Lab Assignment 10

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

Lab Outcome attained: LO6

GPG is the OpenPGP part of the GNU Privacy Guard (GnuPG). It is a tool to provide digital encryption and signing services using the OpenPGP standard. gpg features complete key management and all the bells and whistles you would expect from a full OpenPGP implementation.

Step 1: Generate private key and public key pairs for sender and receiverusing command

```
gpg --gen-key  or gpg –full-generate-key
```

(repeat for sender and receiver)

Step 2: Create a file containing sender's public key which then can be sent to other users.

```
gpg --export -a username>filename
```

(creates file in ascii format) **or**

```
gpg --output filename  --armor --export  user's_email
```

(for sender)

Step 3: Similarly create file containing sender's private key.

```
gpg --export-secret-key -a username>filename
```

(for sender)

Step 4: You can create a fingerprint of key using the command

```
gpg --fingerprint  receiver's_email
```

(for receiver)

Step 5: Sender needs to add in his public key ring, the public key of receiver **(for sender)**

```
gpg --import   filename_containing_public_key_of_receiver
```

Step 6: Listing public keys in keyring

```
gpg --list-keys
```

(from public key rings of all users)

```
gpg --list-keys shachi_natu@yahoo.com
```

(from public key rings of specific users)

How do you know that the person giving you the public key is who they say they are?

Step 7: Snder can sign the public key of receiver using command

```
gpg --sign-key  receiver_email
```

When you sign the key, it means you verify that you trust the person is who they claim to be. This can help other people decide whether to trust that person too. If someone trusts you, and they see that you've signed this person's key, they may be more likely to trust their identity too.

Step 8: Encrypt the data to send. (create a file beforehand to be encrypted)

```
gpg --encrypt -r receiver_email   name_of_file
```

(only encrypt, .gpg file created)

OR

```
gpg --encrypt --sign --armor -r receiver_email   name_of_file
```

(encrypt and sign, ascii file created)

OR

```
gpg --encrypt --sign  -r receiver_email   name_of_file
```

(encrypt and sign, .gpg file created)

Step 9: Decrypt the file

```
gpg -o myfiledecrypted  -d myfile.txt.gpg
```