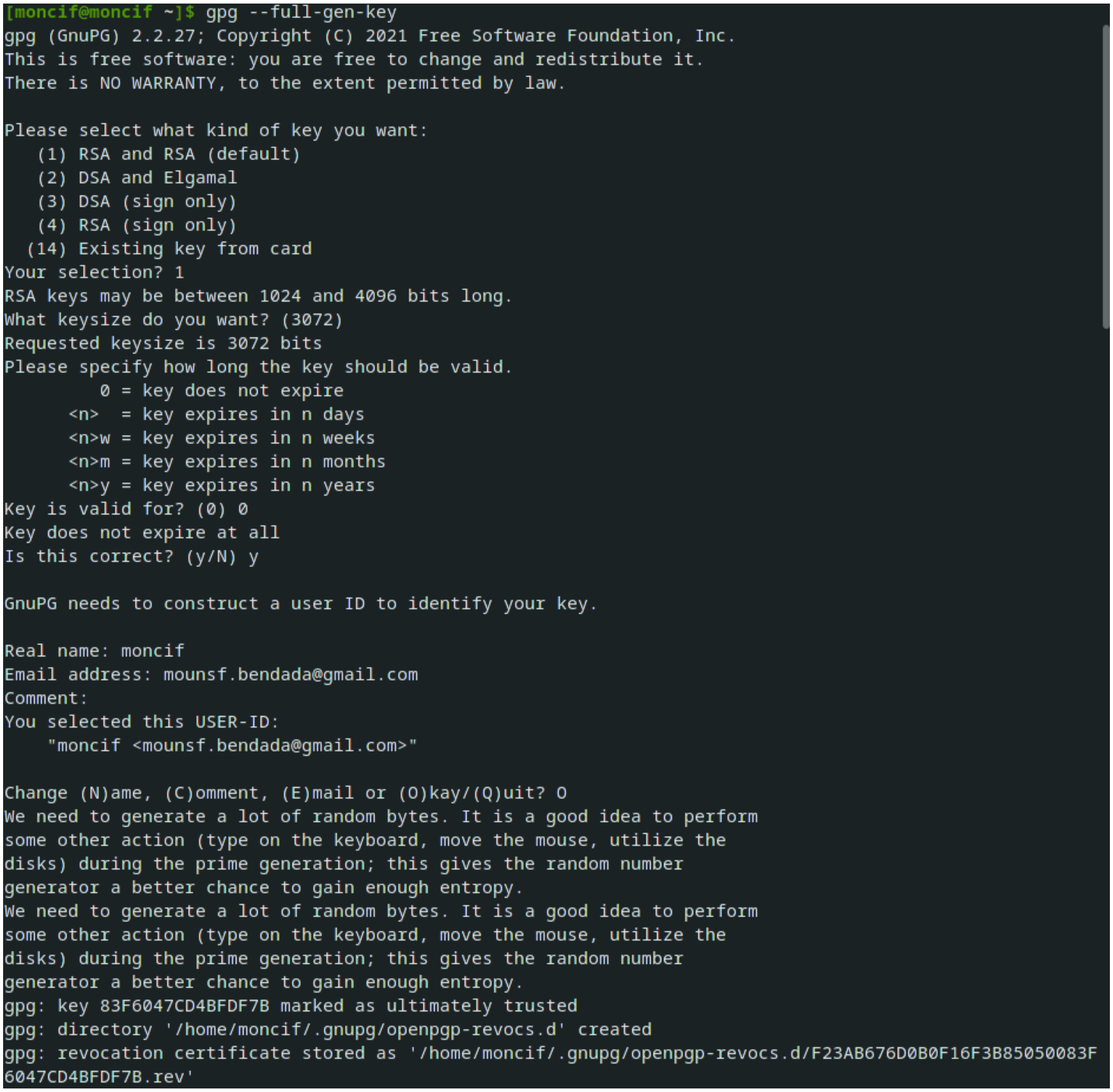
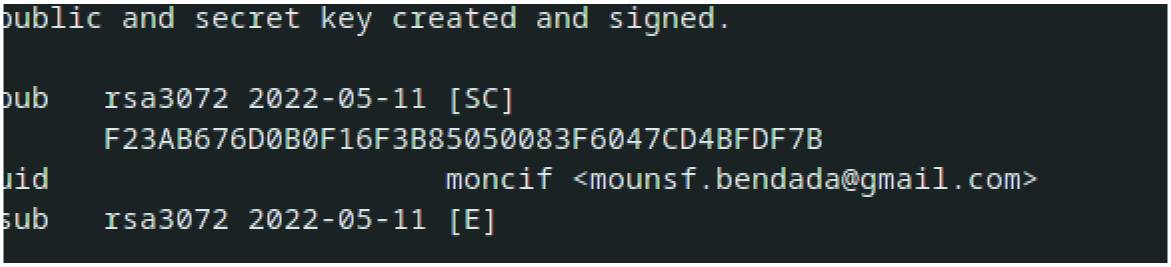
1- generate key : gpg --full-gen-key

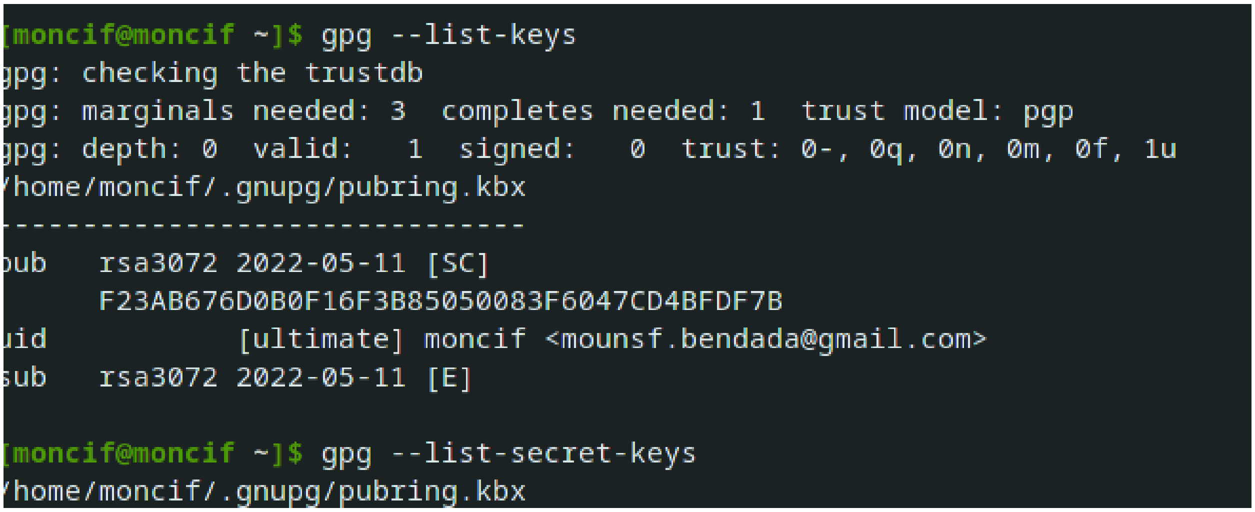


```
[moncif@moncif ~]$ gpg --full-gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

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)
Requested keysize is 3072 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) 0
Key does not expire at all
Is this correct? (y/N) y

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

Real name: moncif
Email address: mounsf.bendada@gmail.com
Comment:
You selected this USER-ID:
    "moncif <mounsf.bendada@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.
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 83F6047CD4BFDF7B marked as ultimately trusted
gpg: directory '/home/moncif/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/moncif/.gnupg/openpgp-revocs.d/F23AB676D0B0F16F3B85050083F
6047CD4BFDF7B.rev'
```



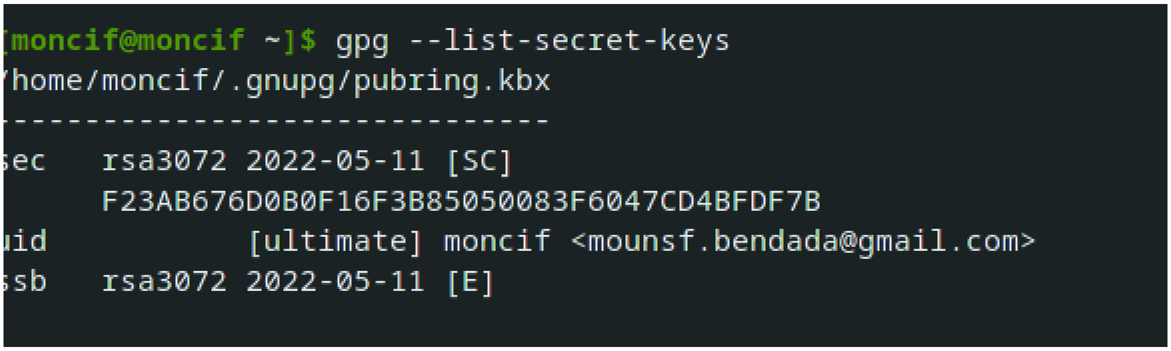
```
public and secret key created and signed.

pub   rsa3072 2022-05-11 [SC]
      F23AB676D0B0F16F3B85050083F6047CD4BFDF7B
uid                      moncif <mounsf.bendada@gmail.com>
sub   rsa3072 2022-05-11 [E]
```

2-To list keys in your public key ring: `gpg --list-keys`



```
[moncif@moncif ~]$ 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
/home/moncif/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2022-05-11 [SC]
      F23AB676D0B0F16F3B85050083F6047CD4BFDF7B
uid           [ultimate] moncif <mounsf.bendada@gmail.com>
sub   rsa3072 2022-05-11 [E]

[moncif@moncif ~]$ gpg --list-secret-keys
/home/moncif/.gnupg/pubring.kbx
```

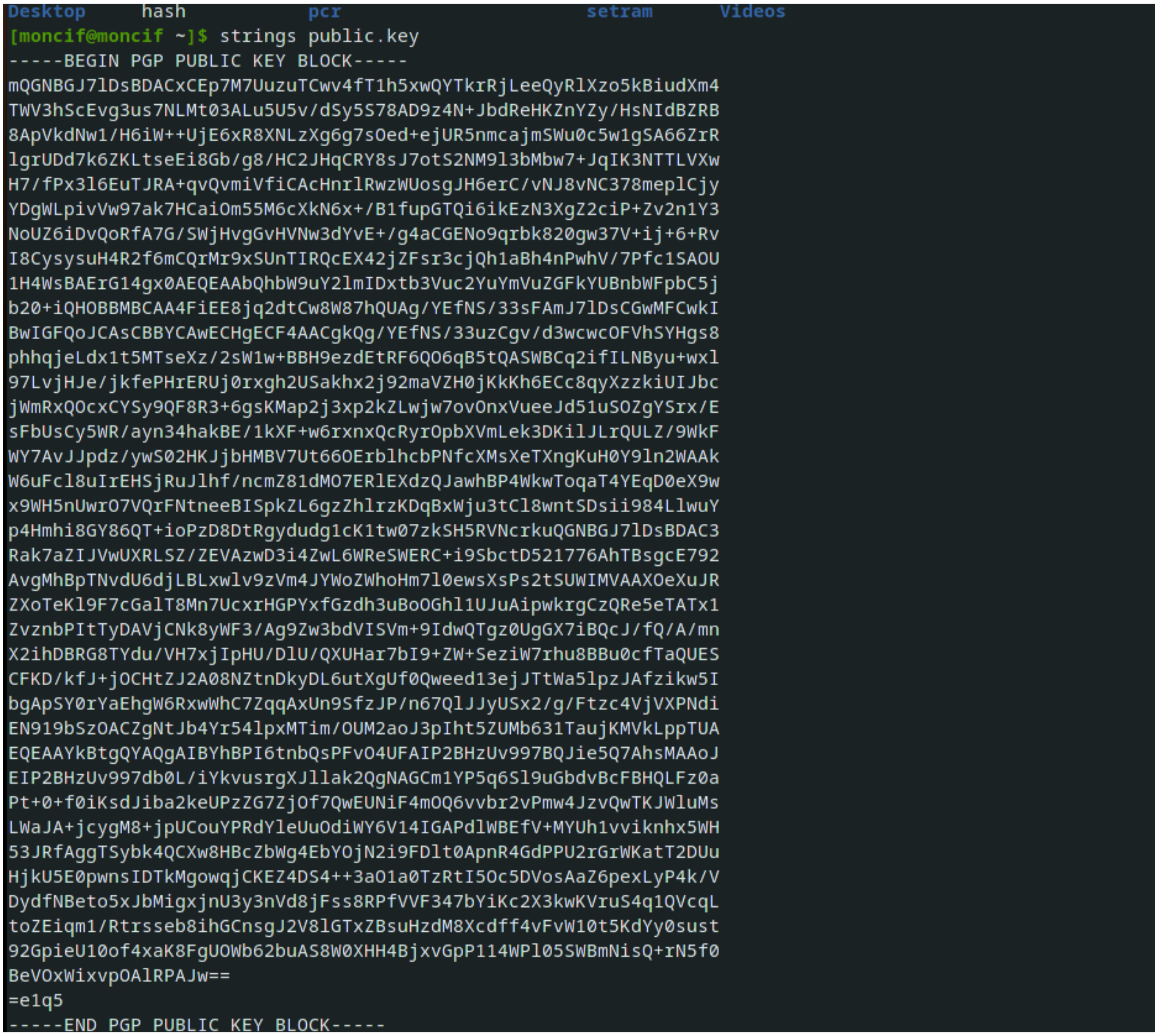
3-To list keys in your secret key ring: `gpg --list-secret-keys`



```
[moncif@moncif ~]$ gpg --list-secret-keys
/home/moncif/.gnupg/pubring.kbx
------------------------------
sec   rsa3072 2022-05-11 [SC]
      F23AB676D0B0F16F3B85050083F6047CD4BFDF7B
uid           [ultimate] moncif <mounsf.bendada@gmail.com>
ssb   rsa3072 2022-05-11 [E]
```

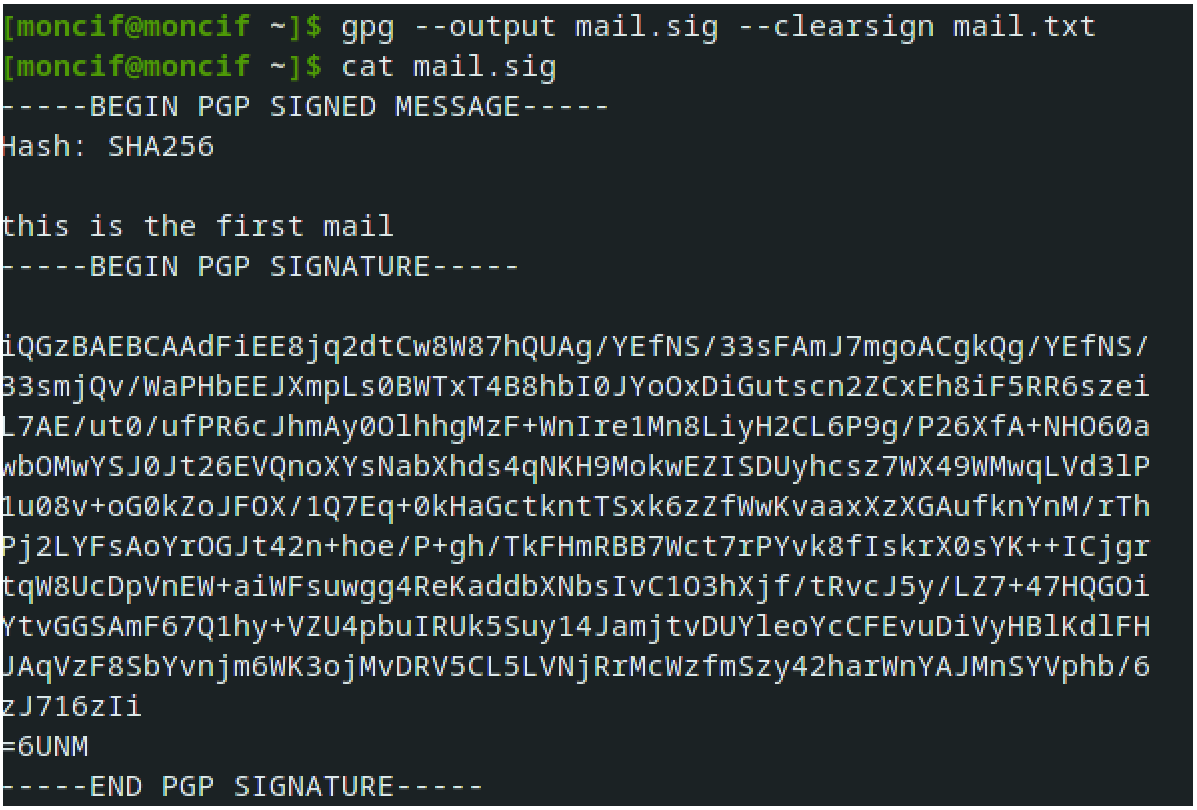
4-Export public key : gpg --export --armor --output public.key moncif

5



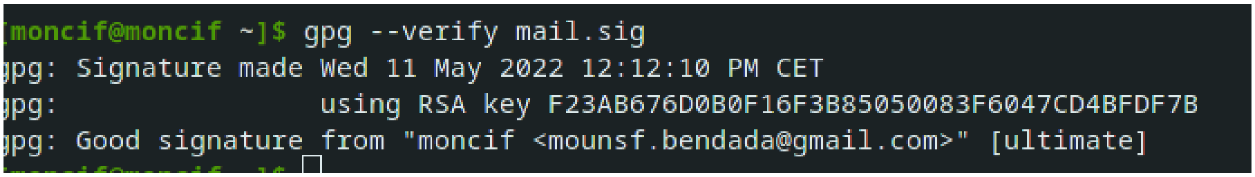
```
Desktop     hash          pcr                         setram      Videos
[moncif@moncif ~]$ strings public.key
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQGNBGJ7lDsBDACxCEp7M7UuzuTCwv4fT1h5xwQYTkrRjLeeQyRlXzo5kBiudXm4
TWV3hScEvg3us7NLMt03ALu5U5v/dSy5S78AD9z4N+JbdReHKZnYZy/HsNIdBZRB
8ApVkdNw1/H6iW++UjE6xR8XNLzXg6g7sOed+ejUR5nmcajmSWu0c5w1gSA66ZrR
lgrUDd7k6ZKLtseEi8Gb/g8/HC2JHqCRY8sJ7otS2NM9l3bMbw7+JqIK3NTTLVXw
H7/fPx3l6EuTJRA+qvQvmiVfiCAcHnrlRwzWUosgJH6erC/vNJ8vNC378meplCjy
YDgWLpivVw97ak7HCaiOm55M6cXkN6x+/B1fupGTQi6ikEzN3XgZ2ciP+Zv2n1Y3
NoUZ6iDvQoRfA7G/SWjHvgGvHVNw3dYvE+/g4aCGENo9qrbk820gw37V+ij+6+Rv
I8CysysuH4R2f6mCQrMr9xSUnTIRQcEX42jZFsr3cjQh1aBh4nPwhV/7Pfc1SAOU
1H4WsBAErG14gx0AEQEAAbQhbW9uY2lmIDxtb3Vuc2YuYmVuZGFkYUBnbWFpbC5j
b20+iQHOBBMBCAA4FiEE8jq2dtCw8W87hQUAg/YEfNS/33sFAmJ7lDsCGwMFCwkI
BwIGFQoJCAsCBBYCAwECHgECF4AACgkQg/YEfNS/33uzCgv/d3wcwcOFVhSYHgs8
phhqjeLdx1t5MTseXz/2sW1w+BBH9ezdEtRF6QO6qB5tQASWBCq2ifILNByu+wxl
97LvjHJe/jkfePHrERUj0rxgh2USakhx2j92maVZH0jKkKh6ECc8qyXzzkiUIJbc
jWmRxQOcxCYSy9QF8R3+6gsKMap2j3xp2kZLwjw7ovOnxVueeJd51uSOZgYSrx/E
sFbUsCy5WR/ayn34hakBE/1kXF+w6rxnxQcRyrOpbXVmLek3DKilJLrQULZ/9WkF
WY7AvJJpdz/ywS02HKJjbHMBV7Ut66OErblhcbPNfcXMsXeTXngKuH0Y9ln2WAAk
W6uFcl8uIrEHSjRuJlhf/ncmZ81dMO7ERlEXdzQJawhBP4WkwToqaT4YEqD0eX9w
x9WH5nUwrO7VQrFNtneeBISpkZL6gzZhlrzKDqBxWju3tCl8wntSDsii984LlwuY
p4Hmhi8GY86QT+ioPzD8DtRgydudg1cK1tw07zkSH5RVNcrkuQGNBGJ7lDsBDAC3
Rak7aZIJVwUXRLSZ/ZEVAzwD3i4ZwL6WReSWERC+i9SbctD521776AhTBsgcE792
AvgMhBpTNvdU6djLBLxwlv9zVm4JYWoZWhoHm7l0ewsXsPs2tSUWIMVAAXOeXuJR
ZXoTeKl9F7cGalT8Mn7UcxrHGPYxfGzdh3uBoOGhl1UJuAipwkrgCzQRe5eTATx1
ZvznbPItTyDAVjCNk8yWF3/Ag9Zw3bdVISVm+9IdwQTgz0UgGX7iBQcJ/fQ/A/mn
X2ihDBRG8TYdu/VH7xjIpHU/DlU/QXUHar7bI9+ZW+SeziW7rhu8BBu0cfTaQUES
CFKD/kfJ+jOCHtZJ2A08NZtnDkyDL6utXgUf0Qweed13ejJTtWa5lpzJAfzikw5I
bgApSY0rYaEhgW6RxwWhC7ZqqAxUn9SfzJP/n67QlJJyUSx2/g/Ftzc4VjVXPNdi
EN919bSzOACZgNtJb4Yr54lpxMTim/OUM2aoJ3pIht5ZUMb631TaujKMVkLppTUA
EQEAAYkBtgQYAQgAIBYhBPI6tnbQsPFvO4UFAIP2BHzUv997BQJie5Q7AhsMAAoJ
EIP2BHzUv997db0L/iYkvusrgXJllak2QgNAGCm1YP5q6Sl9uGbdvBcFBHQLFz0a
Pt+0+f0iKsdJiba2keUPzZG7ZjOf7QwEUNiF4mOQ6vvbr2vPmw4JzvQwTKJWluMs
LWaJA+jcygM8+jpUCouYPRdYleUuOdiWY6V14IGAPdlWBEfV+MYUh1vviknhx5WH
53JRfAggTSybk4QCXw8HBcZbWg4EbYOjN2i9FDlt0ApnR4GdPPU2rGrWKatT2DUu
HjkU5E0pwnsIDTkMgowqjCKEZ4DS4++3aO1a0TzRtI5Oc5DVosAaZ6pexLyP4k/V
DydfNBeto5xJbMigxjnU3y3nVd8jFss8RPfVVF347bYiKc2X3kwKVruS4q1QVcqL
toZEiqm1/Rtrsseb8ihGCnsgJ2V8lGTxZBsuHzdM8Xcdff4vFvW10t5KdYy0sust
92GpieU10of4xaK8FgUOWb62buAS8W0XHH4BjxvGpP114WPl05SWBmNisQ+rN5f0
BeVOxWixvpOAlRPAJw==
=e1q5
-----END PGP PUBLIC KEY BLOCK-----
```

Create a msg and sign it :



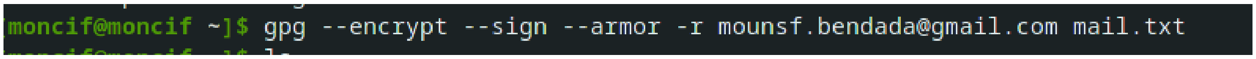
```
[moncif@moncif ~]$ gpg --output mail.sig --clearsign mail.txt
[moncif@moncif ~]$ cat mail.sig
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

this is the first mail
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCAAdFiEE8jq2dtCw8W87hQUAg/YEfNS/33sFAmJ7mgoACgkQg/YEfNS/
33smjQv/WaPHbEEJXmpLs0BWTxT4B8hbI0JYoOxDiGutscn2ZCxEh8iF5RR6szei
L7AE/ut0/ufPR6cJhmAy0OlhhgMzF+WnIre1Mn8LiyH2CL6P9g/P26XfA+NHO60a
wbOMwYSJ0Jt26EVQnoXYsNabXhds4qNKH9MokwEZISDUyhcsz7WX49WMwqLVd3lP
1u08v+oG0kZoJFOX/1Q7Eq+0kHaGctkntTSxk6zZfWwKvaaxXzXGAufknYnM/rTh
Pj2LYFsAoYrOGJt42n+hoe/P+gh/TkFHmRBB7Wct7rPYvk8fIskrX0sYK++ICjgr
tqW8UcDpVnEW+aiWFsuwgg4ReKaddbXNbsIvC1O3hXjf/tRvcJ5y/LZ7+47HQGOi
YtvGGSAmF67Q1hy+VZU4pbuIRUk5Suy14JamjtvDUYleoYcCFEvuDiVyHBlKdlFH
JAqVzF8SbYvnjm6WK3ojMvDRV5CL5LVNjRrMcWzfmSzy42harWnYAJMnSYVphb/6
zJ716zIi
=6UNM
-----END PGP SIGNATURE-----
```

Verify the signature :

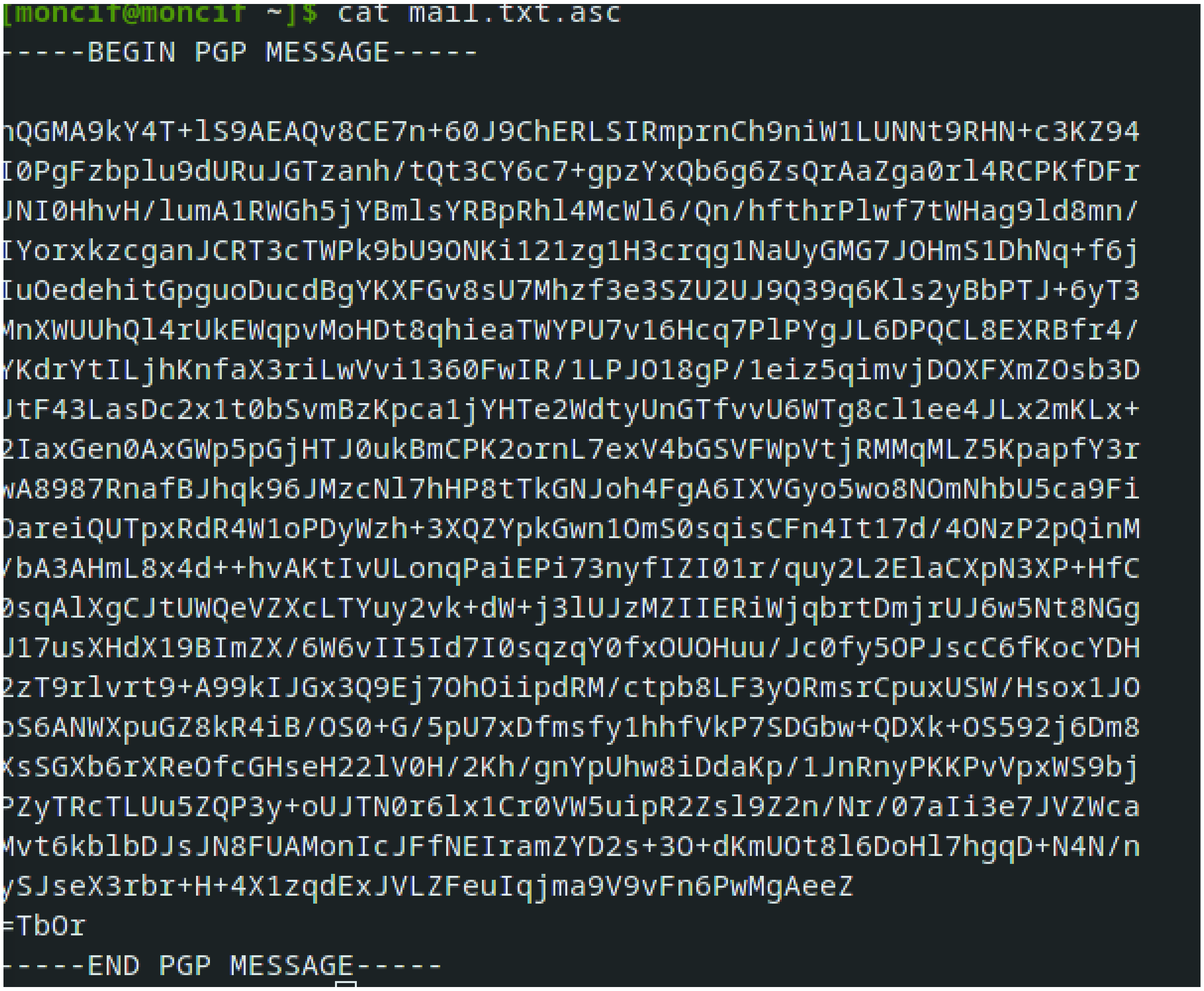


```
[moncif@moncif ~]$ gpg --verify mail.sig
gpg: Signature made Wed 11 May 2022 12:12:10 PM CET
gpg:                using RSA key F23AB676D0B0F16F3B85050083F6047CD4BFDF7B
gpg: Good signature from "moncif <mounsf.bendada@gmail.com>" [ultimate]
```

Encrypt Messages

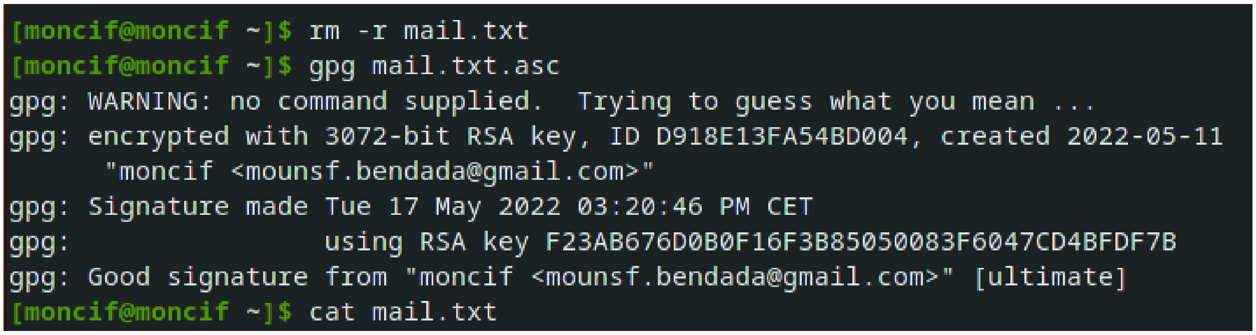


```
[moncif@moncif ~]$ gpg --encrypt --sign --armor -r mounsf.bendada@gmail.com mail.txt
```



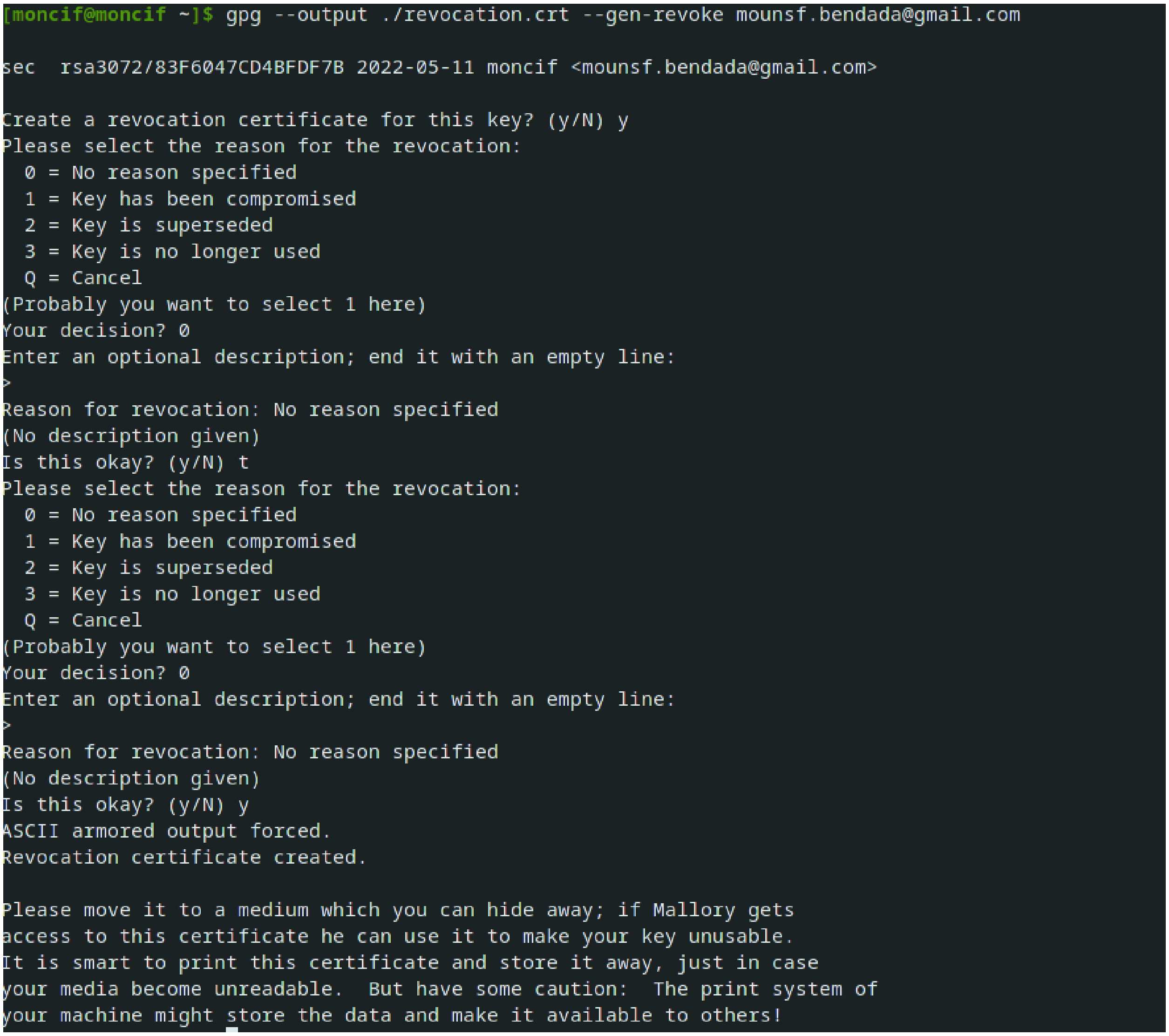
```
[moncif@moncif ~]$ cat mail.txt.asc
-----BEGIN PGP MESSAGE-----

hQGMA9kY4T+lS9AEAQv8CE7n+60J9ChERLSIRmprnCh9niW1LUNNt9RHN+c3KZ94
I0PgFzbplu9dURuJGTzanh/tQt3CY6c7+gpzYxQb6g6ZsQrAaZga0rl4RCPKfDFr
UNI0HhvH/lumA1RWGh5jYBmlsYRBpRhl4McWl6/Qn/hfthrPlwf7tWHag9ld8mn/
IYorxkzcganJCRT3cTWPk9bU9ONKi121zg1H3crqg1NaUyGMG7JOHmS1DhNq+f6j
IuOedehitGpguoDucdBgYKXFGv8sU7Mhzf3e3SZU2UJ9Q39q6Kls2yBbPTJ+6yT3
MnXWUUhQl4rUkEWqpvMoHDt8qhieaTWYPU7v16Hcq7PlPYgJL6DPQCL8EXRBfr4/
YKdrYtILjhKnfaX3riLwVvi1360FwIR/1LPJO18gP/1eiz5qimvjDOXFXmZOsb3D
JtF43LasDc2x1t0bSvmBzKpca1jYHTe2WdtyUnGTfvvU6WTg8cl1ee4JLx2mKLx+
2IaxGen0AxGWp5pGjHTJ0ukBmCPK2ornL7exV4bGSVFWpVtjRMMqMLZ5KpapfY3r
wA8987RnafBJhqk96JMzcNl7hHP8tTkGNJoh4FgA6IXVGyo5wo8NOmNhbU5ca9Fi
DareiQUTpxRdR4W1oPDyWzh+3XQZYpkGwn1OmS0sqisCFn4It17d/4ONzP2pQinM
/bA3AHmL8x4d++hvAKtIvULonqPaiEPi73nyfIZI01r/quy2L2ElaCXpN3XP+HfC
0sqAlXgCJtUWQeVZXcLTYuy2vk+dW+j3lUJzMZIIERiWjqbrtDmjrUJ6w5Nt8NGg
J17usXHdX19BImZX/6W6vII5Id7I0sqzqY0fxOUOHuu/Jc0fy5OPJscC6fKocYDH
2zT9rlvrt9+A99kIJGx3Q9Ej7OhOiipdRM/ctpb8LF3yORmsrCpuxUSW/Hsox1JO
bS6ANWXpuGZ8kR4iB/OS0+G/5pU7xDfmsfy1hhfVkP7SDGbw+QDXk+OS592j6Dm8
XsSGXb6rXReOfcGHseH22lV0H/2Kh/gnYpUhw8iDdaKp/1JnRnyPKKPvVpxWS9bj
PZyTRcTLUu5ZQP3y+oUJTN0r6lx1Cr0VW5uipR2Zsl9Z2n/Nr/07aIi3e7JVZWca
Mvt6kblbDJsJN8FUAMonIcJFfNEIramZYD2s+3O+dKmUOt8l6DoHl7hgqD+N4N/n
ySJseX3rbr+H+4X1zqdExJVLZFeuIqjma9V9vFn6PwMgAeeZ
=TbOr
-----END PGP MESSAGE-----
```

Decrypt the msg



```
[moncif@moncif ~]$ rm -r mail.txt
[moncif@moncif ~]$ gpg mail.txt.asc
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: encrypted with 3072-bit RSA key, ID D918E13FA54BD004, created 2022-05-11
      "moncif <mounsf.bendada@gmail.com>"
gpg: Signature made Tue 17 May 2022 03:20:46 PM CET
gpg:                using RSA key F23AB676D0B0F16F3B85050083F6047CD4BFDF7B
gpg: Good signature from "moncif <mounsf.bendada@gmail.com>" [ultimate]
[moncif@moncif ~]$ cat mail.txt
```

Révocation des clés



```
[moncif@moncif ~]$ gpg --output ./revocation.crt --gen-revoke mounsf.bendada@gmail.com

sec  rsa3072/83F6047CD4BFDF7B 2022-05-11 moncif <mounsf.bendada@gmail.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? 0
Enter an optional description; end it with an empty line:
>
Reason for revocation: No reason specified
(No description given)
Is this okay? (y/N) t
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? 0
Enter an optional description; end it with an empty line:
>
Reason for revocation: No reason specified
(No description given)
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!
```