

2020/2021

CYBER SECURITY



Lab 3: Cryptography

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
30/03/2021		First Issue	Fakhrul Adli Mohd Zaki Dr Farizah Yunus

CONTENTS

INSTRUCTIONS.....	1
TASK 1: Installing A Hash Checking Tool.....	2
TASK 2: Checking The Integrity Of The Downloaded File	6
TASK 3: Installation Of Encryption Tool	13
TASK 4: Sharing A Public Key And Encrypting A File	23
TASK 5: Decrypting An Encrypted File	31

INSTRUCTIONS

Manual makmal ini adalah untuk kegunaan pelajar-pelajar Fakulti Teknologi Kejuruteraan Kelautan dan Informatik (FTKKI), Universiti Malaysia Terengganu (UMT) sahaja. Tidak dibenarkan mencetak dan mengedar manual ini tanpa kebenaran rasmi daripada penulis.

Sila ikuti langkah demi langkah sebagaimana yang dinyatakan di dalam manual.

Arahan laporan makmal:

- a) Pelajar perlu menyediakan laporan makmal untuk aktiviti makmal.
- b) Kandungan laporan makmal mesti terdiri daripada beberapa tangkapan skrin untuk semua tetapan makmal keselamatan maya yang berjaya dengan beberapa penjelasan.
- c) Jawab semua soalan refleksi untuk setiap sesi makmal.
- d) Pelajar dapat memberikan senarai rujukan untuk rujukan tambahan.
- e) Laporan makmal mesti dihantar dalam masa yang diberikan menggunakan pautan yang disediakan di platform eLearning.

This laboratory manual is for use by the students of the Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu (UMT) only. It is not permissible to print and distribute this manual without the official authorisation of the author.

Please follow step by step as described in the manual.

Lab report instructions:

- a) *Students need to prepare lab report for lab activities.*
- b) *The contents of the lab report must consist of several screenshots for all successful setting of virtual security lab with some explanation.*
- c) *Answer all the reflection questions for every lab sessions.*
- d) *Student can provide the list of references for extra references.*
- e) *Lab report must be submitted within the time given using the provided link in the eLearning platform.*

TASK 1: INSTALLING A HASH CHECKING TOOL

OBJECTIVE

To download and install a hash checking tool

TASK DESCRIPTION

The student is required to download a hash checking tool known as HashTools from the given link. Then, student needs to install it to their computer. This tool later will be used to check the integrity of the downloaded program in Task 2.

ESTIMATED TIME

30 Minutes

STEPS:

1. Using your web browser, go to <https://www.binaryfortress.com/HashTools/Download/> to download a tool that has been equipped with various hash functions such as CRC32, MD5, SHA1, SHA256, SHA384 and SHA512.
2. Click the button as shown in the below screenshot:

The screenshot shows the HashTools Download page. The browser address bar displays <https://www.binaryfortress.com/HashTools/Download/>. The page header includes the HashTools logo and navigation links: Home, Download, Screenshots, FAQ, Discussions, Advanced Settings, Donate, and Help. The main content area is titled 'HashTools Download' and describes the tool's capabilities. A red box highlights the 'Download Installer Now' button, with a red arrow pointing to it and the text 'Click this button'. Below this is a banner for 'Take Back Your Inbox!' and a 'Download without Installer' section.

HashTools Download

HashTools computes and checks hashes with just one click! Supports CRC32, MD5, SHA1, SHA256, SHA384, SHA512 and SFV's, as well as integration into the Windows Explorer context menu for one-click access. Click the 'Download Installer Now' button below to begin using HashTools.

HashTools works with these versions of Windows:

- Windows 10, 8.1, 8, and 7 SP1 (32-bit and 64-bit)
- Windows Server 2019, 2016, 2012 R2, 2012, and 2008 R2 (32-bit and 64-bit)

Download Installer (recommended)

- Latest Version: v4.3 (5 MB)
- Release Date: November 26, 2019

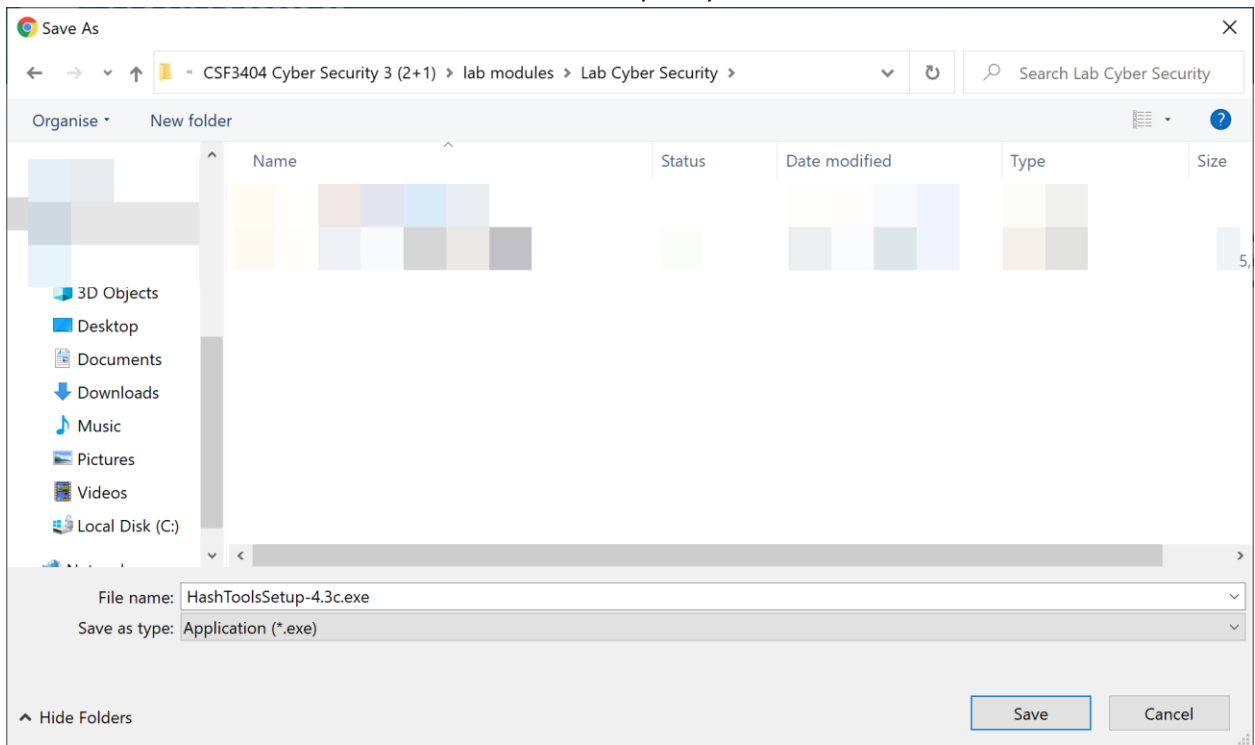
Download Installer Now

FROM THE MAKERS OF displayfusion Take Back Your Inbox! CHECKCENTRAL Discover a better way to handle email notifications TRY FREE!

Download without Installer

- Latest Version: v4.3 (3.1 MB)
- Release Date: November 26, 2019

3. Save the file at a suitable location where it is easy for you to find it later.

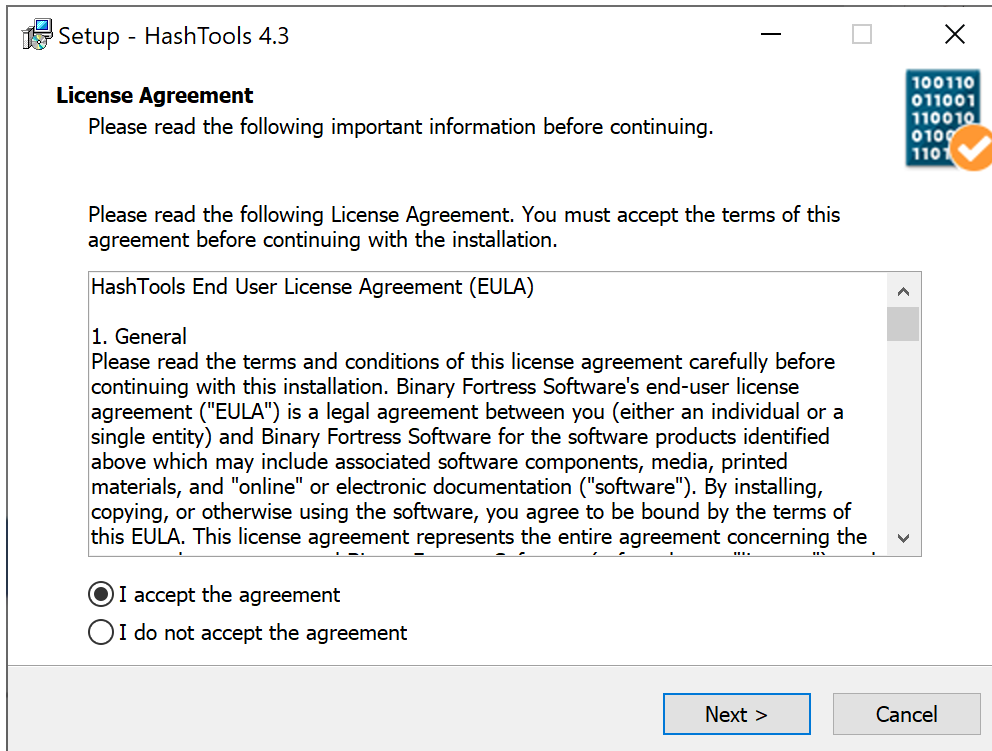


4. After finish the download, you may simply click on the installer icon

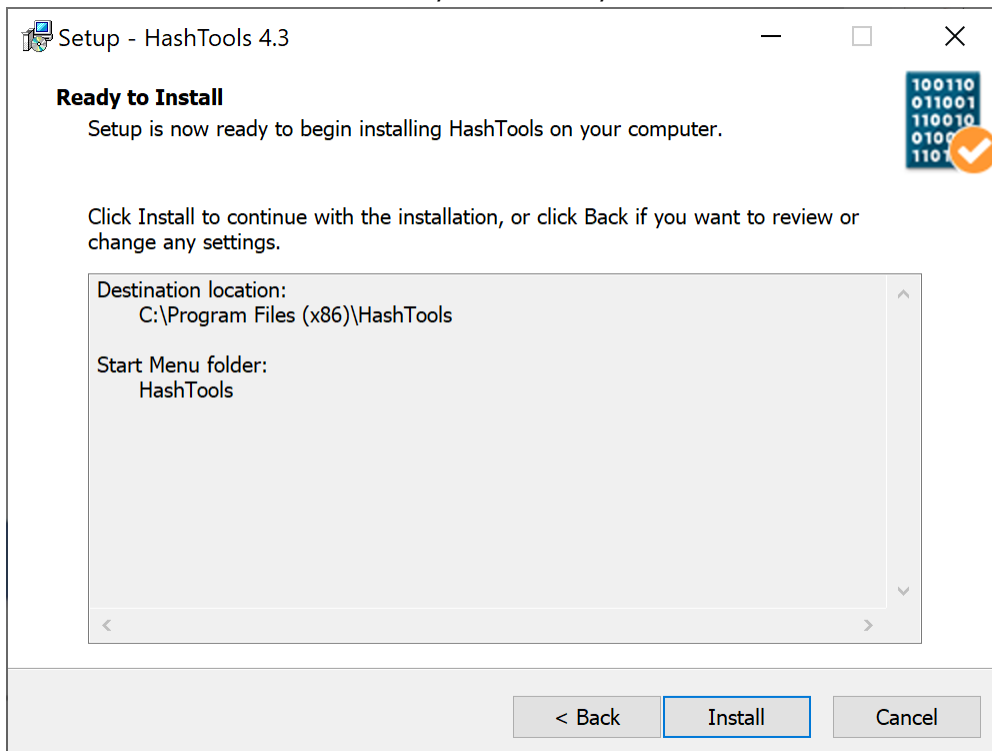


to install the program on your computer.

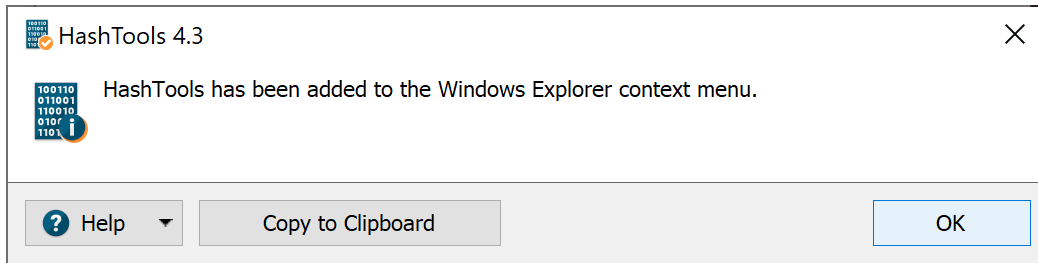
5. When the installer runs for the first time, it will show you a screen of the License Agreement. Accept the agreement and then click **Next**.



6. Click on the **Install** button when you are ready to do so.

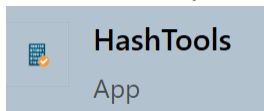


7. After the installation complete, a notification window will be shown.

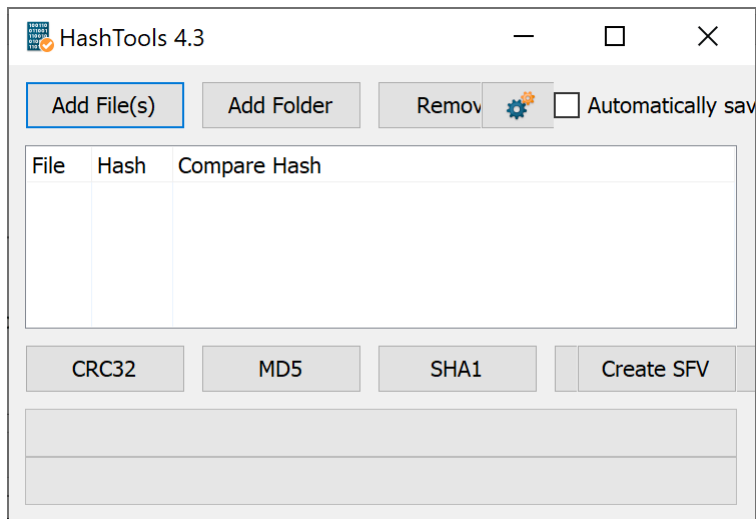


8. If you want to run the installed program, simply click on its icon.

Note: You could find the icon on your desktop screen or by searching it from the Windows search bar on your computer.



9. If you see the following screen, then your installation is successful. Well done and get ready for the next task.



REFLECTION QUESTIONS

- | |
|--|
| 1. List four examples of hash algorithms. |
| 2. What is the issue with the MD5 algorithm? |
| |

TASK 2: CHECKING THE INTEGRITY OF THE DOWNLOADED FILE

OBJECTIVE

To verify the integrity of the downloaded file by using a hash checking tool.

TASK DESCRIPTION

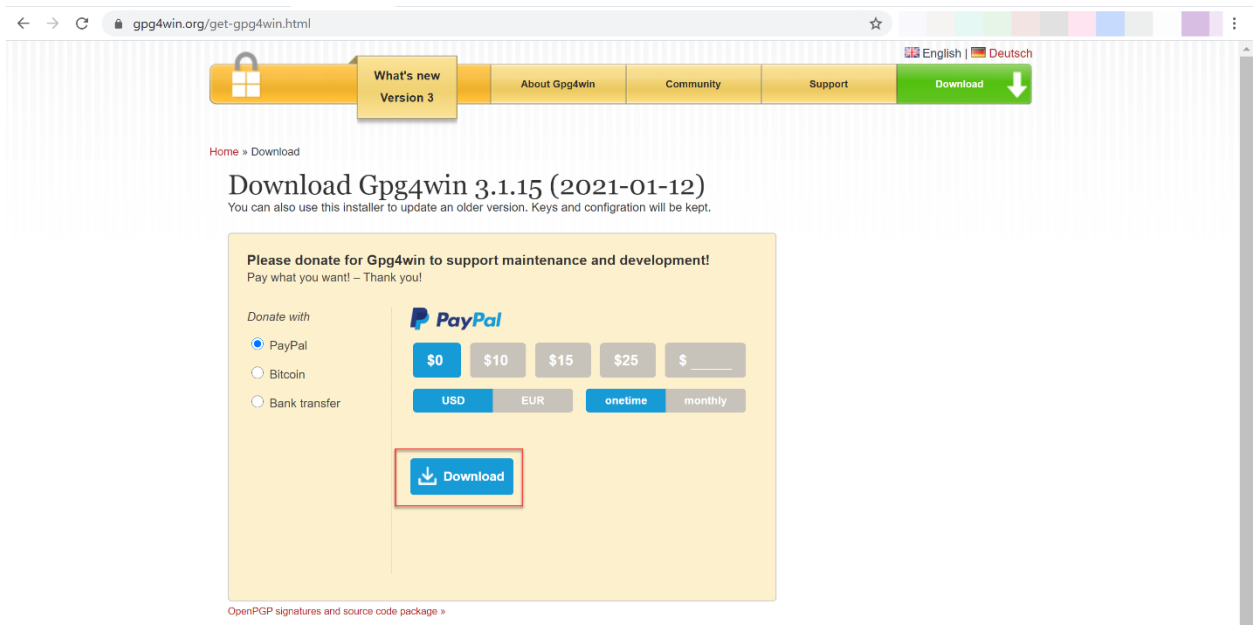
The student needs to download an encryption software known as Gpg4win. This software supports the cryptography standards such as OpenPGP and S/MIME(X.509). Before installing it, the student is required to check the integrity of the program file by using the tool downloaded in Task 1.

ESTIMATED TIME

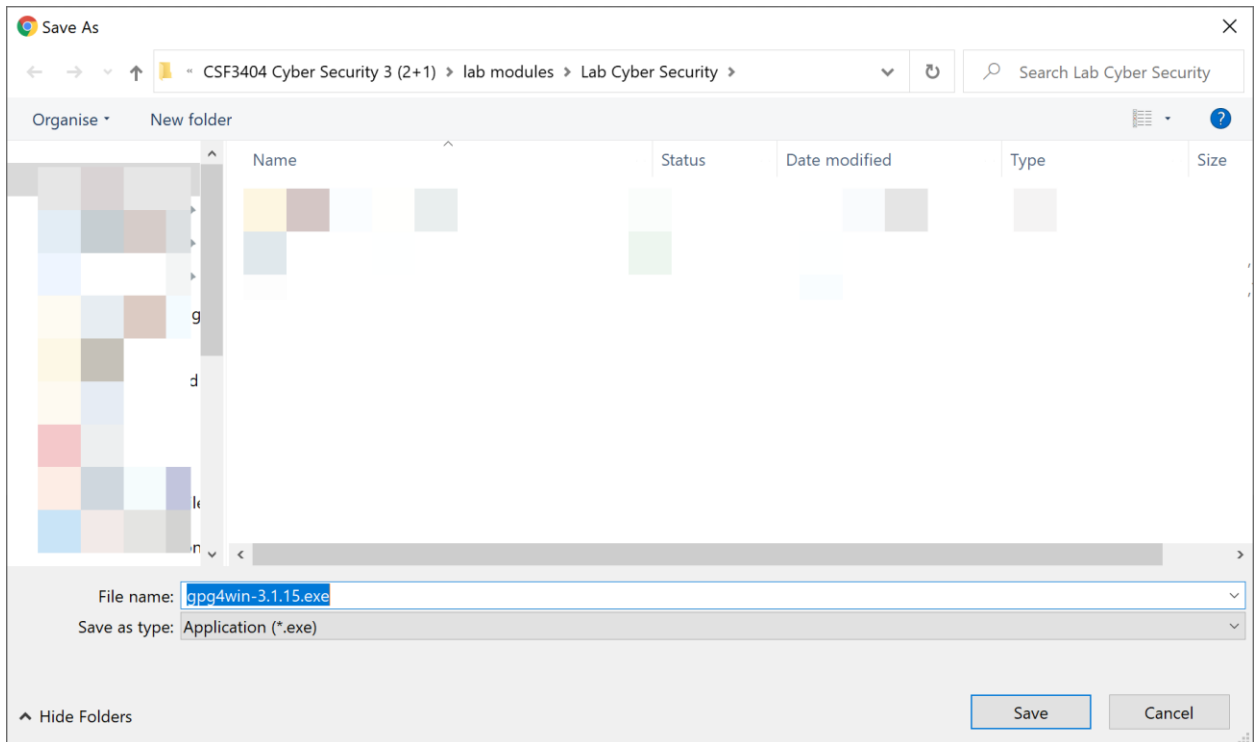
30 Minutes

STEPS:

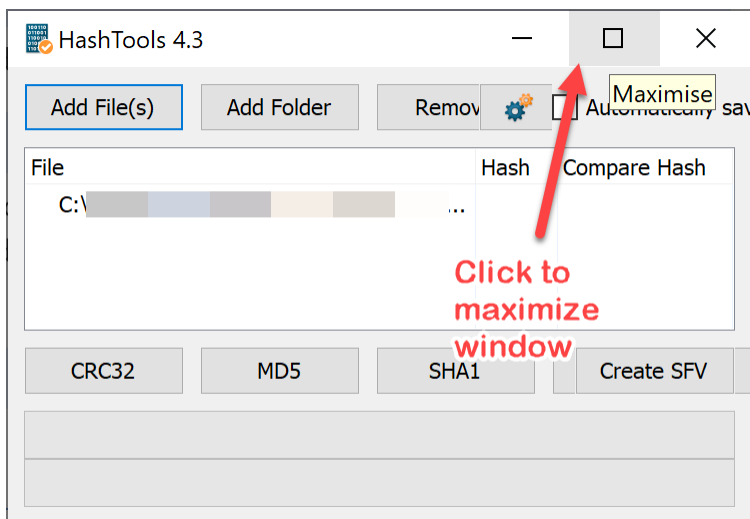
1. Type this URL <https://www.gpg4win.org/get-gpg4win.html> at your browser address bar and hit **Enter**. You will see a screen as below. If you plan to donate, you may choose any amount shown. However, for the simplicity of this task, just choose \$0, then click **Download**.



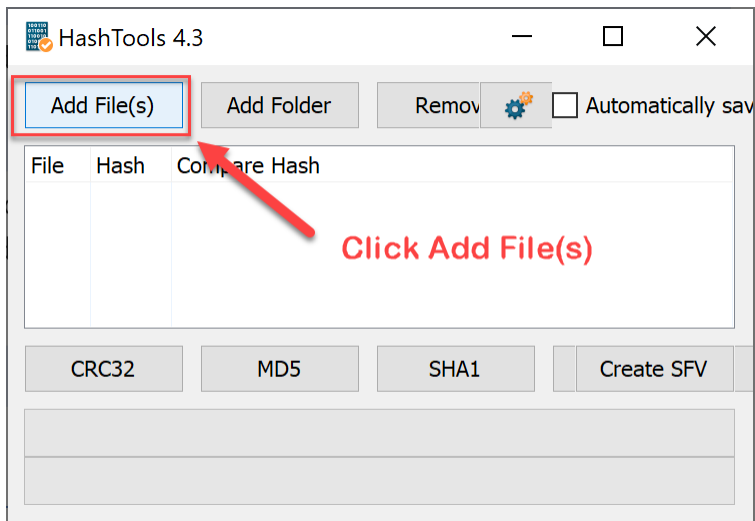
2. Now, save the installer at a suitable location.



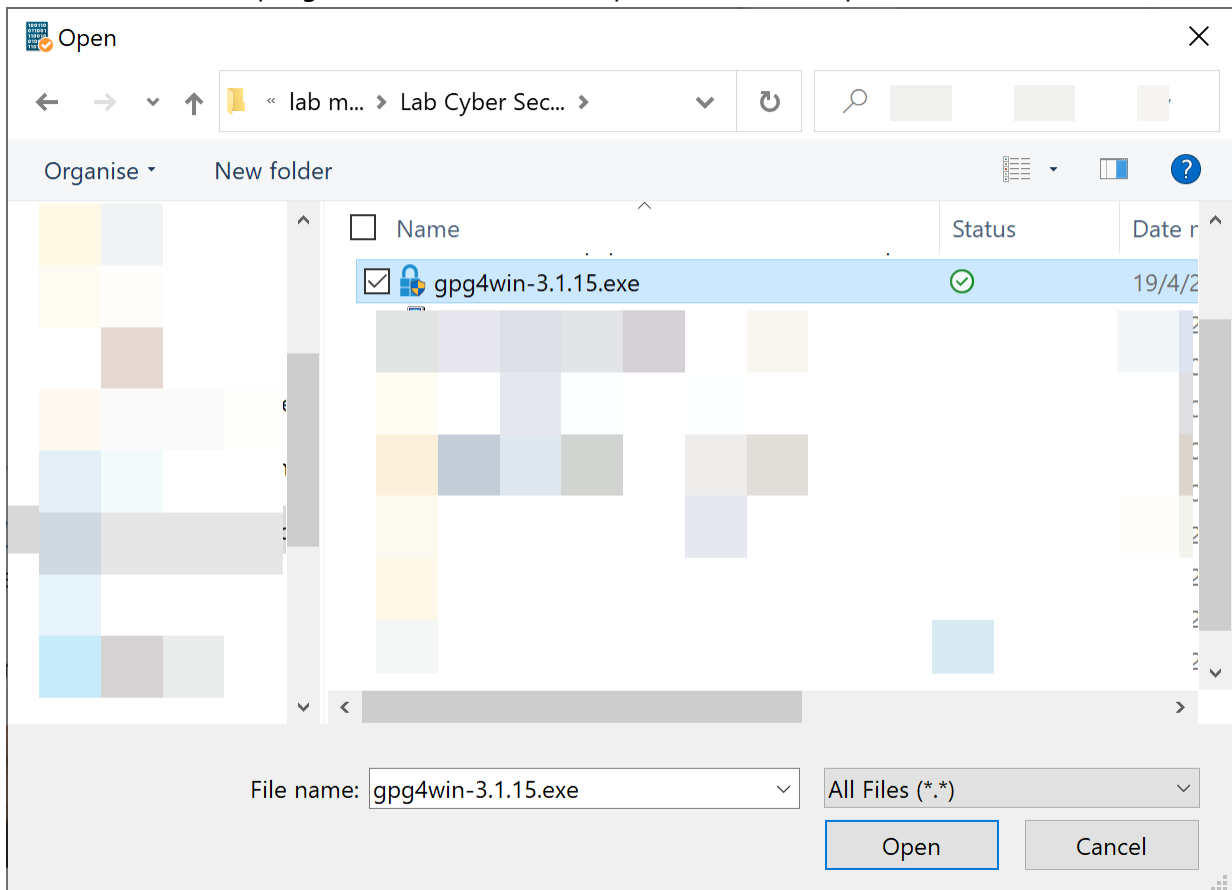
3. Wait until the download complete. **Do not run the installer** yet because we need to verify the checksum first. By checking the checksum (which refers to a value of the message digest of the installer), we can make sure that we have downloaded the verified version and not the version tempered by an attacker.
4. Run the HashTools that has been installed before. Click maximize windows to get a better view.



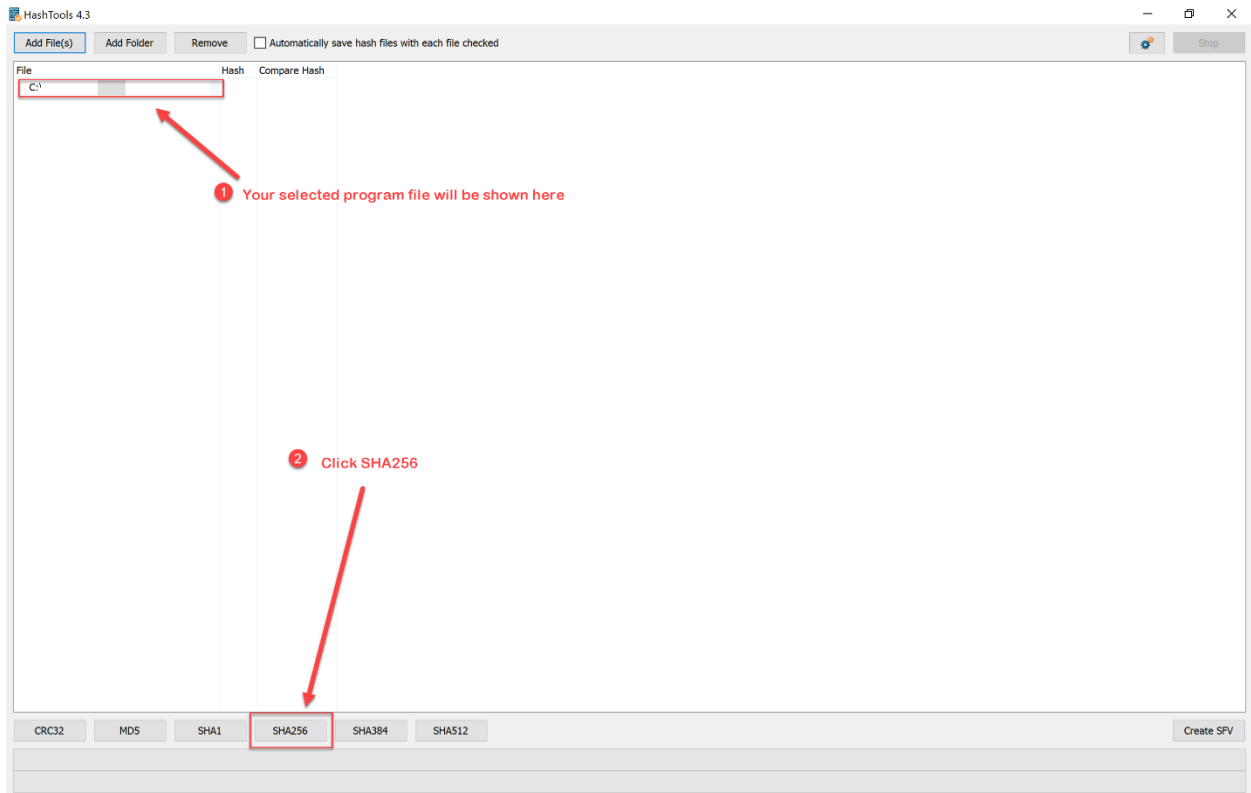
5. Then, click on **Add File(s)** button.



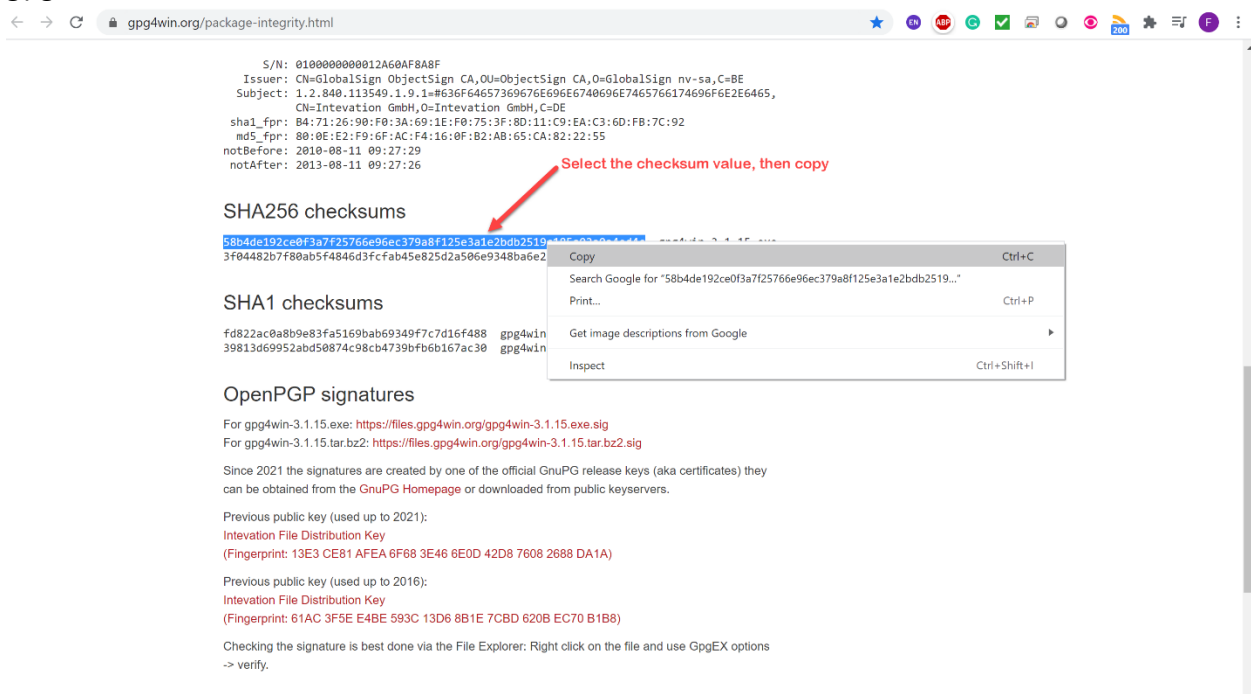
6. Select the installer program from the location you choose in Step 2.



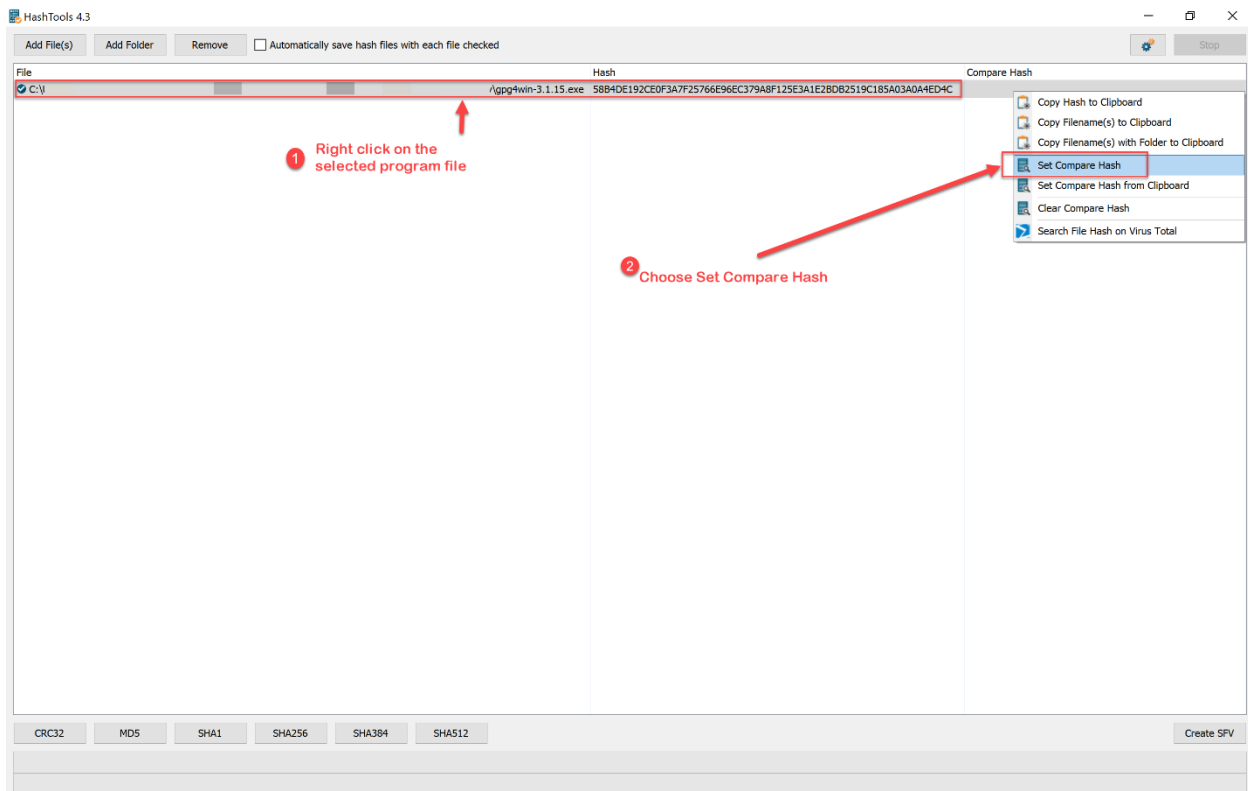
7. Your selected program file will be shown on the HashTools windows. We are going to use the SHA256 hash function to get the hash value (message digest) of the installer. Click on the **SHA256** button.



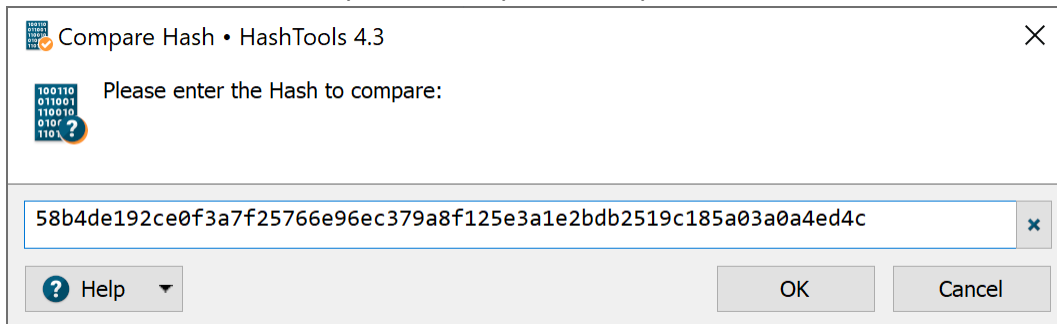
8. As a result, you will see the computed hash value at the column **Hash** on the HashTools window. Next, we need to retrieve the hash value from the gpg4win website.
9. Go to <https://www.gpg4win.org/package-integrity.html>, scroll down until you see the hash value located at the **SHA256 checksum** section. Select and copy the hash value for gpg4win-3.1.15.exe.



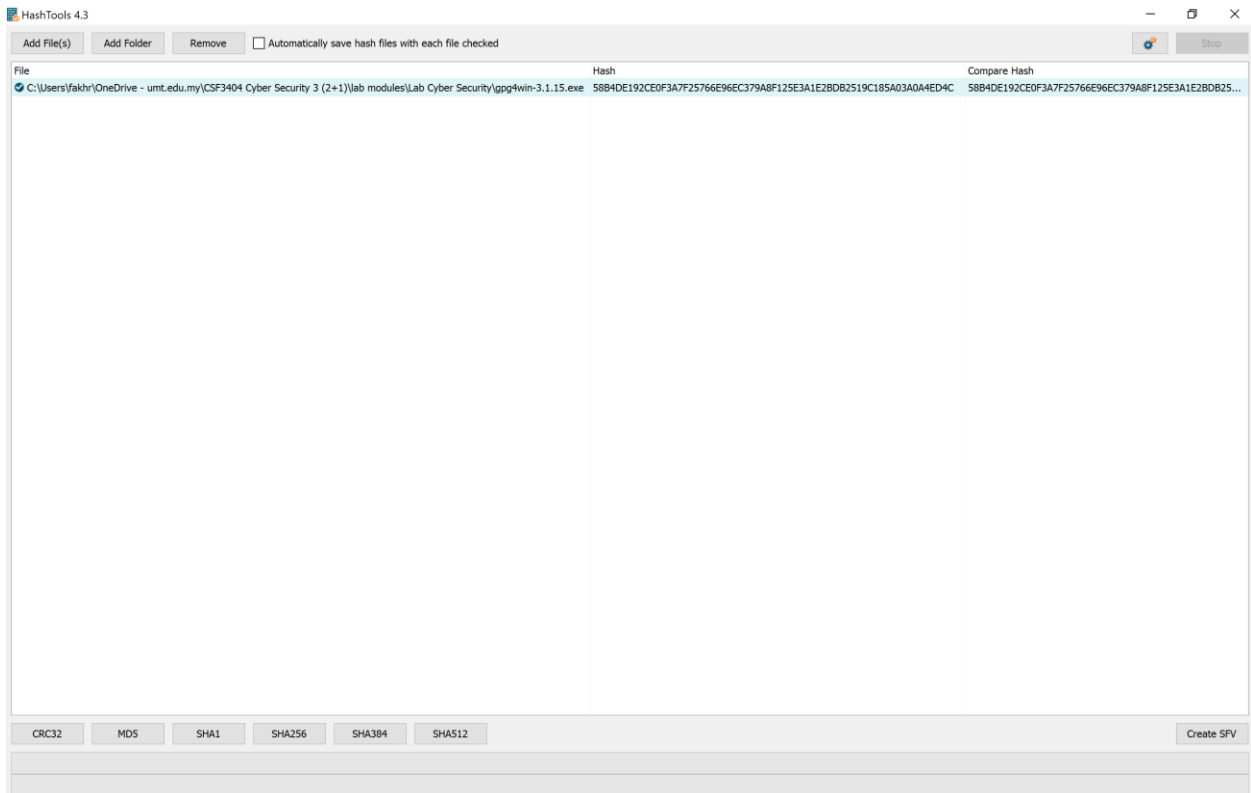
10. Now, go back to the HashTools screen. Follow the steps as shown in the screenshots below:



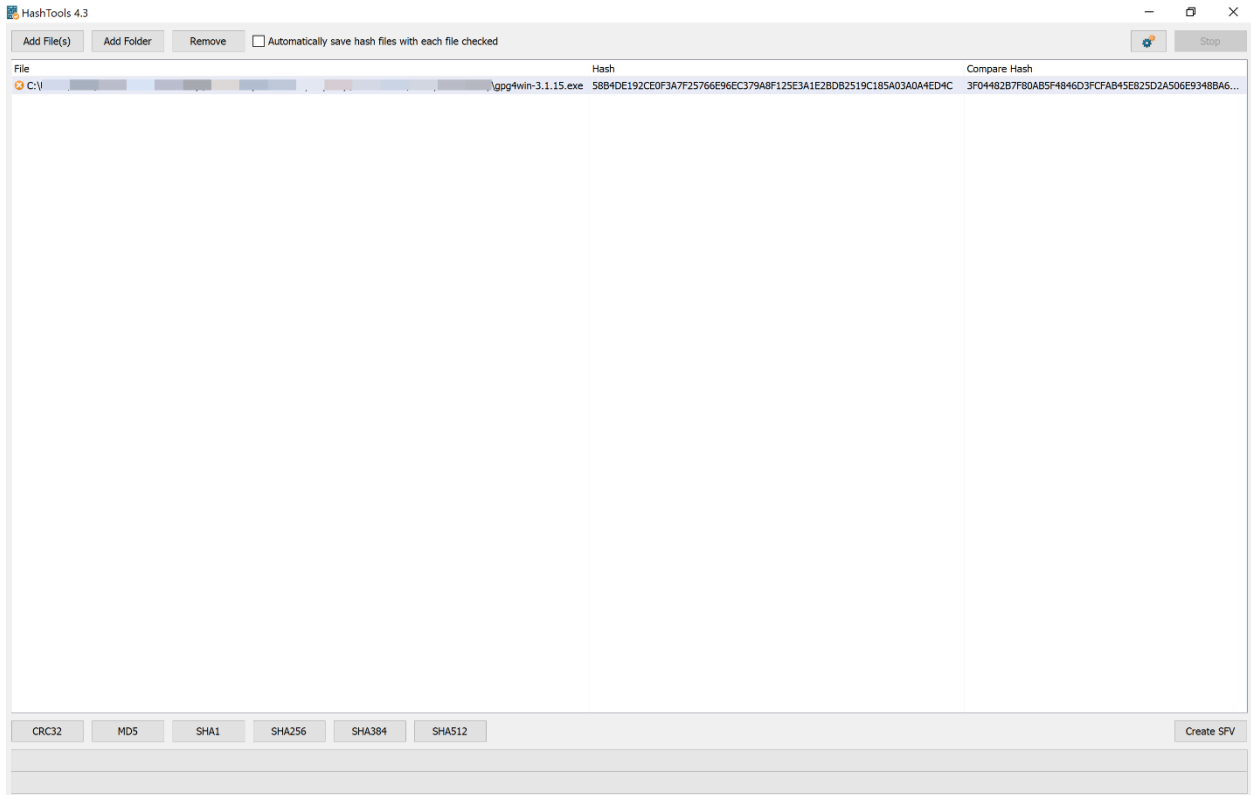
11. Paste the hash value that you have copied in Step 9. Click **OK**.



12. If the values are the same, then you will see a light green colour highlighted with a tick mark on the left. This also means we have downloaded the verified version of the installer software and nothing for us to worry about.



13. Otherwise, if the hash values are different, you will see a screen similar as follows:
Note: Try to copy a different hash value to get a similar result as shown on the screenshot below.



14. Print screen the result of these activities and put it into your lab report.

15. Now, we are ready for the encryption tool installation in Task 3.

REFLECTION QUESTIONS

1. Describe the functionality of hashing encryption compared to symmetric and asymmetric encryption.

TASK 3: INSTALLATION OF ENCRYPTION TOOL

OBJECTIVE

To install and set up the encryption tool.

TASK DESCRIPTION

For this task, the student will install the encryption tools using the installer downloaded in Task 2. This tool later will be used to experiment with the encryption and decryption process.

ESTIMATED TIME

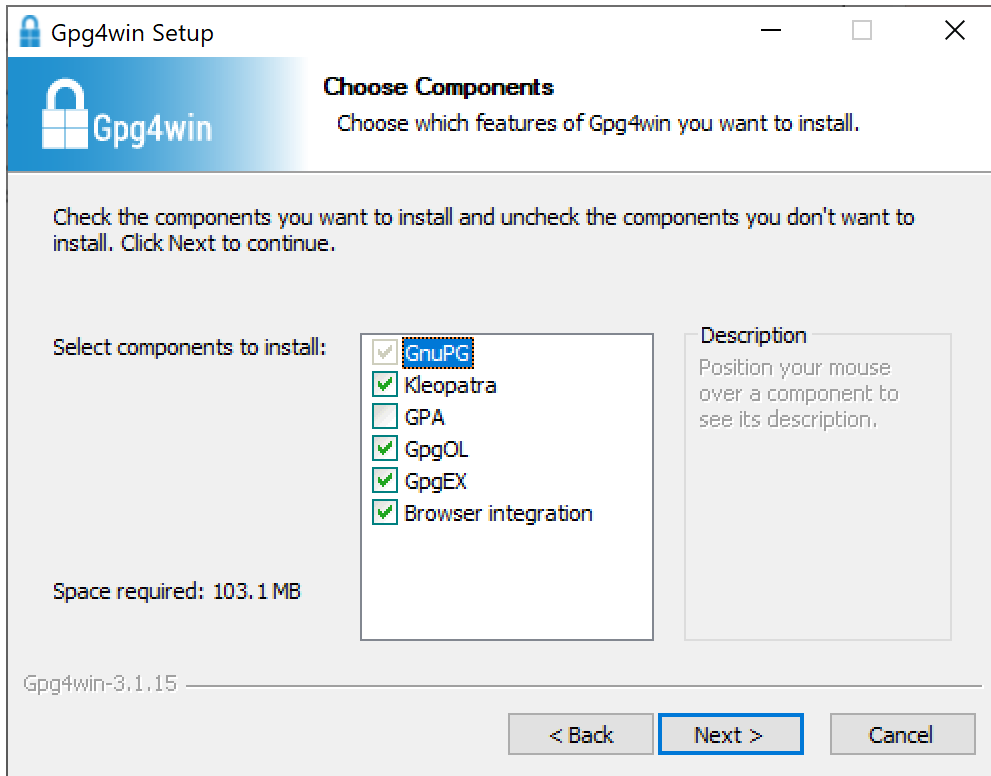
30 Minutes

STEPS:

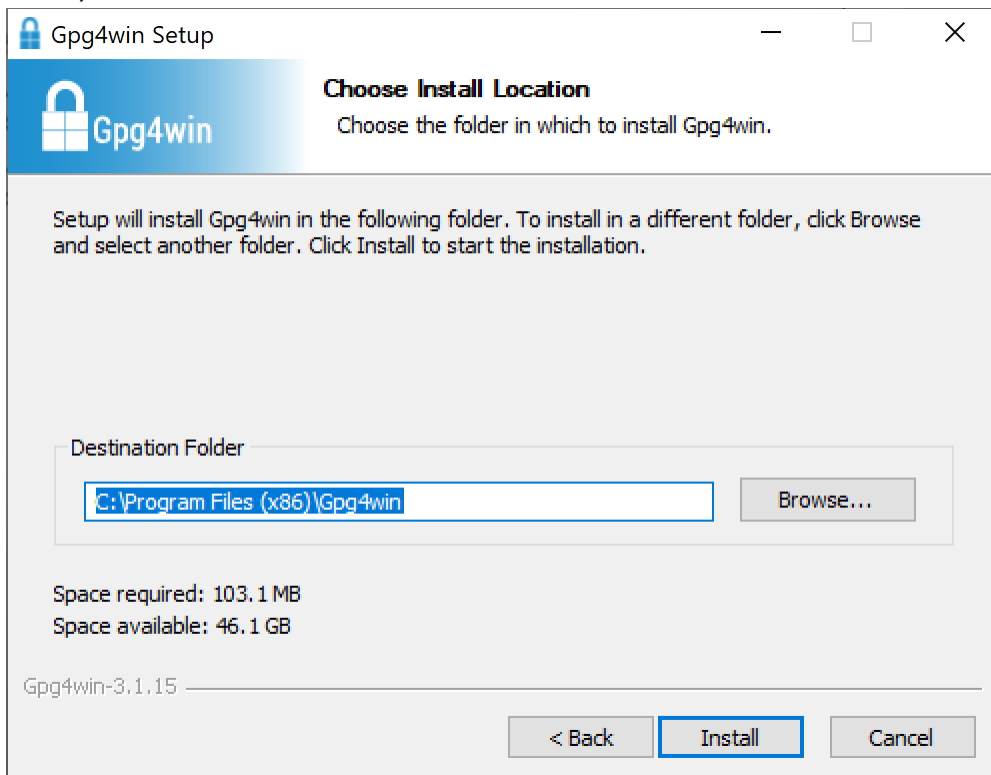
1. To begin the installation, go to the location of **gpg4win** installer. Then, double click on it.
2. You will see a welcome screen as following, then click **Next**.



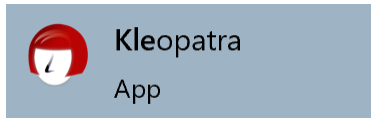
3. Make sure **Kleopatra** is selected as one of the components to be installed.



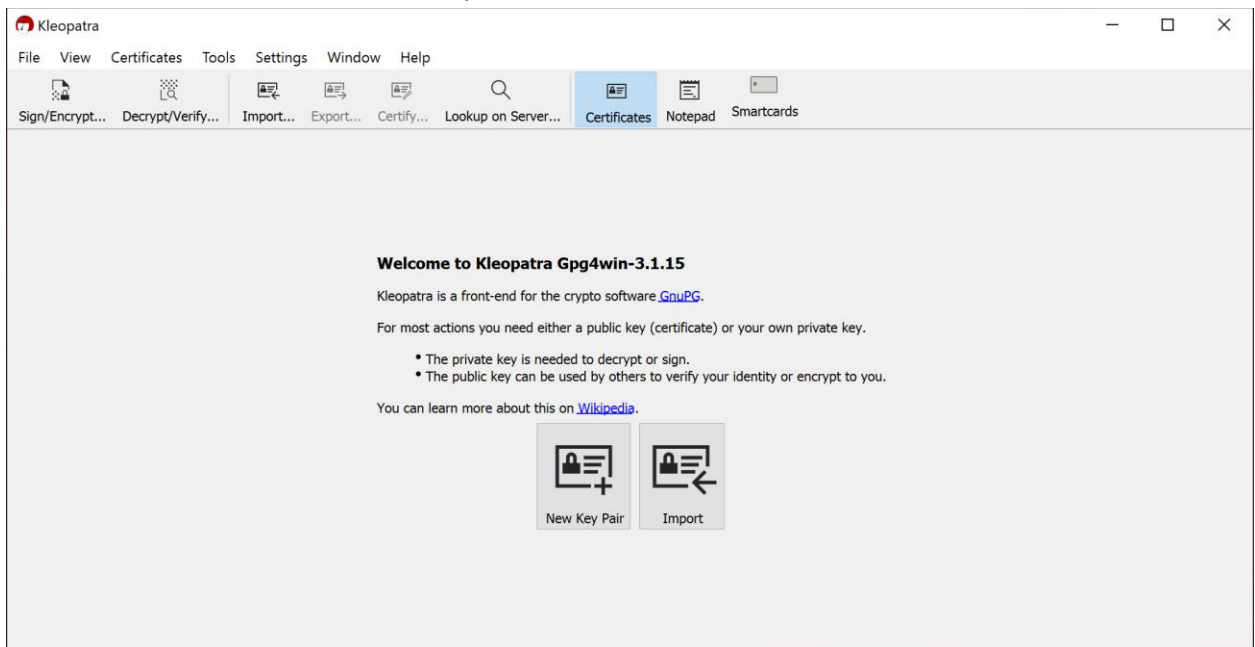
4. Finally, click on the **Install** button. Wait until the installation finish.



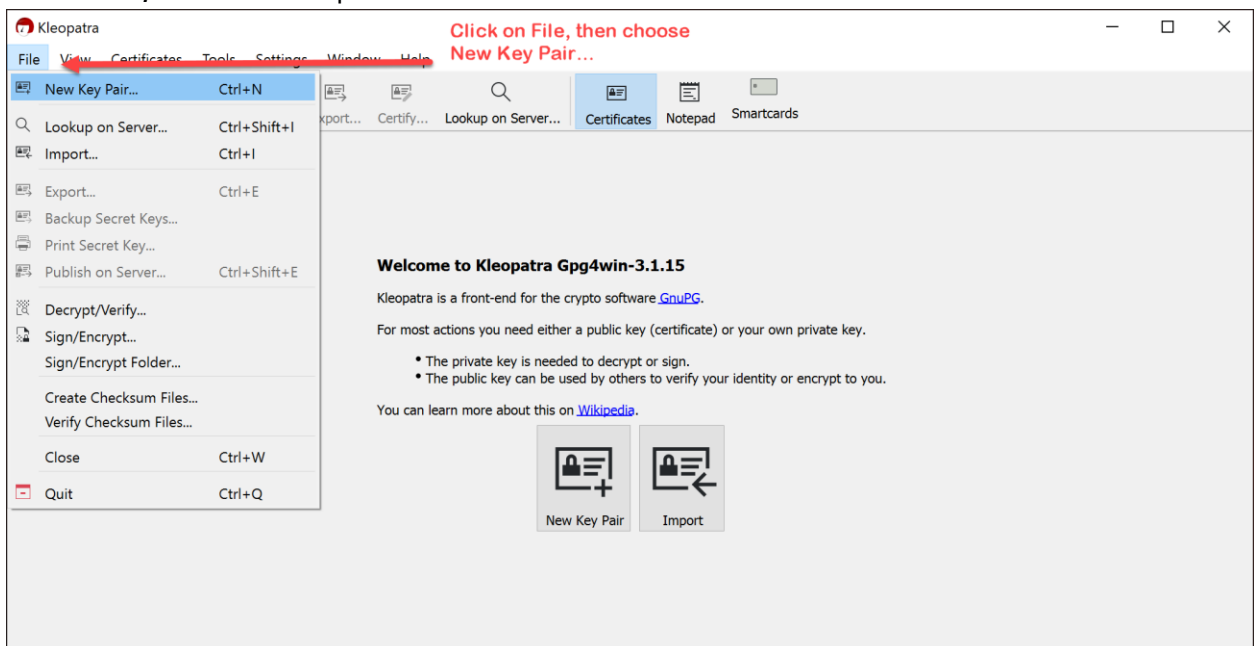
5. After the installation complete, run the Kleopatra program by double-clicking the icon



6. You will see the first screen of Kleopatra as follows:



7. Next, we are going to get our public and private key. These keys will be generated by the gpg module that we have installed earlier.
8. To do that, follow the steps shown in the screenshots below:



9. Now, we are going to choose the format for our key pair. Choose **OpenPGP** key pair.

← Key Pair Creation Wizard

Choose Format

Please choose which type you want to create.

→ **Create a personal OpenPGP key pair**
OpenPGP key pairs are certified by confirming the fingerprint of the public key.

→ **Create a personal X.509 key pair and certification request**
X.509 key pairs are certified by a certification authority (CA). The generated request needs to be sent to a CA to finalize creation.

Next

Cancel

10. Fill the form with your matric number and email. Then, click **Advanced Settings**.

← Key Pair Creation Wizard

Enter Details 1 **Fill in the name and email with your matric number**

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

Name: (optional)

EMail: (optional)

☐ Protect the generated key with a passphrase.

CS12345 <CS12345@gmail.com>

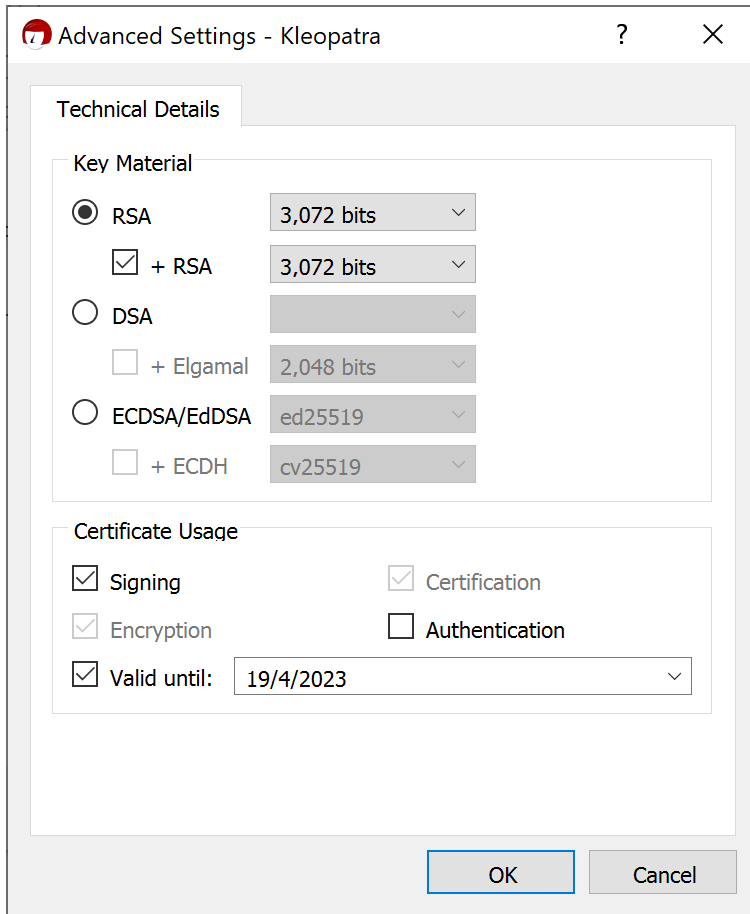
2 **Click Advanced Settings**

Advanced Settings...

Create

Cancel

11. At the **Advanced Settings** screen, we can set the size of our keys. We are going to choose 3072 bits and using the RSA algorithm. Click **OK**.



The image shows a screenshot of the 'Advanced Settings - Kleopatra' dialog box. The window has a title bar with a red icon, the text 'Advanced Settings - Kleopatra', and standard window controls (help, close). The main content area is titled 'Technical Details' and contains two sections: 'Key Material' and 'Certificate Usage'. In the 'Key Material' section, 'RSA' is selected with a radio button, and its key size is set to '3,072 bits'. There is a checkbox for '+ RSA' which is checked, also with a '3,072 bits' key size. Other options include 'DSA' (unselected), '+ Elgamal' (unchecked, '2,048 bits'), 'ECDSA/EdDSA' (unselected, 'ed25519'), and '+ ECDH' (unchecked, 'cv25519'). In the 'Certificate Usage' section, 'Signing' and 'Encryption' are checked, while 'Certification' and 'Authentication' are unchecked. The 'Valid until' field is checked and set to '19/4/2023'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Advanced Settings - Kleopatra

Technical Details

Key Material

- ☒ RSA 3,072 bits
- ☒ + RSA 3,072 bits
- ☐ DSA
- ☐ + Elgamal 2,048 bits
- ☐ ECDSA/EdDSA ed25519
- ☐ + ECDH cv25519

Certificate Usage

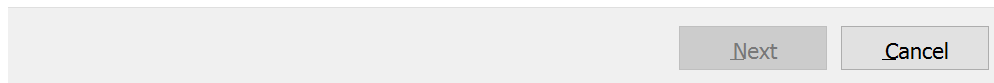
- ☒ Signing
- ☒ Certification
- ☒ Encryption
- ☐ Authentication
- ☒ Valid until: 19/4/2023

OK Cancel

12. This will take us back to the **Key Pair Creation Wizard** screen, then click **Create**.
13. Wait until the key generation process complete.

Creating Key Pair...

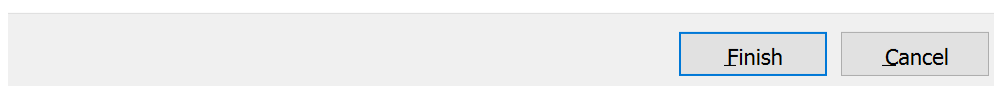
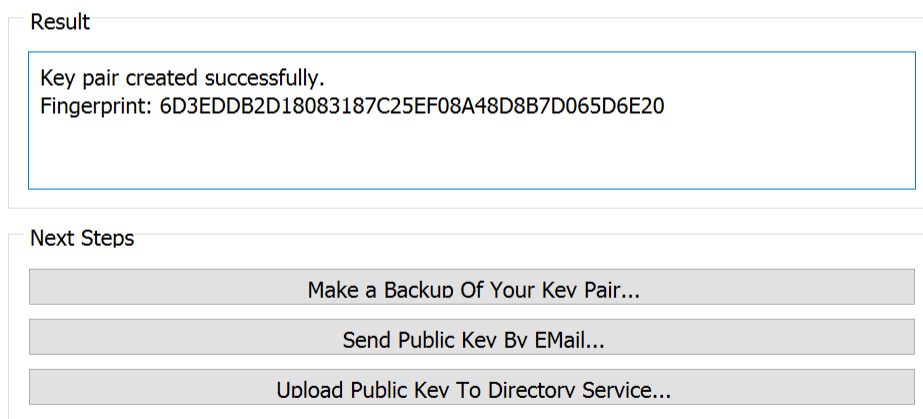
The process of creating a key requires large amounts of random numbers. This may require several minutes...



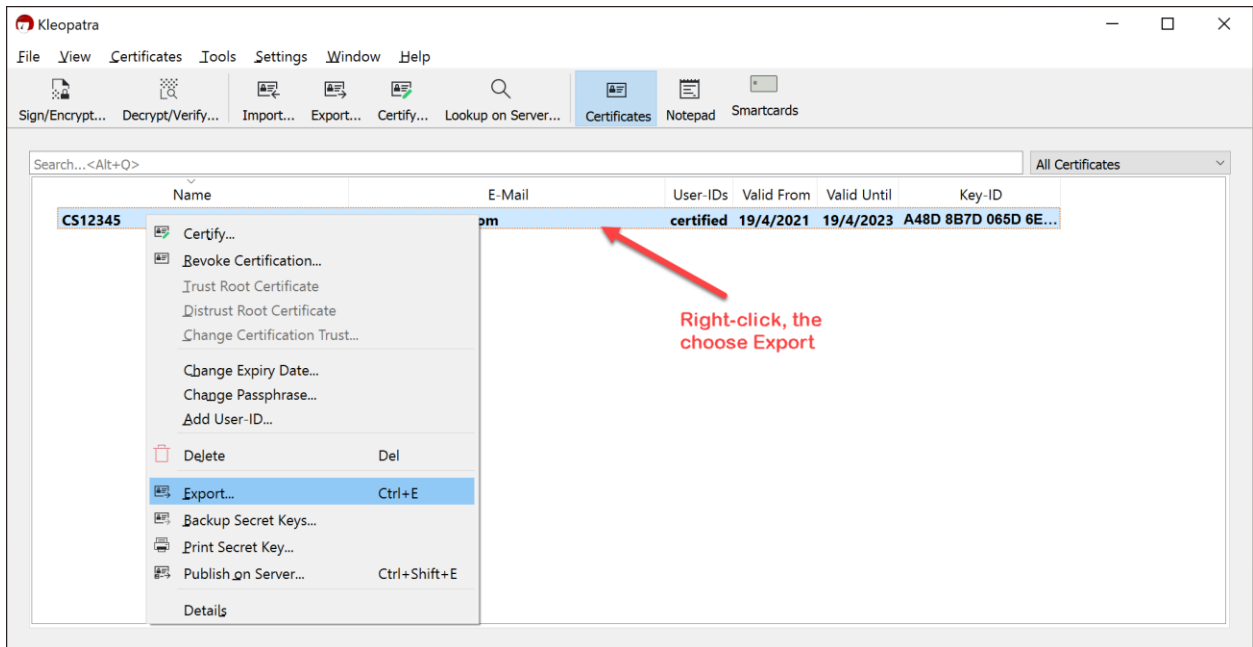
14. Once the key pair is ready, a window below will appear. Click **Finish** to close the window.

Key Pair Successfully Created

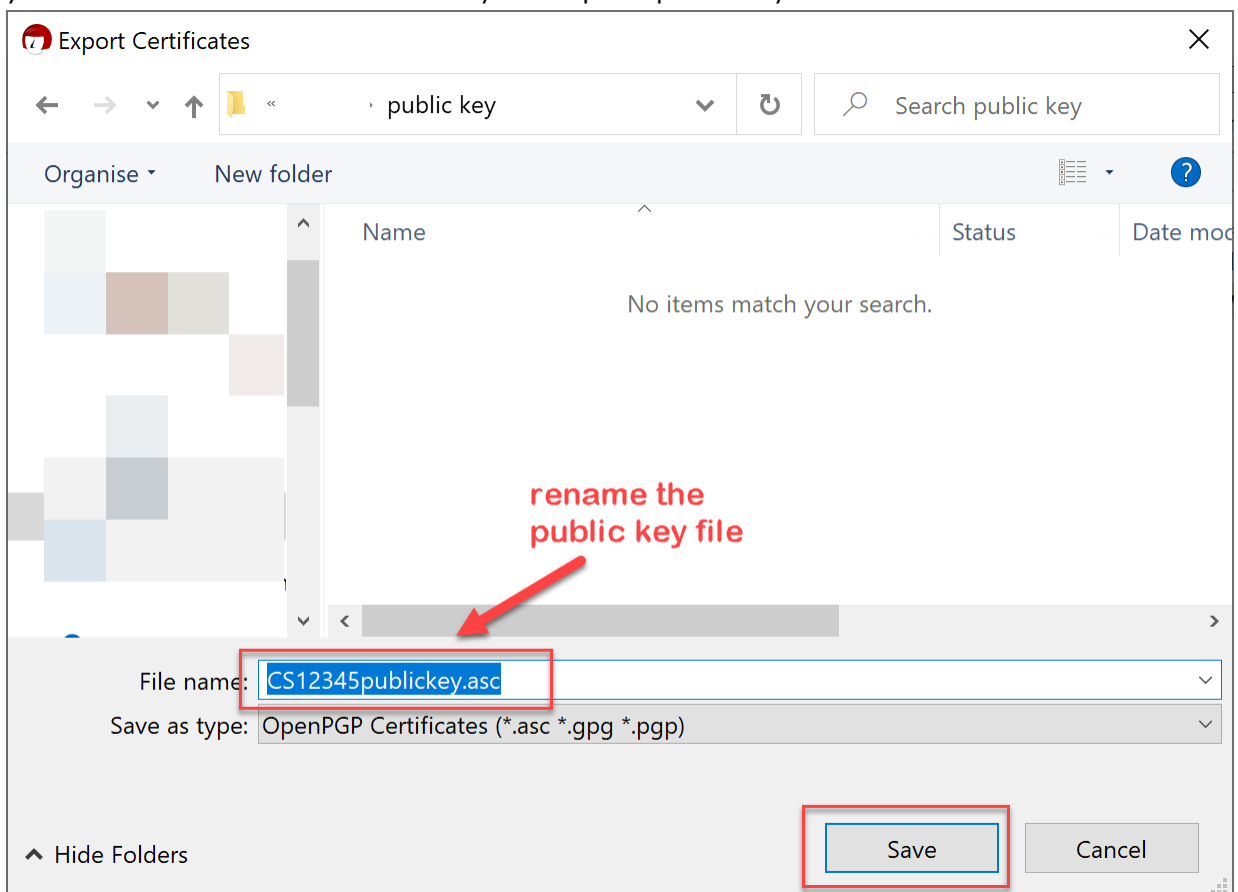
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.



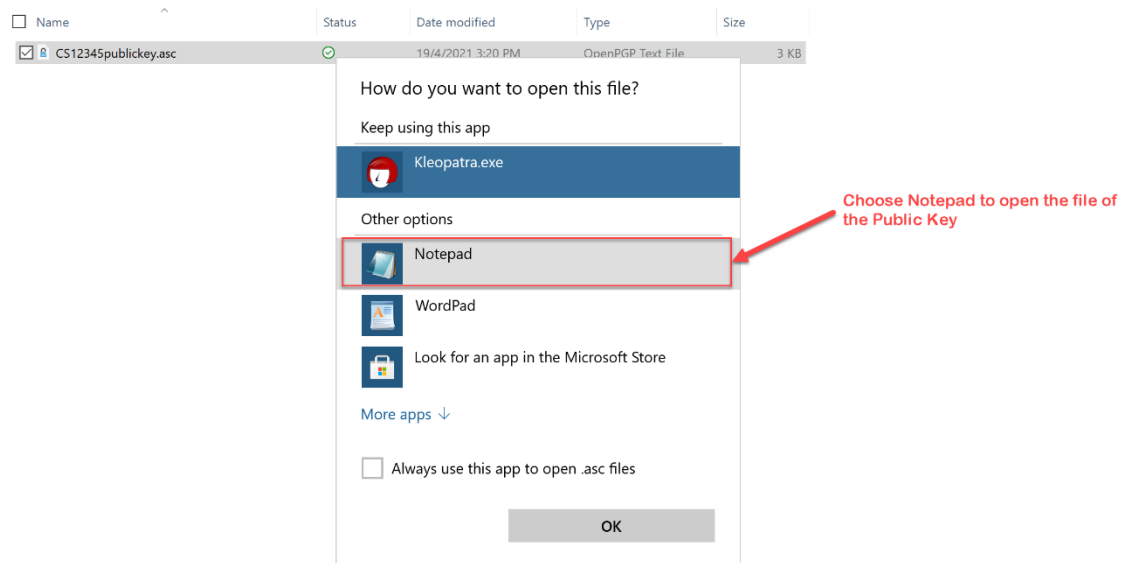
15. Next, we are going to export our public key to a file so that it can be shared with others. Follow the step on the following screenshot:



16. Re-name the public key using this format **[YourMatricNumber]publickey.asc**. Make sure you take note of the location where you keep the public key file.



17. We can use Notepad as an editor to view our public key file. You can do that by right-clicking on the file name, then choose Notepad.



18. Take a screenshot of the content of your public key file and put it into your lab report.
Example of a public key shown on the screenshot below:

CS12345publickey.asc - Notepad

File Edit Format View Help

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQGNBGB9LgQBDADe8WcsuqiEFVsIndwFqknPCSY5rN2de3tD6NN/dAjULW8KixpU
nndULjQsi8udRB8ujz0naIq9I4K7EWIIhNp4d/Zduf/MugyUm1Xo8OKIu1V1yeHB
EHUWopdV/R9MFkoZqHzBkM5WJYJFQbN7LiBKYPqRqDWG9UJh3aDa97VcUky58YCaQ
qdYcjoF9xAtTv7Vc1dQ8/kszzddqLDm8MjbPZIZwKuRmbSdiKVzyXXPktvnzqJuP
wxfvUbk9TWOIXScSLfEMBidhnLO2MPk0LCBa+vOUdgFv/doe49ftJe39+1elQ2g
DsashdcUlo+nVKxej4yJry+DNmAaoVxBIRKvd5/3LbvqR1iJi2H3KEhsvB3R8mHY
u+NswTaWoxtkmJ58Y4K96LXX0PdHbRcWxWqdTHp89V3uuow3AG9J0JY/EUKRB8VP
rsod4gynGcMHAfXwKzafLskvaiSDYJvEkH0sUsJJHfT7rXnlw4rN8oQLxbPCuDE/
sbQGdw0289M85pcAEQEAAbQbQ1MxMjM0NSA8Q1MxMjM0NUBnbWFpbC5jb20+iQHU
BBMBCAA+FiEEbT7dstGAgxh8Je8IpI2LfQZdbiAFAmB9LgQCGwMFCQPCOTwFCwkI
BwIGFQoJCASCBYCAwECHgECF4AACgkQpI2LfQZdbiCfkAv/ShZC/V2LuHn6tVlt
cUOXkoPyqe9cJ/y4YNhjHBgFV9RtJirVTgEty3Dw1RCZWpwqT3ZWMAN8o92VxPs1
zcafa/wJtfn01sMSOzHGZi5+2I3jKuySm9S/oj5Hjfdbj2er4Wsm83Xkg/ndoK/v
l40/ETP/fc7p99Plj7HjcOfGtvJfEl8vXQV5tdBAPSOKqrWqbf9GL3no5I4aGnn9
KK+51TZnjzEayTMnE8hI+yJdDTwCdjimJgfc1cUhPmjtqJOAqnjzvWD8ipY/1JhR
3anFLMs1k8hE5ctzCd58i8nDsE+YwW0GP1zKvU0cfj7ID6FvyT9w1c263lYmBsVs
yNmjyj5Njb8fNgroEgak+1a8fo7QE/TBcgV5IUt5RYkvmAm9IAqrsGdEr26kyakg
0mMKoJ9shvoAL5w7wchXGZxahEidgl2fzXBGb/c1LdyejTYGpgthRl/Asm3QLD0C
xniI8X/qZQYrRvnAy8e1hgePu+hb2htbBpmALYUwDswyk50HuQGNBGB9LgQBDAC7
DhD4hsghnrXuo9nKQ2w5gL/F9mB6H70/hPIg/04KWjL6PStyvkkawmYeIcQbCjz4
BjOGRgsVtZQPGAWvcQj2EUoS5Xqdd+MKJtJzt14LoGRVv2v3EmOV4LggQRqlcF5V
ADC28kRjRA0oP/XHJukm72Ut5M0mt5gPVDs-fm3JOCyoFz6kIB3CmUp8oKxDjyXrH
uS0gf6GgzHfzx0Yur5Q83arfdKuZemUXTNdAOAvnGdN4IFsBnRbnWR92+K5J2Wu
yQeAmRmqHR26YnuH5vDT58HiVgzKzqk5s+rjYZ2AJwTWSywt7t3tsJvIVEqNHWrn
98jiBYCuse2tKQiF/E6V5SBXJKUx2IV3h2Hx8WnqoVkJpxM8sMCE1+hEsCDxNY9A
C/+avvJSASrVPSieS7usKA+jDfp7V9Bm+YiJG8Pybuy6hD5jjMy+Hq2QbL5Wz+U8
fLZJNKbgILkqipLAXc5ws/AFTUUKxC9GCSkIbu+hNql8K+haPznd58vuYBh1DPEA
EQEAAYkBvAQYAQgAJhYhBG0+3bLRgIMYfCXvCKSNi30GXW4gBQJgfs4EAhsMBQkD
wjk8AAoJEKSNi30GXW4giwMAJMF1/mL0HvjEoqcRxfgzQR0pcN81aVAwhv0IsWY
1qnXHpyR77wtFdkhk1u+CTpQm/3lstr3E0kUDgl5z9g03u8/IHdjwUh5n0a478FC
ZQYKn/7wqvK/iYeg/Imka1tEFwK2UiR5nBzU62XqriFO6EdCus7wxI2cEdZDH1EY
R7VJr/2UXFfq2kPanPztm2YmwDFk84Qc5N4+AWmnk+m1GzRn8jOCckjRsFHDEFoJ
l3Ica8N0pZeK6qutAf9Ncc51fV5i3KGDwwIEvAleH9J/pfBIY03eT/4nghAi0ZJo
awb4/KOccxHUinyQuu+qPEJ8RXHwXS9CCbeUR9Ebwz2pHVNqc3dW7z1bzoEpxSC7
4zXJ20WthPVS/RFqr1iFOP1xNr8/idCwfPkgJxPx0Yb/e7cHTVQHY85xzFcb70an
gYKdMvbGZ82ekM9zJm1SeENK2aim/9nOYbrkpmUdmVpJm40Quv0+2Hw3NpChBTY4
pU4o/xsr+eggnsPceQSxaNrwsQ==
=tNZb
-----END PGP PUBLIC KEY BLOCK-----
```

19. Keep the public key file in a safe place. We will use it in the next task.

REFLECTION QUESTIONS

- | |
|--|
| 1. What is the meaning of GPG? |
| 2. Using your own words, explain the difference Between PGP and GnuPG? |

TASK 4: SHARING A PUBLIC KEY AND ENCRYPTING A FILE

OBJECTIVE

To share and use the public key for encryption.

TASK DESCRIPTION

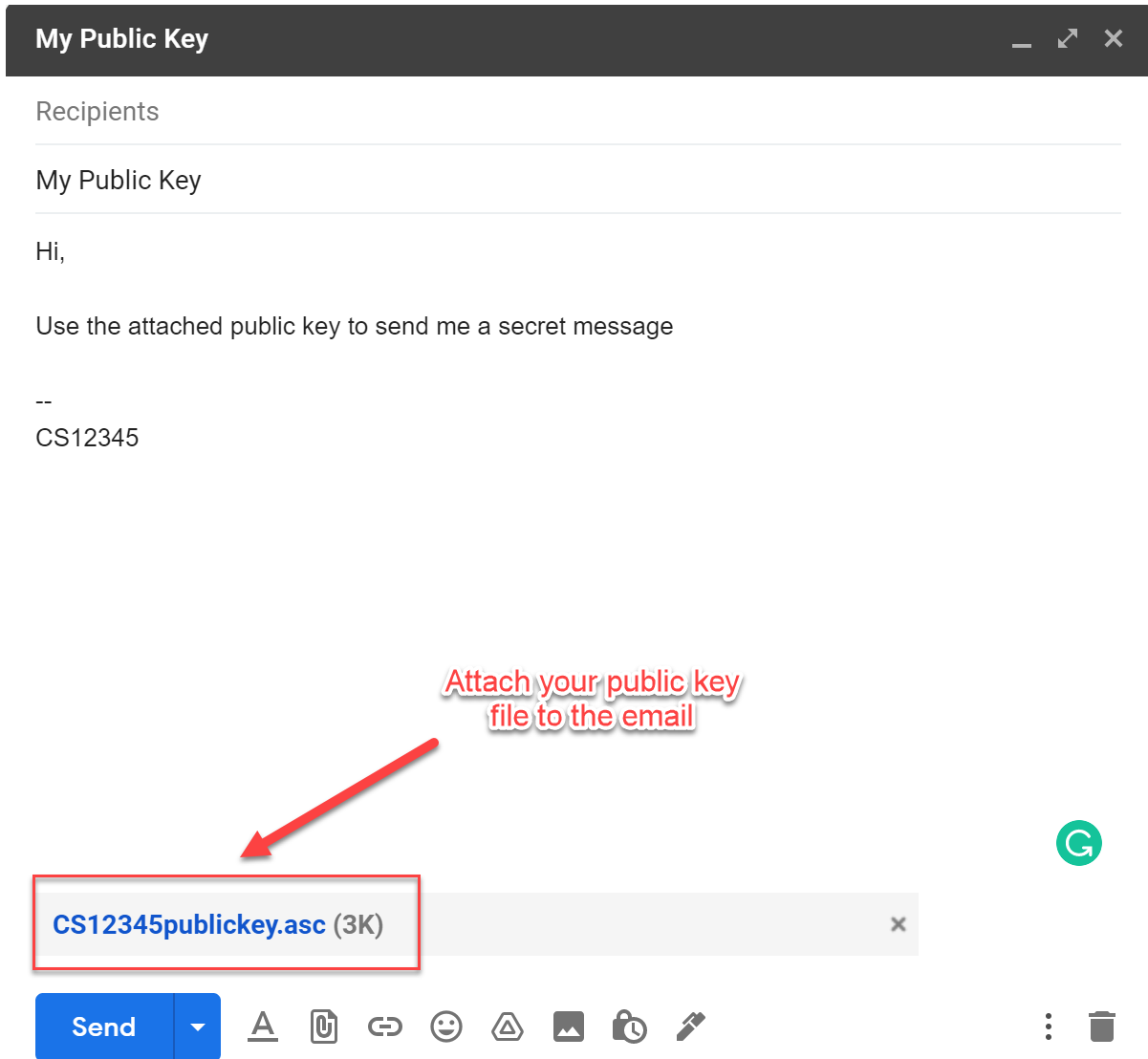
The student is required to share their public key with his/her friend through email communication. Next, the student will encrypt a file with a secret message by using his/her friend's public key, then send it through email.

ESTIMATED TIME

60 Minutes

STEPS:

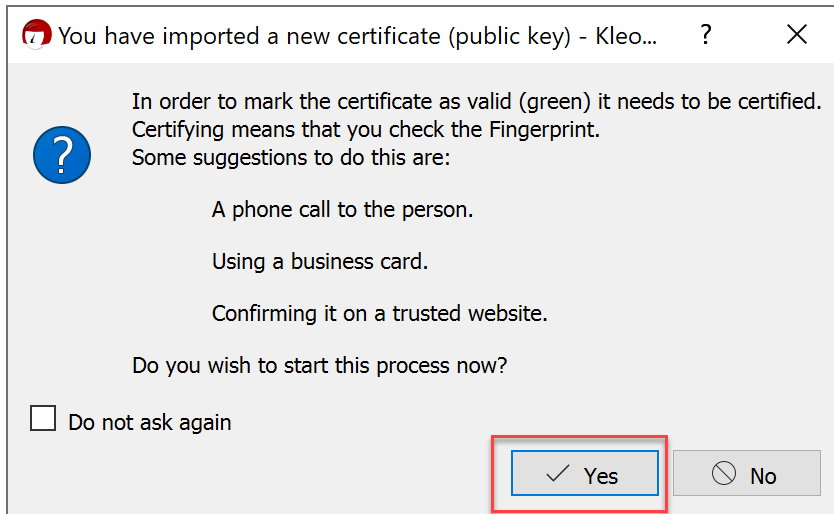
1. For this task, we are going to work in pair. We will begin by sending an email to our friend along with the public key attached. Open your email editor, write a simple message, then attach the public key file that you have created in the previous task.



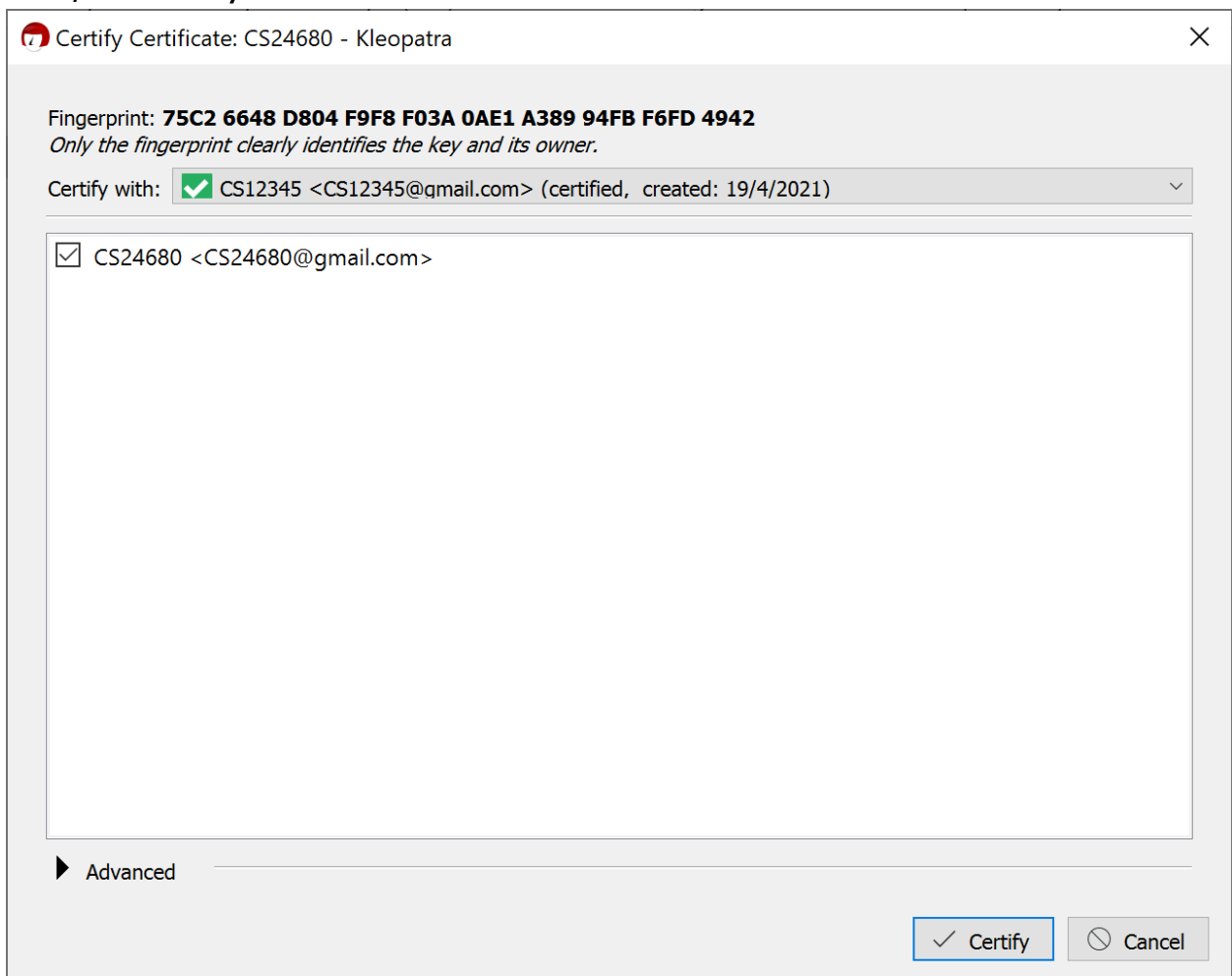
2. After receiving a public key from your friend, download the key file into a safe place. **Double click** on the file so that it can be imported and saved by Kleopatra.

<input type="checkbox"/> Name	Status	Date modified	Type	Size
CS24680publickey.asc			OpenPGP Text File	3 KB

3. Before proceed, Keoplatra will ask you to check the fingerprint. Simply click **Yes**.



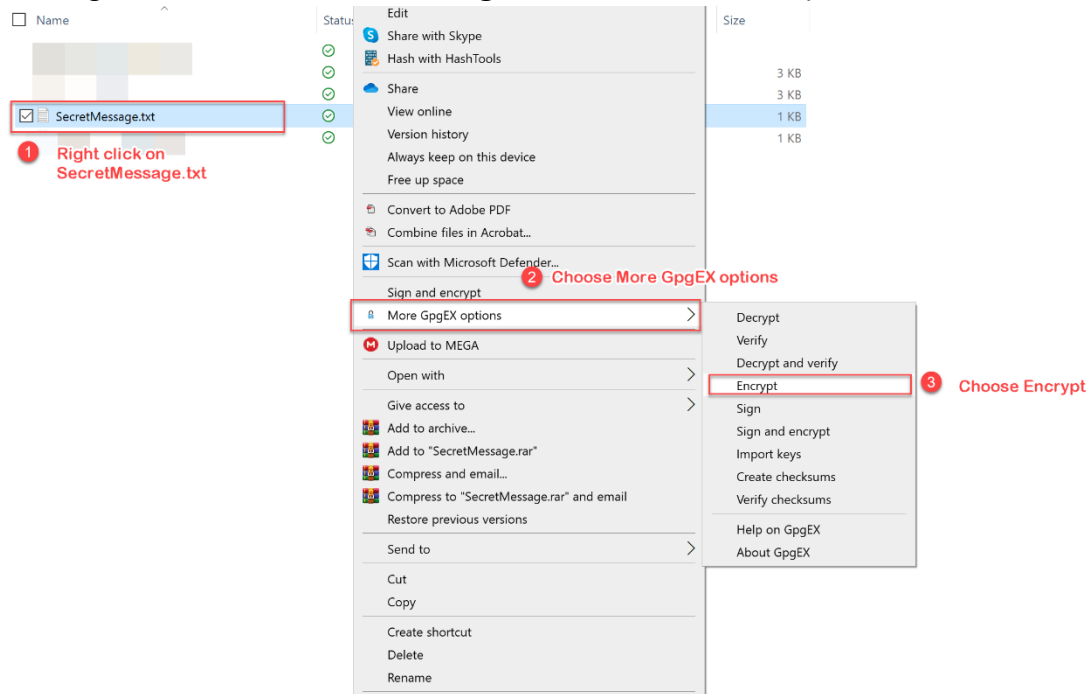
4. Then, click **Certify**.



5. At this moment, your friend's public key is ready to be used for encryption.
6. Next, we are creating a text file with a secret message. Open a Notepad then type this phrase "This is a secret message from [Your Matric Number]". Save the file as

SecretMessage.txt. Take a screenshot of the content of the file and put it into your lab report.

7. Now right-click on the **SecretMessage.txt** and follow the steps below:



8. Select the public key that belongs to our friend.

Sign/Encrypt Files - Kleopatra


Sign / Encrypt Files

Prove authenticity (sign)

☐ Sign as: ✓ CS12345 <CS12345@gmail.com> (certified, created: 19/4/2021)

Encrypt



☒ Encrypt for me: ✓ CS12345 <CS12345@gmail.com> (certified, created: 19/4/2021)

☒ 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.

 /SecretMessage.txt.gpg 

Encrypt Cancel

9. Choose the public key from the list, then click **OK**.

Certificate Selection - Kleopatra

Please select one of the following certificates:

All Certificates

Name	E-Mail
CS24680	CS24680@gmail.com
CS12345	CS12345@gmail.com

Choose recipient's public key from the list

OK Reload Import... Lookup... New... Close

10. Make sure the configuration looks similar to this before clicking on the **Encrypt** button.

Sign / Encrypt Files

Prove authenticity (sign)

☐ Sign as: ✓ CS12345 <CS12345@gmail.com> (certified, created: 19/4/2021)

Encrypt

☒ Encrypt for me: ✓ CS12345 <CS12345@gmail.com> (certified, created: 19/4/2021)

☒ Encrypt for others: ✓ CS24680 <CS24680@gmail.com> (certified, OpenPGP, created: 19/4/2021)

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

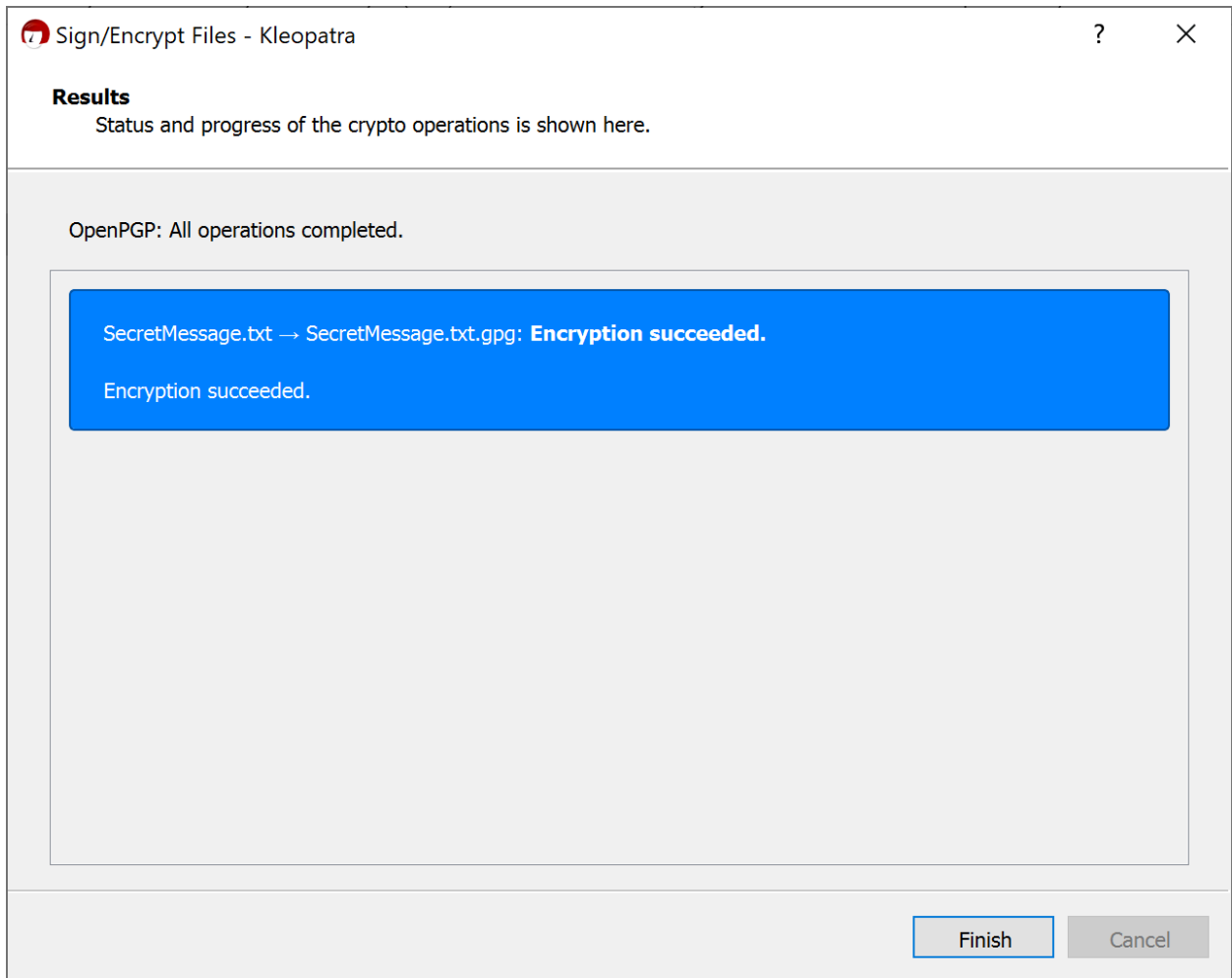
Output

☐ Encrypt / Sign each file separately.

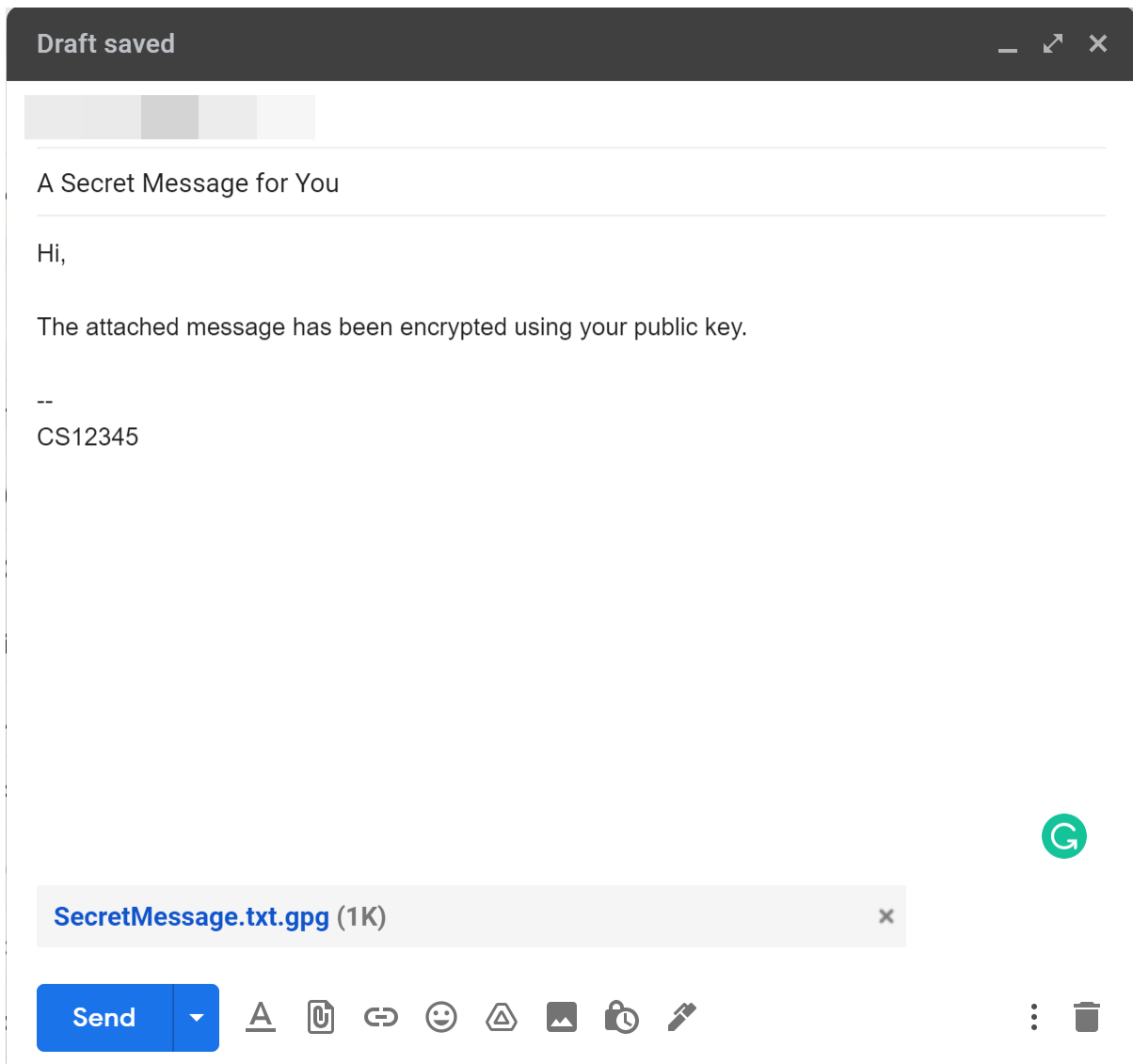
/SecretMessage.txt.gpg

Encrypt **Cancel**

11. After you click the Encrypt button on the above step, a message from Kleopatra will be shown:



12. Well done! We now have the secret file that can be sent to our friend.
13. Next, open your email editor again. This time, we will attach the secret message we have encrypted before.



14. During the process of sending the email, make sure you select the correct version of the secret message file. Select the one with a **.gpg** extension.

<input type="checkbox"/> Name	Status	Date modified	Type	Size
SecretMessage.txt		19/4/2021 4:34 PM	Text Document	1 KB
SecretMessage.txt.gpg		19/4/2021 4:33 PM	OpenPGP Binary File	1 KB

15. Send the email with the secret message to your friend. If you receive the email with a secret message from your friend, then you are ready for the next task, which is decryption.

TASK 5: DECRYPTING AN ENCRYPTED FILE

OBJECTIVE

To decrypt the encrypted file.

TASK DESCRIPTION

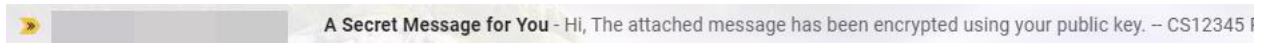
The student will decrypt the encrypted file by using their private key which has been managed and stored by Kleopatra software.

ESTIMATED TIME

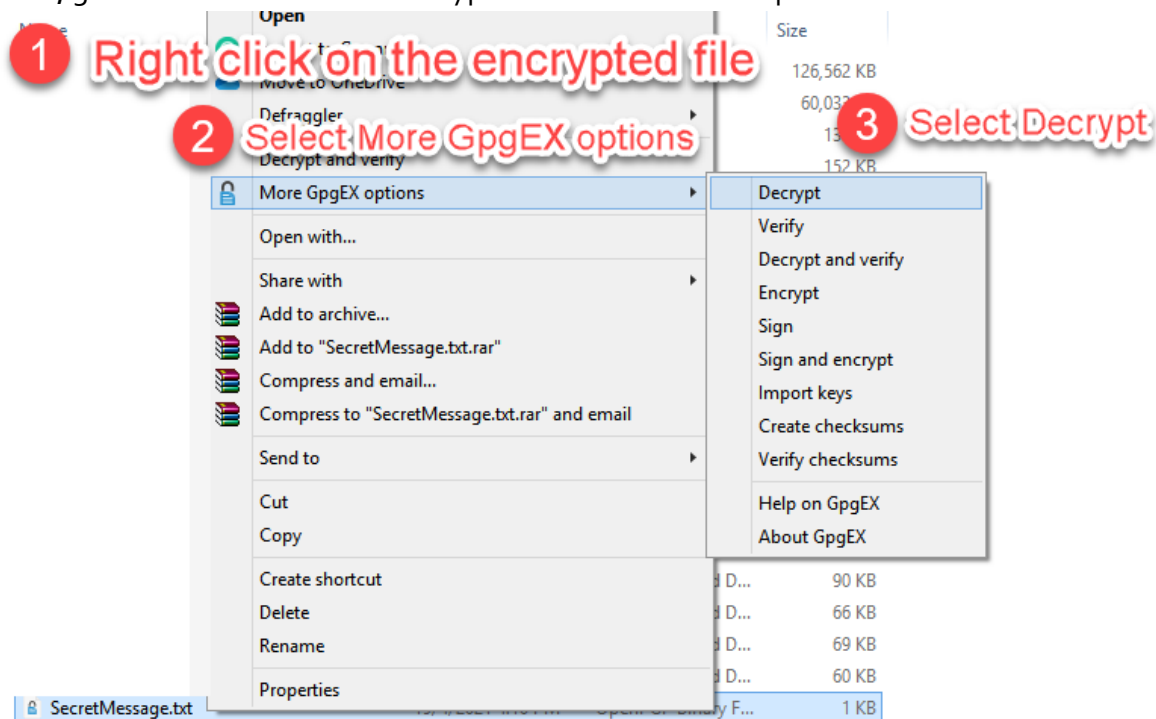
30 Minutes

STEPS:

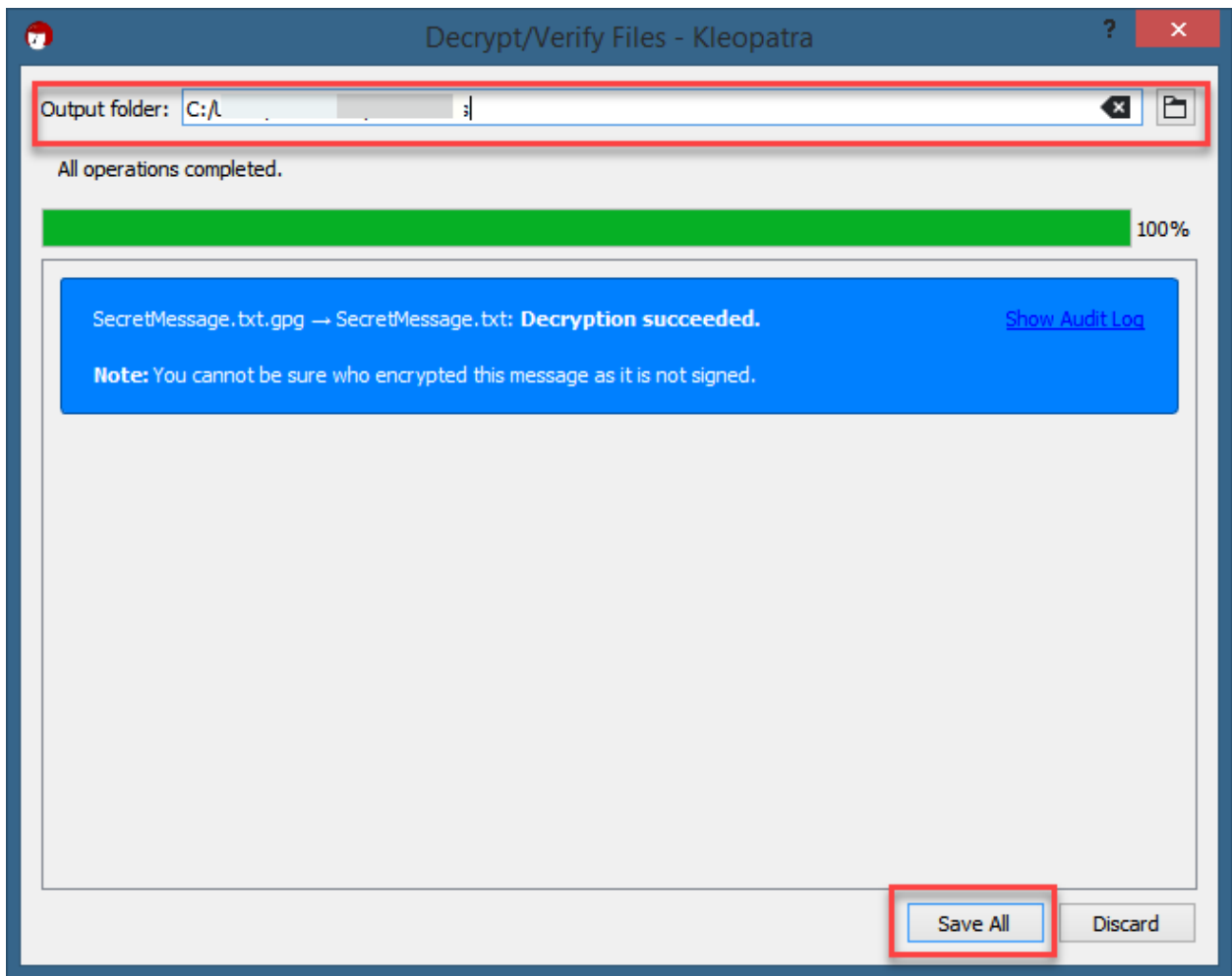
1. To proceed with this task, make sure you have received an email with a secret message from your friend.



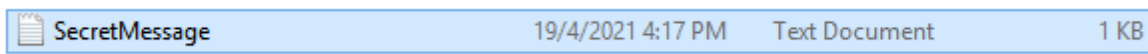
2. Download the attachment of the secret message to a safe location.
3. Next, go to the location of the encrypted file. Follow the steps on the screenshot:



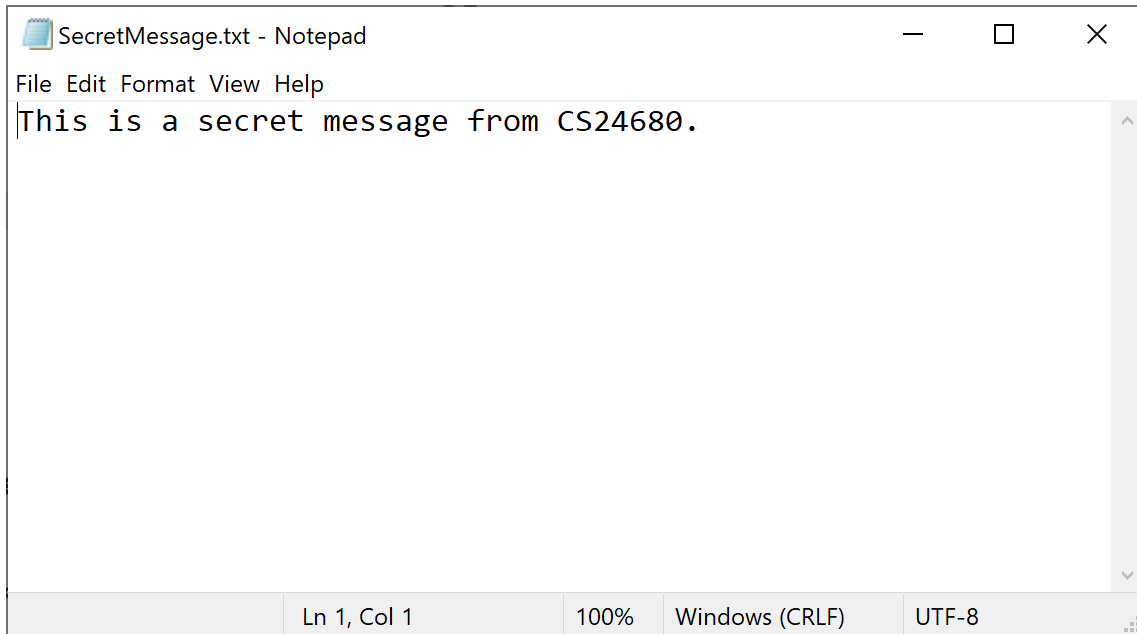
4. Wait until the decryption process complete and click **Save All** button. Take note of the location where the decrypted file being saved.



5. Go to the folder where the plain text is located. You will see the secret file is no more with the **.gpg** extension and now it becomes a **.txt** file.



6. Double click on the file icon and observe the content. Take a screenshot of the plaintext file you received from your friend put it into your lab report.



7. That's all for this task. In conclusion, you should have a clear idea of how asymmetric encryption works. You may use it for email, messaging and another medium of communications. Good job!

REFLECTION QUESTIONS

- | |
|--|
| 1. Why cryptography is important in cybersecurity? |
| 2. Give one example of an application that applied cryptography in our daily life. |
| 3. Describe an example of such an application in question 2 which related to the objectives of cryptography. |
| 4. Describe five (5) differences between symmetric and asymmetric encryption for cryptography. |
| 5. List five (5) differences between cryptography and steganography. |