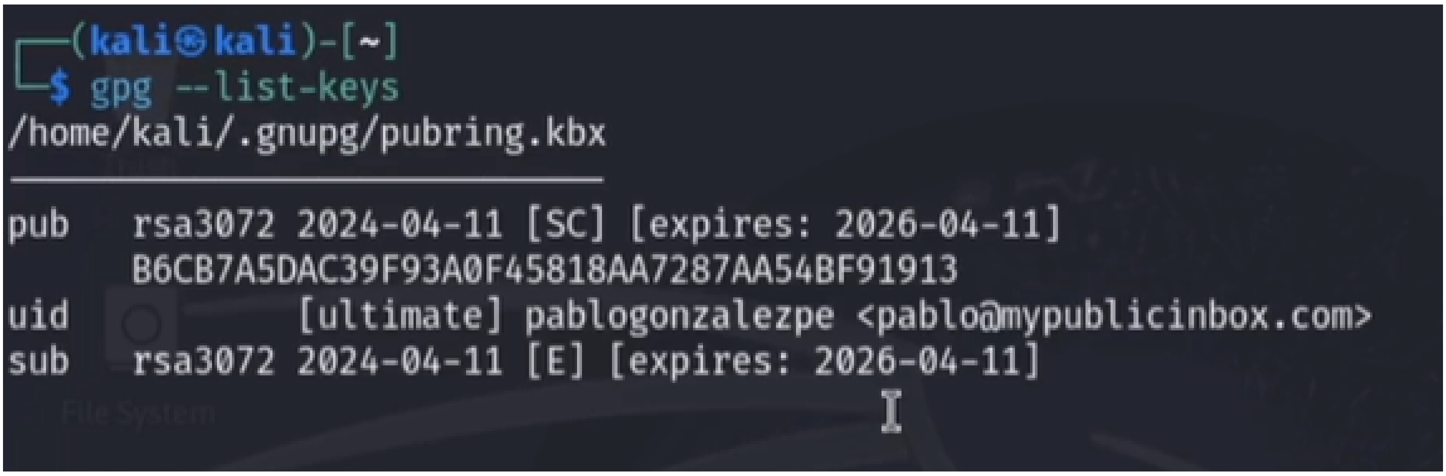
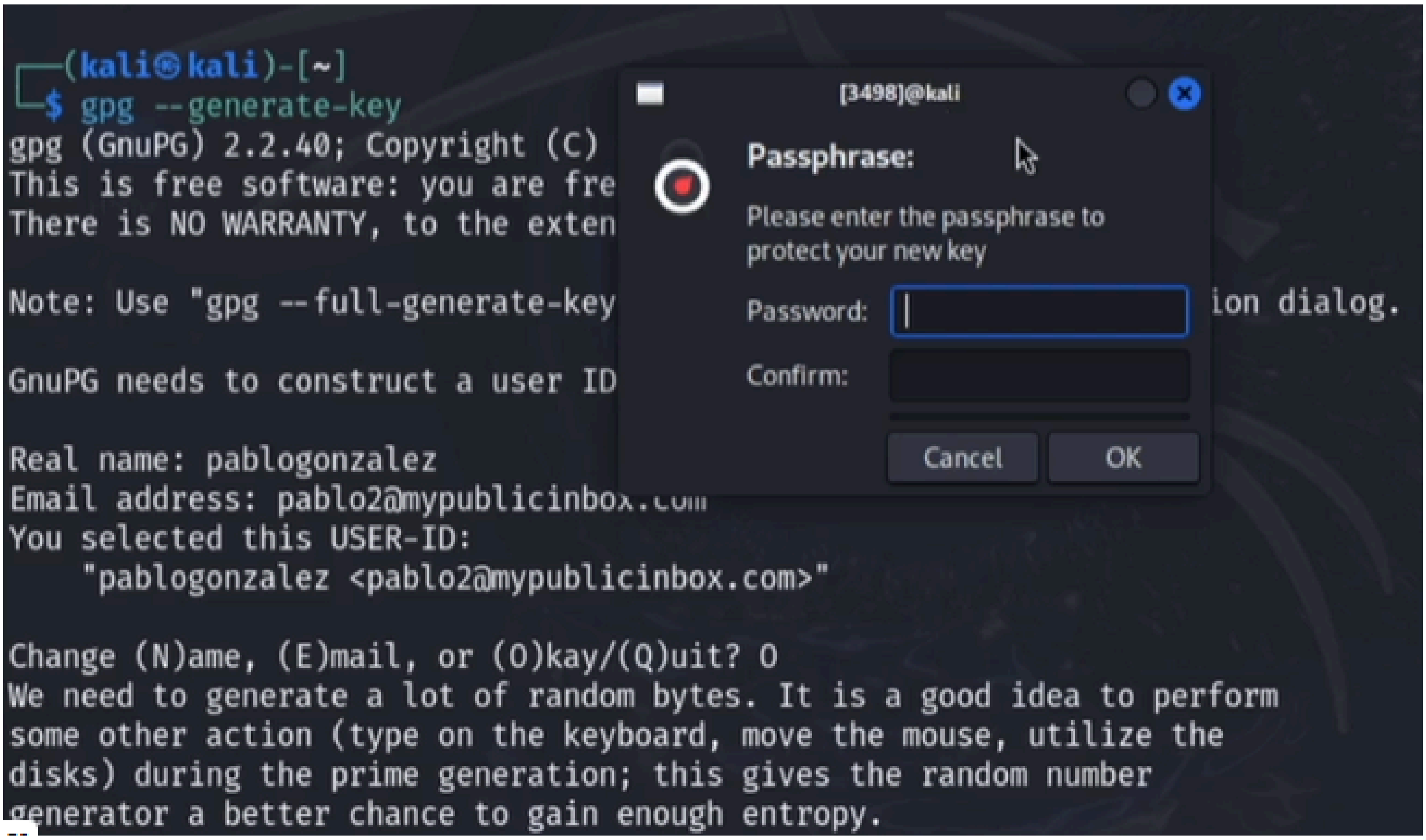
- GPG tool

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



```
┌──(kali㉿kali)-[~]
└─$ gpg --list-keys
/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]
```



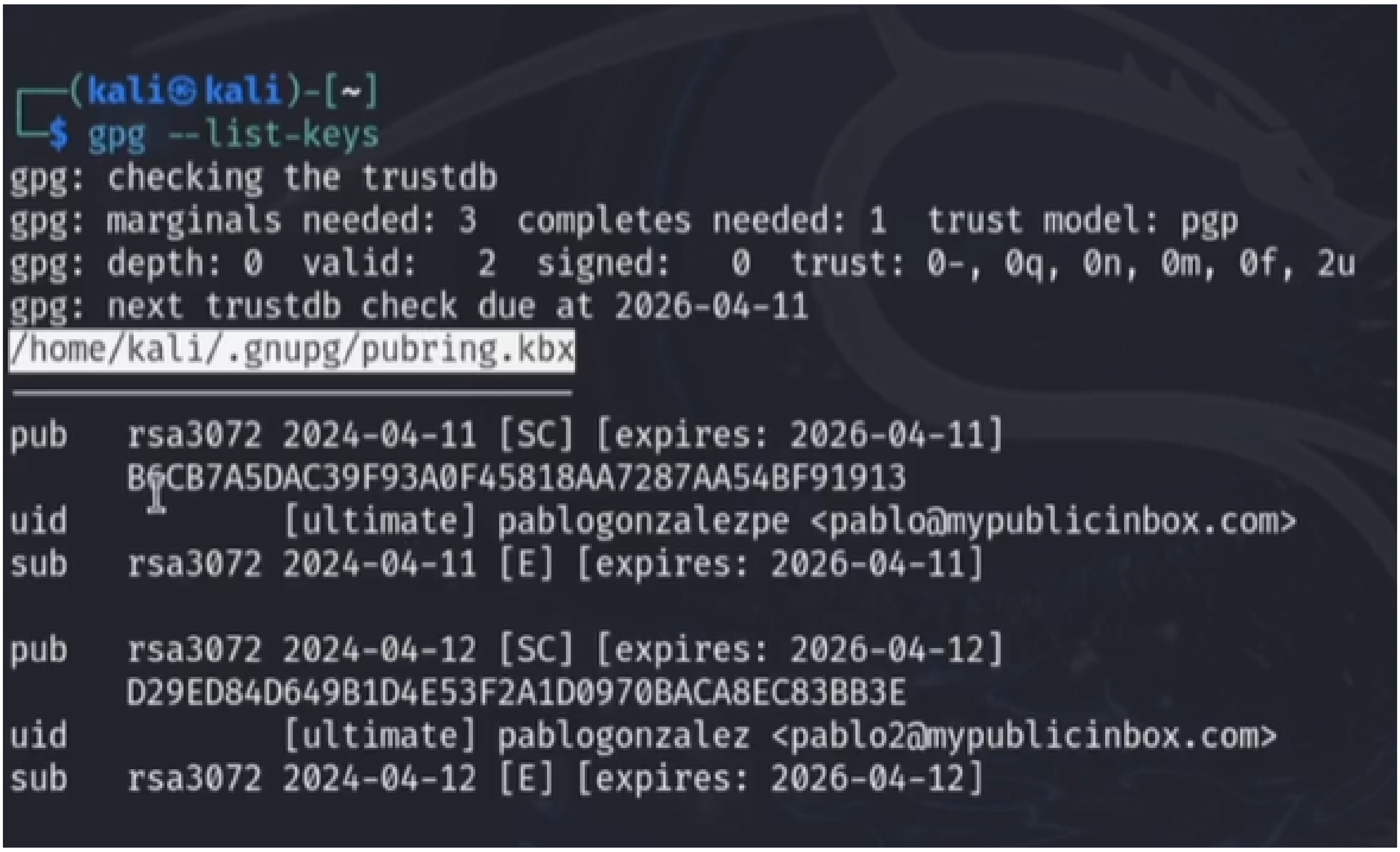
```
┌──(kali㉿kali)-[~]
└─$ gpg --generate-key
gpg (GnuPG) 2.2.40; Copyright (C)
This is free software: you are fre
There is NO WARRANTY, to the exten

Note: Use "gpg --full-generate-key                                ion dialog.

GnuPG needs to construct a user ID

Real name: pablogonzalez
Email address: pablo2@mypublicinbox.com
You selected this USER-ID:
    "pablogonzalez <pablo2@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.
```

Passphrase:

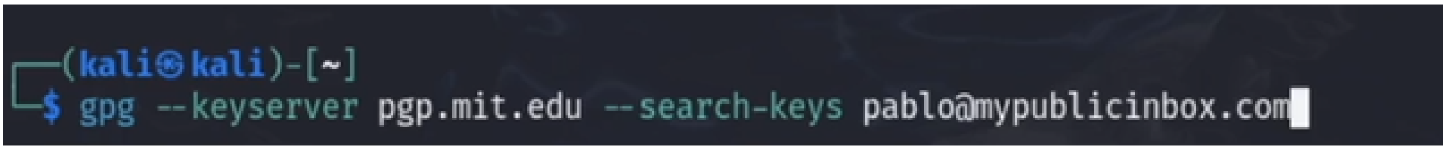
Please enter the passphrase to protect your new key

Password:

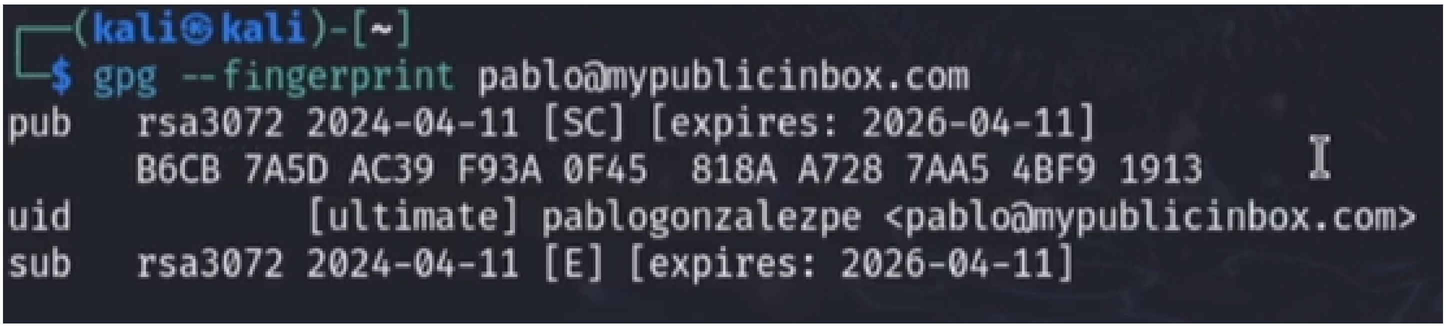
Confirm:



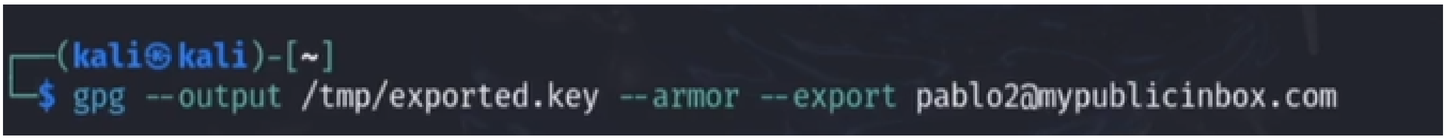
```
┌──(kali㉿kali)-[~]
└─$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2026-04-11
/home/kali/.gnupg/pubring.kbx
─────────────────────────────
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]

pub   rsa3072 2024-04-12 [SC] [expires: 2026-04-12]
      D29ED84D649B1D4E53F2A1D0970BACA8EC83BB3E
uid           [ultimate] pablogonzalez <pablo2@mypublicinbox.com>
sub   rsa3072 2024-04-12 [E] [expires: 2026-04-12]
```



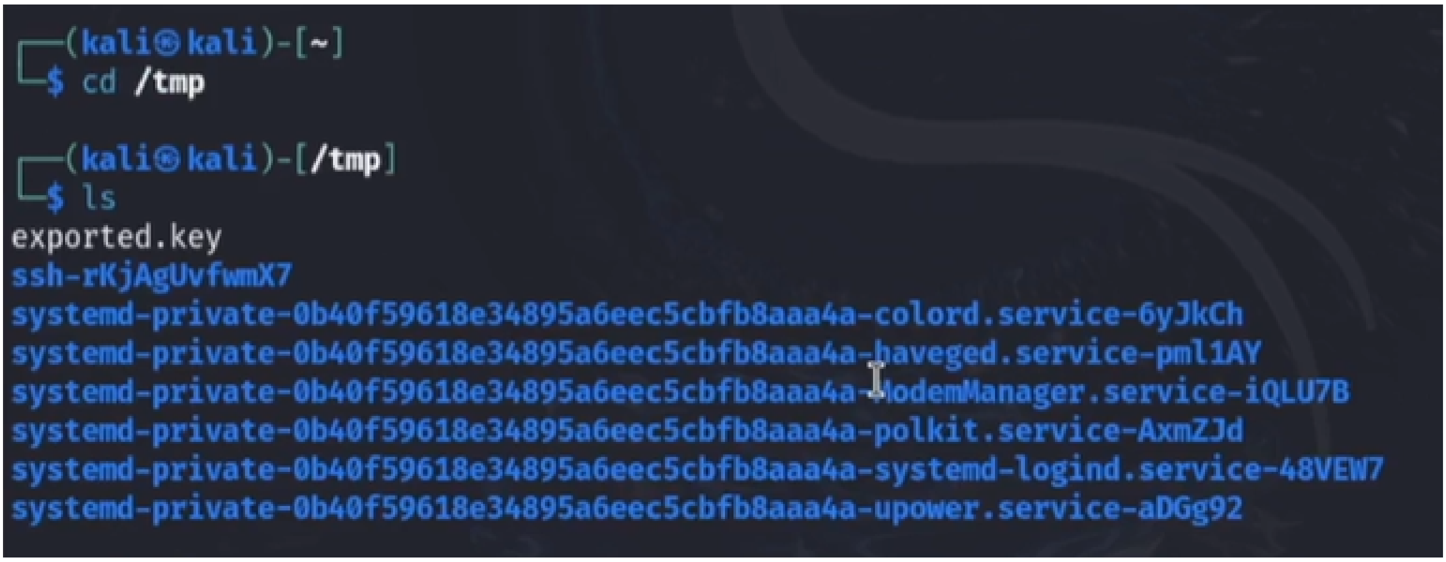
```
┌──(kali㉿kali)-[~]
└─$ gpg --keyserver pgp.mit.edu --search-keys pablo@mypublicinbox.com
```



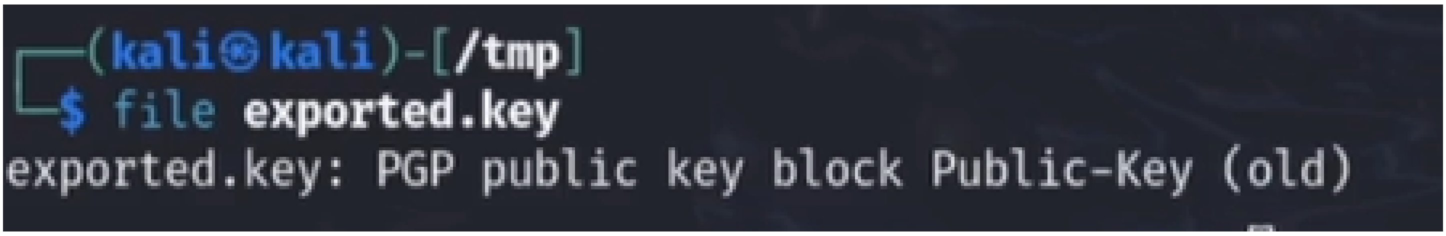
```
┌──(kali㉿kali)-[~]
└─$ gpg --fingerprint pablo@mypublicinbox.com
pub   rsa3072 2024-04-11 [SC] [expires: 2026-04-11]
      B6CB 7A5D AC39 F93A 0F45  818A A728 7AA5 4BF9 1913
uid           [ultimate] pablogonzalezpe <pablo@mypublicinbox.com>
sub   rsa3072 2024-04-11 [E] [expires: 2026-04-11]
```



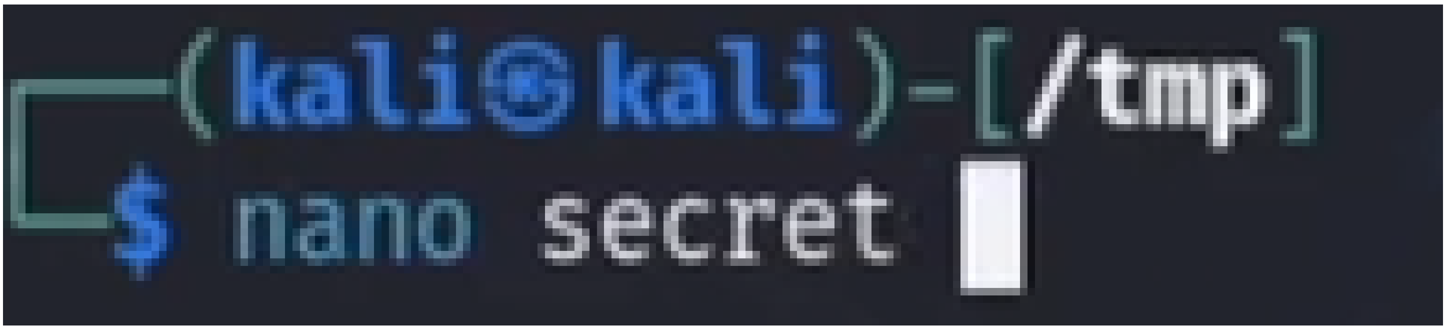
```
┌──(kali㉿kali)-[~]
└─$ gpg --output /tmp/exported.key --armor --export pablo2@mypublicinbox.com
```



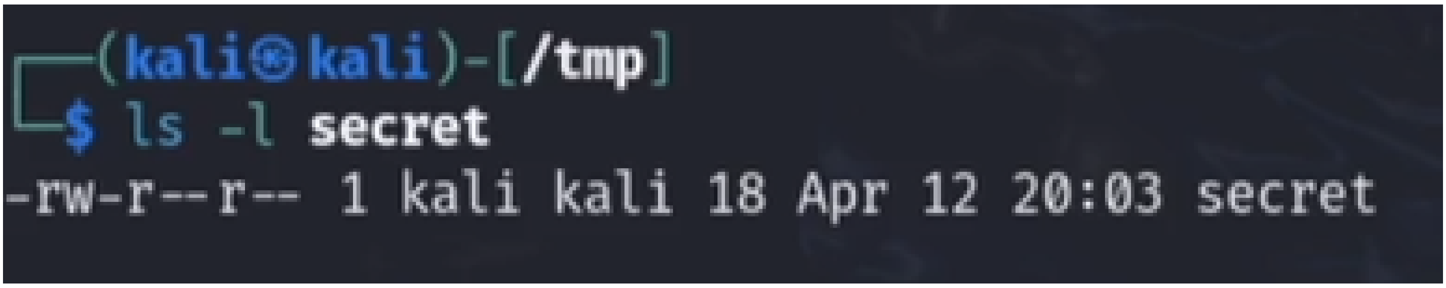
```
┌──(kali㉿kali)-[~]
└─$ cd /tmp

┌──(kali㉿kali)-[/tmp]
└─$ ls
exported.key
ssh-rKjAgUvfwmX7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-colord.service-6yJkCh
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-haveged.service-pml1AY
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-ModemManager.service-iQLU7B
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-polkit.service-AxmZJd
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-systemd-logind.service-48VEW7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-upower.service-aDGg92
```



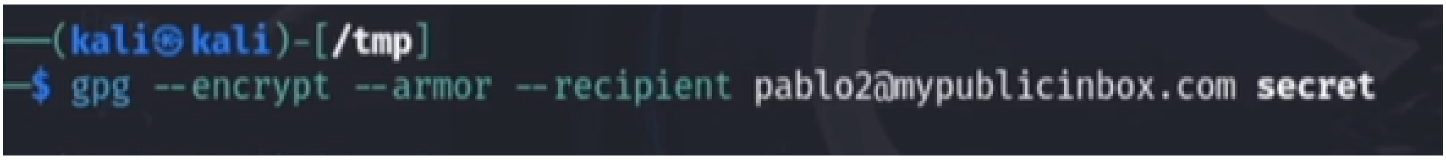
```
┌──(kali㉿kali)-[/tmp]
└─$ file exported.key
exported.key: PGP public key block Public-Key (old)
```



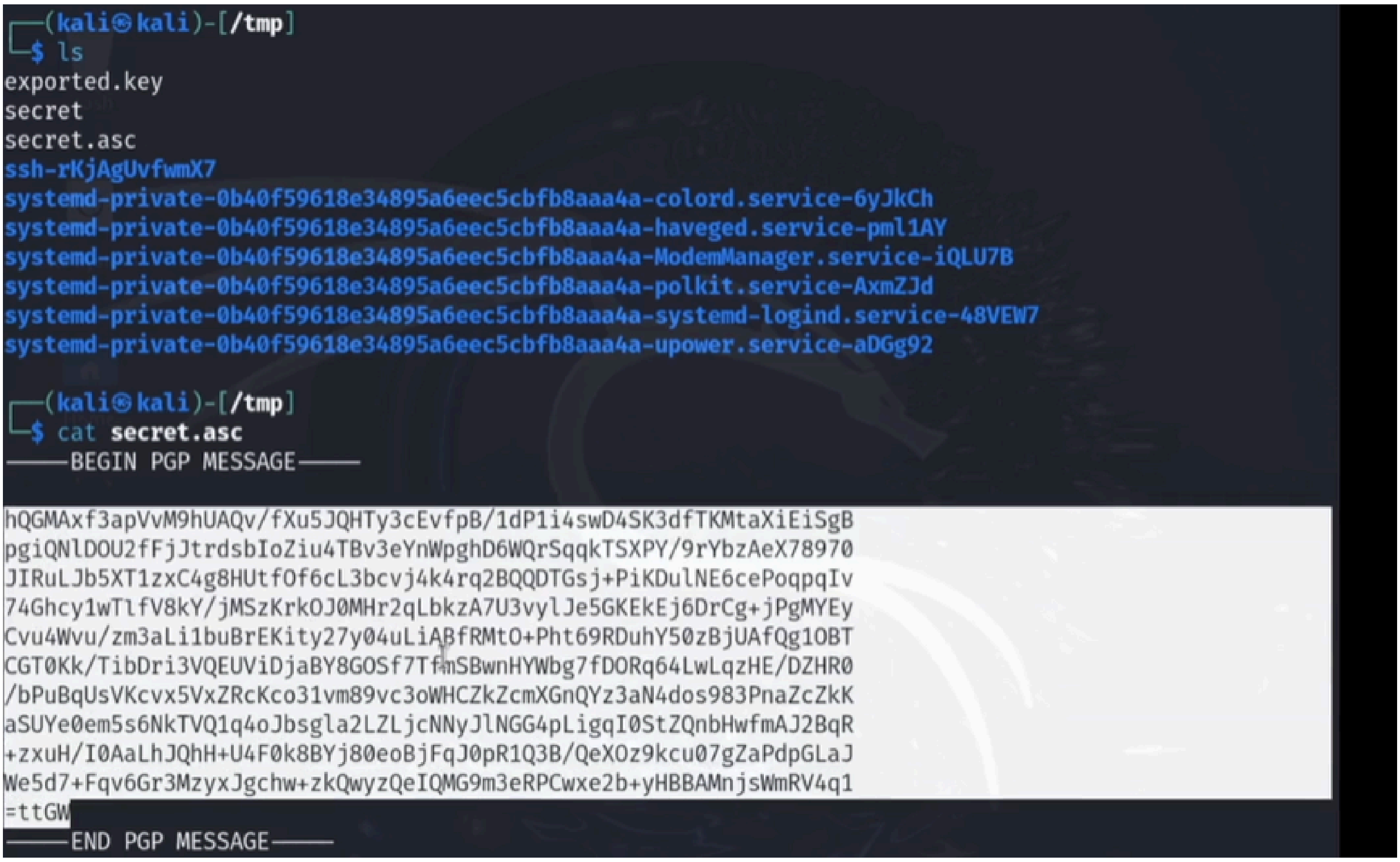
```
┌──(kali㉿kali)-[/tmp]
└─$ nano secret
```



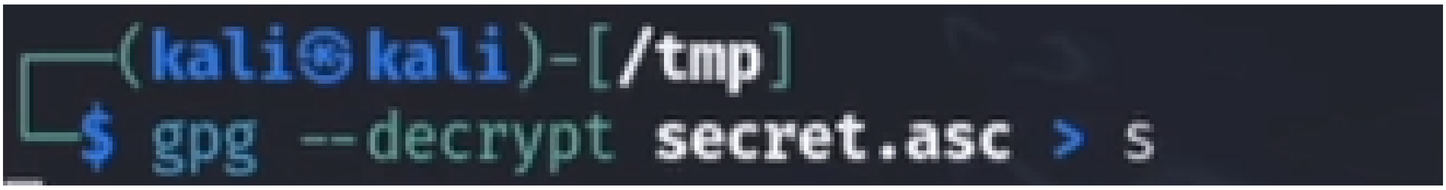
```
┌──(kali㉿kali)-[/tmp]
└─$ ls -l secret
-rw-r--r-- 1 kali kali 18 Apr 12 20:03 secret
```



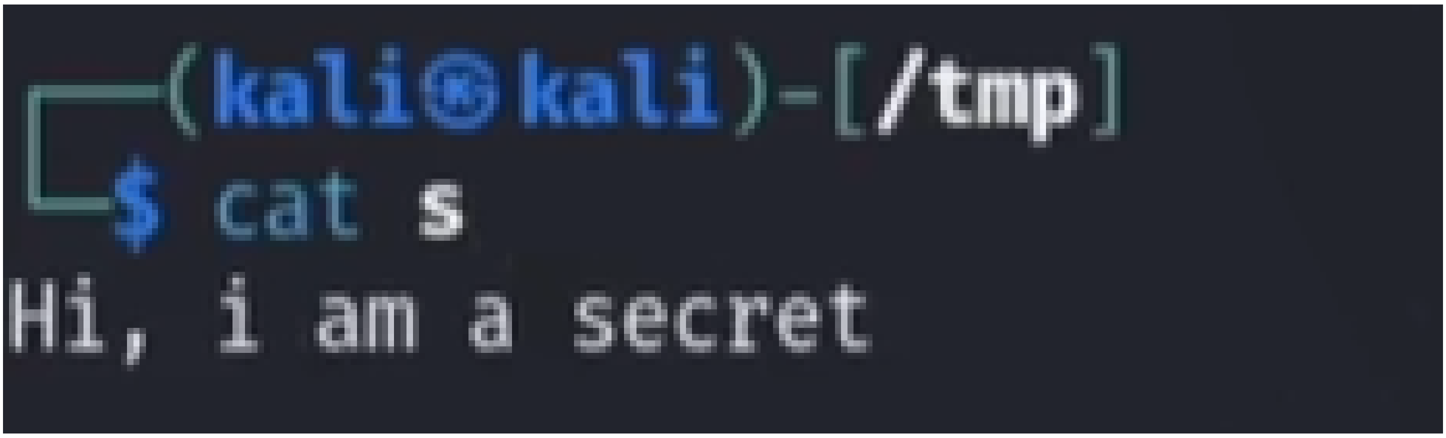
```
──(kali㉿kali)-[/tmp]
─$ gpg --encrypt --armor --recipient pablo2@mypublicinbox.com secret
```



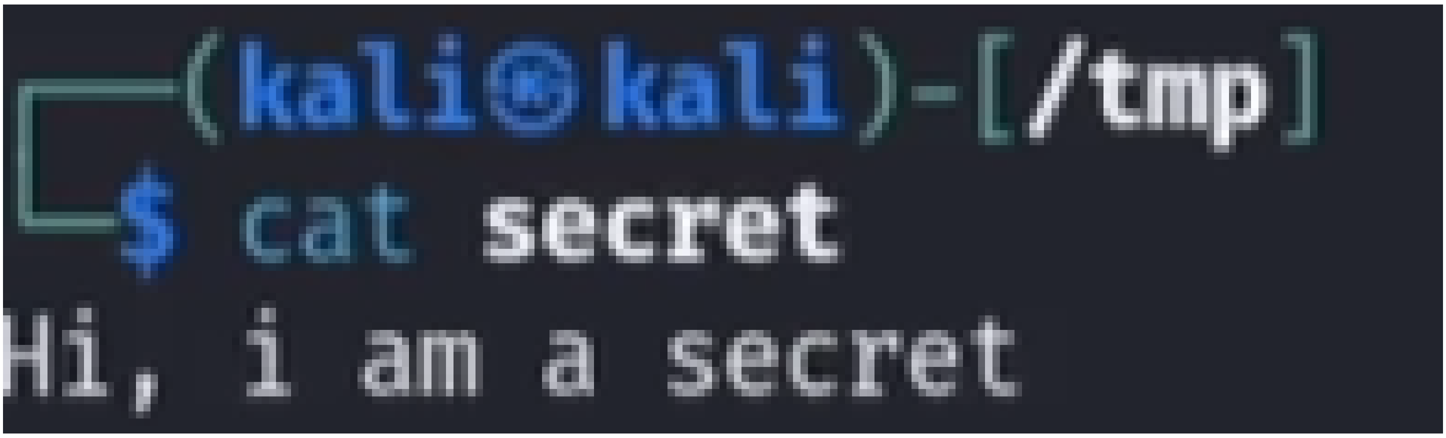
```
┌──(kali㉿kali)-[/tmp]
└─$ ls
exported.key
secret
secret.asc
ssh-rKjAgUvfwmX7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-colord.service-6yJkCh
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-haveged.service-pml1AY
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-ModemManager.service-iQLU7B
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-polkit.service-AxmZJd
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-systemd-logind.service-48VEW7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-upower.service-aDGg92

┌──(kali㉿kali)-[/tmp]
└─$ cat secret.asc
-----BEGIN PGP MESSAGE-----

hQGMAxf3apVvM9hUAQv/fXu5JQHTy3cEvfpB/1dP1i4swD4SK3dfTKMtaXiEiSgB
pgiQNlDOU2fFjJtrdsbIoZiu4TBv3eYnWpghD6WQrSqqkTSXPY/9rYbzAeX78970
JIRuLJb5XT1zxC4g8HUtfOf6cL3bcvj4k4rq2BQQDTGsj+PiKDulNE6cePoqpqIv
74Ghcy1wTlfV8kY/jMSzKrkOJ0MHr2qLbkzA7U3vylJe5GKEkEj6DrCg+jPgMYEy
Cvu4Wvu/zm3aLi1buBrEKity27y04uLiABfRMtO+Pht69RDuhY50zBjUAfQg1OBT
CGT0Kk/TibDri3VQEUViDjaBY8GOSf7TfmSBwnHYWbg7fDORq64LwLqzHE/DZHR0
/bPuBqUsVKcvx5VxZRcKco31vm89vc3oWHCZkZcmXGnQYz3aN4dos983PnaZcZkK
aSUYe0em5s6NkTVQ1q4oJbsgla2LZLjcNNyJlNGG4pLigqI0StZQnbHwfmAJ2BqR
+zxuH/I0AaLhJQhH+U4F0k8BYj80eoBjFqJ0pR1Q3B/QeXOz9kcu07gZaPdpGLaJ
We5d7+Fqv6Gr3MzyxJgchw+zkQwyzQeIQMG9m3eRPCwxe2b+yHBBAMnjsWmRV4q1
=ttGW
-----END PGP MESSAGE-----
```



```
┌──(kali㉿kali)-[/tmp]
└─$ gpg --decrypt secret.asc > s
```

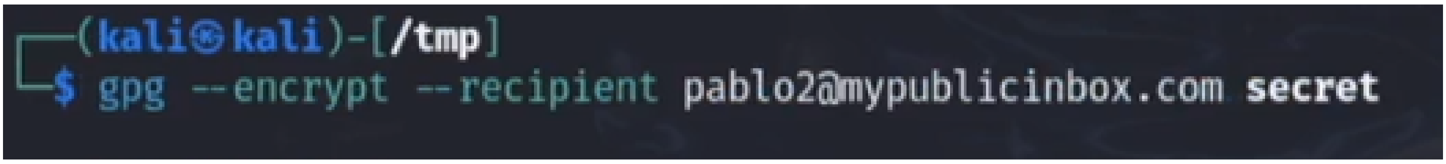


```
┌──(kali㉿kali)-[/tmp]
└─$ cat s
Hi, i am a secret
```

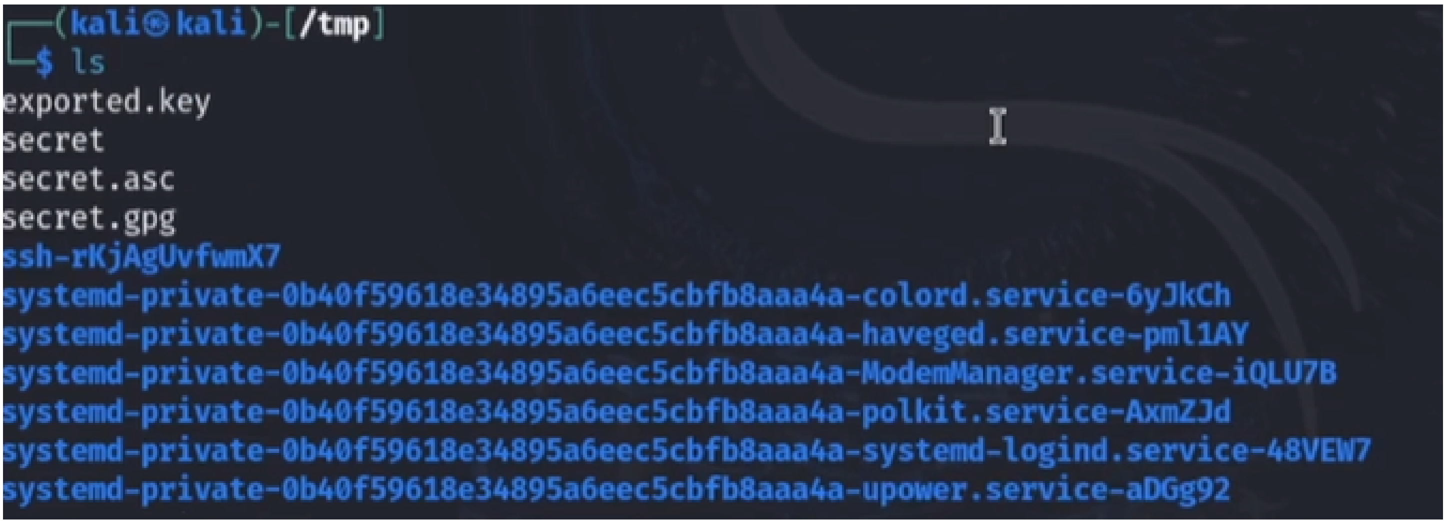


```
┌──(kali㉿kali)-[/tmp]
└─$ cat secret
Hi, i am a secret
```

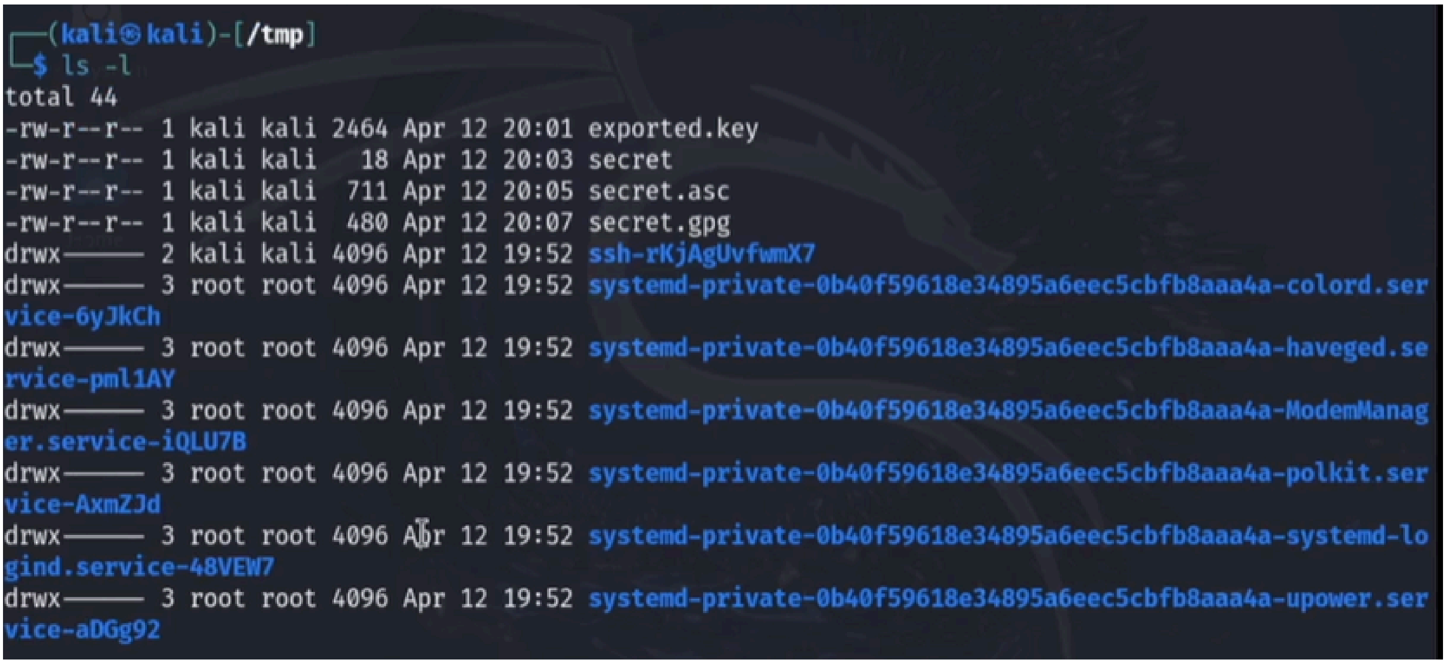
Diferente manera sin --armor:



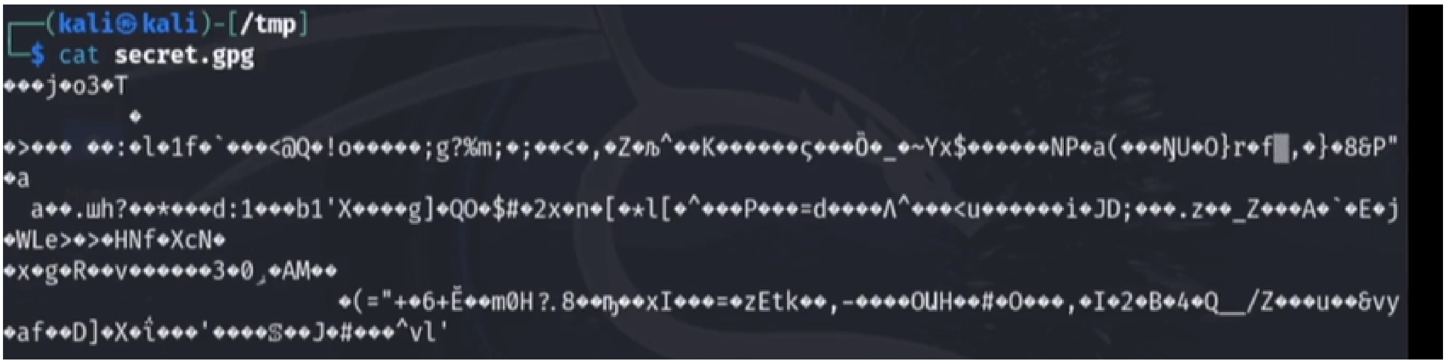
```
┌──(kali㉿kali)-[/tmp]
└─$ gpg --encrypt --recipient pablo2@mypublicinbox.com secret
```



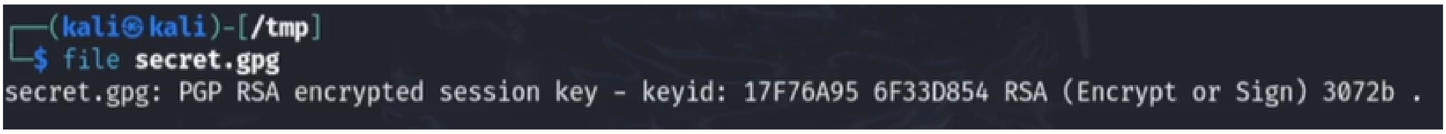
```
┌──(kali㉿kali)-[/tmp]
└─$ ls
exported.key
secret
secret.asc
secret.gpg
ssh-rKjAgUvfwmX7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-colord.service-6yJkCh
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-haveged.service-pml1AY
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-ModemManager.service-iQLU7B
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-polkit.service-AxmZJd
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-systemd-logind.service-48VEW7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-upower.service-aDGg92
```



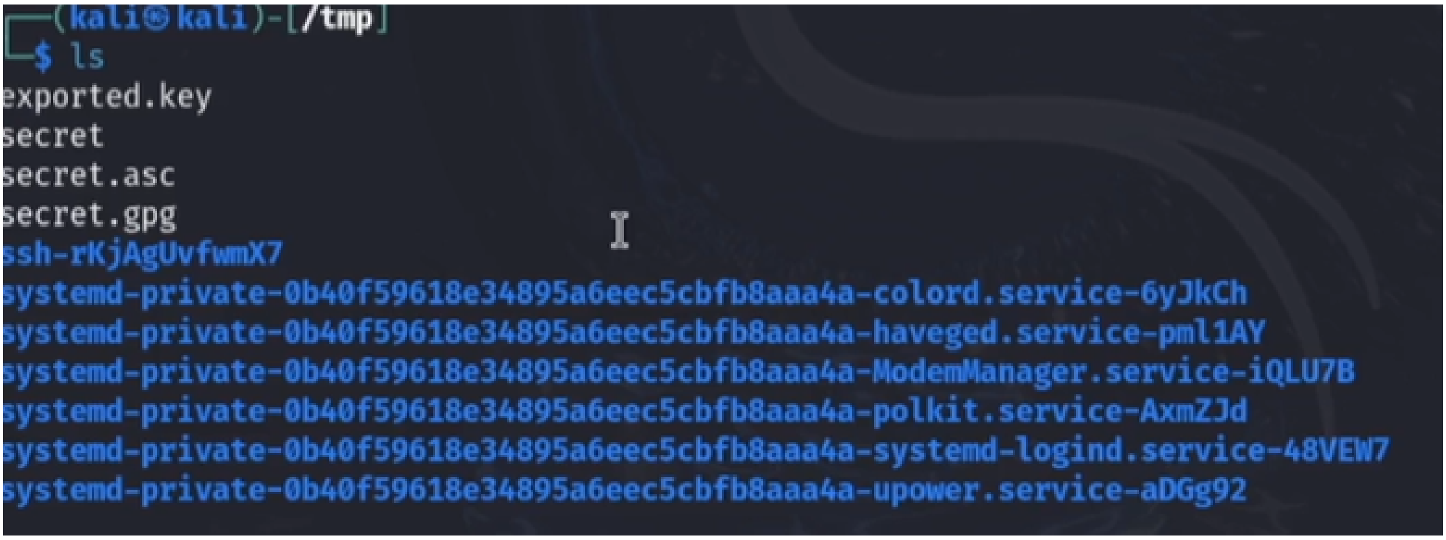
```
┌──(kali㉿kali)-[/tmp]
└─$ ls -l
total 44
-rw-r--r-- 1 kali kali 2464 Apr 12 20:01 exported.key
-rw-r--r-- 1 kali kali   18 Apr 12 20:03 secret
-rw-r--r-- 1 kali kali  711 Apr 12 20:05 secret.asc
-rw-r--r-- 1 kali kali  480 Apr 12 20:07 secret.gpg
drwx------ 2 kali kali 4096 Apr 12 19:52 ssh-rKjAgUvfwmX7
drwx------ 3 root root 4096 Apr 12 19:52 systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-colord.ser
vice-6yJkCh
drwx------ 3 root root 4096 Apr 12 19:52 systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-haveged.se
rvice-pml1AY
drwx------ 3 root root 4096 Apr 12 19:52 systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-ModemManag
er.service-iQLU7B
drwx------ 3 root root 4096 Apr 12 19:52 systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-polkit.ser
vice-AxmZJd
drwx------ 3 root root 4096 Apr 12 19:52 systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-systemd-lo
gind.service-48VEW7
drwx------ 3 root root 4096 Apr 12 19:52 systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-upower.ser
vice-aDGg92
```



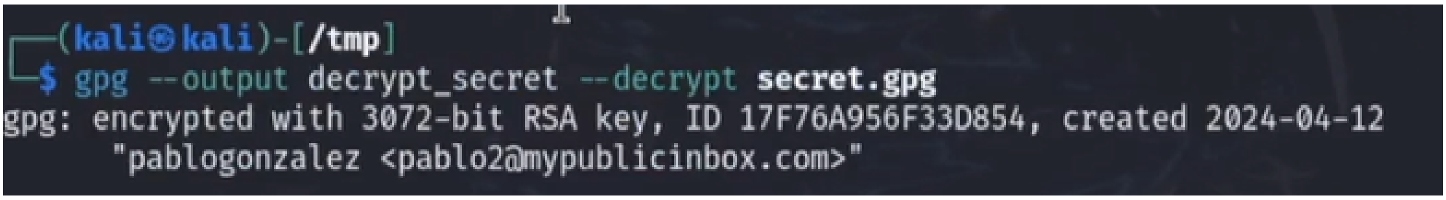
```
┌──(kali㉿kali)-[/tmp]
└─$ cat secret.gpg
◆◆◆j◆o3◆T
        ◆
◆>◆◆◆ ◆◆:◆l◆1f◆`◆◆◆<@Q◆!o◆◆◆◆◆;g?%m;◆;◆◆<◆,◆Z◆ҕ^◆◆K◆◆◆◆◆◆ς◆◆◆Ö◆_◆~Yx$◆◆◆◆◆◆NP◆a(◆◆◆ŊU◆O}r◆f█,◆}◆8&P"
◆a
  a◆◆.wh?◆◆*◆◆◆d:1◆◆◆b1'X◆◆◆◆g]◆QO◆$#◆2x◆n◆[◆*l[◆^◆◆◆P◆◆◆=d◆◆◆◆Λ^◆◆◆<u◆◆◆◆◆◆◆i◆JD;◆◆◆.z◆◆_Z◆◆◆A◆`◆E◆j
◆WLe>◆>◆HNf◆XcN◆
◆x◆g◆R◆◆v◆◆◆◆◆◆◆3◆0¸◆AM◆◆
                        ◆(="+◆6+Ĕ◆◆m0H?.8◆◆ŋ◆◆xI◆◆◆=◆zEtk◆◆,-◆◆◆◆OUH◆◆#◆O◆◆◆,◆I◆2◆B◆4◆Q__/Z◆◆◆u◆◆&vy
◆af◆◆D]◆X◆î◆◆◆'◆◆◆◆S◆◆J◆#◆◆◆^vl'
```



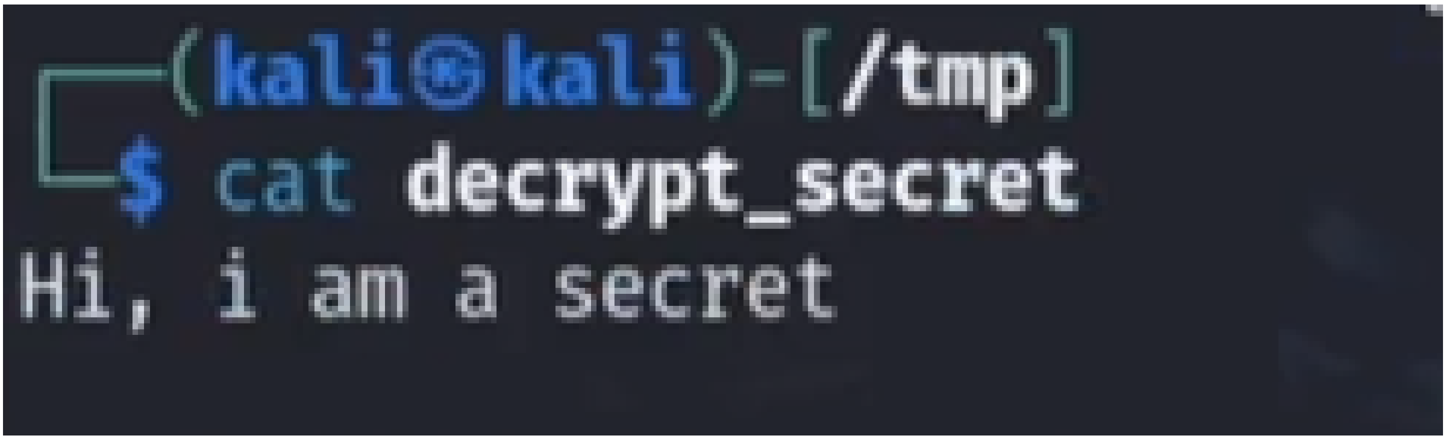
```
┌──(kali㉿kali)-[/tmp]
└─$ file secret.gpg
secret.gpg: PGP RSA encrypted session key - keyid: 17F76A95 6F33D854 RSA (Encrypt or Sign) 3072b .
```



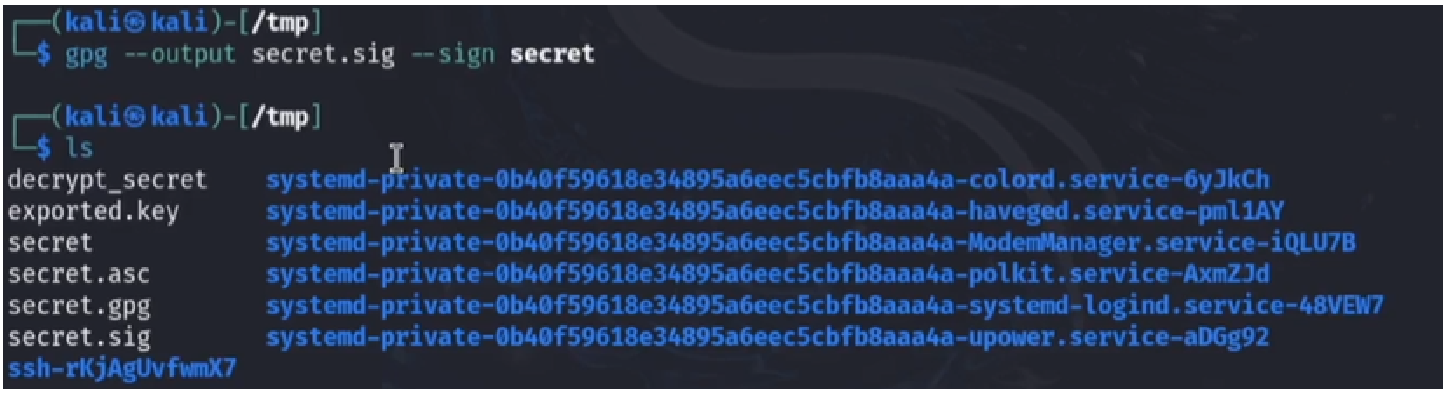
```
┌──(kali㉿kali)-[/tmp]
└─$ ls
exported.key
secret
secret.asc
secret.gpg
ssh-rKjAgUvfwmX7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-colord.service-6yJkCh
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-haveged.service-pml1AY
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-ModemManager.service-iQLU7B
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-polkit.service-AxmZJd
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-systemd-logind.service-48VEW7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-upower.service-aDGg92
```



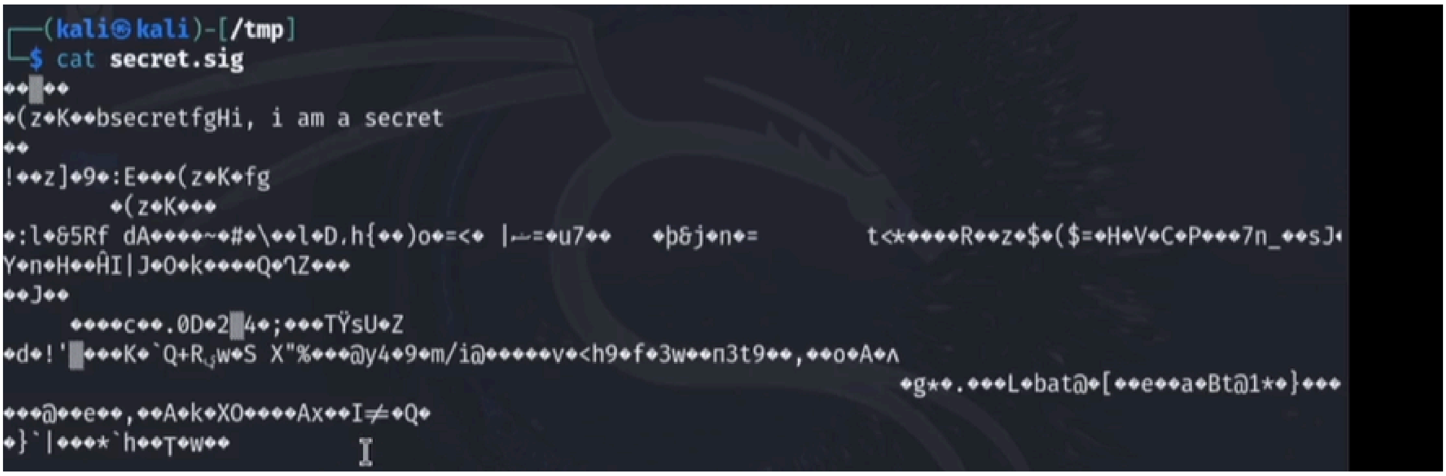
```
┌──(kali㉿kali)-[/tmp]
└─$ gpg --output decrypt_secret --decrypt secret.gpg
gpg: encrypted with 3072-bit RSA key, ID 17F76A956F33D854, created 2024-04-12
      "pablogonzalez <pablo2@mypublicinbox.com>"
```



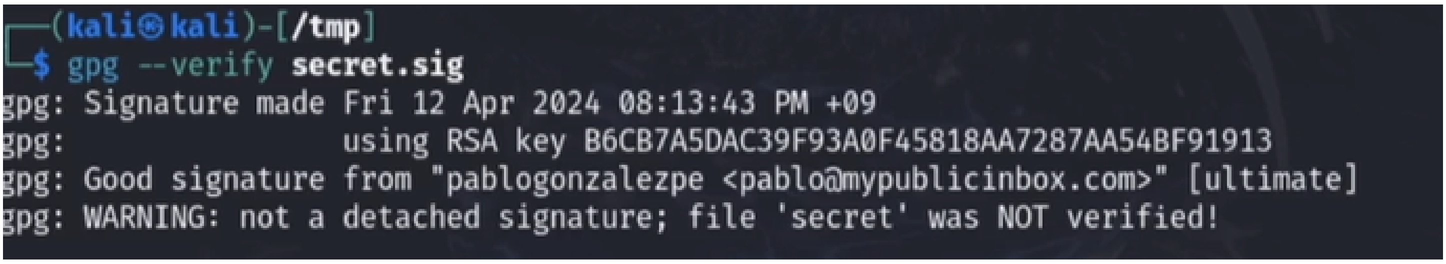
```
┌──(kali㉿kali)-[/tmp]
└─$ cat decrypt_secret
Hi, i am a secret
```



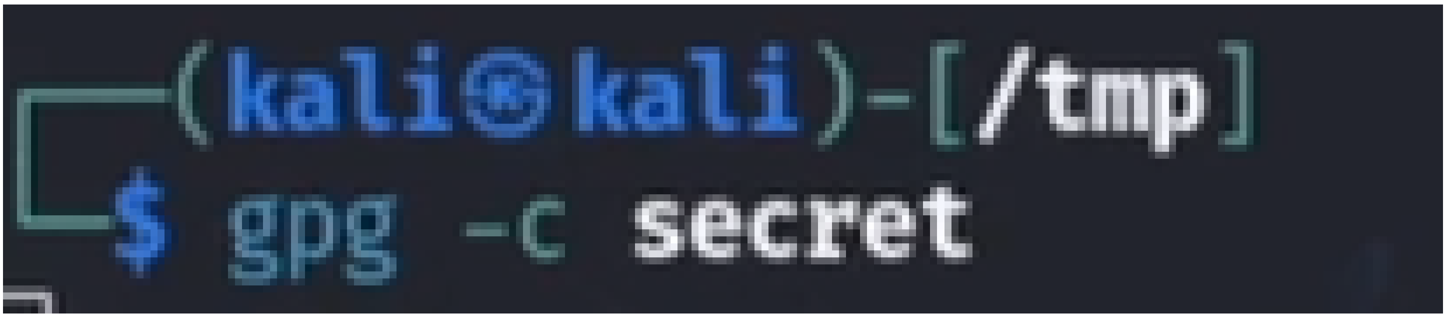
```
┌──(kali㉿kali)-[/tmp]
└─$ gpg --output secret.sig --sign secret

┌──(kali㉿kali)-[/tmp]
└─$ ls
decrypt_secret    systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-colord.service-6yJkCh
exported.key      systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-haveged.service-pml1AY
secret            systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-ModemManager.service-iQLU7B
secret.asc        systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-polkit.service-AxmZJd
secret.gpg        systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-systemd-logind.service-48VEW7
secret.sig        systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-upower.service-aDGg92
ssh-rKjAgUvfwmX7
```



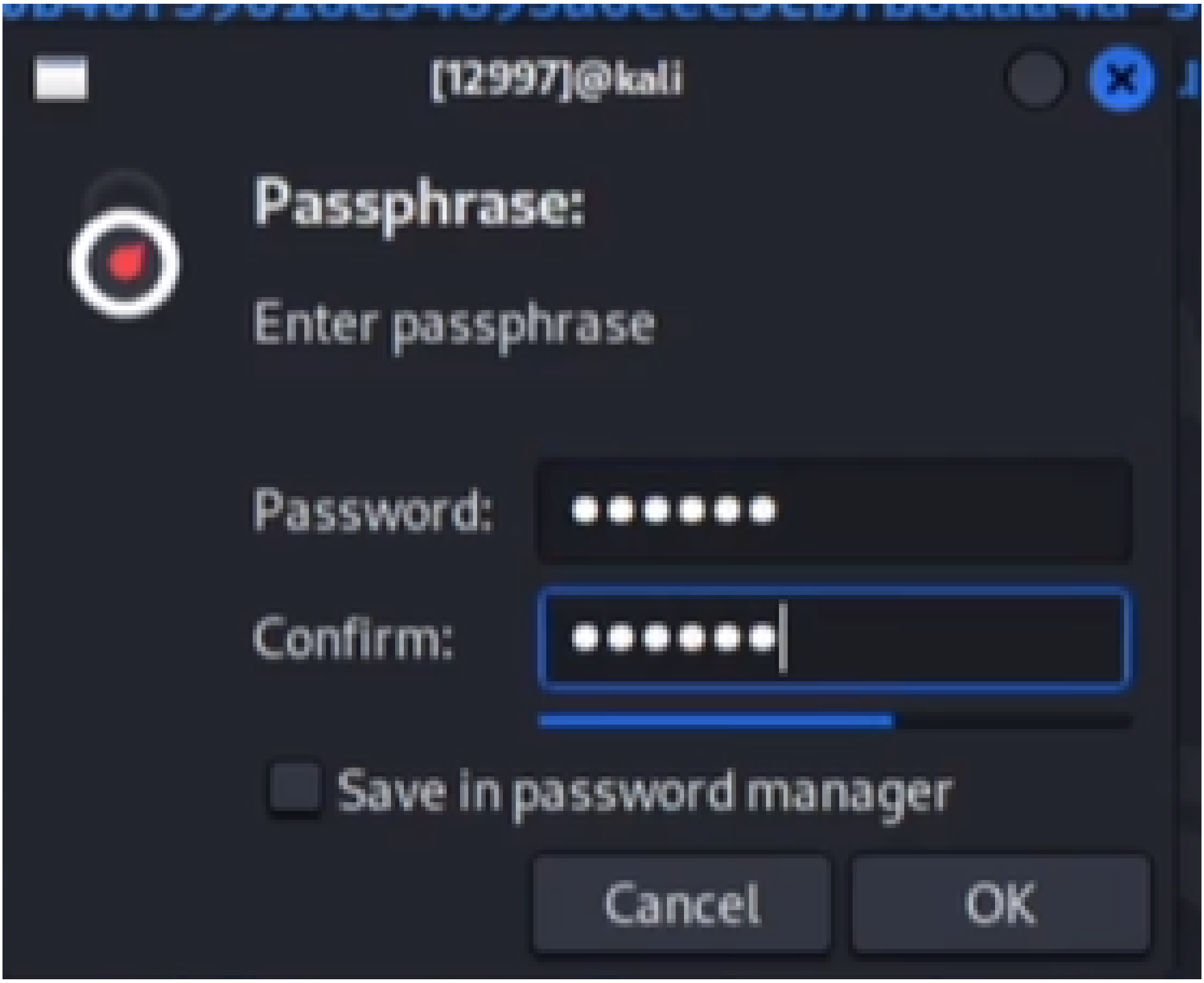
```
┌──(kali㉿kali)-[/tmp]
└─$ cat secret.sig
��█��
�(z�K��bsecretfgHi, i am a secret
��
!��z]�9�:E���(z�K�fg
        �(z�K���
�:l�&5Rf dA����~�#�\��l�D.h{��)o�=<� |⎵=�u7��   �þ&j�n�=        t<*����R��z�$�($=�H�V�C�P���7n_��sJ�
Y�n�H��ÂI|J�O�k����Q�ˀZ���
��J��
     ����c��.0D�2█4�;���TŸsU�Z
�d�!'█���K�`Q+R꜖w�S X"%���@y4�9�m/i@�����v�<h9�f�3w��п3t9��,��o�A�ʌ
                                                                        �g*�.���L�bat@�[��e���a�Bt@1*�}���
���@��e��,��A�k�XO����Ax��I≠�Q�
�}`|���*`h��ᴛ�w��
```



```
┌──(kali㉿kali)-[/tmp]
└─$ gpg --verify secret.sig
gpg: Signature made Fri 12 Apr 2024 08:13:43 PM +09
gpg:                using RSA key B6CB7A5DAC39F93A0F45818AA7287AA54BF91913
gpg: Good signature from "pablogonzalezpe <pablo@mypublicinbox.com>" [ultimate]
gpg: WARNING: not a detached signature; file 'secret' was NOT verified!
```



```
┌──(kali㉿kali)-[/tmp]
└─$ gpg -c secret
```



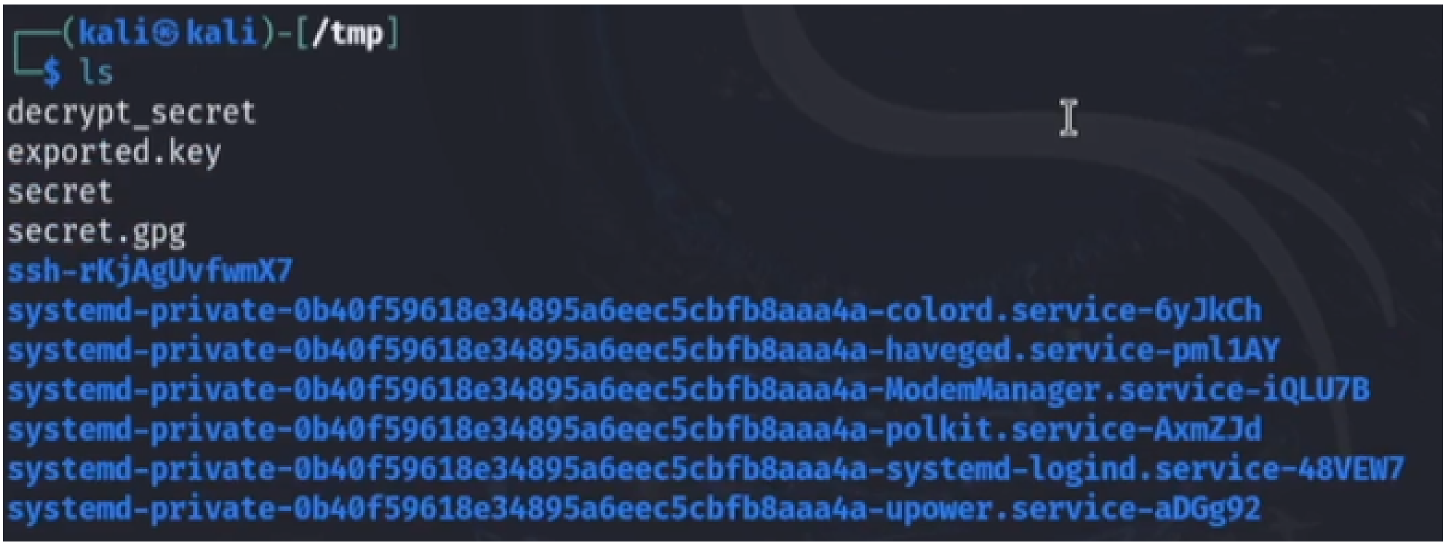
Passphrase:

Enter passphrase

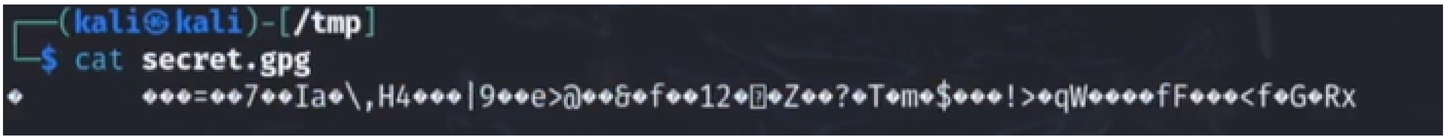
Password: ●●●●●●

Confirm: ●●●●●●

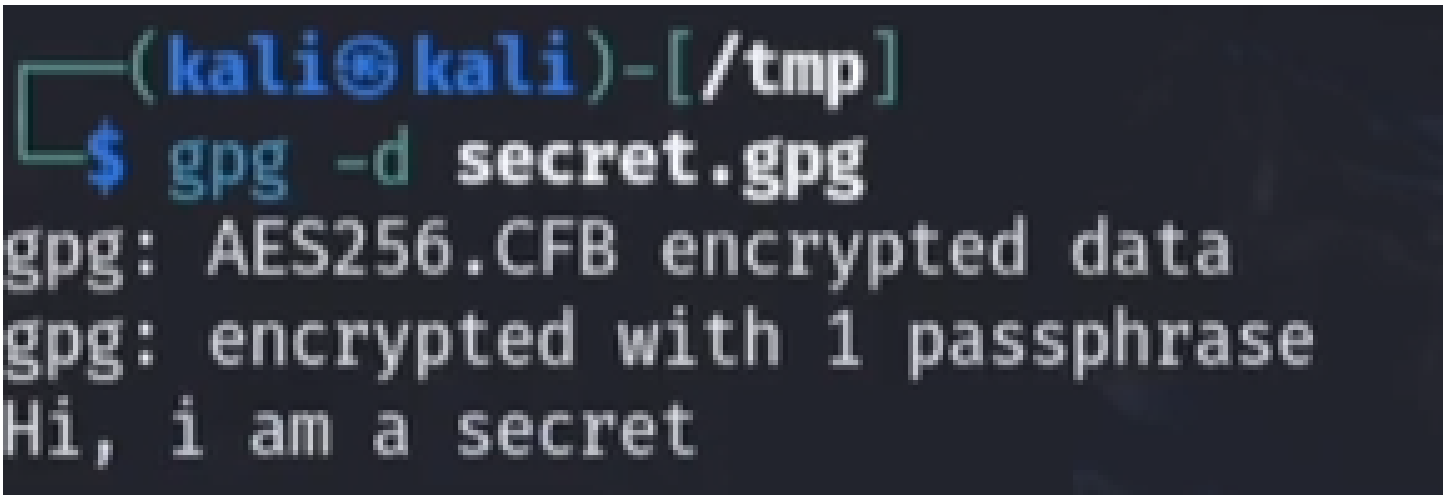
□ Save in password manager



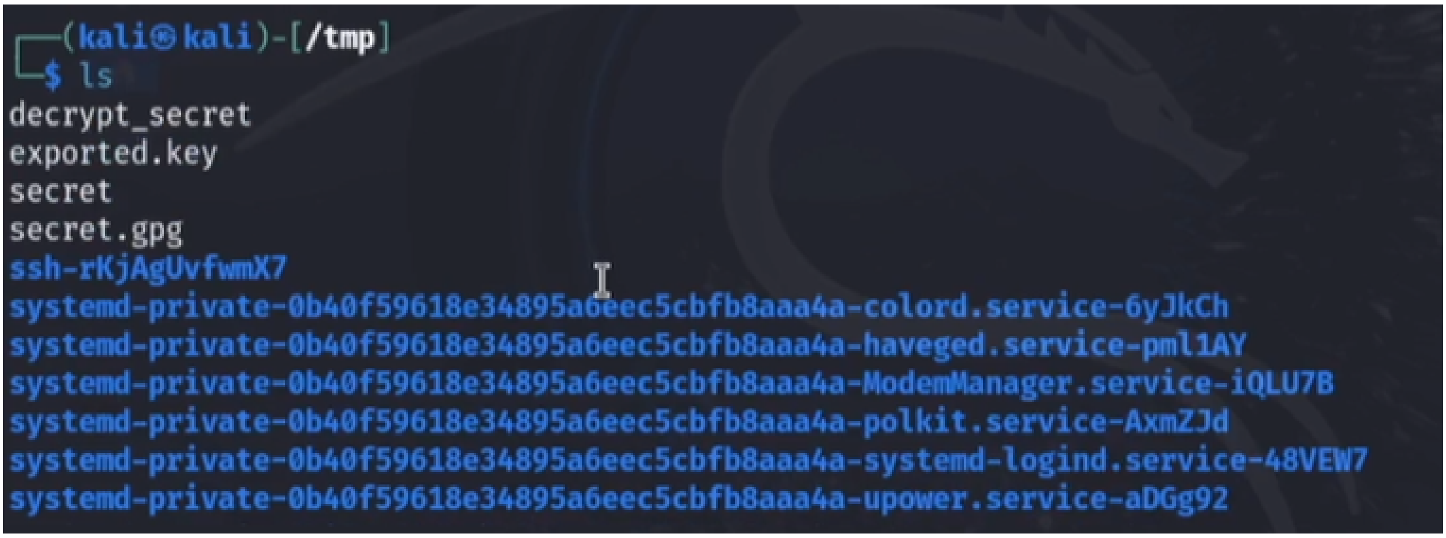
```
┌──(kali㉿kali)-[/tmp]
└─$ ls
decrypt_secret
exported.key
secret
secret.gpg
ssh-rKjAgUvfwmX7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-colord.service-6yJkCh
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-haveged.service-pml1AY
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-ModemManager.service-iQLU7B
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-polkit.service-AxmZJd
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-systemd-logind.service-48VEW7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-upower.service-aDGg92
```



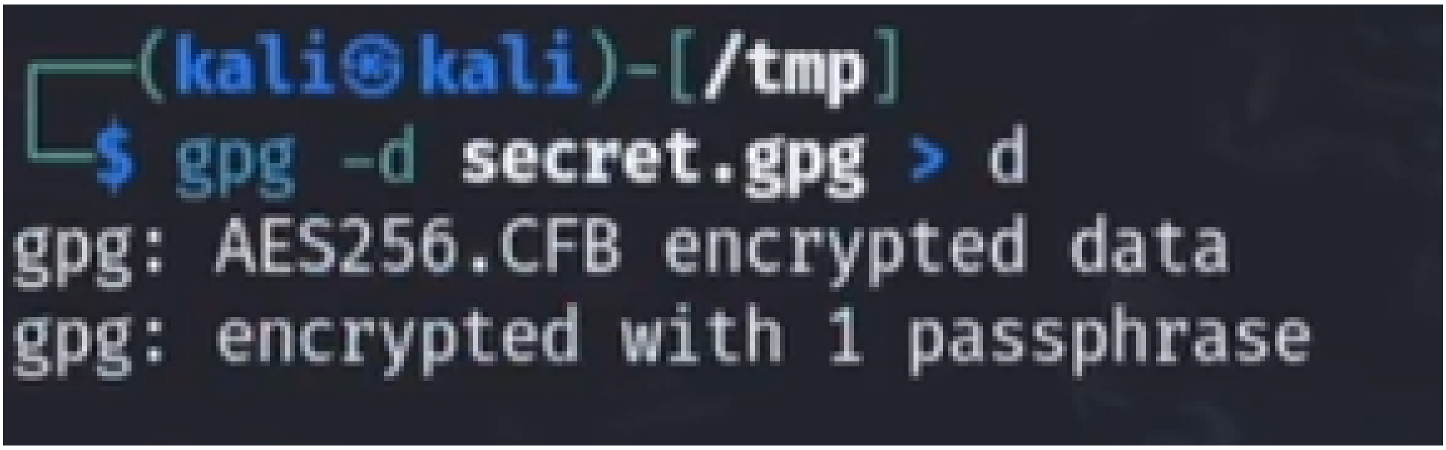
```
┌──(kali㉿kali)-[/tmp]
└─$ cat secret.gpg
◆       ◆◆◆=◆◆7◆◆Ia◆\,H4◆◆◆|9◆◆e>@◆◆&◆f◆◆12◆⍰◆Z◆◆?◆T◆m◆$◆◆◆!>◆qW◆◆◆◆fF◆◆◆<f◆G◆Rx
```



```
┌──(kali㉿kali)-[/tmp]
└─$ gpg -d secret.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
Hi, i am a secret
```



```
┌──(kali㉿kali)-[/tmp]
└─$ ls
decrypt_secret
exported.key
secret
secret.gpg
ssh-rKjAgUvfwmX7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-colord.service-6yJkCh
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-haveged.service-pml1AY
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-ModemManager.service-iQLU7B
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-polkit.service-AxmZJd
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-systemd-logind.service-48VEW7
systemd-private-0b40f59618e34895a6eec5cbfb8aaa4a-upower.service-aDGg92
```



```
┌──(kali㉿kali)-[/tmp]
└─$ gpg -d secret.gpg > d
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
```