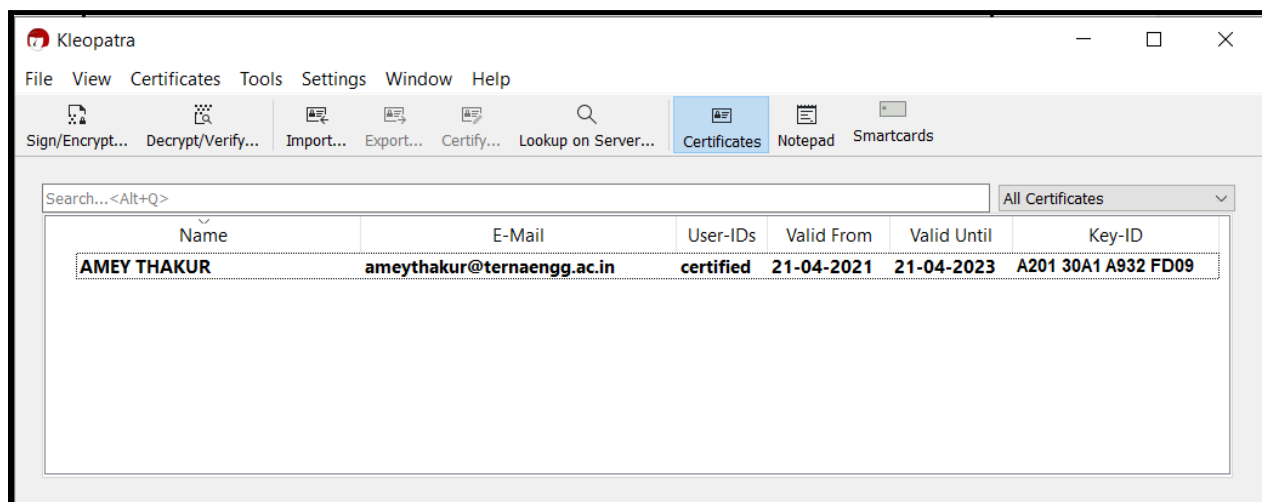
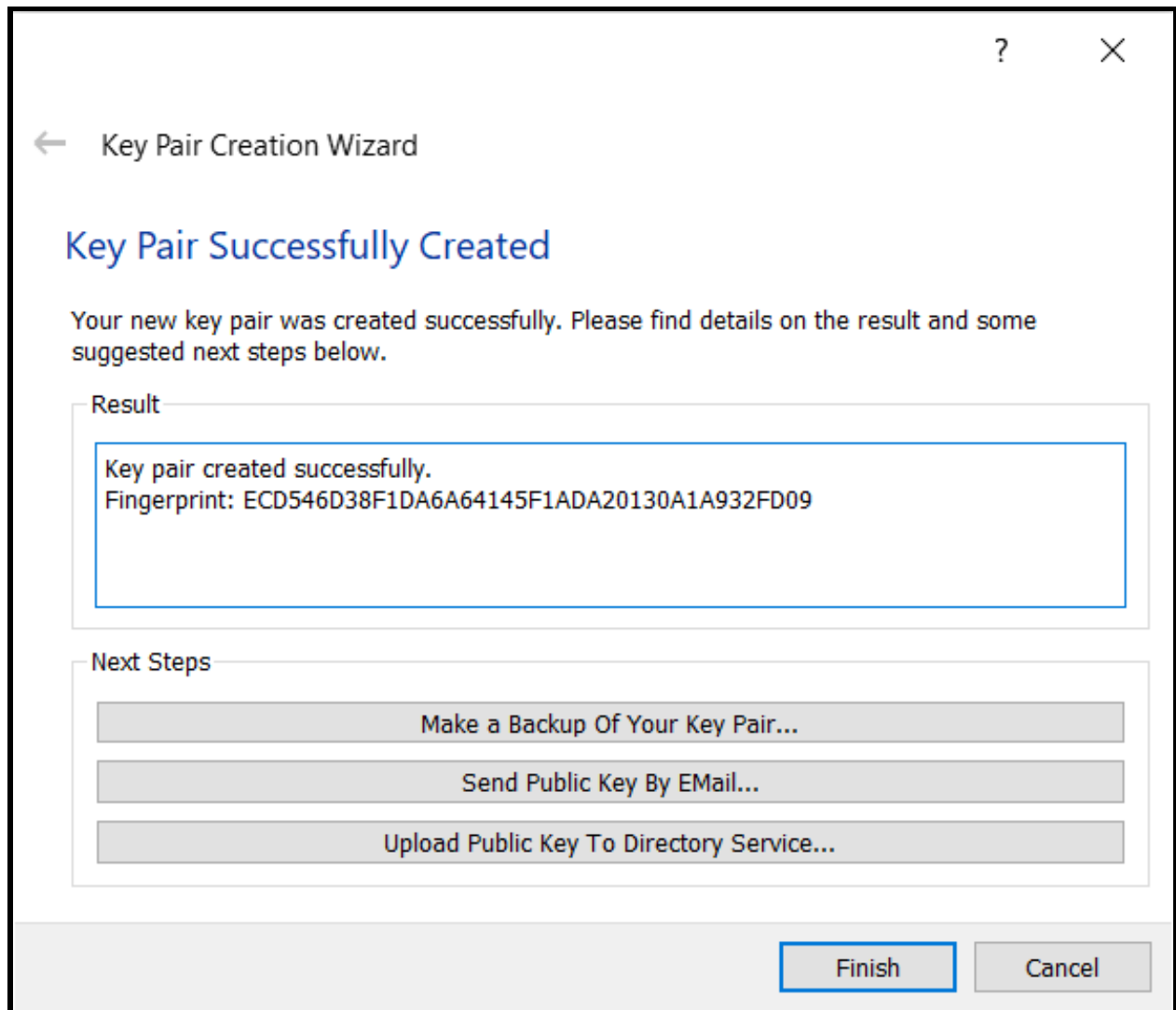


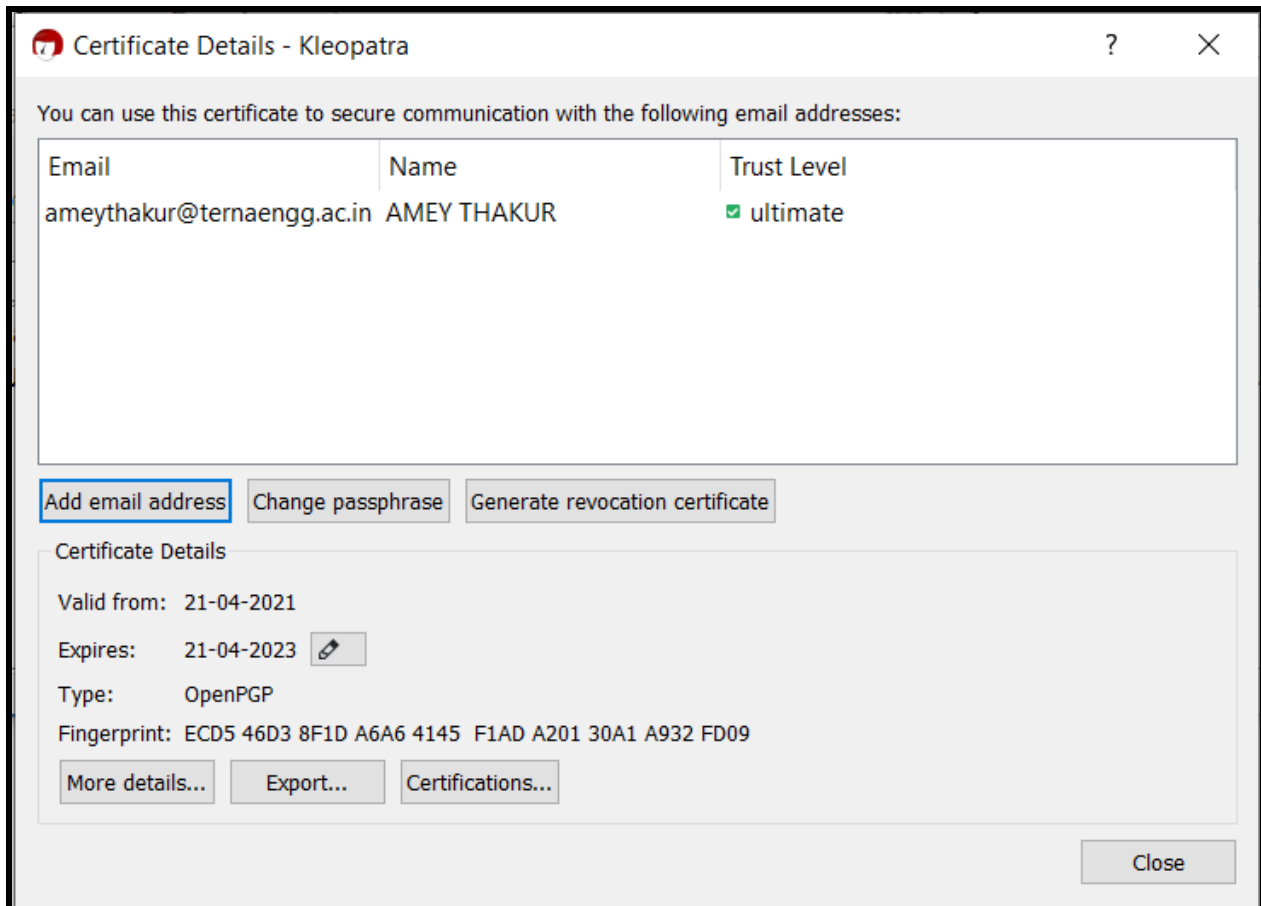
Repeat:

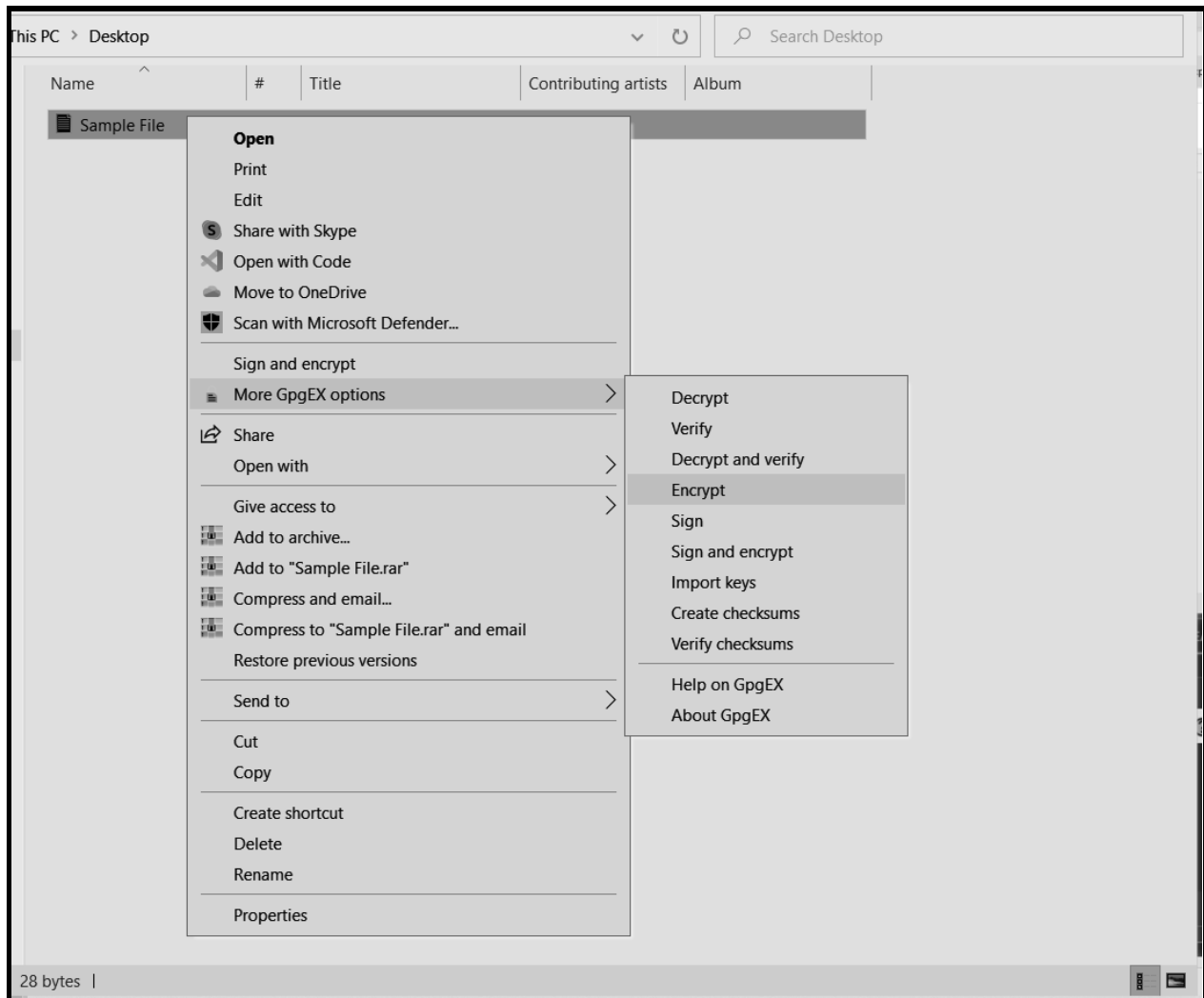
●●●●●●●●

OK

Cancel







Sign/Encrypt Files - Kleopatra

?

×

Sign / Encrypt Files

Prove authenticity (sign)

☐ Sign as:

✓

AMEY THAKUR <ameythakur@ternaengg.ac.in> (certified, created: 21-04-2021) ▾

Encrypt

☒ Encrypt for me:

✓

AMEY THAKUR <ameythakur@ternaengg.ac.in> (certified, created: 21-04-2021) ▾

☒ Encrypt for others:

👤

Please enter a name or email address...

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

Output

☐ Encrypt / Sign each file separately.

🔒


C:/Users/ameyt/Desktop/Sample File.txt.gpg

⌫

📁

Encrypt

Cancel

 Sign/Encrypt Files - Kleopatra ? ×

Sign / Encrypt Files


Prove authenticity (sign)


☒ Sign as: ✓ AMEY THAKUR <ameythakur@ternaengg.ac.in> (certified, created: 21-04-2021) ▾


Encrypt

☒ Encrypt for me: ✓ AMEY THAKUR <ameythakur@ternaengg.ac.in> (certified, created: 21-04-2021) ▾

☒ Encrypt for others:

 Please enter a name or email address...



 Please enter a name or email address...

 Please enter a name or email address...


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

Output


☒ Encrypt / Sign each file separately.


 

Sign / Encrypt Cancel

 pinentry-qt — □ ×

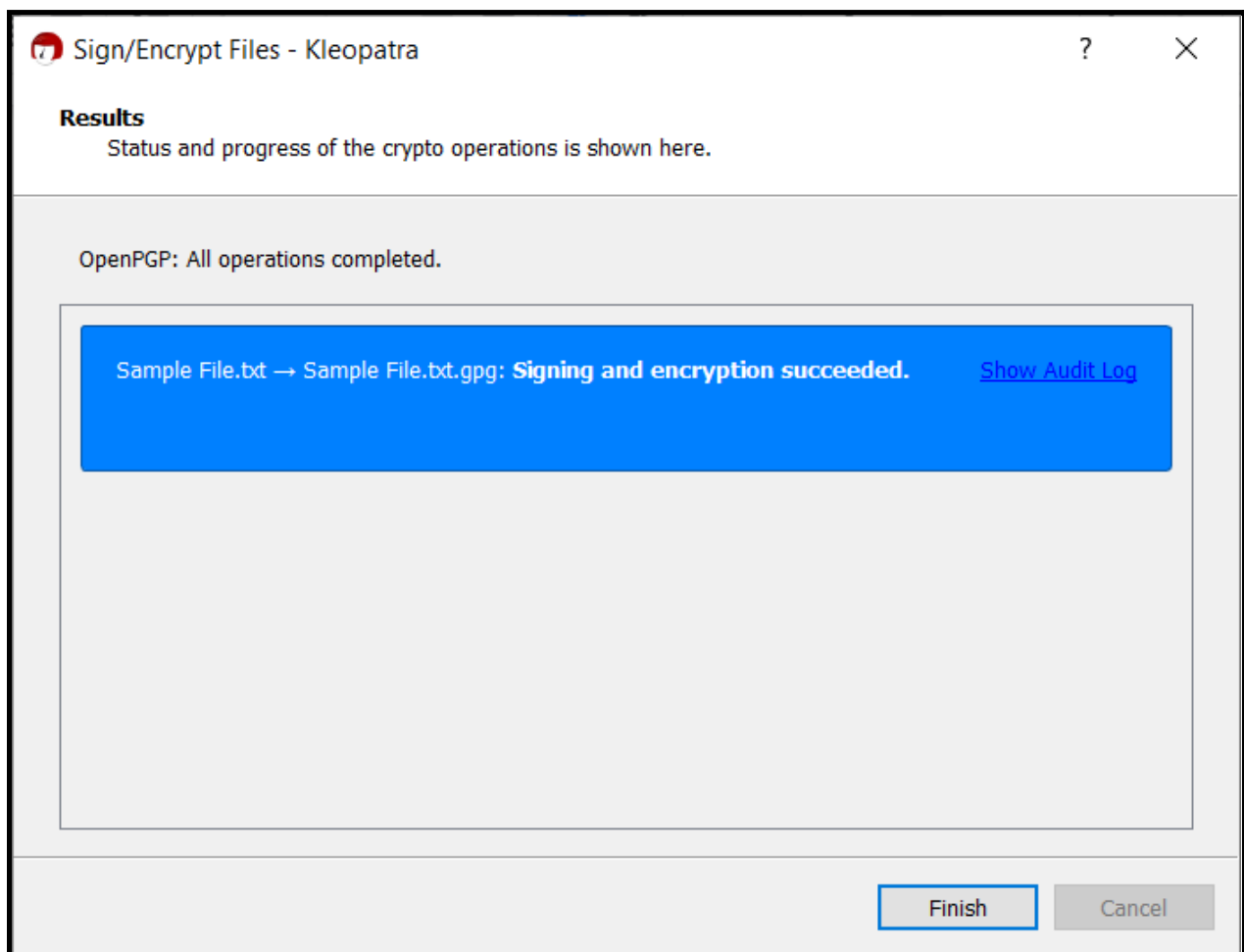
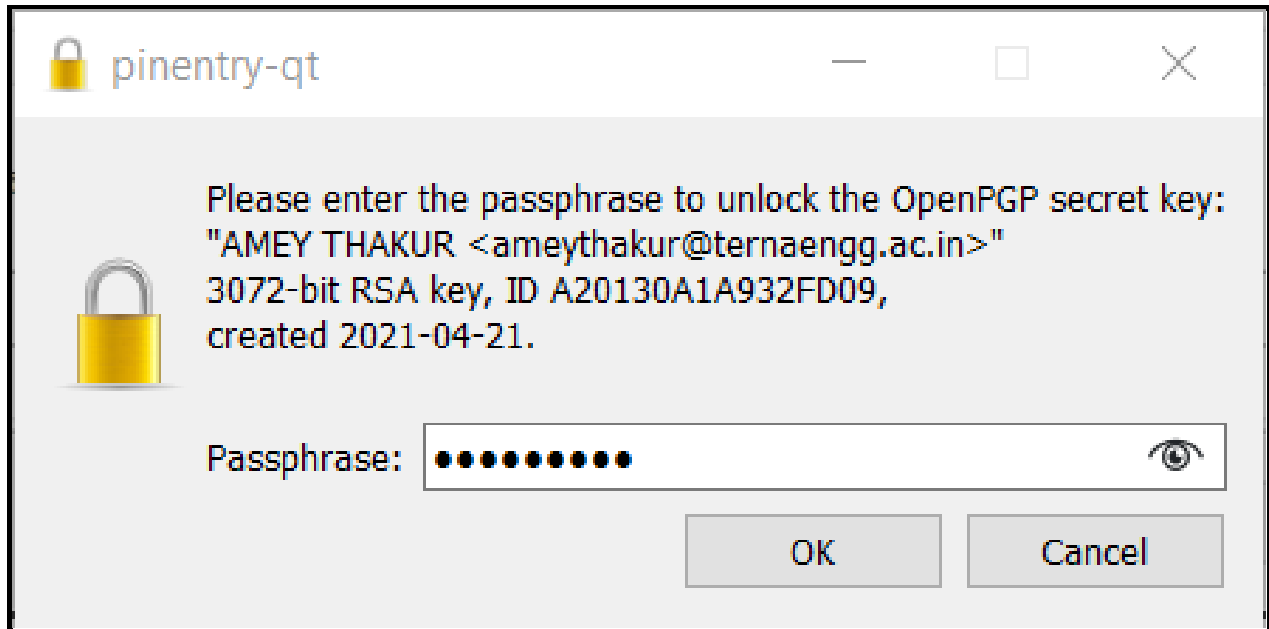
Enter passphrase

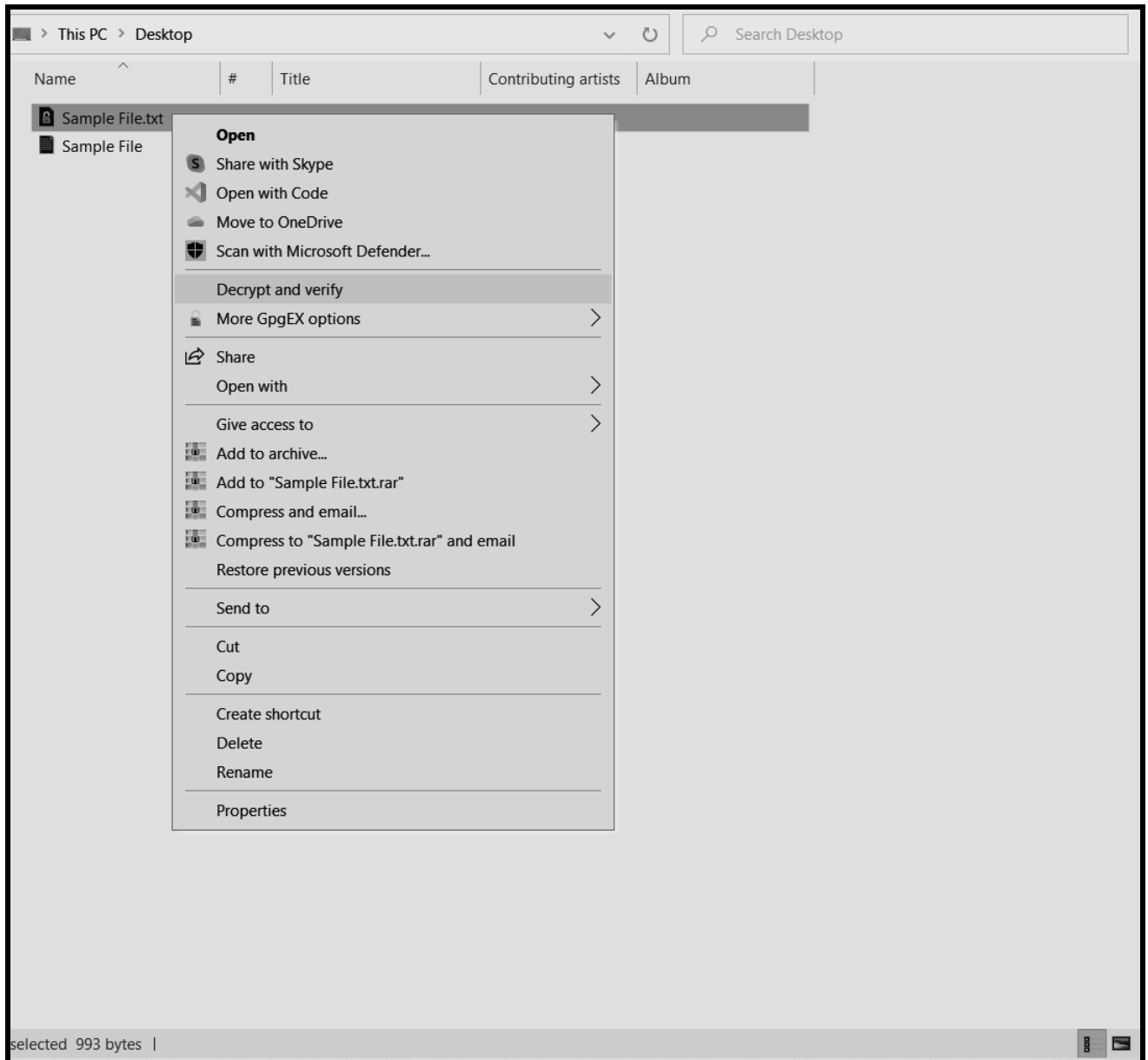
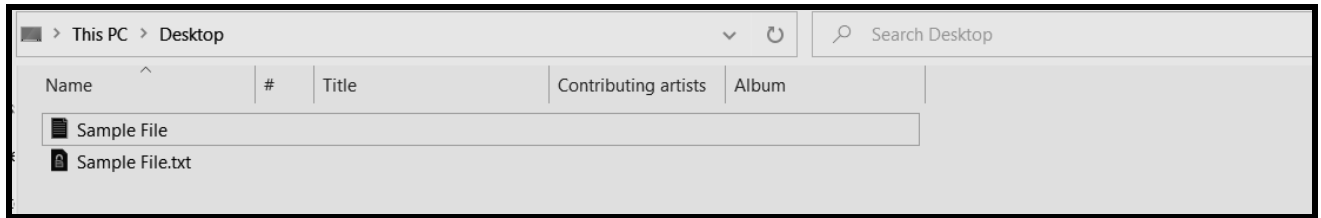


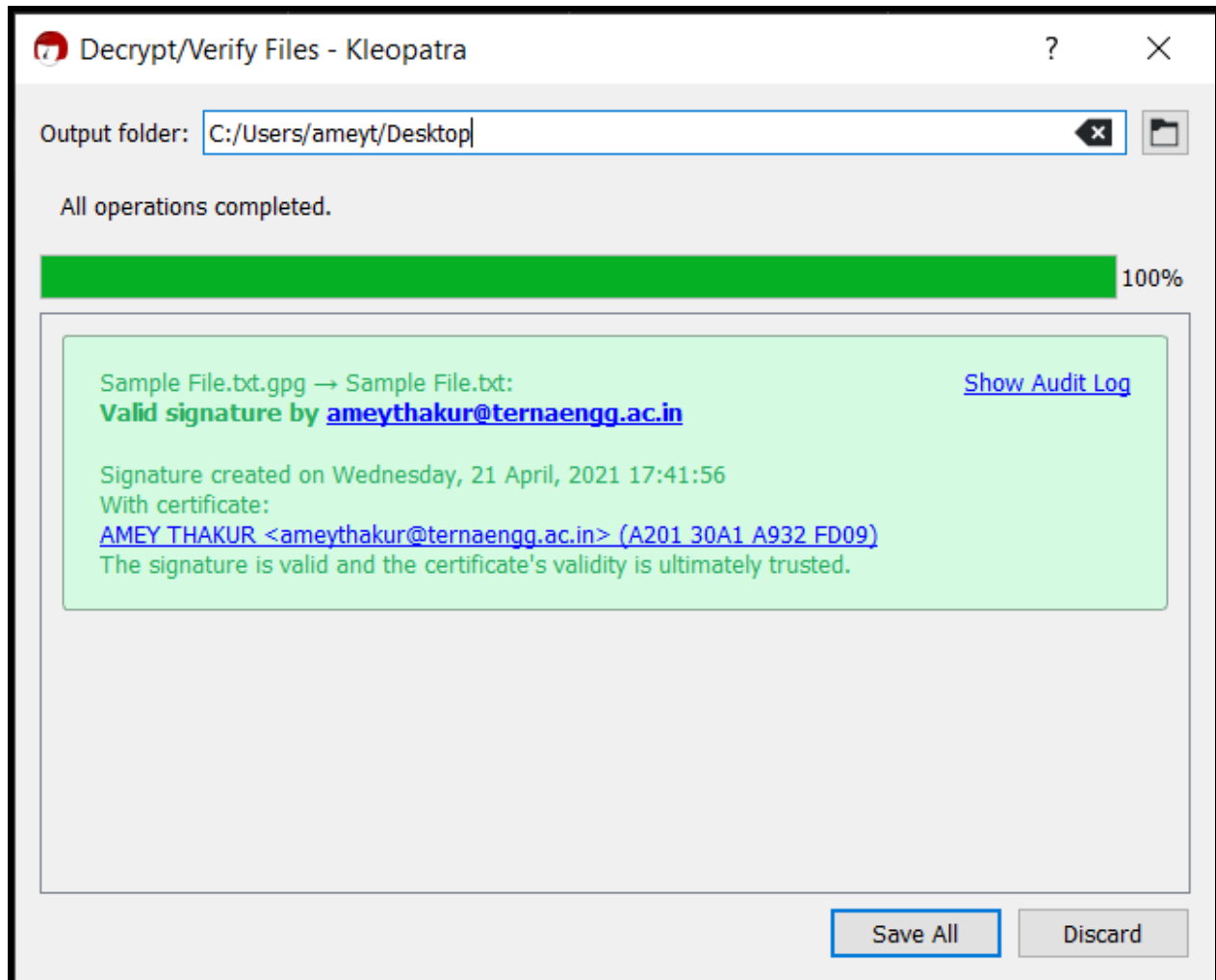
Passphrase: 

Repeat:

OK Cancel







B.2 Commands/tools used with the syntax:

KLEOPATRA and GPGwin tool is used in the experiment.

B.3 Question of Curiosity:

1. What is the full form of PGP?

Ans:

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

2. Why email security is required?

Ans:

1. Avoid Business Risks

These days there is so much at stake, so no one wants to send unencrypted emails. Without encryption, any stranger can have access to the information which is contained in your mail. Your competitors can use such information against you. Therefore to avoid business as well as other kinds of risks you should go in for email encryption.

2. Protect Confidential Information

Email encryption protects confidential information such as your credit card number, banking account number, social security number etc. In case your mail is not encrypted some wrong elements can make use of your personal information for their ulterior motives. Can you imagine that the messages which you sent can be read or even altered in transit? Even the username as well as password which you type can be stolen without much difficulty. So to avoid leakage of such vital information email encryption is important.

3. Nullify Message Replay Possibilities

You already know that the message you sent can be modified, but then there is one more thing that is possible with the messages you send. Messages can be saved, altered, and then re-sent later on. One can get an authentic message first, and then receive fake messages which appear to be official later on. The recipient cannot tell whether the email message which has been sent to him is altered. In case the message was just deleted they will not even know that it had ever been sent.

4. Avoid Identity Theft

If any person gets hold of your username as well as password which you use to get to your email servers, he or she can read the emails which you send and also send false email messages on your behalf. This is referred to as identity theft and can be avoided if you go in for email encryption.

B.4 Conclusion:

(Write an appropriate conclusion.)

After the successful completion of this experiment, we can use open source technologies and explore email security and explore various attacks.