University of Colombo, School of Computing

GNU PGP

Practical Environment

Please use your Ubuntu environment (Laptop or VM) to work on this practical. In Ubuntu (Linux) OpenSSL is preinstalled. You have to install gpg (**`sudo apt-get install gnupg`**).

PGP

PGP encryption or Pretty Good Privacy encryption, is a data encryption standard that gives cryptographic privacy and authentication for data storage and communication. It is often used to encrypt and decrypt texts, emails, and files to increase the security of emails. PGP encryption uses a mix of data compression, hashing, and public-key cryptography. It also uses symmetric and asymmetric keys to encrypt data that is transferred across networks. It combines features of private and public key cryptography.

1. Creating PGP Key Pair

We should generate a public key that you can distribute on the internet and a private key which should be guarded and protected.

```
$ gpg --gen-key
```

List Keys

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

2. Distributing You Public Keys

Your public key should be distributed to the other people. Thus export it to a file.

```
$ gpg --export -a <youremail> > <publickeyfile>
```

This is for private key. You should not distribute your private key.

```
$ gpg –export-secret-keys -a <youremail> > <privatekeyfile>
```

3. Importing and Signing Public Keys of your friends

In order to send the encrypted data you should import public keys of your friends and sign these public keys as trusted public keys.

```
$ gpg --import <friendspublickeyfile>
$ gpg --sign-key <firendsemail>
```

4. Sending a Signed and Encrypted messages

Signed and encrypted messaged can be created as follows.

```
$ gpg --encrypt --sign -r <firendsemail> <filetobeencryped>
```

When you receive a PGP message, simply call GPG on the message file:

```
$ gpg <encrypedfile>
```

+++ end +++