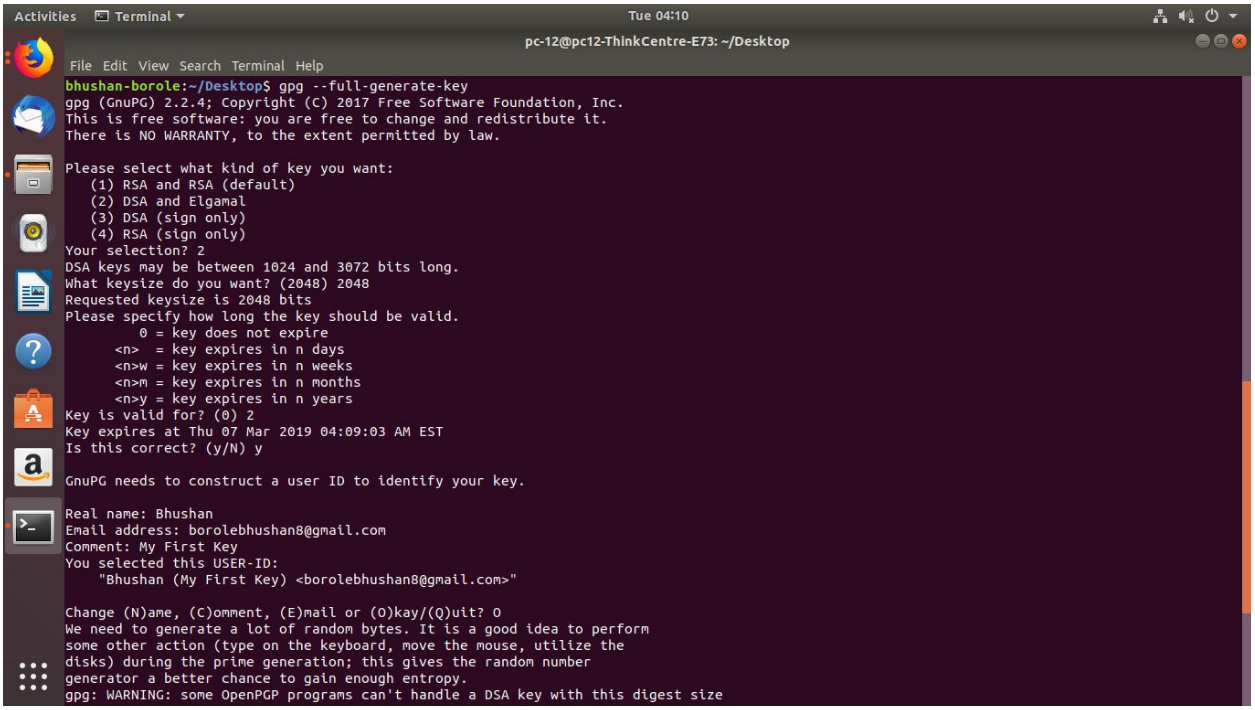
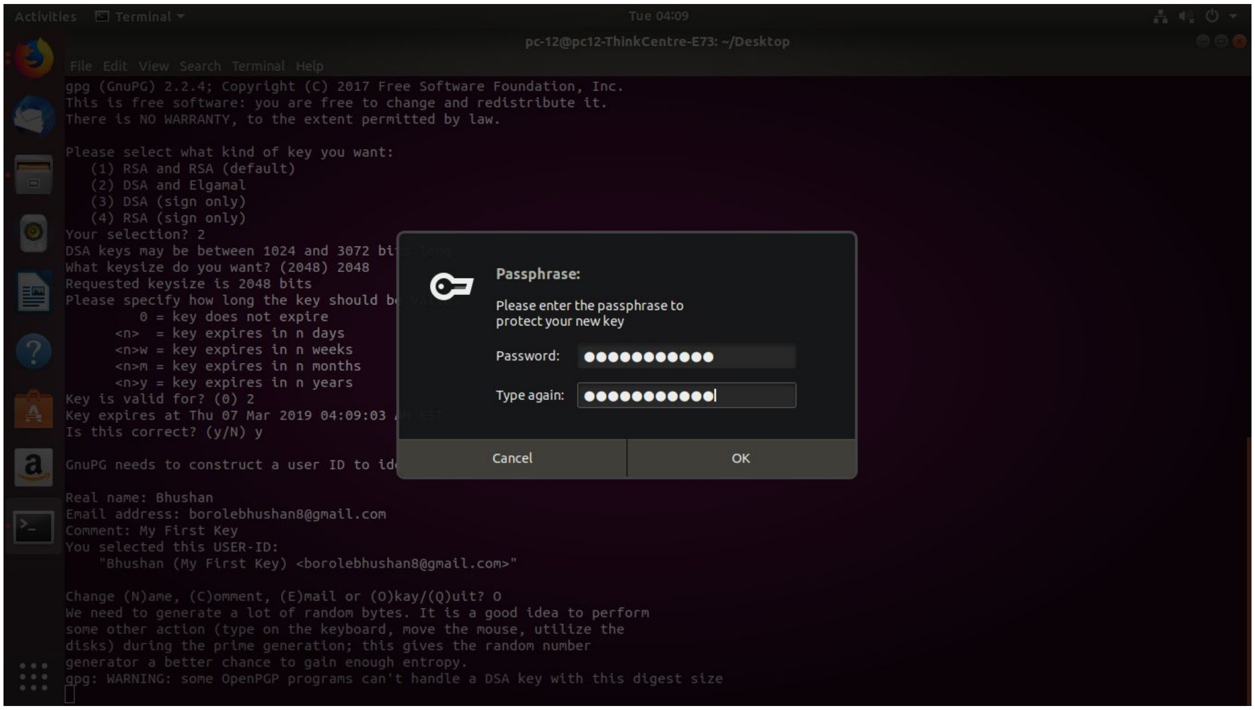
1) Generating new keys:


Activities
Terminal
Tue 04:10
pc-12@pc12-ThinkCentre-E73: ~/Desktop
File Edit View Search Terminal Help

```
bhushan-borole:~/Desktop$ gpg --full-generate-key
gpg (GnuPG) 2.2.4; Copyright (C) 2017 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.

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)
Your selection? 2
DSA keys may be between 1024 and 3072 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 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) 2
Key expires at Thu 07 Mar 2019 04:09:03 AM EST
Is this correct? (y/N) y

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

Real name: Bhushan
Email address: borolebhushan8@gmail.com
Comment: My First Key
You selected this USER-ID:
    "Bhushan (My First Key) <borolebhushan8@gmail.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.
gpg: WARNING: some OpenPGP programs can't handle a DSA key with this digest size
```

2) Entering Password:


Activities
Terminal
Tue 04:09
pc-12@pc12-ThinkCentre-E73: ~/Desktop
File Edit View Search Terminal Help
Cancel
OK

Passphrase:

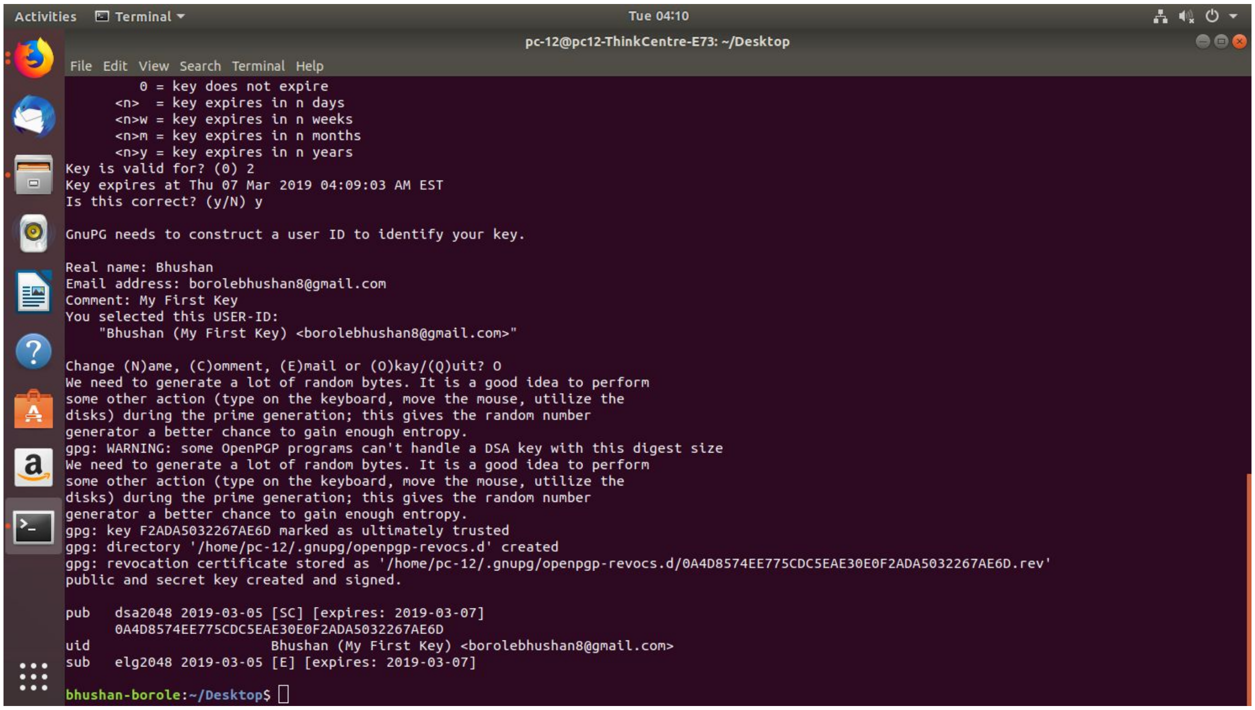
Please enter the passphrase to protect your new key

Password: ●●●●●●●●●●●

Type again: ●●●●●●●●●●●

```
gpg (GnuPG) 2.2.4; Copyright (C) 2017 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.

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)
Your selection? 2
DSA keys may be between 1024 and 3072 bi
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be
         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) 2
Key expires at Thu 07 Mar 2019 04:09:03
Is this correct? (y/N) y

GnuPG needs to construct a user ID to id

Real name: Bhushan
Email address: borolebhushan8@gmail.com
Comment: My First Key
You selected this USER-ID:
    "Bhushan (My First Key) <borolebhushan8@gmail.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.
gpg: WARNING: some OpenPGP programs can't handle a DSA key with this digest size
```

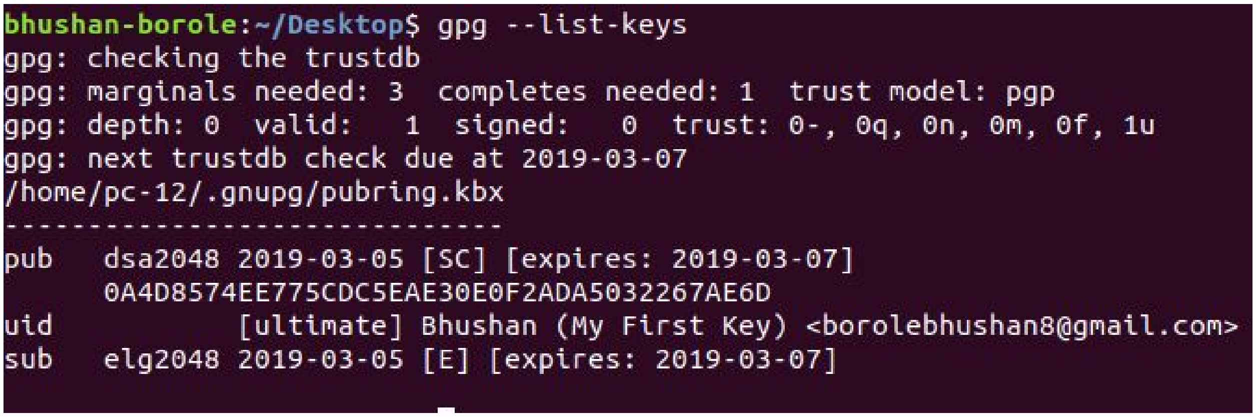
3) Key Generated:



Activities
Terminal
Tue 04:10
pc-12@pc12-ThinkCentre-E73: ~/Desktop
File Edit View Search Terminal Help

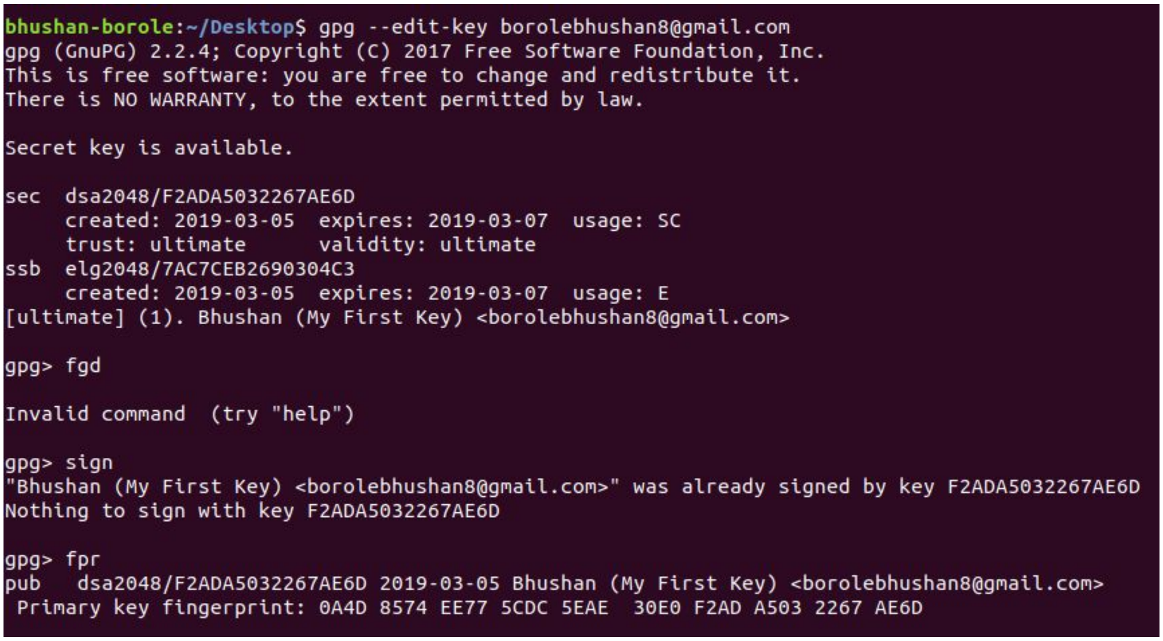
```
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 2
Key expires at Thu 07 Mar 2019 04:09:03 AM EST
Is this correct? (y/N) y

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

Real name: Bhushan
Email address: borolebhushan8@gmail.com
Comment: My First Key
You selected this USER-ID:
    "Bhushan (My First Key) <borolebhushan8@gmail.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.
gpg: WARNING: some OpenPGP programs can't handle a DSA key with this digest size
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 F2ADA5032267AE6D marked as ultimately trusted
gpg: directory '/home/pc-12/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/pc-12/.gnupg/openpgp-revocs.d/0A4D8574EE775CDC5EAE30E0F2ADA5032267AE6D.rev'
public and secret key created and signed.

pub   dsa2048 2019-03-05 [SC] [expires: 2019-03-07]
      0A4D8574EE775CDC5EAE30E0F2ADA5032267AE6D
uid                      Bhushan (My First Key) <borolebhushan8@gmail.com>
sub   elg2048 2019-03-05 [E] [expires: 2019-03-07]

bhushan-borole:~/Desktop$ 
```

4) Finding all the keys on the current system:



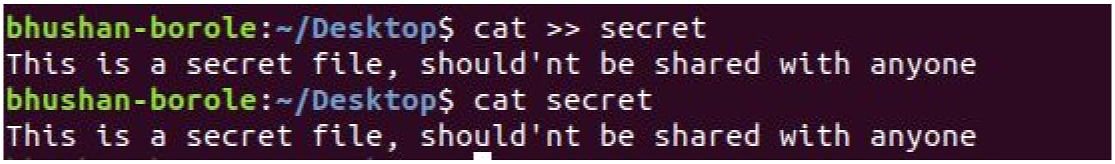
```
bhushan-borole:~/Desktop$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2019-03-07
/home/pc-12/.gnupg/pubring.kbx
------------------------------
pub   dsa2048 2019-03-05 [SC] [expires: 2019-03-07]
      0A4D8574EE775CDC5EAE30E0F2ADA5032267AE6D
uid           [ultimate] Bhushan (My First Key) <borolebhushan8@gmail.com>
sub   elg2048 2019-03-05 [E] [expires: 2019-03-07]
```

5) Signing process:



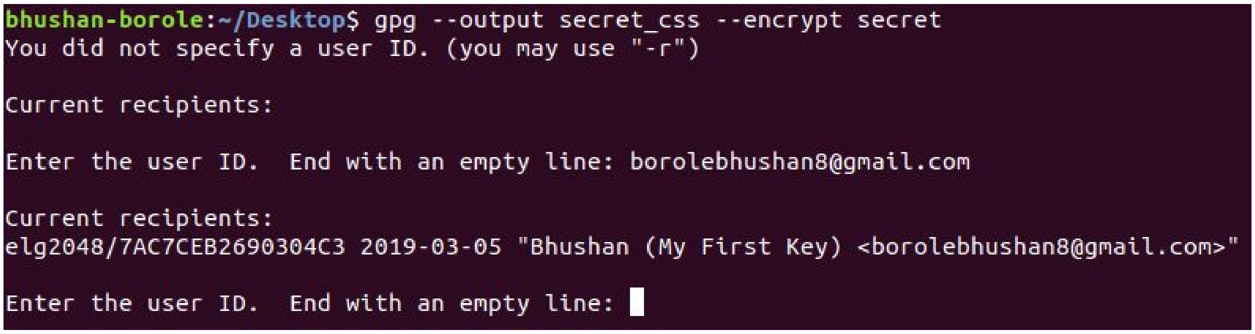
```
bhushan-borole:~/Desktop$ gpg --edit-key borolebhushan8@gmail.com
gpg (GnuPG) 2.2.4; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec  dsa2048/F2ADA5032267AE6D
     created: 2019-03-05  expires: 2019-03-07  usage: SC
     trust: ultimate      validity: ultimate
ssb  elg2048/7AC7CEB2690304C3
     created: 2019-03-05  expires: 2019-03-07  usage: E
[ultimate] (1). Bhushan (My First Key) <borolebhushan8@gmail.com>

gpg> fgd

Invalid command  (try "help")

gpg> sign
"Bhushan (My First Key) <borolebhushan8@gmail.com>" was already signed by key F2ADA5032267AE6D
Nothing to sign with key F2ADA5032267AE6D

gpg> fpr
pub   dsa2048/F2ADA5032267AE6D 2019-03-05 Bhushan (My First Key) <borolebhushan8@gmail.com>
 Primary key fingerprint: 0A4D 8574 EE77 5CDC 5EAE  30E0 F2AD A503 2267 AE6D
```

6) Creating a secret file that shouldn't be shared with anyone:

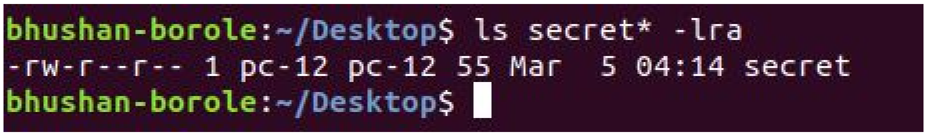


```
bhushan-borole:~/Desktop$ cat >> secret
This is a secret file, should'nt be shared with anyone
bhushan-borole:~/Desktop$ cat secret
This is a secret file, should'nt be shared with anyone
```

7) signing the file with the key generated.

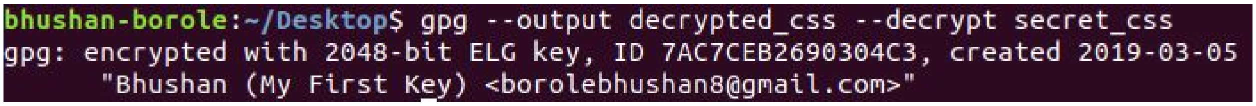


```
bhushan-borole:~/Desktop$ gpg --output secret_css --encrypt secret
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID.  End with an empty line: borolebhushan8@gmail.com

Current recipients:
elg2048/7AC7CEB2690304C3 2019-03-05 "Bhushan (My First Key) <borolebhushan8@gmail.com>"

Enter the user ID.  End with an empty line:
```

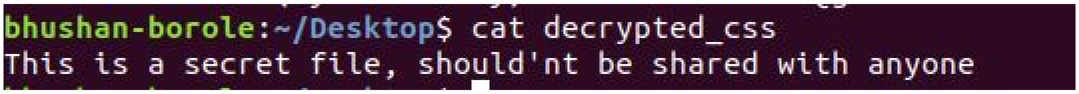


```
bhushan-borole:~/Desktop$ ls secret* -lra
-rw-r--r-- 1 pc-12 pc-12 55 Mar  5 04:14 secret
bhushan-borole:~/Desktop$
```

8) Dercyption:



```
bhushan-borole:~/Desktop$ gpg --output decrypted_css --decrypt secret_css
gpg: encrypted with 2048-bit ELG key, ID 7AC7CEB2690304C3, created 2019-03-05
      "Bhushan (My First Key) <borolebhushan8@gmail.com>"
```



```
bhushan-borole:~/Desktop$ cat decrypted_css
This is a secret file, should'nt be shared with anyone
```