Date : 28/10/23

E10 A CREATING PUBLIC & PRIVATE KEYS (KLEOPETRA)

Page No. : 29
Expt. No. : 10a

AIM

To create public and private keys using Kleopetra

Procedure

1) Install Kleopetra and start the Kleopetra management software

2) GUI will be displayed.

3) From file drop down, click on new certificate option.

4) Click on "create a personal OpenGPG key pair and next button.

5) Certificate wizard will start & display.

6) Enter name & email id
Enter optional comment if required.

7) Review extended values if ok, create the key.

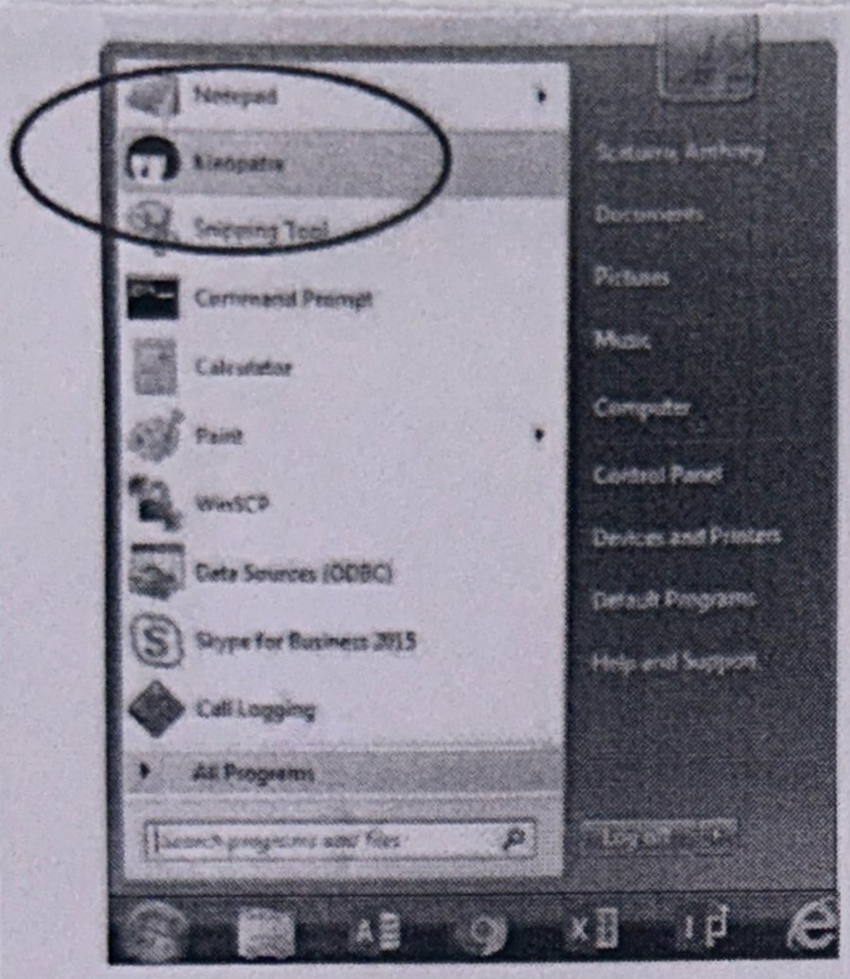
8) Passphrase will be asked, create ie enter it.

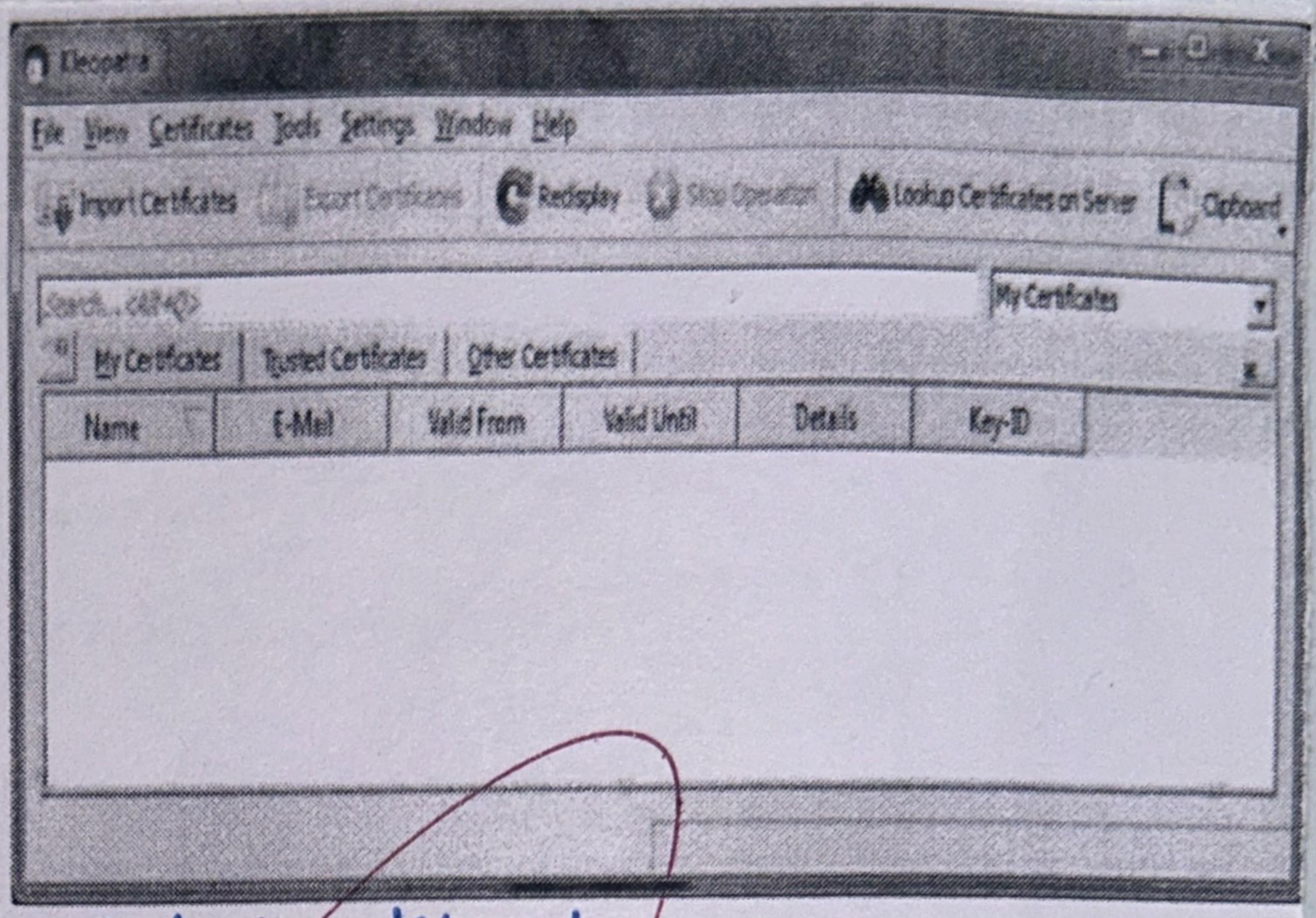
9) Passphrase should follow strong password standards

10) Reenter passphrase and click ok

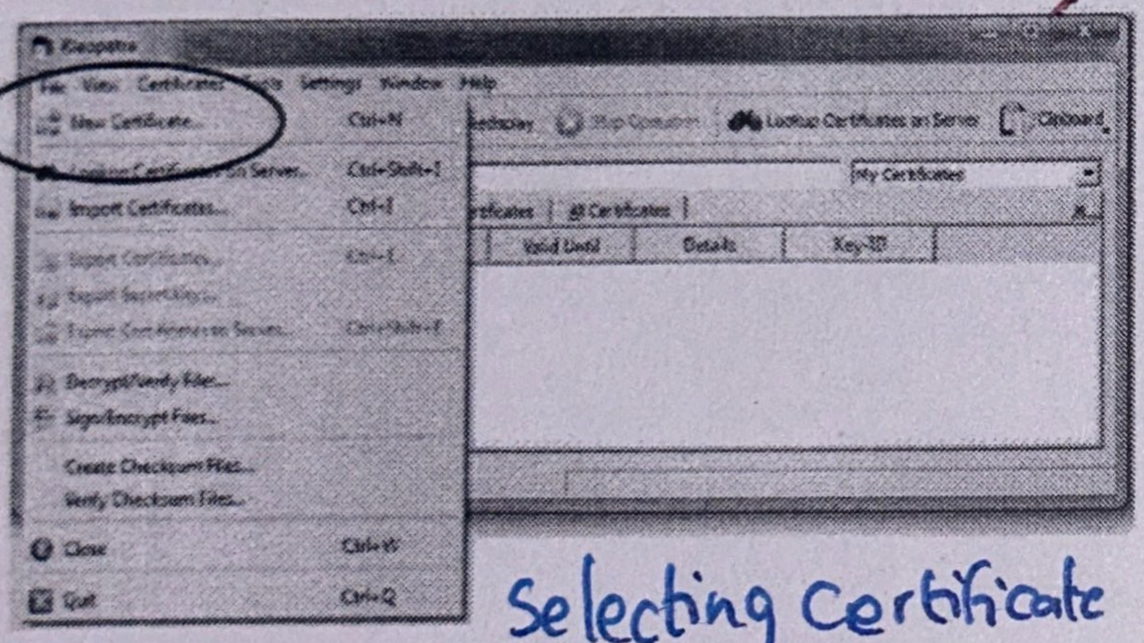
11) Once certificate is created, backup of Keys will be displayed

Teacher's Signature:

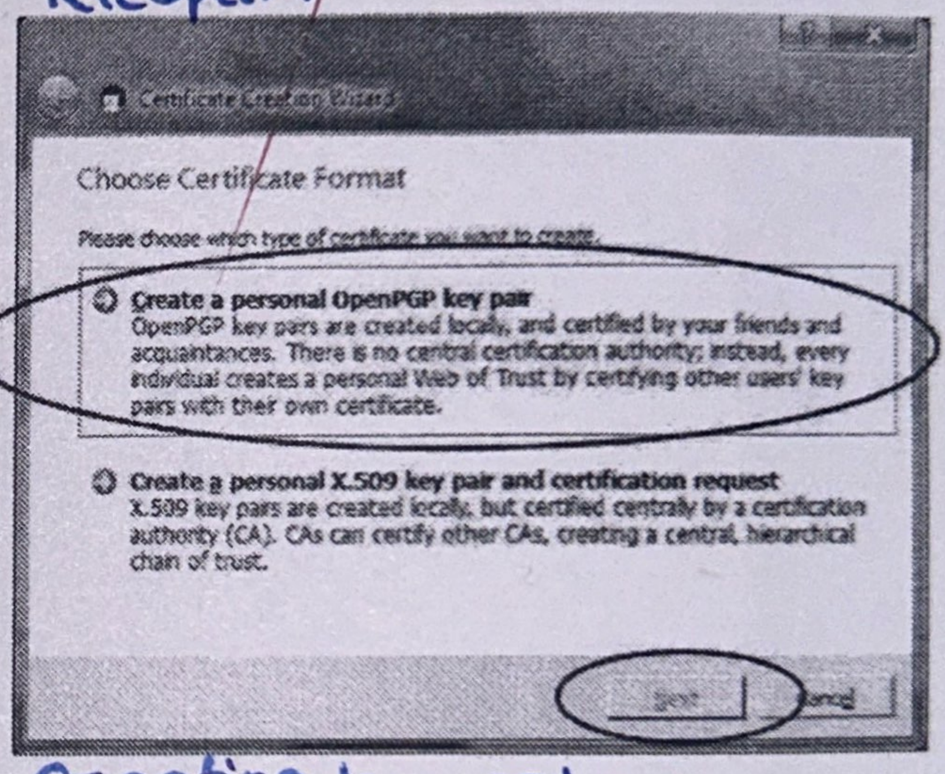




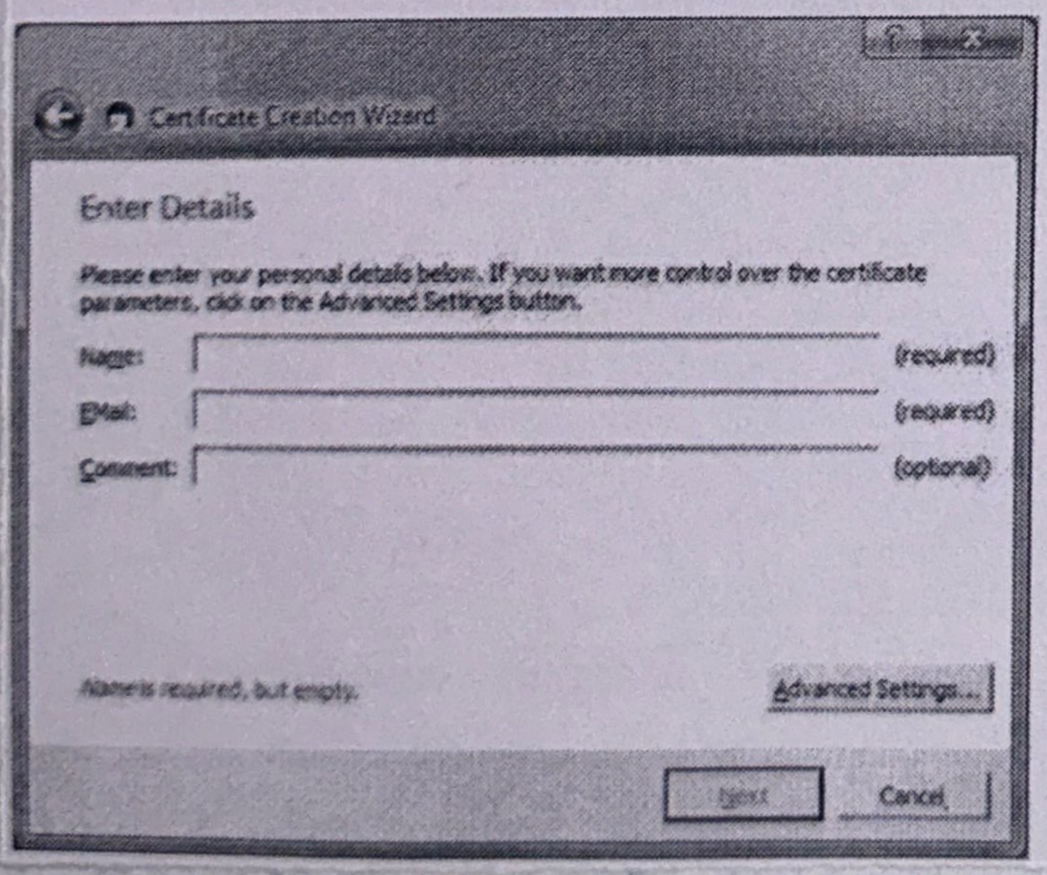
1) entering Kleopetra

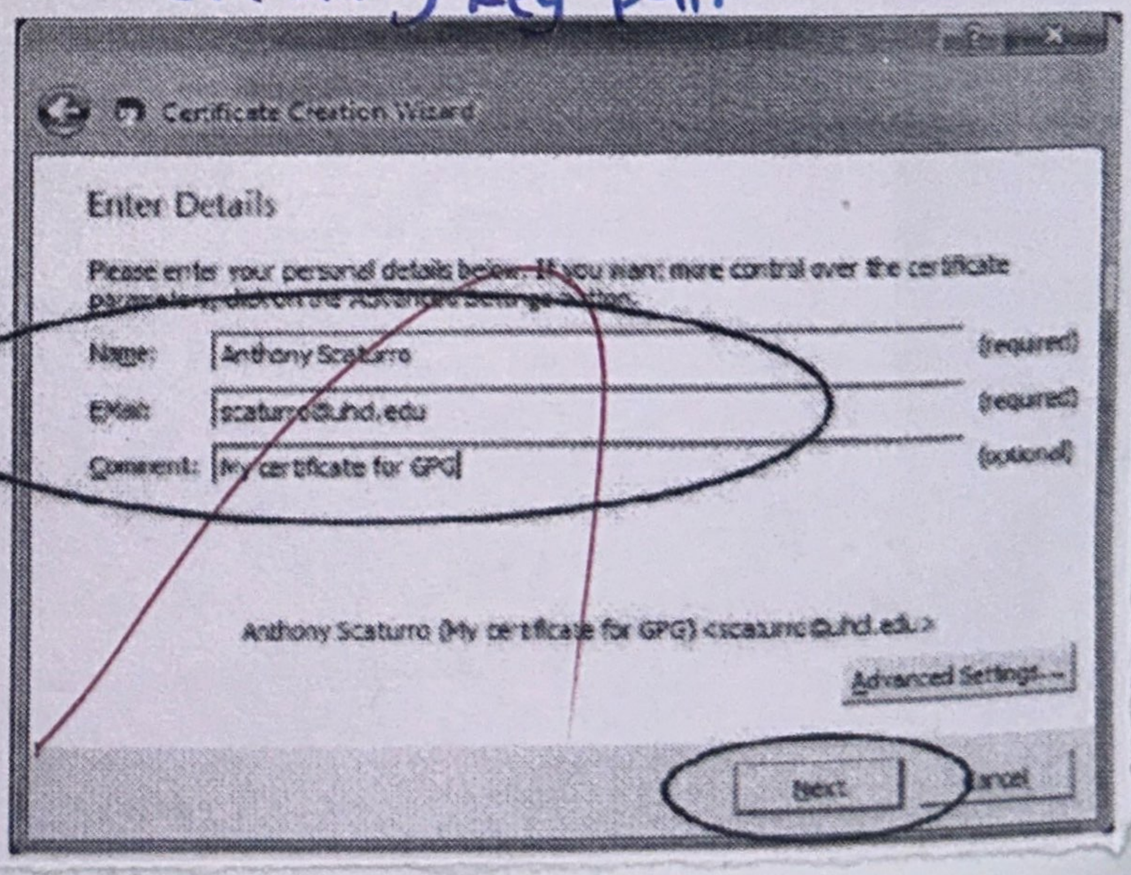


Selecting Certificate

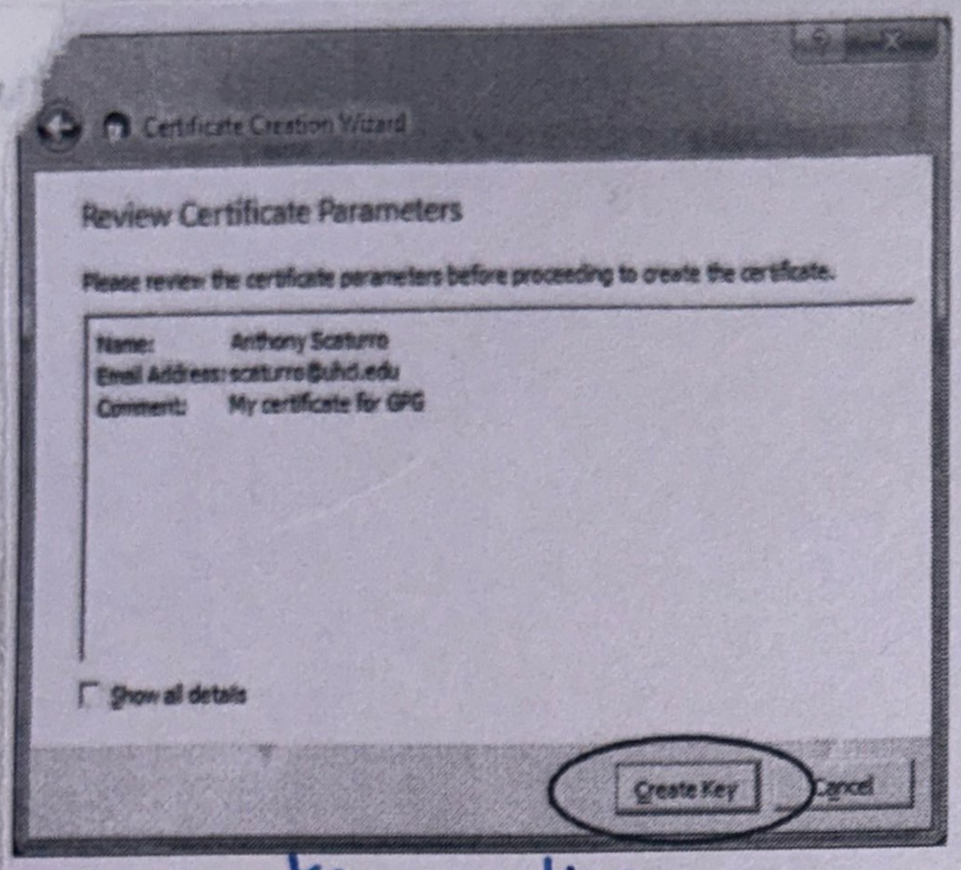


Creating key pair

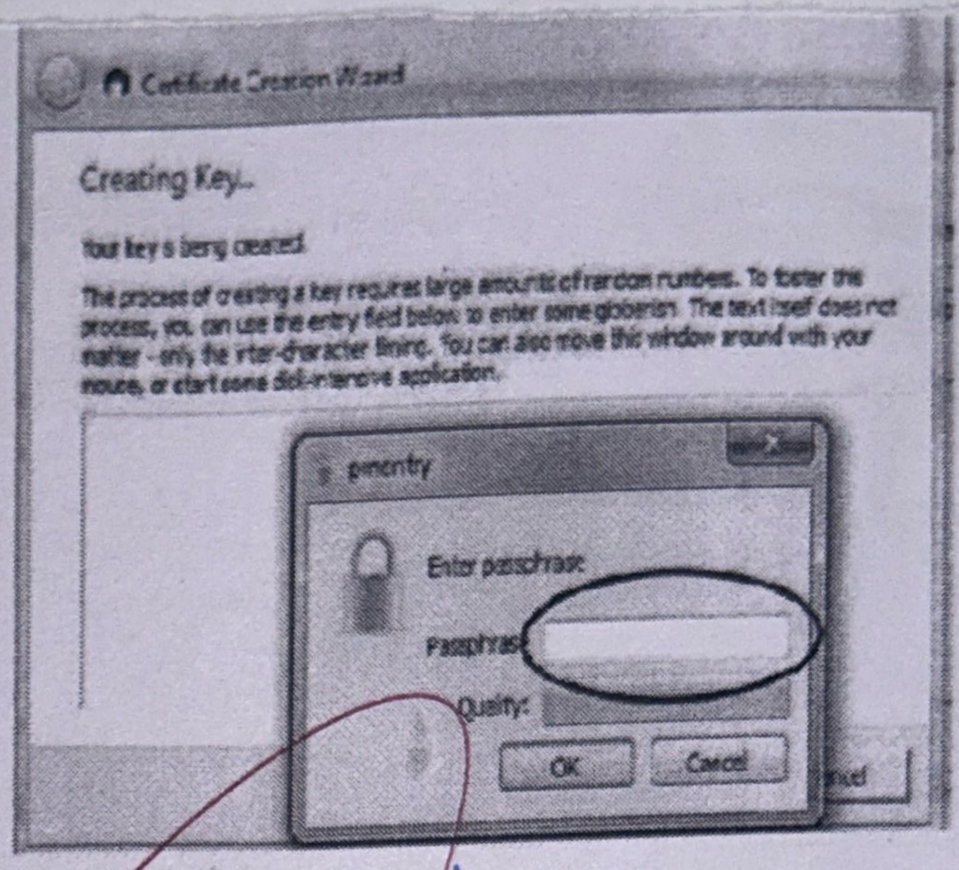




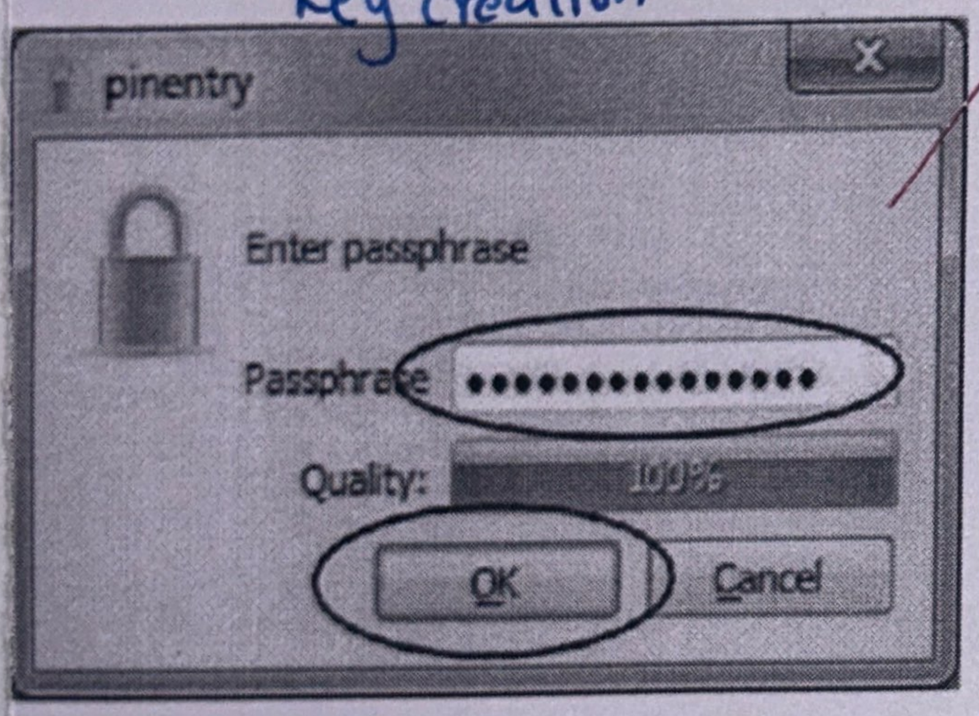
Certificate input

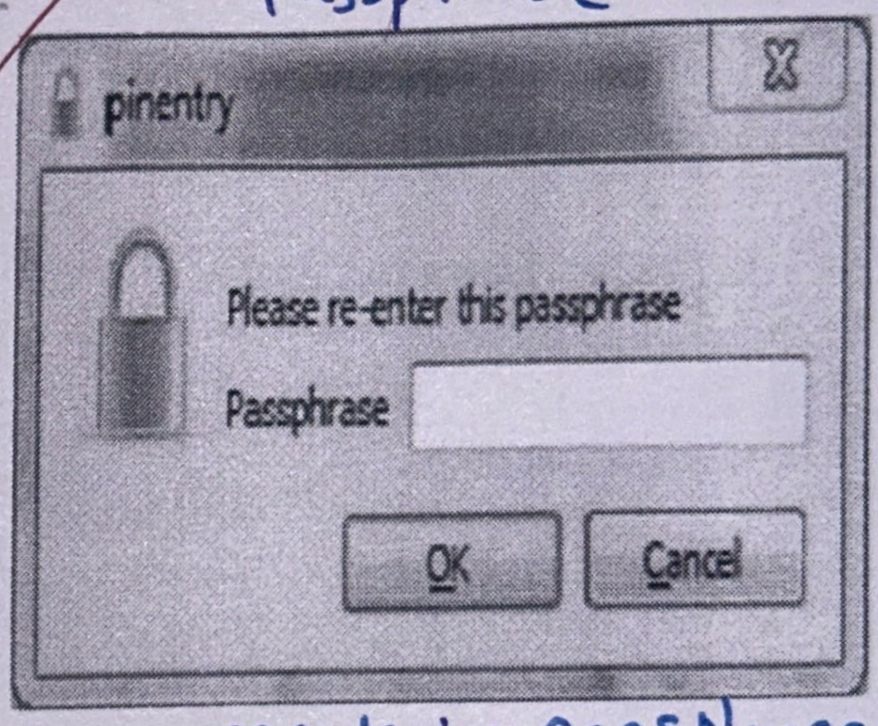


key creation

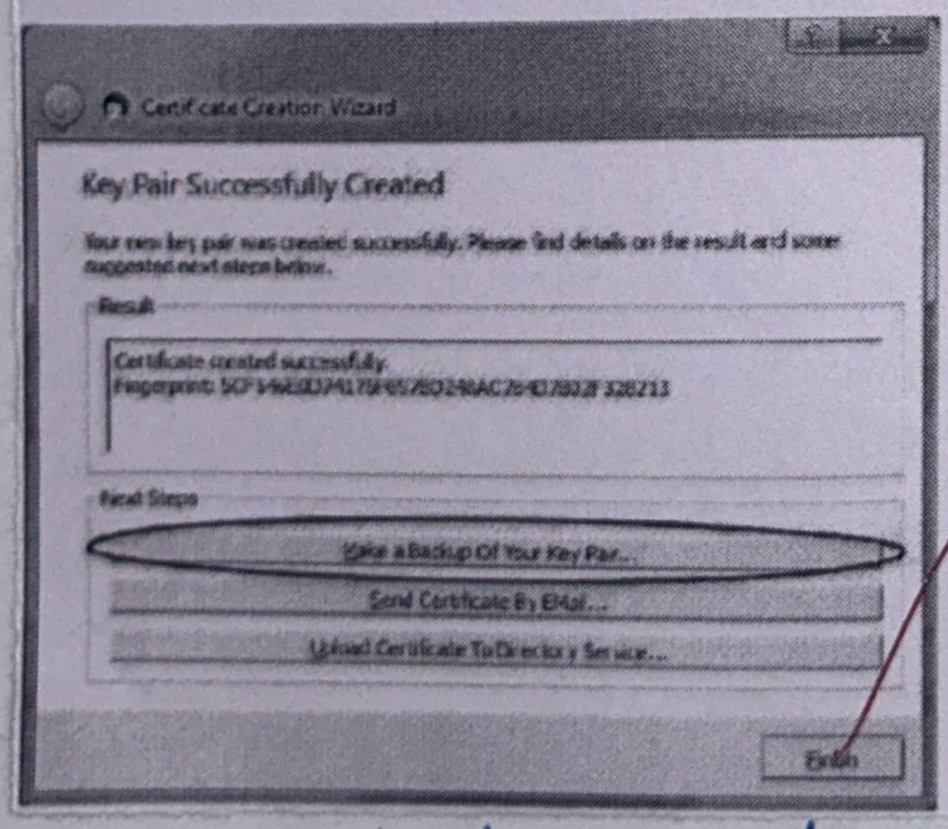


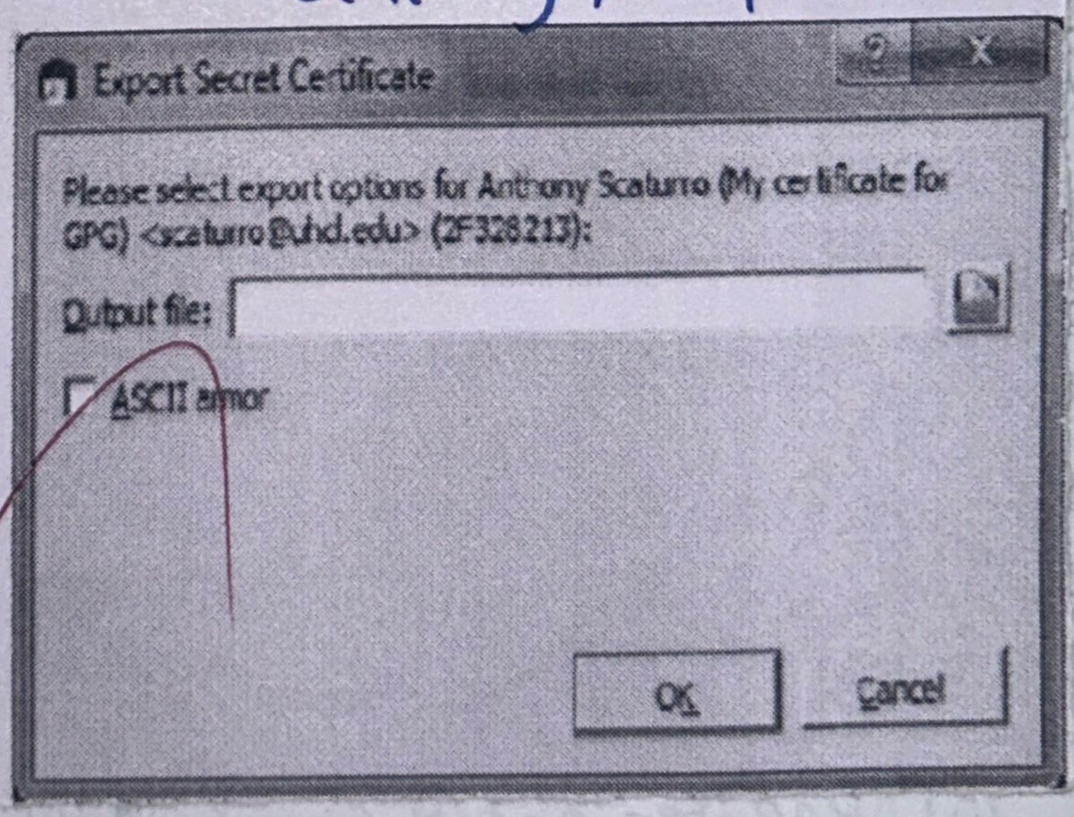
passphrase





reentering passphrase





backup & export

Date :

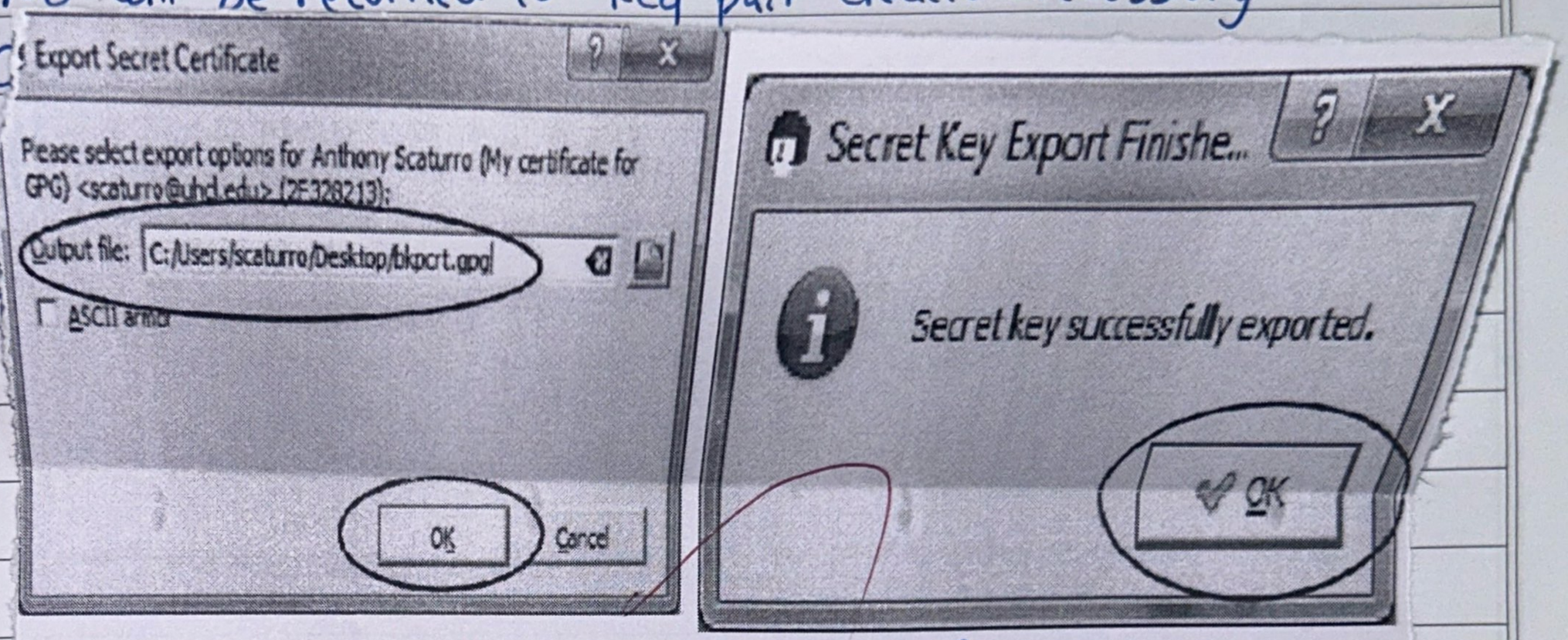
Page No. : 30
Expt. No. : 10a

12) You may backup key pair in folder of choice or skip it

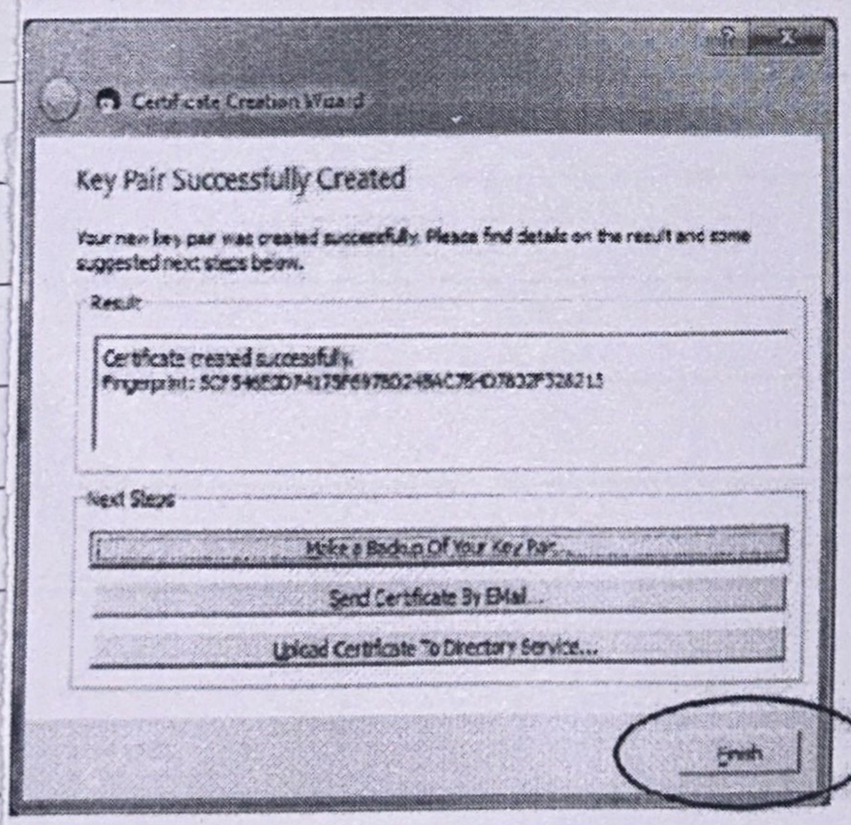
13) After key is exported, it will be displayed, click ok

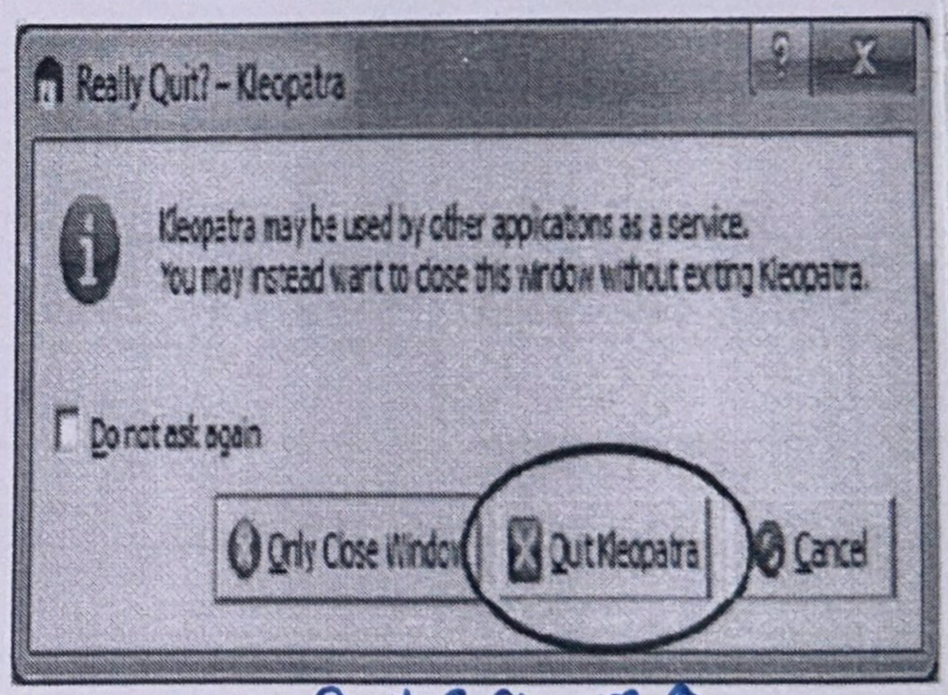
14) You will be returned to key pair created successfully

15)

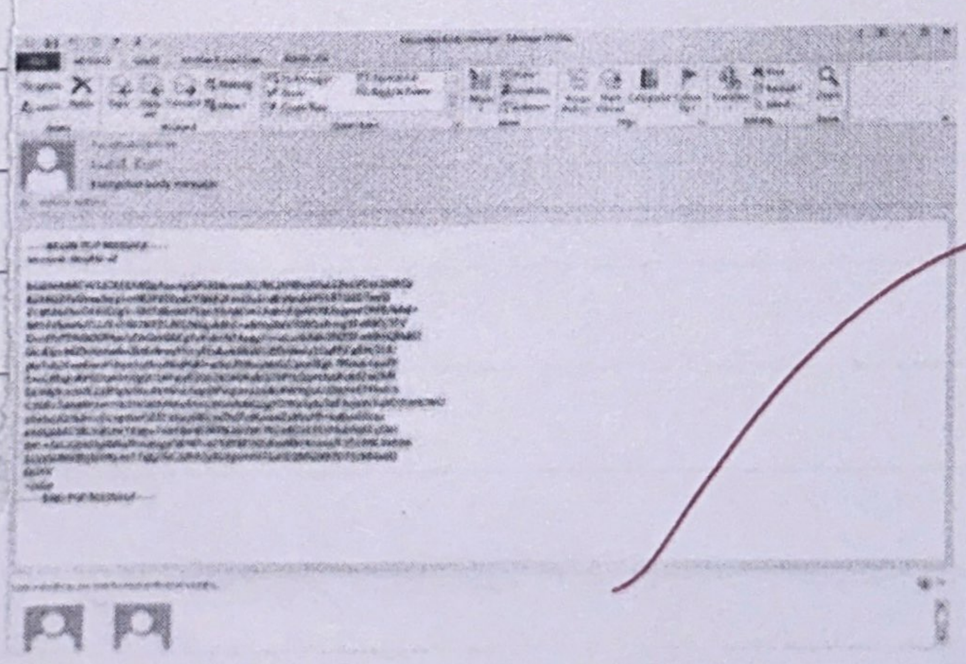


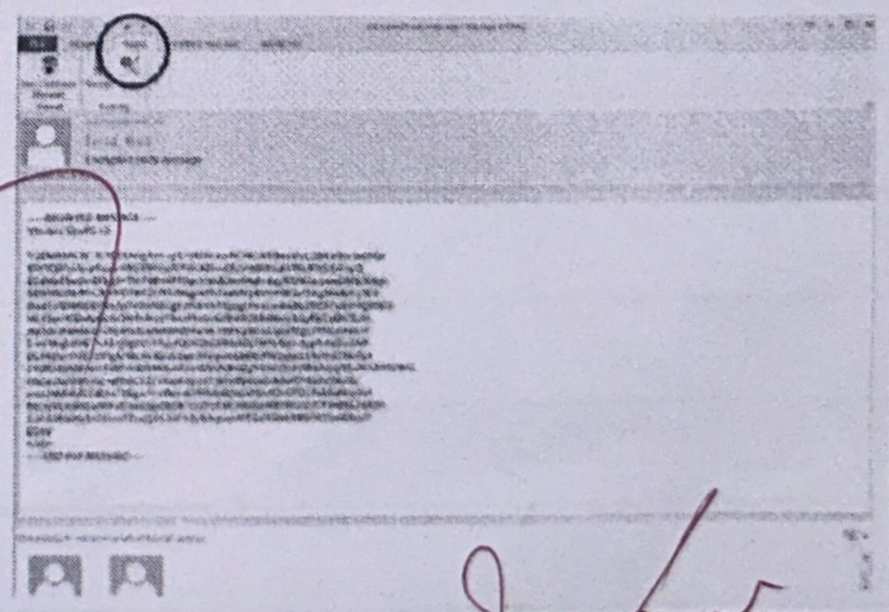
exporting ↑





Quit Software ↑

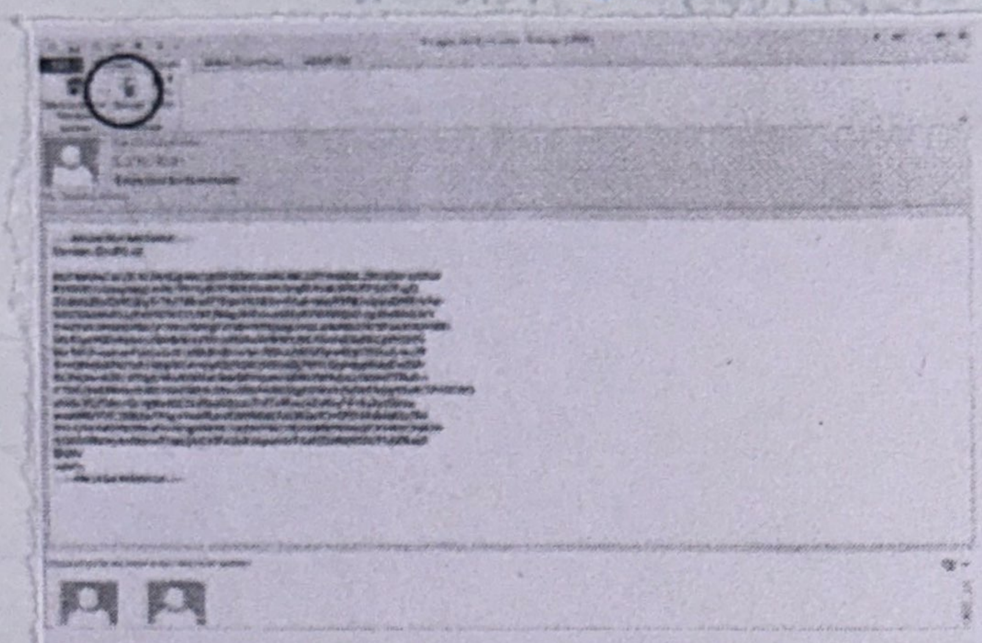


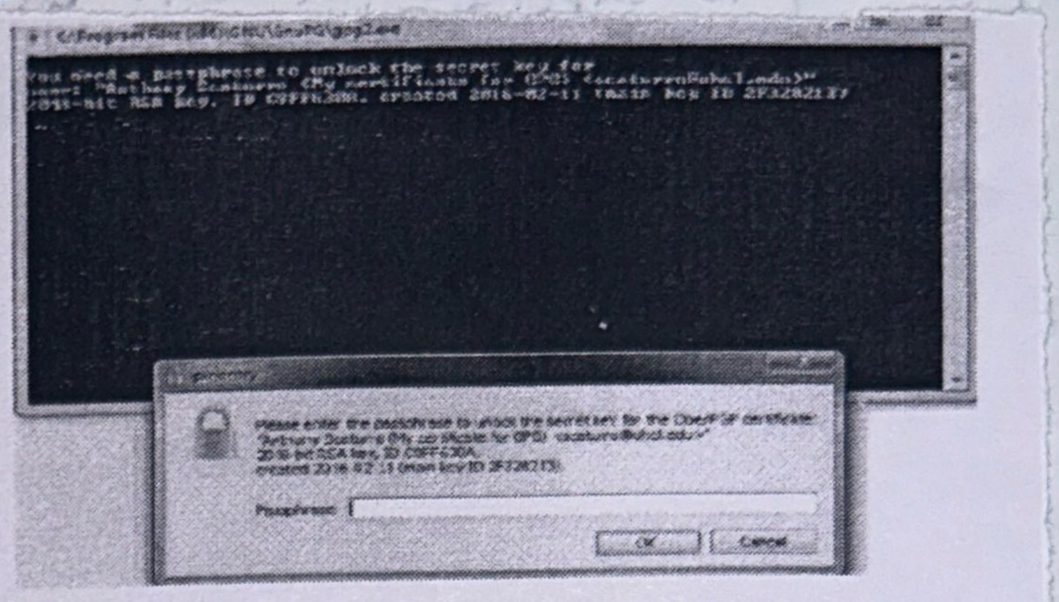


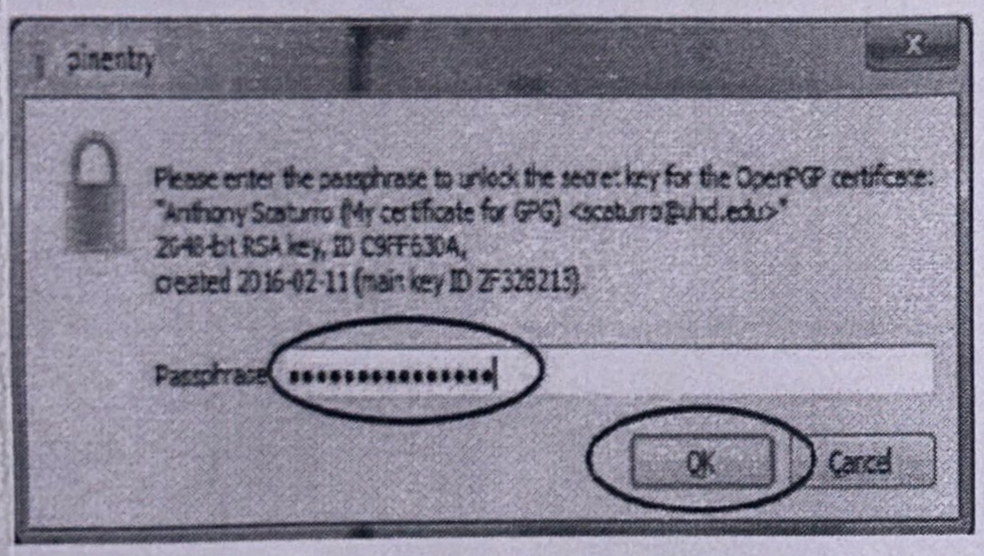
GPGOL tab

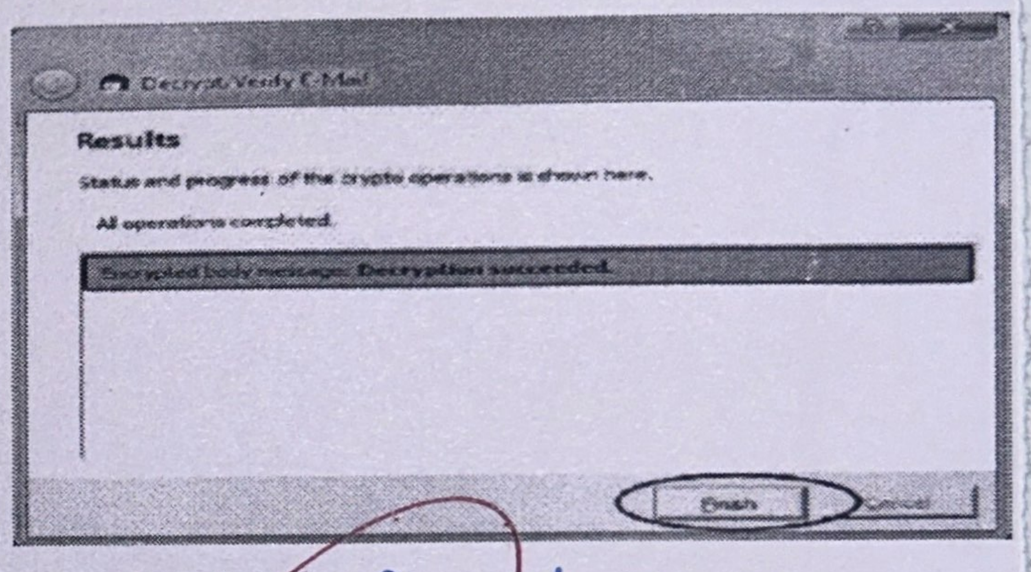
Teacher's Signature:

Selecting decryption ↓



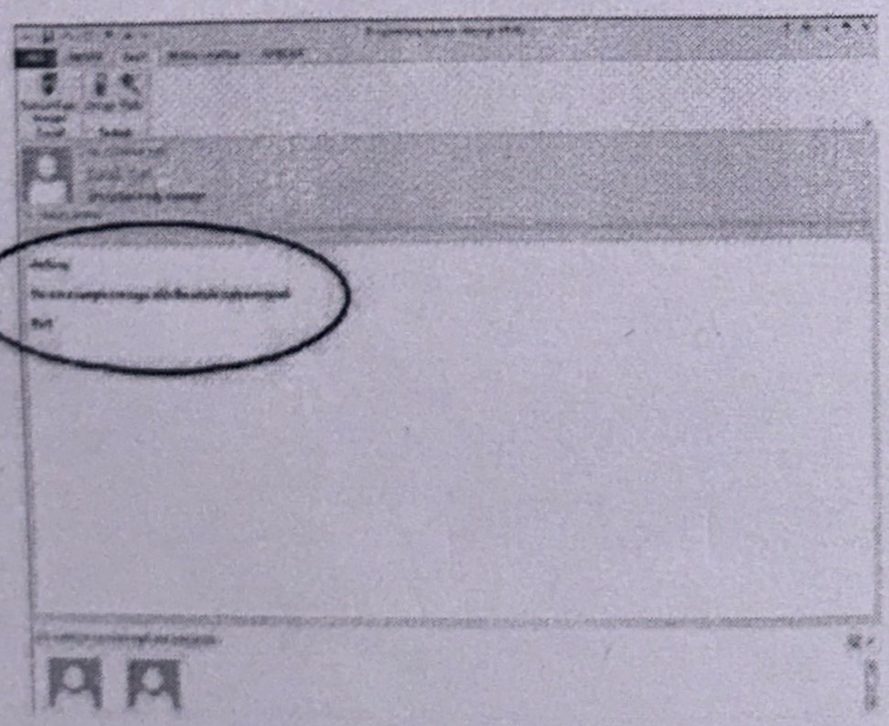


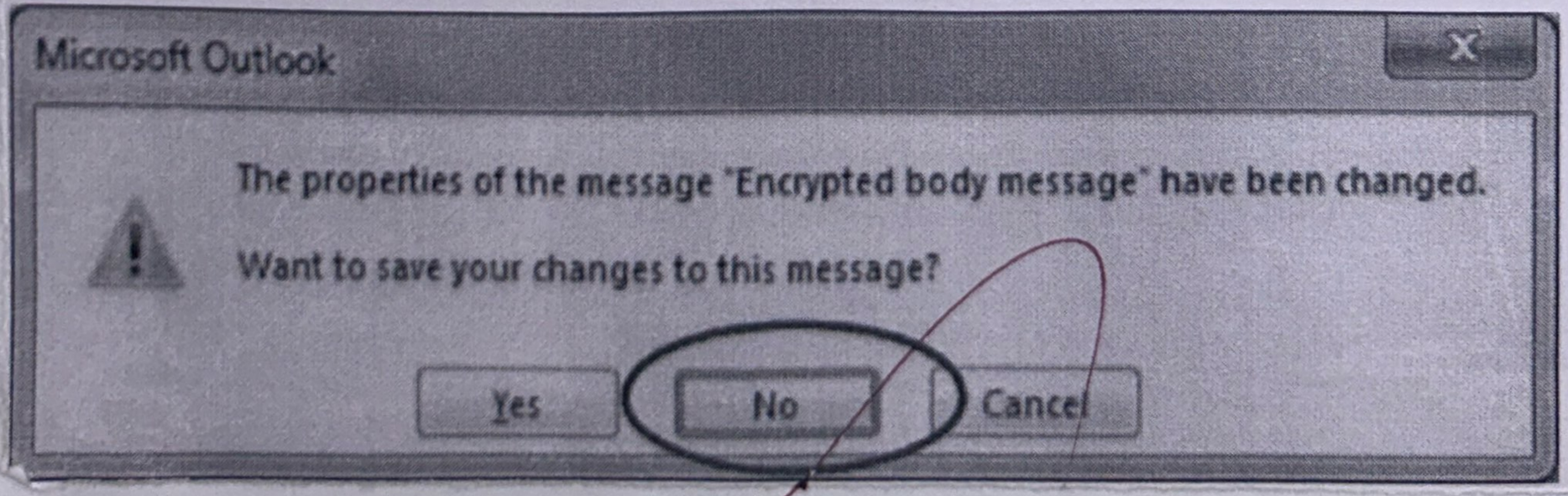




entering Passphrase

and confirming decryption





Date :

Page No. : 31

Expt. No. : 10 a

Decrypting an encrypted email that's sent to you:

1 Open email msg

2 OpenGL tab

3 Click decrypt button

4 In cmd, enter private passphrase

5 Enter passphrase, click ok

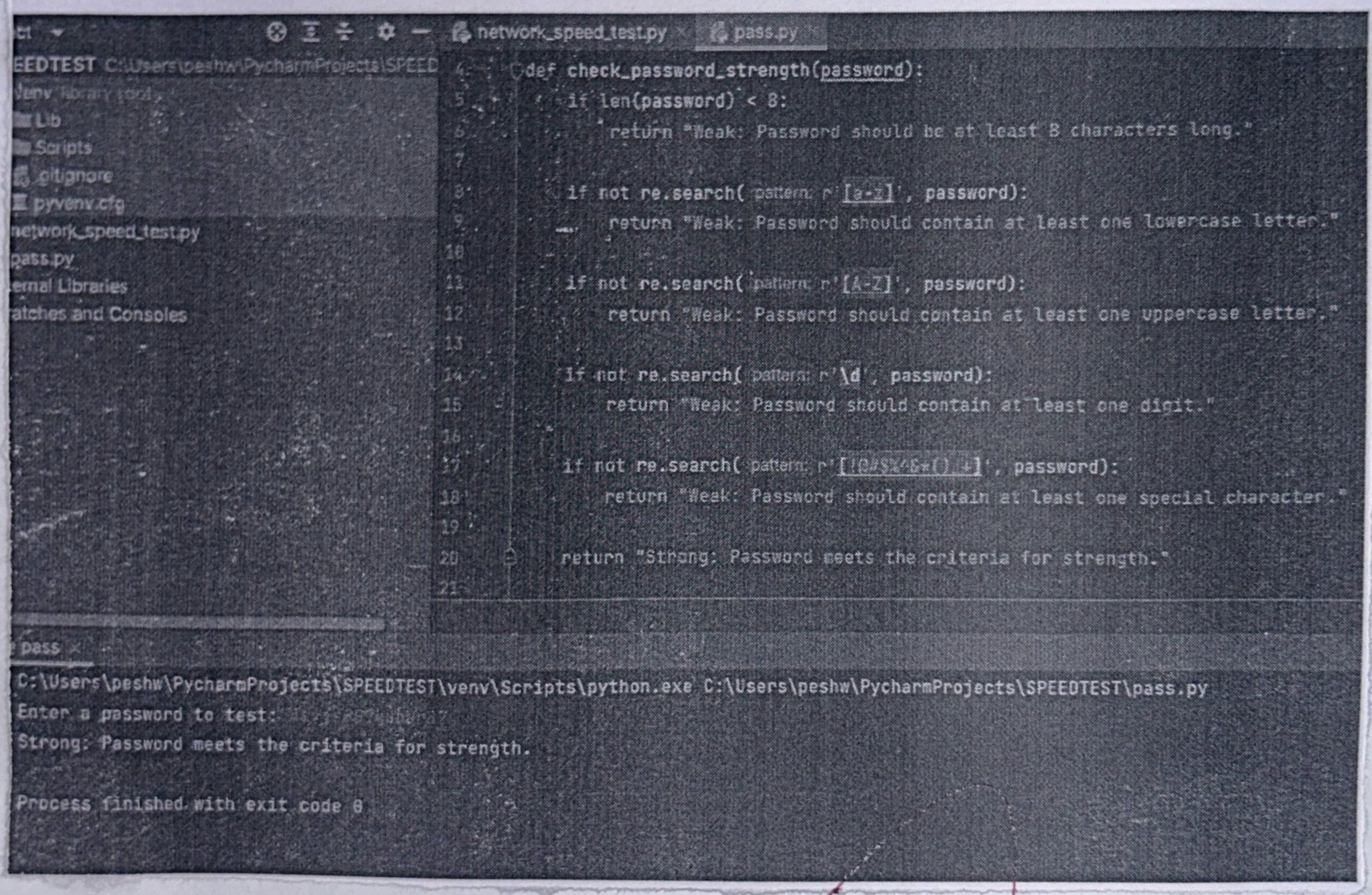
6 Result window shows status of decryption
Click on Finish

7 Your encryption mail msg will be displayed

8 Close mail and Click no, Email will remain encrypted

Result Kleopetra tool Demonstration is Completed Successfully

Teacher's Signature:



Password is input & confirming result

Date : 28/10/23

10B Subtask Password Strength TestingTool

Page No. : 32
Expt. No. : 10b

Aim

To check the strength of "user input" password

Program

```
import re

def password check_password_strength(password):
    if len(password) <8;
        return "weak: atleast 8 char is to be present"
    if not re.search(pattern: r'[a-z]', password):
        return "weak: atleast 1 lowercase is must"
    if not re.search(pattern: r'[A-Z]', password):
        return "weak: atleast 1 uppercase is must"
    if not re.search(pattern: r'\d', password):
        return "weak: atleast 1digit is must"
    if not re.search(pattern: r'[!@#$%.^&*()_+]', password):
        return" weak: atleast one special character is must"
    return "Strong Password, criteria is met"


if __name__ == "__main__":
    password = input("Enter password to test").
    result = check_ password_strength(password)
    print(result)
```

Result

Password strength testing tool implemented successfully

Teacher's Signature: