Roll Number:- 2105048
Name:-Manav Jain
Date:- 13/09/2023

Lab Assignment No:-13

Aim:- Explore the GPG tool of Linux to implement email security

Lab Outcome Attained :- LO6

Theory:-

What is private key ring and public key ring ?

a)Public key ring

The public key ring contains the public keys of other users. These keys are made available to the public so that anyone can encrypt messages to the user. The public key ring is typically shared with other users by exporting it to a file or by adding it to a PGP keyserver.

The public key contains the following information:

The user's name or email address
The user's fingerprint, which is a unique identifier for the key
The key's algorithm and strength
The key's expiration date
When someone wants to encrypt a message to you, they will use your public key. The message will be encrypted using the public key, but it can only be decrypted using the corresponding private key.

b)Private key ring

The private key ring contains the private keys of the user. These keys are kept secret and should not be shared with anyone. The private key ring is typically protected by a password or passphrase.

The private key contains the following information:

The user's name or email address

The user's fingerprint, which is a unique identifier for the key

The key's algorithm and strength

The key's expiration date

The private key is used to decrypt messages that have been encrypted with the user's public key. It is also used to sign messages, which allows the recipient to verify that the message was sent by the intended sender.

The public key ring and the private key ring are essential for using PGP. They allow users to encrypt and decrypt messages securely.

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

Key generation

The following command generates a new GPG key pair:

gpg --gen-key

This command will prompt you for some information, such as your name, email address, and key length.

Export and import of keys

The following command exports the public key to a file:

```
gpg --export --output public.key
```

The following command imports the public key from a file:

```
gpg --import public.key
```

The following command exports the private key to a file:

```
gpg --export-secret-key --output private.key
```

The following command imports the private key from a file:

```
gpg --import-secret-key private.key
```

Signing and encrypting the message The

following command signs a message:

```
gpg --sign message.txt
```

The following command encrypts a message:

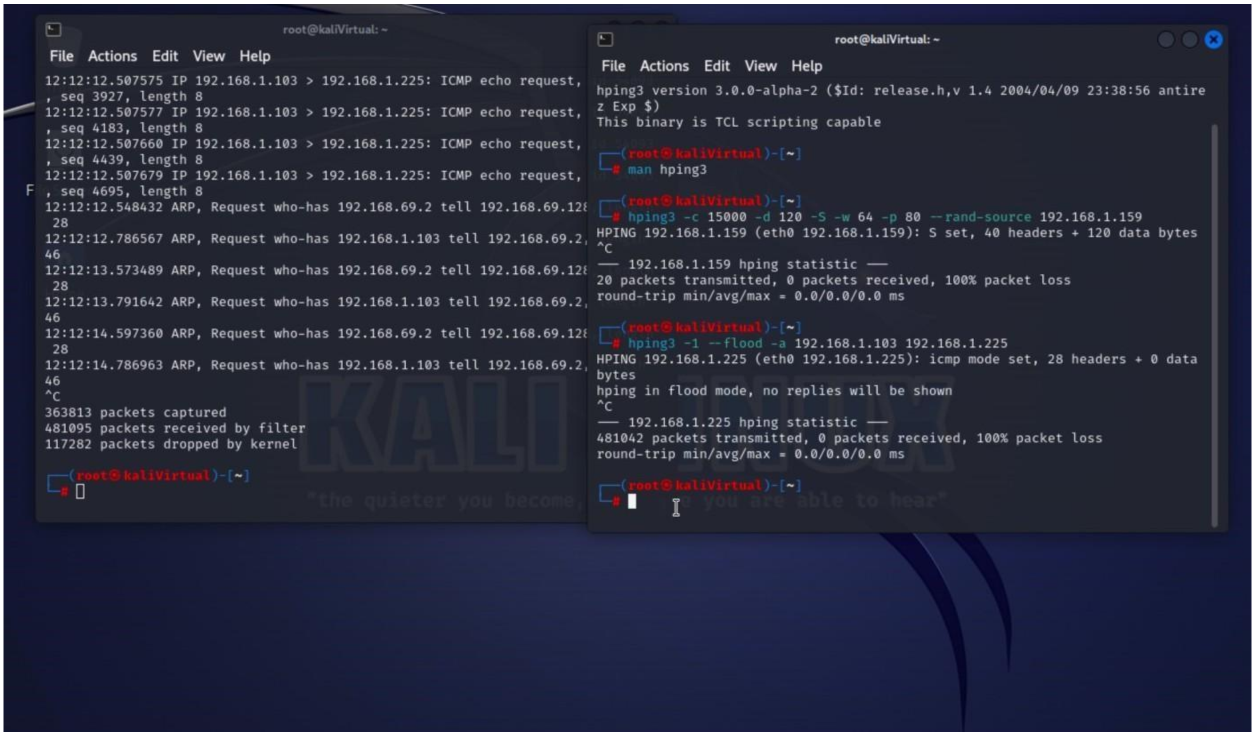
```
gpg --encrypt --recipient recipient@example.com message.txt
```

The recipient can then decrypt the message using their private key.

Some additional details about the commands:

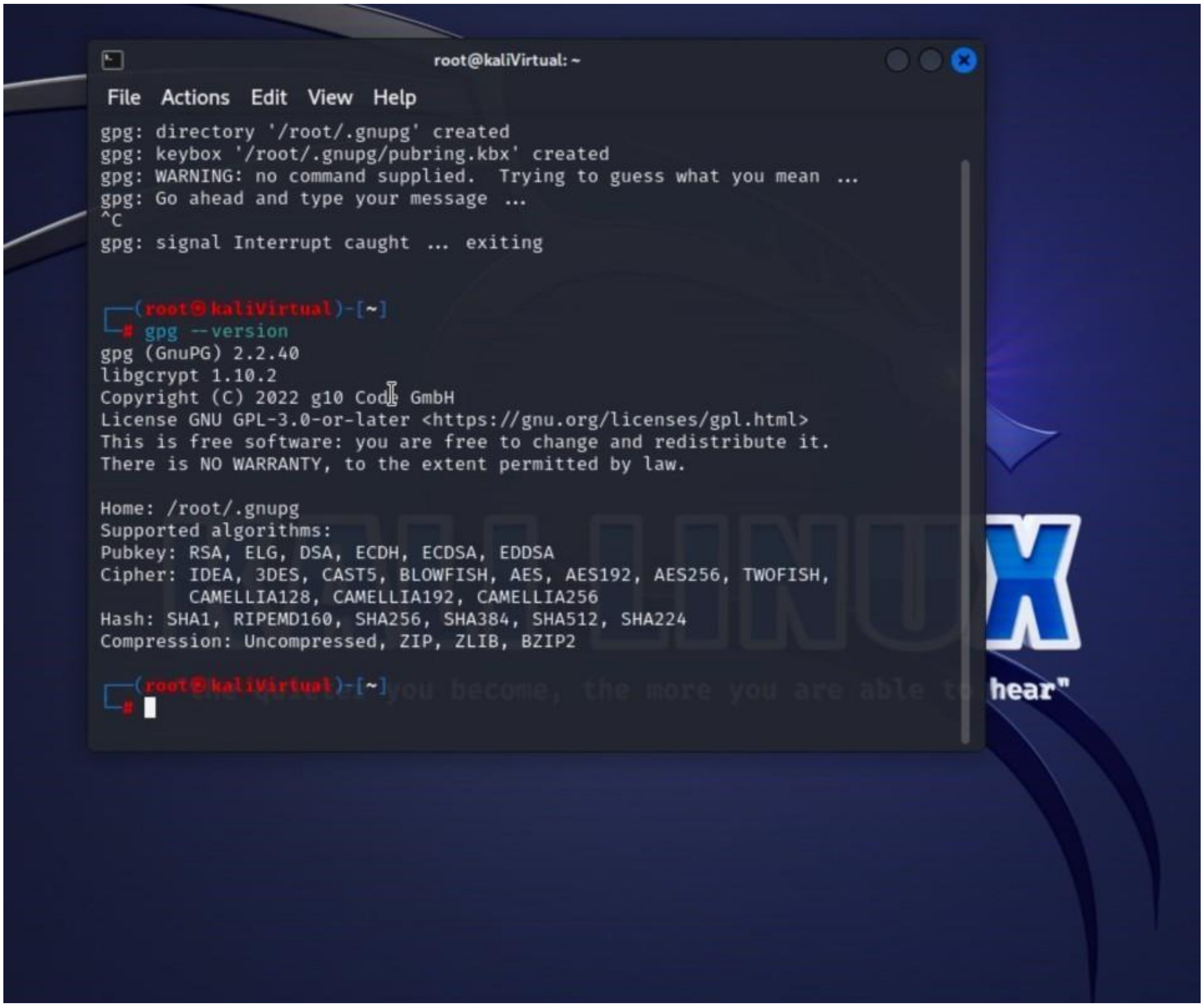
The gpg command is the main GPG command.
The **--gen-key** option generates a new GPG key pair.
The **--export** option exports a key to a file.
The **--import** option imports a key from a file.
The **--sign** option signs a message.
The **--encrypt** option encrypts a message.
The **--recipient** option specifies the recipient of the encrypted message.

Output Screenshots

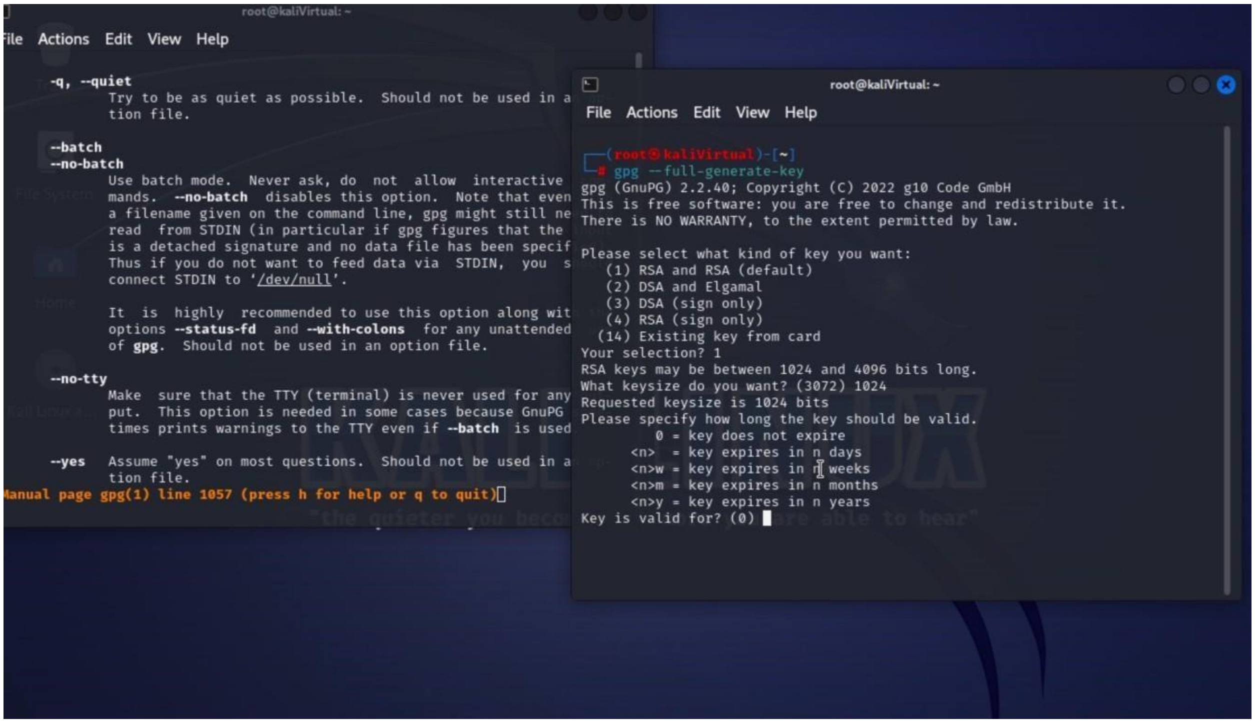


```
12:12:12.507575 IP 192.168.1.103 > 192.168.1.225: ICMP echo request,
, seq 3927, length 8
12:12:12.507577 IP 192.168.1.103 > 192.168.1.225: ICMP echo request,
, seq 4183, length 8
12:12:12.507660 IP 192.168.1.103 > 192.168.1.225: ICMP echo request,
, seq 4439, length 8
12:12:12.507679 IP 192.168.1.103 > 192.168.1.225: ICMP echo request,
, seq 4695, length 8
12:12:12.548432 ARP, Request who-has 192.168.69.2 tell 192.168.69.128
 28
12:12:12.786567 ARP, Request who-has 192.168.1.103 tell 192.168.69.2,
46
12:12:13.573489 ARP, Request who-has 192.168.69.2 tell 192.168.69.128
 28
12:12:13.791642 ARP, Request who-has 192.168.1.103 tell 192.168.69.2,
46
12:12:14.597360 ARP, Request who-has 192.168.69.2 tell 192.168.69.128
 28
12:12:14.786963 ARP, Request who-has 192.168.1.103 tell 192.168.69.2,
46
^C
363813 packets captured
481095 packets received by filter
117282 packets dropped by kernel

┌──(root㉿kaliVirtual)-[~]
└─# 
```

```
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antire
z Exp $)
This binary is TCL scripting capable

┌──(root㉿kaliVirtual)-[~]
└─# man hping3

┌──(root㉿kaliVirtual)-[~]
└─# hping3 -c 15000 -d 120 -S -w 64 -p 80 --rand-source 192.168.1.159
HPING 192.168.1.159 (eth0 192.168.1.159): S set, 40 headers + 120 data bytes
^C
--- 192.168.1.159 hping statistic ---
20 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿kaliVirtual)-[~]
└─# hping3 -1 --flood -a 192.168.1.103 192.168.1.225
HPING 192.168.1.225 (eth0 192.168.1.225): icmp mode set, 28 headers + 0 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.225 hping statistic ---
481042 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿kaliVirtual)-[~]
└─# 
```

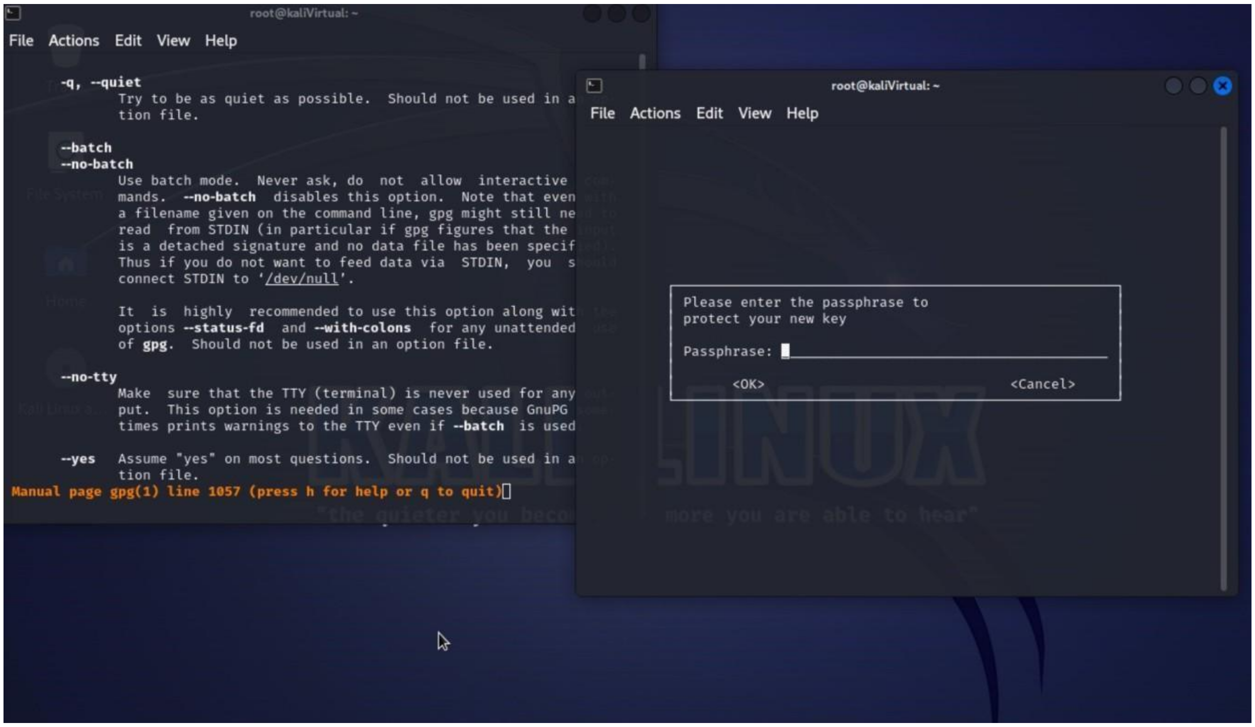


```
gpg: directory '/root/.gnupg' created
gpg: keybox '/root/.gnupg/pubring.kbx' created
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: Go ahead and type your message ...
^C
gpg: signal Interrupt caught ... exiting


┌──(root㉿kaliVirtual)-[~]
└─# gpg --version
gpg (GnuPG) 2.2.40
libgcrypt 1.10.2
Copyright (C) 2022 g10 Code GmbH
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /root/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2

┌──(root㉿kaliVirtual)-[~]
└─# 
```



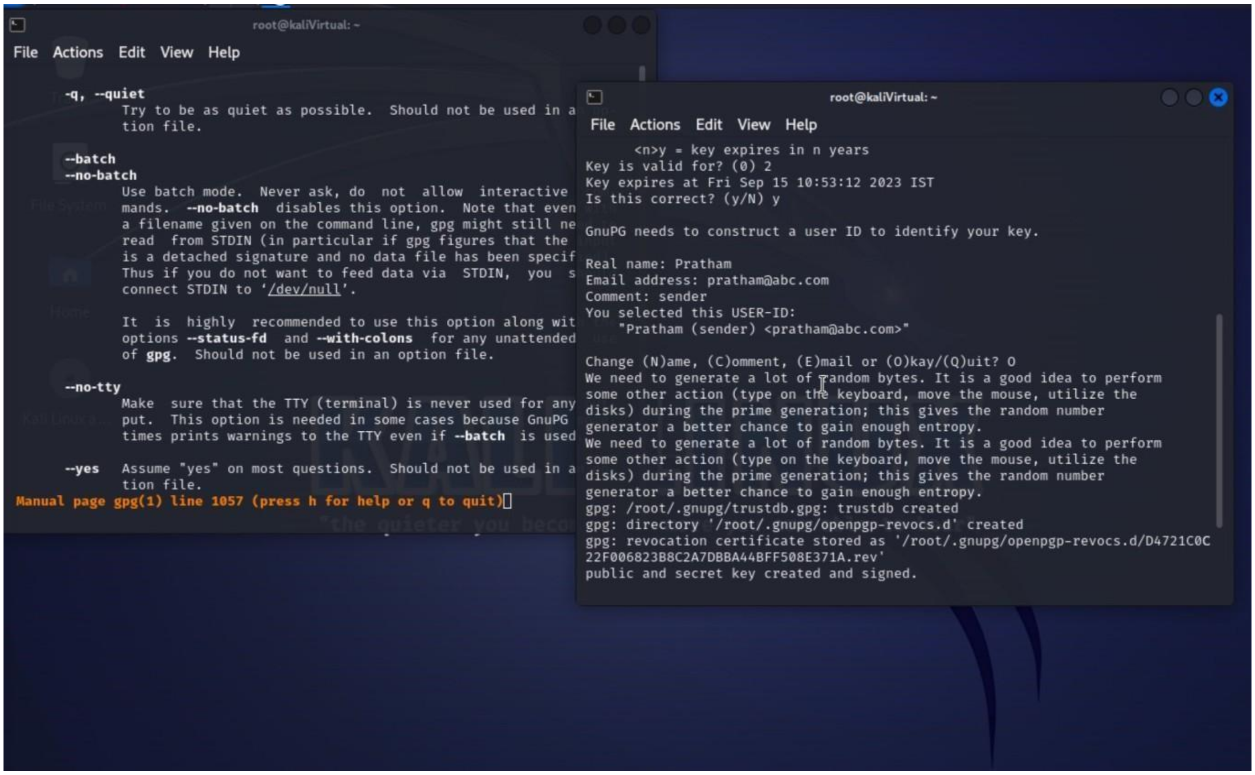
```
   -q, --quiet
          Try to be as quiet as possible.  Should not be used in a
          tion file.

   --batch
   --no-batch
          Use batch mode.  Never ask, do  not  allow  interactive
          mands.  --no-batch  disables this option.  Note that even
          a filename given on the command line, gpg might still ne
          read  from STDIN (in particular if gpg figures that the
          is a detached signature and no data file has been specif
          Thus if you do not want to feed data via  STDIN,  you  s
          connect STDIN to '/dev/null'.

          It  is  highly  recommended to use this option along wit
          options --status-fd  and --with-colons  for any unattended
          of gpg.  Should not be used in an option file.

   --no-tty
          Make  sure that the TTY (terminal) is never used for any
          put.  This option is needed in some cases because GnuPG
          times prints warnings to the TTY even if --batch  is used

   --yes  Assume "yes" on most questions.  Should not be used in a
          tion file.
Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
┌──(root㉿kaliVirtual)-[~]
└─# gpg --full-generate-key
gpg (GnuPG) 2.2.40; Copyright (C) 2022 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 1024
Requested keysize is 1024 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
```



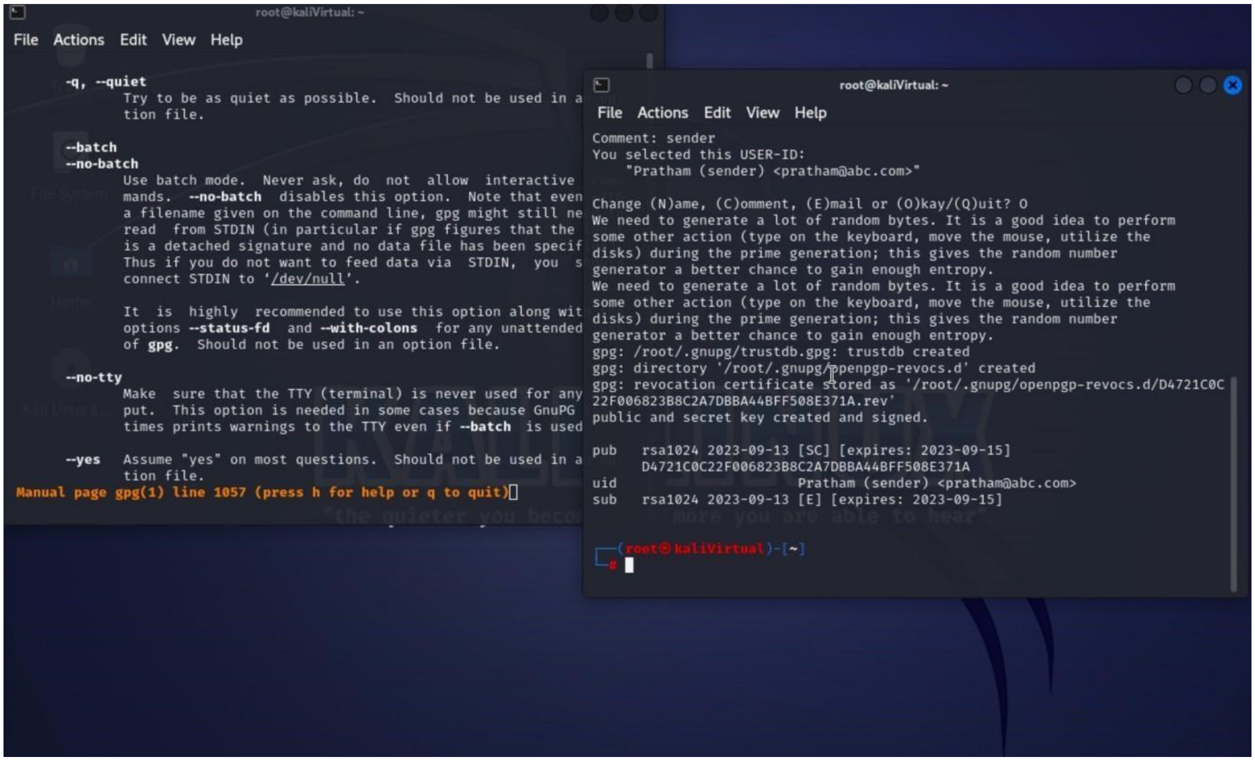
```
   -q, --quiet
          Try to be as quiet as possible.  Should not be used in a
          tion file.

   --batch
   --no-batch
          Use batch mode.  Never ask, do  not  allow  interactive
          mands.  --no-batch  disables this option.  Note that even
          a filename given on the command line, gpg might still ne
          read  from STDIN (in particular if gpg figures that the
          is a detached signature and no data file has been specif
          Thus if you do not want to feed data via  STDIN,  you  s
          connect STDIN to '/dev/null'.

          It  is  highly  recommended to use this option along wit
          options --status-fd  and --with-colons  for any unattended
          of gpg.  Should not be used in an option file.

   --no-tty
          Make  sure that the TTY (terminal) is never used for any
          put.  This option is needed in some cases because GnuPG
          times prints warnings to the TTY even if --batch  is used

   --yes  Assume "yes" on most questions.  Should not be used in a
          tion file.
Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
Please enter the passphrase to
protect your new key

Passphrase: ________________________________

     <OK>                               <Cancel>
```



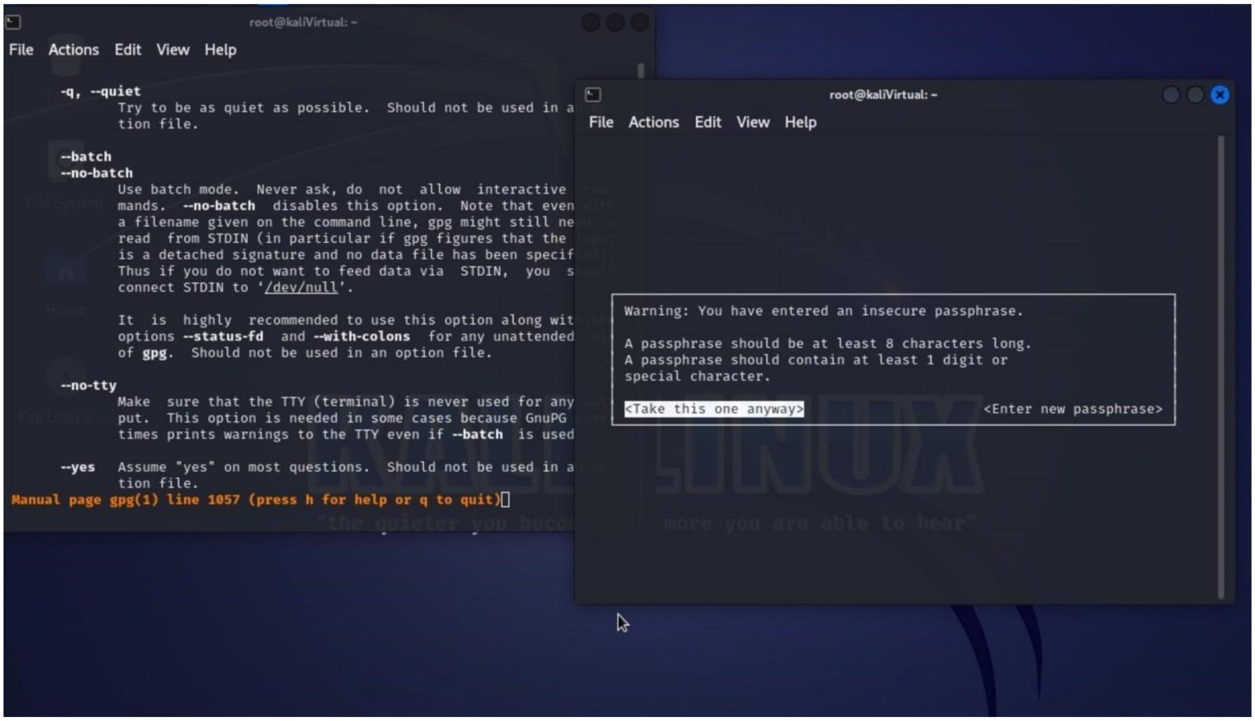
```
       -q, --quiet
              Try to be as quiet as possible.  Should not be used in a
              tion file.

       --batch
       --no-batch
              Use batch mode.  Never ask, do  not  allow  interactive
              mands.  --no-batch  disables this option.  Note that even
              a filename given on the command line, gpg might still ne
              read  from STDIN (in particular if gpg figures that the
              is a detached signature and no data file has been specif
              Thus if you do not want to feed data via  STDIN,  you  s
              connect STDIN to '/dev/null'.

              It  is  highly  recommended to use this option along wit
              options --status-fd  and --with-colons  for any unattended
              of gpg.  Should not be used in an option file.

       --no-tty
              Make  sure that the TTY (terminal) is never used for any
              put.  This option is needed in some cases because GnuPG
              times prints warnings to the TTY even if --batch  is used

       --yes  Assume "yes" on most questions.  Should not be used in a
              tion file.
 Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
      <n>y = key expires in n years
Key is valid for? (0) 2
Key expires at Fri Sep 15 10:53:12 2023 IST
Is this correct? (y/N) y

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

Real name: Pratham
Email address: pratham@abc.com
Comment: sender
You selected this USER-ID:
    "Pratham (sender) <pratham@abc.com>"

Change (N)ame, (C)omment, (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: /root/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/root/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/D4721C0C
22F006823B8C2A7DBBA44BFF508E371A.rev'
public and secret key created and signed.
```



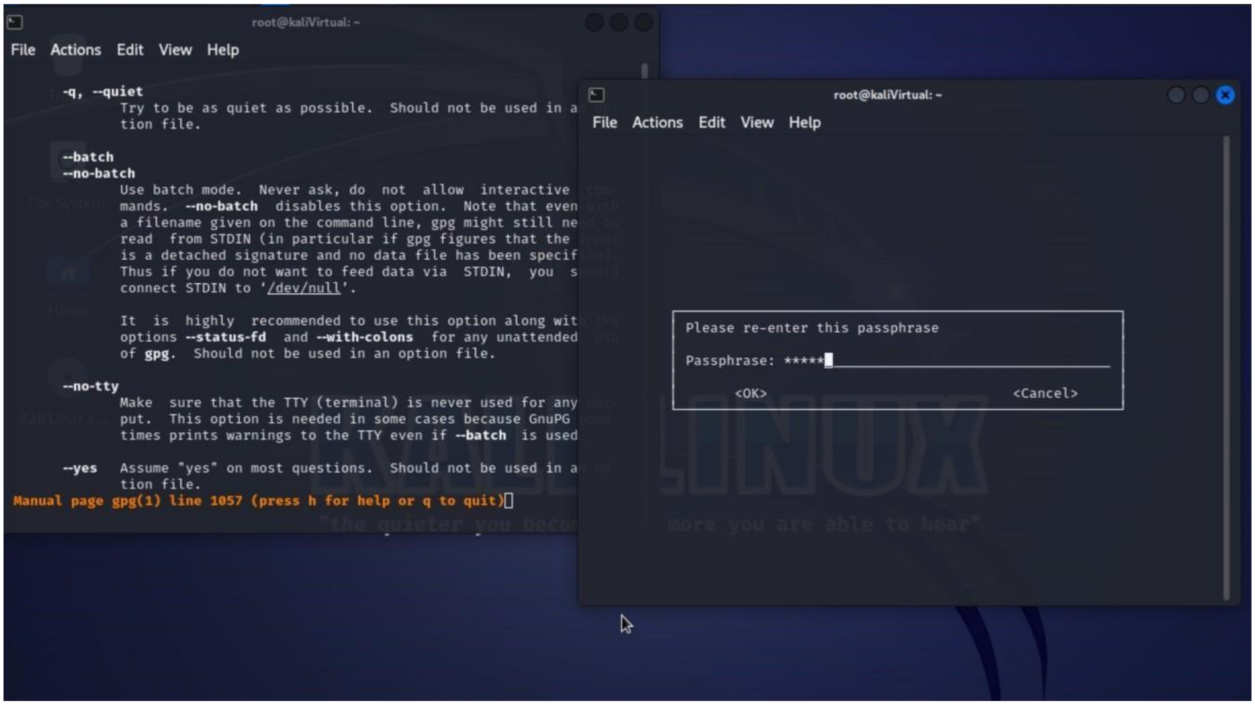
```
       -q, --quiet
              Try to be as quiet as possible.  Should not be used in a
              tion file.

       --batch
       --no-batch
              Use batch mode.  Never ask, do  not  allow  interactive
              mands.  --no-batch  disables this option.  Note that even
              a filename given on the command line, gpg might still ne
              read  from STDIN (in particular if gpg figures that the
              is a detached signature and no data file has been specif
              Thus if you do not want to feed data via  STDIN,  you  s
              connect STDIN to '/dev/null'.

              It  is  highly  recommended to use this option along wit
              options --status-fd  and --with-colons  for any unattended
              of gpg.  Should not be used in an option file.

       --no-tty
              Make  sure that the TTY (terminal) is never used for any
              put.  This option is needed in some cases because GnuPG
              times prints warnings to the TTY even if --batch  is used

       --yes  Assume "yes" on most questions.  Should not be used in a
              tion file.
 Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
Comment: sender
You selected this USER-ID:
    "Pratham (sender) <pratham@abc.com>"

Change (N)ame, (C)omment, (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: /root/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/root/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/D4721C0C
22F006823B8C2A7DBBA44BFF508E371A.rev'
public and secret key created and signed.

pub   rsa1024 2023-09-13 [SC] [expires: 2023-09-15]
      D4721C0C22F006823B8C2A7DBBA44BFF508E371A
uid                      Pratham (sender) <pratham@abc.com>
sub   rsa1024 2023-09-13 [E] [expires: 2023-09-15]


┌──(root㉿kaliVirtual)-[~]
└─# 
```



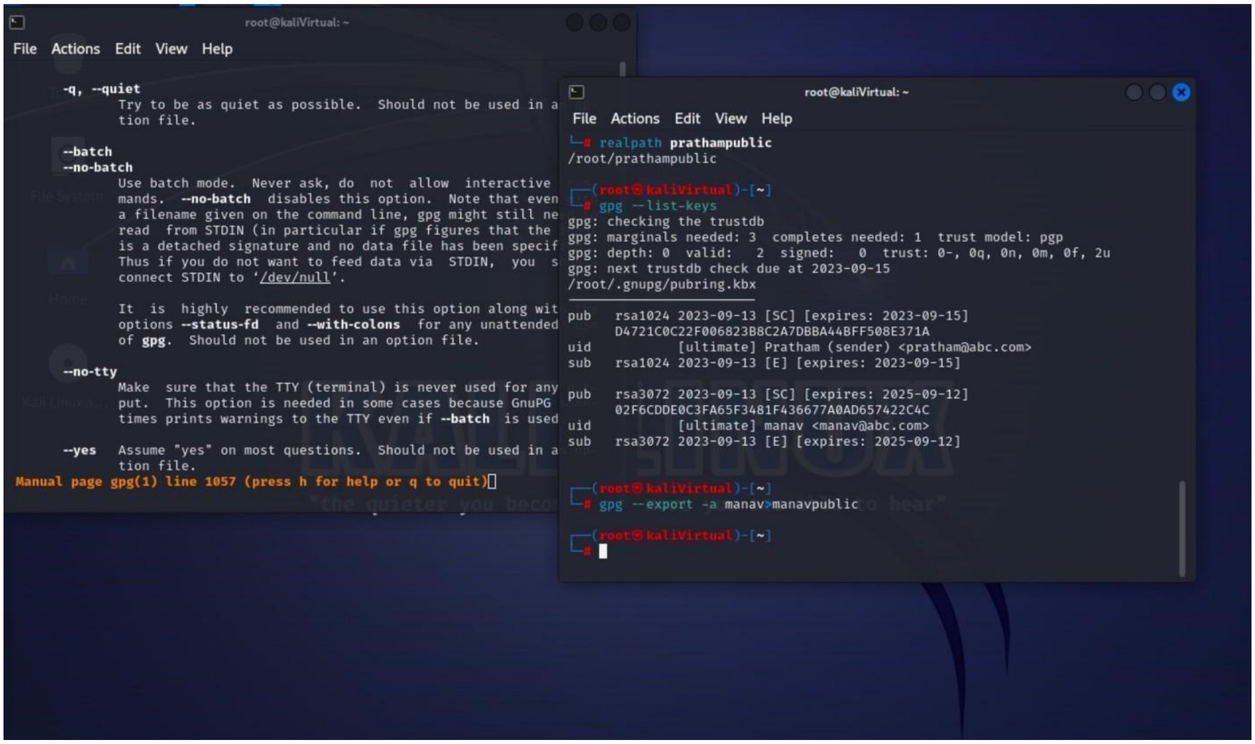
```
   -q, --quiet
          Try to be as quiet as possible.  Should not be used in a
          tion file.

   --batch
   --no-batch
          Use batch mode.  Never ask, do  not  allow  interactive
          mands.  --no-batch  disables this option.  Note that even
          a filename given on the command line, gpg might still ne
          read  from STDIN (in particular if gpg figures that the
          is a detached signature and no data file has been specif
          Thus if you do not want to feed data via  STDIN,  you  s
          connect STDIN to '/dev/null'.

          It  is  highly  recommended to use this option along wit
          options --status-fd  and --with-colons  for any unattended
          of gpg.  Should not be used in an option file.

   --no-tty
          Make  sure that the TTY (terminal) is never used for any
          put.  This option is needed in some cases because GnuPG
          times prints warnings to the TTY even if --batch  is used

   --yes  Assume "yes" on most questions.  Should not be used in a
          tion file.
Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
Warning: You have entered an insecure passphrase.

A passphrase should be at least 8 characters long.
A passphrase should contain at least 1 digit or
special character.

<Take this one anyway>                    <Enter new passphrase>
```



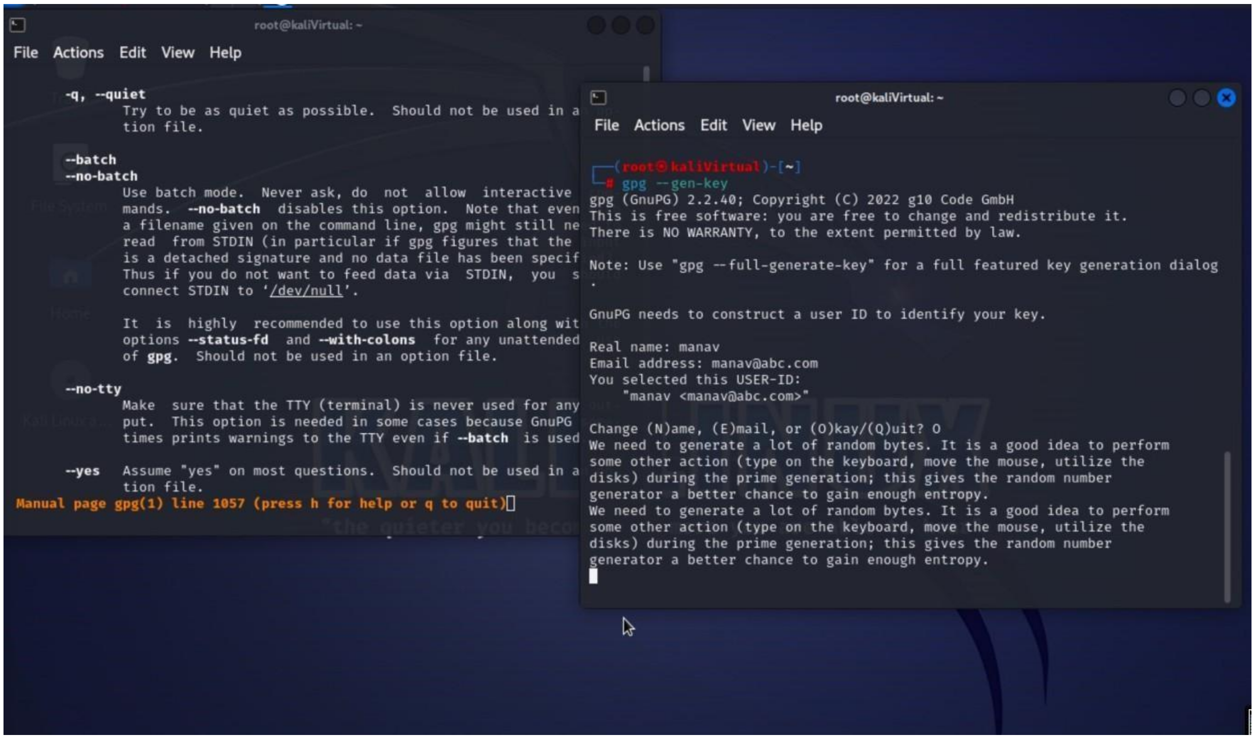
```
   -q, --quiet
          Try to be as quiet as possible.  Should not be used in a
          tion file.

   --batch
   --no-batch
          Use batch mode.  Never ask, do  not  allow  interactive
          mands.  --no-batch  disables this option.  Note that even
          a filename given on the command line, gpg might still ne
          read  from STDIN (in particular if gpg figures that the
          is a detached signature and no data file has been specif
          Thus if you do not want to feed data via  STDIN,  you  s
          connect STDIN to '/dev/null'.

          It  is  highly  recommended to use this option along wit
          options --status-fd  and --with-colons  for any unattended
          of gpg.  Should not be used in an option file.

   --no-tty
          Make  sure that the TTY (terminal) is never used for any
          put.  This option is needed in some cases because GnuPG
          times prints warnings to the TTY even if --batch  is used

   --yes  Assume "yes" on most questions.  Should not be used in a
          tion file.
Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
Please re-enter this passphrase

Passphrase: *****_______________________________

      <OK>                              <Cancel>
```



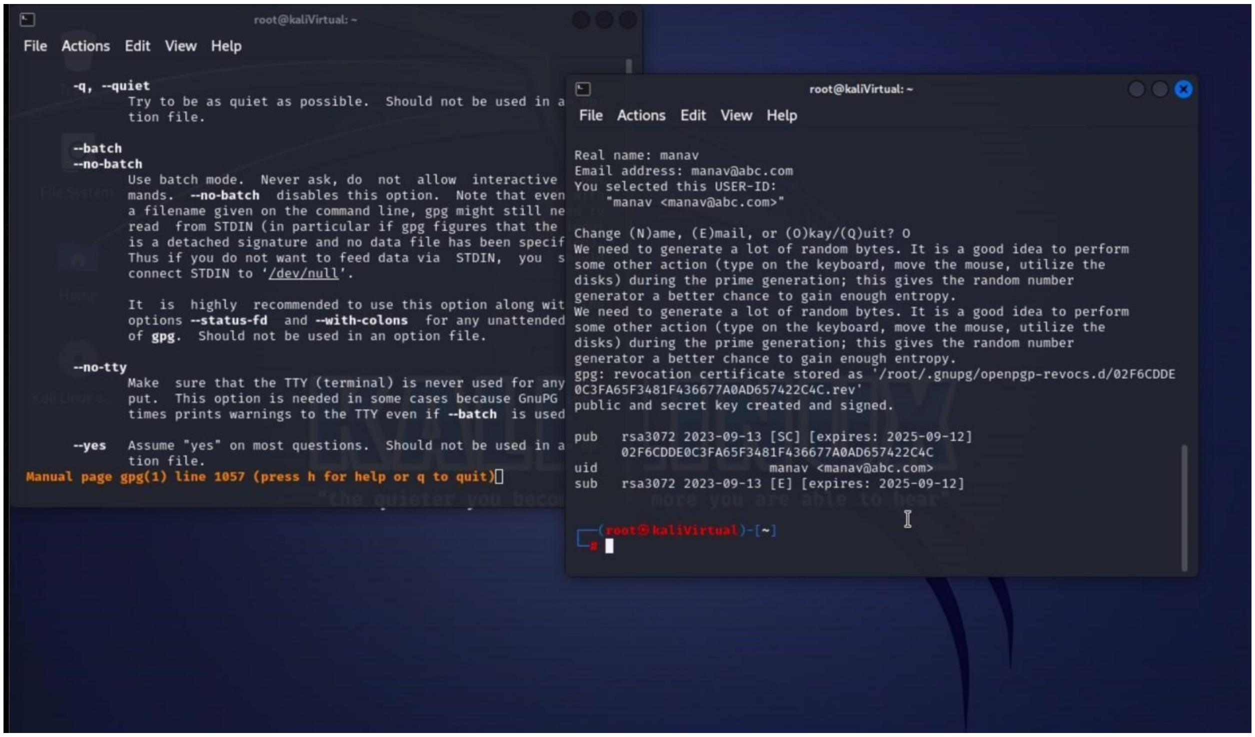
```
       -q, --quiet
              Try to be as quiet as possible.  Should not be used in a
              tion file.

       --batch
       --no-batch
              Use batch mode.  Never ask, do  not  allow  interactive
              mands.  --no-batch  disables this option.  Note that even
              a filename given on the command line, gpg might still ne
              read  from STDIN (in particular if gpg figures that the
              is a detached signature and no data file has been specif
              Thus if you do not want to feed data via  STDIN,  you  s
              connect STDIN to '/dev/null'.

              It  is  highly  recommended to use this option along wit
              options --status-fd  and --with-colons  for any unattended
              of gpg.  Should not be used in an option file.

       --no-tty
              Make  sure that the TTY (terminal) is never used for any
              put.  This option is needed in some cases because GnuPG
              times prints warnings to the TTY even if --batch  is used

       --yes  Assume "yes" on most questions.  Should not be used in a
              tion file.
 Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
└─# realpath prathampublic
/root/prathampublic

┌──(root㉿kaliVirtual)-[~]
└─# gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2023-09-15
/root/.gnupg/pubring.kbx
────────────────────────
pub   rsa1024 2023-09-13 [SC] [expires: 2023-09-15]
      D4721C0C22F006823B8C2A7DBBA44BFF508E371A
uid           [ultimate] Pratham (sender) <pratham@abc.com>
sub   rsa1024 2023-09-13 [E] [expires: 2023-09-15]

pub   rsa3072 2023-09-13 [SC] [expires: 2025-09-12]
      02F6CDDE0C3FA65F3481F436677A0AD657422C4C
uid           [ultimate] manav <manav@abc.com>
sub   rsa3072 2023-09-13 [E] [expires: 2025-09-12]


┌──(root㉿kaliVirtual)-[~]
└─# gpg --export -a manav>manavpublic

┌──(root㉿kaliVirtual)-[~]
└─# 
```



```
       -q, --quiet
              Try to be as quiet as possible.  Should not be used in a
              tion file.

       --batch
       --no-batch
              Use batch mode.  Never ask, do  not  allow  interactive
              mands.  --no-batch  disables this option.  Note that even
              a filename given on the command line, gpg might still ne
              read  from STDIN (in particular if gpg figures that the
              is a detached signature and no data file has been specif
              Thus if you do not want to feed data via  STDIN,  you  s
              connect STDIN to '/dev/null'.

              It  is  highly  recommended to use this option along wit
              options --status-fd  and --with-colons  for any unattended
              of gpg.  Should not be used in an option file.

       --no-tty
              Make  sure that the TTY (terminal) is never used for any
              put.  This option is needed in some cases because GnuPG
              times prints warnings to the TTY even if --batch  is used

       --yes  Assume "yes" on most questions.  Should not be used in a
              tion file.
 Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
┌──(root㉿kaliVirtual)-[~]
└─# gpg --gen-key
gpg (GnuPG) 2.2.40; Copyright (C) 2022 g10 Code GmbH
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: manav
Email address: manav@abc.com
You selected this USER-ID:
    "manav <manav@abc.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.
```



```
       -q, --quiet
              Try to be as quiet as possible.  Should not be used in a
              tion file.

       --batch
       --no-batch
              Use batch mode.  Never ask, do  not  allow  interactive
              mands.  --no-batch  disables this option.  Note that even
              a filename given on the command line, gpg might still ne
              read  from STDIN (in particular if gpg figures that the
              is a detached signature and no data file has been specif
              Thus if you do not want to feed data via  STDIN,  you  s
              connect STDIN to '/dev/null'.

              It  is  highly  recommended to use this option along wit
              options --status-fd  and --with-colons  for any unattended
              of gpg.  Should not be used in an option file.

       --no-tty
              Make  sure that the TTY (terminal) is never used for any
              put.  This option is needed in some cases because GnuPG
              times prints warnings to the TTY even if --batch  is used

       --yes  Assume "yes" on most questions.  Should not be used in a
              tion file.
 Manual page gpg(1) line 1057 (press h for help or q to quit)
```

```
Real name: manav
Email address: manav@abc.com
You selected this USER-ID:
    "manav <manav@abc.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: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/02F6CDDE
0C3FA65F3481F436677A0AD657422C4C.rev'
public and secret key created and signed.

pub   rsa3072 2023-09-13 [SC] [expires: 2025-09-12]
      02F6CDDE0C3FA65F3481F436677A0AD657422C4C
uid                      manav <manav@abc.com>
sub   rsa3072 2023-09-13 [E] [expires: 2025-09-12]


┌──(root㉿kaliVirtual)-[~]
└─#
```

Conclusion:-

Learnt about GPG tool in linux and how it provides email security , executed several commands related to GPG and also explored more about public key ring and private key rings