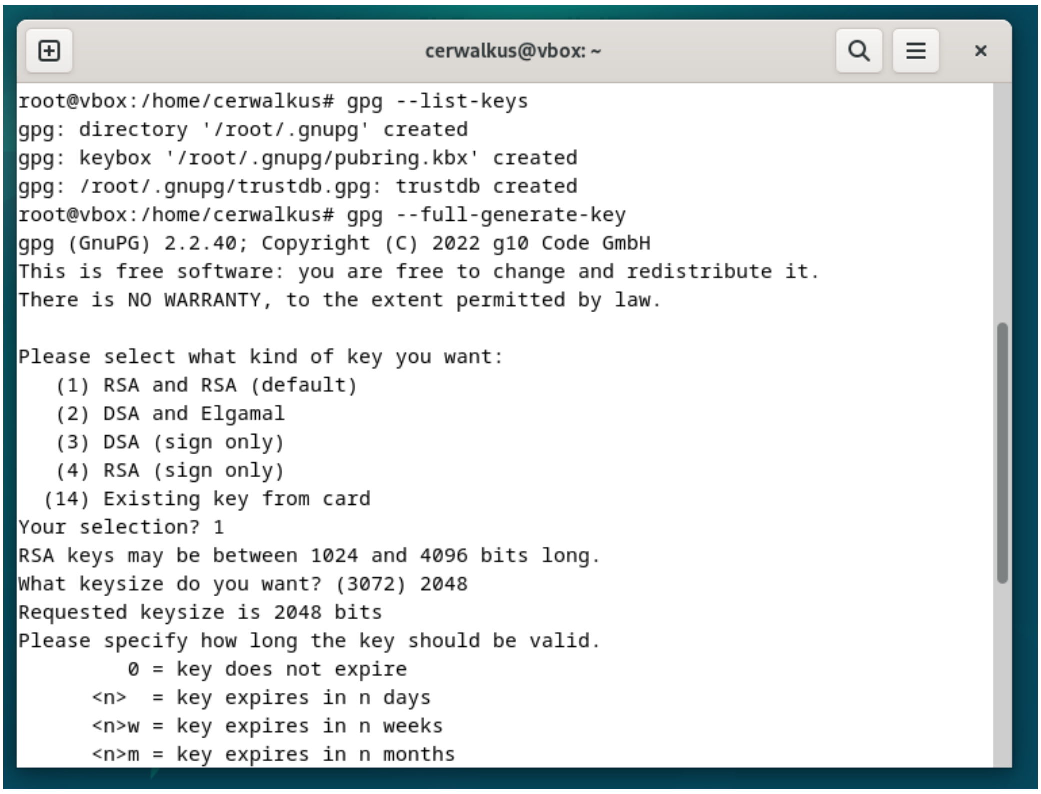
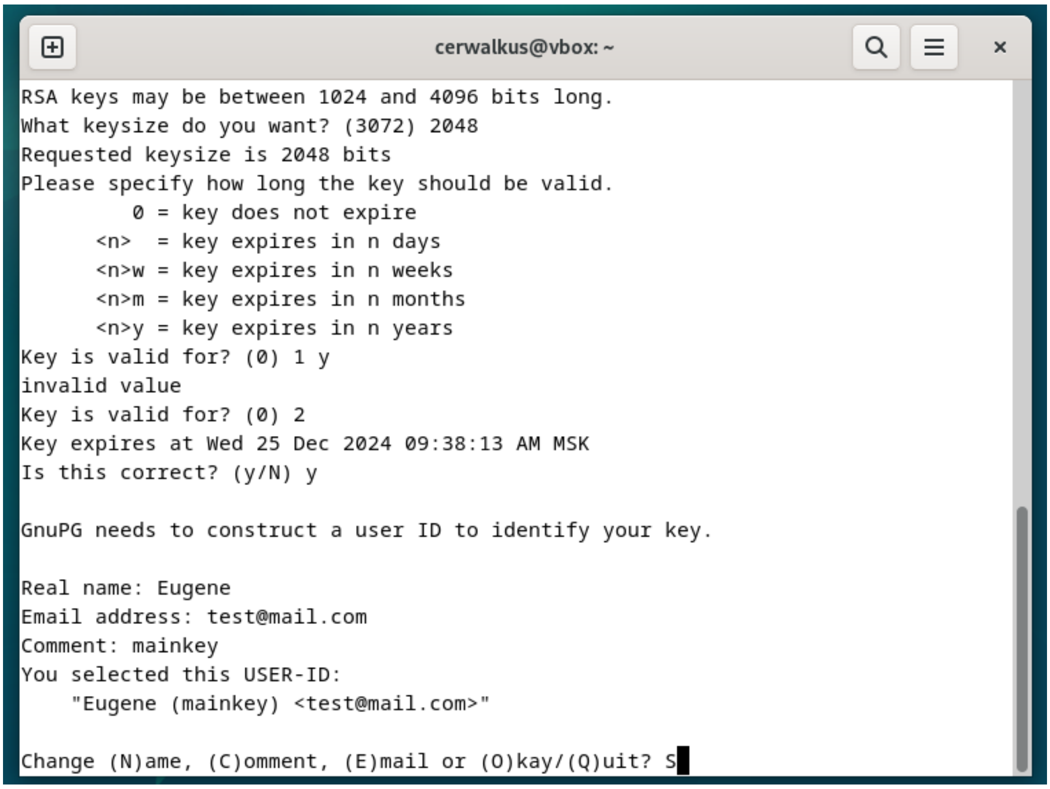
Гиндин Евгений Михайлович
Отчёт по практической 7

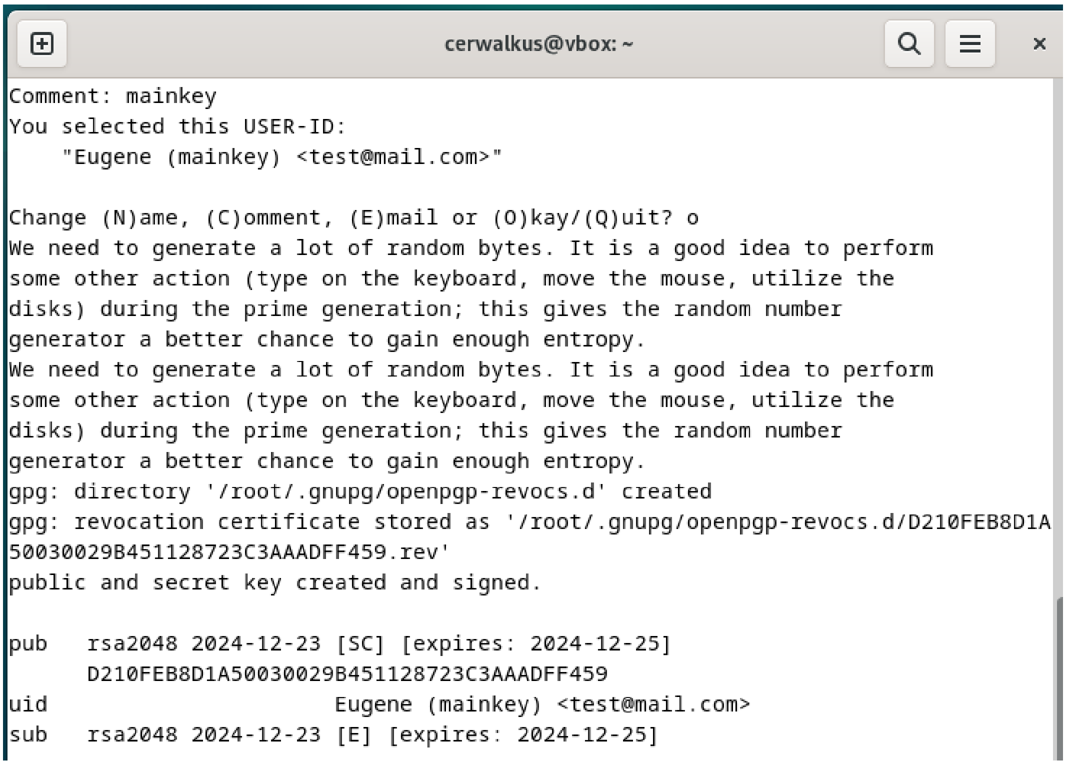
Задание 1. Настройка GnuPG



```
root@vbox:/home/cerwalkus# gpg --list-keys
gpg: directory '/root/.gnupg' created
gpg: keybox '/root/.gnupg/pubring.kbx' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
root@vbox:/home/cerwalkus# 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) 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
```

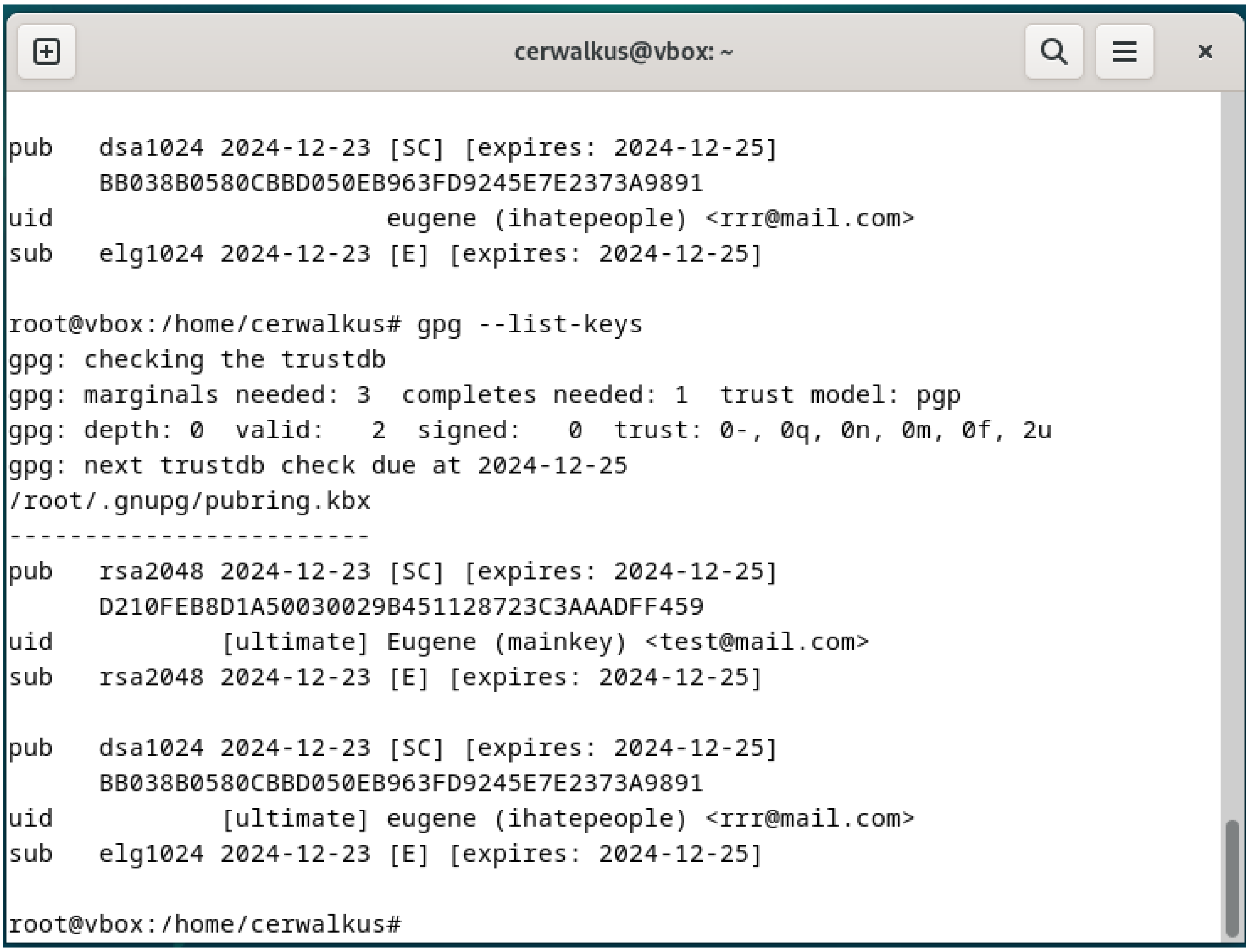


```
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 1 y
invalid value
Key is valid for? (0) 2
Key expires at Wed 25 Dec 2024 09:38:13 AM MSK
Is this correct? (y/N) y

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

Real name: Eugene
Email address: test@mail.com
Comment: mainkey
You selected this USER-ID:
    "Eugene (mainkey) <test@mail.com>"

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

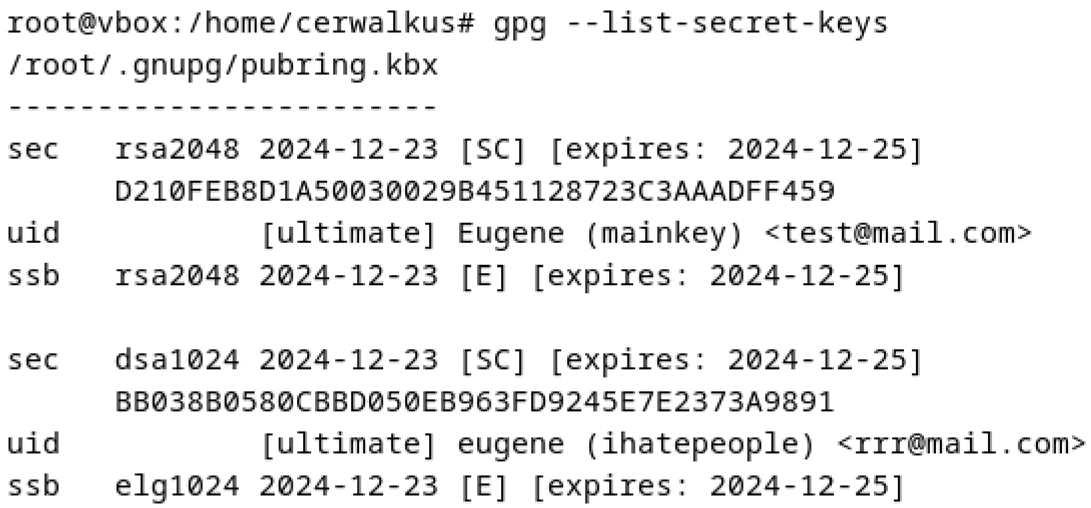


```
Comment: mainkey
You selected this USER-ID:
    "Eugene (mainkey) <test@mail.com>"

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: directory '/root/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/D210FEB8D1A
50030029B451128723C3AAADFF459.rev'
public and secret key created and signed.

pub   rsa2048 2024-12-23 [SC] [expires: 2024-12-25]
      D210FEB8D1A50030029B451128723C3AAADFF459
uid                      Eugene (mainkey) <test@mail.com>
sub   rsa2048 2024-12-23 [E] [expires: 2024-12-25]
```

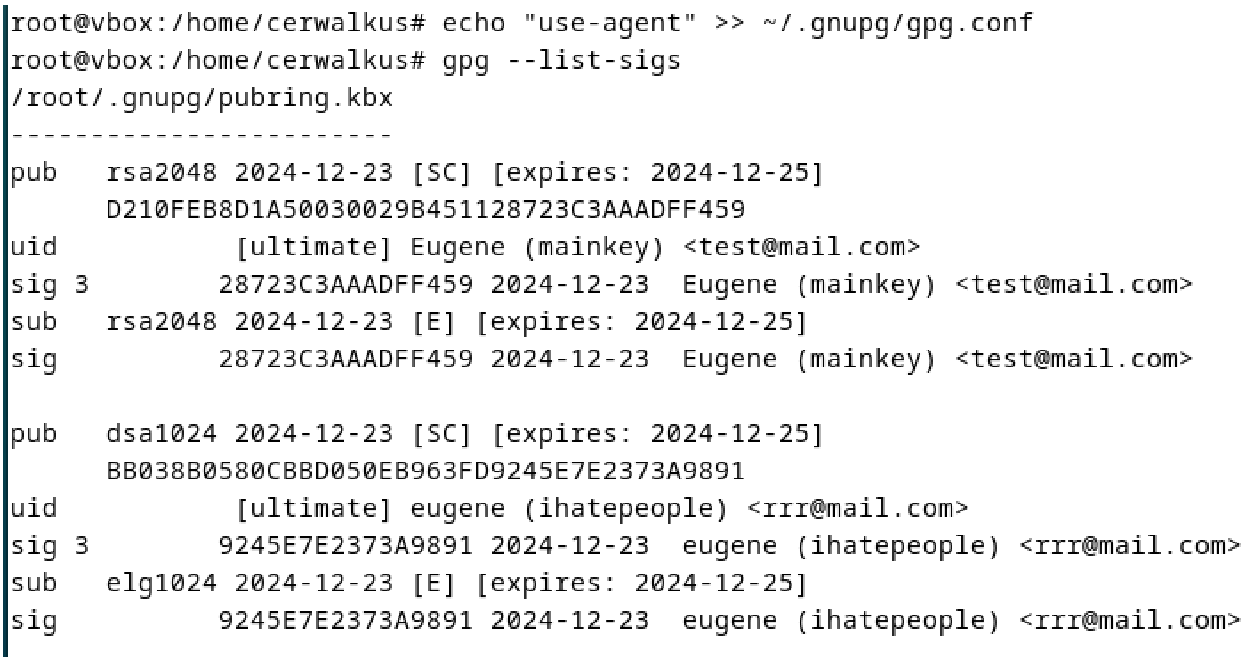
Задание 2. Управление ключами



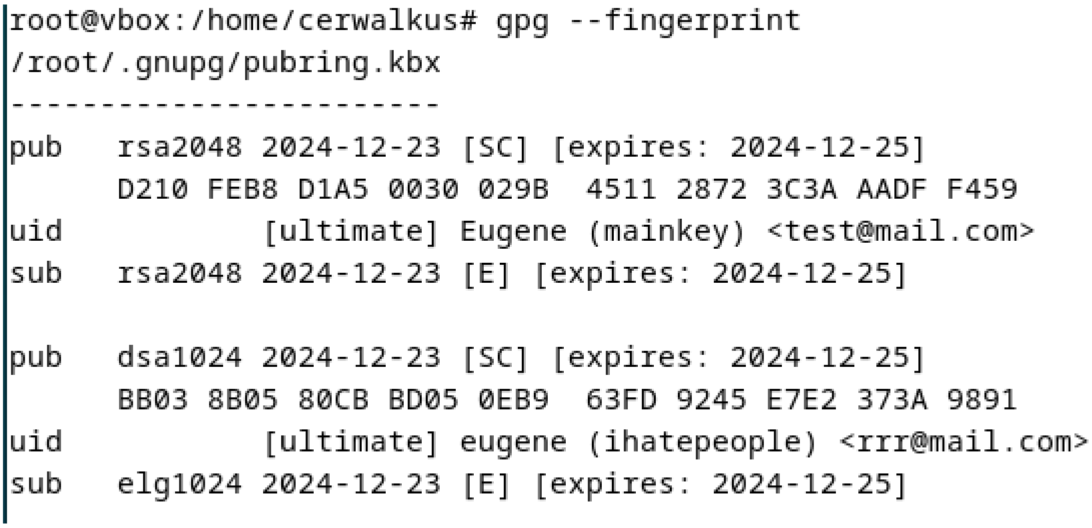
```
pub   dsa1024 2024-12-23 [SC] [expires: 2024-12-25]
      BB038B0580CBBD050EB963FD9245E7E2373A9891
uid                      eugene (ihatepeople) <rrr@mail.com>
sub   elg1024 2024-12-23 [E] [expires: 2024-12-25]

root@vbox:/home/cerwalkus# 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 2024-12-25
/root/.gnupg/pubring.kbx
------------------------
pub   rsa2048 2024-12-23 [SC] [expires: 2024-12-25]
      D210FEB8D1A50030029B451128723C3AAADFF459
uid           [ultimate] Eugene (mainkey) <test@mail.com>
sub   rsa2048 2024-12-23 [E] [expires: 2024-12-25]

pub   dsa1024 2024-12-23 [SC] [expires: 2024-12-25]
      BB038B0580CBBD050EB963FD9245E7E2373A9891
uid           [ultimate] eugene (ihatepeople) <rrr@mail.com>
sub   elg1024 2024-12-23 [E] [expires: 2024-12-25]

root@vbox:/home/cerwalkus#
```



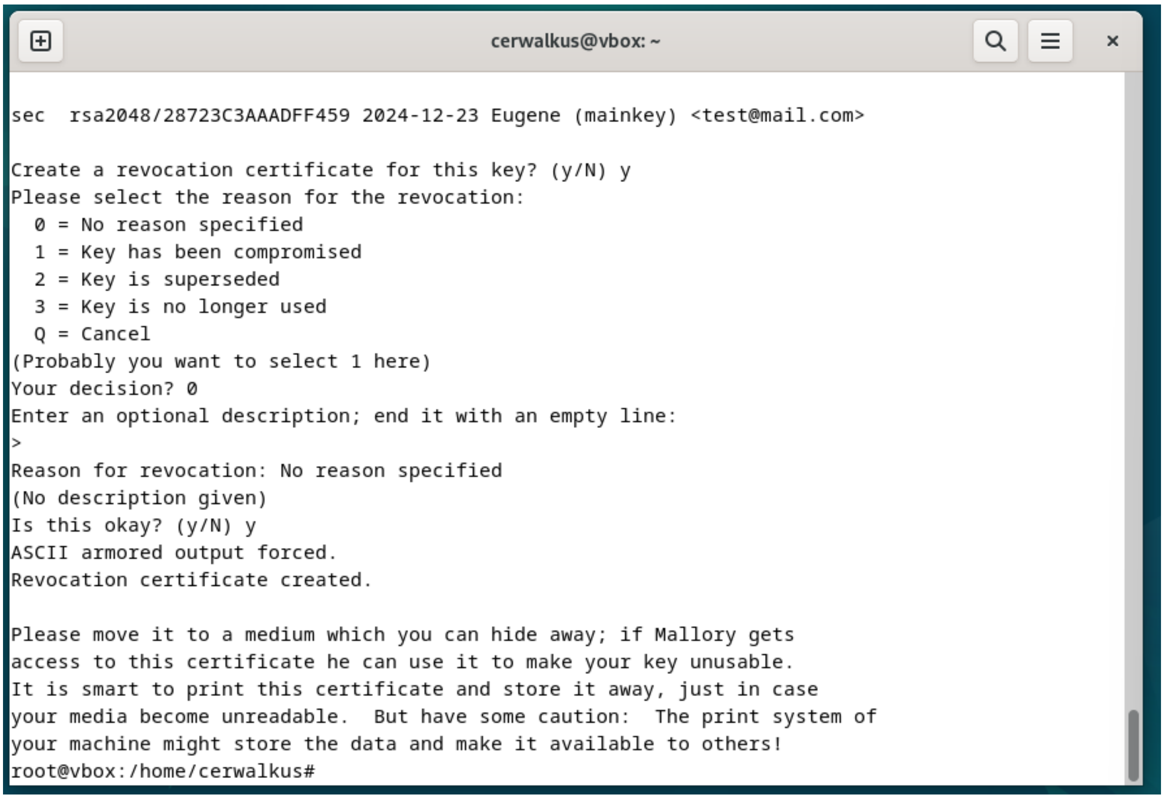
```
root@vbox:/home/cerwalkus# gpg --list-secret-keys
/root/.gnupg/pubring.kbx
------------------------
sec   rsa2048 2024-12-23 [SC] [expires: 2024-12-25]
      D210FEB8D1A50030029B451128723C3AAADFF459
uid           [ultimate] Eugene (mainkey) <test@mail.com>
ssb   rsa2048 2024-12-23 [E] [expires: 2024-12-25]

sec   dsa1024 2024-12-23 [SC] [expires: 2024-12-25]
      BB038B0580CBBD050EB963FD9245E7E2373A9891
uid           [ultimate] eugene (ihatepeople) <rrr@mail.com>
ssb   elg1024 2024-12-23 [E] [expires: 2024-12-25]
```



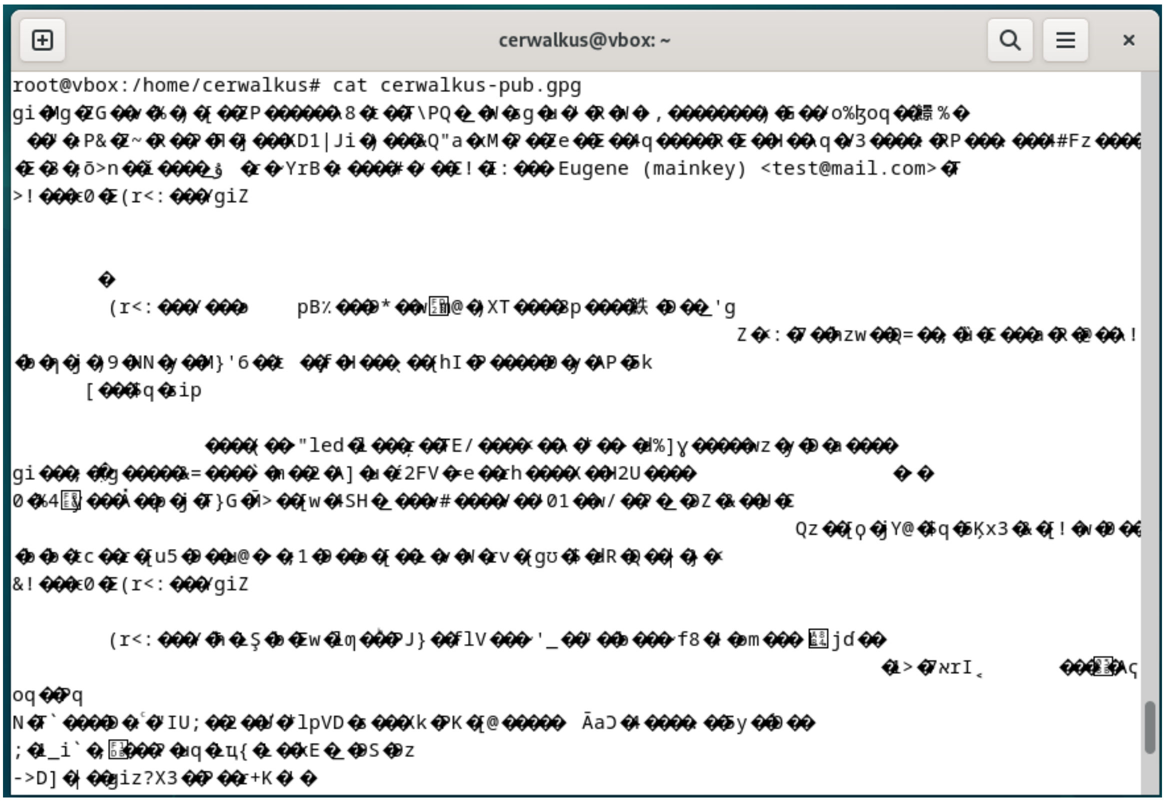
```
root@vbox:/home/cerwalkus# echo "use-agent" >> ~/.gnupg/gpg.conf
root@vbox:/home/cerwalkus# gpg --list-sigs
/root/.gnupg/pubring.kbx
------------------------
pub   rsa2048 2024-12-23 [SC] [expires: 2024-12-25]
      D210FEB8D1A50030029B451128723C3AAADFF459
uid           [ultimate] Eugene (mainkey) <test@mail.com>
sig 3        28723C3AAADFF459 2024-12-23  Eugene (mainkey) <test@mail.com>
sub   rsa2048 2024-12-23 [E] [expires: 2024-12-25]
sig          28723C3AAADFF459 2024-12-23  Eugene (mainkey) <test@mail.com>

pub   dsa1024 2024-12-23 [SC] [expires: 2024-12-25]
      BB038B0580CBBD050EB963FD9245E7E2373A9891
uid           [ultimate] eugene (ihatepeople) <rrr@mail.com>
sig 3        9245E7E2373A9891 2024-12-23  eugene (ihatepeople) <rrr@mail.com>
sub   elg1024 2024-12-23 [E] [expires: 2024-12-25]
sig          9245E7E2373A9891 2024-12-23  eugene (ihatepeople) <rrr@mail.com>
```



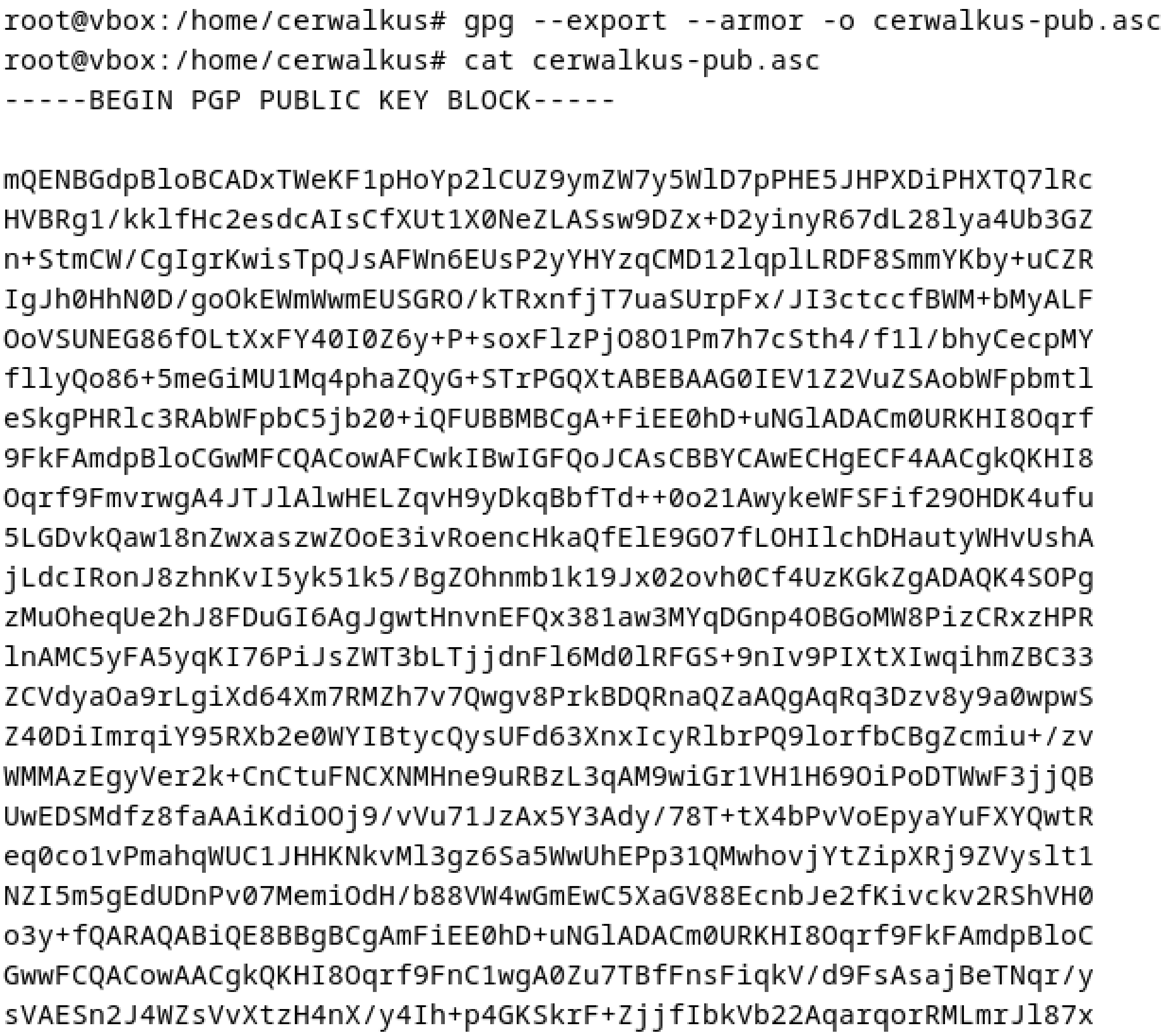
```
root@vbox:/home/cerwalkus# gpg --fingerprint
/root/.gnupg/pubring.kbx
------------------------
pub   rsa2048 2024-12-23 [SC] [expires: 2024-12-25]
      D210 FEB8 D1A5 0030 029B  4511 2872 3C3A AADF F459
uid           [ultimate] Eugene (mainkey) <test@mail.com>
sub   rsa2048 2024-12-23 [E] [expires: 2024-12-25]

pub   dsa1024 2024-12-23 [SC] [expires: 2024-12-25]
      BB03 8B05 80CB BD05 0EB9  63FD 9245 E7E2 373A 9891
uid           [ultimate] eugene (ihatepeople) <rrr@mail.com>
sub   elg1024 2024-12-23 [E] [expires: 2024-12-25]
```



```
sec  rsa2048/28723C3AAADFF459 2024-12-23 Eugene (mainkey) <test@mail.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) 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!
root@vbox:/home/cerwalkus#
```

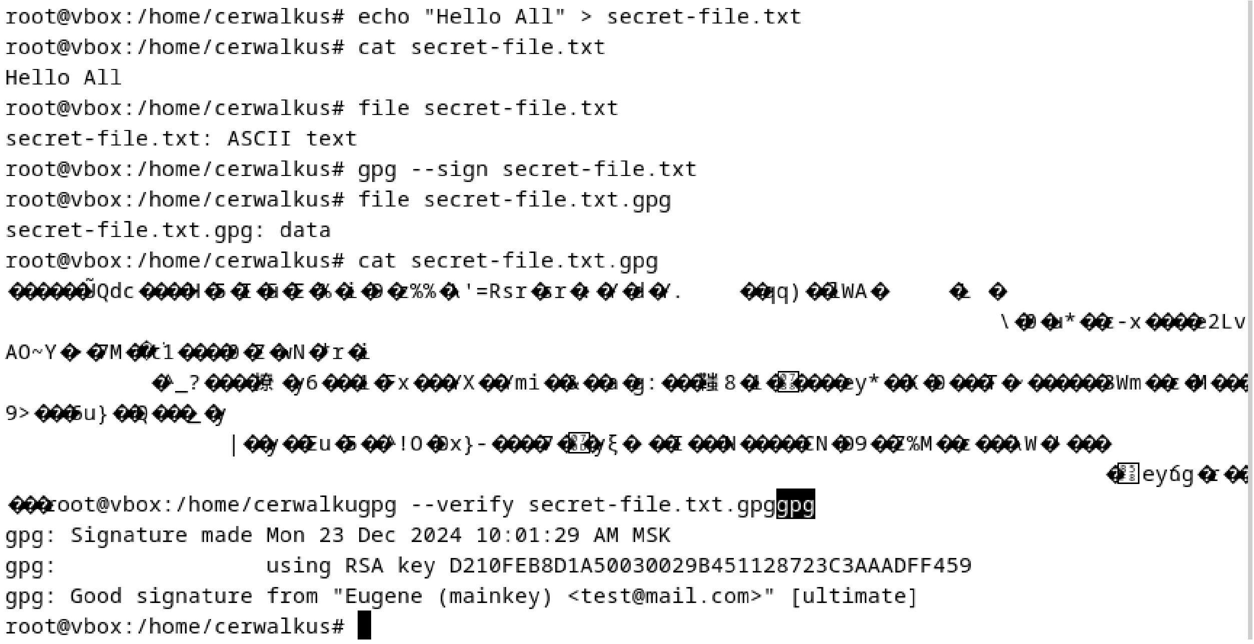


```
root@vbox:/home/cerwalkus# cat cerwalkus-pub.gpg
gi�Mg�ZG��%�)�{��ZP������8�ȶ��T\PQ�_�N�sg�u� �R�N�,��������)�G��/o%ʒoq���%�
 ��'�P&�Z~�R��P�ŋ�j���XD1|Ji�)���&Q"a�xM�?��Ze��E��4q�����R�E��H��q�/3���� �RP��� ���4#Fz���
�E�3�;ō>n��ĭ����ş  �ȶ�YrB� ����#� ��E!�I:��� Eugene (mainkey) <test@mail.com>�T
>!���ɛ0�E(ɼ<:���/giZ



        �
         (ɼ<:���/���     pB⁄���*��w�m@�)XT����3p����鉄 �D��_'g
                                                                   Z�ˣ:�7��hzw��Q=��,�ŭ�E���a�R�@��ѧ!
�b�ɲ�j�)9�NN�y��M}'6��t  ��f�H���˛��{hI�P�����D�y�AP�5k
       [���$q�sip


                 ����(��"led�l���ɽ��TE/����ˣ��ѧ�'��d%]ɣ�����vz�y�D�a����
gi���;��g�����&=����`�n��2�A]�u�ɛ2FV�=e��ɽh����X��H2U����               ��
0�%4�y���Ȧ��p�j�T}G�M̄>��{w�4SH�_���#����/��01��v/��?�_�DZ�&��J�E
                                                                          Qz��{ǫ�jY@�$q�5Ķx3�&�{!�v�D��
�b�b�ȶc��ɼ�{u5�D��u@��,1�D��b�{��ɛ�v�N�ɼv�{gʊ�$�dR�Q��|�)�ˣ
&!���ɛ0�E(ɼ<:���/giZ

        (ɼ<:���/�h�ɛŞ�b�Ew�lɱ���PJ}��flV���'_��'��b���f8�4 �m����jɗ��
                                                                             �l>�7ɤrI˛      ����Aç
oq��Pq
N�T`����D�ˁ�'IU;��2��/�'lpVD�s���Xk�PK�{@�����  ĀaϽ�4����.��5y��D��
;�l_i`�,����P�uq�ɛɥ{�ɛ��xE�_�DS�9z
->D]�|��giz?X3��P��r+K�'�
```

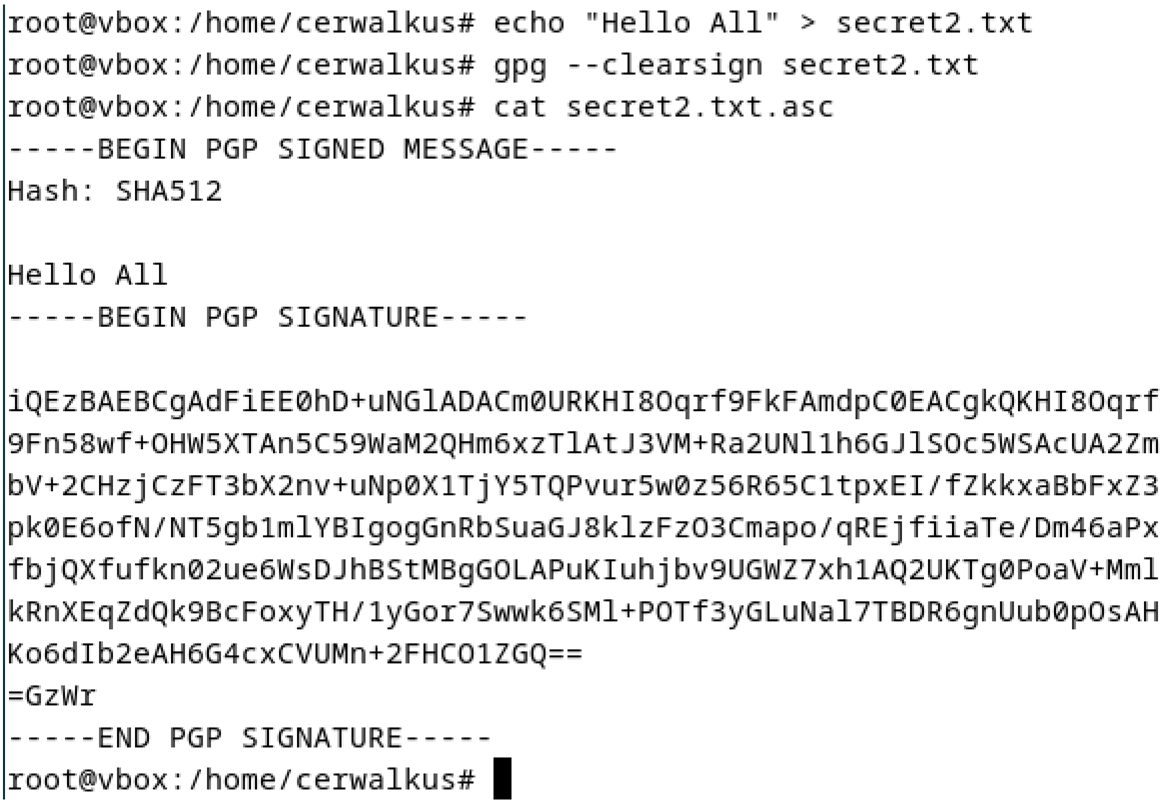


```
root@vbox:/home/cerwalkus# gpg --export --armor -o cerwalkus-pub.asc
root@vbox:/home/cerwalkus# cat cerwalkus-pub.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBGdpBloBCADxTWeKF1pHoYp2lCUZ9ymZW7y5WlD7pPHE5JHPXDiPHXTQ7lRc
HVBRg1/kklfHc2esdcAIsCfXUt1X0NeZLASsw9DZx+D2yinyR67dL28lya4Ub3GZ
n+StmCW/CgIgrKwisTpQJsAFWn6EUsP2yYHYzqCMD12lqplLRDF8SmmYKby+uCZR
IgJh0HhN0D/goOkEWmWwmEUSGRO/kTRxnfjT7uaSUrpFx/JI3ctccfBWM+bMyALF
OoVSUNEG86fOLtXxFY40I0Z6y+P+soxFlzPjO8O1Pm7h7cSth4/f1l/bhyCecpMY
fllyQo86+5meGiMU1Mq4phaZQyG+STrPGQXtABEBAAG0IEV1Z2VuZSAobWFpbmtl
eSkgPHRlc3RAbWFpbC5jb20+iQFUBBMBCgA+FiEE0hD+uNGlADACm0URKHI8Oqrf
9FkFAmdpBloCGwMFCQACowAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQKHI8
Oqrf9FmvrwgA4JTJlAlwHELZqvH9yDkqBbfTd++0o21AwykeWFSFif29OHDK4ufu
5LGDvkQaw18nZwxaszwZOoE3ivRoencHkaQfElE9GO7fLOHIlchDHautyWHvUshA
jLdcIRonJ8zhnKvI5yk51k5/BgZOhnmb1k19Jx02ovh0Cf4UzKGkZgADAQK4SOPg
zMuOheqUe2hJ8FDuGI6AgJgwtHnvnEFQx381aw3MYqDGnp4OBGoMW8PizCRxzHPR
lnAMC5yFA5yqKI76PiJsZWT3bLTjjdnFl6Md0lRFGS+9nIv9PIXtXIwqihmZBC33
ZCVdyaOa9rLgiXd64Xm7RMZh7v7Qwgv8PrkBDQRnaQZaAQgAqRq3Dzv8y9a0wpwS
Z40DiImrqiY95RXb2e0WYIBtycQysUFd63XnxIcyRlbrPQ9lorfbCBgZcmiu+/zv
WMMAzEgyVer2k+CnCtuFNCXNMHne9uRBzL3qAM9wiGr1VH1H69OiPoDTWwF3jjQB
UwEDSMdfz8faAAiKdiOOj9/vVu71JzAx5Y3Ady/78T+tX4bPvVoEpyaYuFXYQwtR
eq0co1vPmahqWUC1JHHKNkvMl3gz6Sa5WwUhEPp31QMwhovjYtZipXRj9ZVyslt1
NZI5m5gEdUDnPv07MemiOdH/b88VW4wGmEwC5XaGV88EcnbJe2fKivckv2RShVH0
o3y+fQARAQABiQE8BBgBCgAmFiEE0hD+uNGlADACm0URKHI8Oqrf9FkFAmdpBloC
GwwFCQACowAACgkQKHI8Oqrf9FnC1wgA0Zu7TBfFnsFiqkV/d9FsAsajBeTNqr/y
sVAESn2J4WZsVvXtzH4nX/y4Ih+p4GKSkrF+ZjjfIbkVb22AqarqorRMLmrJl87x
```

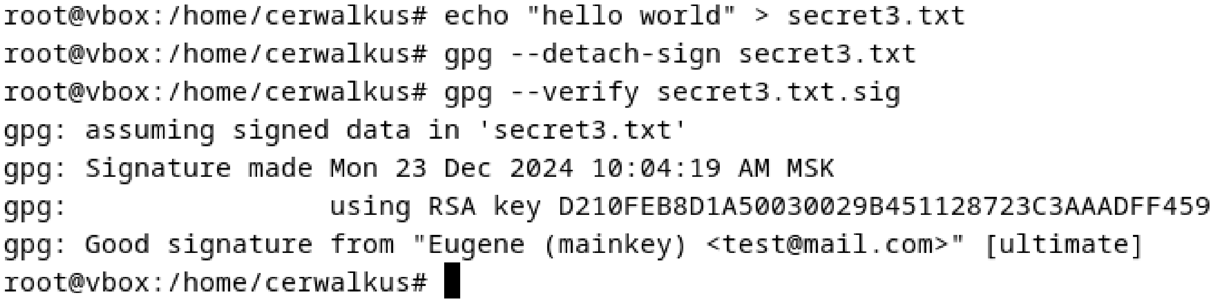
Задание 3. Настройка цифровых подписей



```
root@vbox:/home/cerwalkus# echo "Hello All" > secret-file.txt
root@vbox:/home/cerwalkus# cat secret-file.txt
Hello All
root@vbox:/home/cerwalkus# file secret-file.txt
secret-file.txt: ASCII text
root@vbox:/home/cerwalkus# gpg --sign secret-file.txt
root@vbox:/home/cerwalkus# file secret-file.txt.gpg
secret-file.txt.gpg: data
root@vbox:/home/cerwalkus# cat secret-file.txt.gpg
������Qdc ����H� �I �a �E �% �i �� ��z%% �A '=Rsr �sr � �/ �d �/.      ��q) ��WA �       �   �
                                                                              \ �� �u* ��z-x ����e2Lv
AO~Y � �7M ��t1 ����� �Z �wN �'r �i
          �_? ����� �y6 ���1 �x ���/X ��/mi ��� ��a �g: ���8 �1 �����ey* ��X �� ���T � ������Wm ��z �M ��
9> ���u} ��� ���_�y
                |��y ��Eu �5 ��!O �x}- ����7 ��yξ � ��I ���N �����EN ��9 ��Z%M ��z ���AW � ���
                                                                                        ��eyбg �r ��
���root@vbox:/home/cerwalkugpg --verify secret-file.txt.gpggpg
gpg: Signature made Mon 23 Dec 2024 10:01:29 AM MSK
gpg:                using RSA key D210FEB8D1A50030029B451128723C3AAADFF459
gpg: Good signature from "Eugene (mainkey) <test@mail.com>" [ultimate]
root@vbox:/home/cerwalkus# █
```



```
root@vbox:/home/cerwalkus# echo "Hello All" > secret2.txt
root@vbox:/home/cerwalkus# gpg --clearsign secret2.txt
root@vbox:/home/cerwalkus# cat secret2.txt.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Hello All
-----BEGIN PGP SIGNATURE-----

iQEzBAEBCgAdFiEE0hD+uNGlADACm0URKHI8Oqrf9FkFAmdpC0EACgkQKHI8Oqrf
9Fn58wf+OHW5XTAn5C59WaM2QHm6xzTlAtJ3VM+Ra2UNl1h6GJlSOc5WSAcUA2Zm
bV+2CHzjCzFT3bX2nv+uNp0X1TjY5TQPvur5w0z56R65C1tpxEI/fZkkxaBbFxZ3
pk0E6ofN/NT5gb1mlYBIgogGnRbSuaGJ8klzFzO3Cmapo/qREjfiiaTe/Dm46aPx
fbjQXfufkn02ue6WsDJhBStMBgGOLAPuKIuhjbv9UGWZ7xh1AQ2UKTg0PoaV+Mml
kRnXEqZdQk9BcFoxyTH/1yGor7Swwk6SMl+POTf3yGLuNal7TBDR6gnUub0pOsAH
Ko6dIb2eAH6G4cxCVUMn+2FHCO1ZGQ==
=GzWr
-----END PGP SIGNATURE-----
root@vbox:/home/cerwalkus# █
```



```
root@vbox:/home/cerwalkus# echo "hello world" > secret3.txt
root@vbox:/home/cerwalkus# gpg --detach-sign secret3.txt
root@vbox:/home/cerwalkus# gpg --verify secret3.txt.sig
gpg: assuming signed data in 'secret3.txt'
gpg: Signature made Mon 23 Dec 2024 10:04:19 AM MSK
gpg:                using RSA key D210FEB8D1A50030029B451128723C3AAADFF459
gpg: Good signature from "Eugene (mainkey) <test@mail.com>" [ultimate]
root@vbox:/home/cerwalkus# █
```