Experiment No. 5: GPG Tool for File Security

Aim: To demonstrate the use of GPG tool for File Security.

Theory:

GPG, or GNU Privacy Guard, is a widely used encryption tool that provides cryptographic privacy and authentication for data communication. It is a free and open-source implementation of the OpenPGP standard. Here's an overview of what GPG can do:

1. Encryption: GPG can encrypt files and communications using public-key cryptography. This means that you can send encrypted messages to others using their public key, which only they can decrypt using their private key.

2. Digital Signatures: GPG can create and verify digital signatures. Digital signatures provide assurance that a message or file was created by a particular person or entity and has not been tampered with since it was signed.

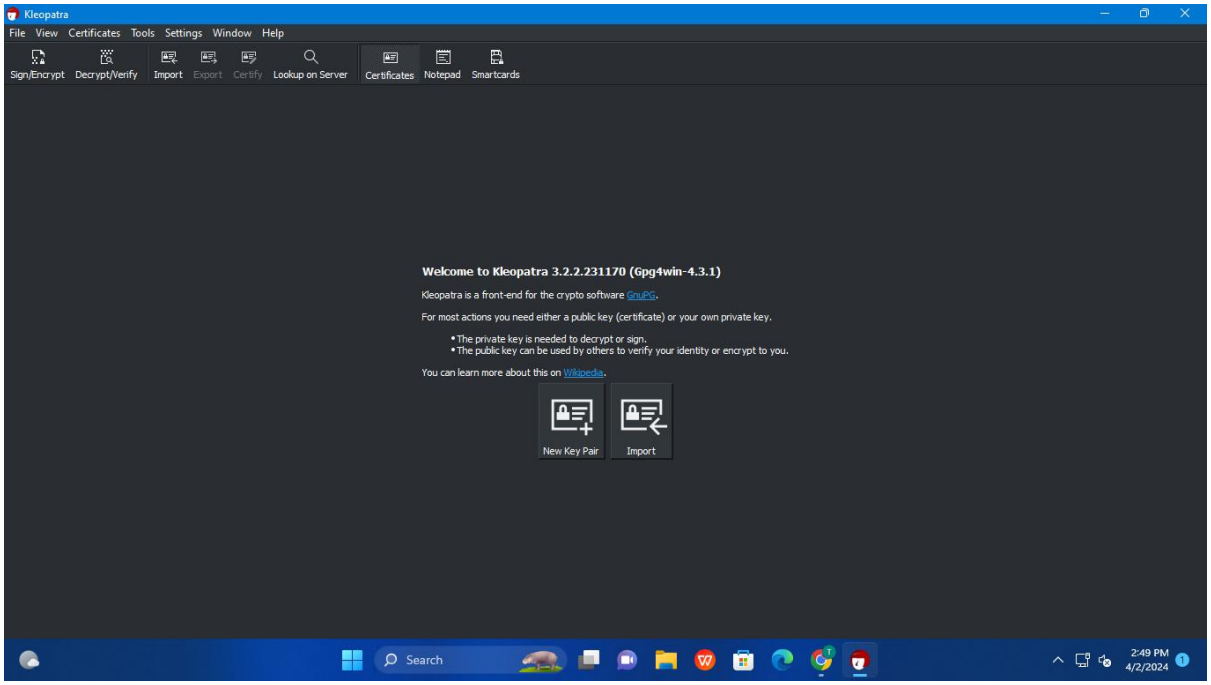
3. Key Management: GPG allows you to manage your encryption keys, including generating new keys, exporting and importing keys, revoking keys if they are compromised, and managing trust relationships between keys.

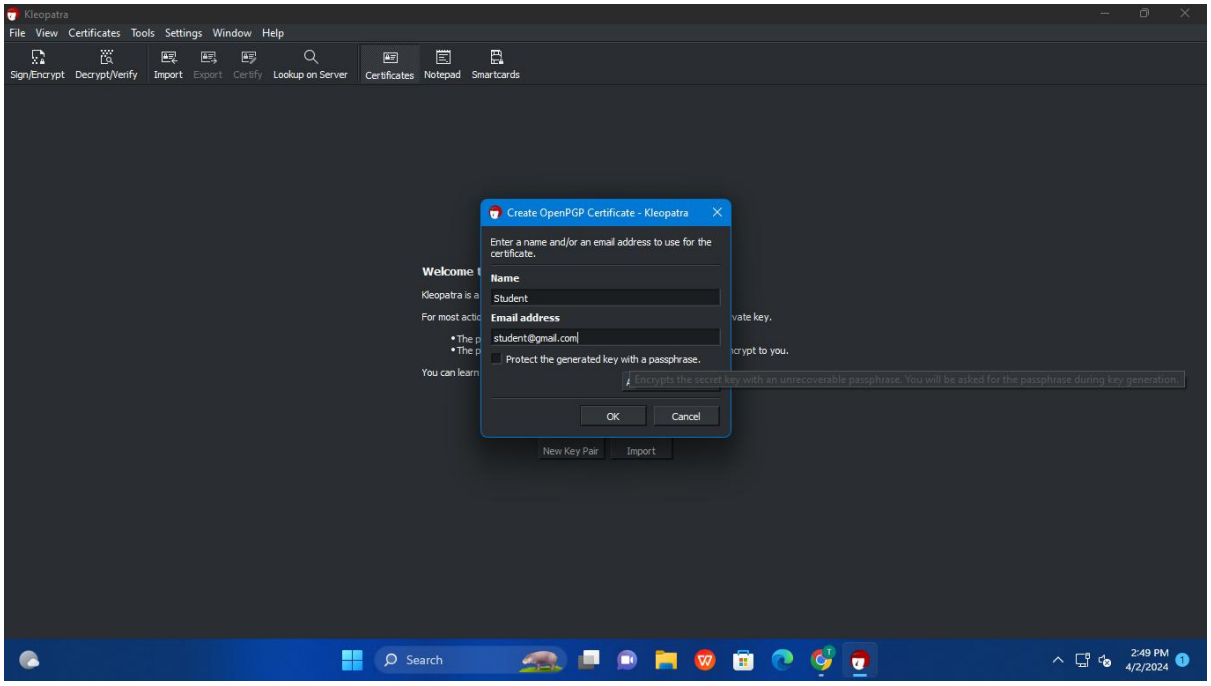
4. Authentication: GPG can be used for user authentication in various scenarios, such as SSH authentication.

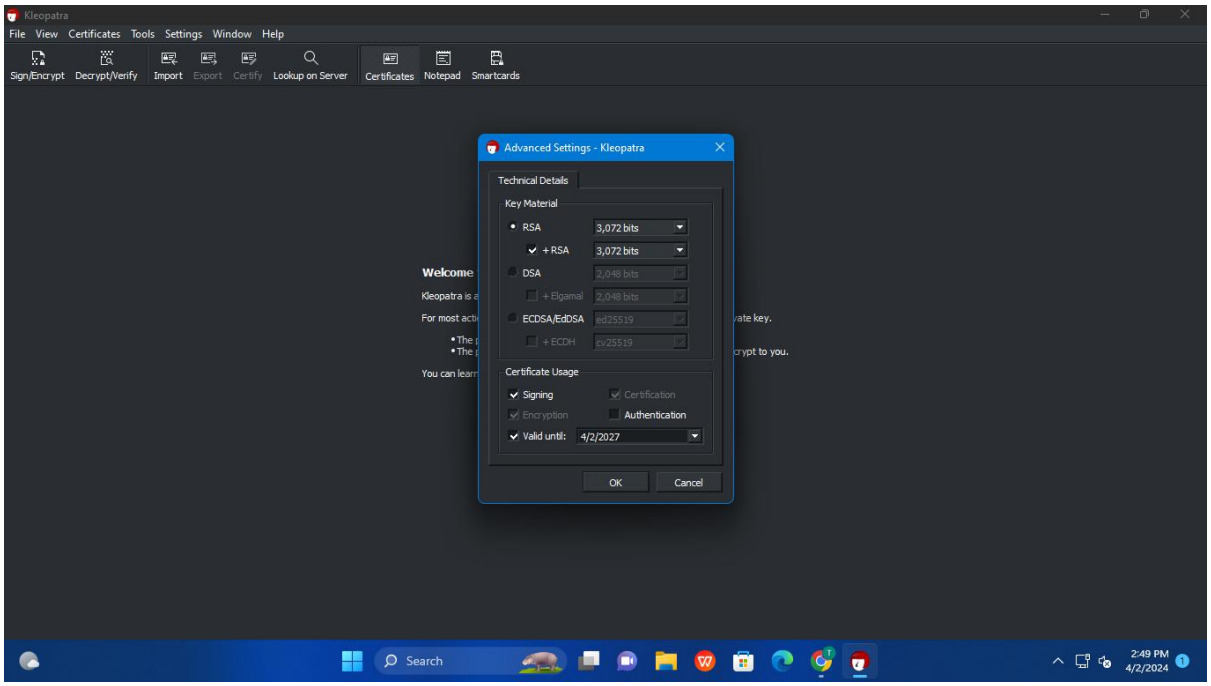
5. Secure Communication: GPG can be used to secure email communication, ensuring that messages are encrypted and digitally signed.

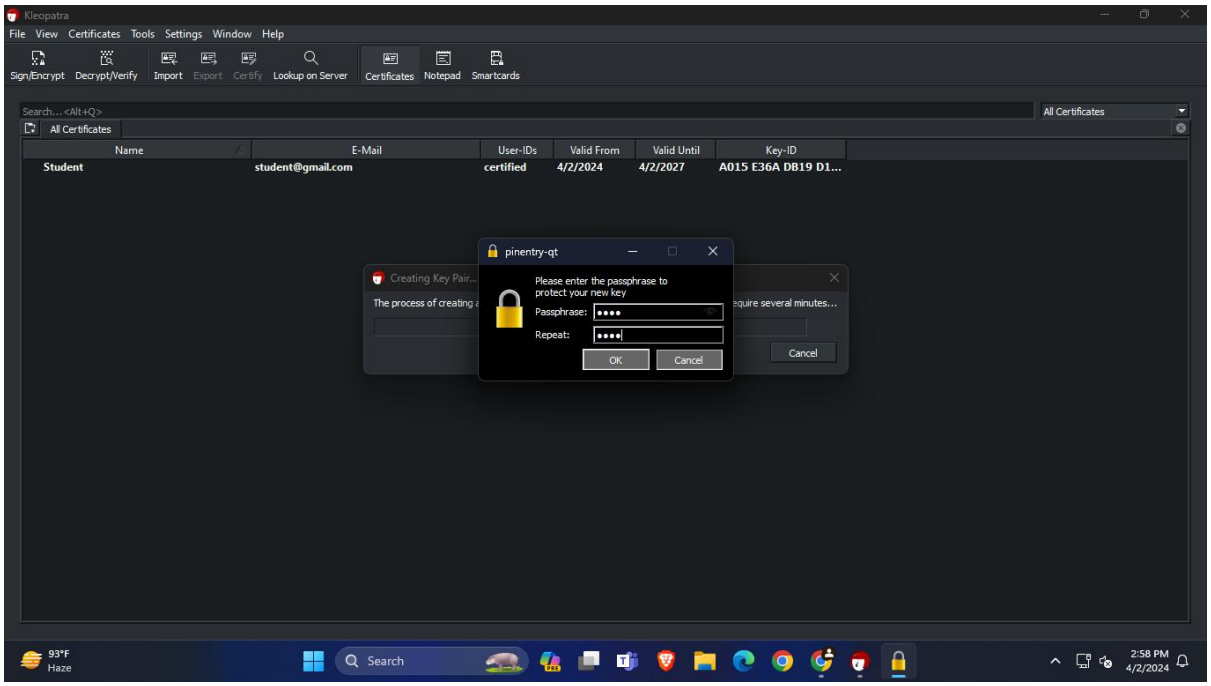
GPG is often used via command-line interface (CLI), but there are also graphical user interfaces (GUIs) available for those who prefer them. It's a powerful tool for ensuring privacy and security in communication and data storage.

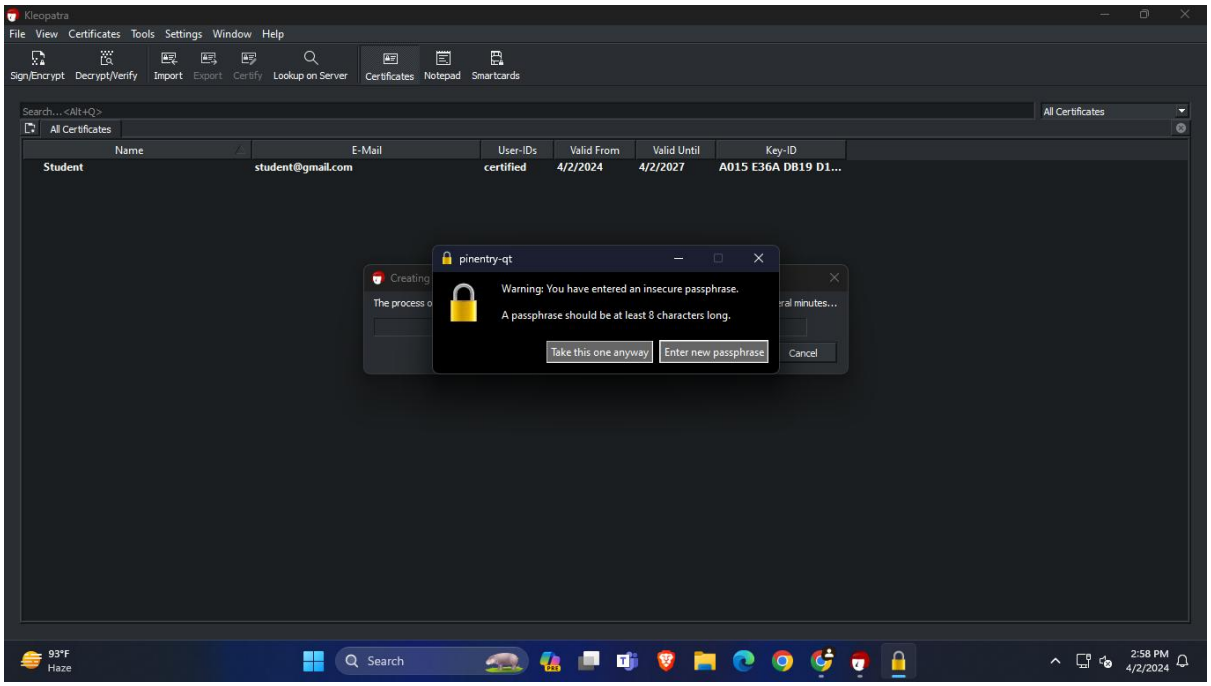
Output:

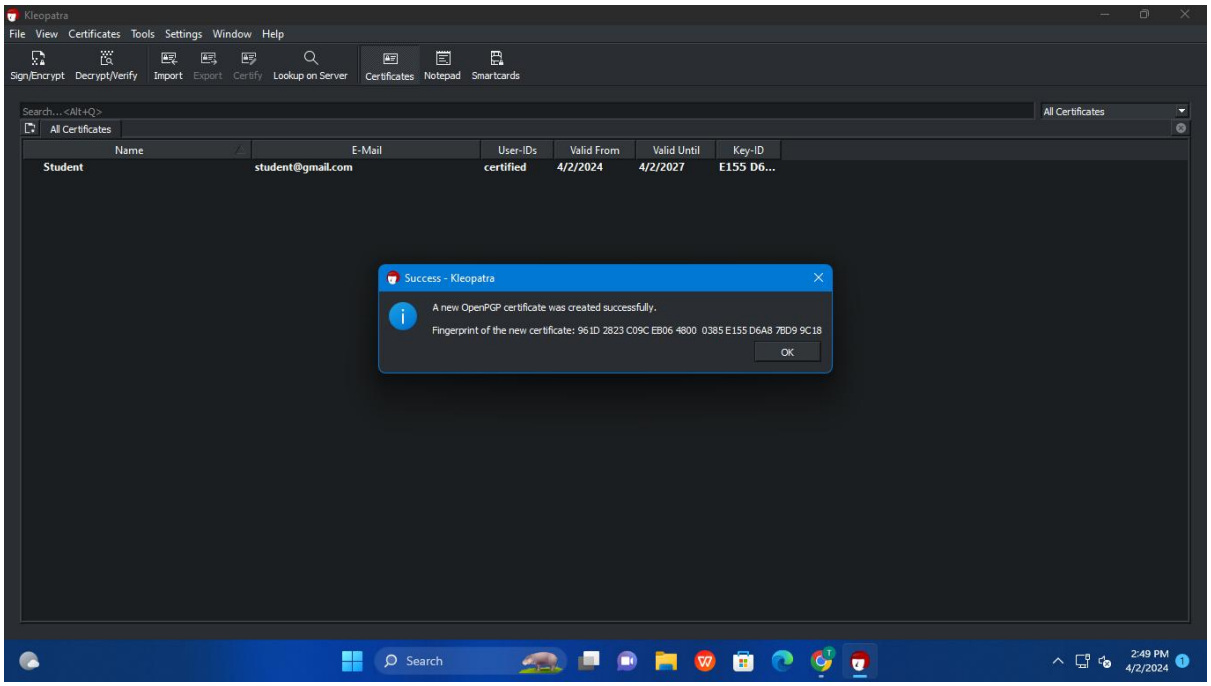

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt
Decrypt/Verify
Import
Export
Certify
Lookup on Server
Certificates
Notepad
Smartcards
Welcome to Kleopatra 3.2.2.231170 (Gpg4win-4.3.1)
Kleopatra is a front-end for the crypto software GnuPG.
For most actions you need either a public key (certificate) or your own private key.
• The private key is needed to decrypt or sign.
• The public key can be used by others to verify your identity or encrypt to you.
You can learn more about this on Wikipedia.
New Key Pair
Import
Search
2:49 PM
4/2/2024

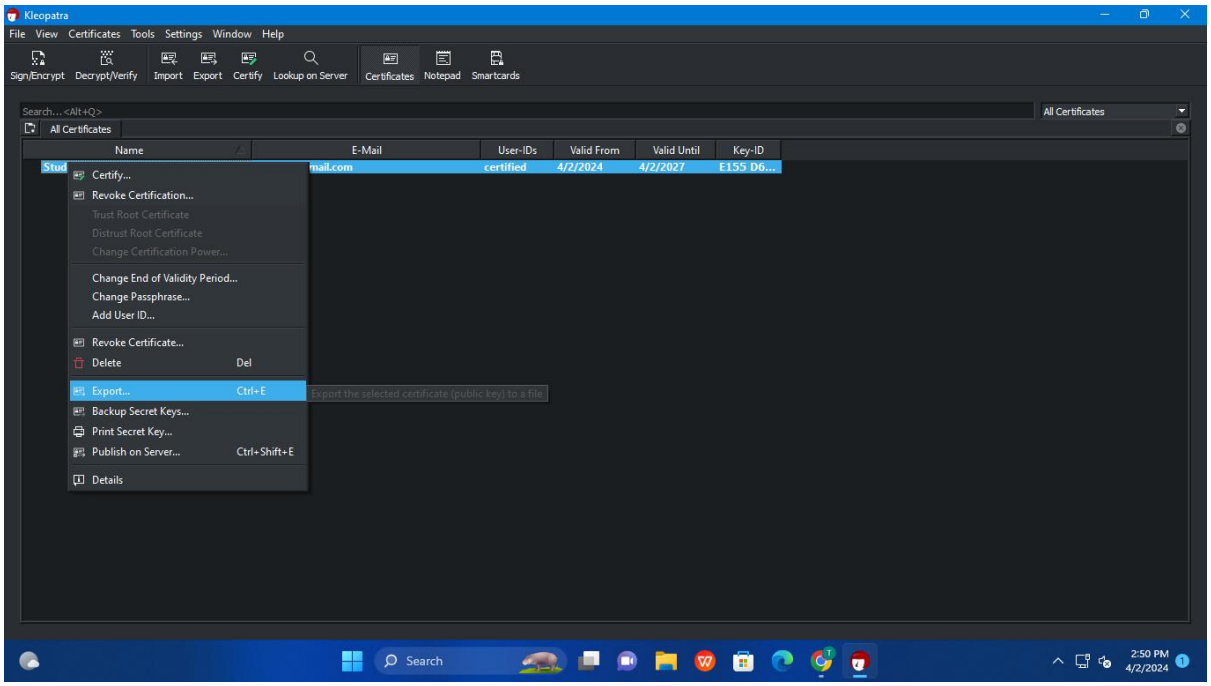

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt
Decrypt/Verify
Import
Export
Certify
Lookup on Server
Certificates
Notepad
Smartcards
Create OpenPGP Certificate - Kleopatra
Enter a name and/or an email address to use for the certificate.
Name
Student
Email address
student@gmail.com
Protect the generated key with a passphrase.
Encrypts the secret key with an unrecoverable passphrase. You will be asked for the passphrase during key generation.
OK
Cancel
New Key Pair
Import
Search
2:49 PM
4/2/2024

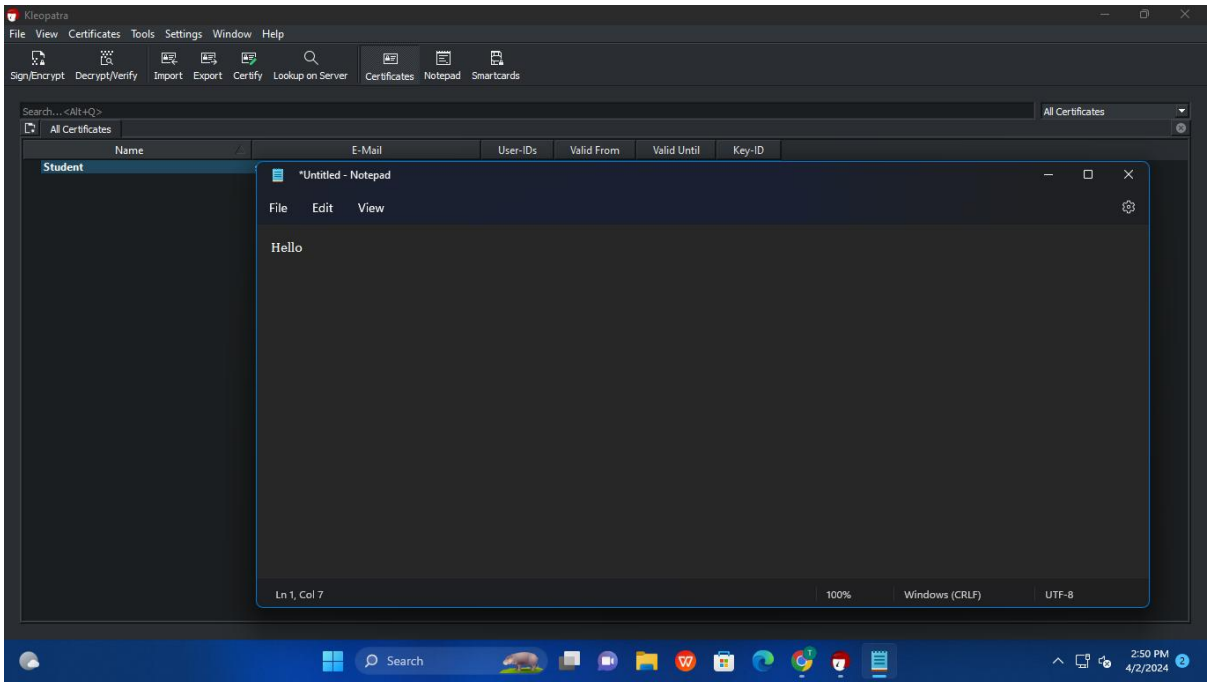

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Advanced Settings - Kleopatra
Technical Details
Key Material
RSA 3,072 bits
+ RSA 3,072 bits
DSA 2,048 bits
+ Elgamal 2,048 bits
ECDSA/EdDSA ed25519
+ ECDH cv25519
Certificate Usage
Signing Certification
Encryption Authentication
Valid until: 4/2/2027
OK Cancel
Welcome
Search
2:49 PM
4/2/2024

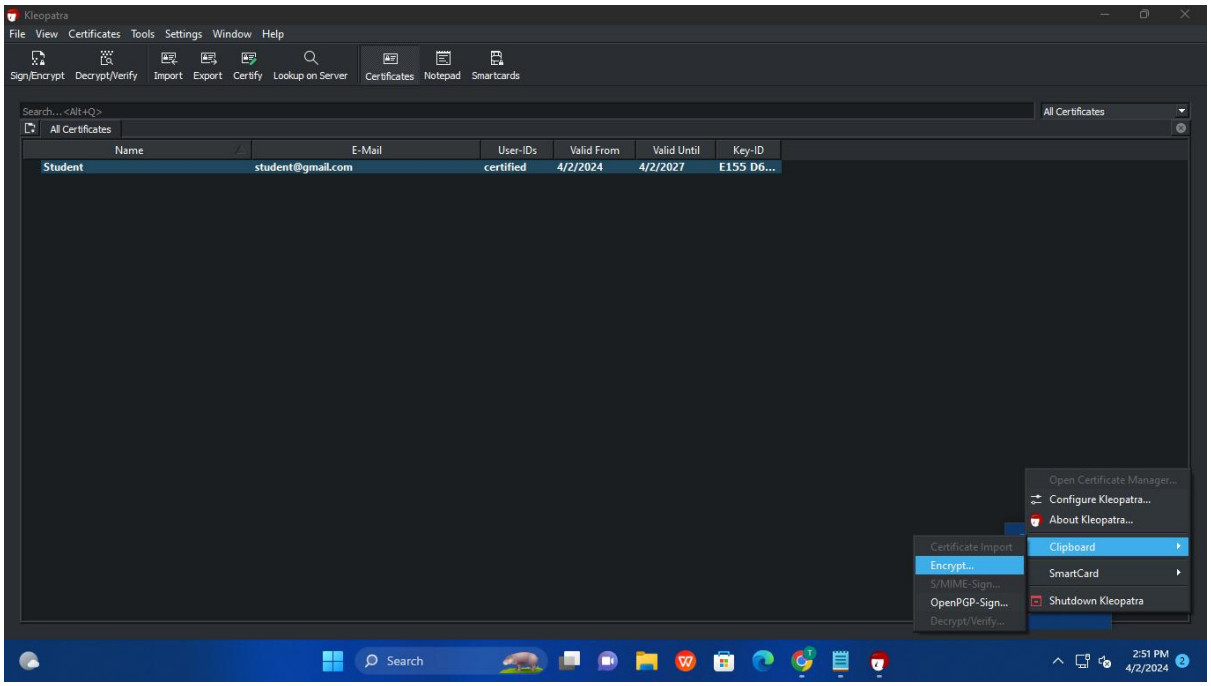

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Search... <Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student student@gmail.com certified 4/2/2024 4/2/2027 A015 E36A DB19 D1...
pinentry-qt
Please enter the passphrase to protect your new key
Passphrase:
Repeat:
OK Cancel
Creating Key Pair...
Cancel
93°F
Haze
Search
2:58 PM
4/2/2024

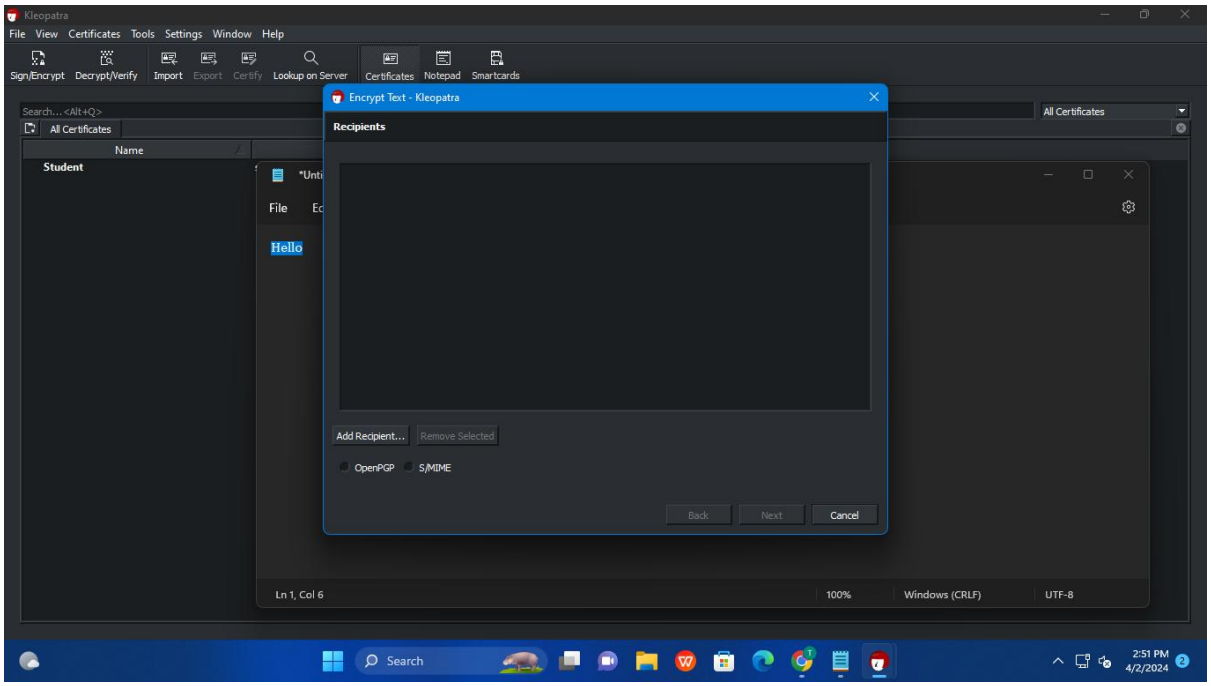

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Search... <Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student student@gmail.com certified 4/2/2024 4/2/2027 A015 E36A DB19 D1...
pinentry-qt
Warning: You have entered an insecure passphrase.
A passphrase should be at least 8 characters long.
Take this one anyway
Enter new passphrase
Cancel
93°F Haze
Search
2:58 PM 4/2/2024


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Search... <Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student student@gmail.com certified 4/2/2024 4/2/2027 E155 D6...
Success - Kleopatra
A new OpenPGP certificate was created successfully.
Fingerprint of the new certificate: 961D 2823 C09C EB06 4800 0385 E155 D6A8 7BD9 9C18
OK
Search
2:49 PM 4/2/2024


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
certified 4/2/2024 4/2/2027
Certify...
Revoke Certification...
Trust Root Certificate
Distrust Root Certificate
Change Certification Power...
Change End of Validity Period...
Change Passphrase...
Add User ID...
Revoke Certificate...
Delete Del
Export... Ctrl+E
Backup Secret Keys...
Print Secret Key...
Publish on Server... Ctrl+Shift+E
Details
Search
2:50 PM
4/2/2024


Kleopatra
File View Certificates Tools Settings Window Help
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student
*Untitled - Notepad
File Edit View
Hello
Ln 1, Col 7
100%
Windows (CRLF)
UTF-8
Search
2:50 PM
4/2/2024

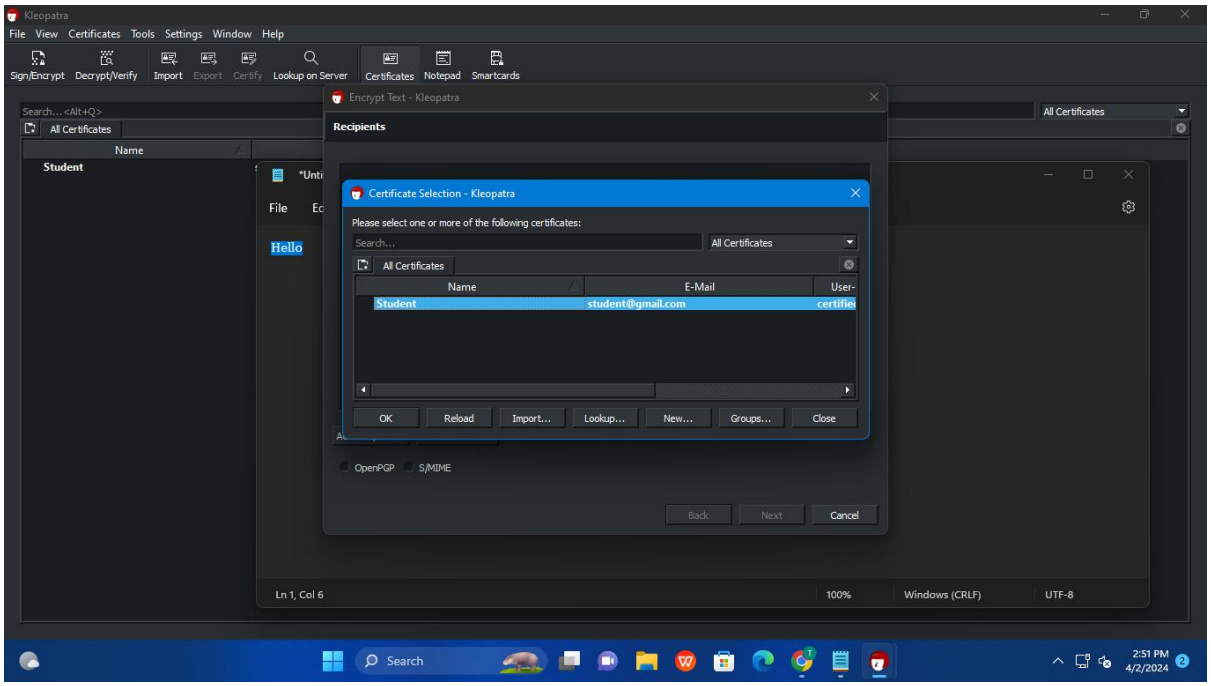

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Search... <Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student student@gmail.com certified 4/2/2024 4/2/2027 E155 D6...
Open Certificate Manager...
Configure Kleopatra...
About Kleopatra...
Certificate Import
Clipboard
Encrypt...
SmartCard
S/MIME-Sign...
OpenPGP-Sign...
Shutdown Kleopatra
Decrypt/Verify...
Search
2:51 PM
4/2/2024

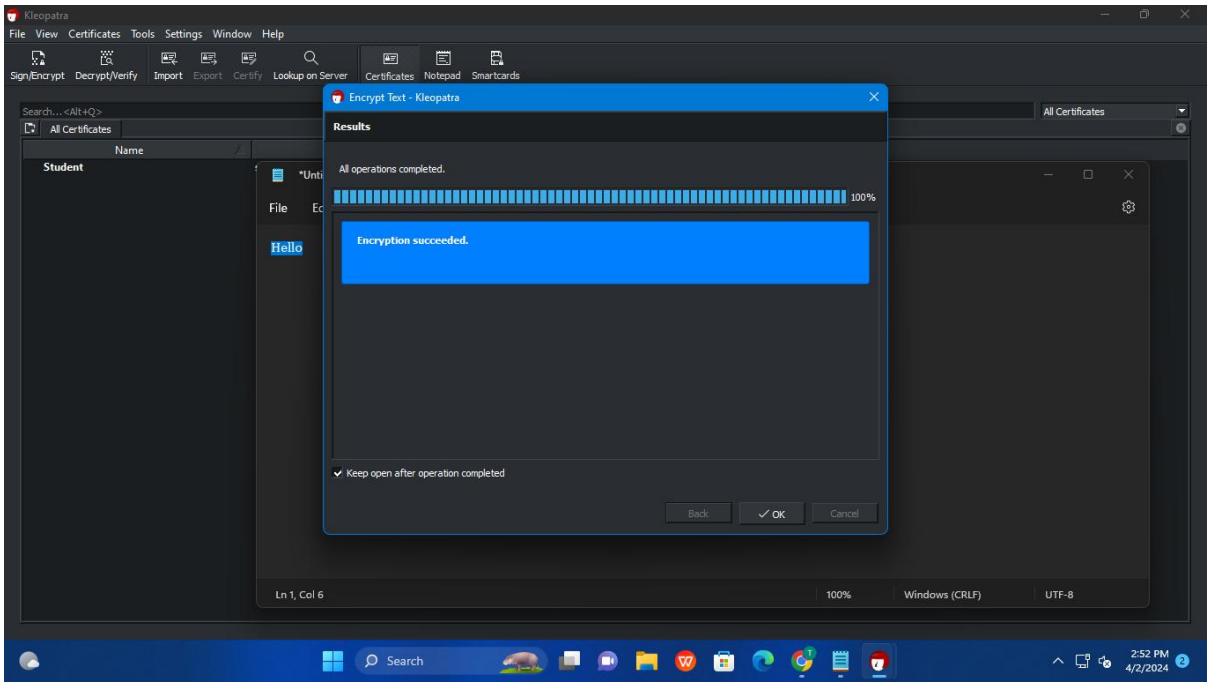

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Encrypt Text - Kleopatra
Recipients
Add Recipient... Remove Selected
OpenPGP S/MIME
Back Next Cancel
Hello
Ln 1, Col 6
100%
Windows (CRLF)
UTF-8
Search
2:51 PM
4/2/2024

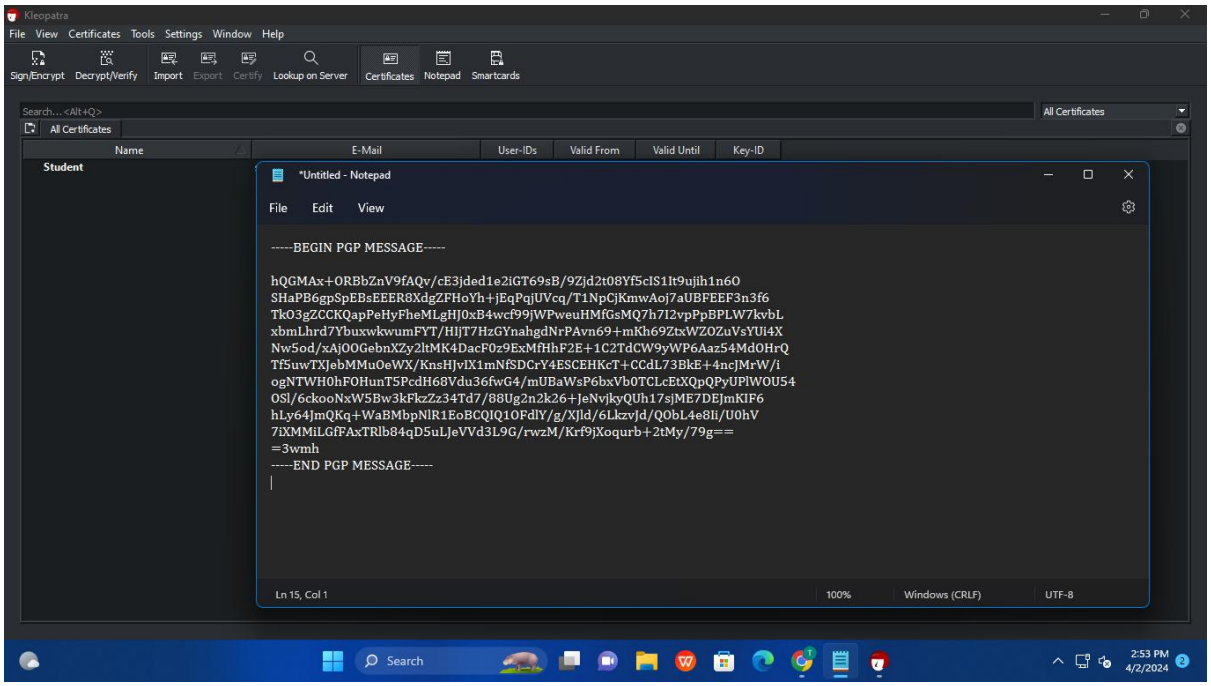
Vidyavardhini's College of Engineering & Technology

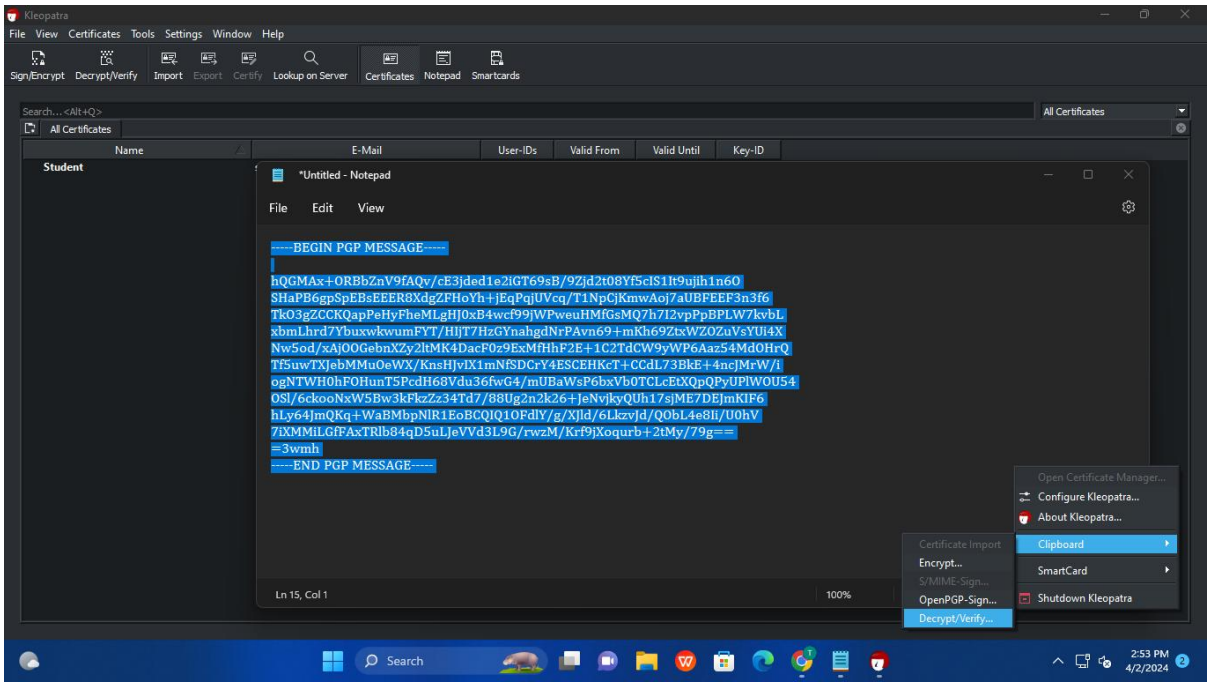
Department of Computer Engineering

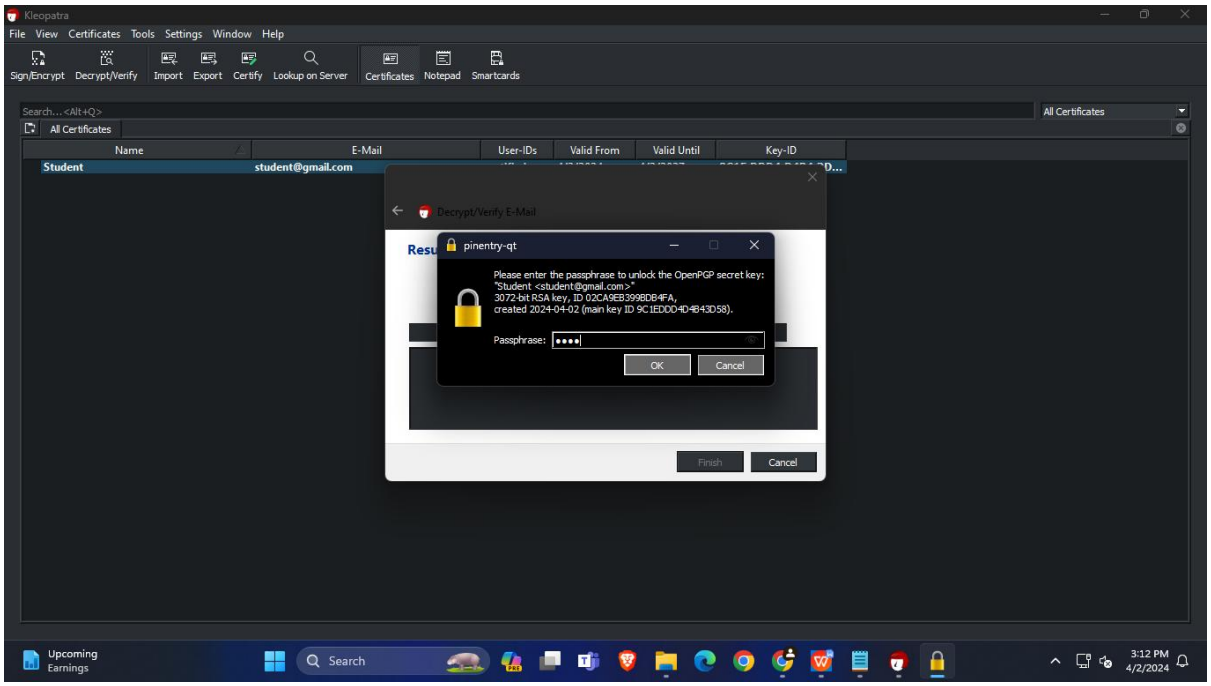
Academic Year 2023-24

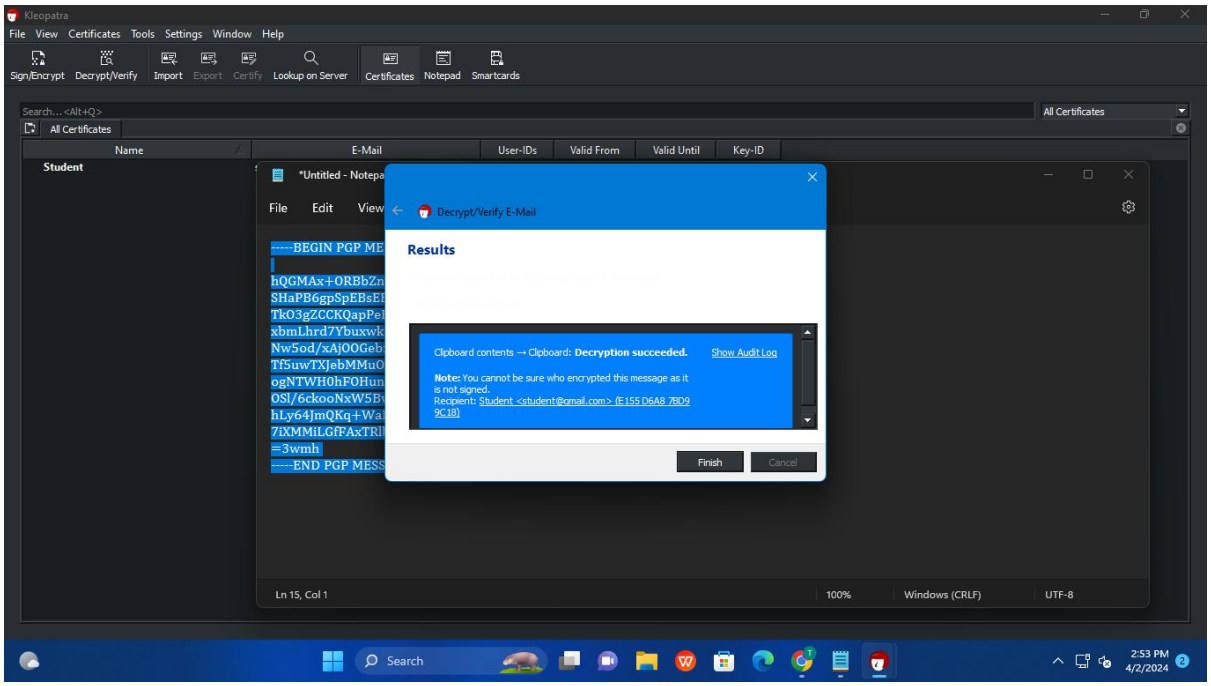


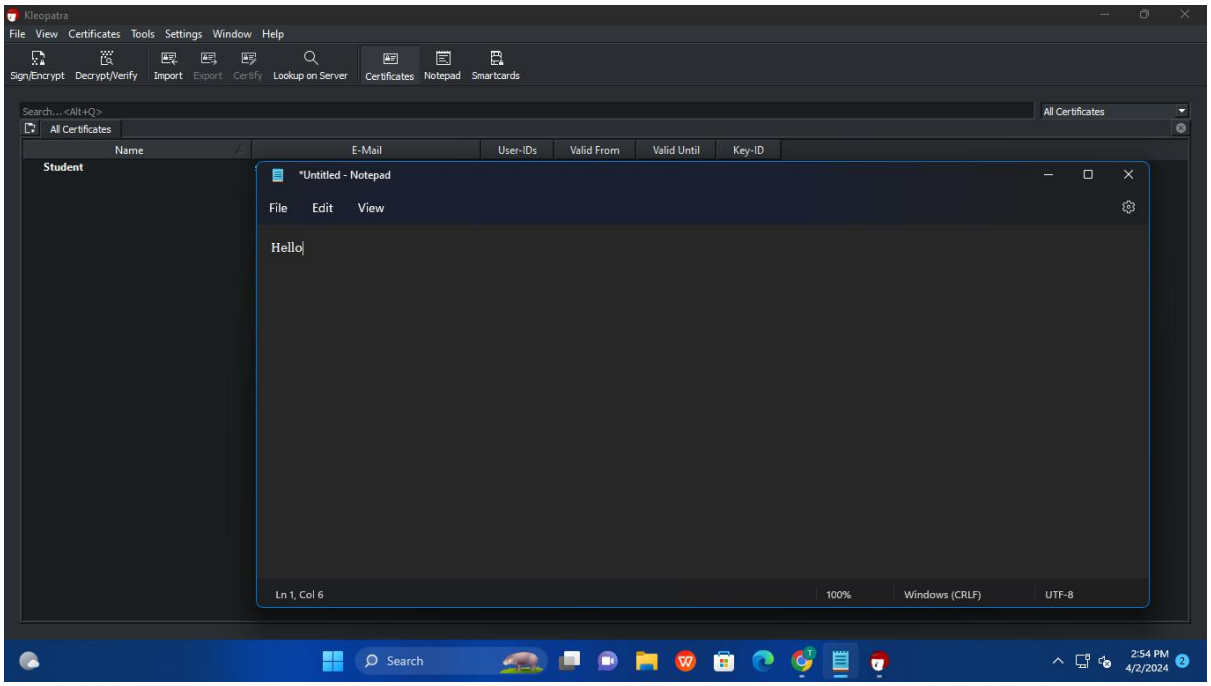



Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Search... <Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student
*Untitled - Notepad
File Edit View
-----BEGIN PGP MESSAGE-----
hQGMAx+ORBbZnV9fAQv/cE3jded1e2iGT69sB/9Zjd2t08Yf5cIS1lt9ujih1n6O
SHaPB6gpSpEBsEEER8XdgZFHoYh+jEqPqjUVcq/T1NpCjKmwAoj7aUBFEEF3n3f6
Tk03gZCCKQapPeHyFheMLgHJ0xB4wcf99jWPweuHMfGsMQ7h7I2vpPpBPLW7kvbL
xbmLhrd7YbuxwkwumFYT/HIjT7HzGYnahgdNrPAvn69+mKh69ZtxWZOZuVsYUi4X
Nw5od/xAjOOGebnXZy2ltMK4DacF0z9ExMfHhF2E+1C2TdCW9yWP6Aaz54MdOHrQ
Tf5uwTXJebMMuOeWX/KnsHJvlX1mNfSDCrY4ESCEHKcT+CCdL73BkE+4ncjMrW/i
ogNTWH0hFOHunT5PcdH68Vdu36fwG4/mUBaWsP6bxVb0TCLcEtXQpQPyUPlWOU54
OSl/6ckooNxW5Bw3kFkzZz34Td7/88Ug2n2k26+JeNvjkyQUh17sjME7DEJmKIF6
hLy64JmQKq+WaBMbpNlR1EoBCQIQ10FdlY/g/XJld/6LkzvJd/Q0bL4e8li/U0hV
7iXMMiLGfFAxTRlb84qD5uLJeVVd3L9G/rwzM/Krf9jXoqurb+2tMy/79g==
=3wmh
-----END PGP MESSAGE-----
Ln 15, Col 1
100%
Windows (CRLF)
UTF-8
Search
2:53 PM
4/2/2024


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Search... <Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student
*Untitled - Notepad
File Edit View
-----BEGIN PGP MESSAGE-----
hQGMAx+ORBbZnV9fAQv/cE3jded1e2iGT69sB/9Zjd2t08Yf5cIS1lt9ujih1n6O
SHaPB6gpSpEBsEEER8XdgZFHoYh+jEqPqjUVcq/T1NpCjKmwAoj7aUBFEEF3n3f6
Tk03gZCCKQapPeHyFheMLgHJ0xB4wcf99jWPweuHMfGsMQ7h7I2vpPpBPLW7kvbL
xbmLhrd7YbuxwkwumFYT/HIjT7HzGYnahgdNrPAvn69+mKh69ZtxWZOZuVsYUi4X
Nw5od/xAjOOGebnXZy2ltMK4DacF0z9ExMfHhF2E+1C2TdCW9yWP6Aaz54MdOHrQ
Tf5uwTXJebMMuOeWX/KnsHJvlX1mNfSDCrY4ESCEHKcT+CCdL73BkE+4ncjMrW/i
ogNTWH0hFOHunT5PcdH68Vdu36fwG4/mUBaWsP6bxVb0TCLcEtXQpQPyUPlWOU54
OSl/6ckooNxW5Bw3kFkzZz34Td7/88Ug2n2k26+JeNvjkyQUh17sjME7DEJmKIF6
hLy64JmQKq+WaBMbpNlR1EoBCQIQ10FdlY/g/XJld/6LkzvJd/Q0bL4e8li/U0hV
7iXMMiLGfFAxTRlb84qD5uLJeVVd3L9G/rwzM/Krf9jXoqurb+2tMy/79g==
=3wmh
-----END PGP MESSAGE-----
Ln 15, Col 1
100%
Open Certificate Manager...
Configure Kleopatra...
About Kleopatra...
Clipboard
SmartCard
Shutdown Kleopatra
Certificate Import
Encrypt...
S/MIME-Sign...
OpenPGP-Sign...
Decrypt/Verify...
Search
2:53 PM
4/2/2024


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student student@gmail.com
Decrypt/Verify E-Mail
pinentry-qt
Please enter the passphrase to unlock the OpenPGP secret key:
"Student <student@gmail.com>"
3072-bit RSA key, ID 02CA9EB398BDB4FA,
created 2024-04-02 (main key ID 9C1EDDD4D4B43D58).
Passphrase:
OK
Cancel
Finish
Cancel
Upcoming Earnings
Search
3:12 PM 4/2/2024


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
All Certificates
Name E-Mail User-IDs Valid From Valid Until Key-ID
Student
*Untitled - Notepad
File Edit View
-----BEGIN PGP ME
hQGMAx+ORBbZn
SHaPB6gpSpEBsEI
Tk03gZCCKQapPei
xbmLhrd7Ybuxwk
Nw5od/xAjOOGeb
Tf5uwTXJebMMu0
ogNTWH0hFOHun
OSl/6ckooNxW5Bs
hLy64JmQKq+Wa
7iXMMiLGfFAxTRl
=3wmh
-----END PGP MESS
Decrypt/Verify E-Mail
Results
Clipboard contents → Clipboard: Decryption succeeded.
Show Audit Log
Note: You cannot be sure who encrypted this message as it is not signed.
Recipient: Student <student@gmail.com> (E155 D6A8 76D9 9C18)
Finish
Cancel
Ln 15, Col 1
100%
Windows (CRLF)
UTF-8
Search
2:53 PM 4/2/2024



Conclusion: In conclusion, the experiment involving the GPG tool has provided valuable insights into the intricacies of data encryption and security. Through its implementation, we have witnessed the robustness of GPG in safeguarding sensitive information by employing asymmetric encryption techniques. The experiment has underscored the importance of utilizing such tools in protecting data integrity and confidentiality, especially in an era marked by increasing cyber threats. Furthermore, the successful execution of the experiment highlights the efficacy of GPG as a reliable solution for individuals and organizations seeking to enhance their data protection measures. As technology continues to evolve, GPG remains a critical asset in ensuring the privacy and security of digital communications and information exchange.