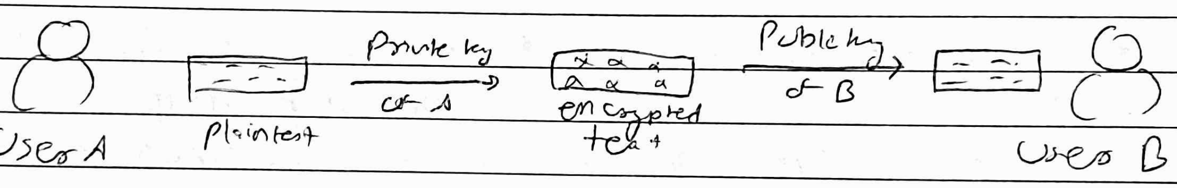
CSS lab.

Aim: Explore the GPG tool or linux to implement email security.

Theory:

1) GnuGP, popularly known as GPG, is an extremely versatile tool, being used as the industry standard for encryption of things like emails, messages, files or just anything you need to send someone securely.



2) A GPG key is what you'll use to encrypt or decrypt files.

3) GPG allows you to encrypt files locally and then allow others to be ensured that the files they received were actually sent from you.

→ Encrypting and decrypting files with GPG.

1) Install GPG
2) Generate a GPG key
3) Encrypt a file with GPG
4) Decrypt an encrypted file with GPG.

→ Commands used in GPG:

1) sudo apt install gpg

2) gpg --full-generate-key:

3) gpg --list-secret-keys.

4) gpg --encrypt --output file-gpg -- recipient <email> file
To encrypt the Messge & store in a file.

5) gpg --decrypt --output file file.gpg: To decrypt the Messge and store in filed.

→ Uses of GPG: One of the Most common example of using GPG is in Linux packge Manager, specially the external repositories. You add the public key of the developer into your system's trusted keys. The developer signs the packges with his/her private key. Since your Linux systems has public file, it understands that the packge is actually coming from trusted source.

→ Conclusion:

Thus, I have successfully studied and used GPG tool of linux to implement email security.