CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment (Extra Credit)

Using Public Key Encryption to Secure Messages

Student Info:

Name : Akhila Parankusham

Student ID: 00810899

Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

- Using Kleopatra, create certificates (public and private key pairs) for a student and administrator.
- The certificates can be imported and exported into Windows computers.
- With Opera Mail, encrypt a message by using the public key of the recipient.
- Using the recipient's private key, decrypt the message that was received.

Objectives

- Acquire knowledge about encryption methods to protect confidential information and lab files.
- Make certificates and run encryption and decryption processes under several user identities.
- Examine how public key infrastructure (PKI) can be used to secure communications.

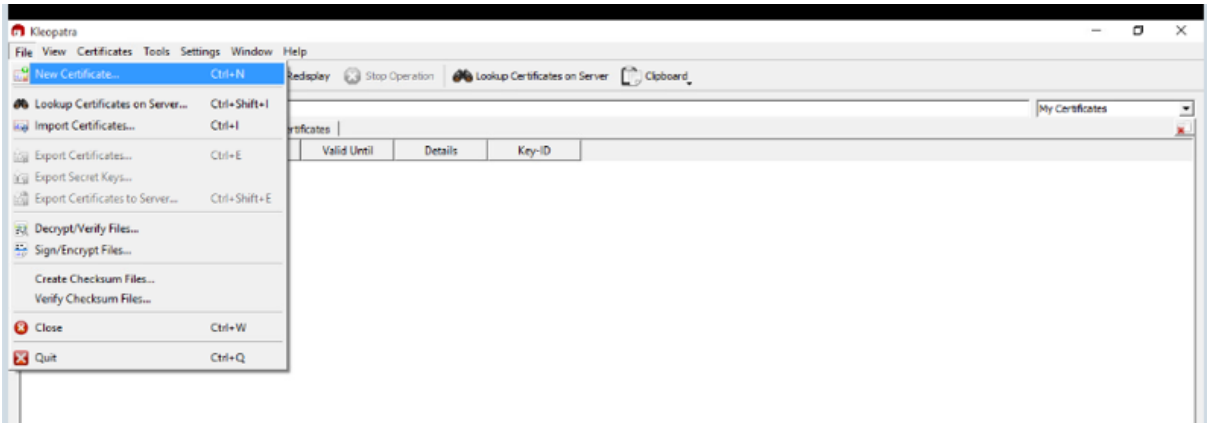
Lab Description Details

Steps Taken, Notes, & Screen Shots demonstrating completion of the lab

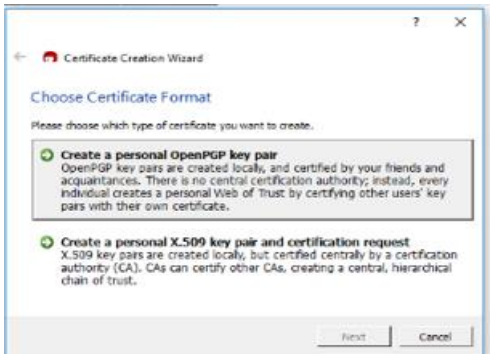
Supporting Evidence

Step 1: Launch the internal Windows 10 machine. Open Kleopatra.

Step 2: Select File>New Certificate



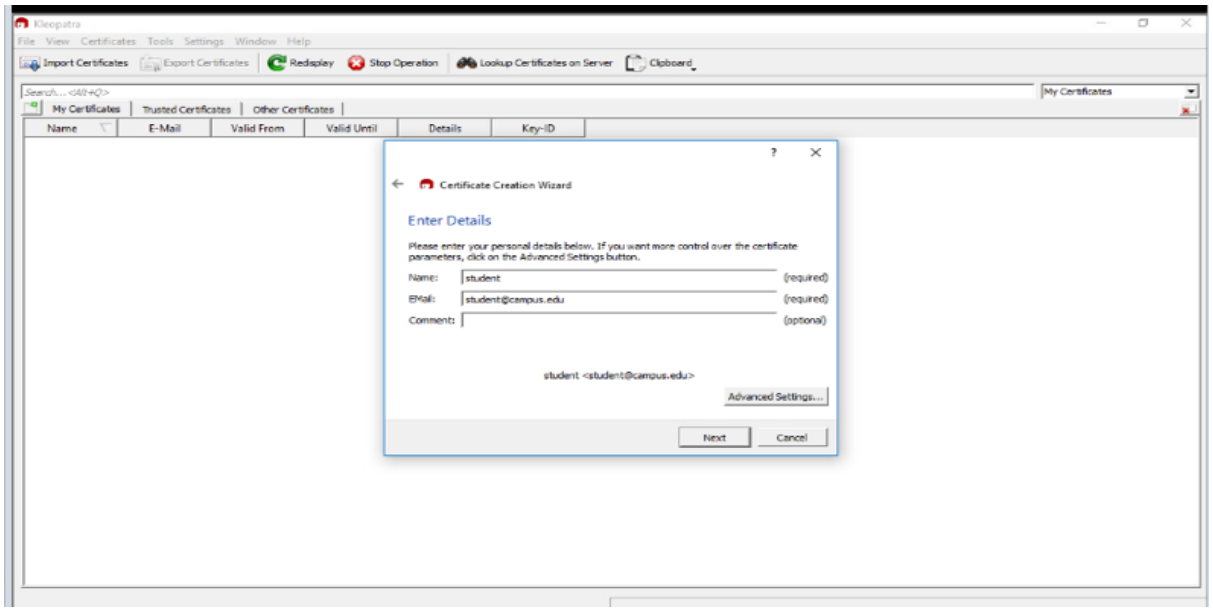
Step 3: Create a personal OpenPGP key pair.



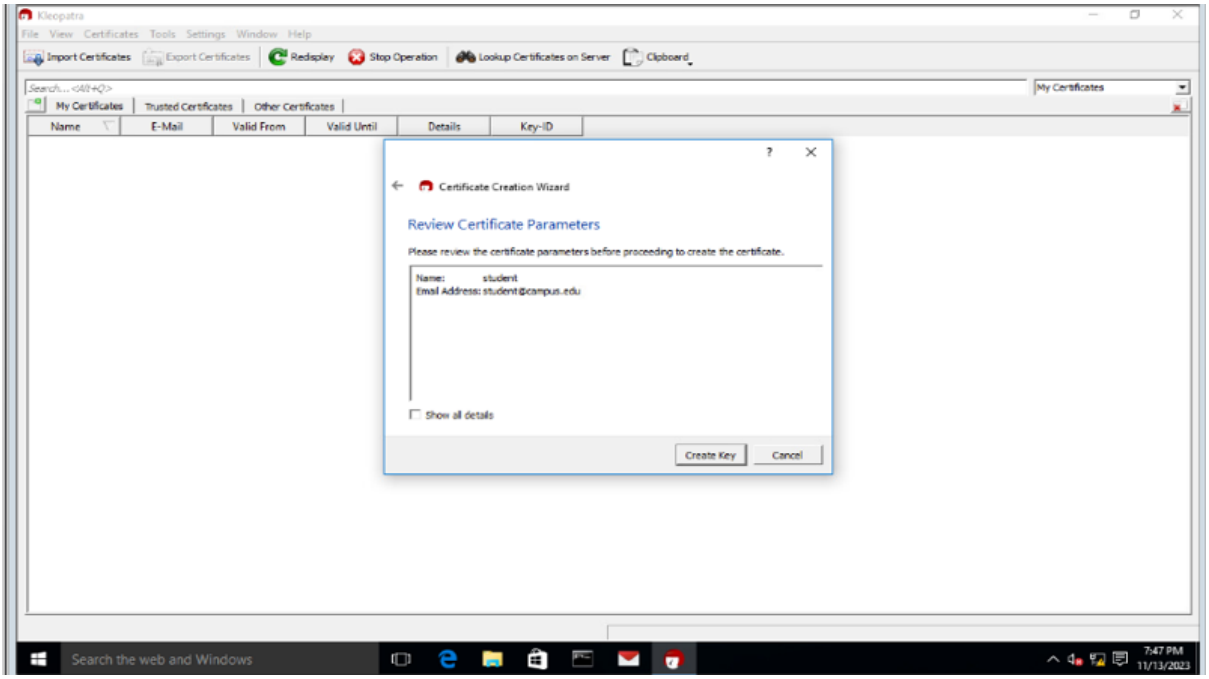
Step 4: Enter the details.

Name: student

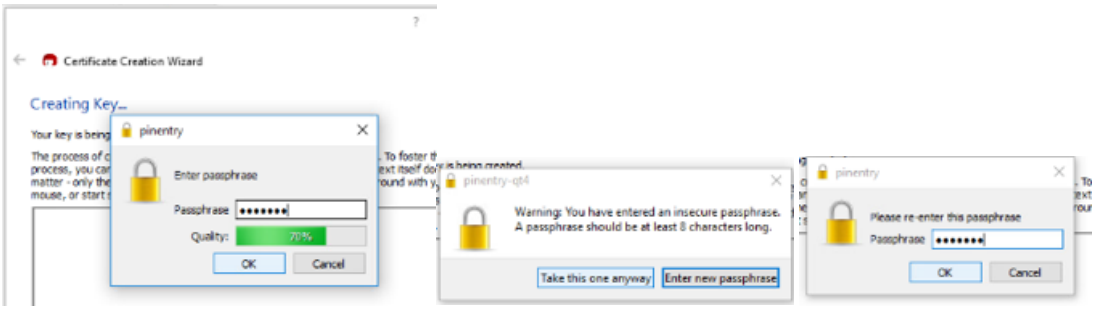
Email: student@campus.edu



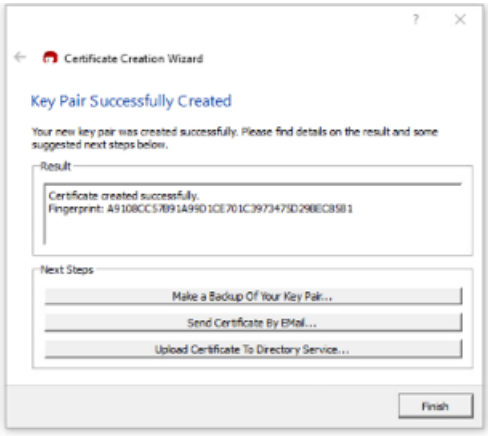
Step 5: Create the key.



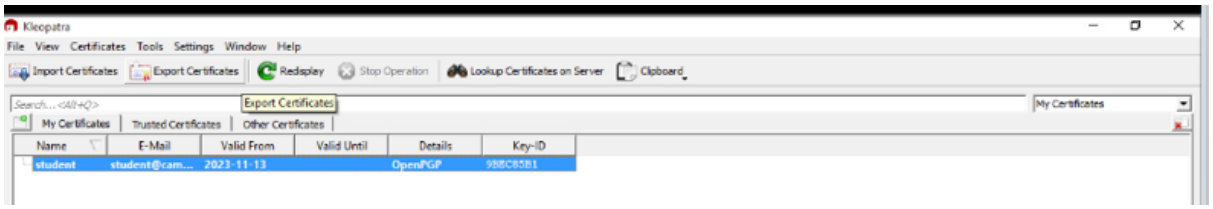
Step 6: Type student as passphrase at the pinentry screen. Choose take this one anyway if the screen appears again. Re-enter the passphrase again.



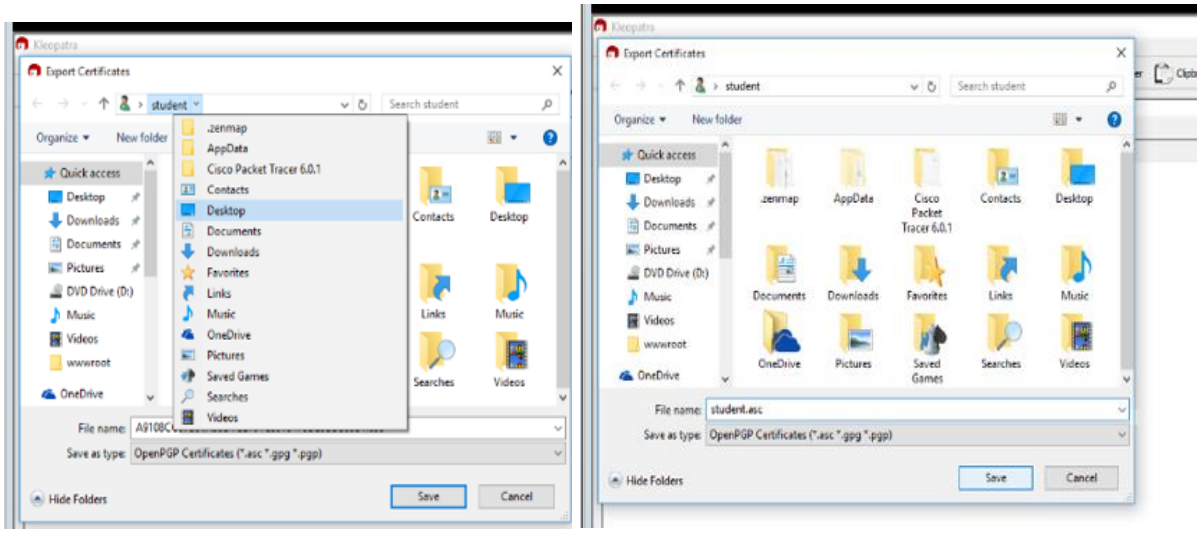
Step 7: Finish the certificate creation.



Step 8: Select student certificate>Export Certificates



Step 9: Select Desktop>student.asc>Save

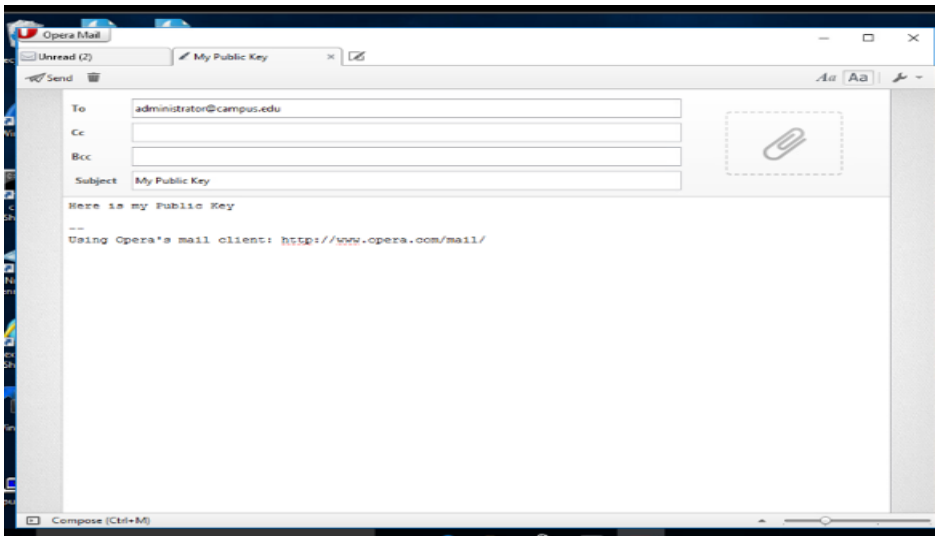


Step 10: Open Opera Mail and compose a mail. Attach a file.

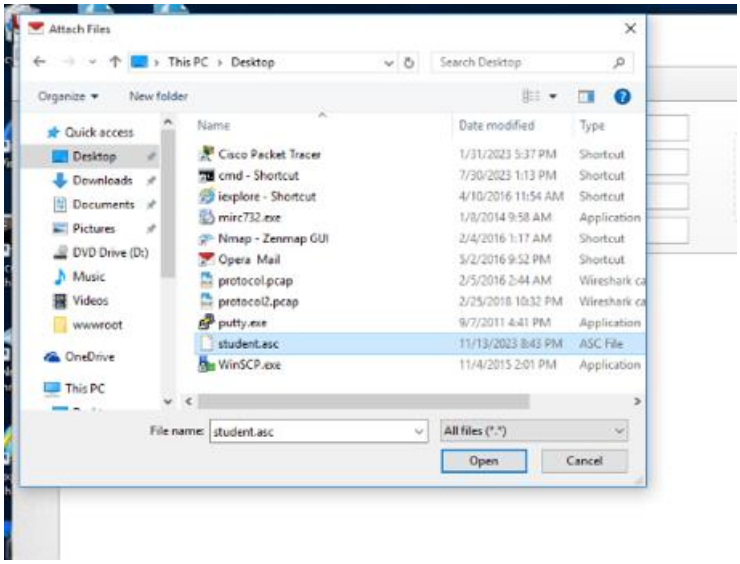
To: administrator@campus.edu

Subject: My Public key

Body: Here is my Public Key.



Step 11: Save the file(student.asc) to Desktop and Open it. Send the mail.

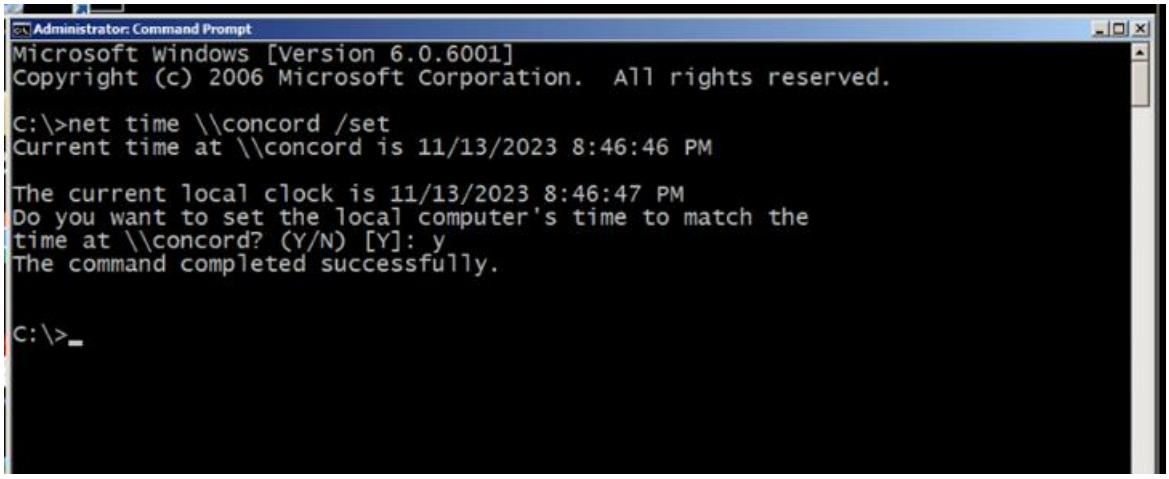


Step 12: Launch Windows Server. Enter the credentials.

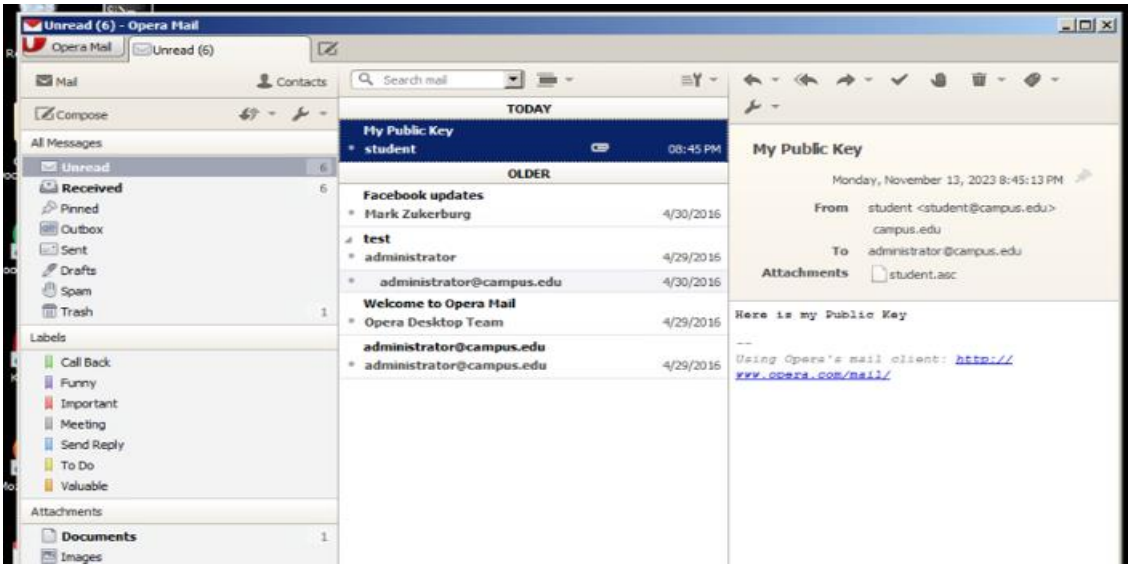
Username: administrator

Password: P@ssw0rd

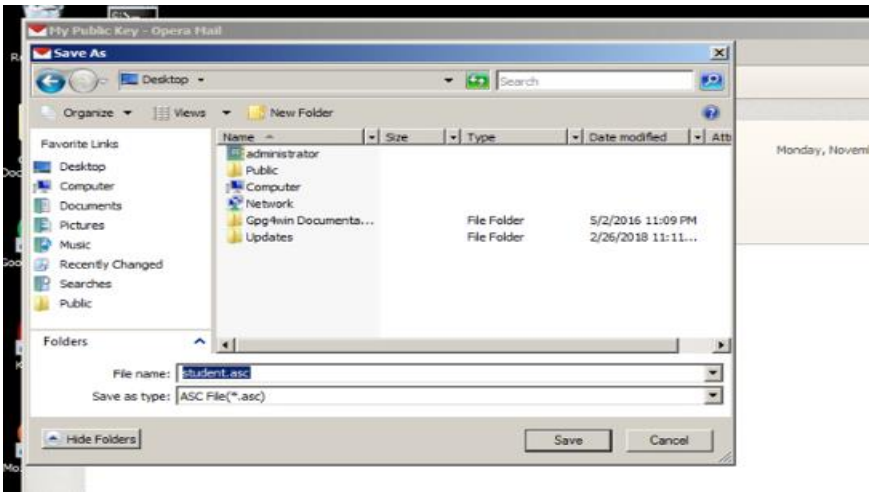
Step 13: Set the clock on the VM.



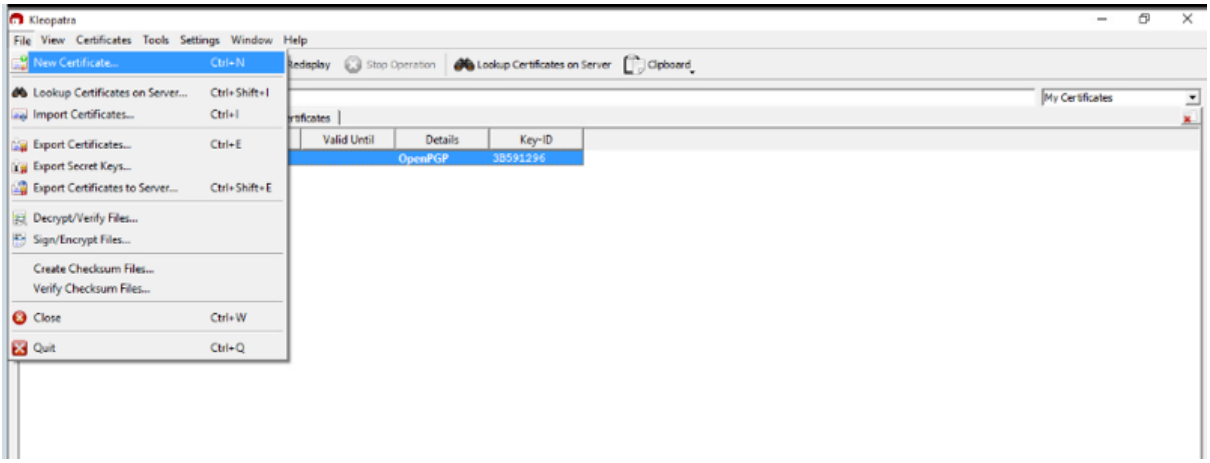
Step 14: Open the mail. Select My Public Key mail from send/receive mails.



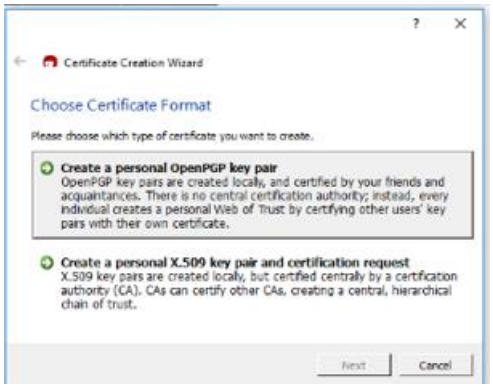
Step 15: Save the file.



Step 16: Open Kleopatra. Create a certificate for an administrator.



Step 17: Create a personal OpenPGP key pair.

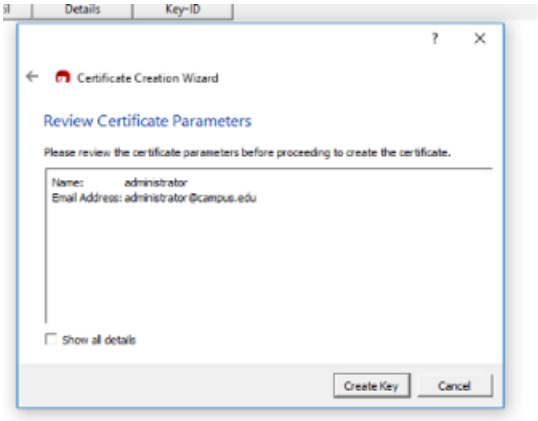


Step 18: Enter the details.

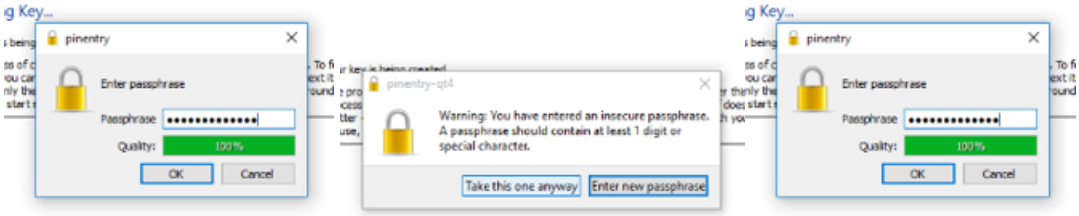
Name: administrator

Email: administrator@campus.edu

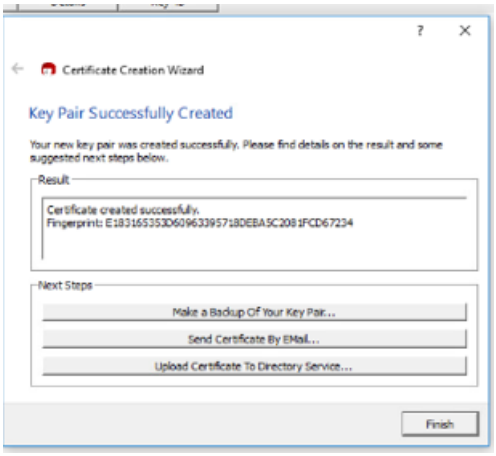
Step 19: Create the key.



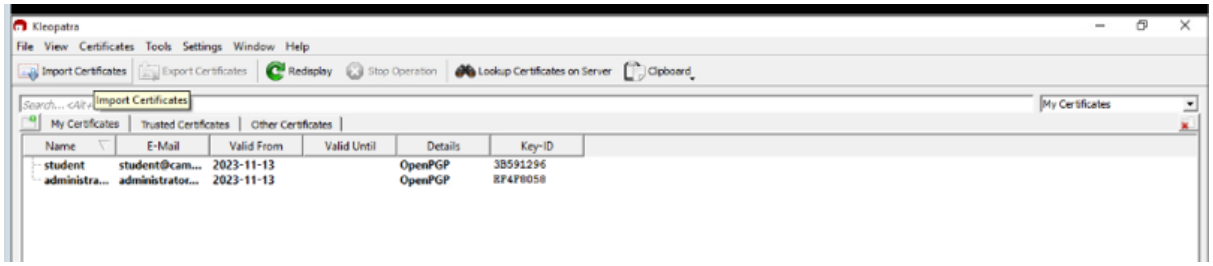
Step 20: Type administrator as the passphrase at the pinentry screen. Choose take this one anyway. Re-enter the passphrase as administrator when the pinentry screen appears.



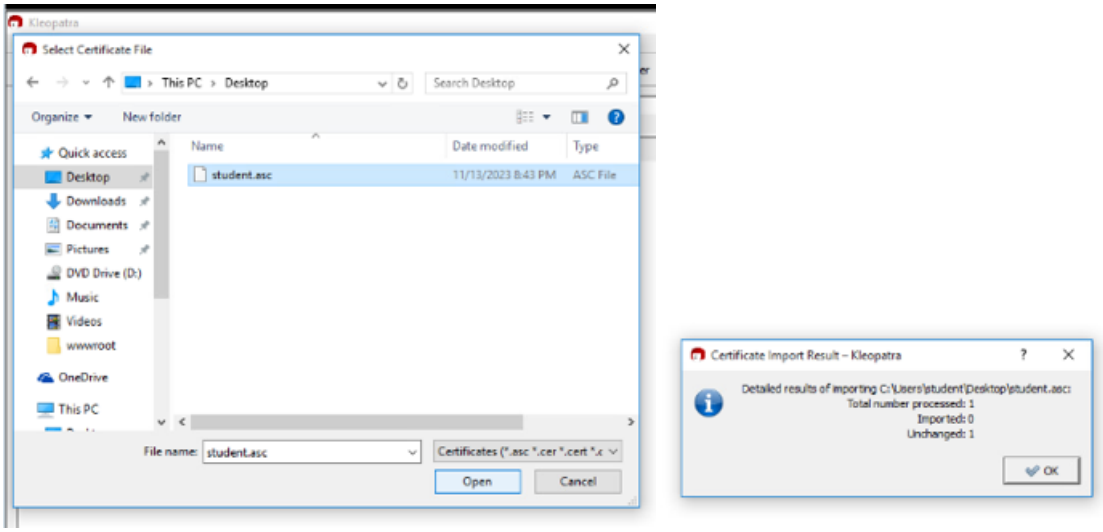
Step 21: Complete the certificate creation.



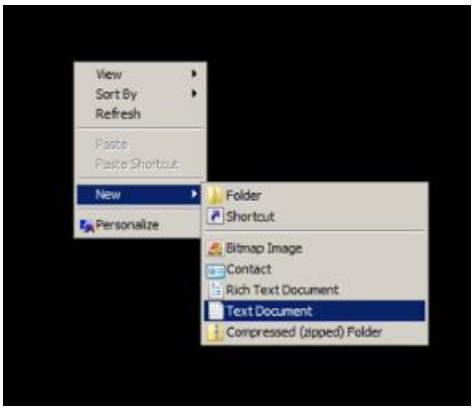
Step 22: Import certificates.



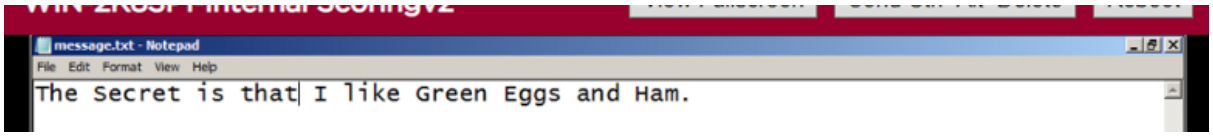
Step 23: Save the file(student.asc) to Desktop.



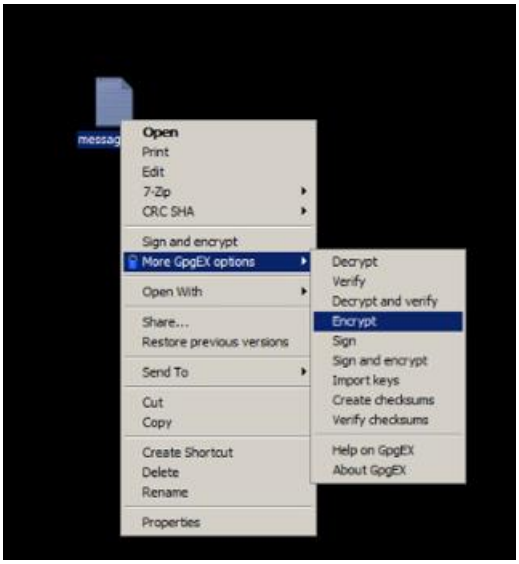
Step 24: Create a new text document in Windows Server desktop and name it as message.txt



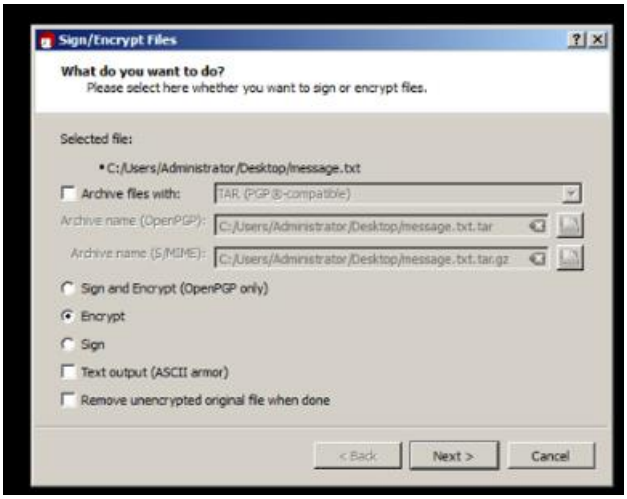
Step 25: Type the message in the text file and save it.



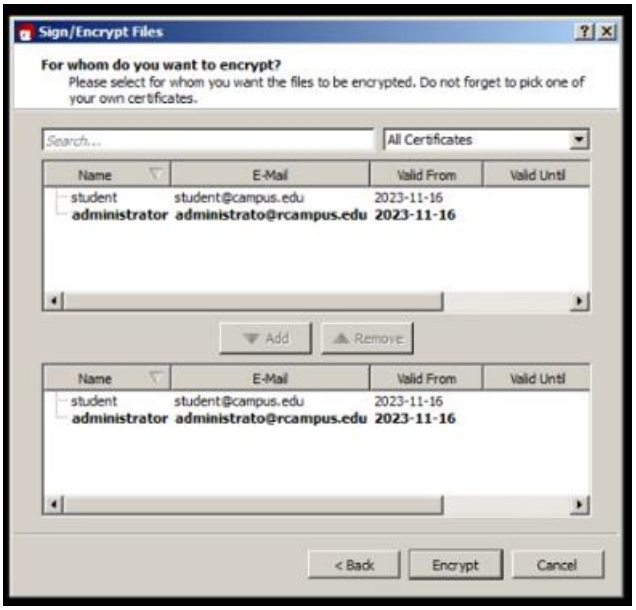
Step 26: Click message.txt. Select More GpgEX>Encrypt.



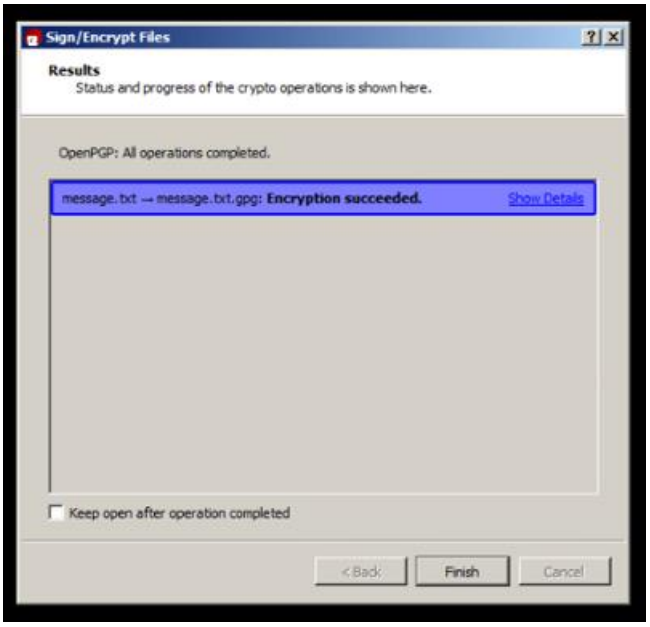
Step 27: Sign the files.



Step 28: Add the student and administrator certificates and encrypt them.



Step 29: Uncheck the box and click finish.

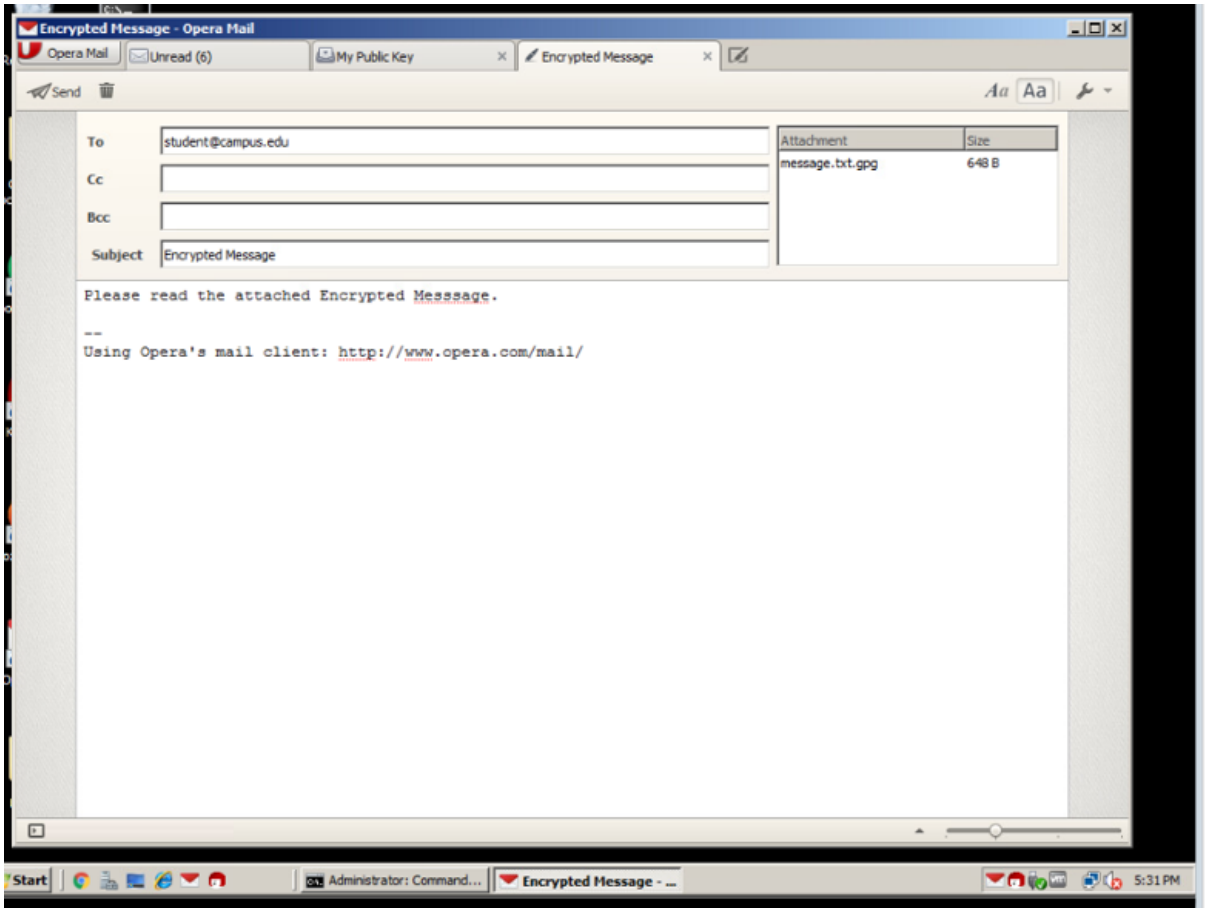


Step 30: Open the mail and compose the mail.

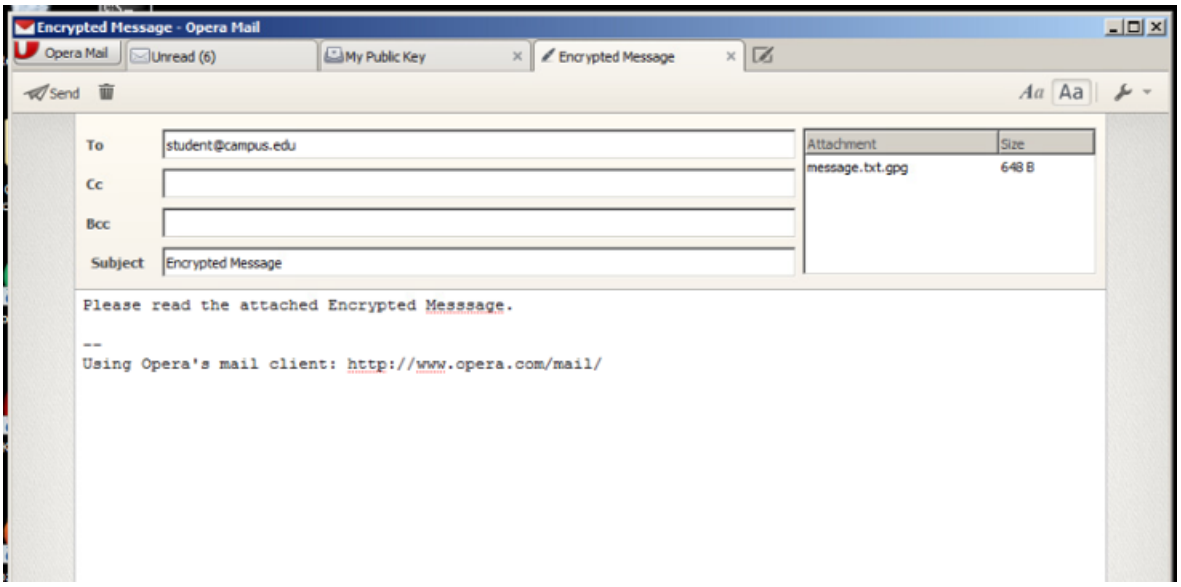
To: student@campus.edu

Subject: Encrypted Message

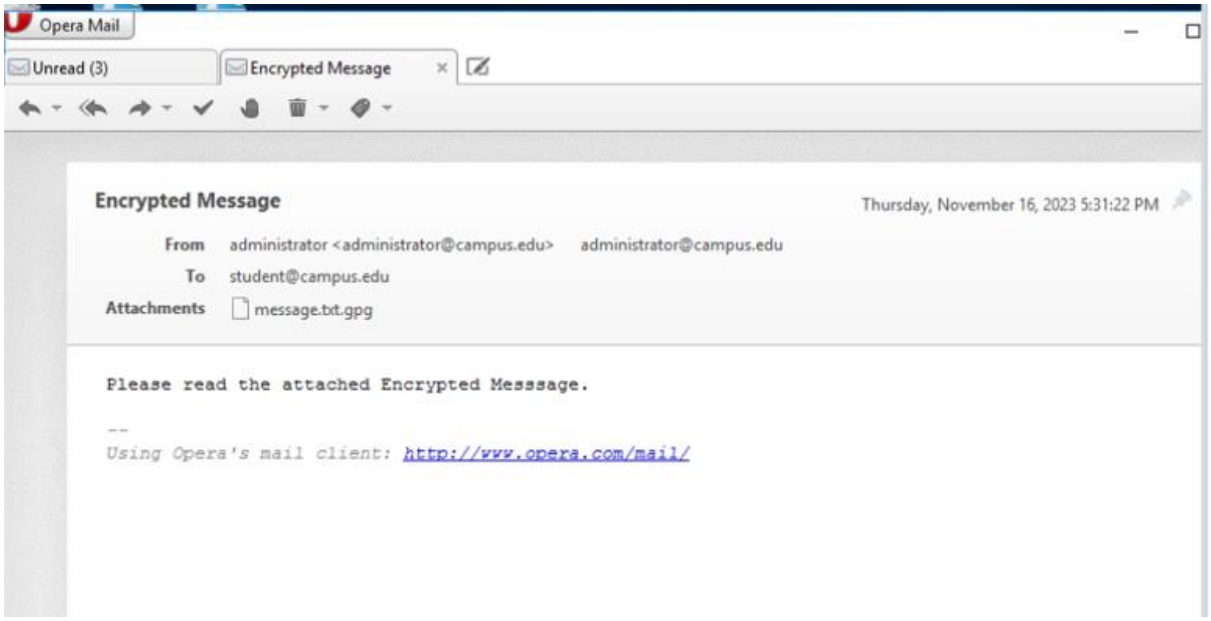
Body: Please find the attached Encrypted Message.



Step 31: Open message.txt.gpg message and send it.

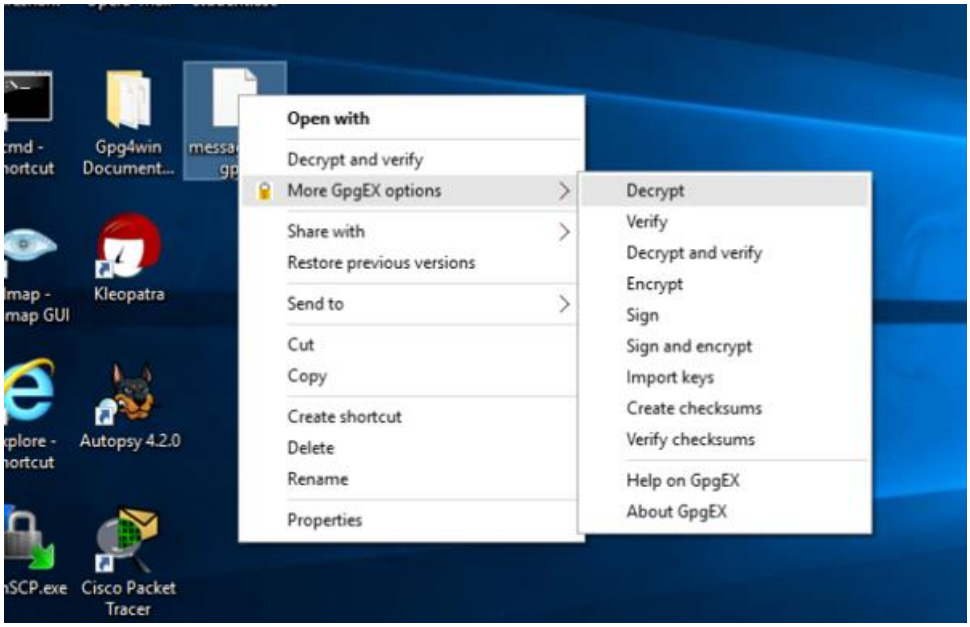


Step 32: Open Opera Mail on a Windows 10 machine. Open the received emails and read encrypted message.

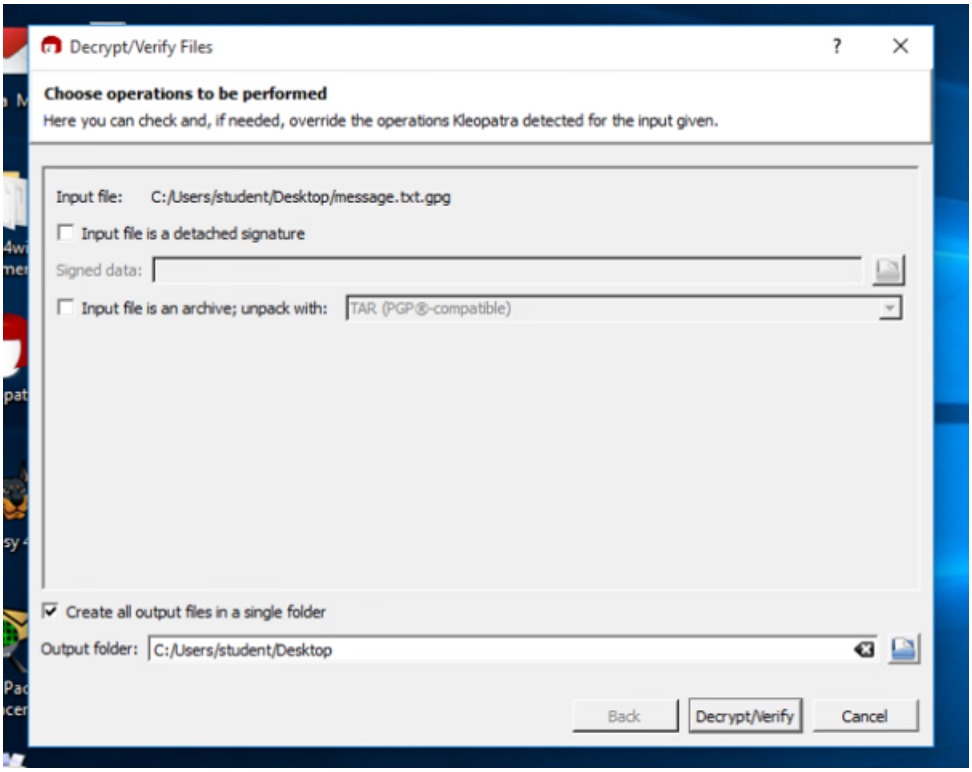


Step 33: Save the file(message.txt.gpg) to Desktop.

Step 34: Select message.txt.gpg>More GpgEX options>Decrypt

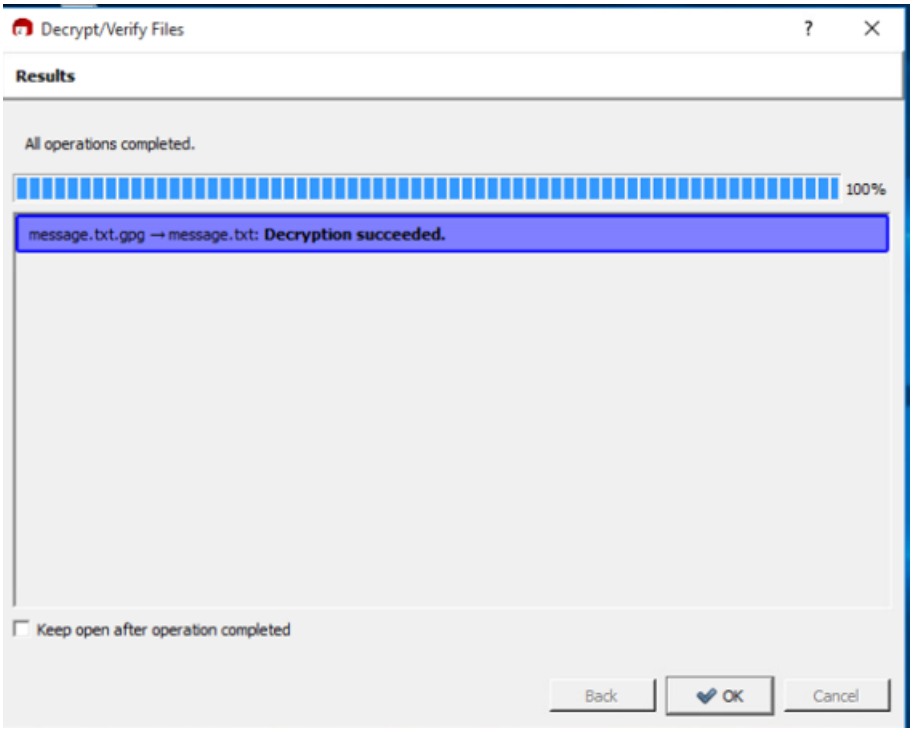


Step 35: Decrypt the file.



Step 36: Enter the passphrase as student.

Step 37: Uncheck the box.

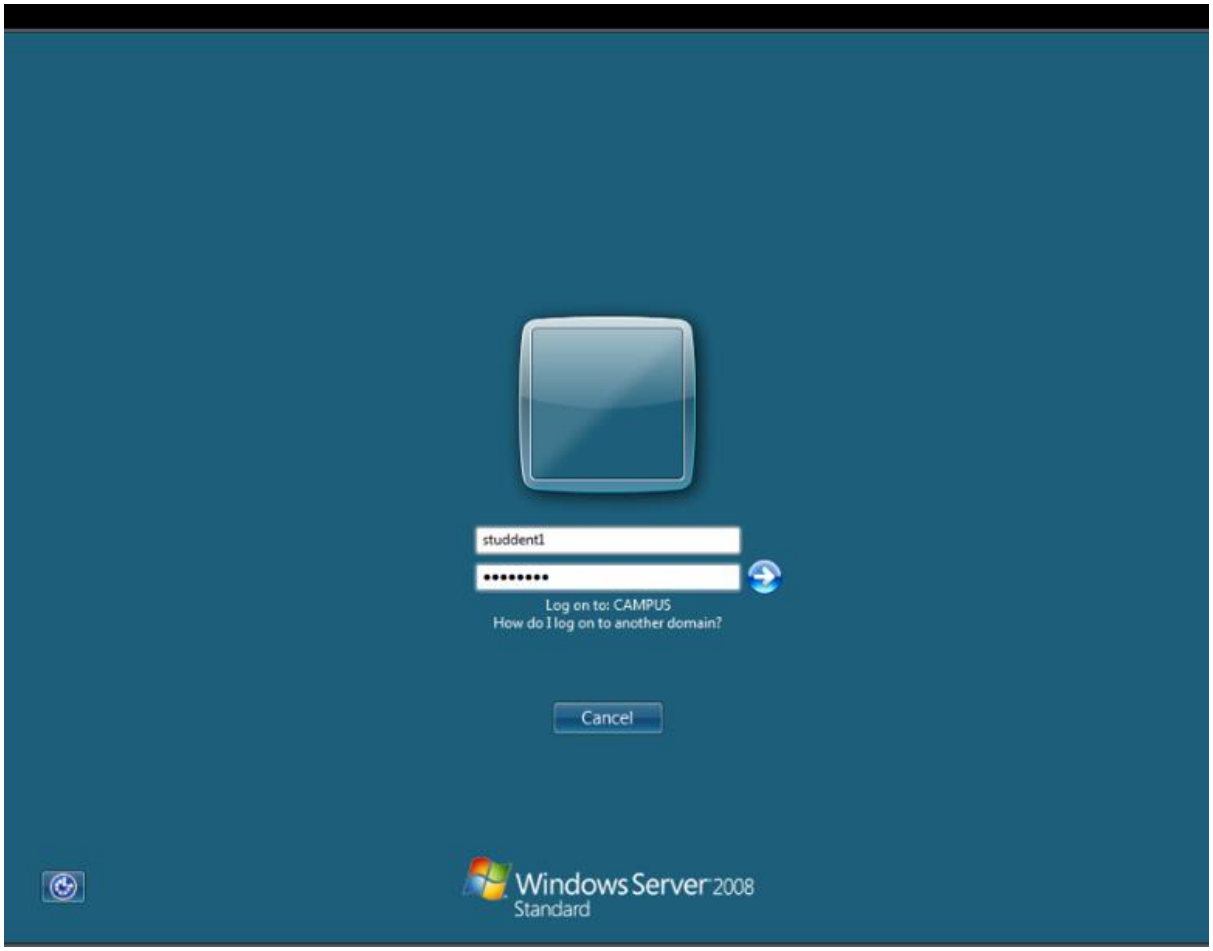


Step 38: Open the file and read the message.

Step 39: Log in to the virtual machine and enter the details.

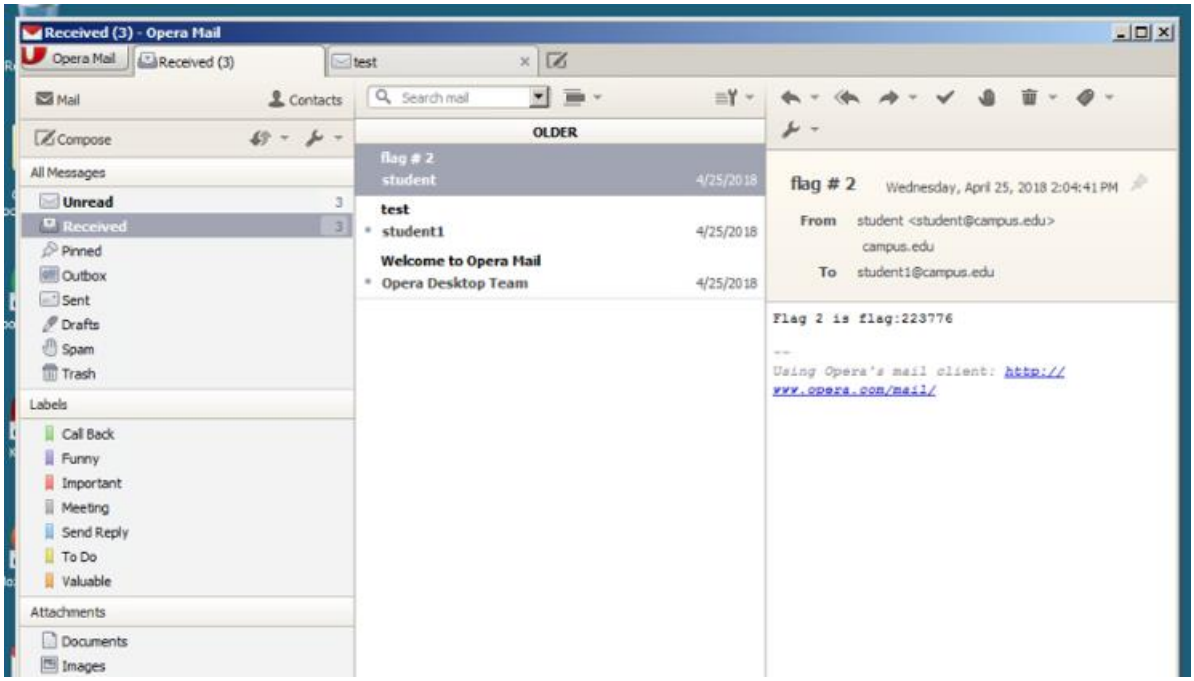
Username: student1

Password: P@ssw0rd



Step 40: Open the sample flag file.

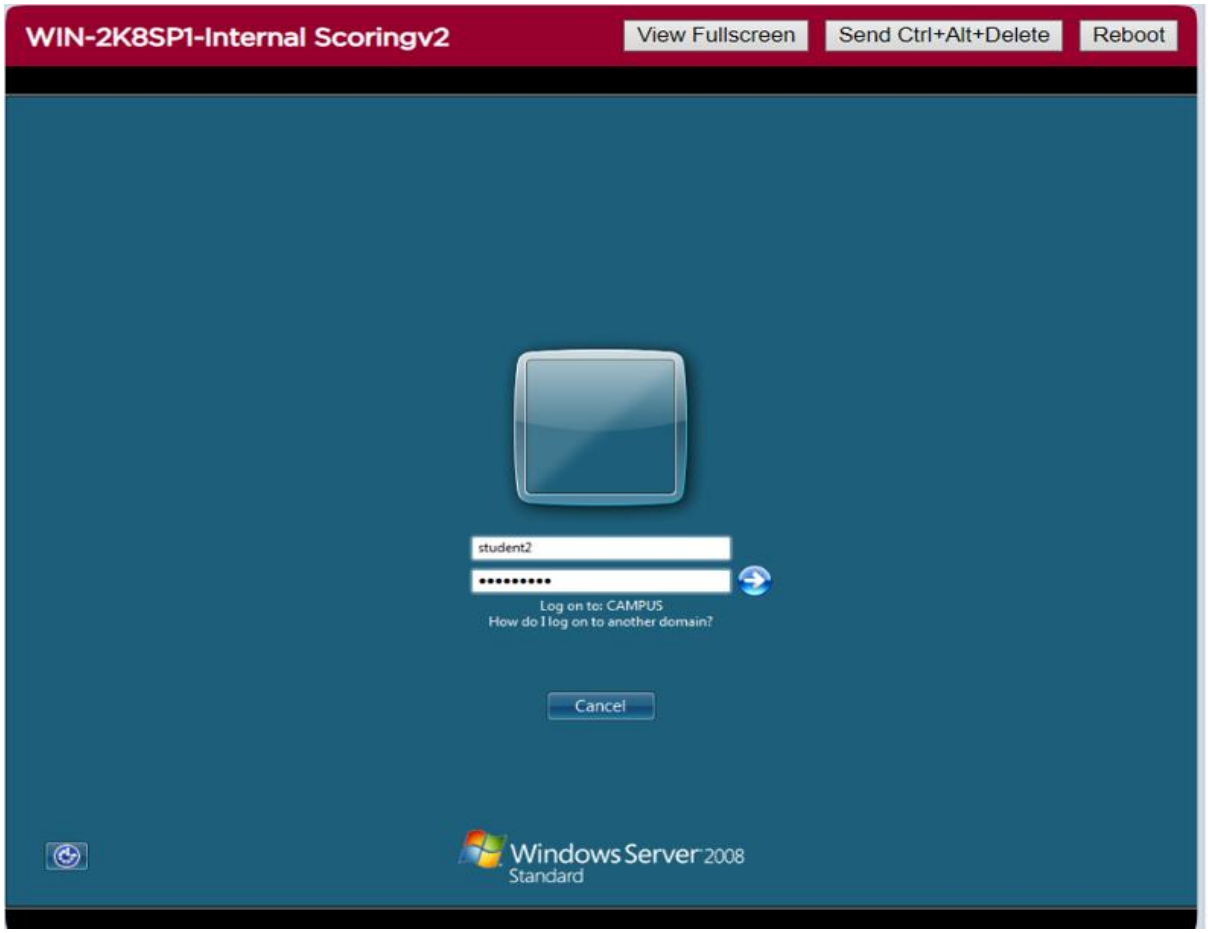
Step 41: Open the Opera Mail. Solve the challenge 1.



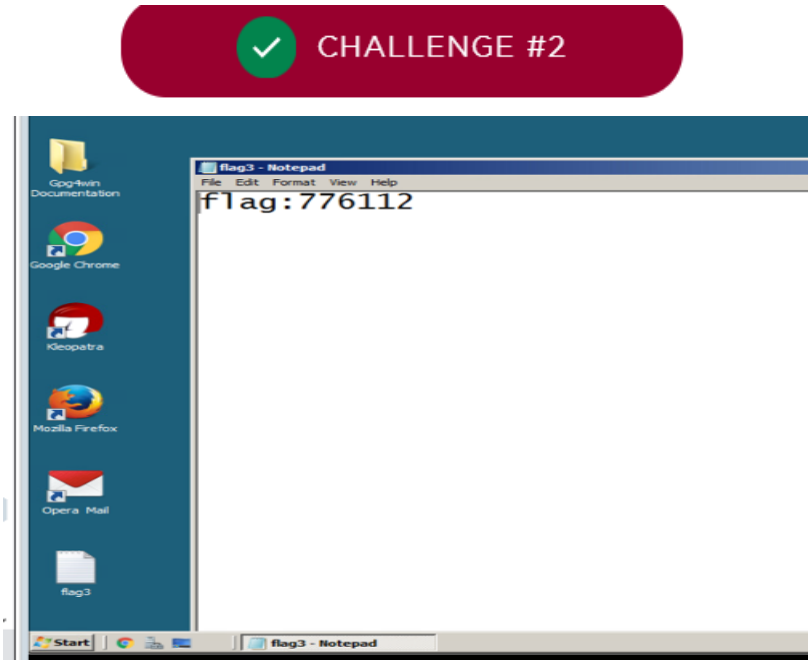
Step 42: Log in to the virtual machine and enter the details.

Username: student2

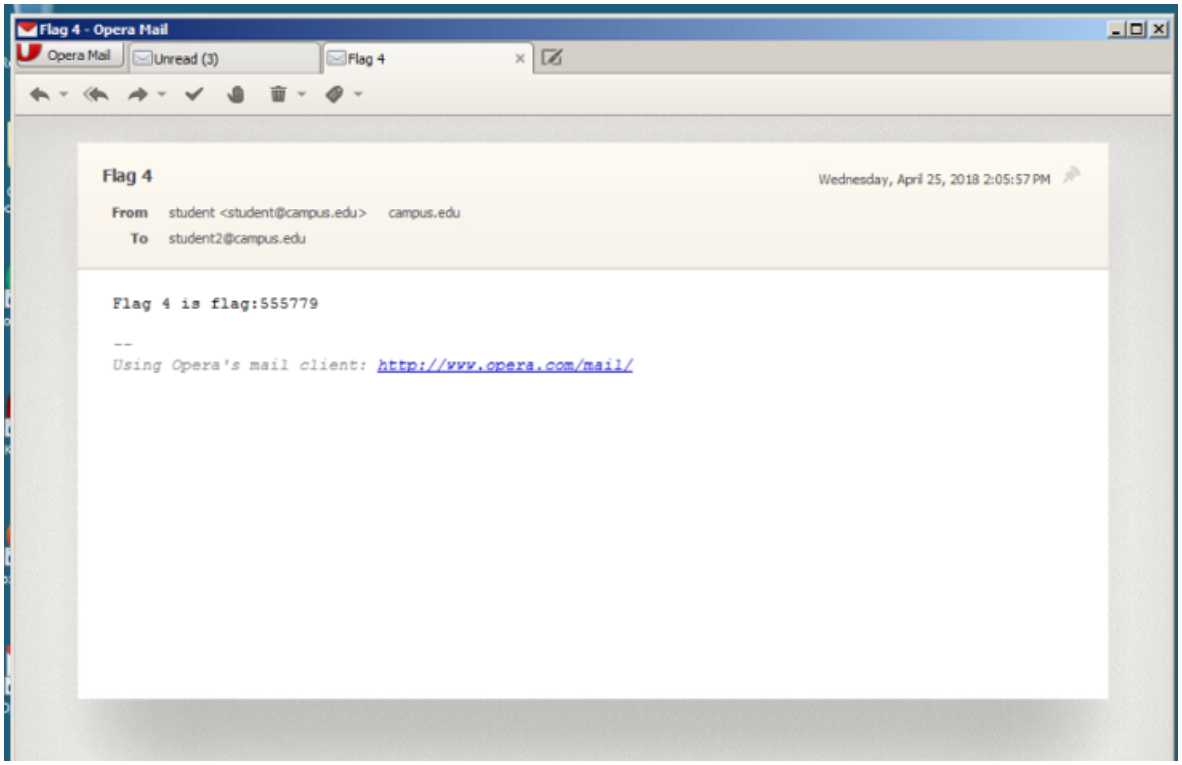
Password: P@ssw0rd



Step 43: Open the flag3 file on your desktop. Solve the challenge 2.



Step 44: Open the Opera Mail. Solve the challenge 3.

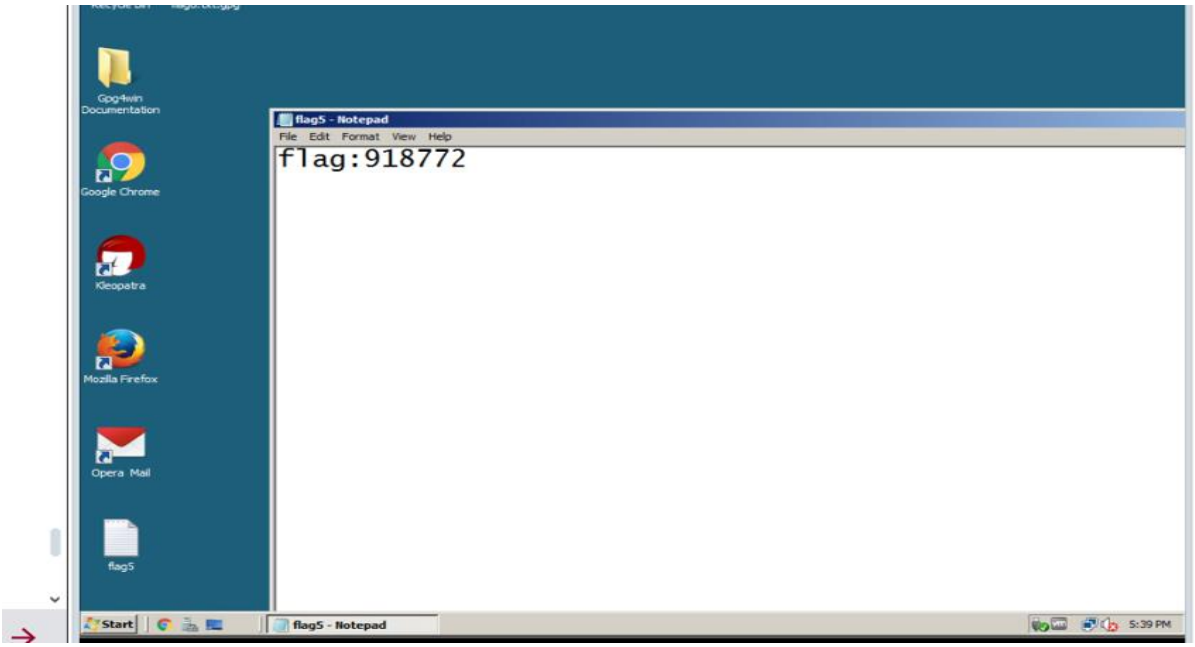


Step 45: Log in to the virtual machine and enter the details.

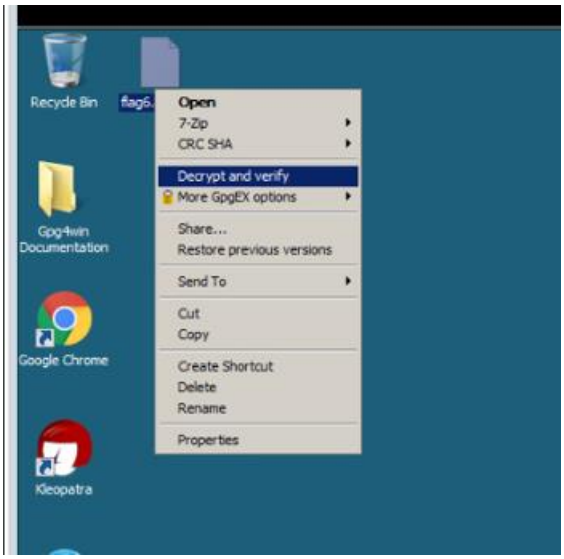
Username: student3

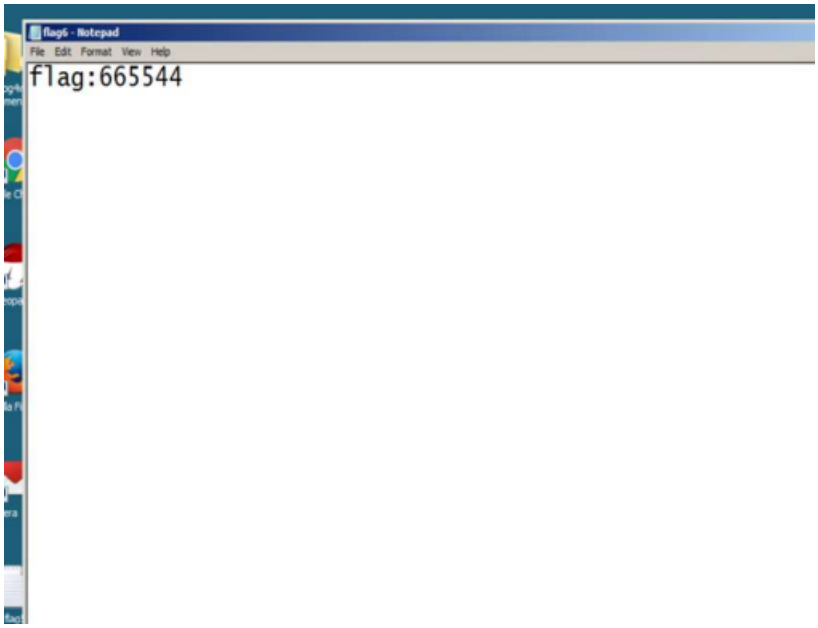
Password: P@ssw0rd

Step 46: Open the flag5 file. Solve the challenge 4.



Step 47: Open flag6.txt.gpg file. Decrypt the file. Solve the challenge.




flag6 - Notepad
File Edit Format View Help
flag:665544

Conclusion & Wrap-Up

Summary with observations, Successes & Failures, Challenges

- Generated certificates with Kleopatra that included the admin's and the student's private keys.
- Windows computers can import exported certificates from Kleopatra.
- Using the student's public key, the administrator encrypted a message in Opera Mail.
- Using their private key, the student was able to decrypt the message.

Observations:

- It was simple to generate certificates and key pairs with Kleopatra.
- It was successful to import and export certificates between Windows and Kleopatra.
- Using public and private keys, communications in Opera Mail were successfully encrypted and decrypted.

Successes:

- Credentials for the admin and student have been created successfully.
- Using the private key, the communication was successfully encrypted, decrypted, and signed.

Risks:

- Weak passphrases on private keys might make it possible for attackers to use passphrase guessing to decode messages.
- If an unencrypted private key is stored on a disk and the disk gets lost, stolen, or compromised, there is a danger of theft.
- An attacker's man-in-the-middle attack could be made possible by improper certificate validation.
- Potential attacks could be made easier by bogus certificates issued by compromised certificate authorities.
- Brute force techniques could be used by attackers to take advantage of encryption algorithms that are out-of-date or key breaches.

Remediations:

- To prevent guessing attacks, make sure your private key passphrases are long and complex.
- Keep private keys encrypted on disk and keep encryption keys safe. If at all possible, think about encrypting the entire disk.
- Before putting your reliance on certificates, make sure you thoroughly verify certificate chains and check certificate revocation listings.
- Select trustworthy certificate authorities and keep a close eye on their security procedures.

- AES 256, ECC, and RSA 2048+ bit are examples of contemporary encryption algorithms that should be adopted while gradually phasing out older encryption approaches.