- GPG tool

Option	Description
--generate-key	Generate key
--encrypt	Encrypt file
--decrypt	Decrypt file
--list-keys	List keys on GPG
--import / --export	Import or export keys
--full-generate-key	Generate key (more details)
--gen-revoke	Generate certificate to revoke key
--keyserver	Interact with public keyserver
--search-keys	Search keys on public keyserver
--fingerprint	Fingerprint of certificate / key
--recipient	Email associated

- GPG tool – Generate key

```
└─$ gpg --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.

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: pablogonzalezpe
Email address: pablo@mypublicinbox.com
You selected this USER-ID:
    "pablogonzalezpe <pablo@mypublicinbox.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.
```

```
gpg: directory '/home/kali/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/kali/.gnupg/openpgp-revocs.d/B6CB7A5DAC39F93A0F45818AA7287AA54B
F91913.rev'
public and secret key created and signed.

pub   rsa3072 2024-04-11 [SC] [expires: 2026-04-11]
      B6CB7A5DAC39F93A0F45818AA7287AA54BF91913
uid                      pablogonzalezpe <pablo@mypublicinbox.com>
sub   rsa3072 2024-04-11 [E] [expires: 2026-04-11]
```

- GPG tool – List keys

```
└─$ 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 2026-04-11
/home/kali/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2024-04-11 [SC] [expires: 2026-04-11]
      B6CB7A5DAC39F93A0F45818AA7287AA54BF91913
uid           [ultimate] pablogonzalezpe <pablo@mypublicinbox.com>
sub   rsa3072 2024-04-11 [E] [expires: 2026-04-11]
```

- GPG tool – Revoke Certificate

```
└─$ gpg  --output /tmp/myrevocation.crt --gen-revoke pablo@mypublicinbox.com

sec  rsa3072/A7287AA54BF91913 2024-04-11 pablogonzalezpe <pablo@mypublicinbox.com>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 1
Enter an optional description; end it with an empty line:
>
Reason for revocation: Key has been compromised
(No description given)
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.
```

- GPG tool – Import / export and search keys
- $> gpg --import <file.key>
- $> gpg --keyserver <domain keyserver> --search-keys <email>
- $> gpg --output <file.key> --armor --export <email>

```
└─$ gpg --output /tmp/exported.key --armor --export pablo@mypublicinbox.com

┌──(kali㉿kali)-[~]
└─$ ls -lh /tmp/exported.key
-rw-r--r-- 1 kali kali 2.5K Apr 11 22:35 /tmp/exported.key

┌──(kali㉿kali)-[~]
└─$ file /tmp/exported.key
/tmp/exported.key: PGP public key block Public-Key (old)
```


- $> gpg --output <file.key> --armor --export <email>

- $> gpg --send-keys --keyserver <domain keyserver> <fingerprint>
  - $> gpg --fingerprint <email>

- GPG tool – encrypt / decrypt

- $> gpg --encrypt --armor --recipient <email> <file>
  - Output: file.asc
- $> gpg --encrypt --recipient <email> <file>
  - Output: file.gpg (file illegible)

- $> gpg --decrypt > <file>
  - Output: plaintext file

```
┌──(kali㉿kali)-[/tmp]
└─$ gpg --output secrets.sig --sign secrets.txt

┌──(kali㉿kali)-[/tmp]
└─$ gpg --verify secrets.sig
gpg: Signature made Thu 11 Apr 2024 10:52:49 PM +09
gpg:                using RSA key B6CB7A5DAC39F93A0F45818AA7287AA54BF91913
gpg: Good signature from "pablogonzalezpe <pablo@mypublicinbox.com>" [ultimate]
```

- $> gpg --encrypt --recipient <email> <file>

```
┌──(kali㉿kali)-[/tmp]
└─$ gpg --output secrets.gpg --encrypt --recipient pablo@mypublicinbox.com secrets.txt

┌──(kali㉿kali)-[/tmp]
└─$ gpg --output new_secrets.txt --decrypt secrets.gpg
gpg: encrypted with 3072-bit RSA key, ID 431280AC41D1DBA2, created 2024-04-11
      "pablogonzalezpe <pablo@mypublicinbox.com>"
```