Using Public Key Encryption to Secure Messages

OBJECTIVE:

CompTIA Security+ Domain
Domain 6.0: Cryptography and PKI

CompTIA Security+ Objective Mapping
Objective 6.4: Public Key Cryptography

CEH Exam Domains:
Domain 1: Background
Domain 3: Security
Domain 4: Tools/Systems/Programs
Domain 5: Procedures/Methodologies

CEH Objective Mapping:
Objective 1.3 Information Security Technologies
Objective 3.3: Information Security Attack Prevention
Objective 4.3: Information Security Tools
Objective 5.1 Information Security Procedures

OVERVIEW:

In this lab, you will use encryption to protect data and sensitive information. Data protection is imperative for companies and organizations. Encryption is used as a part of layered security architecture in an organization's networks.

OUTCOMES:

In this lab, you will learn to:

1. Use PKI to generate a certificate for a student and administrator.
2. Use PKI to encrypt and decrypt a file.

Key Term	Description
Social Engineering Toolkit	Tools that can be used by an attacker to exploit victims.
Kleopatra	A certificate manager and a universal crypto graphical user interface (GUI). Kleopatra supports management of X.509 and OpenPGP certificates in the GpgSM and GPG keyboxes and for retrieving certificates from LDAP and other certificate servers.
Certificate	An electronic document used to authenticate ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate.

Key Term	Description
Opera	A free browser and e-mail client.
Public key encryption	A cryptographic system that uses two keys—a public key known to everyone and a private key known only to the recipient of the message. These keys are related in that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.

Reading Assignment

Introduction

In this lab, you will use encryption to protect data and sensitive information. Data protection is imperative for companies and organizations. Encryption is used as a part of layered security architecture in organization's networks. Figure 1 shows the lab topology with a Windows client and Windows Server machine.

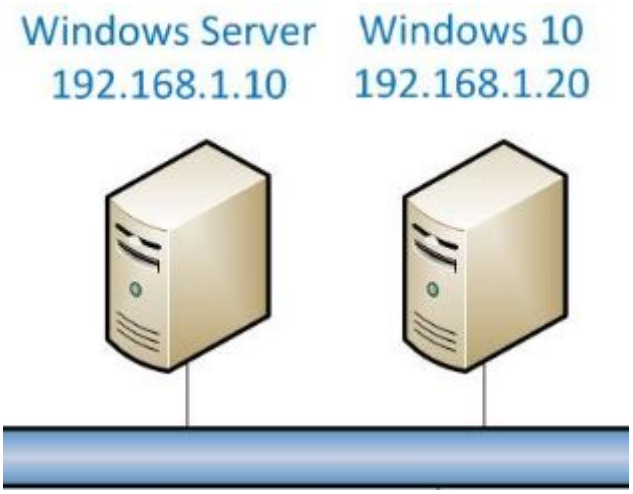


FIGURE 1 – LAB TOPOLOGY

You will generate a student and administrator certificate on the Windows client, export it, and import it into Windows for use to encrypt/decrypt a message that you will send using Opera mail. The Opera e-mail client is free software. Opera also makes a free multiplatform browser.

Introduction to Public Key Encryption

Recall, from earlier reading assignments, we investigated the CIA (confidentiality, integrity, and availability) triad. Encryption is a technique to secure data and communication channels from hackers. Encryption is the process of encoding messages to protect the message from being seen by hackers. There are synchronous encryption algorithms that use a shared key in communication and also asymmetric keys that use a public/private key which is called public key cryptography. There are two uses of public key cryptography—public key encryption and digital signatures which satisfies two of the three goals of CIA: confidentiality and integrity.

Public key encryption uses an asymmetric encryption algorithm that requires two keys—a public key that is distributed to others and a private key which must be kept secret and will not be shared. There is a public key infrastructure (PKI) that is in place to allow people to get these keys from trustworthy organizations known as a certificate authority. There are a few trustworthy vendors that you can use to get certificates from. Digital signatures are used to sign electronic messages, so you know who the message comes from.

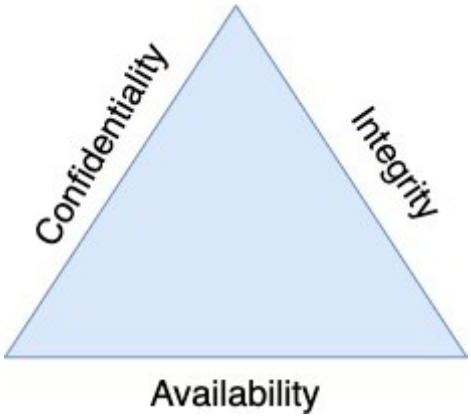


FIGURE 2 – CIA TRIAD

Certificates – Kleopatra

In this lab, you will use Kleopatra to generate your public and private keys and as the certificate authority. Figure 3 shows the process of key generation that a certificate authority uses. Figure 4 shows the user interface of Kleopatra. Kleopatra is a certificate management graphical user interface (GUI) tool for GnuPG. GnuPG is an OpenPGP clone. OpenPGP is an open e-mail encryption standard. Pretty Good Privacy (PGP) is an encryption system that is used to secure messages. You will use GnuPG to send encrypted messages using a public/private key.

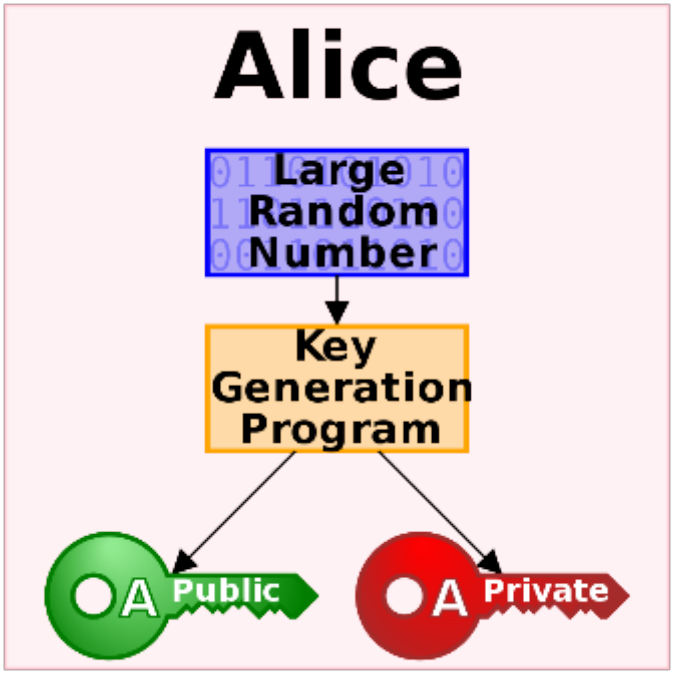


FIGURE 3 – CERTIFICATE GENERATION (SOURCE: **WIKIPEDIA**)

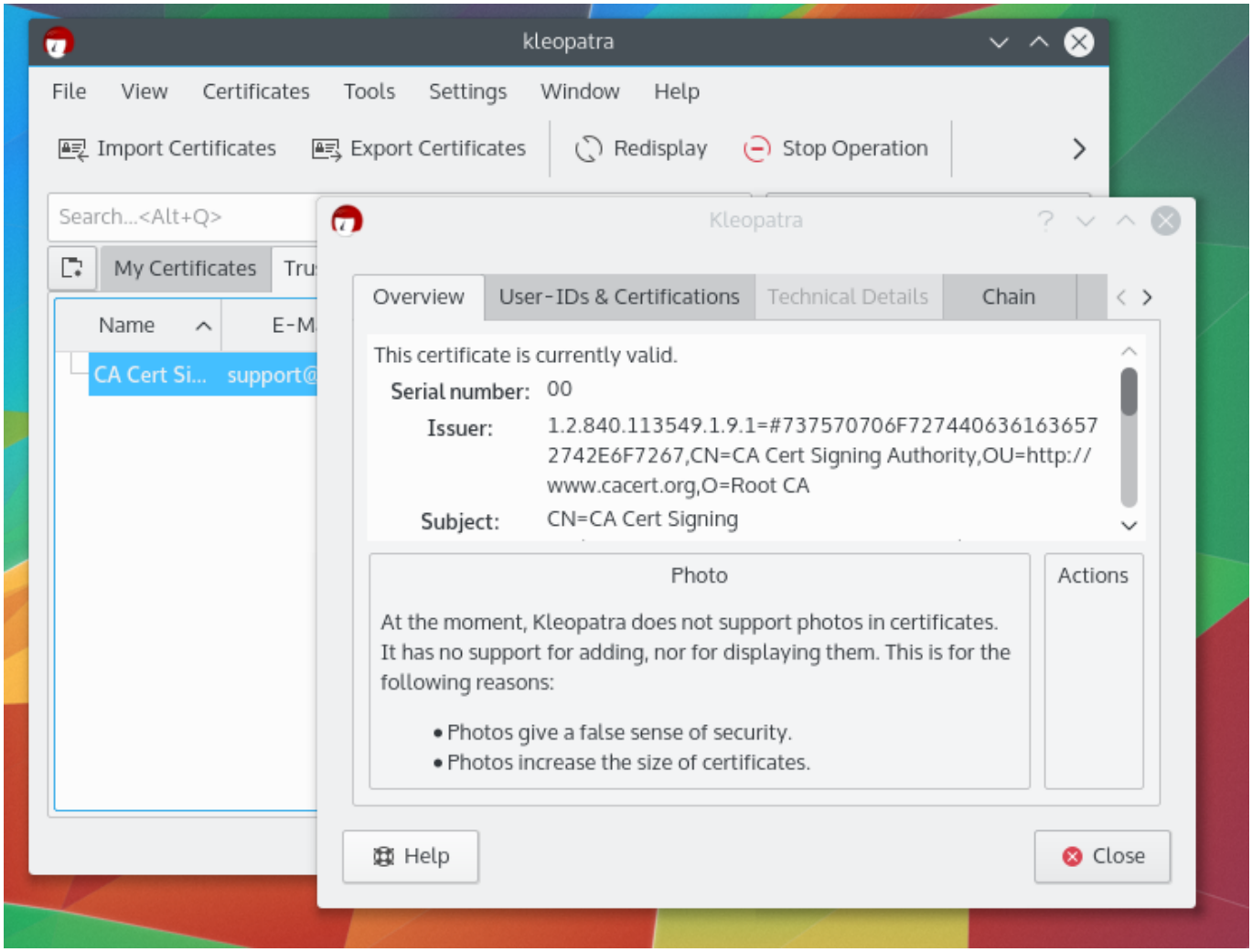


FIGURE 4 – KLEOPATRA INTERFACE (SOURCE: BING)

Public Key Encryption

One of the applications of the public key encryption infrastructure is to encrypt messages sent between people. Securing communication is used to provide confidentiality. An e-mail message that a sender (Bob) encrypts using the recipient's (Alice) public key can be decrypted only by the recipient's (Alice) paired private key as shown in Figure 5. In this lab, you will send an encrypted message and decrypt that message as a separate user once the message is received.

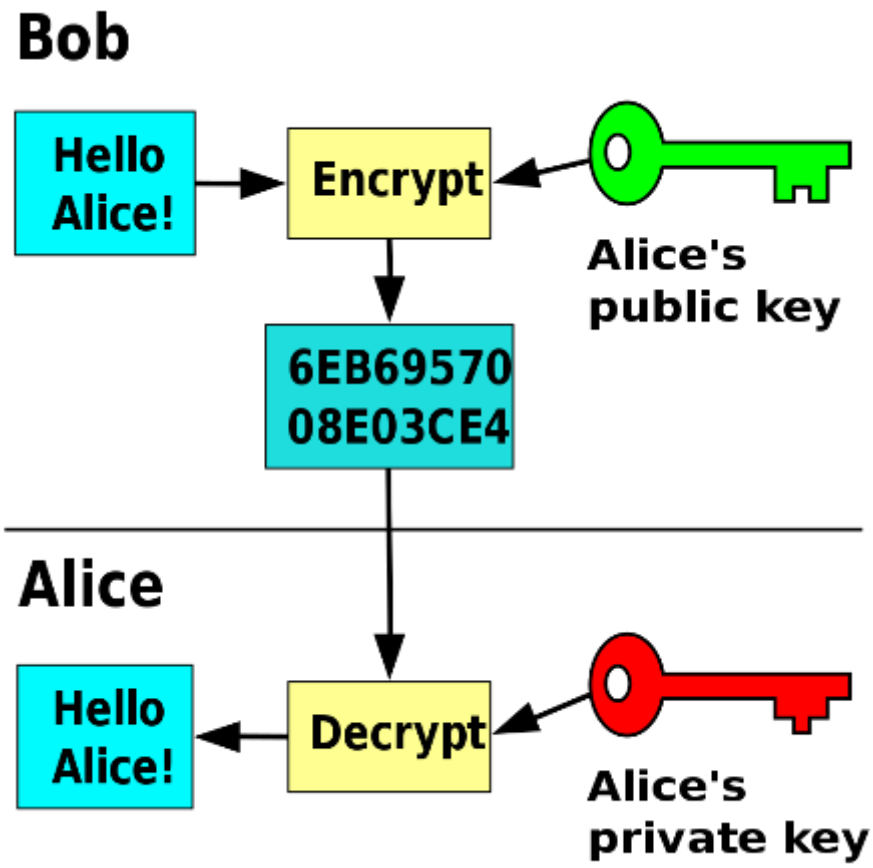


FIGURE 5 – SENDING AND RECEIVING AN ENCRYPTED MESSAGE (SOURCE: **WIKIPEDIA**)

Digital Signatures

Another application in the public key encryption infrastructure is the digital signature. Digital signatures are used to authenticate the sender. An e-mail message that a sender (Alice) sends is digitally signed with Alice's private key. Bob receives that message and verifies that Alice sent the message by using Alice's public key for verification.

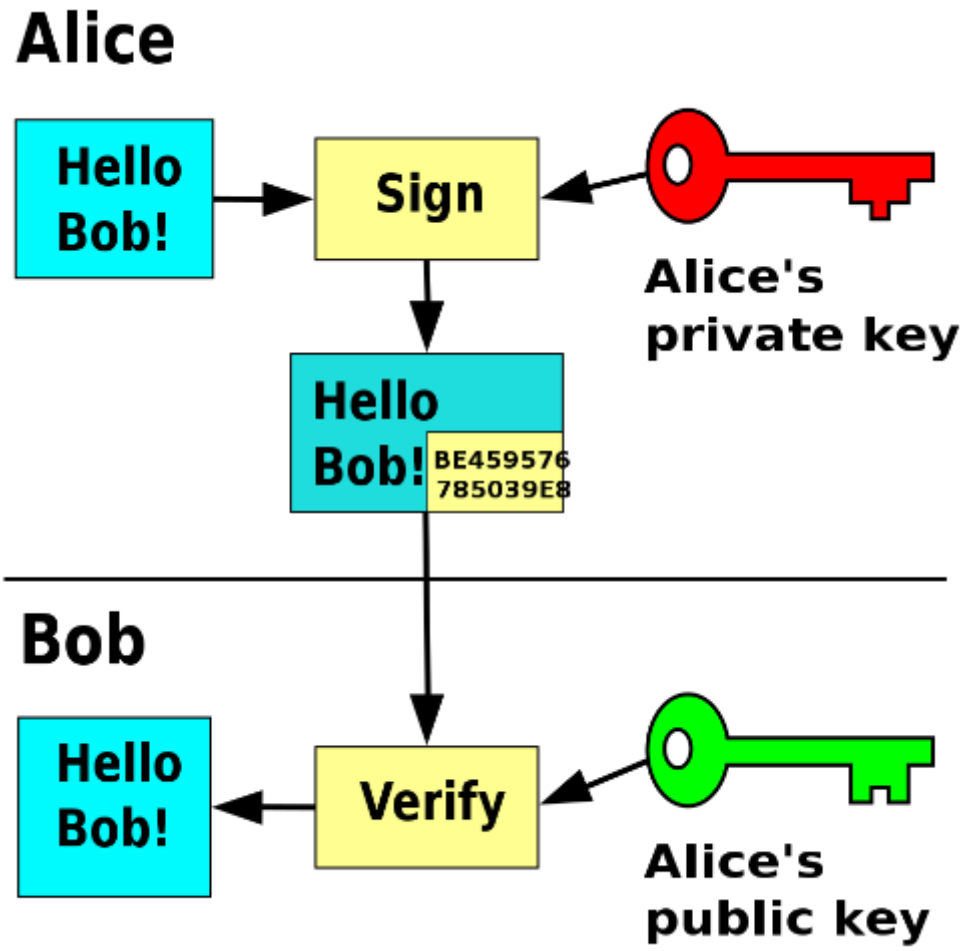


FIGURE 6 – DIGITAL SIGNATURE PROCESS (SOURCE: WIKIPEDIA)

CONCLUSION:

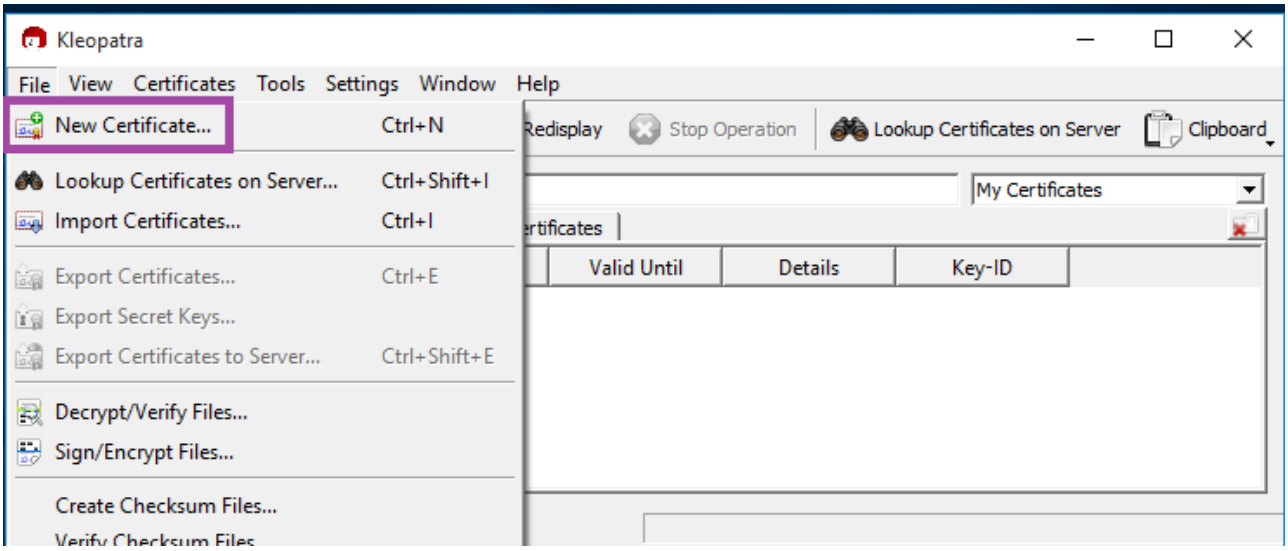
In this lab, you will use Kleopatra to create several certificates. The certificate contains the private and public key pairs for both the student and the administrator. Then, it is exported out of Opera and imported in Windows client and server to be used by Opera mail to encrypt a message with the public key of the receiver. Then, on the receiving end, the recipient's private key is used to decrypt the message using Opera mail.

Creating the Certificate for Student

1. **Click** on the internal Windows 10 icon on the topology. **Double-click** on the shortcut to Kleopatra on the desktop.

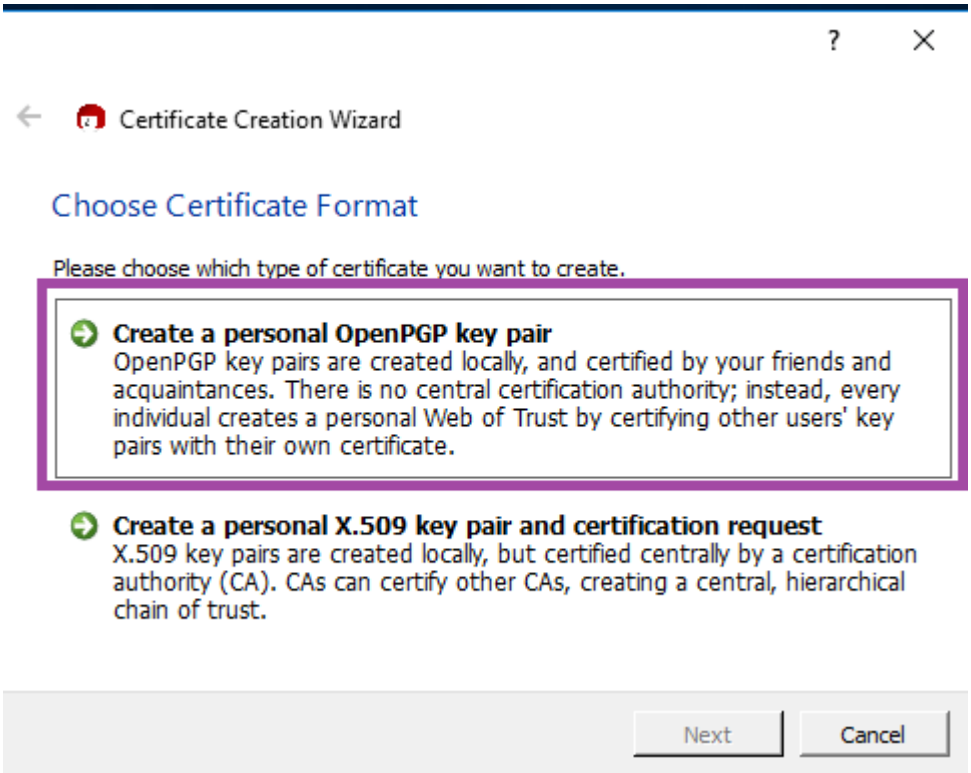
KLEOPATRA

2. From the Kleopatra menu, **select** File and **select** New Certificate.



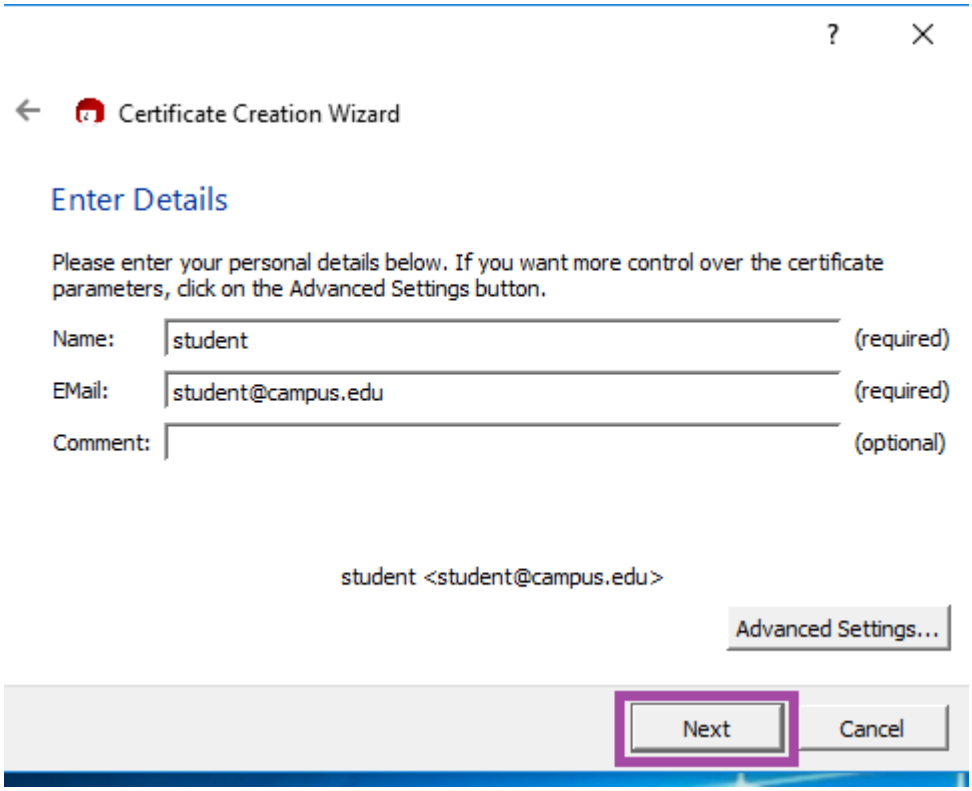
NEW CERTIFICATE

3. **Click** Create a personal OpenPGP key pair.



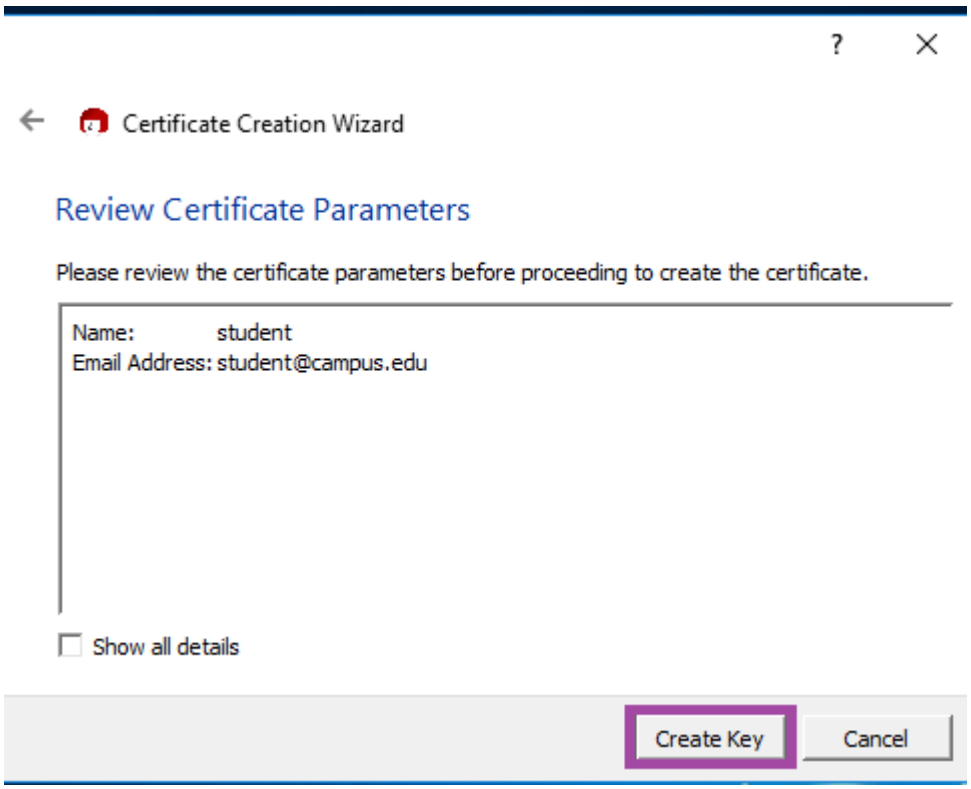
OPEN PGP KEY PAIR

4. For the Name, **type** `student`. For the EMail, **type** `student@campus.edu`. **Click** Next.



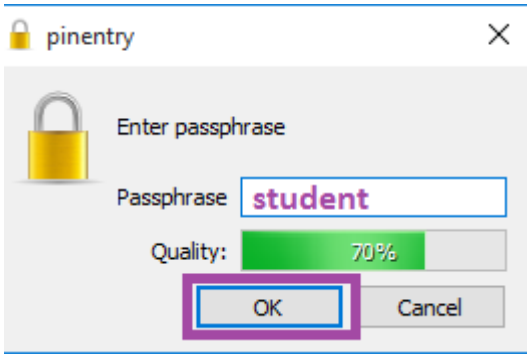
CLICK NEXT

5. At the Certificate Creation Wizard screen, **click** Create Key.



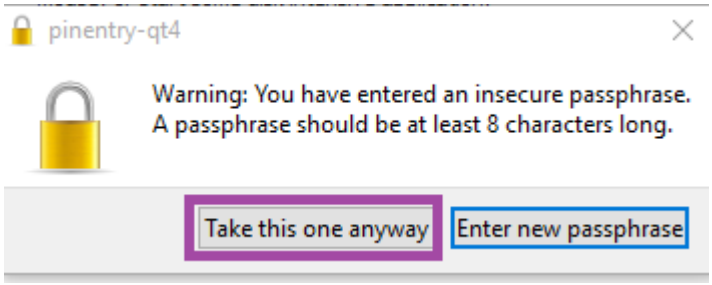
CLICK CREATE KEY

6. At the pinentry screen, **type** `student` for the Passphrase and **click** OK.



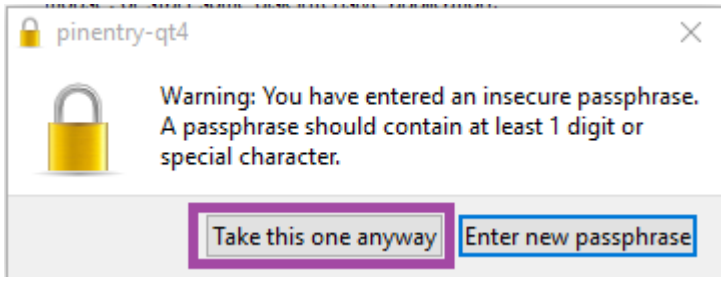
ENTER PASSPHRASE

7. At the pinentry-qt4 screen, **click** Take this one anyway.



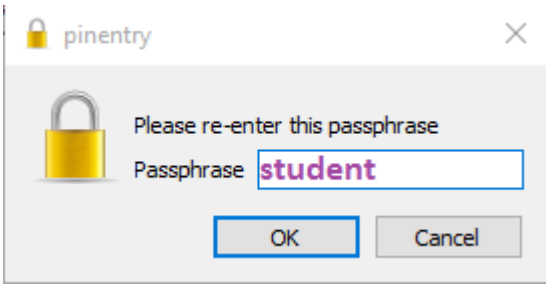
TAKE THIS ONE ANYWAY

8. At the pinentry-qt4 screen, **click** Take this one anyway.



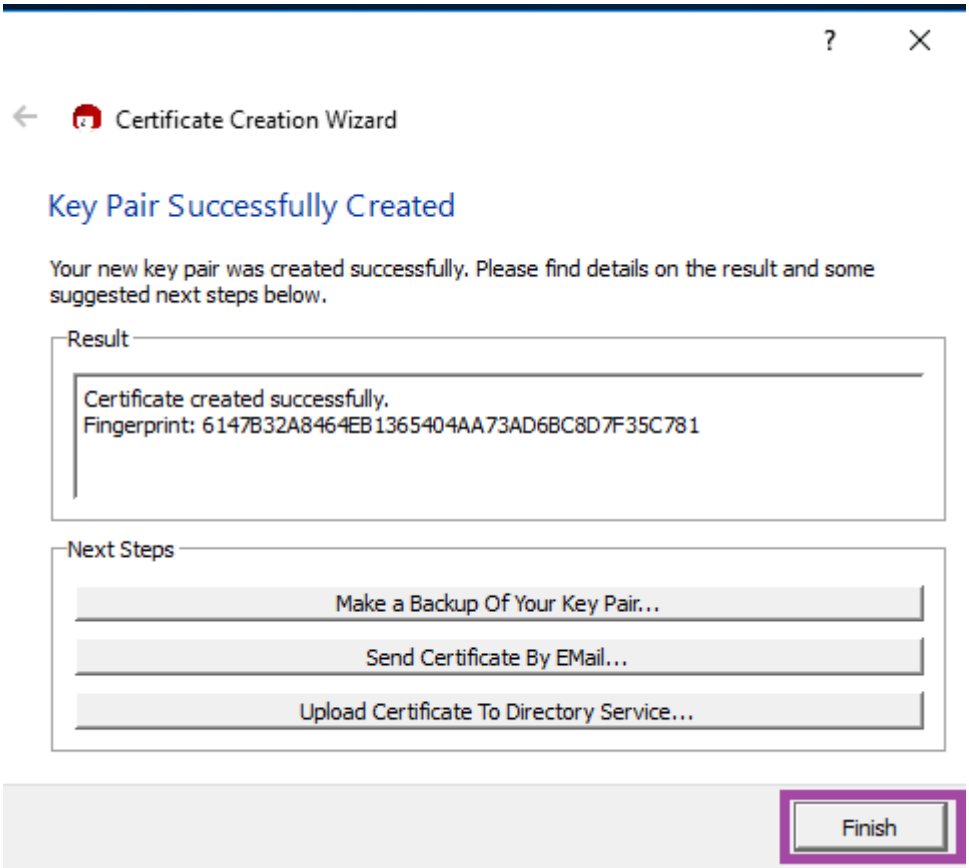
TAKE THIS ONE ANYWAY

9. At the pinentry screen, **re-enter** the Passphrase of `student`.



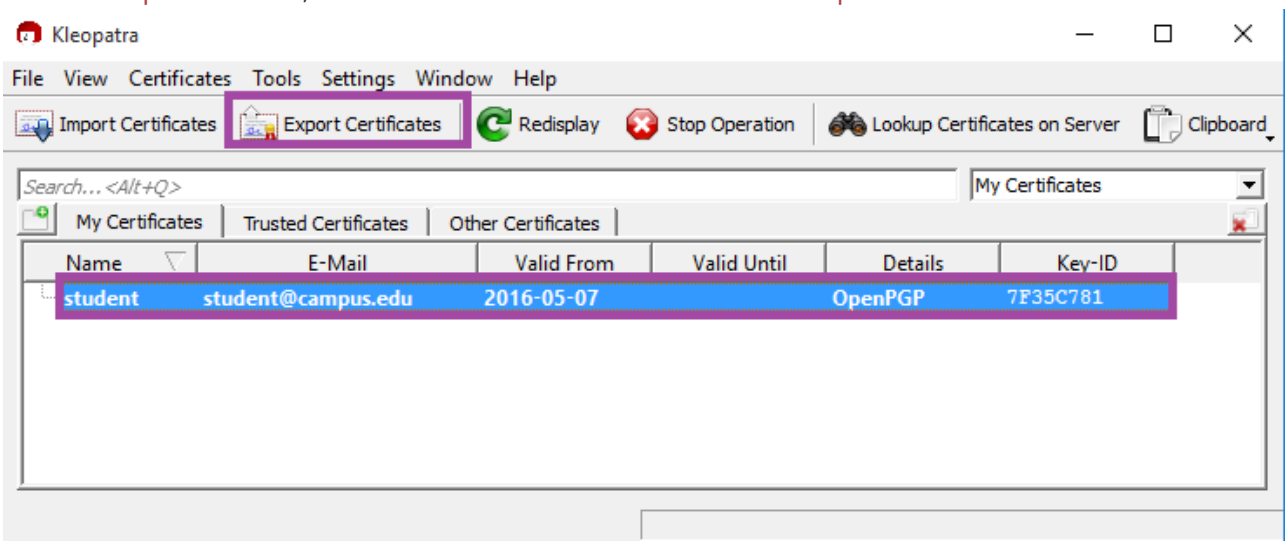
RE-ENTER PASSPHRASE

10. **Click** Finish to close the Certificate Creation Wizard.



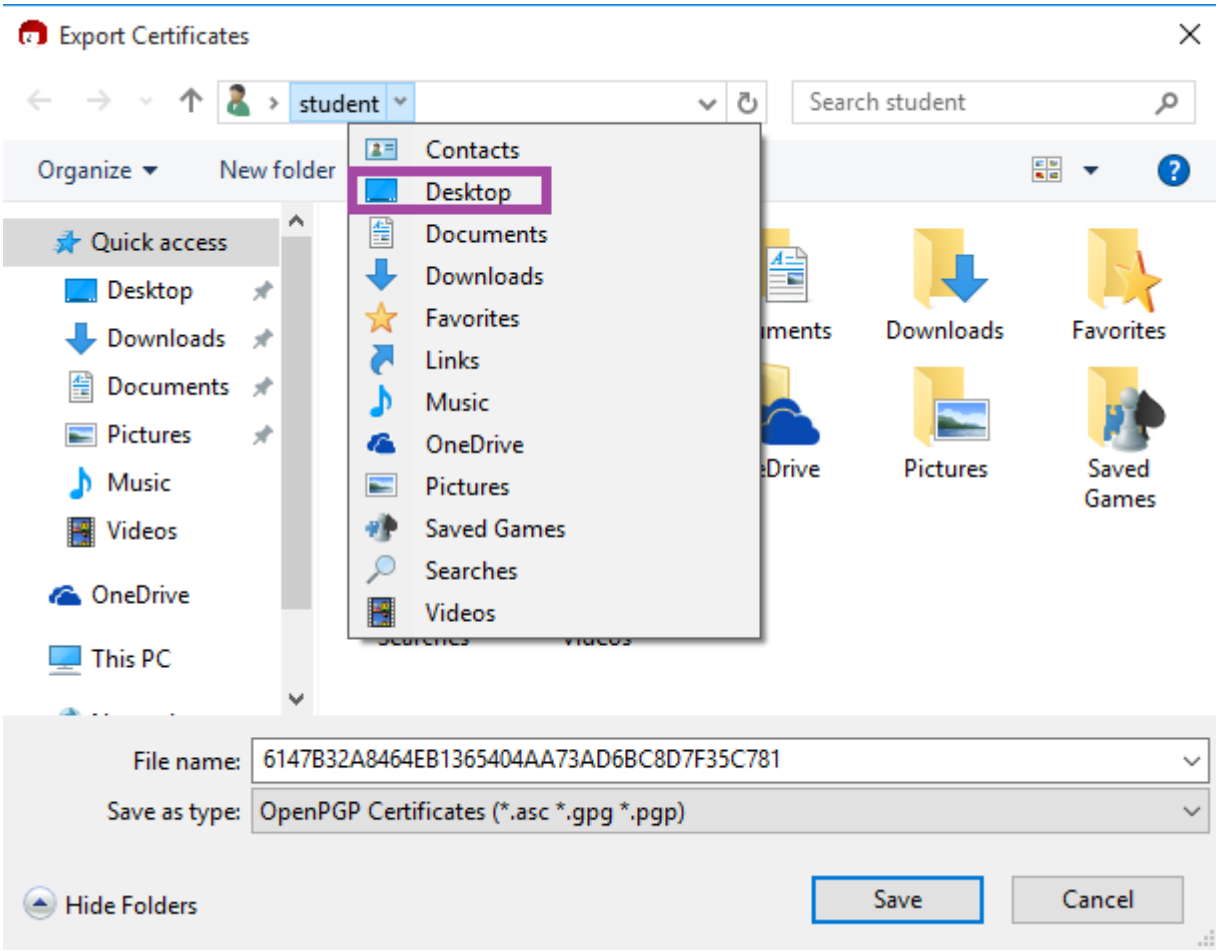
FINISH

11. At the Kleopatra screen, **click** the student certificate and **click** Export Certificates.



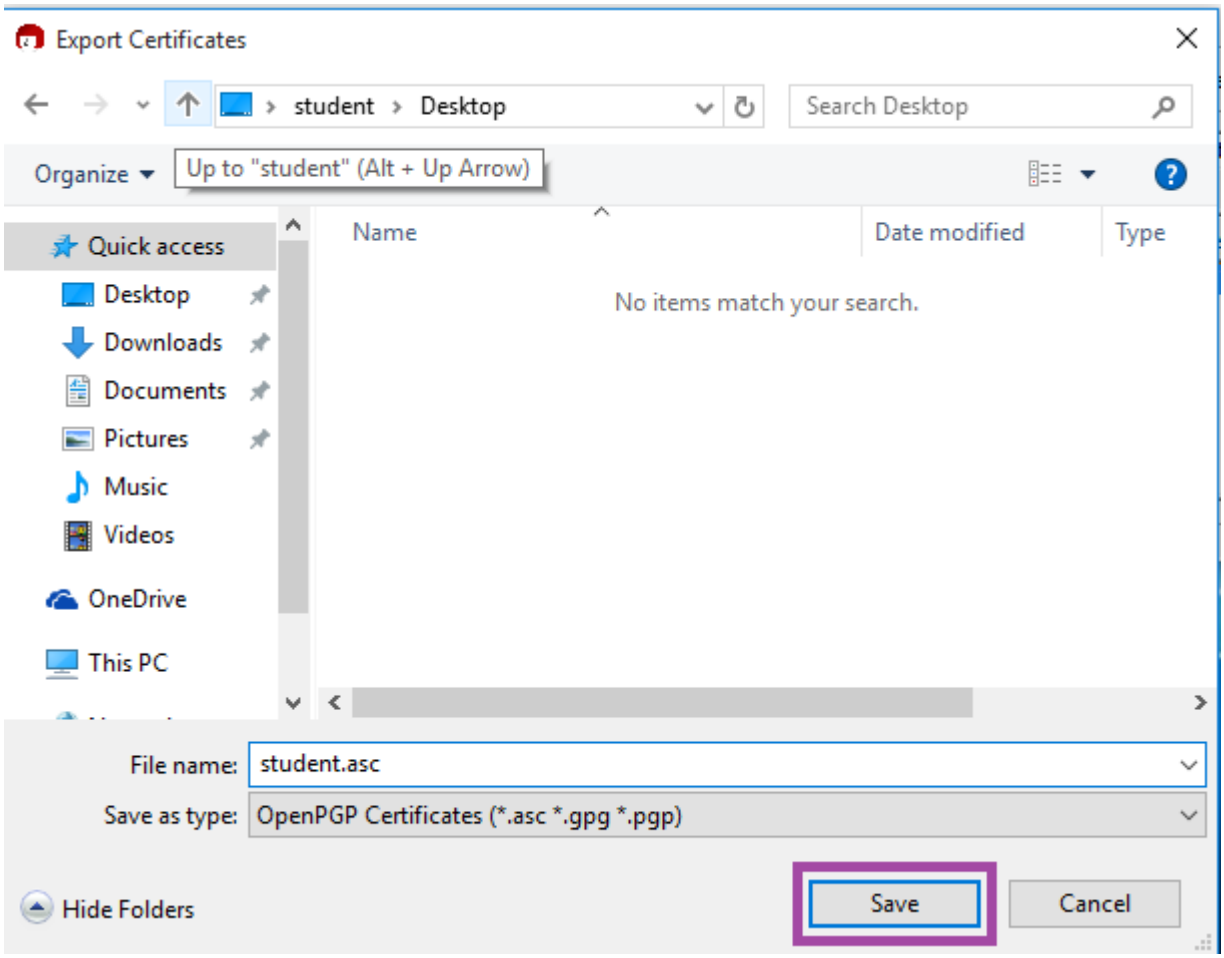
EXPORT CERTIFICATES

12. **Click** the drop-down arrow to the right of student and **select** Desktop.



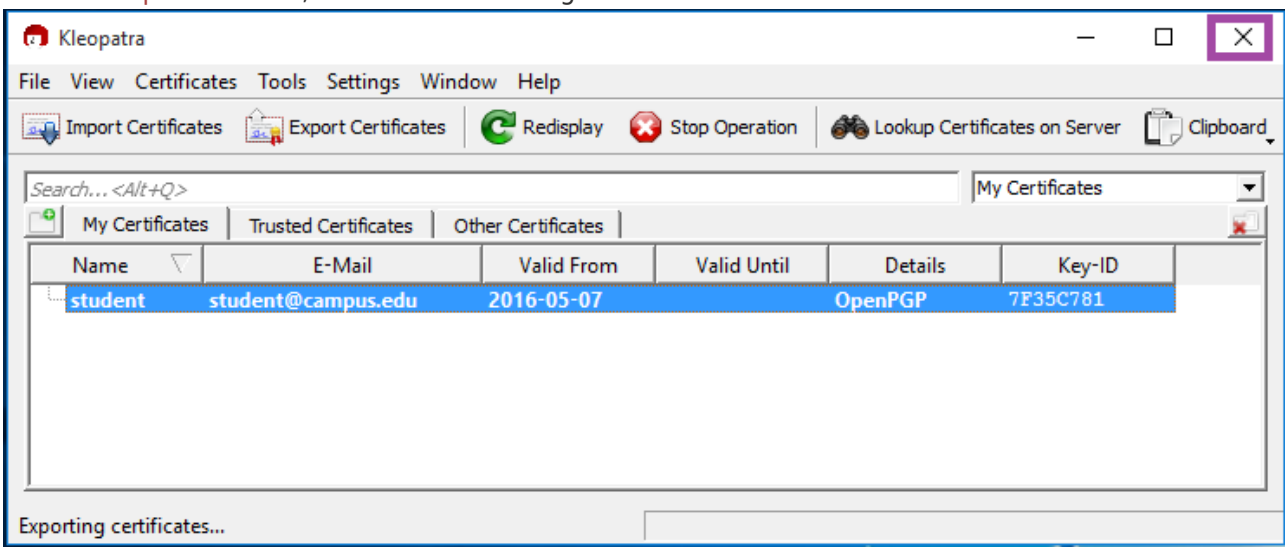
DESKTOP FOLDER

13. In the File name box, **type** `student.asc`. **Click** the Save button.



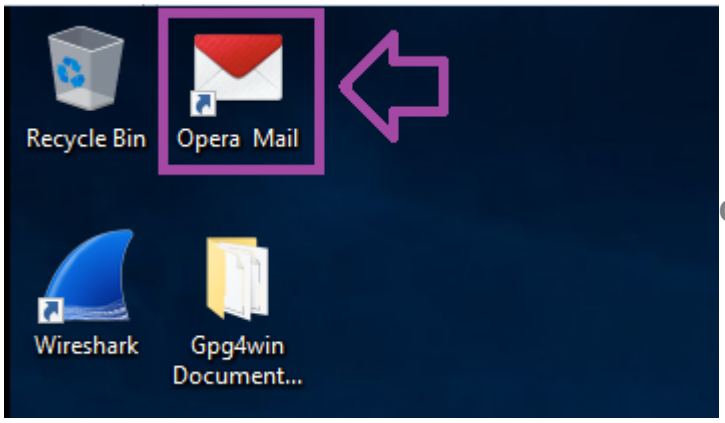
SAVE THE FILE

14. At the Kleopatra screen, **click** the x in the right hand corner to close the screen.



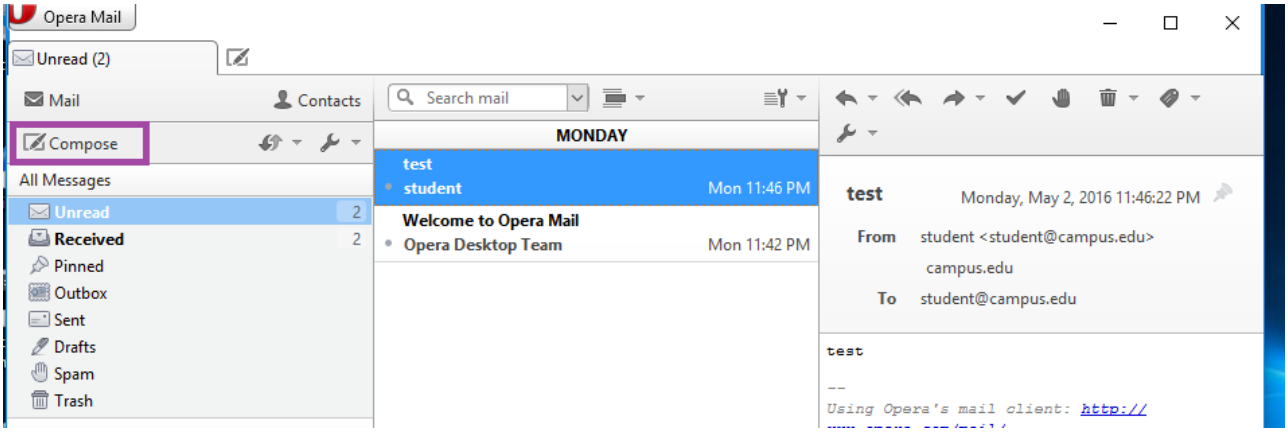
CLOSE CERTIFICATES

15. **Double-click** on the shortcut to Opera Mail on the desktop.



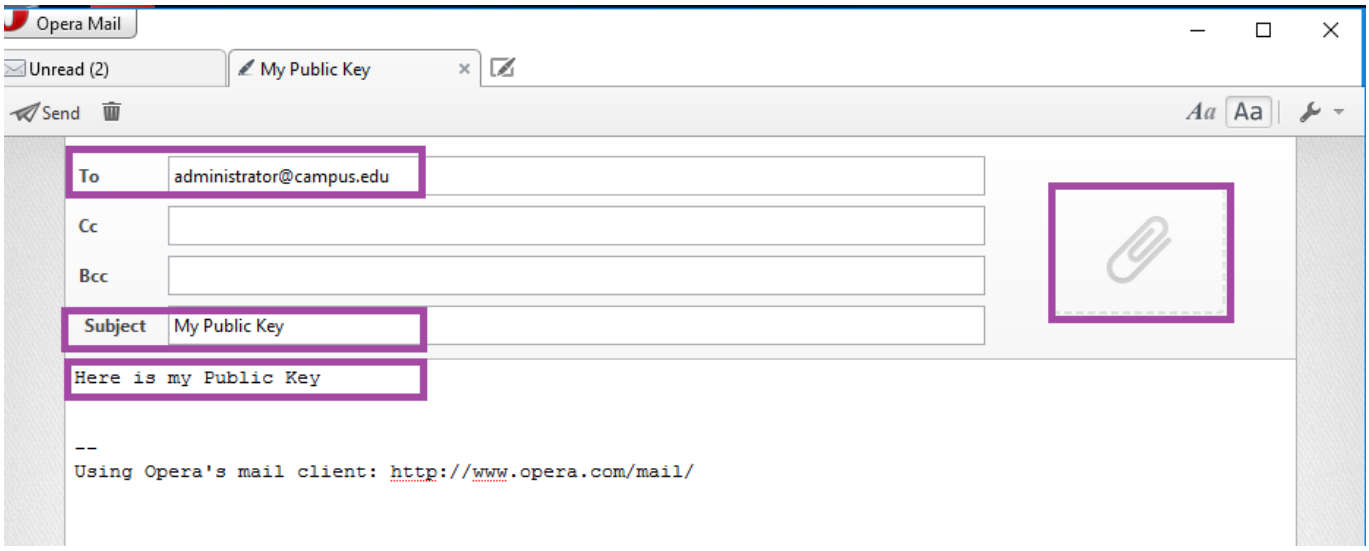
OPERA MAIL

16. **Click** the Compose button, which is located on the left side of Opera Mail.



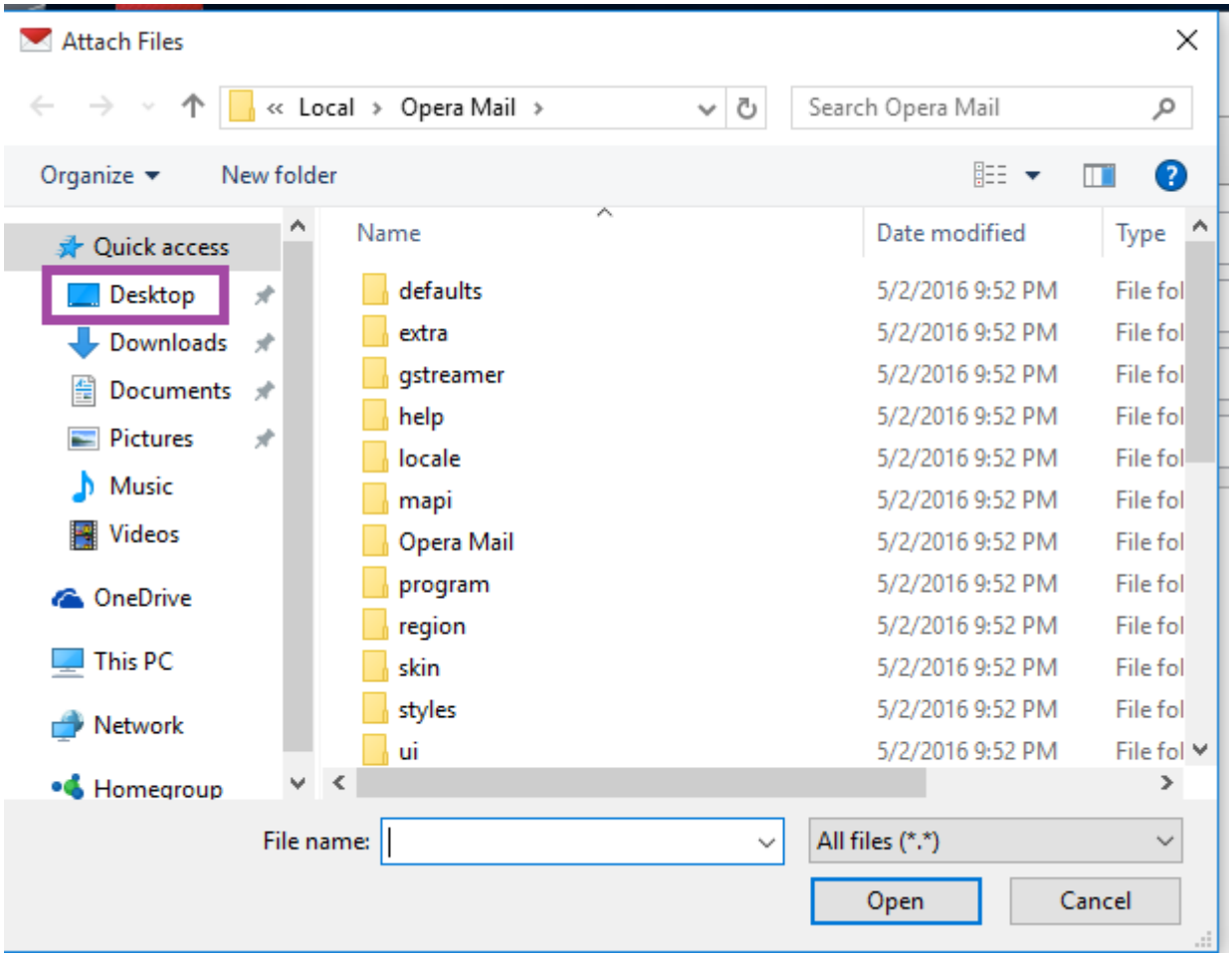
COMPOSE EMAIL

17. In the To box, **type** `administrator@campus.edu`. In the Subject box, **type** `My Public Key`. In the body, **type** `Here is my Public Key`. **Click** the paper clip to attach a file.



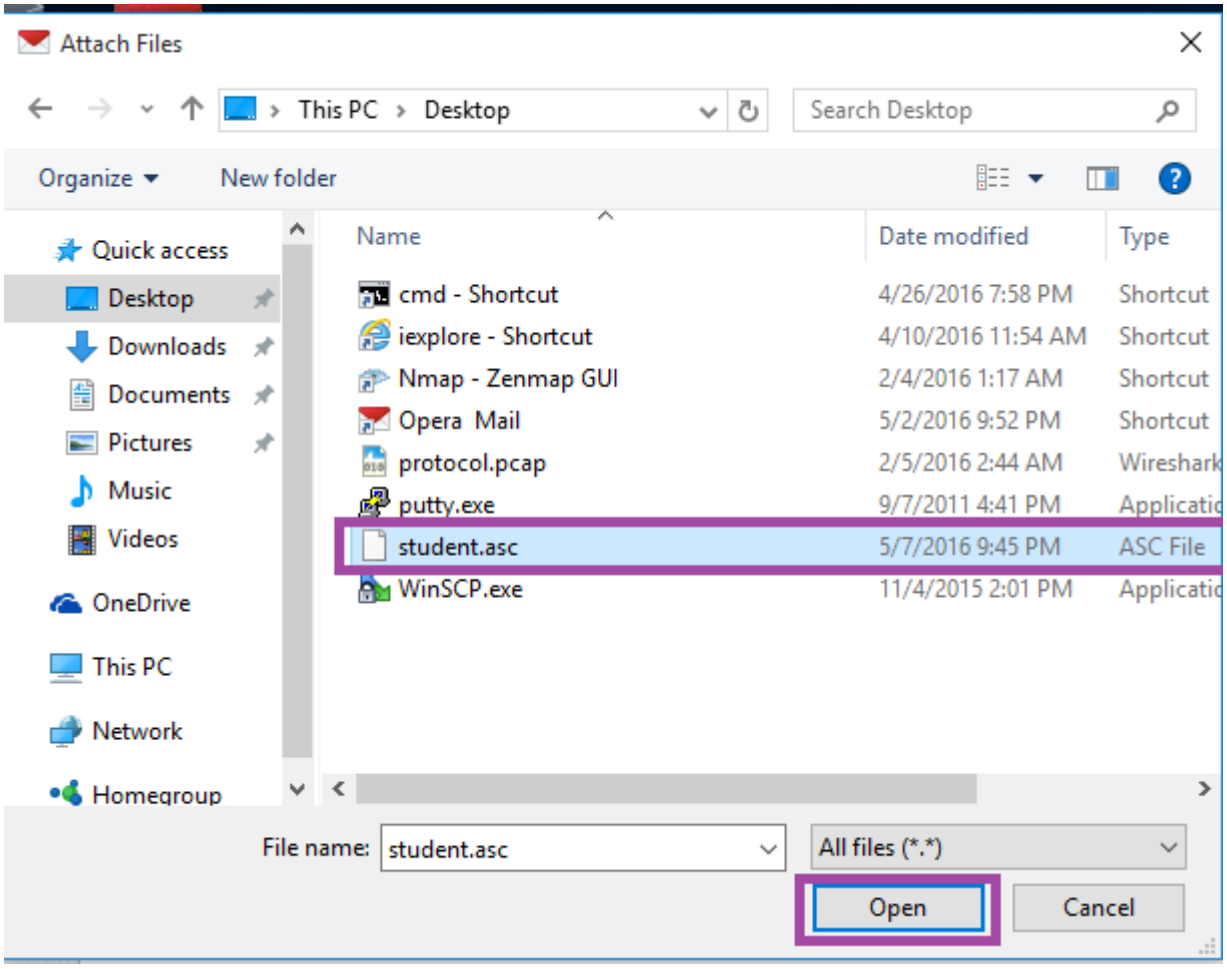
COMPOSE EMAIL

18. **Click** the link to Desktop.



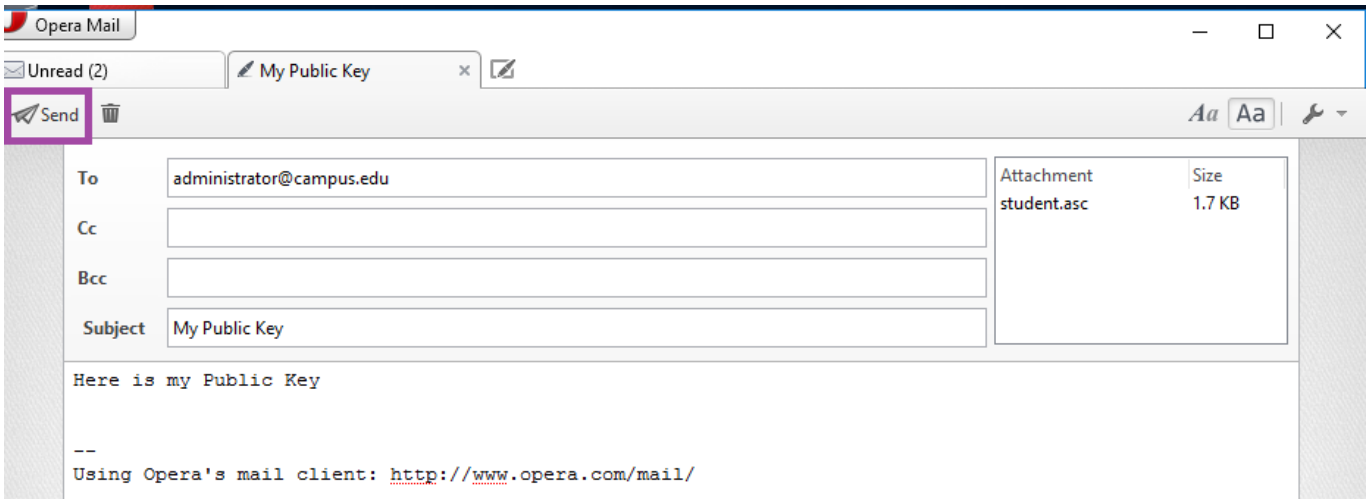
DESKTOP LINK

19. **Click** the student.asc file and then **click** the Open button.



ATTACHMENT

20. **Click** the Send button to send the email.



OPERA MAIL

21. **Click** on the Windows Server icon on the topology. After sending a control alt delete to the virtual machine, **log in** as `administrator` with the password of `P@ssw0rd`.

LOG ON TO WINDOWS SERVER

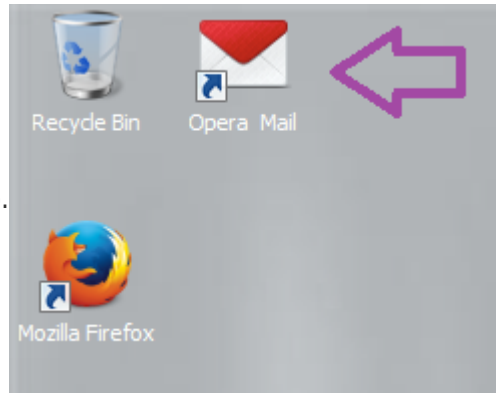
22. **Double-click** on the shortcut to Command Prompt on your desktop.

23. **Type** the following command and **press** Enter to set the clock on the VM. When asked to set the clock, **type** Y.

C:\`net time \\concord /set`

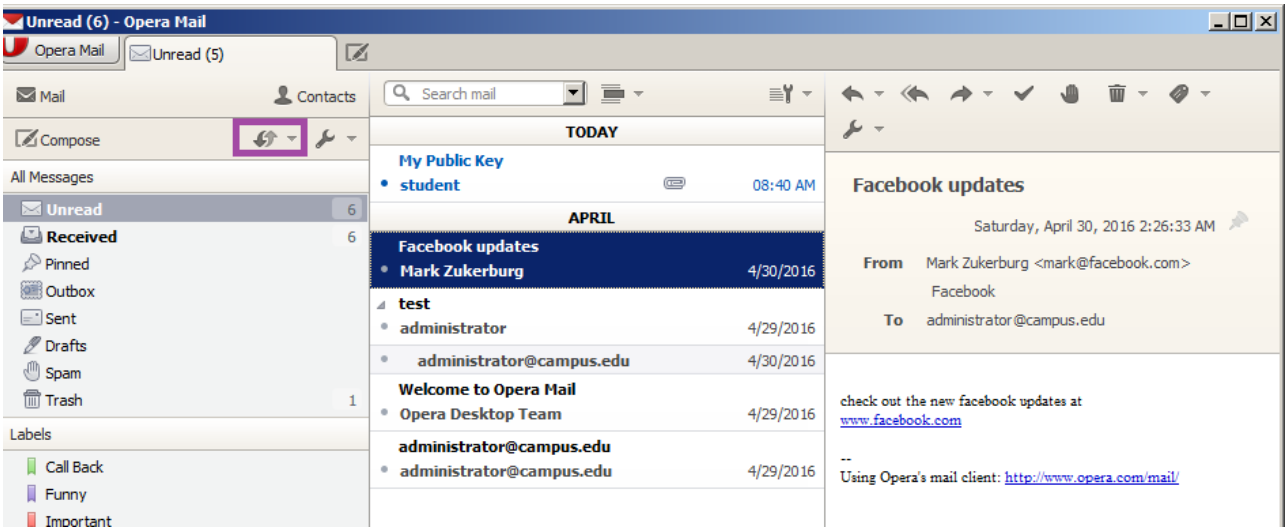
```
C:\>net time \\concord /set
Current time at \\concord is 9/15/2021 11:07:18 AM

The current local clock is 9/15/2021 3:15:05 AM
Do you want to set the local computer's time to match the
time at \\concord? (Y/N) [Y]: y
The command completed successfully.
```

22. **Double-click** on the shortcut to Opera Mail on your desktop.



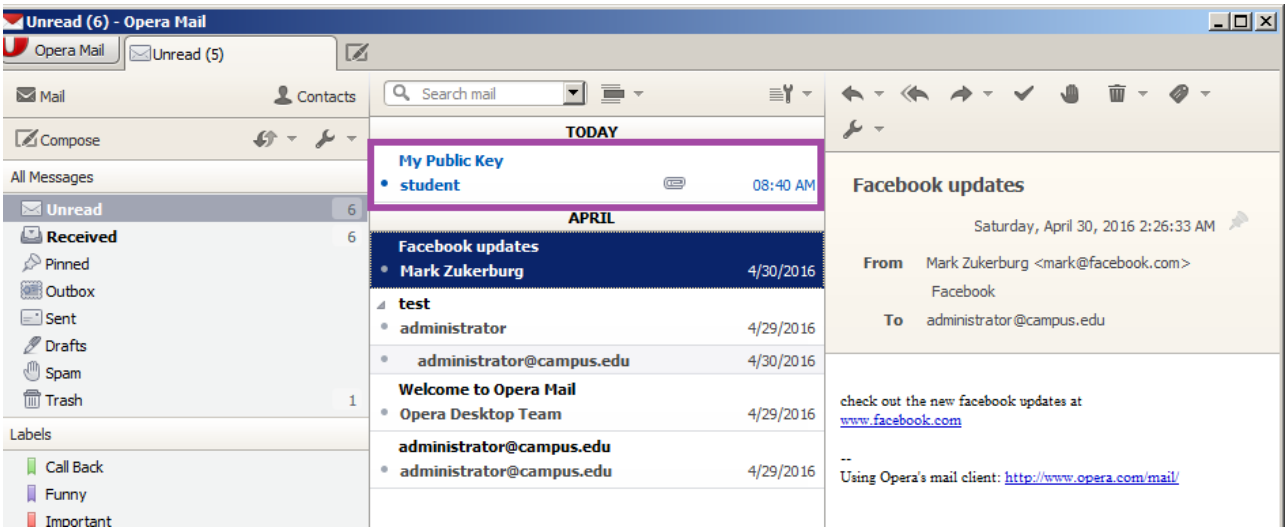
SHORTCUT TO OPERA MAIL

23. **Click** the send/receive button.



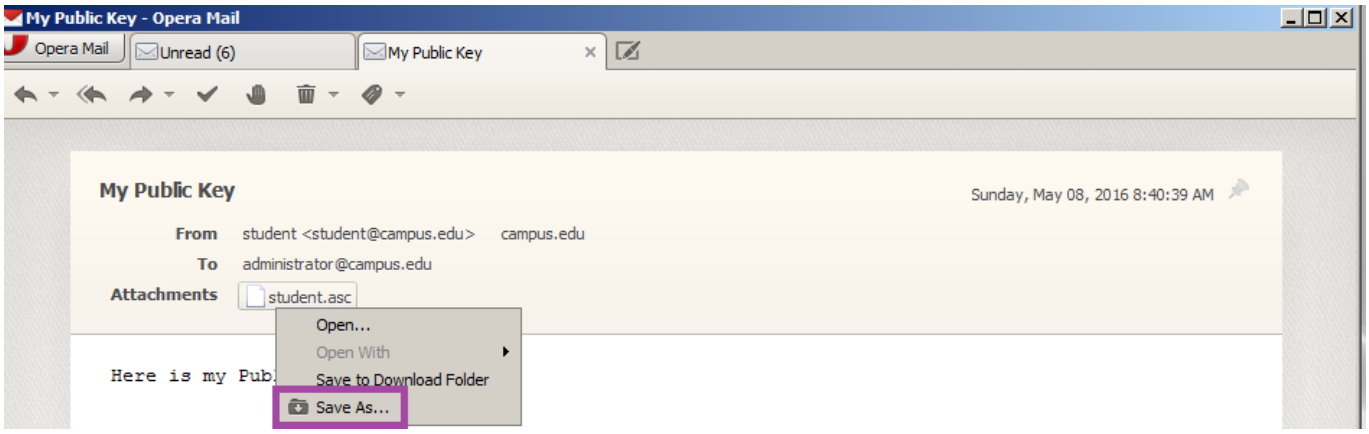
OPERA MAIL

24. **Double-click** on the email from student with the subject My Public Key.



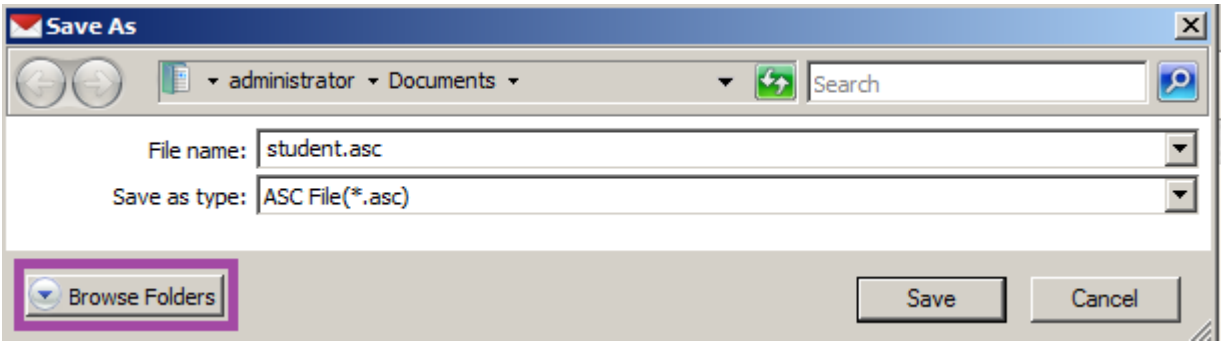
OPERA MAIL

25. **Click** the student.asc file and **select** Save As.



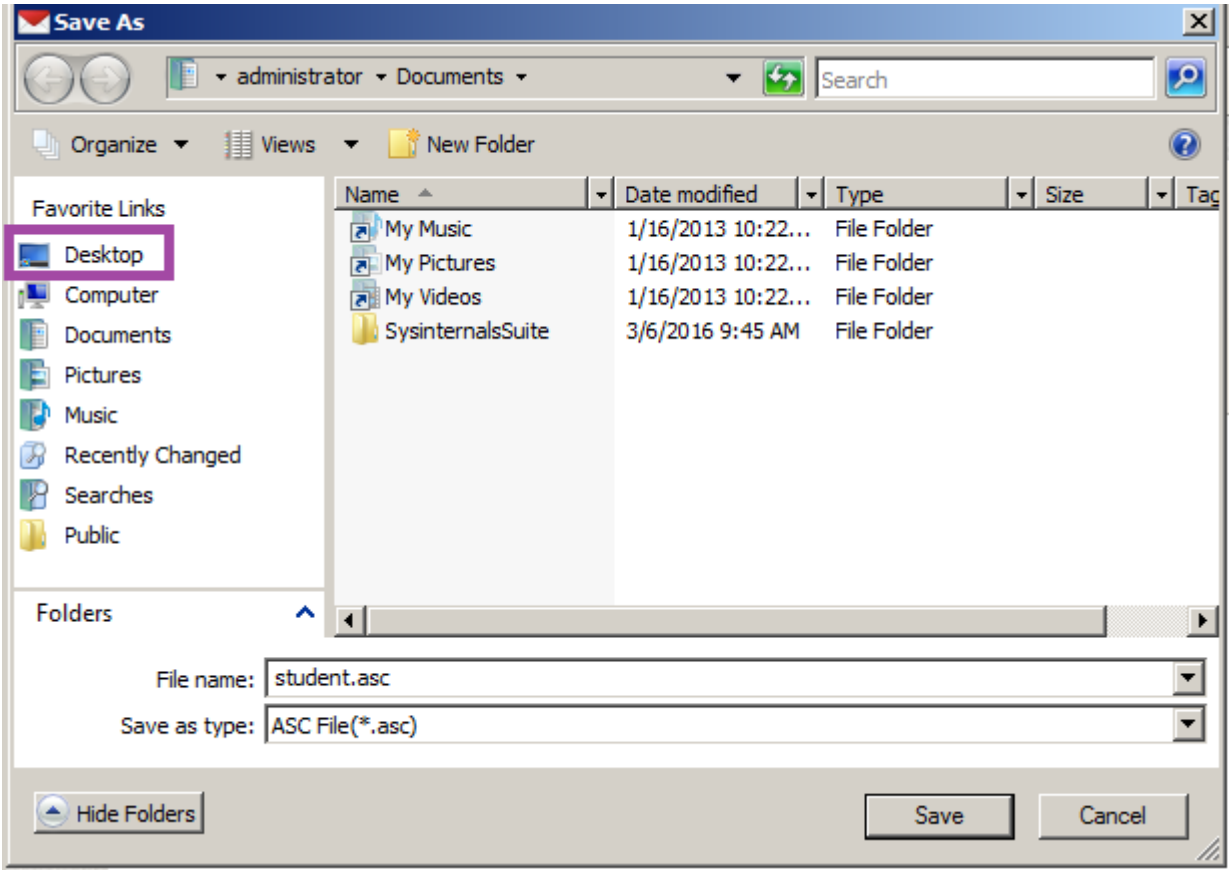
OPERA MAIL

26. **Click** Browse Folders.



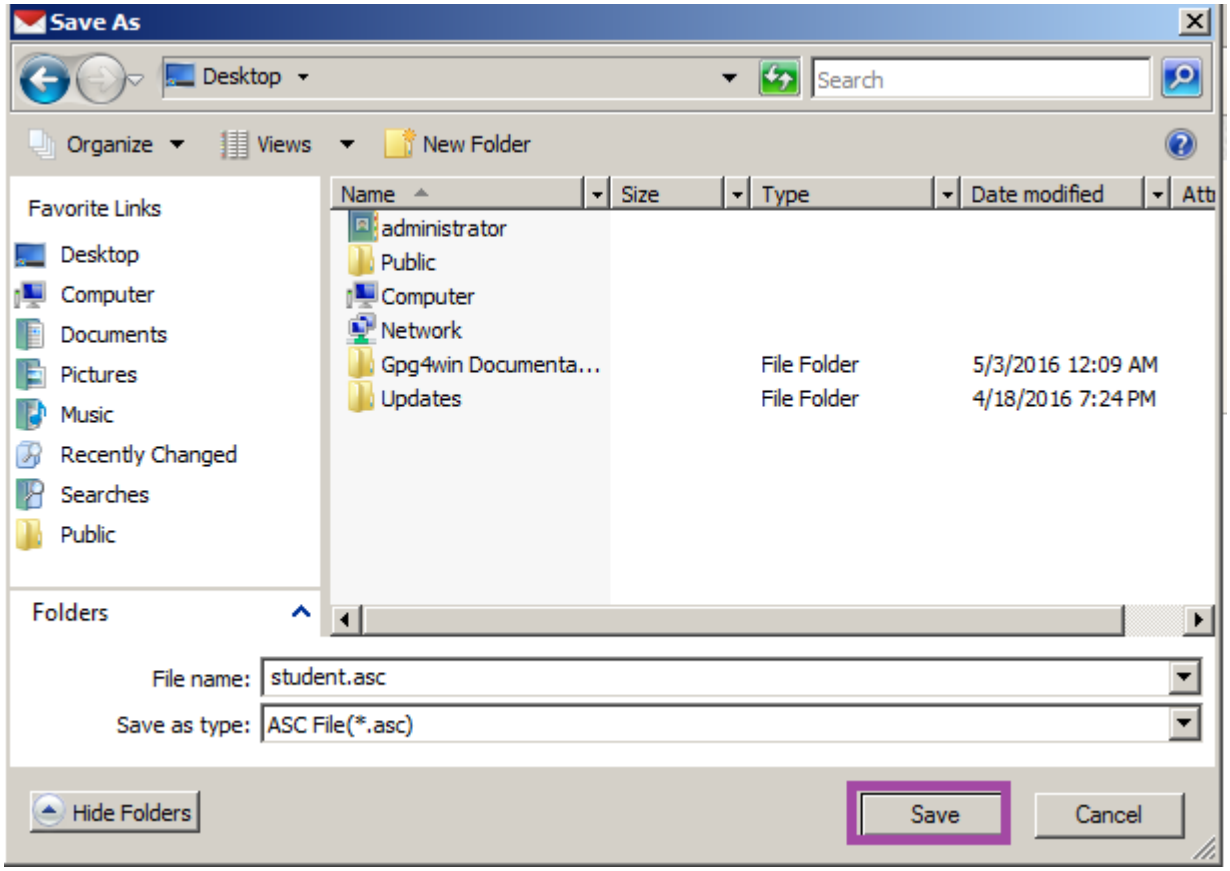
BROWSE FOLDERS

27. **Click** the link to Desktop.



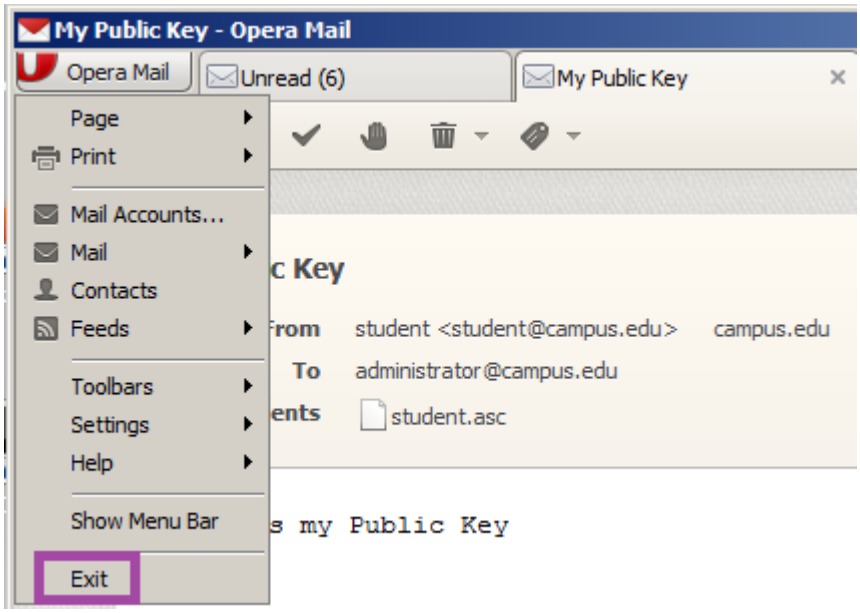
DESKTOP

28. **Click** Save.



SAVE

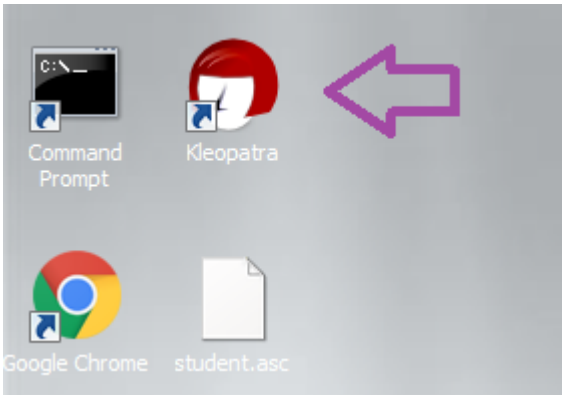
29. **Click** Opera Mail and then **select** Exit.



EXIT

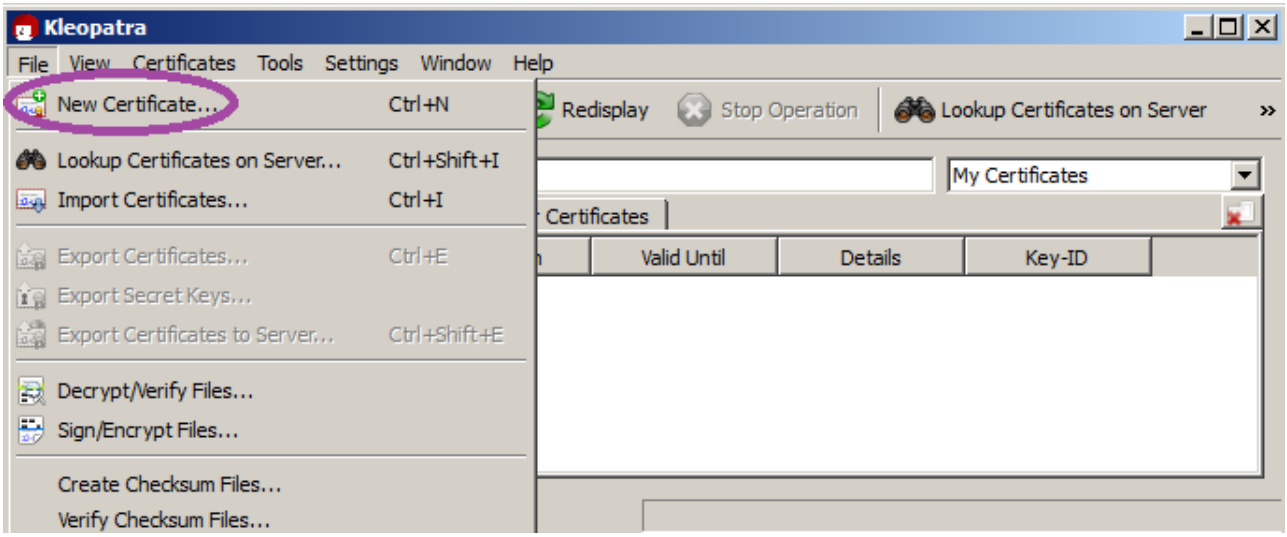
Creating the Certificate for Administrator

1. **Double-click** on the shortcut to Kleopatra on the desktop.



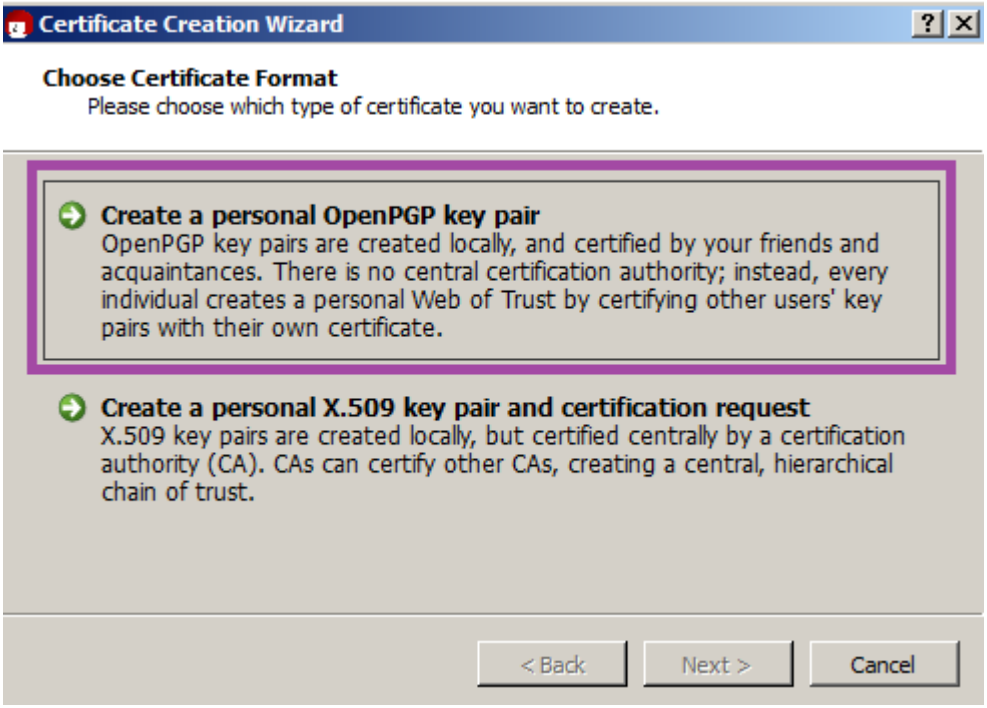
KLEOPATRA

3. From the Kleopatra menu, **select** File and **select** New Certificate.



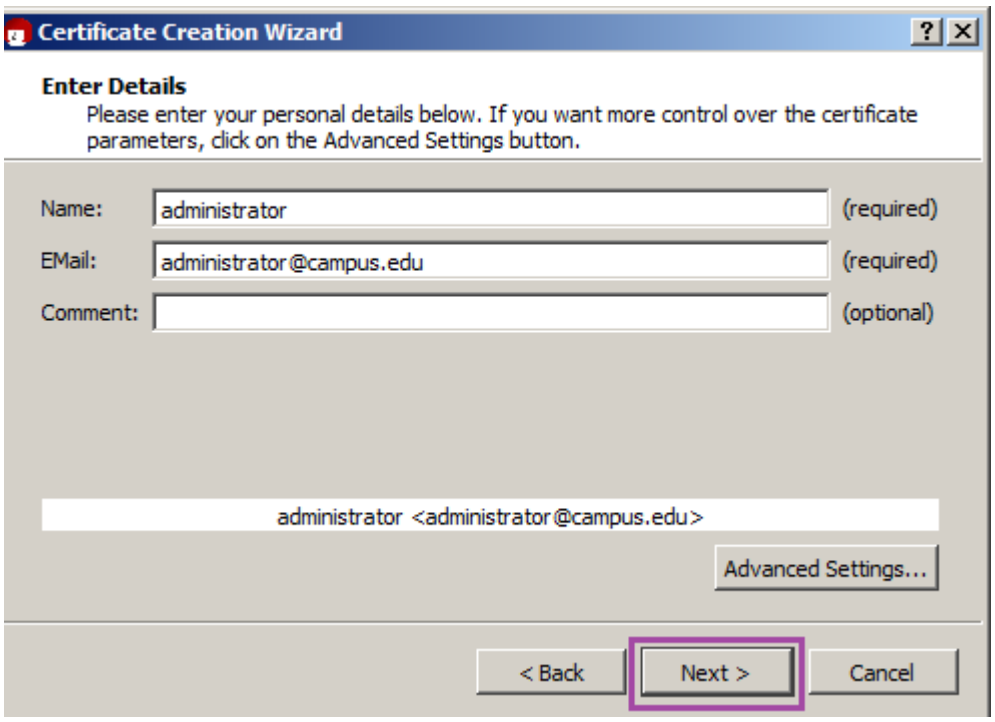
NEW CERTIFICATE

4. **Click** Create a personal OpenPGP key pair.



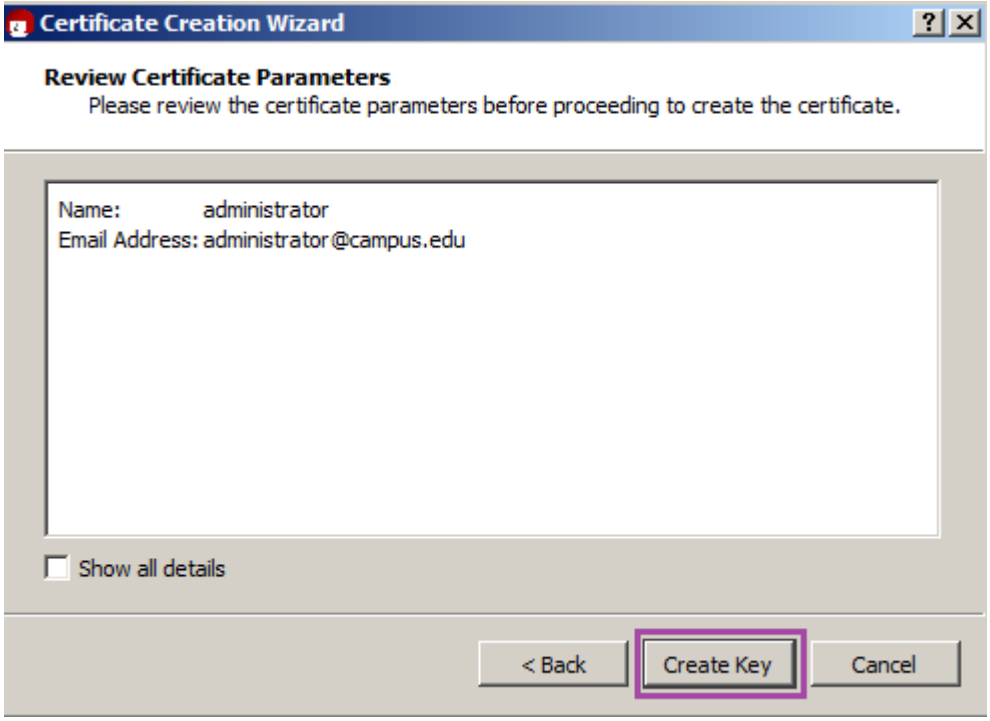
OPENPGP KEY PAIR

5. For the Name, **type** administrator. For the EMail, **type** `administrator@campus.edu`. **Click** Next.



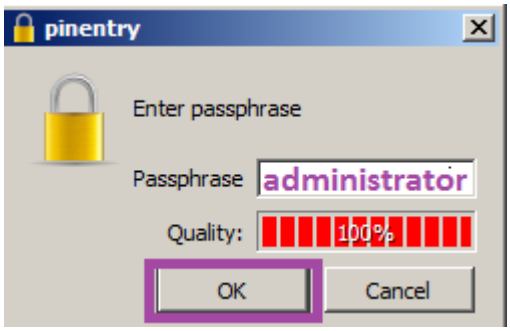
CLICK NEXT

6. At the Certificate Creation Wizard screen, **click** Create Key.



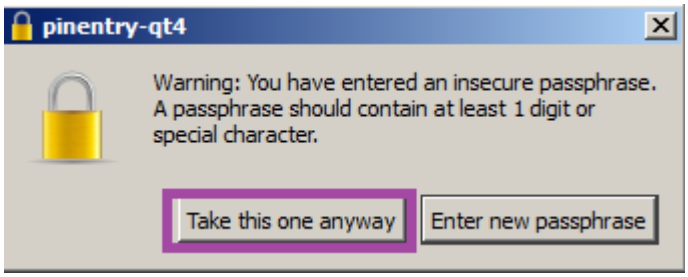
CLICK CREATE KEY

7. At the pinentry screen, **type** `administrator` for the Passphrase and **click** OK.



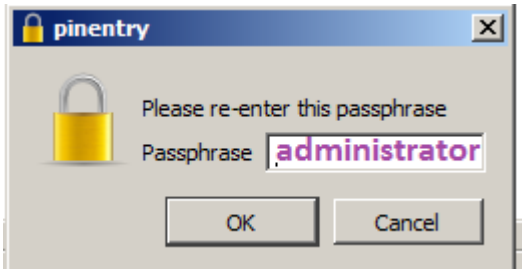
ENTER PASSPHRASE

8. At the pinentry-qt4 screen, **click** Take this one anyway.



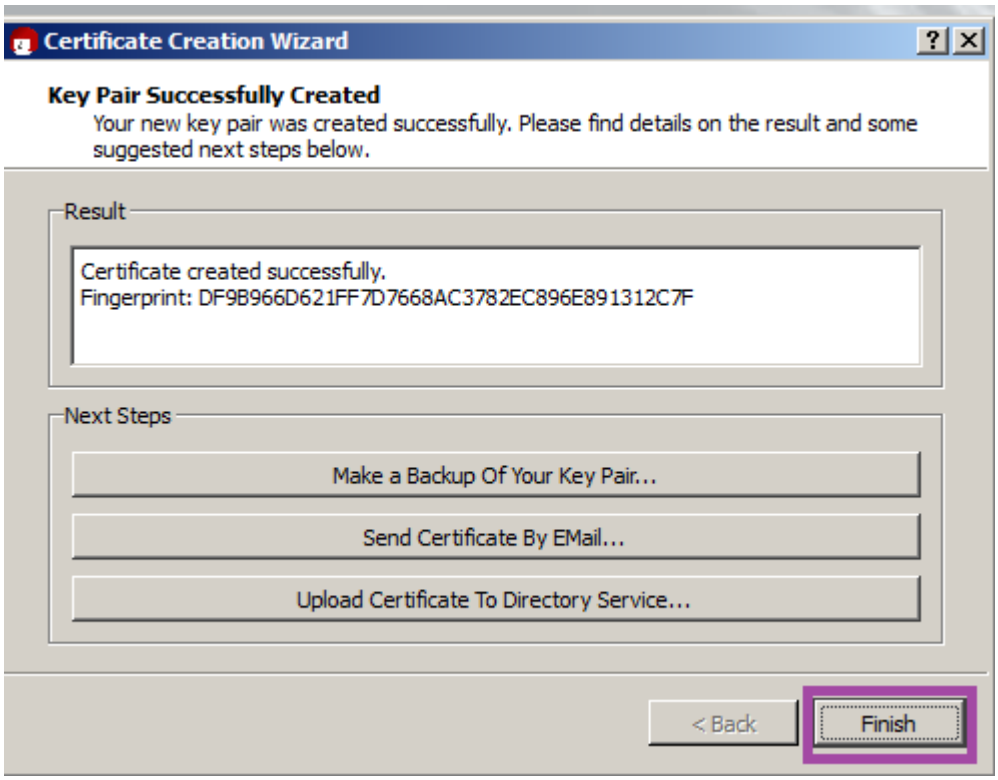
TAKE THIS ONE ANYWAY

9. At the pinentry screen, **re-enter** the Passphrase of `administrator`.



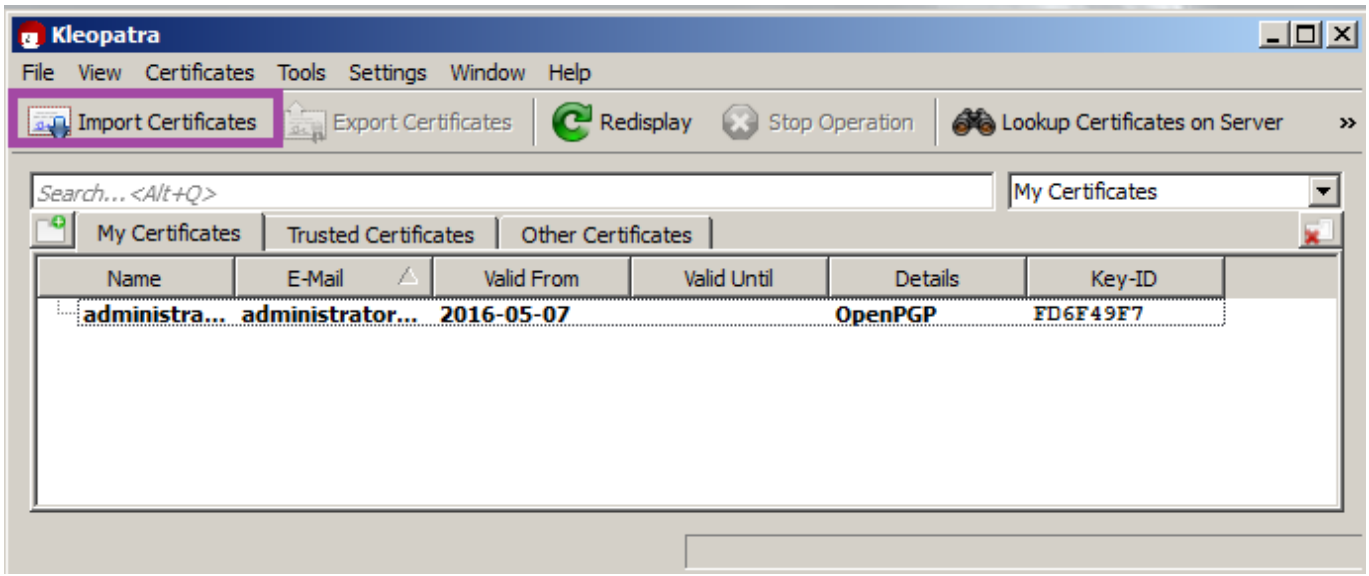
CLICK CREATE KEY

10. **Click** Finish to close the Certificate Creation Wizard.



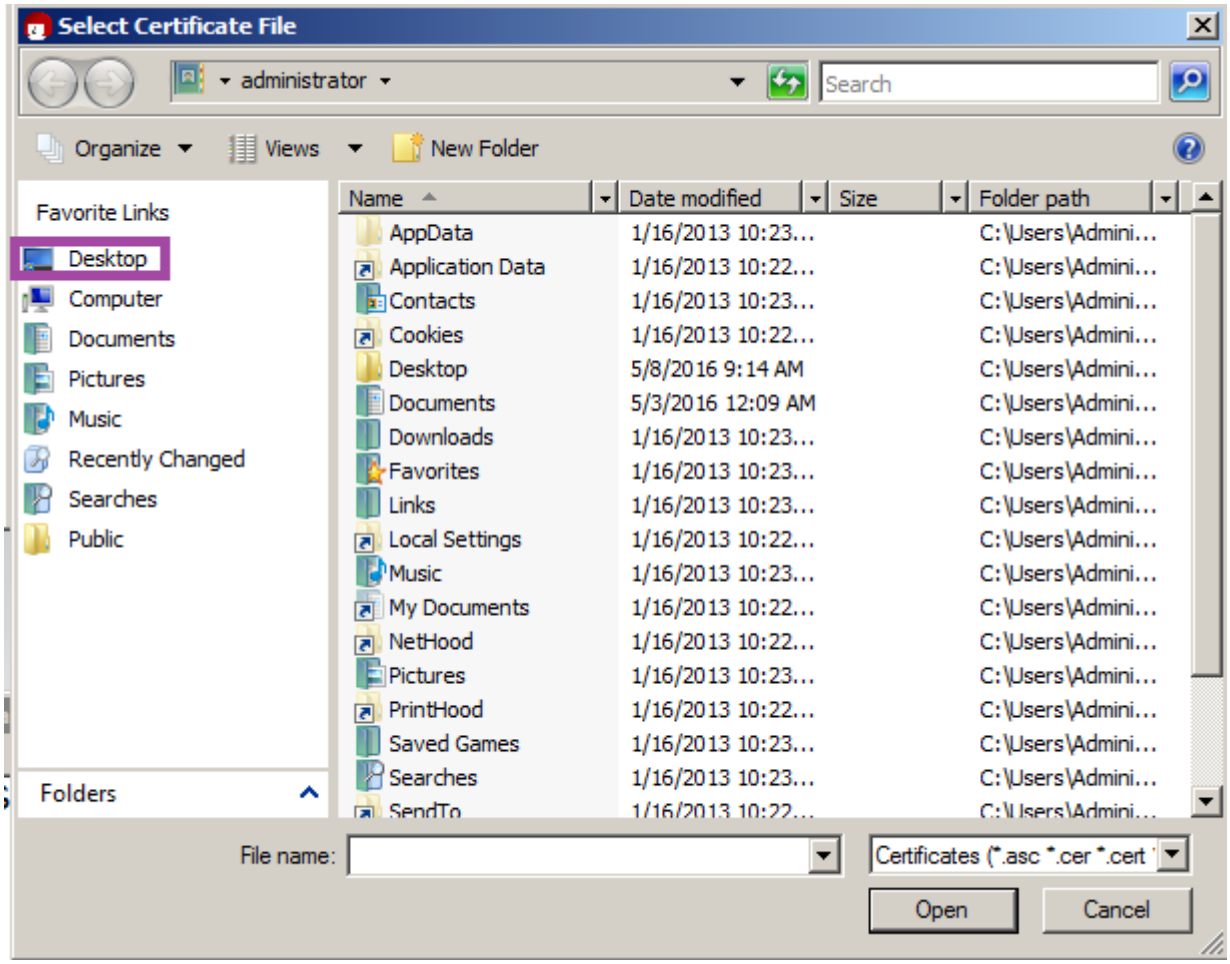
FINISH

11. **Click** Import Certificates.



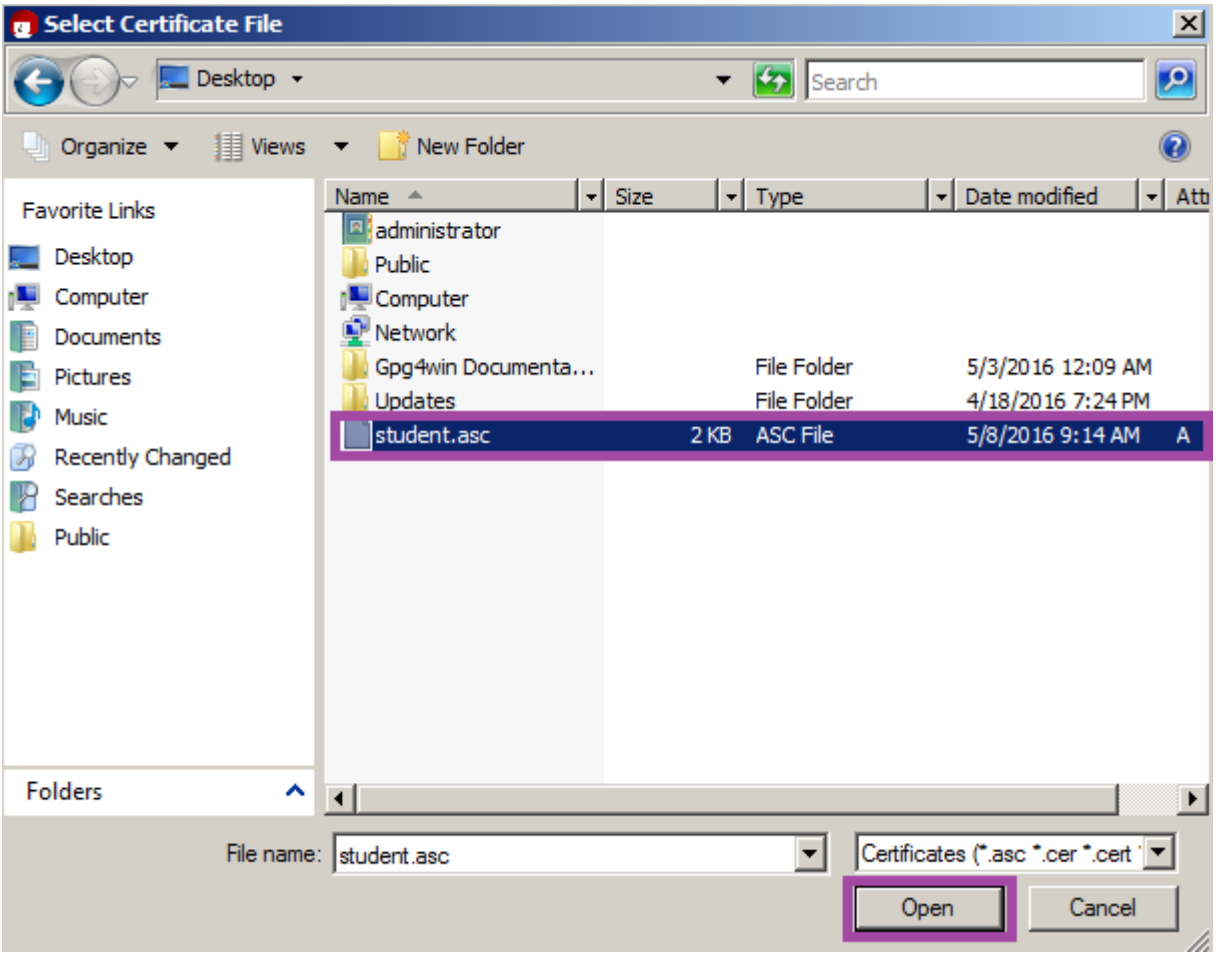
IMPORT CERTIFICATES

12. **Click** the Desktop link.



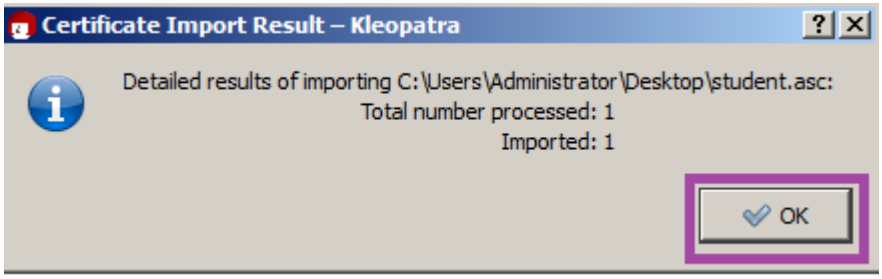
DESKTOP

13. **Click** the student.asc file and **click** Open.



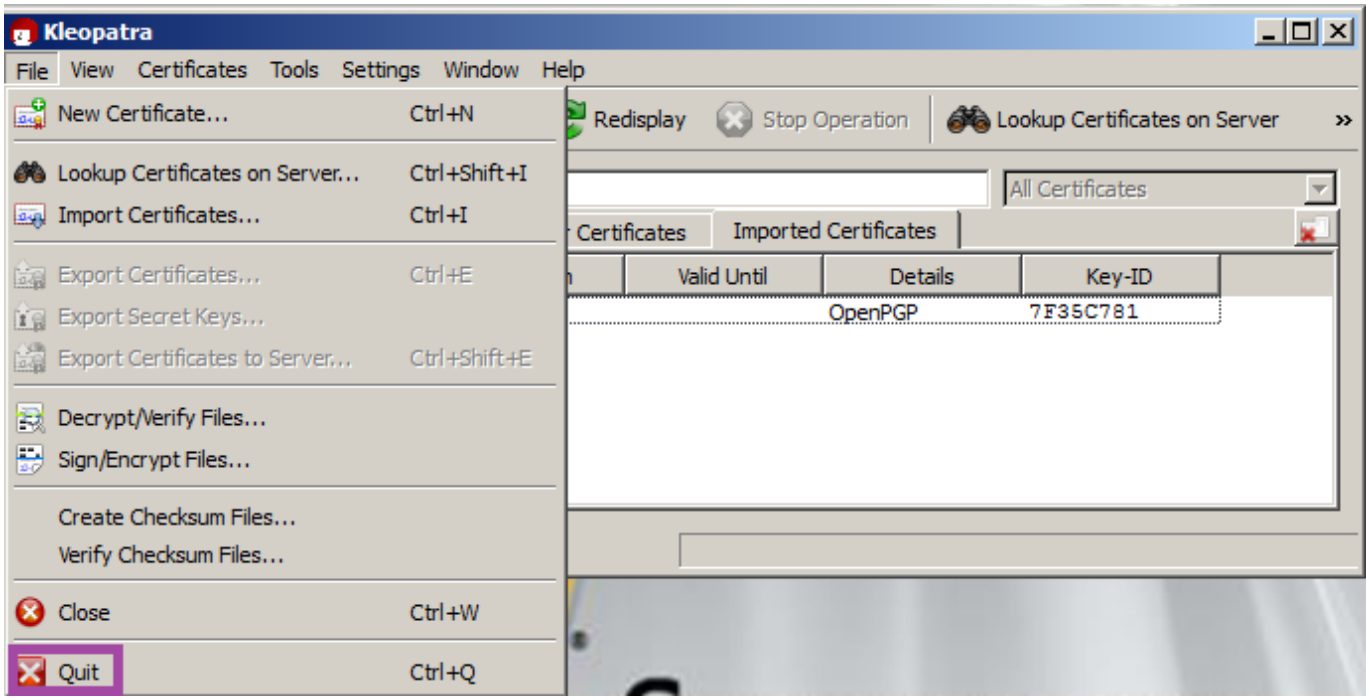
CLICK OPEN

14. **Click** OK to the Certificate Import Result – Kleopatra.



CLICK OK

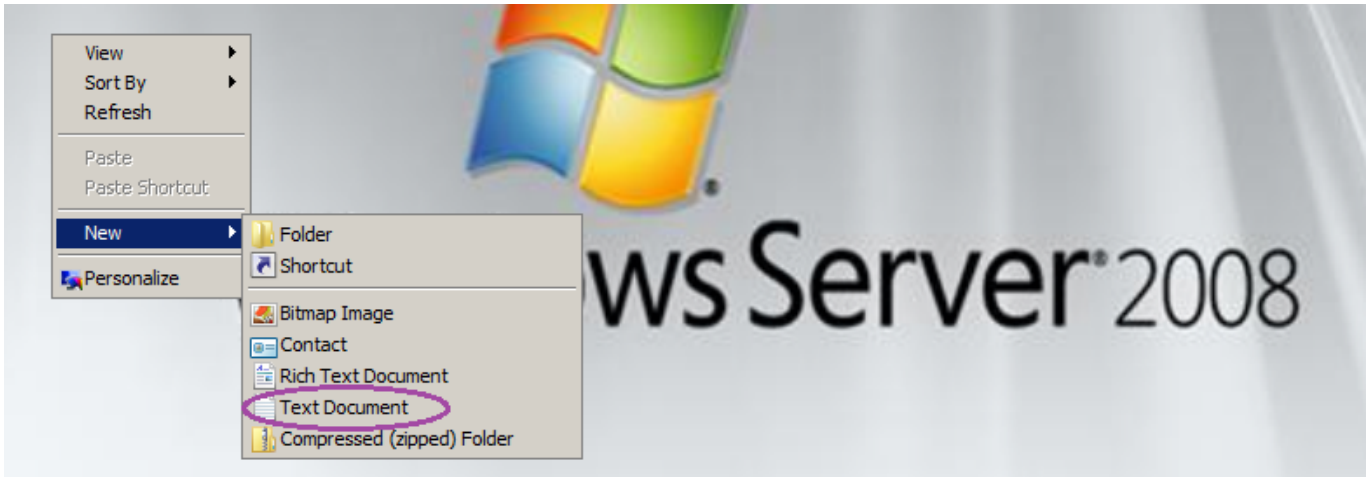
15. **Click** File from the Kleopatra mean and **select** Quit.



QUIT

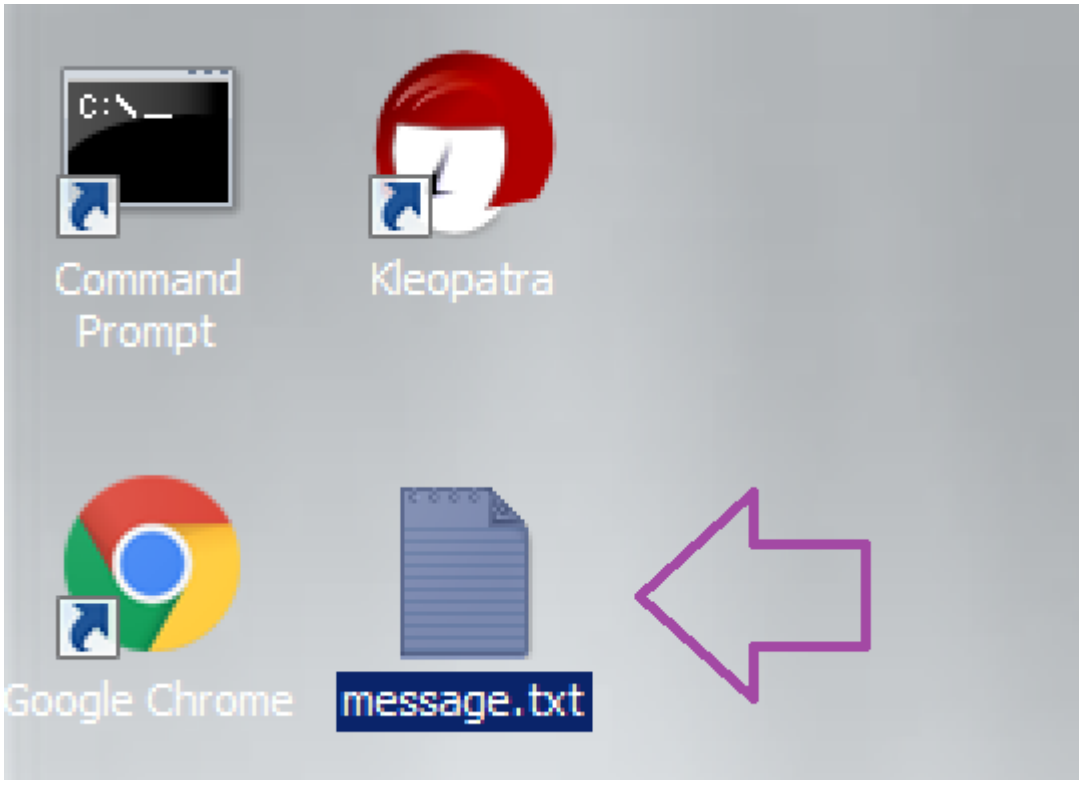
Encrypting and Decrypting the File

1. **Right-click** on the Windows Server desktop, **click** New then **select** Text Document.



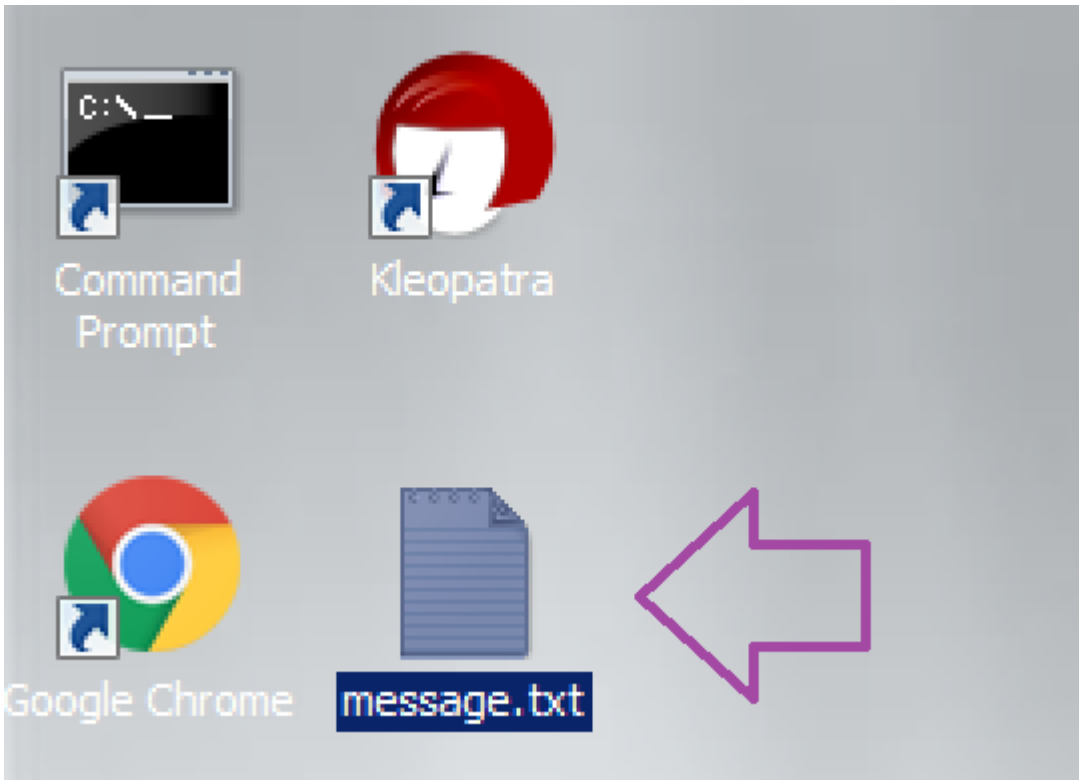
NEW TEXT DOCUMENT

2. **Name** the file message.txt.



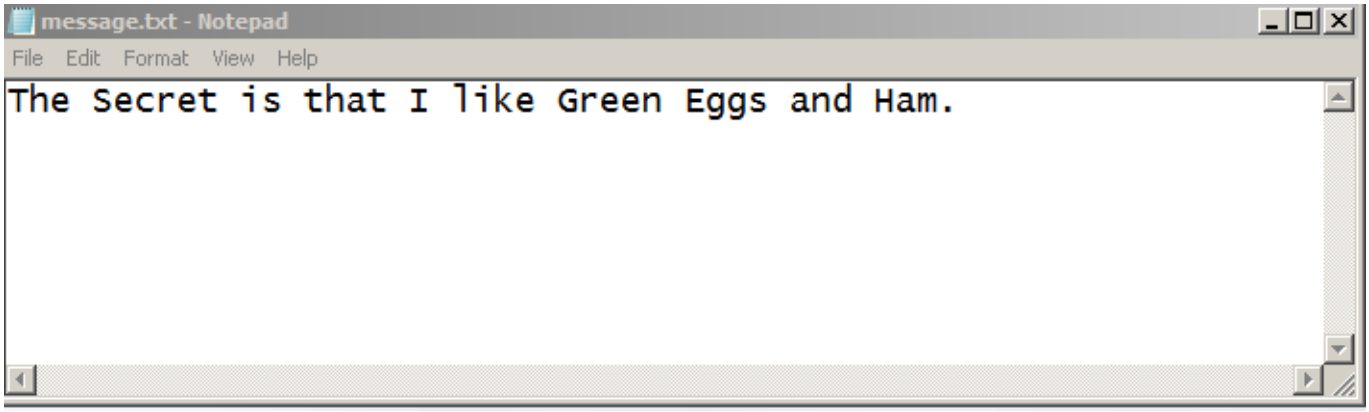
NAME THE FILE

3. **Double-click** on the file to open it.



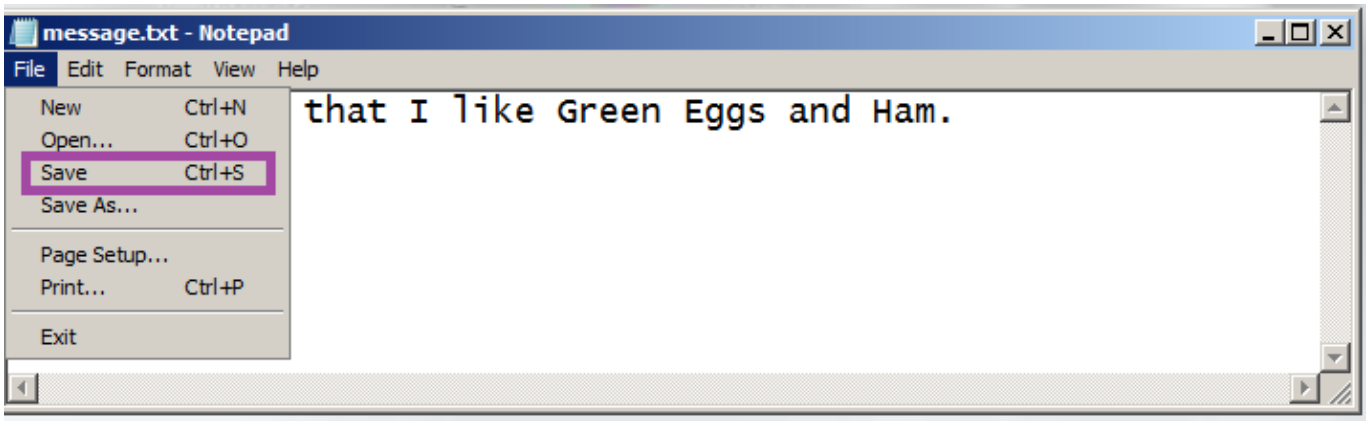
NAME THE FILE

4. **Type** the message `The Secret is that I like Green Eggs and Ham`.



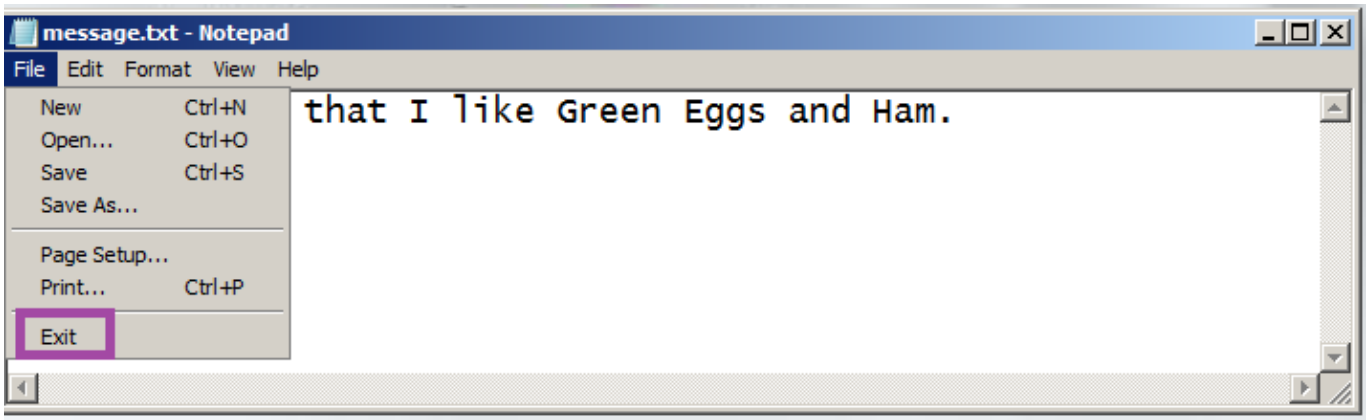
MESSAGE.TXT

5. **Click** File from the Notepad menu and **select** Save.



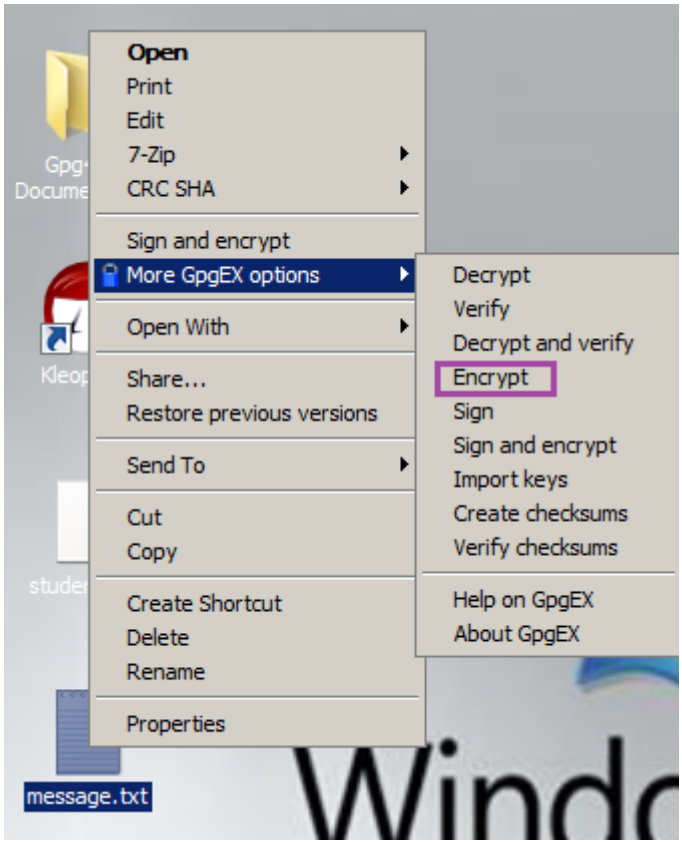
MESSAGE.TXT

6. **Click** File from the Notepad menu and **select** Exit.



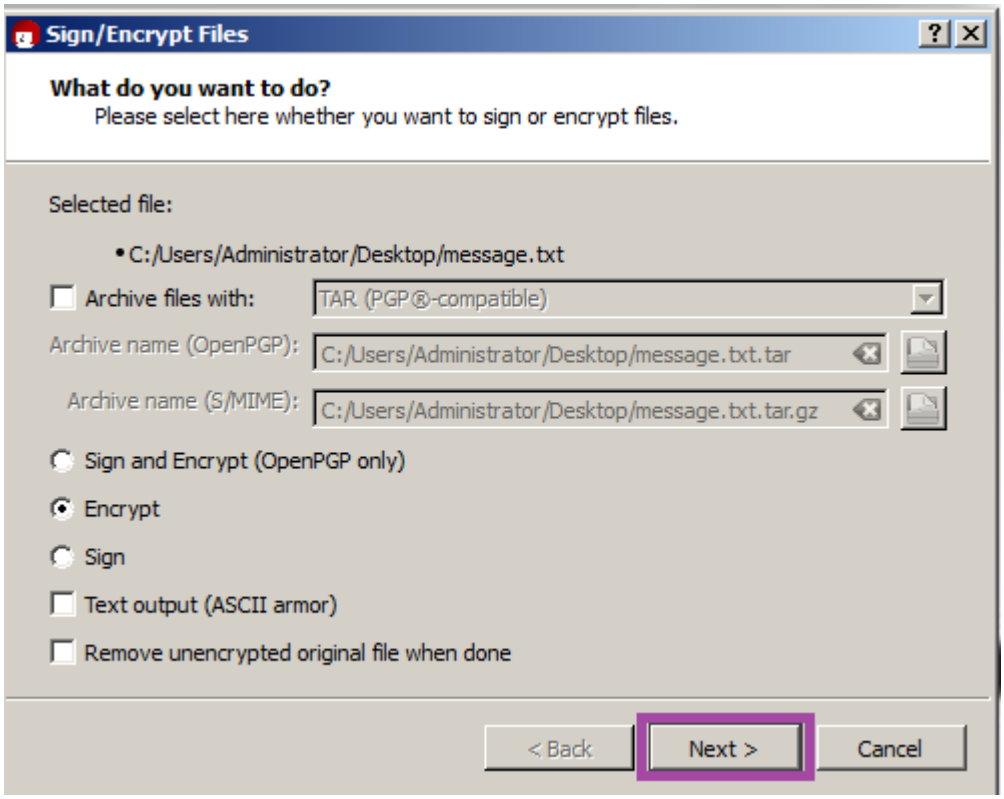
MESSAGE.TXT

7. **Right-click** on message.txt and **select** More GpgEX options and then **select** Encrypt.



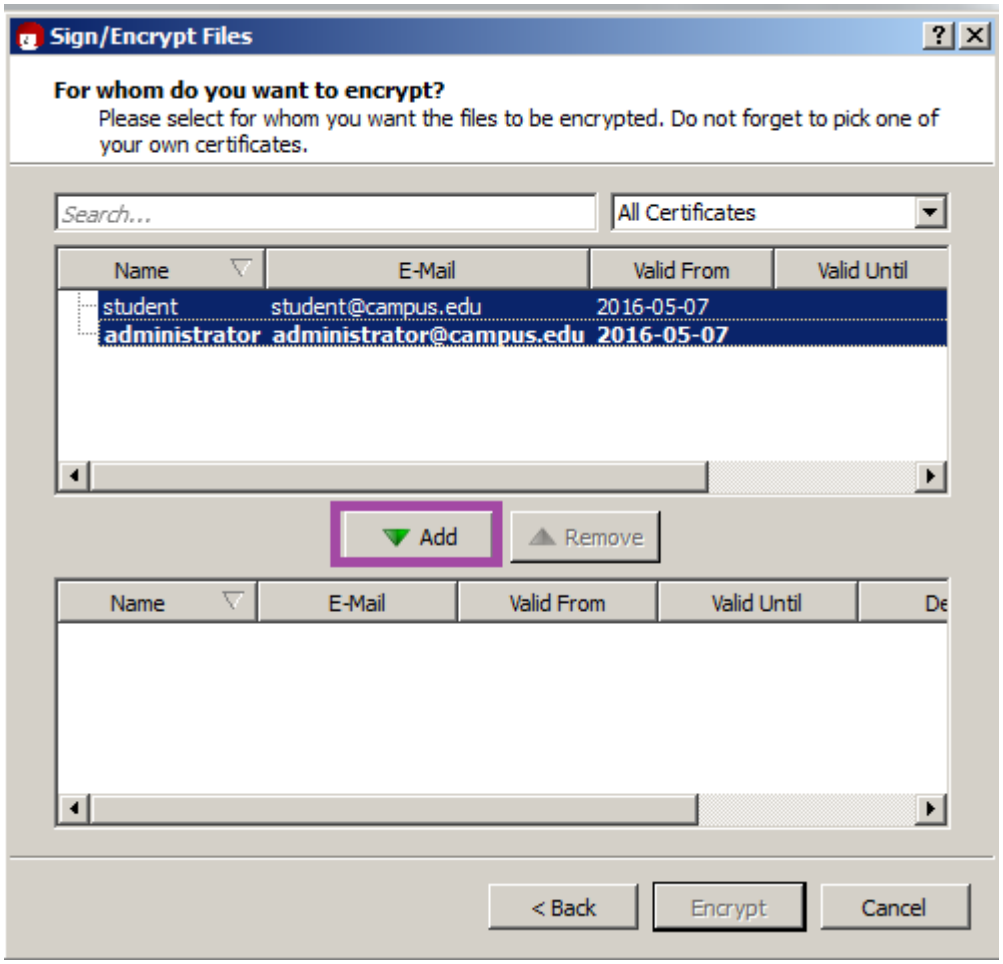
ENCRYPT

8. **Click** Next at the Sign/Encrypt Files screen.



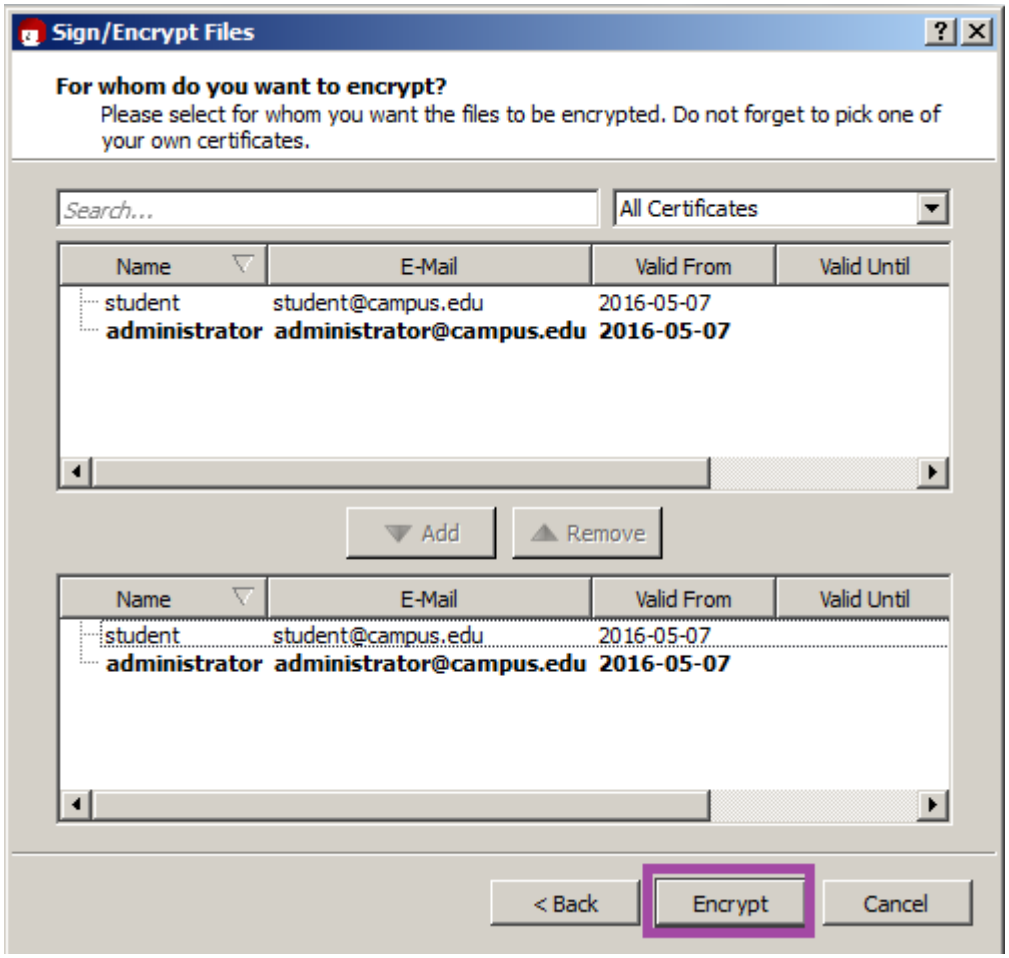
NEXT

9. **Hold down** Control to select the student and the administrator certificates. **Click** Add.



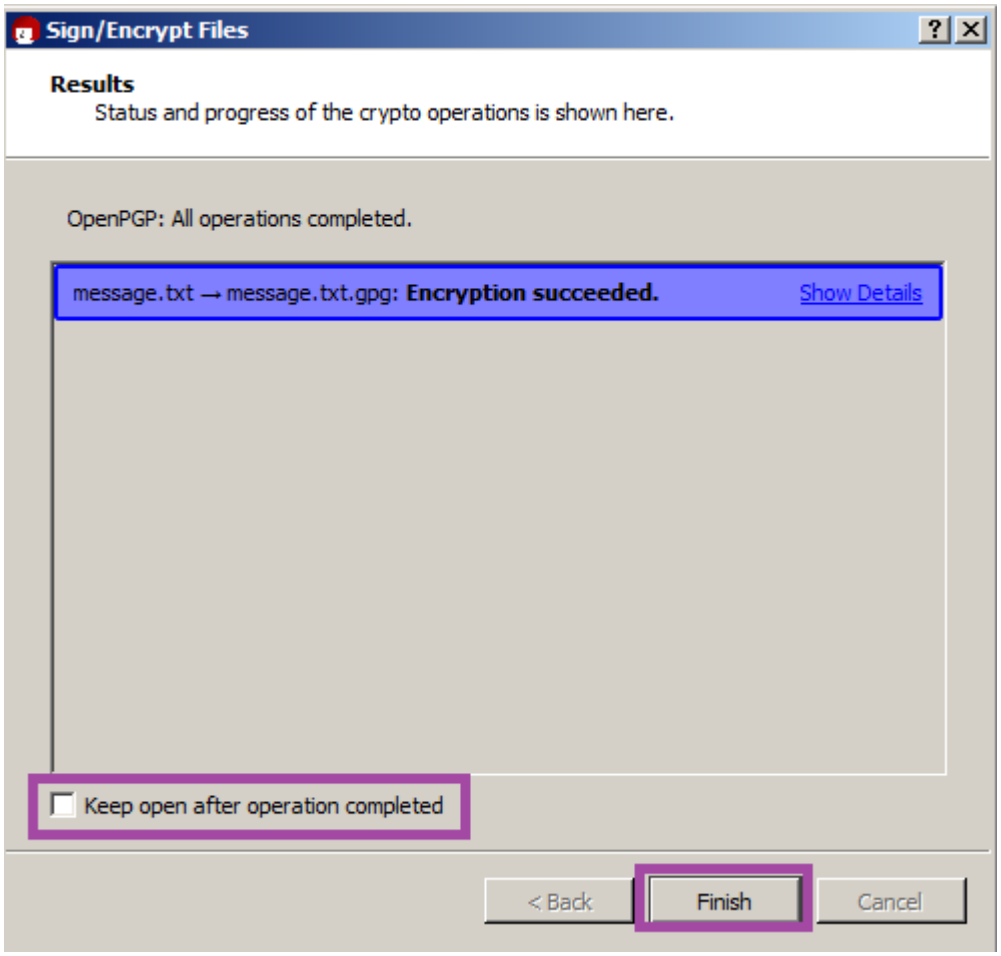
CERTIFICATES

10. Both certificates should appear in the bottom box. **Click** Encrypt.



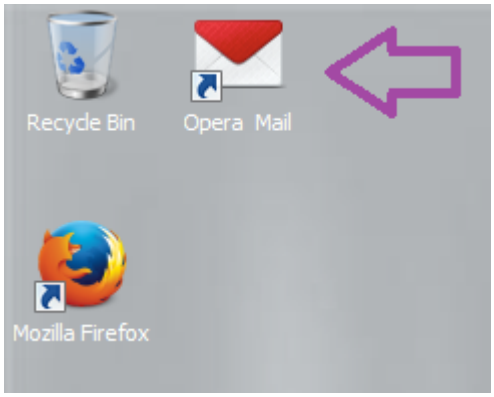
CERTIFICATES

11. You should see the message in blue that Encryption succeeded. **Remove** the check to Keep open after operation completed. **Click** the Finish button.



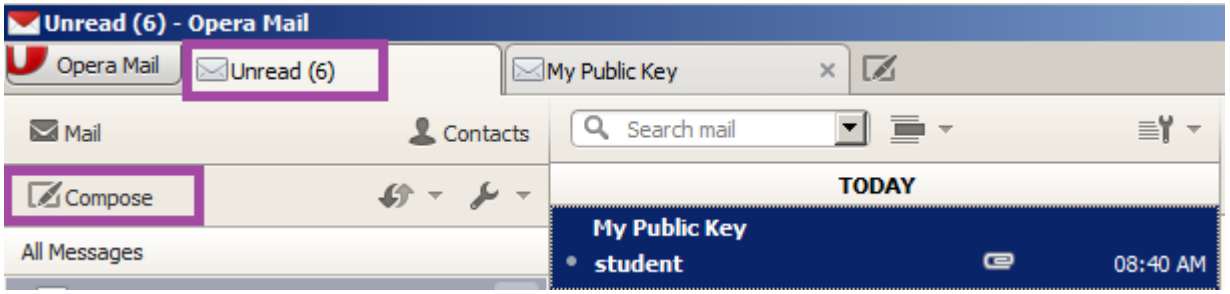
CLICK FINISH

12. **Double-click** on the shortcut to Opera Mail on the desktop.



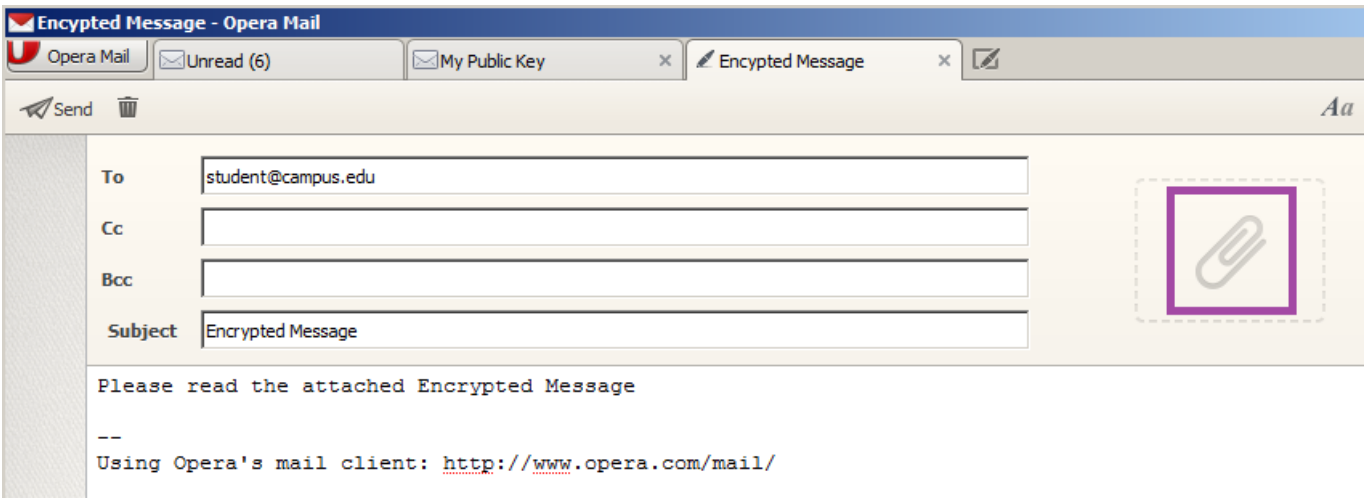
OPERA MAIL

13. **Click** Unread and **click** the Compose button located on the left side of Opera Mail.



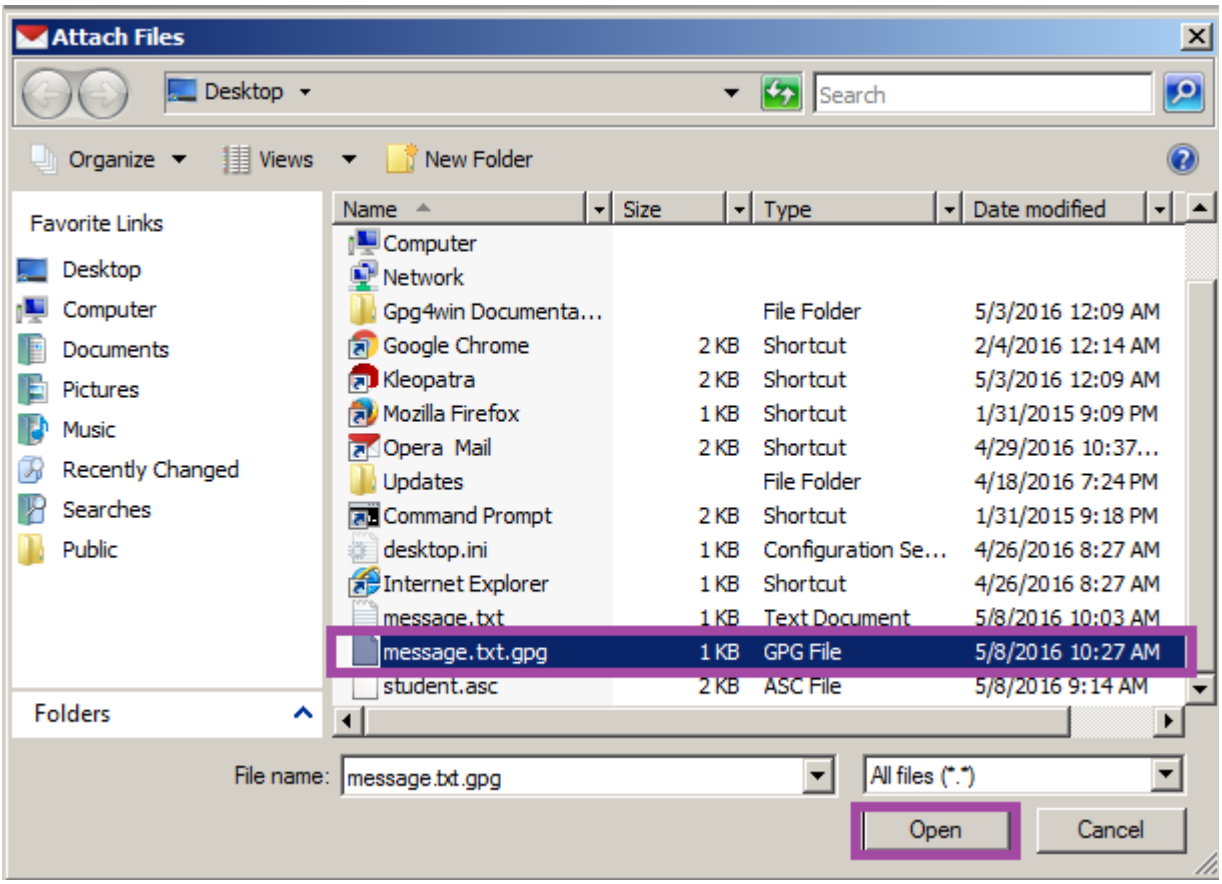
COMPOSE EMAIL

14. In the To box, **type** `student@campus.edu`. In the Subject box, **type** `Encrypted Message`. In the body, **type** `Please read the attached Encrypted Message`. **Click** the paper clip to attach a file.



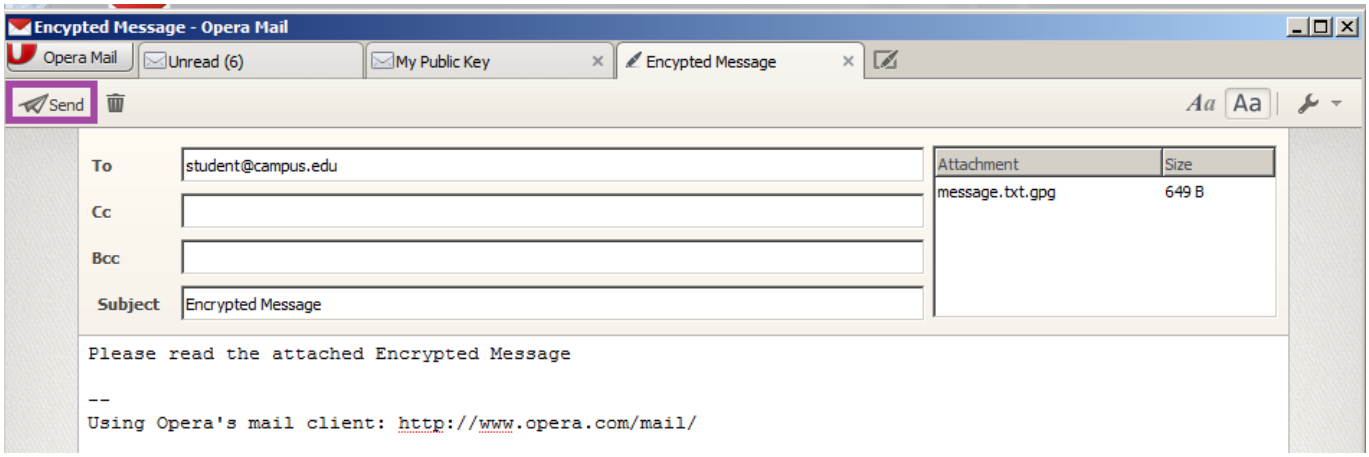
COMPOSE EMAIL

15. **Find** message.txt.gpg in the list and then **click** Open.



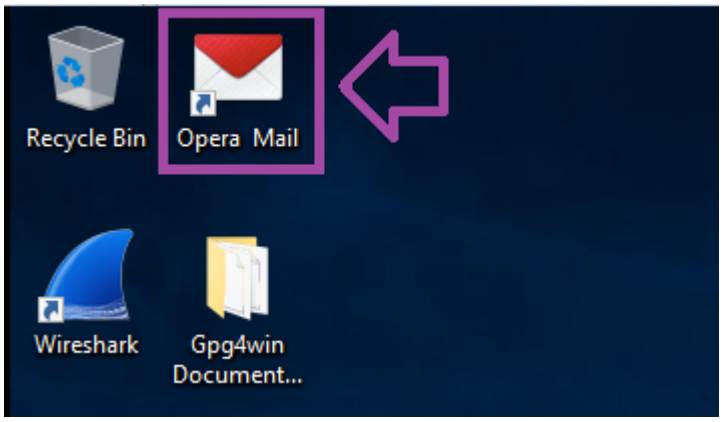
DESKTOP LINK

16. **Click** the Send button to send the email.



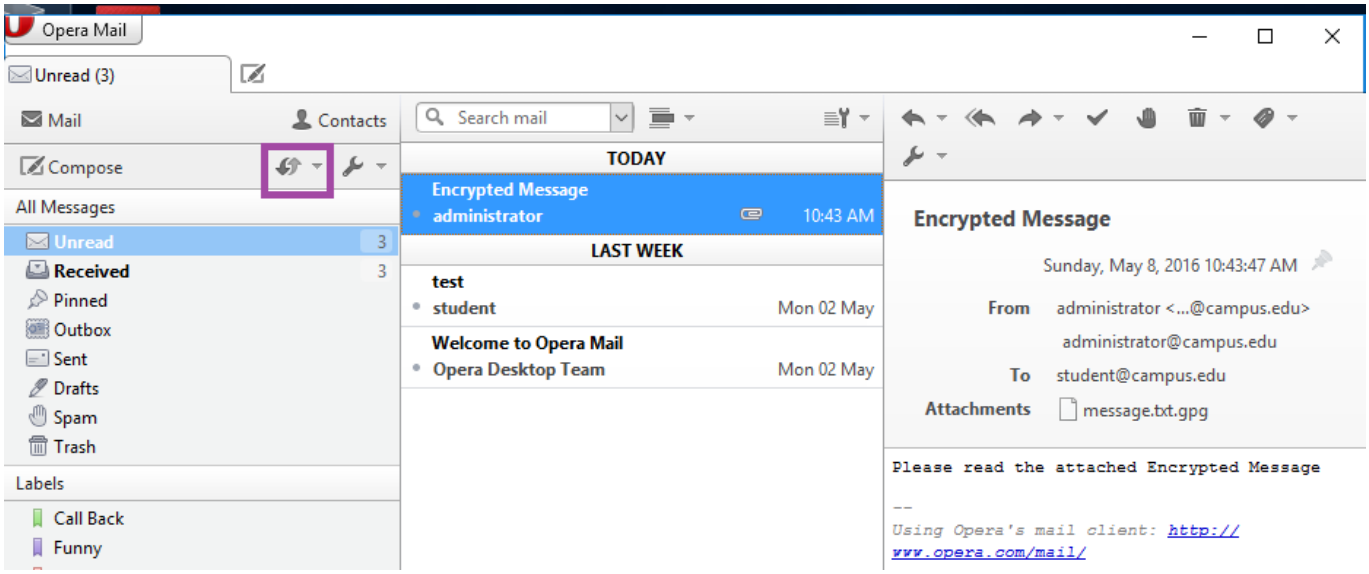
OPERA MAIL

17. **Click** on the Windows 10 machine. If the Opera Mail program is not already open, **double-click** on the shortcut to Opera Mail.



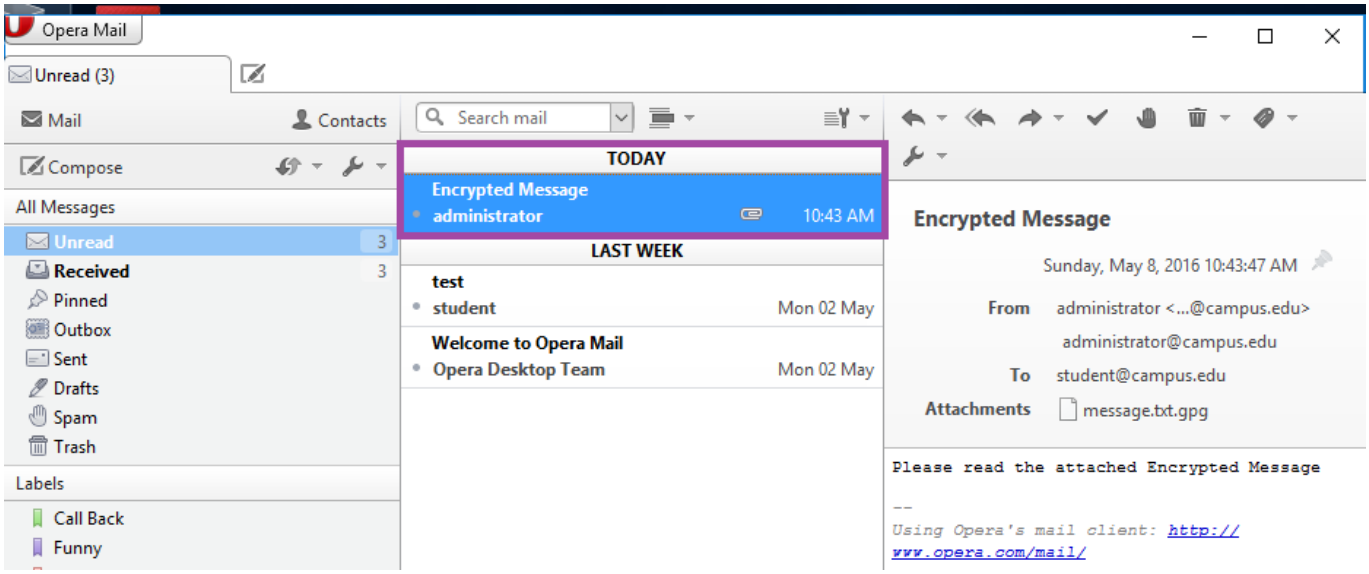
OPERA MAIL

18. **Click** the send/receive button.



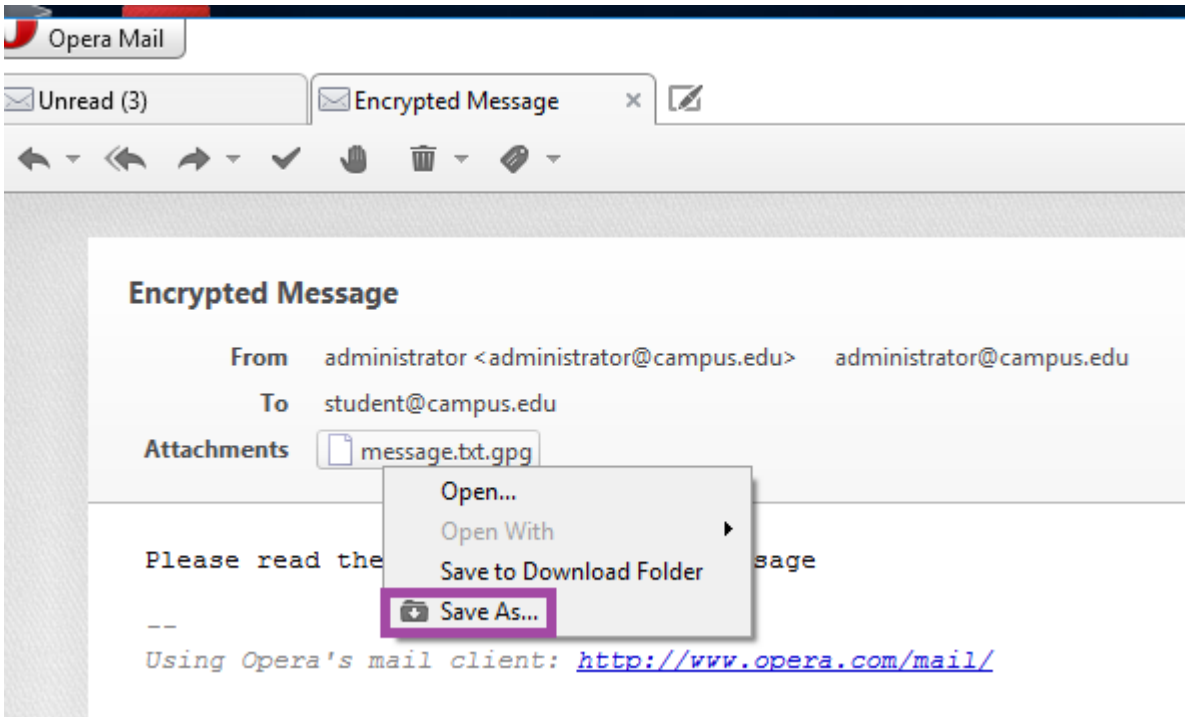
OPERA MAIL

19. **Double-click** on the email from administrator with the subject Encrypted Message.



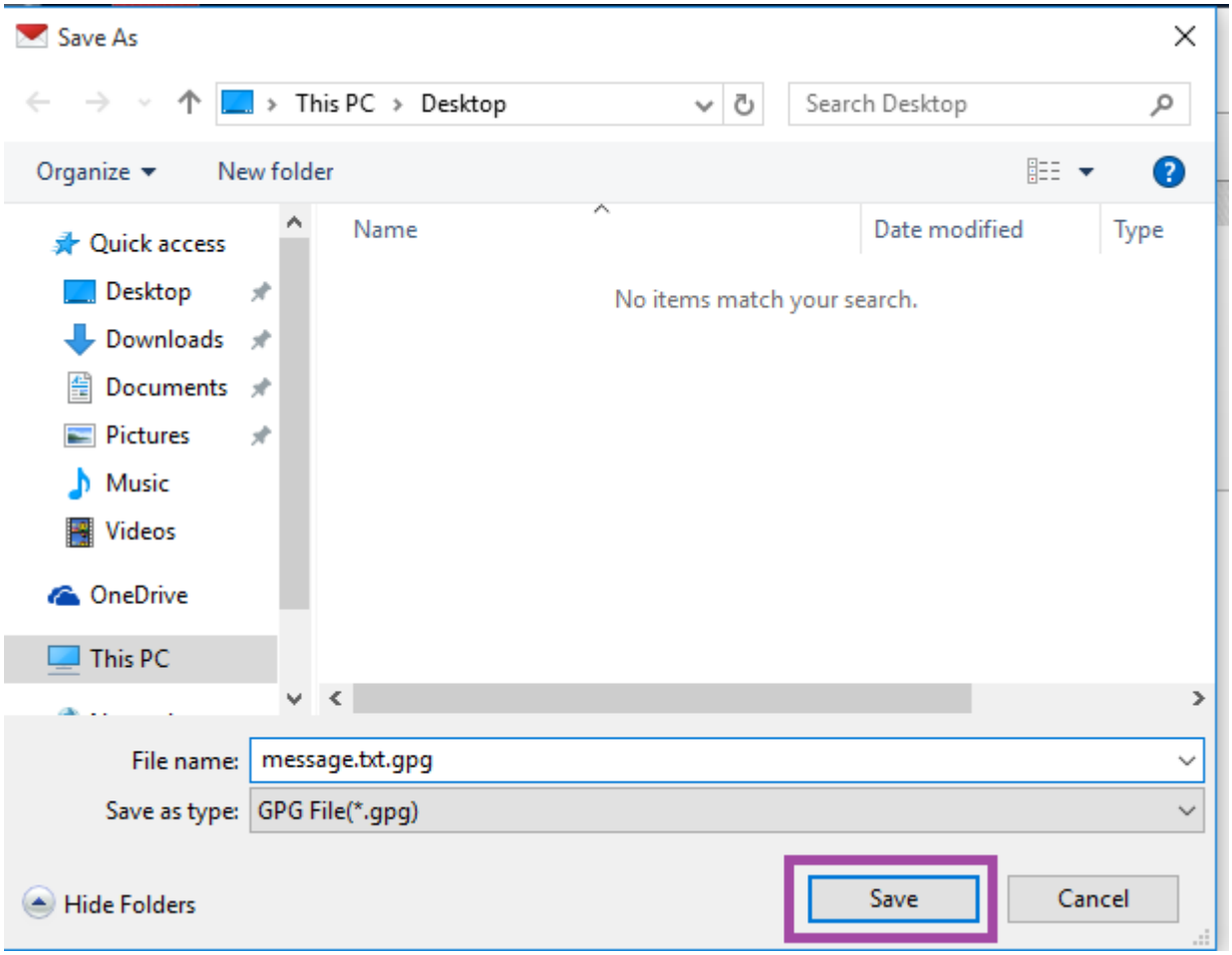
OPERA MAIL

20. **Click** the message.txt.gpg file and **select** Save As.



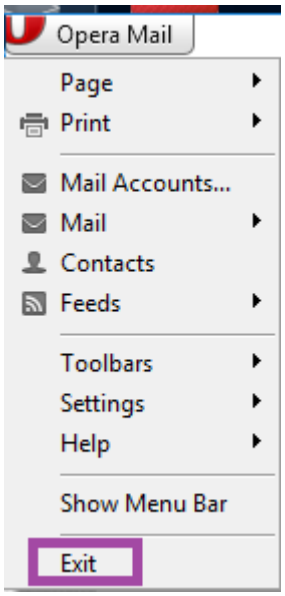
SAVE AS

21. **Click** Save.



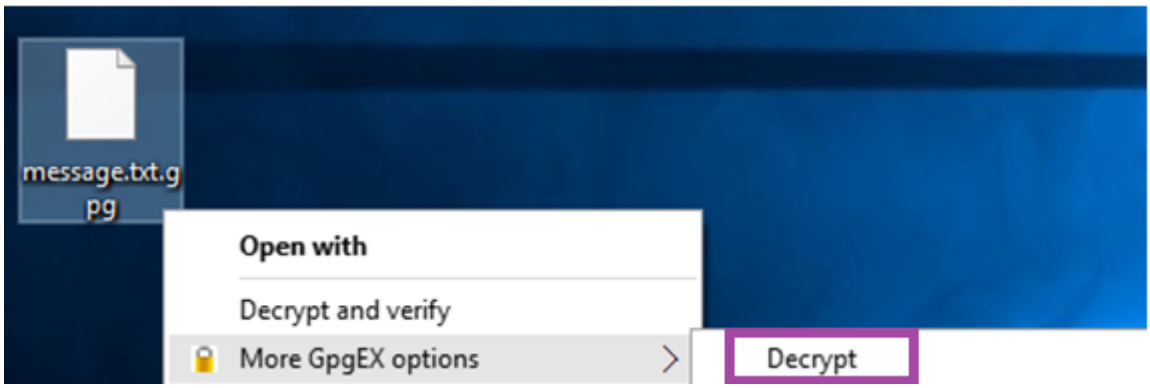
SAVE

22. **Click** Opera Mail and then **select** Exit.



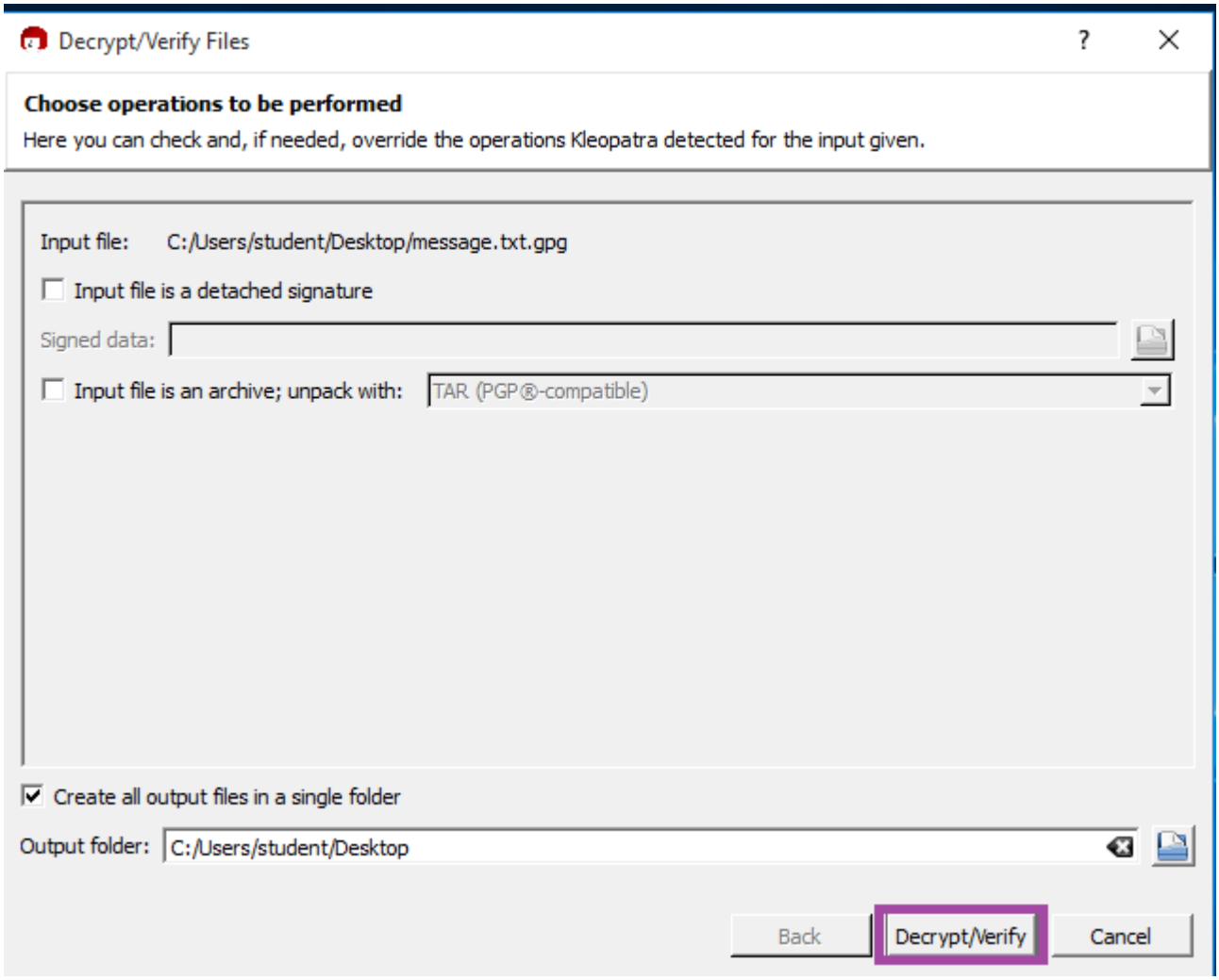
EXIT

23. **Right-click** on message.txt.gpg and **select** More GpgEX options and **select** Decrypt.



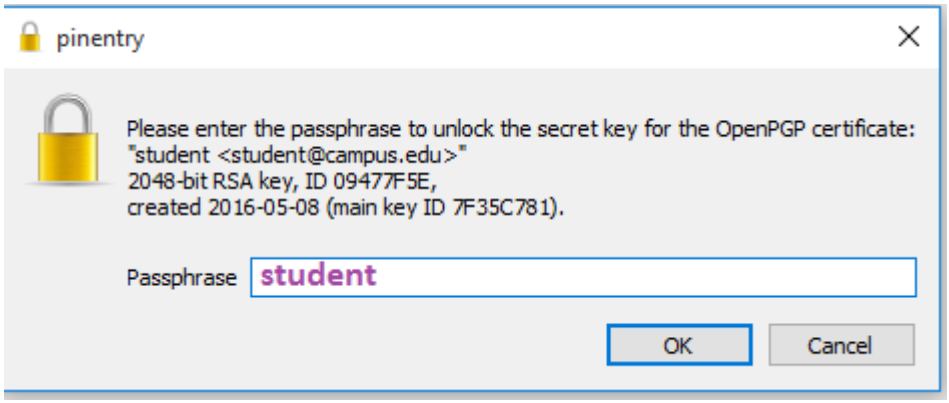
EXIT

24. **Click** Decrypt/Verify.



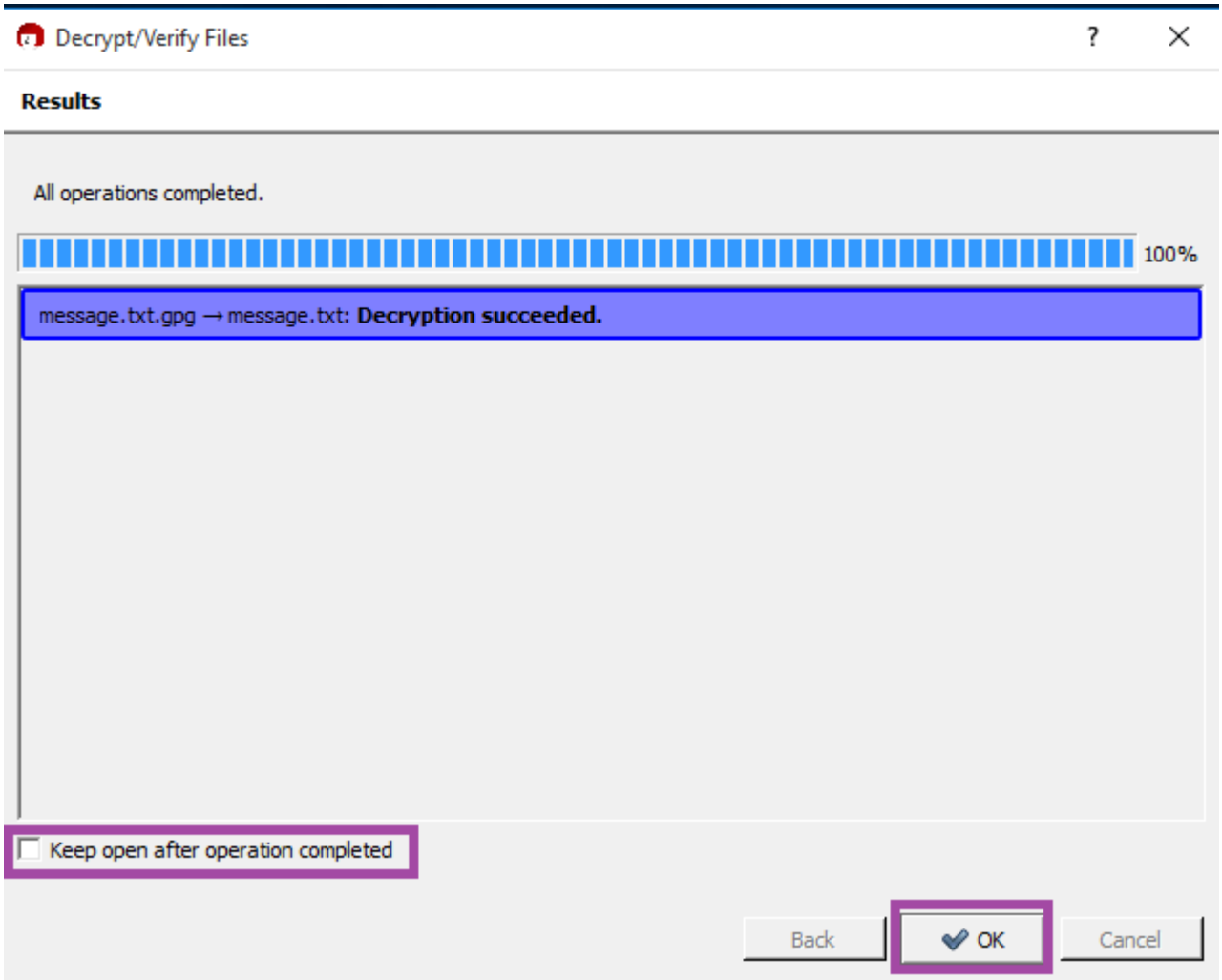
DECRYPT

25. For the Passphrase, **type** `student` and then **click** OK.



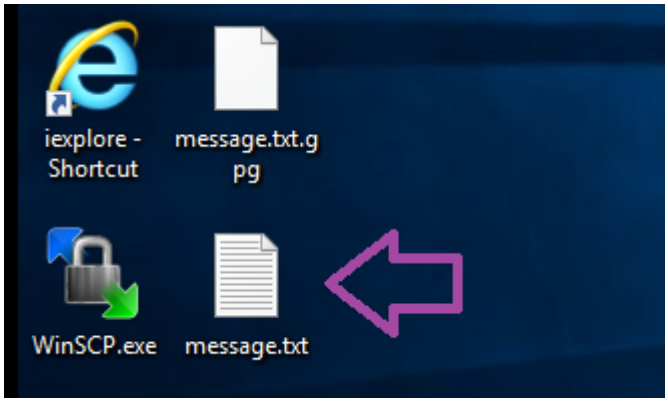
PASSPHRASE

26. You should see the message in blue that Decryption succeeded. **Remove** the check to Keep open after operation completed. **Click** the OK button.



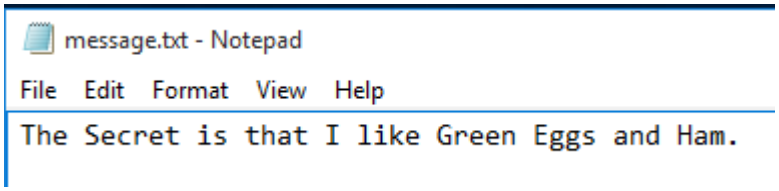
OK

27. **Double-click** on the message.txt file on the Windows 10 desktop.



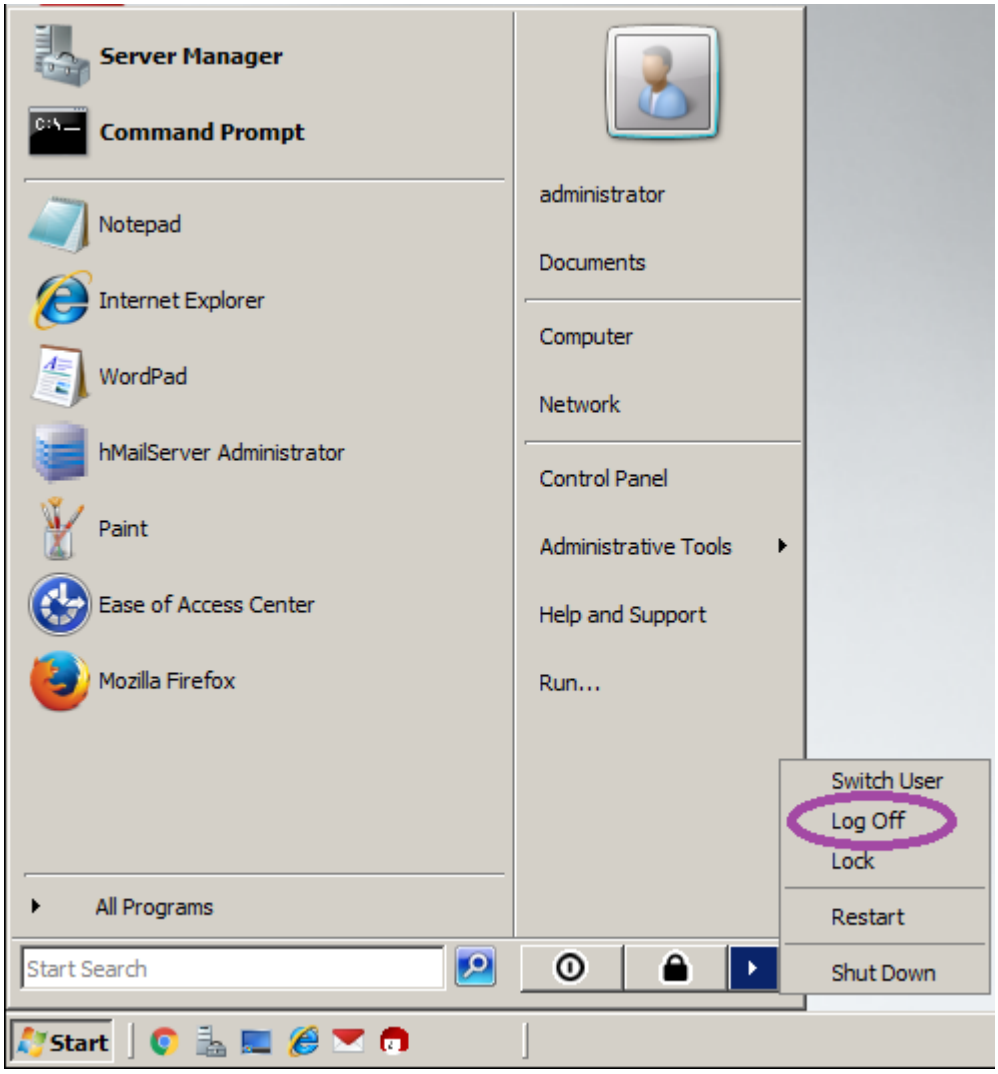
EXIT

28. **Read** the message The Secret is that I like Green Eggs and Ham.

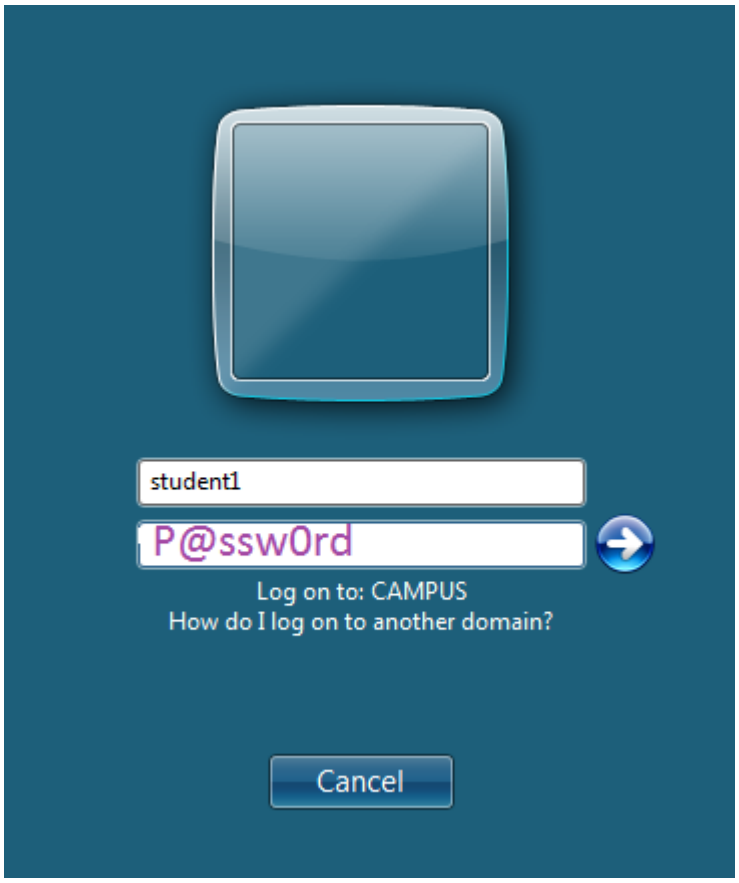


SECRET MESSAGE

29. **Click** on the Windows Server icon on the topology. **Click** on the start button and then **click** the arrow, displayed below and **choose** logoff.

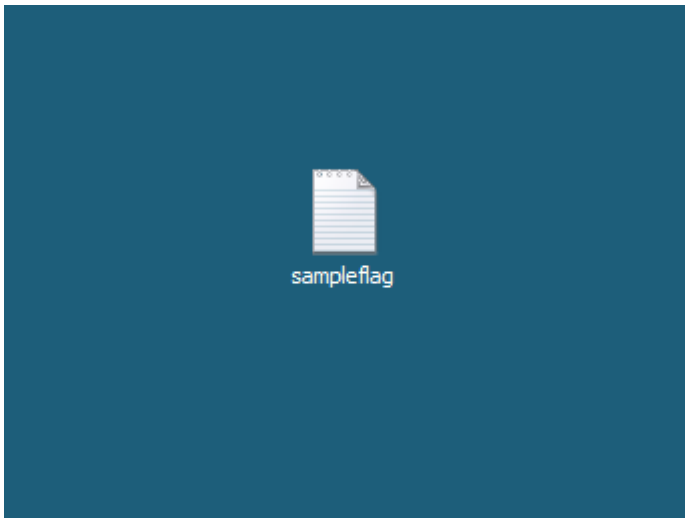


30. After sending a control alt delete to the virtual machine, **log in** as `student1` with the password of `P@ssw0rd`.



LOG ON TO WINDOWS SERVER

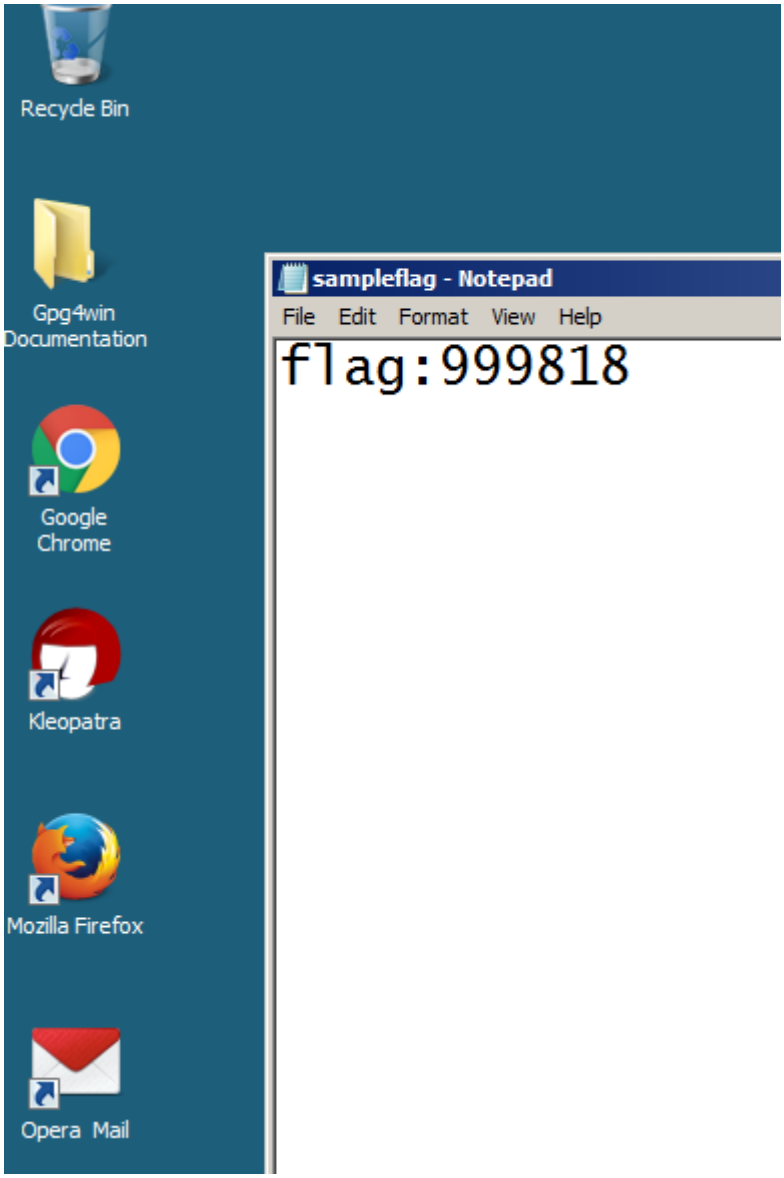
31. **Double-click** on the sample flag file on your desktop.



SAMPLE FLAG FILE

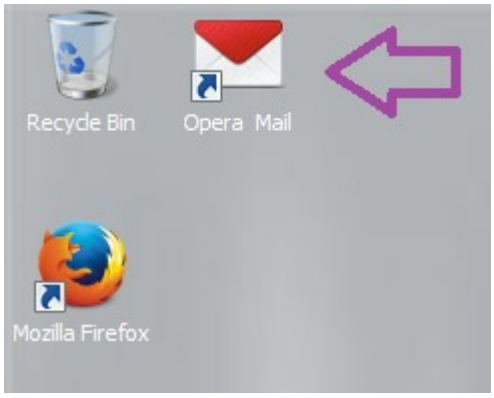
32. **Notice** the flag of 999818. **Click** on the Challenge icon and **type** the flag number into the left hand pane in the field for flag#1 answer box. This is just to show you how to **capture** Challenge Flags you will see throughout this lab.

Challenge Sample #



FLAG:999818

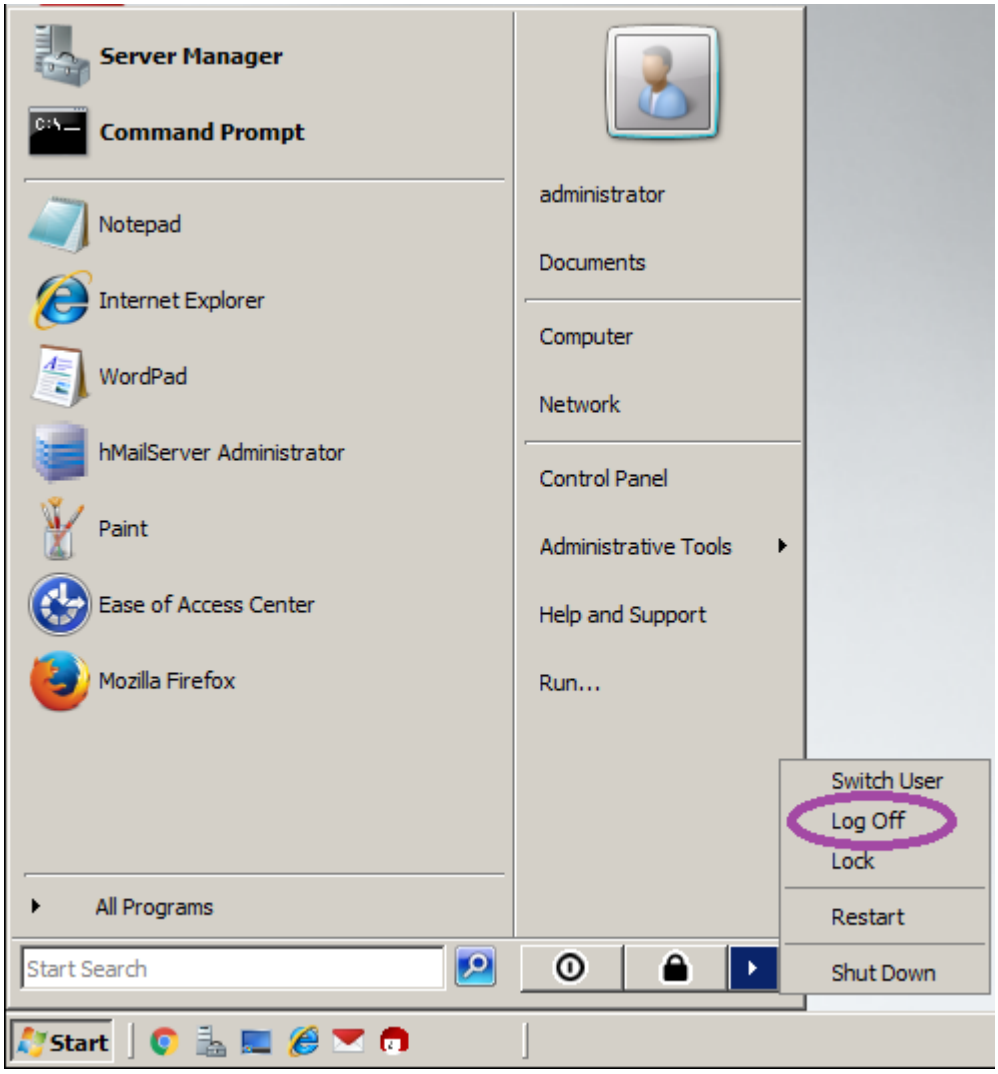
32. **Double-click** on the shortcut to Opera Mail on your desktop.



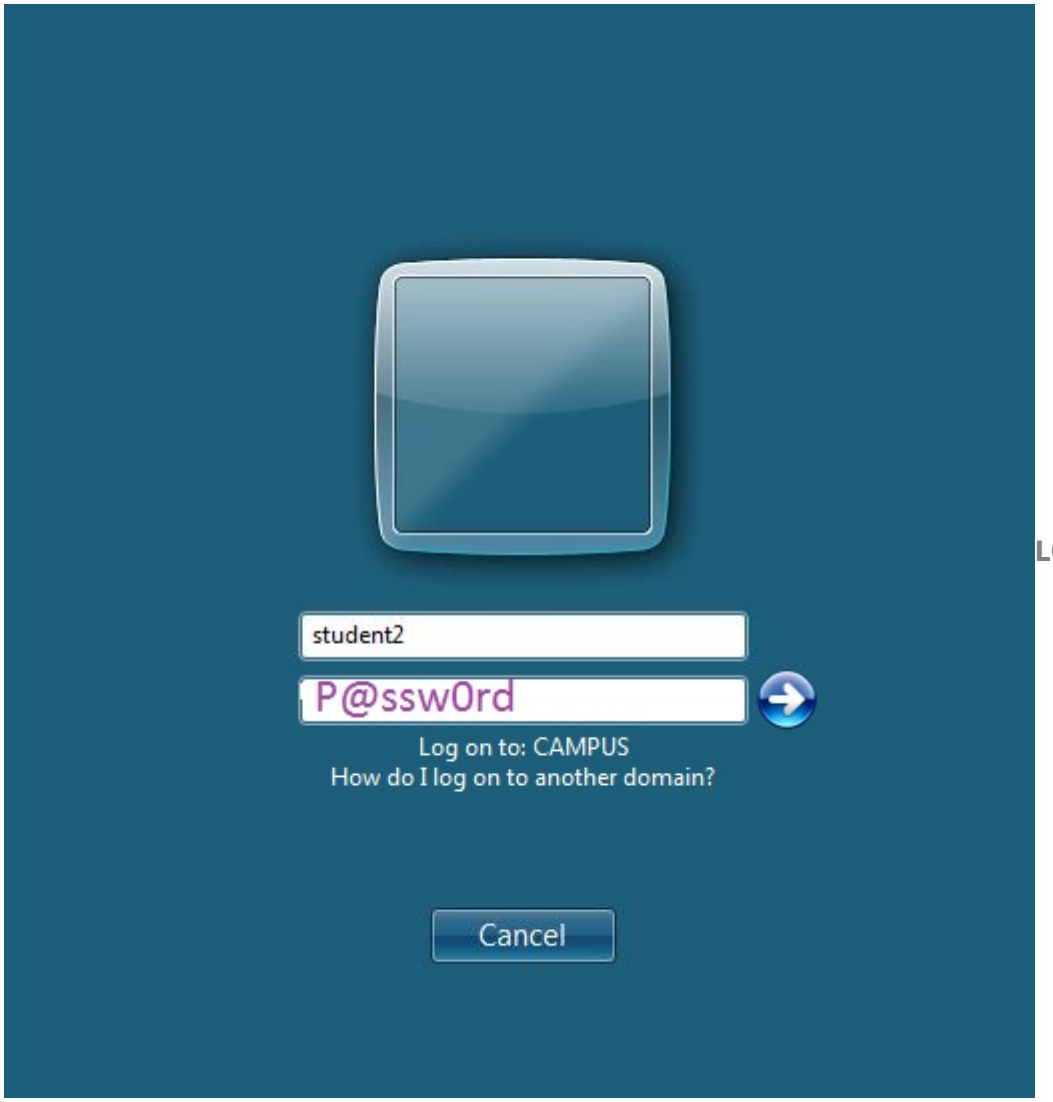
SHORTCUT TO OPERA MAIL

33. **Click** the unread tab. **Click** the send/receive button.

34. **Click** on the Windows Server icon on the topology. **Click** on the start button and then **click** the arrow, displayed below and choose logoff.

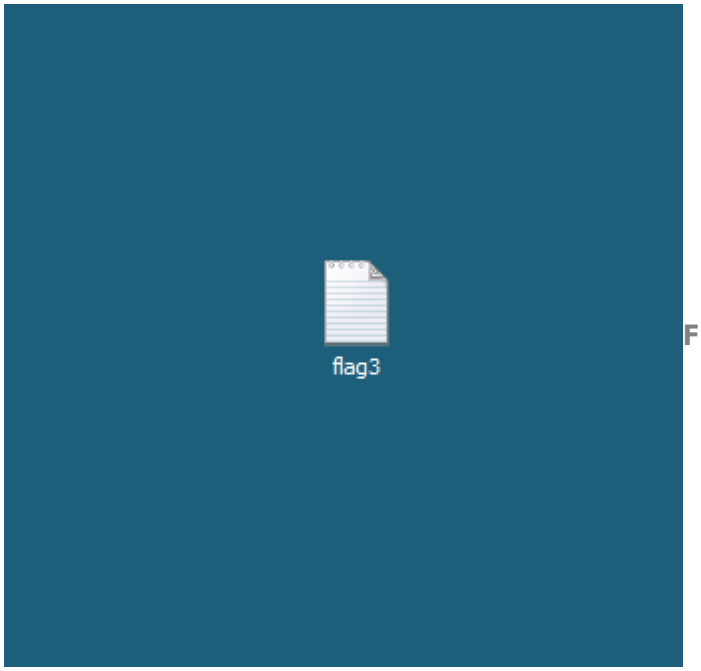


35. After sending a control alt delete to the virtual machine, **log in** as student2 with the password of `P@ssw0rd`.



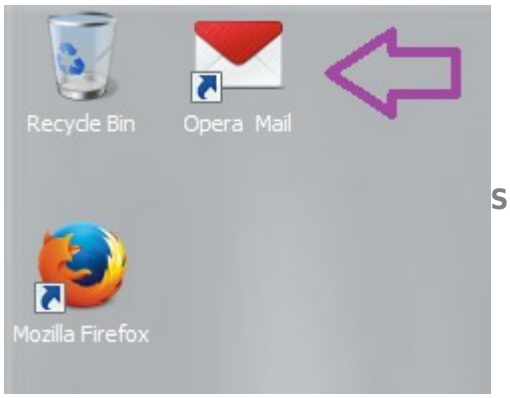
LOG ON TO WINDOWS SERVER

36. **Double-click** on the flag3 file on your desktop.



FLAG 3 FILE

37. **Double-click** on the shortcut to Opera Mail on your desktop.



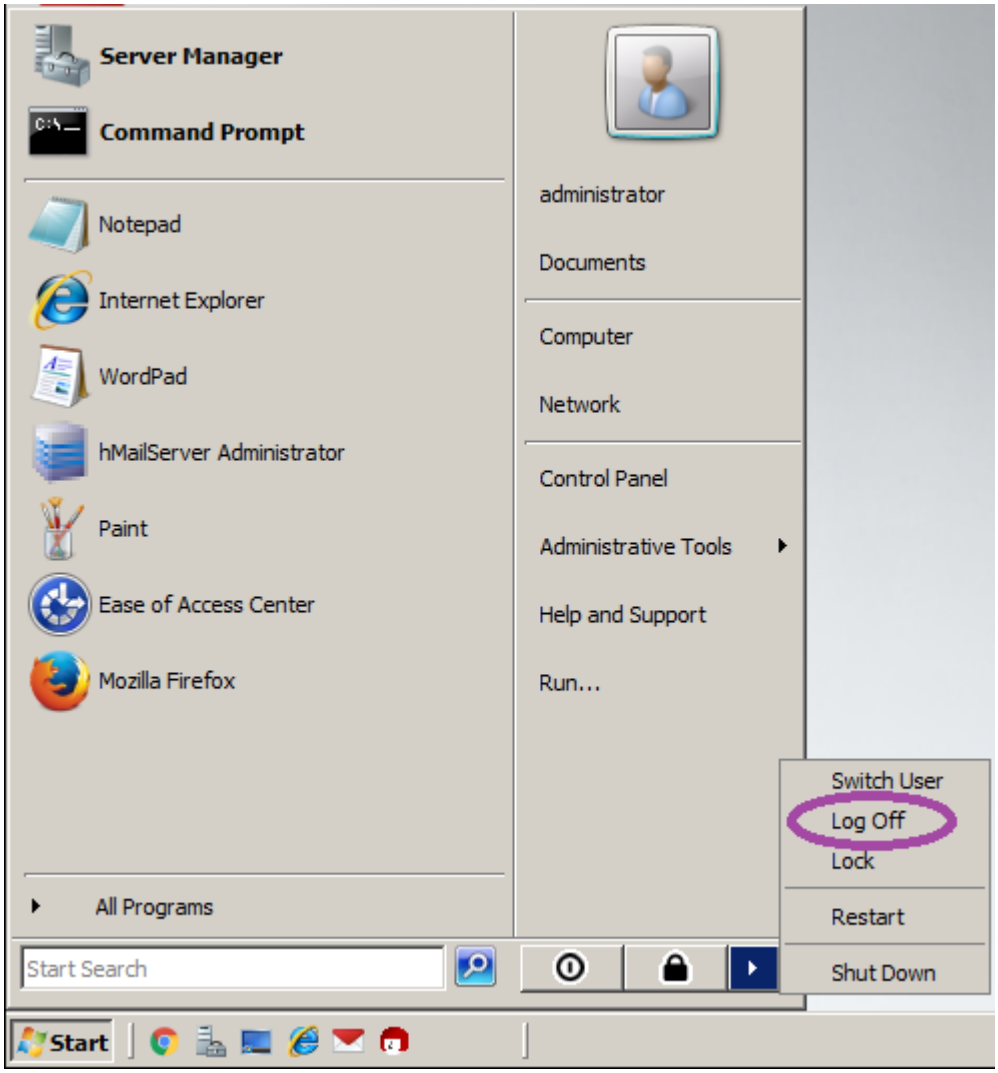
SHORTCUT TO OPERA MAIL

38. **Click** the send/receive button.

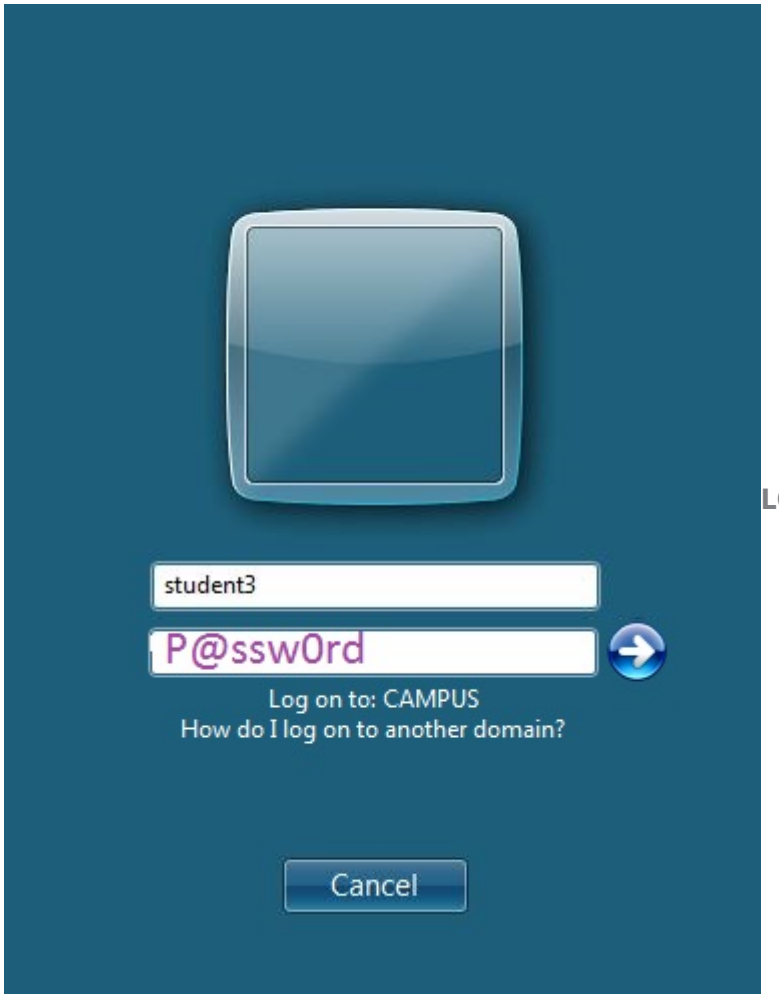
Challenge #

OPERA MAIL

39. **Click** on the Windows Server icon on the topology. **Click** on the start button and then **click** the arrow, displayed below and **choose** logoff.

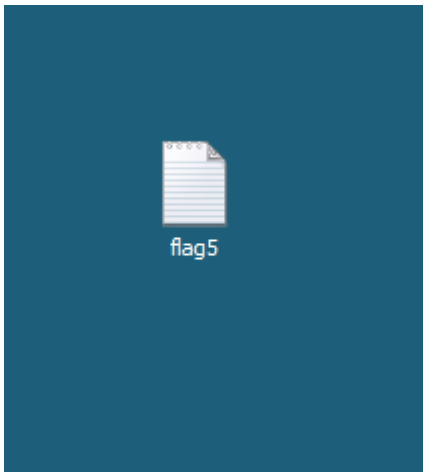


40. After sending a control alt delete to the virtual machine, **log in** as `student3` with the password of `P@ssw0rd`.



LOG ON TO WINDOWS SERVER

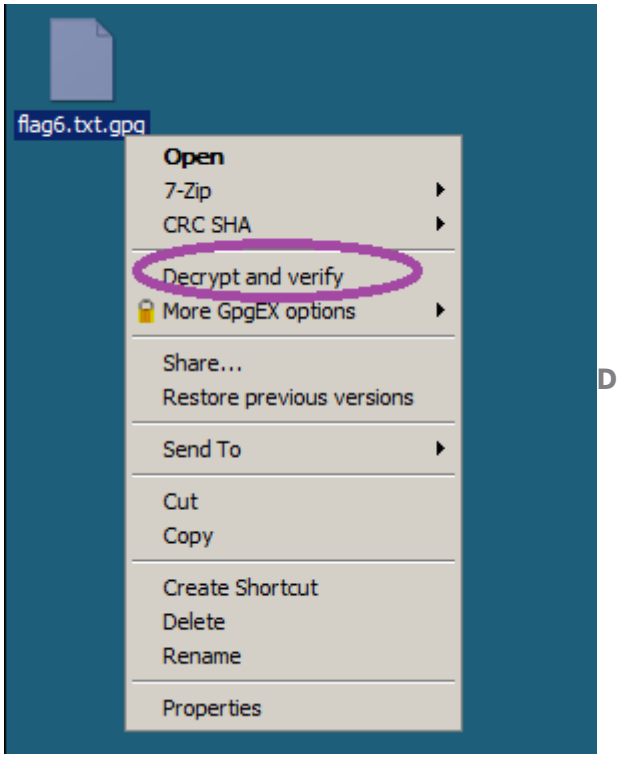
42. **Double-click** on the flag5 file on your desktop.



FILE

Challenge #

43. **Right click** on the flag6.txt.gpg. for the password, **type** `student3` (all lowercase)



DECRYPT AND VERIFY

Challenge #

OPERA MAIL

Note: Press the STOP button to complete the lab.