PRACTICAL-6

AIM:

Implement GPG for windows.

THEORY:

- Gpg4win is an email and file encryption package for most versions of Microsoft Windows and Microsoft Outlook, which utilises the GnuPG framework for symmetric and public-key cryptography, such as data encryption, digital signatures, hash calculations etc.
- Gpg4win enables users to securely transport emails and files with the help of encryption and digital signatures. Encryption protects the contents against an unwanted party reading it. Digital signatures make sure that it was not modified and comes from a specific sender.
- GPG is an excellent method to ensure secure communication between two parties. It allows sensitive information to be easily shared across an insecure network.

HOW IT WORKS

- It allows you to send or publish your public key out in the open on an insecure network.
- The party looking to send you a secure message uses your public key to encrypt a
 message using that key.

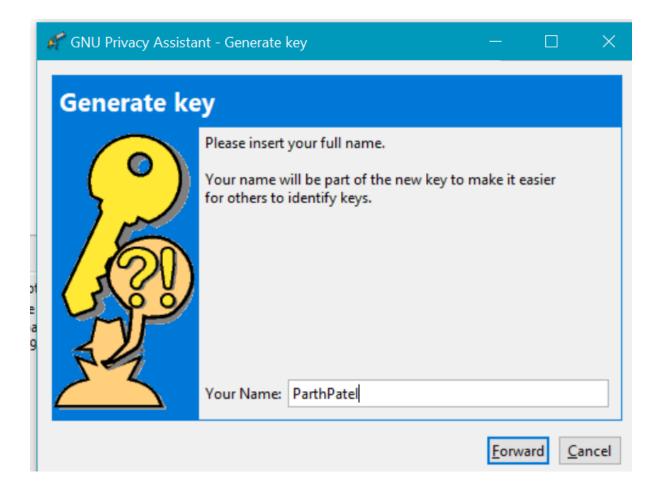
The message is then sent to you where you then use your private key to decrypt it. You
can then reply using the sender's public key which allows you to securely encrypt
messages to them. They then use their private key to decrypt messages encrypted by
you.

IMPLEMENTATION:

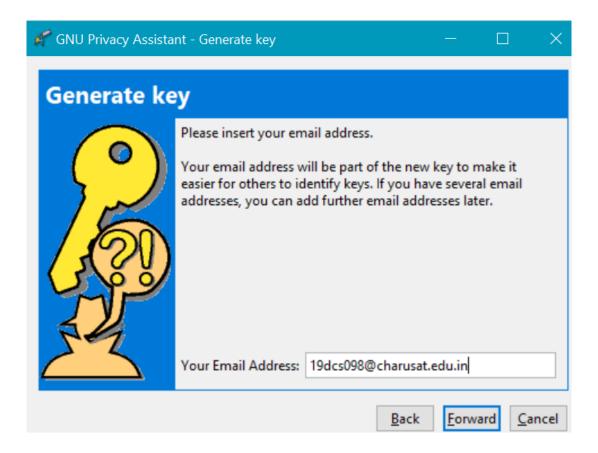
- Firstly, you need to install the software from the setup file.
- Upon successful installation, the following two icons will be visible on desktop



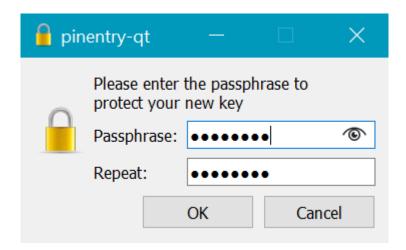
- Click on GPA and "Generate Key" and Enter the name
- For this, go to keys tab and click New Key



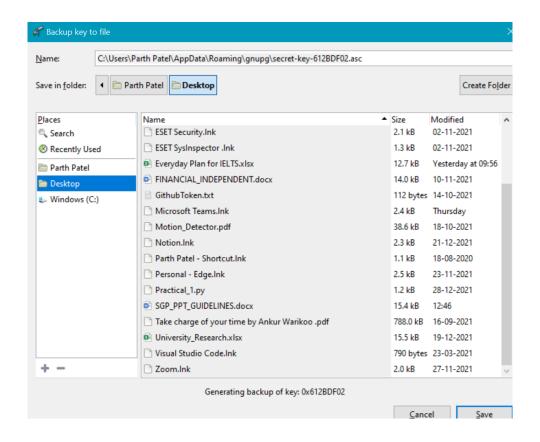
• Now, Enter the E-mail



• Enter the password



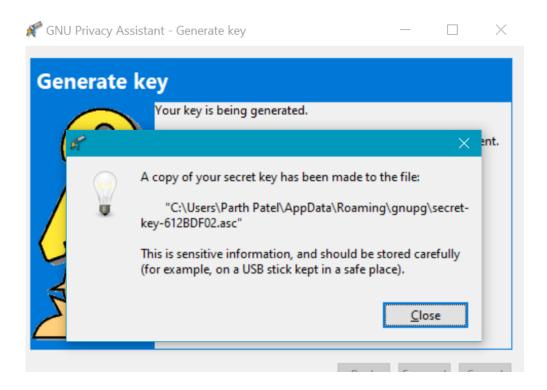
• Save the back-up file



• Enter the password again to confirm

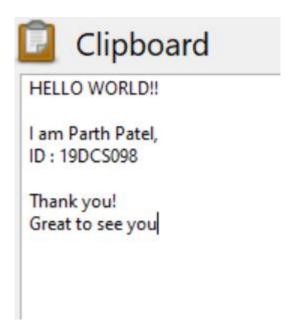


• Process Successful

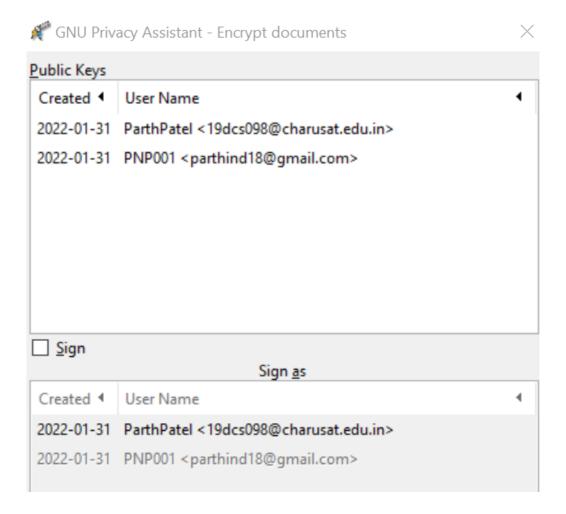


ENCRPYTION

• Write the message in the clipboard



• Click on Encrypt button and following screen will prompt



- Select the user through which encryption will take place.
- The Encrypted message displayed as below



Clipboard

----BEGIN PGP MESSAGE-----

hQEMAzkJRyJLiZiiAQf9ErccHtuEbZVXuqs/Ks5KrK8OitHuj6VS3zNS9Avsnw3f
FsFM1hqhgbTa6vndcCTgxA9F29ZO4SKt7ny/WFkwkGZFWaClhJABJUNgtx8kBDCC
kEAER9yDO0gTBuSiU0hu/pl6RgYQUntj/+8LAVNQL4jSHgvPHPY5OcKgAroJPJOw
GvyDJrUxcO3LqD/+qH3ihNyiZR+oqoKUoHDKI+ugBz30/bDSNoEE6gxZWEv0Cq1A
nEdS2ZgwMeH7XSVwfuJewx4ZgrFuFJICWv6qKm6YVgkqZh3qJ86SUIWe6CTE9EWN
xXwtQO3lsv58l1HRQdYwudU7zsuUKBuZeeyaqnX/SdSNAQkCEG8jFt+4CGBSwSes
kB3M4zjvemJF9dcD0CZA6fC3TmVCKRtpF/y7Qax5aGw+9OroQ1L1FRlh5ca2Cv8e
K2kGV6+anS36i3yma8UovpPiTEKCCh4eq+H/yMV5B0g1rFWA4/Wc7eDxueQocvb2
GB/rb82wVn40amC/JEg6xczrnQ2Ly1oD77v8E2eD
=zOpH

----END PGP MESSAGE-----

• On clicking Decrypt button, original message will appear

CONCLUSION:

By performing the practical, I learnt the basic concepts of GFG.