Ex. 9 IMPLEMENTATION OF SECURITY UTILITIES

AIM:

To implement the security utilities using GNU privacy guard (GPG) in linux.

PROCEDURE:

1] GENERATING A KEY:

This command generates a new set of private and public keys.

```
#gpg --gen-key
```

2] ENCRYPTION:

This command encrypts data.

```
#gpg  -e  , --encrypt
```

3] DECRYPTION:

This command decrypts the given file.If the decrypted file is signed,the signature is veified.

```
#gpg  --decrypt [file]
```

4] ARMOR:

This option creates ASCII armored output,ASCII verstion of encrypted data.

```
#gpg  --a , --armor
```

5] LISTING THE KEYS:

*This command list all keys from the keyrings or those specified.

```
#gpg --list-key [name]
```

*This command list all keys ffrom the public keyrings or those specified.

```
#gpg  --list -public-keys  [name]
```

*This command list our own private key.

```
#gpg  --list -secret-keys  [name]
```

*The following command lists all keys along with its signature they have.

```
# gpg  --list –signs [name]
```

6] SIGNING THE KEYS:

* The following command is used to sign a document and creatind a signature.

```
# gpg -s , --sign
```

* The following command is used to verify the signature.

```
# gpg --check-signs [names]
```

* The following command list the fingerprint for specified keys.

```
# gpg --fingerprint [names]
```

7] DELETING THE KEYS:

*The following command removes the public key from the keyring.

```
# gpg --delete-key name
```

* The following command removes both private and public key from the keyring.

```
# gpg --delete-secret-key name
```

8] REVOCATION:

The following command generate a revocation certificate for our own key.

```
# gpg --gen-revoke keyname
```