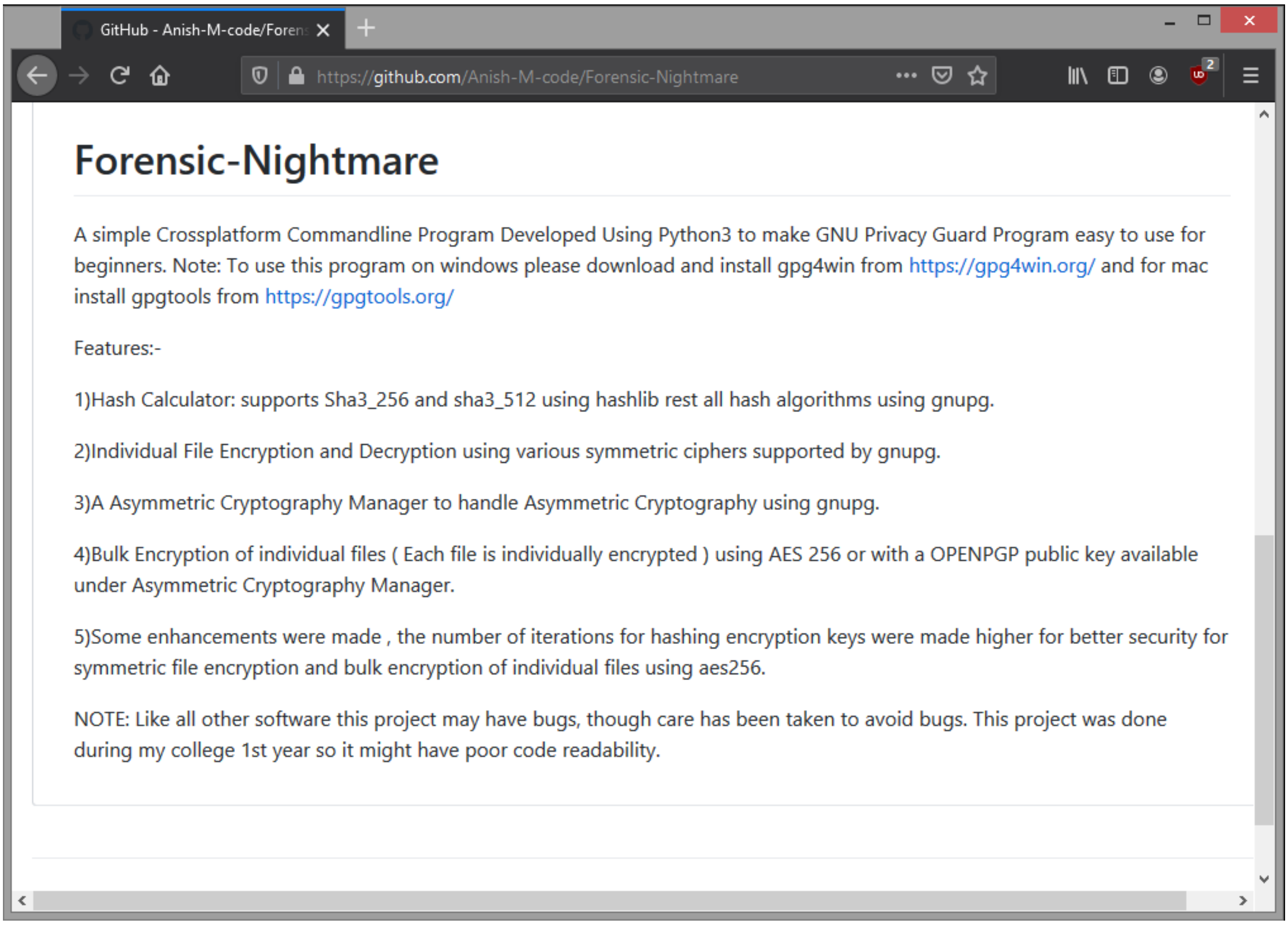
Forensic Nightmare v8 Manual

Project Link: https://github.com/Anish-M-code/Forensic-Nightmare


GitHub - Anish-M-code/Foren
https://github.com/Anish-M-code/Forensic-Nightmare

Forensic-Nightmare

A simple Crossplatform Commandline Program Developed Using Python3 to make GNU Privacy Guard Program easy to use for beginners. Note: To use this program on windows please download and install gpg4win from https://gpg4win.org/ and for mac install gpgtools from https://gpgtools.org/

Features:-

1)Hash Calculator: supports Sha3_256 and sha3_512 using hashlib rest all hash algorithms using gnupg.

2)Individual File Encryption and Decryption using various symmetric ciphers supported by gnupg.

3)A Asymmetric Cryptography Manager to handle Asymmetric Cryptography using gnupg.

4)Bulk Encryption of individual files (Each file is individually encrypted) using AES 256 or with a OPENPGP public key available under Asymmetric Cryptography Manager.

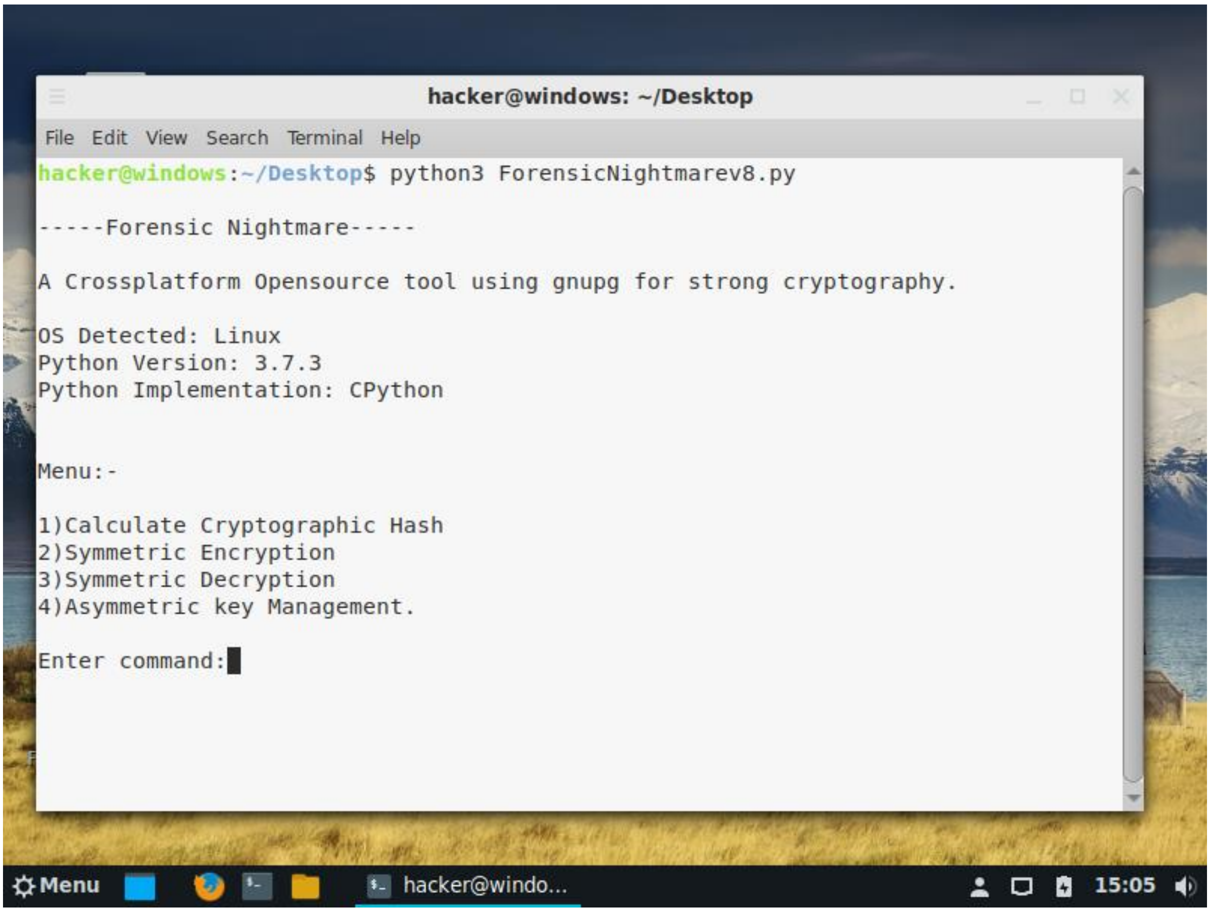
5)Some enhancements were made , the number of iterations for hashing encryption keys were made higher for better security for symmetric file encryption and bulk encryption of individual files using aes256.

NOTE: Like all other software this project may have bugs, though care has been taken to avoid bugs. This project was done during my college 1st year so it might have poor code readability.

This is a Portable Program. It requires no installation. Simply Run it like any other python Program!

```
Windows:  py ForensicNightmarev8.py
Linux:       python3 ForensicNightmarev8.py
```

Main Menu:-



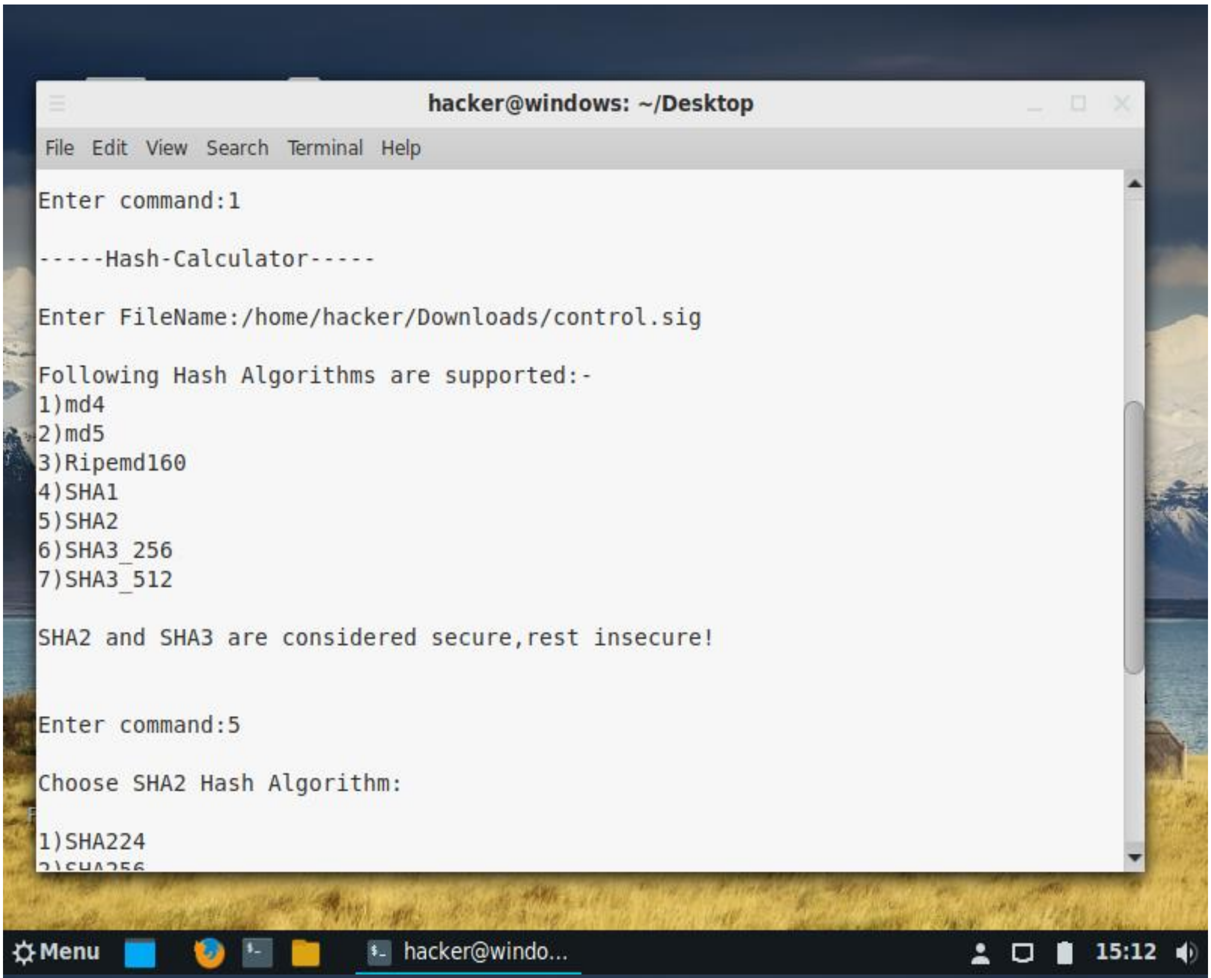
hacker@windows: ~/Desktop
File Edit View Search Terminal Help
Menu
hacker@windo...
15:05

```
hacker@windows:~/Desktop$ python3 ForensicNightmarev8.py

-----Forensic Nightmare-----

A Crossplatform Opensource tool using gnupg for strong cryptography.

OS Detected: Linux
Python Version: 3.7.3
Python Implementation: CPython


Menu:-

1)Calculate Cryptographic Hash
2)Symmetric Encryption
3)Symmetric Decryption
4)Asymmetric key Management.

Enter command:
```

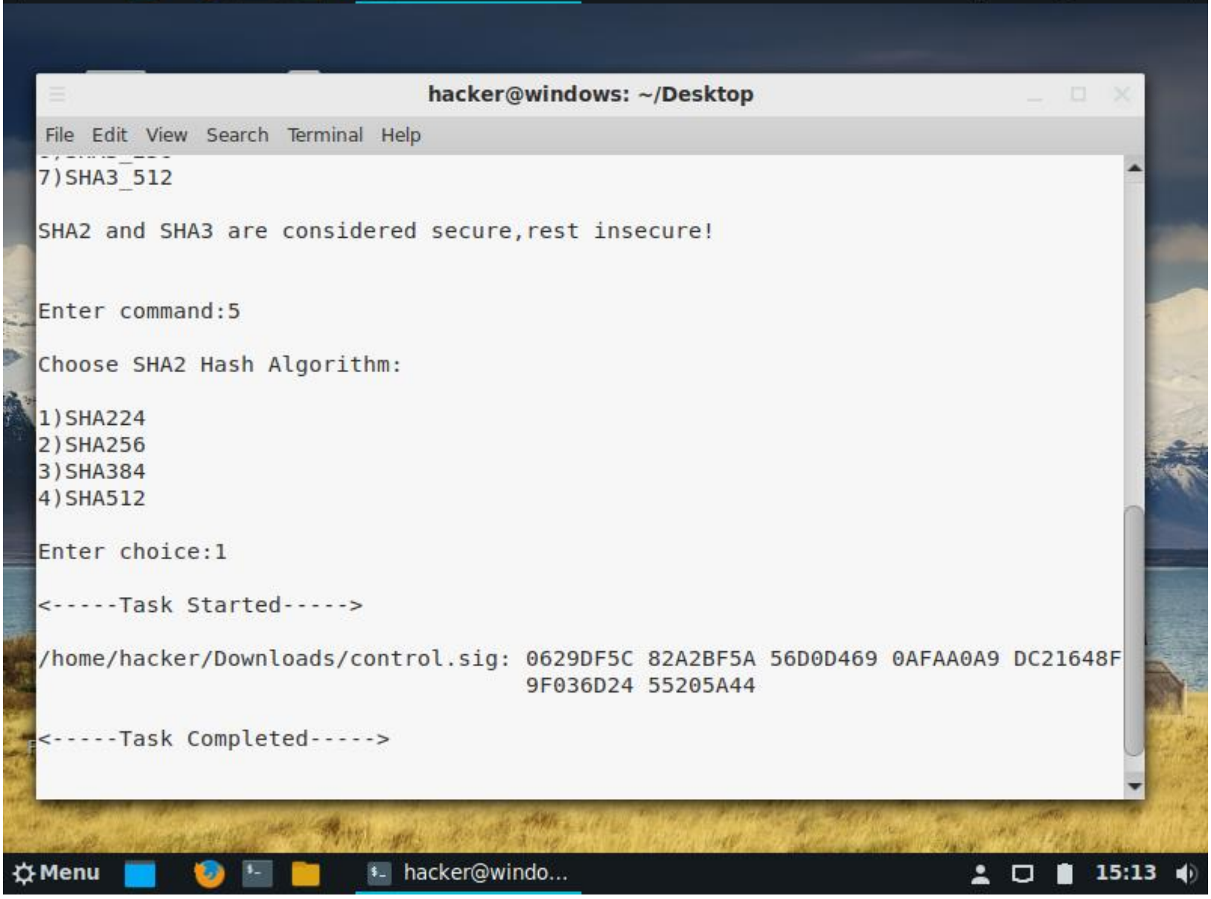
Calculating Cryptographic Hash of Files:-

Cryptographic hash is used to verify integrity of files. It is Used to ensure that your files are not modified unintentionally. 2 Files with same contents will have same hash.

Forensic Nightmare supports Cryptographic hash functions in Gnupg and additionally sha3 family hash functions via python’s hashlib.

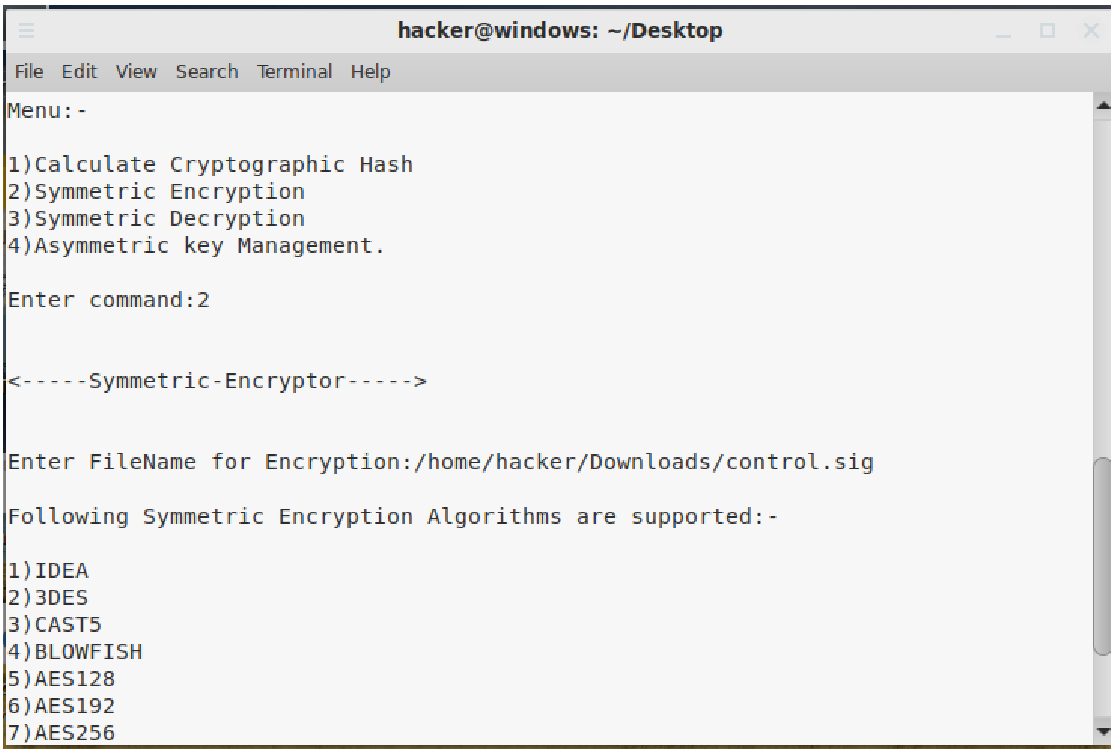

hacker@windows: ~/Desktop
File Edit View Search Terminal Help
Menu
hacker@windo...
15:12

```
Enter command:1

-----Hash-Calculator-----

Enter FileName:/home/hacker/Downloads/control.sig

Following Hash Algorithms are supported:-
1)md4
2)md5
3)Ripemd160
4)SHA1
5)SHA2
6)SHA3_256
7)SHA3_512

SHA2 and SHA3 are considered secure,rest insecure!


Enter command:5

Choose SHA2 Hash Algorithm:

1)SHA224
2)SHA256
```

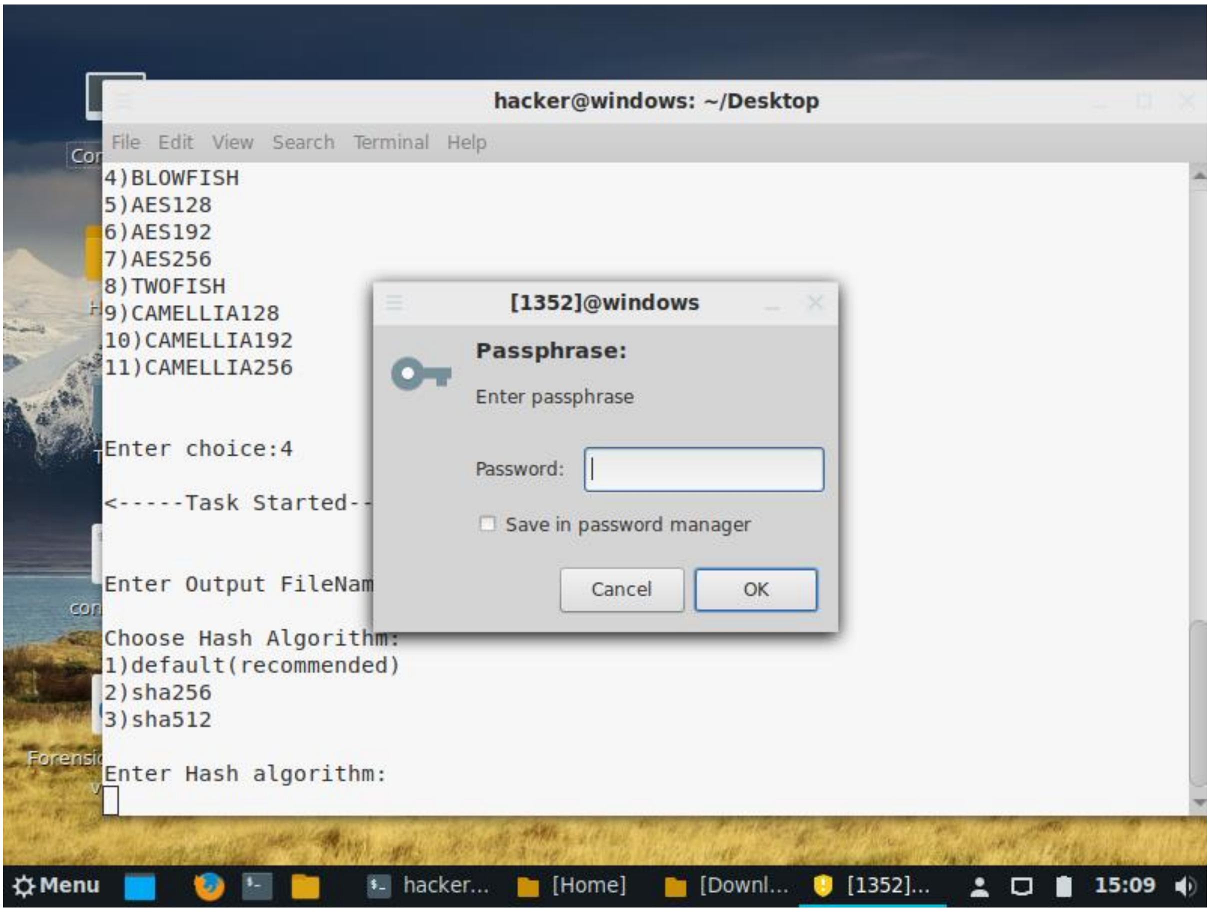

hacker@windows: ~/Desktop
File Edit View Search Terminal Help
Menu
hacker@windo...
15:13

```
6)SHA3_256
7)SHA3_512

SHA2 and SHA3 are considered secure,rest insecure!


Enter command:5

Choose SHA2 Hash Algorithm:

1)SHA224
2)SHA256
3)SHA384
4)SHA512

Enter choice:1

<-----Task Started----->

/home/hacker/Downloads/control.sig: 0629DF5C 82A2BF5A 56D0D469 0AFAA0A9 DC21648F
                                    9F036D24 55205A44

<-----Task Completed----->
```

Symmetric Encryption:-


hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
Menu:-

1)Calculate Cryptographic Hash
2)Symmetric Encryption
3)Symmetric Decryption
4)Asymmetric key Management.

Enter command:2


<-----Symmetric-Encryptor----->


Enter FileName for Encryption:/home/hacker/Downloads/control.sig

Following Symmetric Encryption Algorithms are supported:-

1)IDEA
2)3DES
3)CAST5
4)BLOWFISH
5)AES128
6)AES192
7)AES256
```

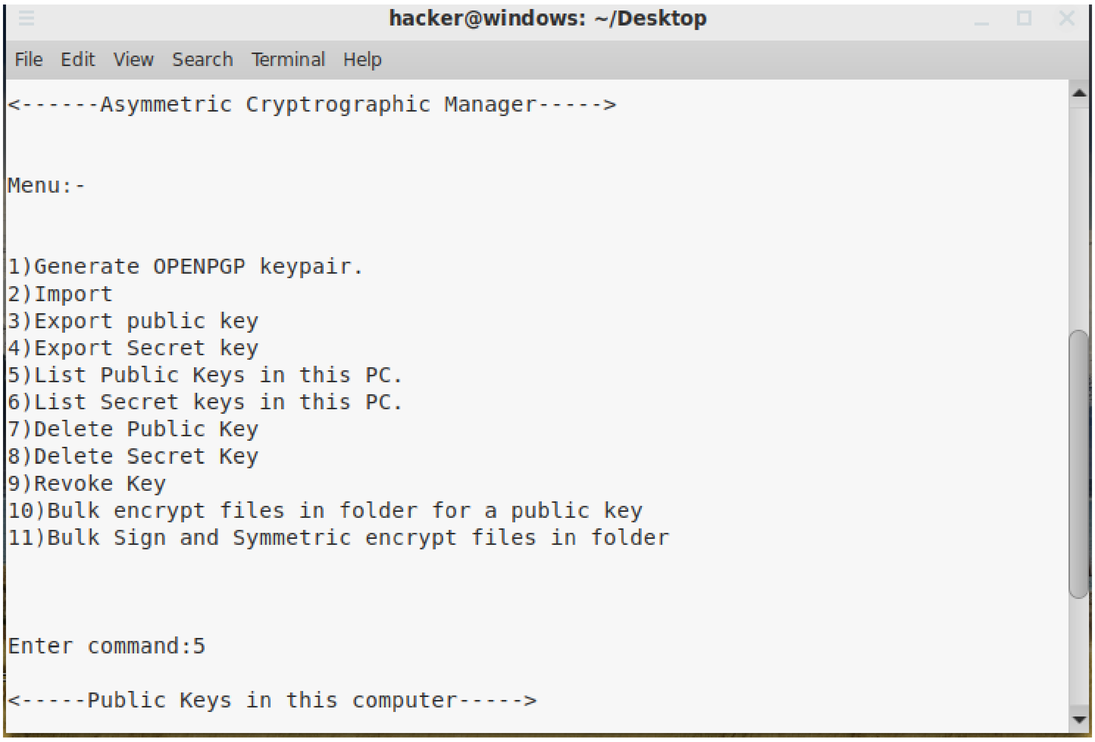


```
4)BLOWFISH
5)AES128
6)AES192
7)AES256
8)TWOFISH
9)CAMELLIA128
10)CAMELLIA192
11)CAMELLIA256


Enter choice:4

<-----Task Started--


Enter Output FileNam

Choose Hash Algorithm:
1)default(recommended)
2)sha256
3)sha512


Enter Hash algorithm:
```

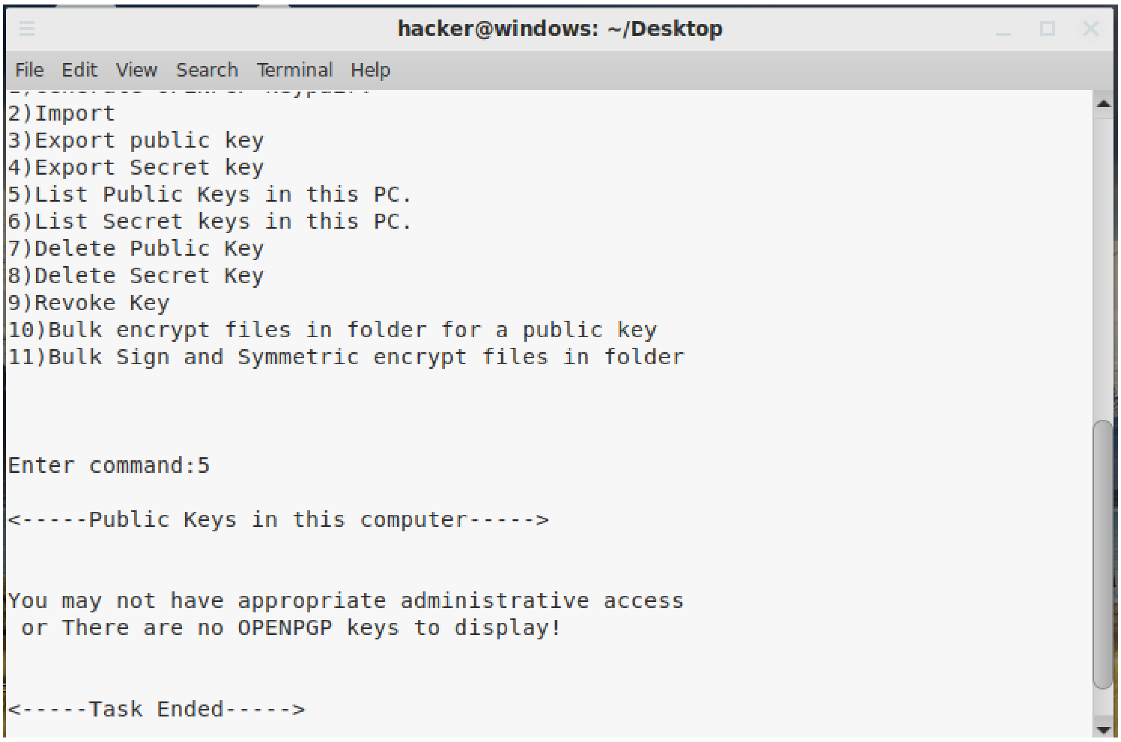
For output Filename give any name or press enter .

Using Asymmetric Cryptography using OPENPGP:-

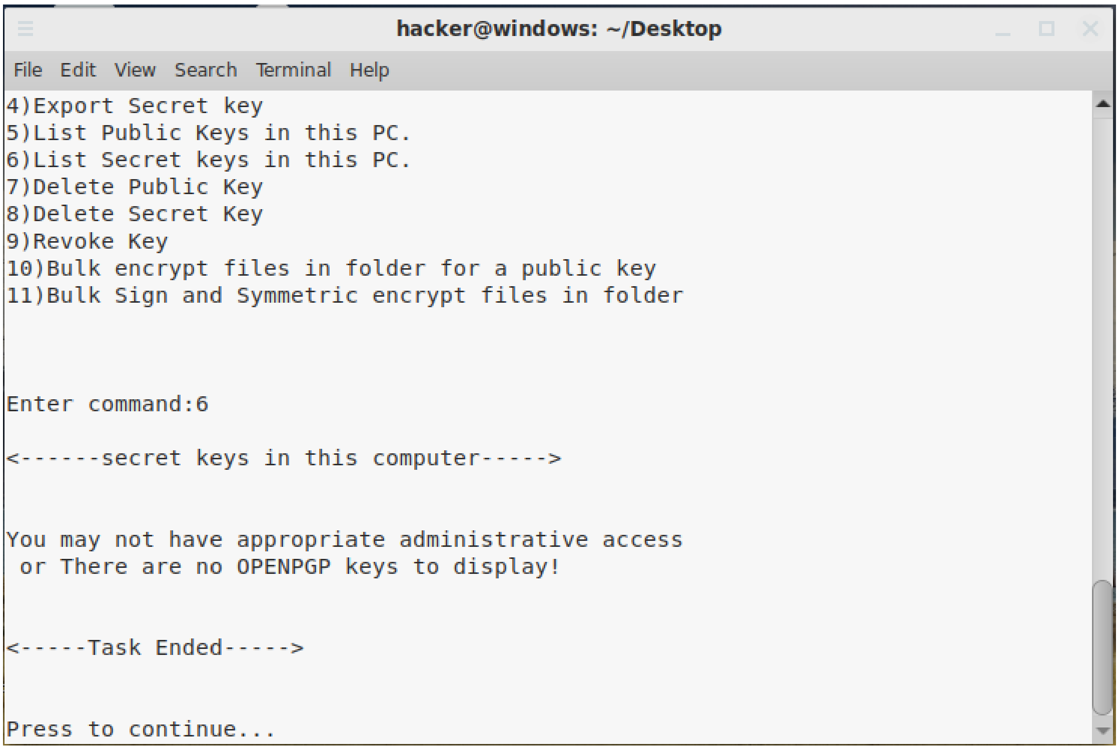
By default while using this program for first time . Mostly Your PC will have neither Private/Secret nor Public OPENPGP keys .


hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
<------Asymmetric Cryptrographic Manager----->


Menu:-


1)Generate OPENPGP keypair.
2)Import
3)Export public key
4)Export Secret key
5)List Public Keys in this PC.
6)List Secret keys in this PC.
7)Delete Public Key
8)Delete Secret Key
9)Revoke Key
10)Bulk encrypt files in folder for a public key
11)Bulk Sign and Symmetric encrypt files in folder



Enter command:5

<-----Public Keys in this computer----->
```


hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
2)Import
3)Export public key
4)Export Secret key
5)List Public Keys in this PC.
6)List Secret keys in this PC.
7)Delete Public Key
8)Delete Secret Key
9)Revoke Key
10)Bulk encrypt files in folder for a public key
11)Bulk Sign and Symmetric encrypt files in folder



Enter command:5

<-----Public Keys in this computer----->


You may not have appropriate administrative access
 or There are no OPENPGP keys to display!


<-----Task Ended----->
```

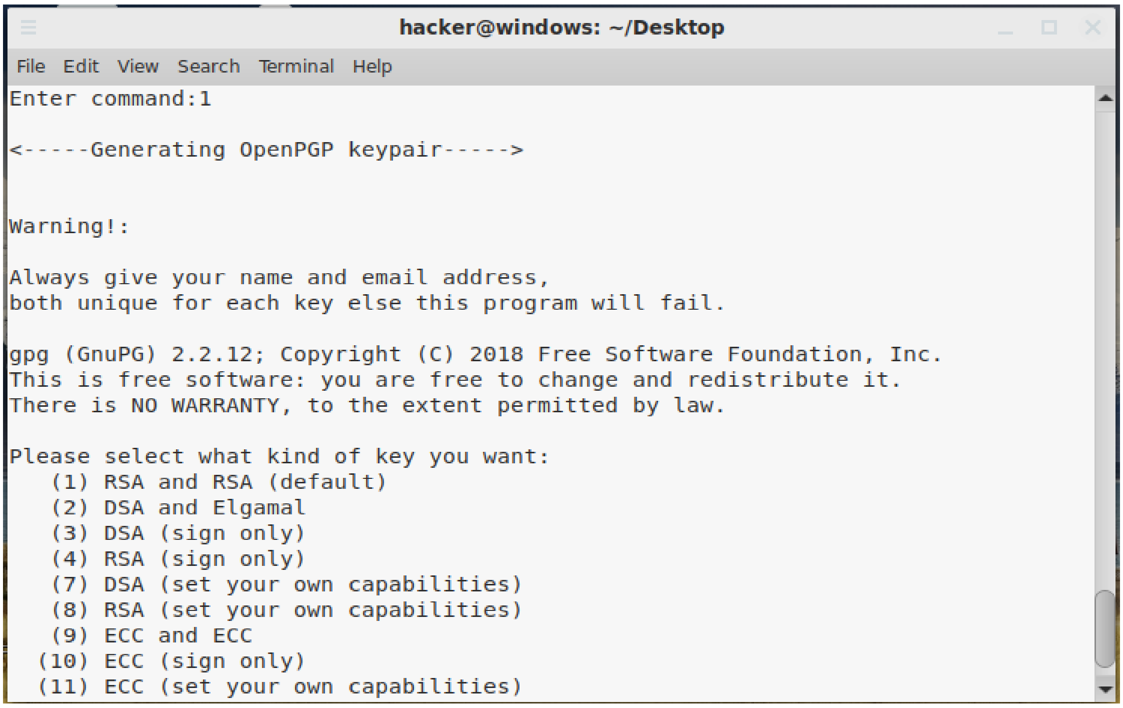


hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
4)Export Secret key
5)List Public Keys in this PC.
6)List Secret keys in this PC.
7)Delete Public Key
8)Delete Secret Key
9)Revoke Key
10)Bulk encrypt files in folder for a public key
11)Bulk Sign and Symmetric encrypt files in folder


Enter command:6

<------secret keys in this computer----->


You may not have appropriate administrative access
 or There are no OPENPGP keys to display!


<-----Task Ended----->


Press to continue...
```

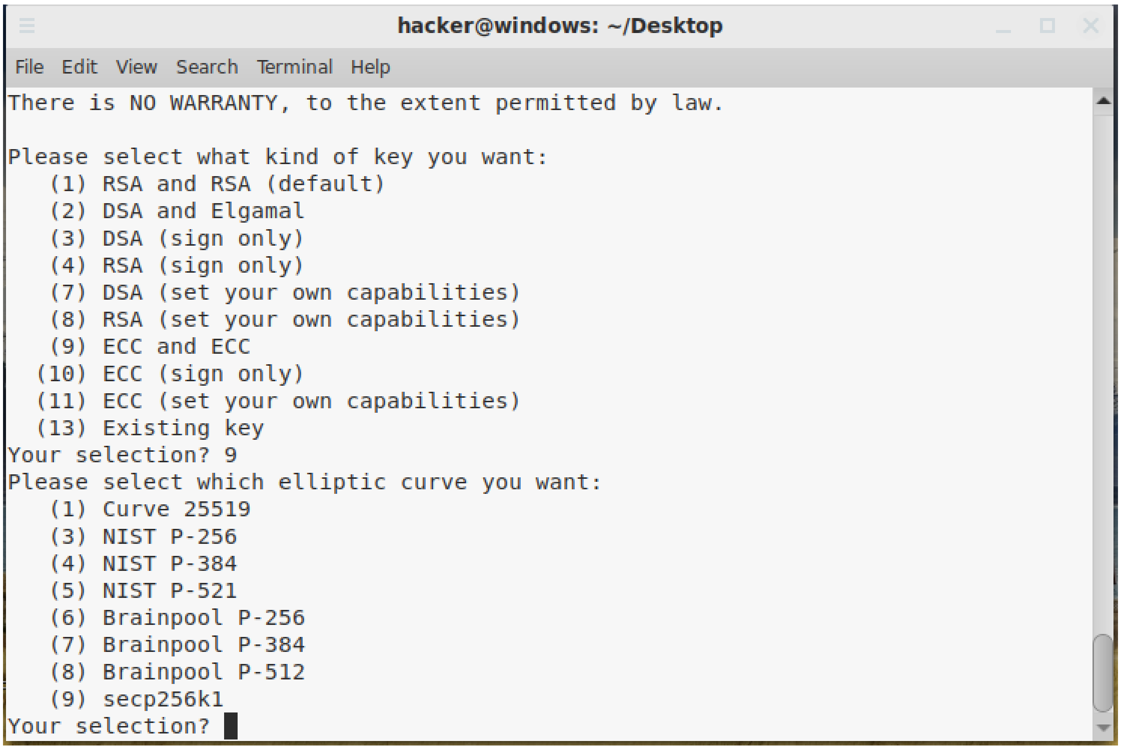
So To use Asymmetric Cryptography you have to generate an OPENPGP key pair!

In Asymmetric Cryptographic Manager enter 1



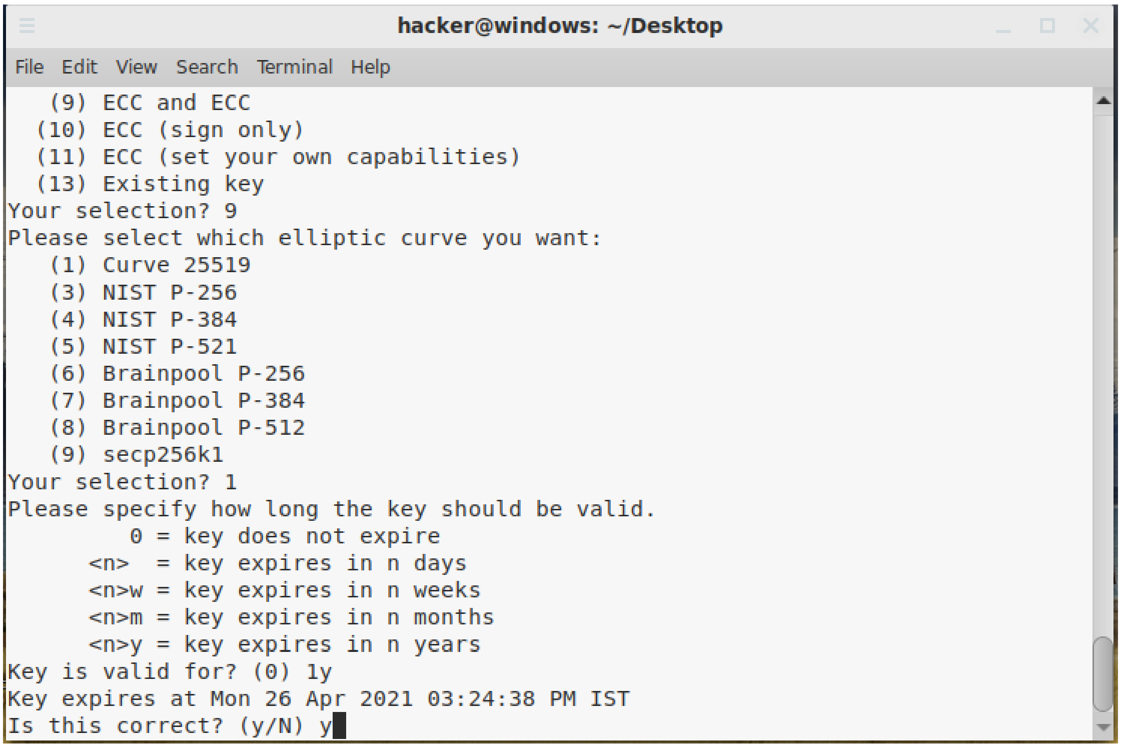
hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
Enter command:1

<-----Generating OpenPGP keypair----->


Warning!:

Always give your name and email address,
both unique for each key else this program will fail.

gpg (GnuPG) 2.2.12; Copyright (C) 2018 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)
   (7) DSA (set your own capabilities)
   (8) RSA (set your own capabilities)
   (9) ECC and ECC
  (10) ECC (sign only)
  (11) ECC (set your own capabilities)
```



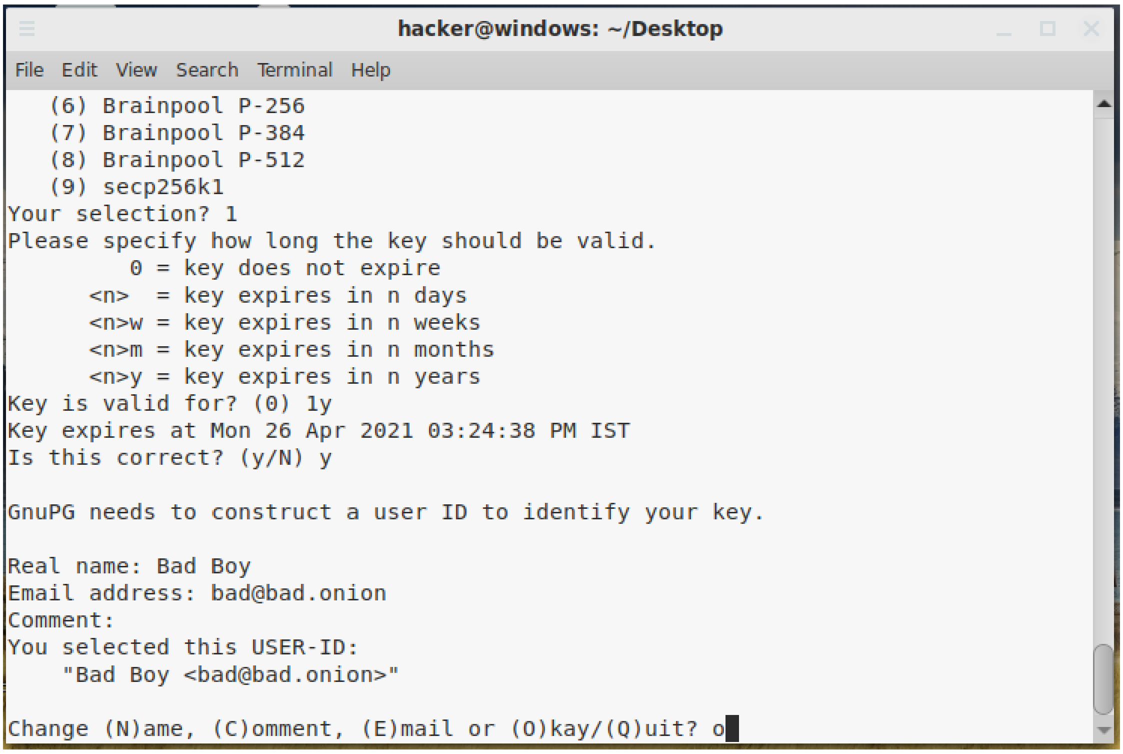
hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
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)
   (7) DSA (set your own capabilities)
   (8) RSA (set your own capabilities)
   (9) ECC and ECC
  (10) ECC (sign only)
  (11) ECC (set your own capabilities)
  (13) Existing key
Your selection? 9
Please select which elliptic curve you want:
   (1) Curve 25519
   (3) NIST P-256
   (4) NIST P-384
   (5) NIST P-521
   (6) Brainpool P-256
   (7) Brainpool P-384
   (8) Brainpool P-512
   (9) secp256k1
Your selection? 
```

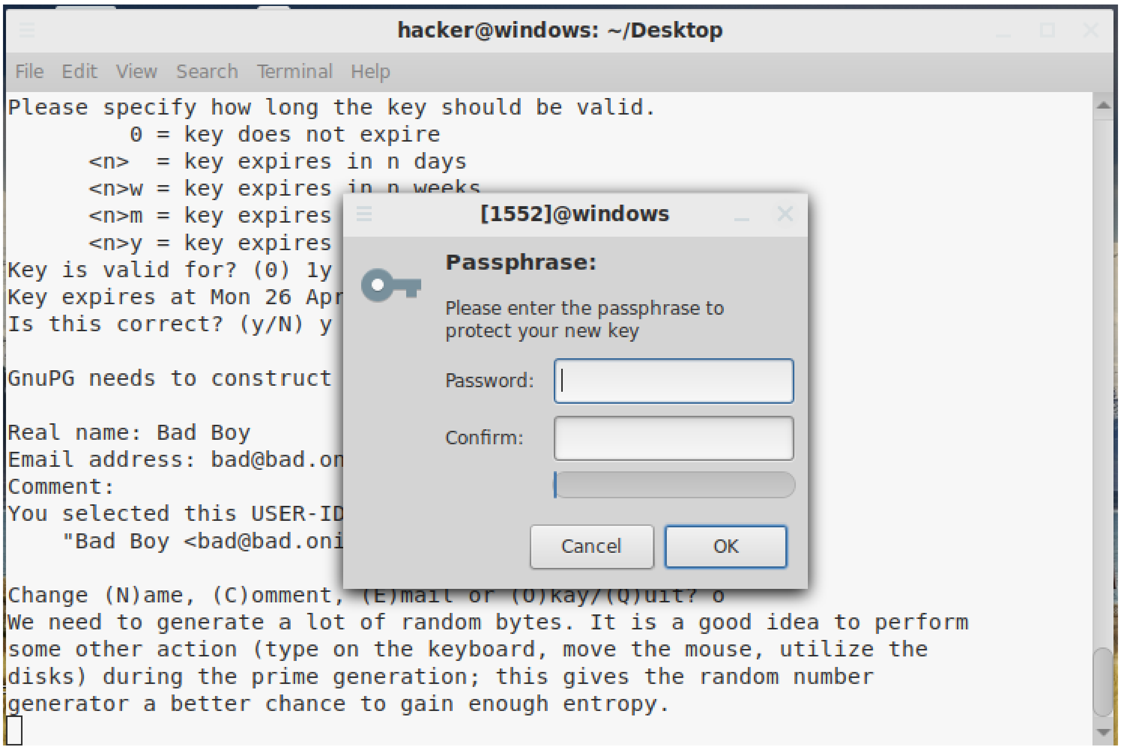


hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
   (9) ECC and ECC
  (10) ECC (sign only)
  (11) ECC (set your own capabilities)
  (13) Existing key
Your selection? 9
Please select which elliptic curve you want:
   (1) Curve 25519
   (3) NIST P-256
   (4) NIST P-384
   (5) NIST P-521
   (6) Brainpool P-256
   (7) Brainpool P-384
   (8) Brainpool P-512
   (9) secp256k1
Your selection? 1
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) 1y
Key expires at Mon 26 Apr 2021 03:24:38 PM IST
Is this correct? (y/N) y
```


hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
   (6) Brainpool P-256
   (7) Brainpool P-384
   (8) Brainpool P-512
   (9) secp256k1
Your selection? 1
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) 1y
Key expires at Mon 26 Apr 2021 03:24:38 PM IST
Is this correct? (y/N) y

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

Real name: Bad Boy
Email address: bad@bad.onion
Comment:
You selected this USER-ID:
    "Bad Boy <bad@bad.onion>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
```


hacker@windows: ~/Desktop
File Edit View Search Terminal Help
[1552]@windows

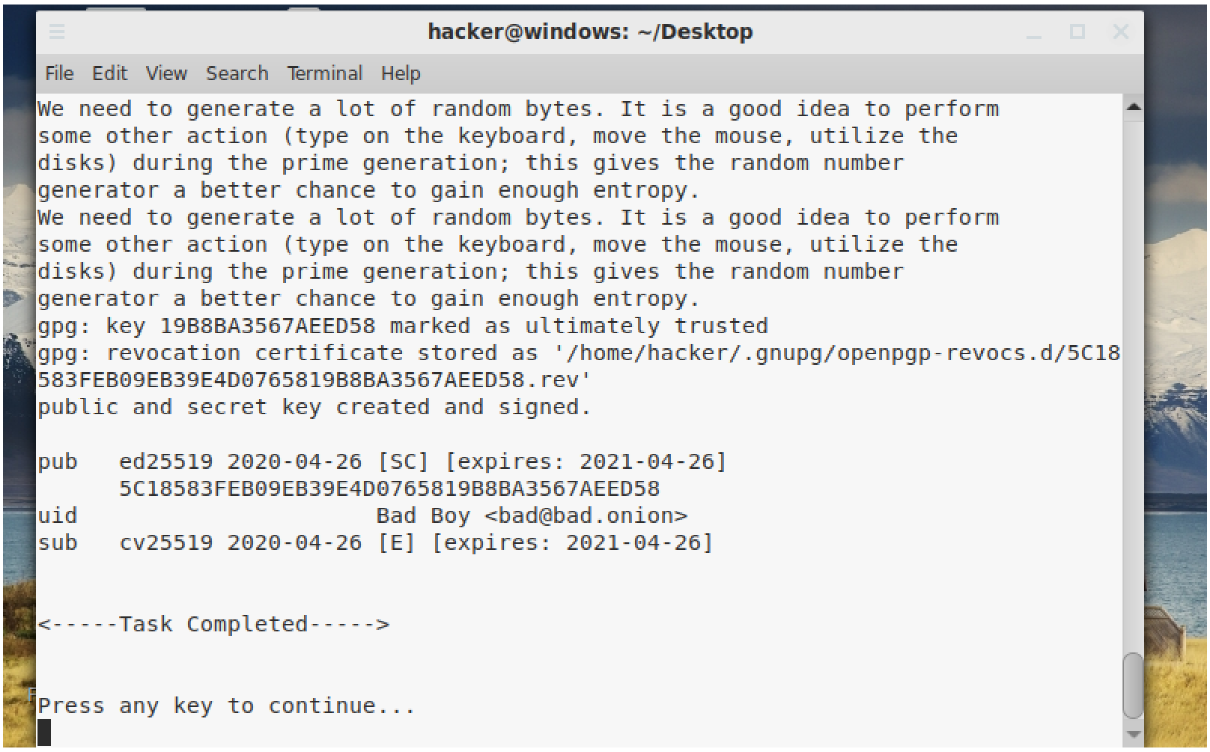
```
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires
      <n>y = key expires
Key is valid for? (0) 1y
Key expires at Mon 26 Apr
Is this correct? (y/N) y

GnuPG needs to construct

Real name: Bad Boy
Email address: bad@bad.on
Comment:
You selected this USER-ID
    "Bad Boy <bad@bad.oni

Change (N)ame, (C)omment,
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.
```

Passphrase:

Please enter the passphrase to protect your new key

Password:

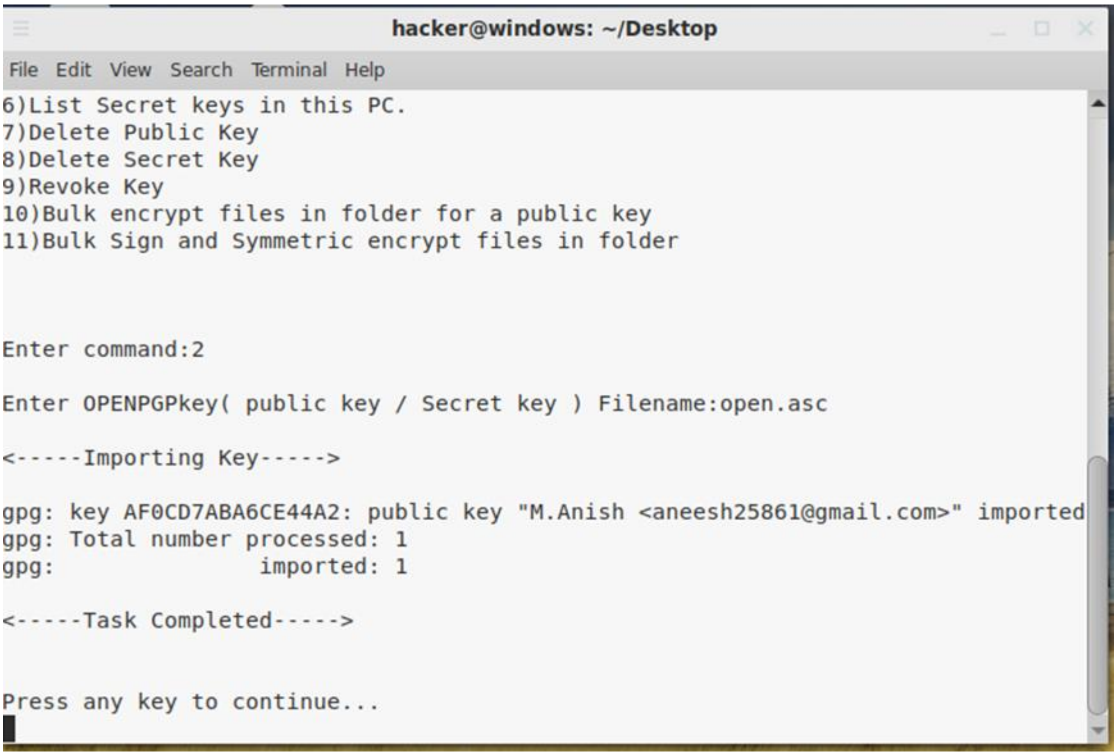
Confirm:


hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
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 19B8BA3567AEED58 marked as ultimately trusted
gpg: revocation certificate stored as '/home/hacker/.gnupg/openpgp-revocs.d/5C18
583FEB09EB39E4D0765819B8BA3567AEED58.rev'
public and secret key created and signed.

pub   ed25519 2020-04-26 [SC] [expires: 2021-04-26]
      5C18583FEB09EB39E4D0765819B8BA3567AEED58
uid                      Bad Boy <bad@bad.onion>
sub   cv25519 2020-04-26 [E] [expires: 2021-04-26]


<-----Task Completed----->


Press any key to continue...
```

Finally we have Successfully Generated our OPENPGP keypair!

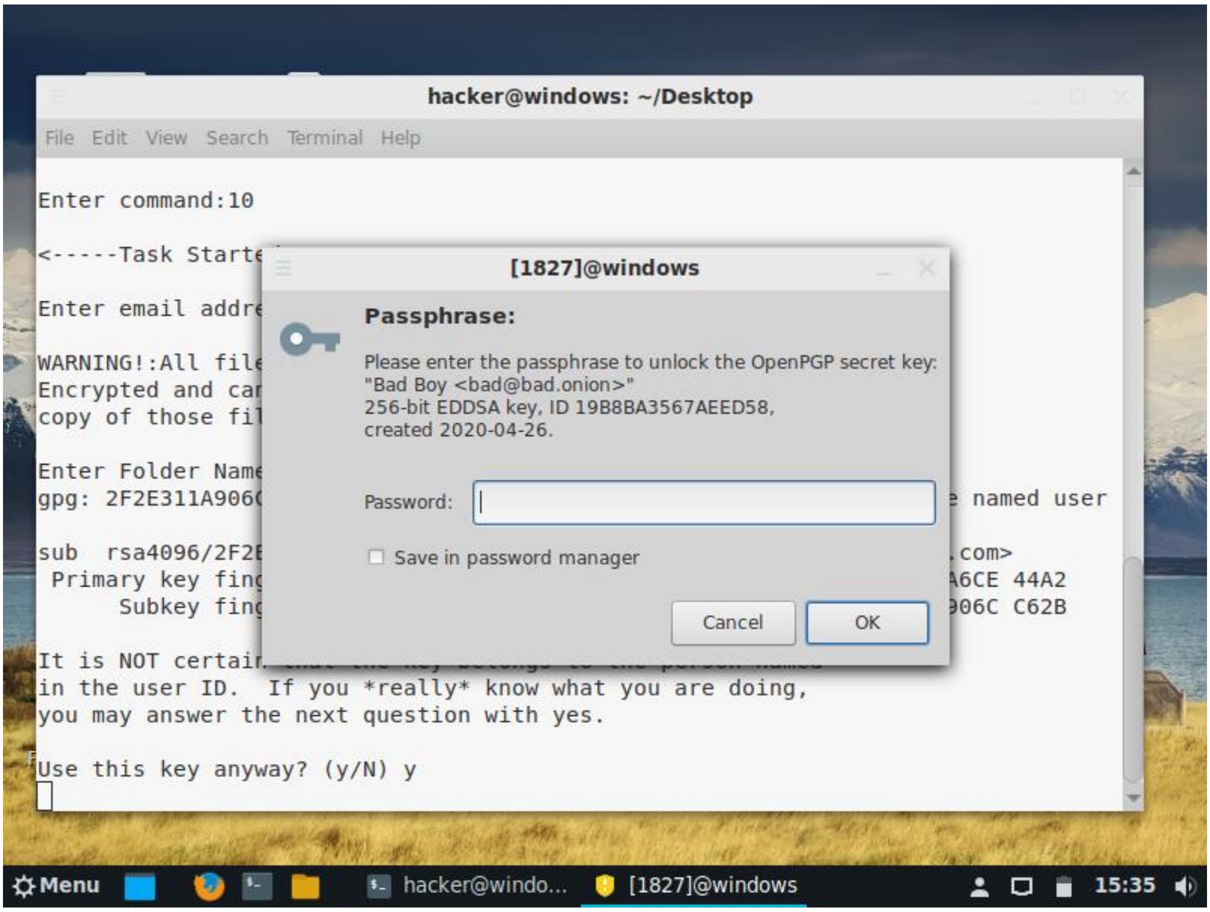
Next to import Public keys.


hacker@windows: ~/Desktop
File Edit View Search Terminal Help

```
6)List Secret keys in this PC.
7)Delete Public Key
8)Delete Secret Key
9)Revoke Key
10)Bulk encrypt files in folder for a public key
11)Bulk Sign and Symmetric encrypt files in folder



Enter command:2

Enter OPENPGPkey( public key / Secret key ) Filename:open.asc

<-----Importing Key----->

gpg: key AF0CD7ABA6CE44A2: public key "M.Anish <aneesh25861@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1

<-----Task Completed----->


Press any key to continue...
```

Once you have created your own OPENPGP keypair and imported another person’s public key obtained securely. You can explore other options in Asymmetric Cryptographic Manager.

Bulk Encryption of Files to Public Key



hacker@windows: ~/Desktop
File Edit View Search Terminal Help
[1827]@windows
Menu
hacker@windo...
[1827]@windows
15:35

```
Enter command:10

<-----Task Starte

Enter email addre

WARNING!:All file
Encrypted and car
copy of those fil

Enter Folder Name
gpg: 2F2E311A906(                                              e named user

sub  rsa4096/2F2E                                              .com>
 Primary key fing                                              A6CE 44A2
      Subkey fing                                              906C C62B

It is NOT certair
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
```

Passphrase:

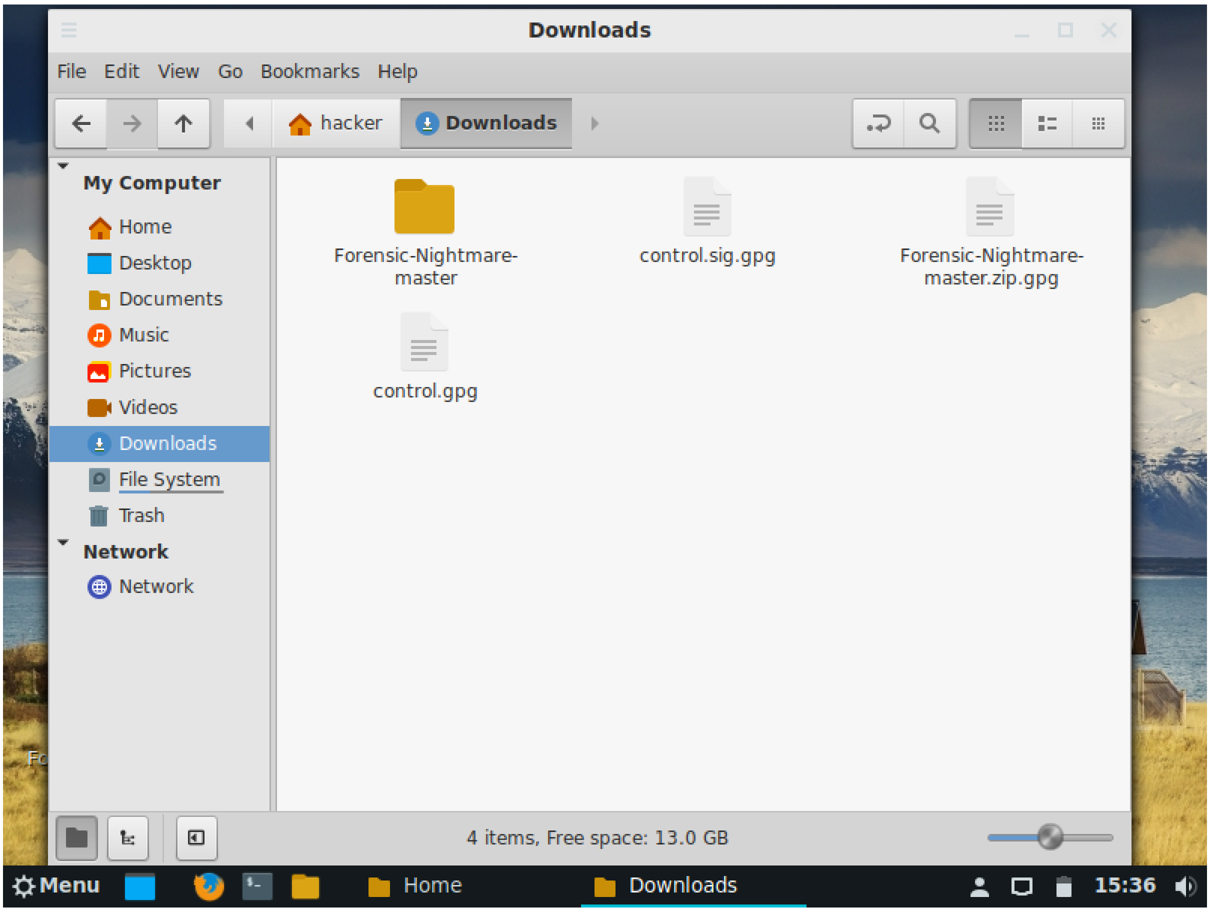
Please enter the passphrase to unlock the OpenPGP secret key:
"Bad Boy <bad@bad.onion>"
256-bit EDDSA key, ID 19B8BA3567AEED58,
created 2020-04-26.

Password:

□ Save in password manager

Cancel OK

Here Password of Your Private/Secret Openpgp key should be entered.



Encrypted Files will end with .gpg extension.

Hope you like this tool. This tool was originally created for kali Linux since from Kali Linux 2020.1 the interface to gnupg has been cumbersome.

For any bugs , enhancements feel free to shoot me an email at aneesh25861[at]gmail.com or raise an issue on github!