Name : Aman Singh

Roll no : 128, Batch : T23 , Subject : Security Lab

Experiment No 13

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

Lab Outcome :

LO6

Theory :

1. What is Private Key Ring and Public Key Ring?

In the context of GPG (GNU Privacy Guard), a private key ring and a public key ring are essential components of the OpenPGP encryption and signing system. These key rings are used for managing cryptographic keys for secure communication.

- Private Key Ring: This is a collection of private keys owned by a user. Private keys are used for decrypting messages sent to you and for signing messages to ensure their authenticity. Each user typically has their private key ring, which should be kept confidential and protected at all costs. Only the owner of the private key ring should have access to it.

- Public Key Ring: This is a collection of public keys, which are meant to be shared openly. Public keys are used by others to encrypt messages meant for you and to verify the digital signatures you create with your private key. Public keys are freely distributed and can be obtained from a keyserver or directly from the person they belong to.

2. Write the commands used for key generation, export and import of keys and signing and encrypting the message in gpg tool.

Key Generation
To generate private and public key pairs for sender and receiver, you can use the following commands:

```bash
gpg --gen-key   or gpg --full-generate-key (repeat for sender and receiver)
```

Exporting and Importing Keys
- Create a file containing sender's public key (ASCII format):
```bash
gpg --export -a username > filename
```
- Create a file containing sender's private key:
```bash
```

Name : Aman Singh

Roll no : 128, Batch : T23 , Subject : Security Lab

gpg --export-secret-key -a username > filename
```
- Import the public key of the receiver:
```bash
gpg --import filename_containing_public_key_of_receiver
```

Signing Keys
Sender can sign the public key of the receiver to establish trust:
```bash
gpg --sign-key receiver_email
```

Encrypting Data
Encrypt a file for a specific receiver:
```bash
gpg --encrypt -r receiver_email name_of_file  .gpg file created
```

Encrypt and sign a file (ASCII format):
```bash
gpg --encrypt --sign --armor -r receiver_email name_of_file  ASCII file created
```

Encrypt and sign a file (.gpg format):
```bash
gpg --encrypt --sign -r receiver_email name_of_file  .gpg file created
```

Decrypting Data
Decrypt a file:
```bash
gpg -o myfiledecrypted -d myfile.txt.gpg
```
```

Name : Aman Singh

Roll no : 128, Batch : T23 , Subject : Security Lab

Output:

```
educatoraman@LAPTOP-SDB

educatoraman@LAPTOP-SDBSD6JR:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: abc
Name must be at least 5 characters long
Real name: abcd1
Email address: abcd@gmail.com
You selected this USER-ID:
    "abcd1 <abcd@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 8560036AC84F72C6 marked as ultimately trusted
gpg: revocation certificate stored as '/home/educatoraman/.gnupg/openpgp-revocs.d/16896F3FFB6566F8983B326F8560036AC84F72C6.rev'
public and secret key created and signed.

pub   rsa3072 2023-10-15 [SC] [expires: 2025-10-14]
      16896F3FFB6566F8983B326F8560036AC84F72C6
uid                      abcd1 <abcd@gmail.com>
```

```
educatoraman@LAPTOP-SDB

educatoraman@LAPTOP-SDBSD6JR:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: erty2
Email address: erty@gmail.com
You selected this USER-ID:
    "erty2 <erty@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 9CC032BE044408FB marked as ultimately trusted
gpg: revocation certificate stored as '/home/educatoraman/.gnupg/openpgp-revocs.d/ECEE696E0AE630BF5EA722729CC032BE044408FB.rev'
public and secret key created and signed.

pub   rsa3072 2023-10-15 [SC] [expires: 2025-10-14]
      ECEE696E0AE630BF5EA722729CC032BE044408FB
uid                      erty2 <erty@gmail.com>
sub   rsa3072 2023-10-15 [E] [expires: 2025-10-14]
```

Name : Aman Singh

Roll no : 128, Batch : T23 , Subject : Security Lab

```
educatoraman@LAPTOP-SDB

educatoraman@LAPTOP-SDBSD6JR:~$ gpg --export -a abcd1>spub
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --export-secret-key -a abcd1>spri
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --export-secret-key -a abcd1 spri
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQWGBGUri64BDACvoIoehlnzf1pBepSJzL+7BaKE6mJupPFriTnBNyrUPyDqPN5d
SOQul/HqB9QCR1y9+8wEF6ns1cqGEX5r1L+hyxgCpTJL/cBOWtmXbpxBh6/3MD/H
sNg3jGUY+WgWDibNdL/Qdwhpk9zPmWHyyiUhC7wAVmIRZbQmlpgJYeTm2X8rzHg8
2OzNG7/U0px/PwRn5rCCVr+QAwN+vMUYDVLWYFYyAIXMVq8D1dFX/OIg748MxmT5
YBVULELFT+Dnvv2+ym4g/a+mtS4zwUE9LHBpt7ezuALE7sVw1e4bcjN8fXs6dvql
ak+ZeniSK6zC1RthlcvZ4o68ubLO7NSsU8lrT7jXlkaCmO6XnyhLY6HRGXp56Eh+
3Xp8PzGqF1CV6eUJqfboU+9GLteTdLs1sphNXz8FhOzSY78Zjea7L7A6UJG8u/Ir
sPpUqtTqfuPF6rp85jxYAFU45Mdu/Y6y9g0sANu244i0v59mVOhbFPu4pXBr5aTQ
2iUJ8wsgZOWq6B8AEQEAAf4HAwJ8cSTSmaVwjP/V8NLEAa6j46aoCzuLqVnDA+2n
0CA6Tpb+rViRuF23O9gIDzptEC615mNZOHV0VAfJehPk4KeUesHspeeYQ/qzKlgk
8pMTicE9mYdFR902hQHzpDJqygiD1XF2fJUadfeC2U1NxNRQafez3uBLsWfCrhN5
scrzhfrpynX552SsnPmaBCXYvZvSgdTlkVVKjWpqZexTbKiBBeyvBb81GXNIb3p5
7FaB+Z2SFOasC1dDa1wG4SBJsZ+pHJYvWy7zIkanOnG8WcBxDQcbmaMEUHV1f4ds
tPaAyve/7oxPYwUVqMPRRkuv4SnrEwCXqkyhGHreDKvEEJfiK+xiL6NrVxfoznZj
PCTJsI9NEU3JJVBOD/rzqWO9qziwOG7R5nN3bB97Nwwtzitru EHwpt2r7dsG9Eat
P+QTZ3F8VesFXZ3Us7RvVsY0/OuDibvbifvy31YA4+2p3LXPVLiJ0yougxkD8/iK
VZBzRr00KgUqGQ5OLMA04oIwOjDCH+XzNNwkQuu3hV6X8STZJyup1Mb0WF/i2Bjq
GpNy6QC30ecqe8AsKCUuXhlhFqLV/UbrSTG7OSC+EP7+0oxvHIkwX8/2Qb0PMKAl
oCUuOaCV3rldtKqsYmMrZkpwlxGWRZGH3o5/pxmQy5BCRkuUx9I+vxbRD5/kx9zo
U2k2IeL7z4H1svaxZPN9q4vn8JBUAxqhyvJfizxDBc8hK2BcFNU48TT9rkDzOLHK
BACtRx/4VOmefNMztc2HFnEZfUueLK85bFm4P6qcyTlwthOCkljJ38AQ900QxKsk
RjpupHVf9kGdZQNMsQf5UamRSOVPRIDUyfsaeA9INv5GdH2krye6KMzY6qRtBe8v
Jma3r7BosWUeJrYZPcTRFyNU7ivp3GlZFb0/ozuhI1Vb9f0Vvnh4a0ZFfPZUCS8o
ARBh9YmStCgu8Bx0WwzTyhX91dhvdFJcTrJJJ81onTdWLqY/B9RBB411Jid14U47
IKc/SIXzMteZes7duh/YNqvbj3hWHAiczRGj93YCcM+7xTUM6lsCS9YrrZMbf4BP
RH25nPiu/azsIYPrlKC8HkQlSBNYadUA7J4jSsFbz8FbimRUSfSlc//xL2vZ6hHR
```

```
educatoraman@LAPTOP-SDB

Y4LkpGtlmvX9GaHpaQJe1eVlN3hRaR9HWdmhS1/zqRY=
=2apW
-----END PGP PRIVATE KEY BLOCK-----
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --export -a erty2>rpub
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --export-secret-key -a erty2>rpri
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --export-secret-key -a erty2 rpri
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQWGBGUrjAIBDADyWq/q4xytt5paCM1EkPFGRcpi2+9+ahfEeU4pp80nPX9f+uto
zIV67l1EmpZxOSnIKvHQSsGq+MYyc69xhs4Xkkll7RaQFEBc+xPQvivG9WF4KrZl
nBAnooBd+pX+nevoylkKOuMqECtPD8+eckfvnvnKukiscA8CWGzK4A2Pk0X6dfX1
wMkKYf/UOUVGBcAZgUPQpZ6TRq5woMn4UhqVgfSsfqWqNvw6yoPSHOFqS4rsdhDK
vCeWuvqPhYCn5g04+cZmM65KIbNzeyZaBPBUVL3syA/EGfR1wIH8NRO2kSBGI4rY
Lr4z0A0AhFdI3iQtTtPMXXapchKx8NxO6uCq8R+zb6h/gLu4Z6uMWRU3Efmy4UtZ
hmu2CsfkTrKieqlafiHMPRen++3jqR89OiMCjR/qPeByh/UFTzyFFkX2AK3cSENw
iA57WVjbqWFxx0z1upyECwIR2A5951j8EAKgQEj3SAQGlPB76LGJYRZdPVq5Ey3D
v34EJ56ezsn59KEAEQEAAf4HAwJVOPPjb0Z6mP9hEpTJIqyRmthdc6ogYUXDE9jZ
lOVIJ4OzwICBybzFkhXbZ4XjlzoSujKcsU5yZttfZ11AUb6iDJ74BBRcKXm8JA56
QOUbwmOlAisLt2GSnMNBTB1F+AUHqXwuaAGjxuVFhYsTW/8hJNq9U8i5cOoP6JPB
Oi7blVqELiHe6SNeXC+3RODyuZFdPzckhGP/rlyFHe0XbFT+BxCM2+R/7h3k1/qM
TXH+EOTnl9+OPAYPJEa4/ybMsC5zqaqSfDJx0xlVQx692DlrhyOzUTePt3DYTpe7
9ZI5JZH672O/GB1kBp63efXjPYd5axdwjumUKAP/XiLTdY6R5C4Lo3wkgfS/F+HI
Z2DpD+ywFLZGWbrs9kwxhK2m2pgYyiKkAqD/9GSPlGkkJrUA1CIdd1UVTbb5W1GL
JCBXku5PTs6JTLHvt/vNkrhUV/w+tPZTAh6zEC0e8Hh2CFtMi+RRhWux11YM8+8Z
3hXWfGs+SM8fX5bHkNSfz3ne9tE2VOtWNO8Tsj1FXdXaKsDrRANaVW9Q4wjil9ha
Y4jDSlrvgOsNOrZTn/nKYnadHCqsGYYDw0J6Q1ipLAqb0Y/k78/cwojySQ57+INL
79eIzNCTz+dUGap7t8LUgTvMQRigYivyoT5orN32EQxabYjrJTkU+CNsLt0K7c/V
lZKy19CkeaJE0zPqBx6MyzBDjqtWnOthCiDDQxNeQs/B5a2Ufrhy72sm2YgHmI6U
d3Ve215rWO3iLNsyIA/eWAhOpAn8xRaY6gezzz3TRnaoh9iKDUaxQPWBgdDTSzKL
/+Xgsvhh1Q7cHYKNQiJX6DqA8y2Qwx1FCBX/MEokY0RHSzivAl1mE2kEY5C5N6kZ
rtntd6q5dqoii508CoApqtyvBzae/HfZH0QmO8lndS8n2dybfEGVPZWVarHo57H1
gM98HenqgeQJwH5l6602zutWBr2VXNVWVshMk5bFAAOBMg3+Sp2+ze0bJKxot42g
```

Name : Aman Singh

Roll no : 128, Batch : T23 , Subject : Security Lab

```
educatoraman@LAPTOP-SDB

1Q9v3MShLEMwbEGXAEEPmj7JztC+2c17skt1A2kihhpa/rPcT6l8fvYpiqUAXrTV
D8hDQ+WmQ6dXZefg32ObzIc2iPUQJ+2il4MCDfFk+t4=
=b2nE
-----END PGP PRIVATE KEY BLOCK-----
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --import rpub
gpg: key 9CC032BE044408FB: "erty2 <erty@gmail.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --encrypt -r erty2 hi
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:  11  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 11u
gpg: next trustdb check due at 2025-09-25
gpg: can't open 'hi': No such file or directory
gpg: hi: encryption failed: No such file or directory
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --allow-secret-key-import --import rpri
gpg: key 9CC032BE044408FB: "erty2 <erty@gmail.com>" not changed
gpg: key 9CC032BE044408FB: secret key imported
gpg: Total number processed: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:  secret keys unchanged: 1
educatoraman@LAPTOP-SDBSD6JR:~$ gpg --list-keys
/home/educatoraman/.gnupg/pubring.kbx
---------------------------------
pub   rsa3072 2023-09-26 [SC] [expires: 2025-09-25]
      2057E25359431F0827BE6CEA170FA0FD0B969A50
uid           [ultimate] aman singh <aman123@gmail.com>
sub   rsa3072 2023-09-26 [E] [expires: 2025-09-25]

pub   rsa3072 2023-09-26 [SC] [expires: 2025-09-25]
      C731464D9AE08A1AC9C08435FCF02274DE14D00D
```

```
educatoraman@LAPTOP-SDB

ssb   rsa3072 2023-10-15 [E] [expires: 2025-10-14]

sec   rsa3072 2023-10-15 [SC] [expires: 2025-10-14]
      25724A570A5388253B2C6CB5629DBE00EE2E7356
uid           [ultimate] aman2 <aman2@gmail.com>
ssb   rsa3072 2023-10-15 [E] [expires: 2025-10-14]

sec   rsa3072 2023-10-15 [SC] [expires: 2025-10-14]
      E74578ADF901654859539C48174C3A9276934C63
uid           [ultimate] aman1 <aman1@gmail.com>
ssb   rsa3072 2023-10-15 [E] [expires: 2025-10-14]

sec   rsa3072 2023-10-15 [SC] [expires: 2025-10-14]
      2EB833191369E2F72BF1F97F3B87D13B867B81BD
uid           [ultimate] aman2 <aman2@gmail.com>
ssb   rsa3072 2023-10-15 [E] [expires: 2025-10-14]

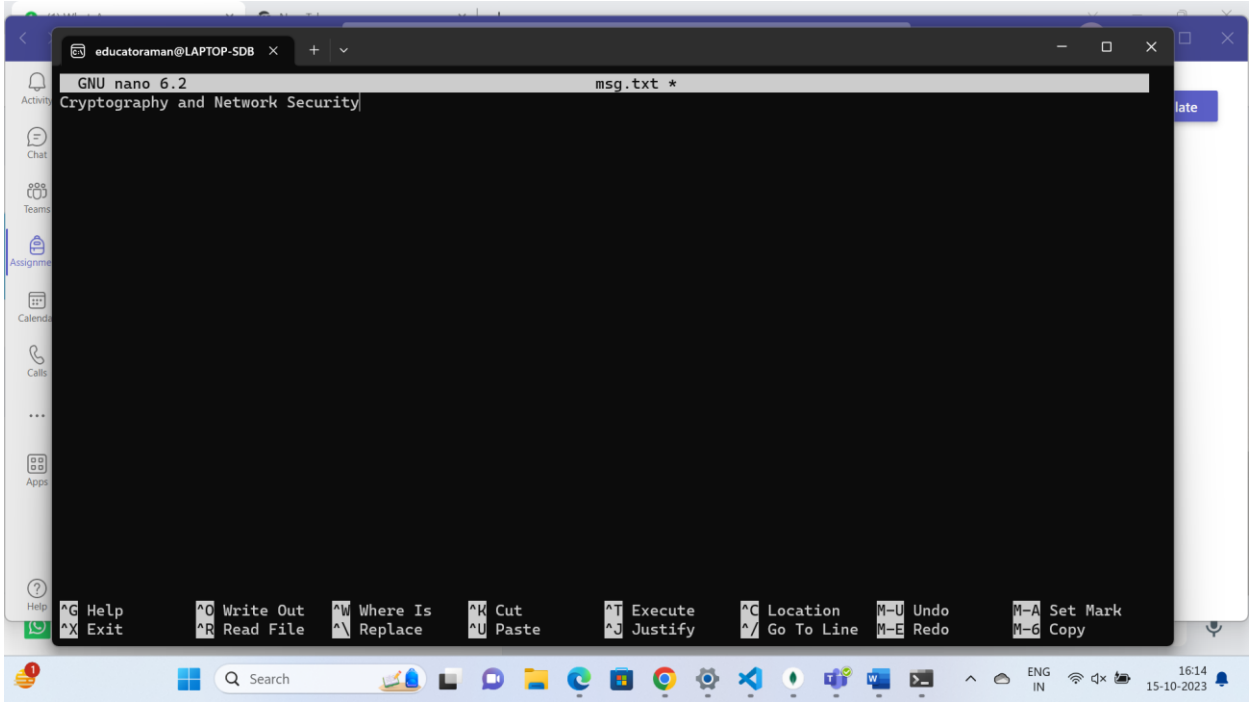
sec   rsa3072 2023-10-15 [SC] [expires: 2025-10-14]
      16896F3FFB6566F8983B326F8560036AC84F72C6
uid           [ultimate] abcd1 <abcd@gmail.com>
ssb   rsa3072 2023-10-15 [E] [expires: 2025-10-14]

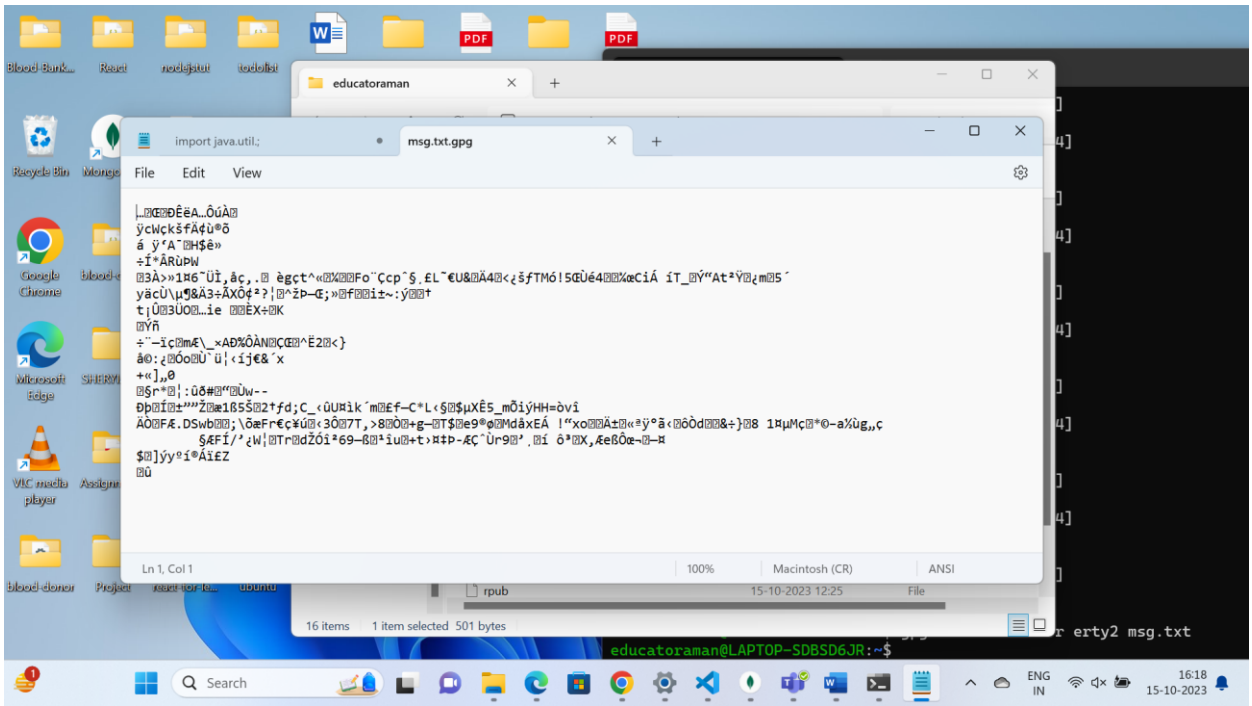
sec   rsa3072 2023-10-15 [SC] [expires: 2025-10-14]
      ECEE696E0AE630BF5EA722729CC032BE044408FB
uid           [ultimate] erty2 <erty@gmail.com>
ssb   rsa3072 2023-10-15 [E] [expires: 2025-10-14]

educatoraman@LAPTOP-SDBSD6JR:~$ nano msg.txt
educatoraman@LAPTOP-SDBSD6JR:~$ gpg -e -u abcd1 -r erty2 msg.txt
educatoraman@LAPTOP-SDBSD6JR:~$
```

Name : Aman Singh

Roll no : 128, Batch : T23 , Subject : Security Lab





Name : Aman Singh

Roll no : 128, Batch : T23 , Subject : Security Lab

Conclusion:

In summary, we explored GPG's private and public key rings, key management, and security processes. These are vital for secure communication and trust verification in digital exchanges.