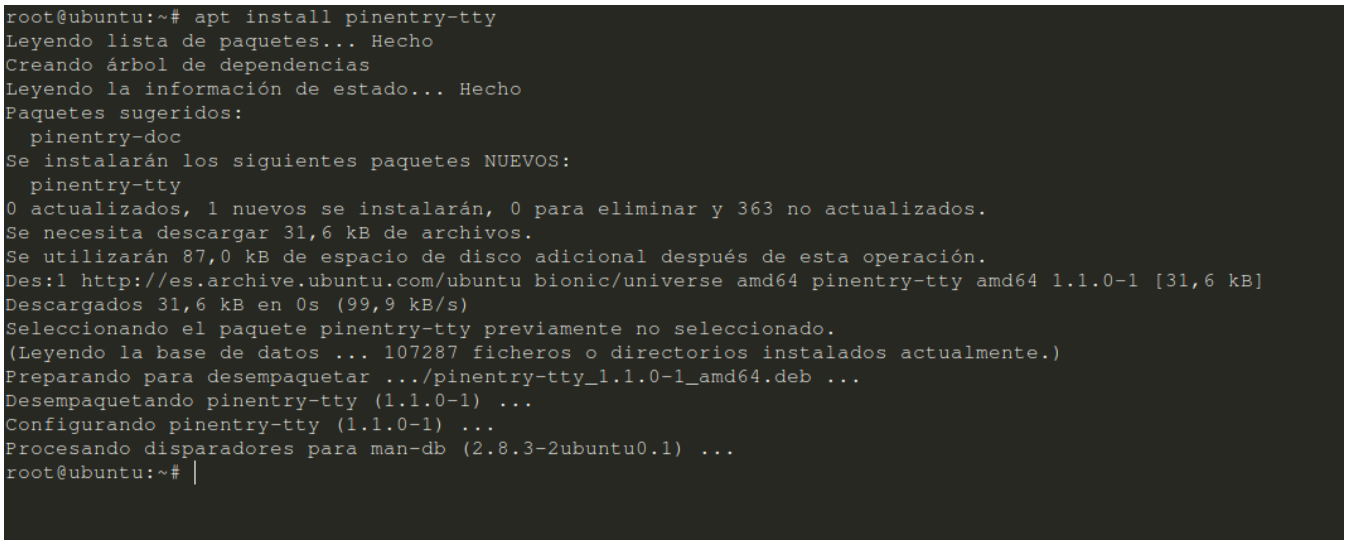
Cifrado Asimetrico

26/09/2023

Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

Contenido

Instalar herramienta pinentry



Ponemos el comando apt install pinentry-tty para instalarlo

¿En que consiste el cifrado asimétrico?

El cifrado asimétrico, también conocido como cifrado de clave pública, es un sistema criptográfico en el que se utilizan dos claves diferentes pero relacionadas para cifrar y descifrar información. Estas dos claves se llaman la "clave pública" y la "clave privada," y cada una tiene una función específica en el proceso de cifrado.

Aquí te explico cómo funciona el cifrado asimétrico y en qué consiste:

Clave pública: Esta clave se utiliza para cifrar un mensaje o datos antes de enviarlos. La clave pública es ampliamente conocida y compartida, por lo que cualquiera puede acceder a ella. Sin embargo, se utiliza solo para cifrar información, no para descifrarla. Si alguien cifra un mensaje con tu clave pública, solo podrás descifrarlo con tu clave privada.

Clave privada: Esta clave se mantiene en secreto y solo el propietario debe tener acceso a ella. Se utiliza para descifrar la información que ha sido cifrada con la clave pública correspondiente. En otras palabras, la clave privada se utiliza para desbloquear o descifrar los datos que han sido cifrados con la clave pública.

El proceso general del cifrado asimétrico es el siguiente:

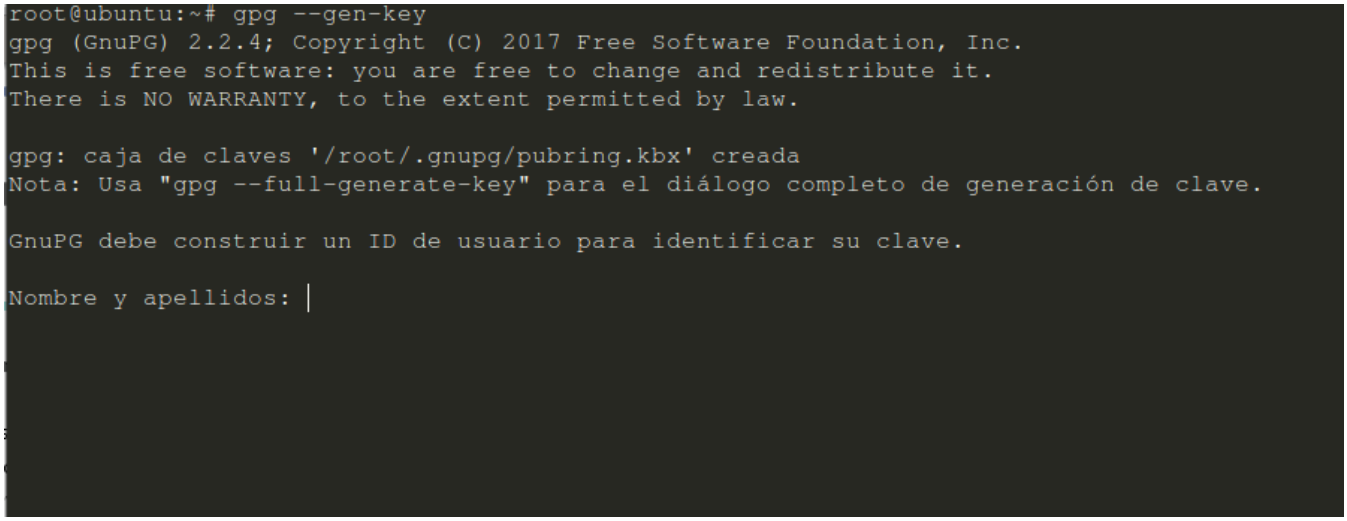
El remitente obtiene la clave pública del destinatario (que generalmente se encuentra en un certificado público o servidor).
El remitente utiliza la clave pública del destinatario para cifrar el mensaje o los datos que desea enviar.
El mensaje cifrado se envía al destinatario.

El destinatario utiliza su clave privada (que es mantenida en secreto) para descifrar el mensaje y acceder a la información original.
El cifrado asimétrico es ampliamente utilizado en la seguridad de la comunicación en línea, especialmente en aplicaciones como el correo electrónico seguro (usando el estándar OpenPGP), la autenticación en línea, la protección de contraseñas y en la creación de firmas digitales. Al utilizar claves pública y privada, este método proporciona una forma segura de comunicarse y autenticar identidades en línea sin necesidad de compartir contraseñas o claves secretas.

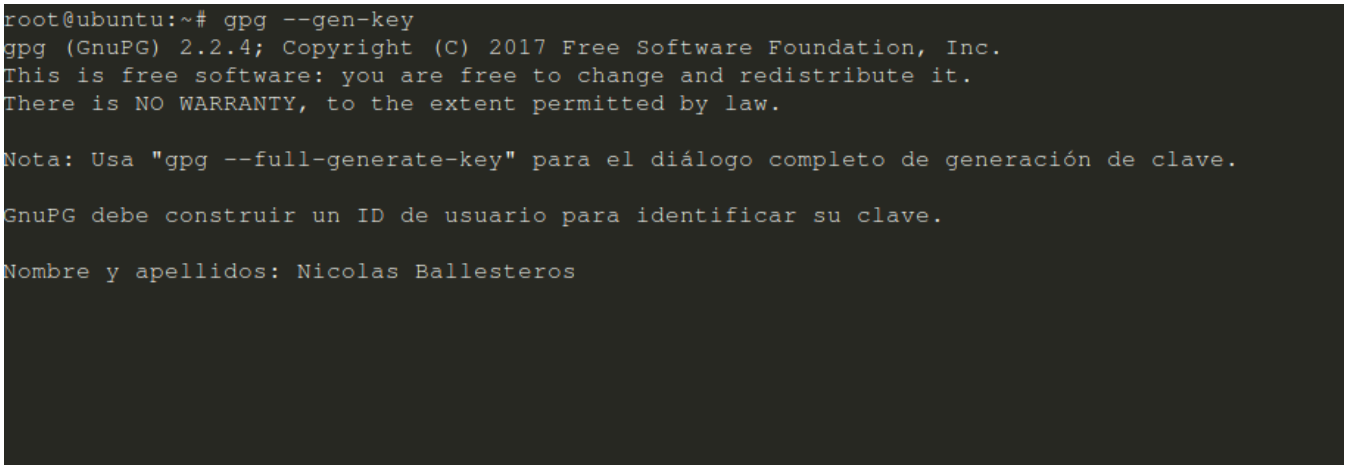
Es importante destacar que el cifrado asimétrico es más lento que el cifrado simétrico (donde se utiliza la misma clave para cifrar y descifrar) y, por lo tanto, se utiliza generalmente para cifrar claves simétricas o pequeñas cantidades de datos críticos, no para cifrar grandes cantidades de datos de manera eficiente.

Como crear clave publica privada y exportarla con la herramienta GPG

Accedemos con el comando gpg –gen-key



Ponemos nombre y apellidos



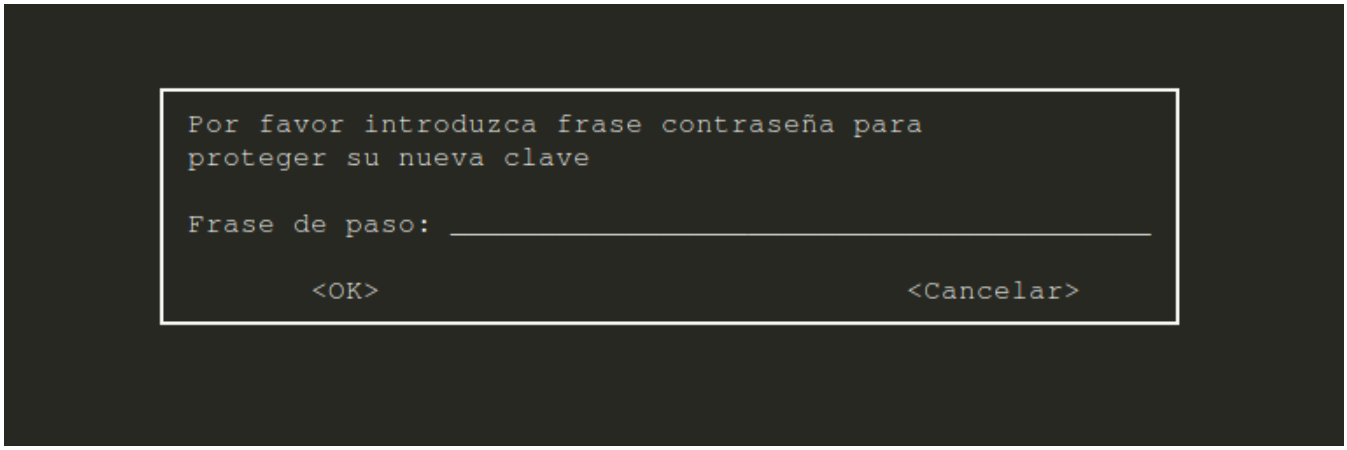
Ponemos correo electrónico

```
GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: Nicolas Ballesteros
Dirección de correo electrónico: nicolasballesteros@gmail.com
Ha seleccionado este ID de usuario:
    "Nicolas Ballesteros <nicolasballesteros@gmail.com>"

¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir?
```

Le damos a siguiente y nos sale para poner una contraseña



Hemos puesto ya la contraseña/Ceu123456

```
¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir? V
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
```

Nos dice claves publicas y secreta creadas y firmadas

```
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
gpg: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave E450542138A94B23 marcada como de confianza absoluta
gpg: creado el directorio '/root/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/root/.gnupg/openpgp-revocs.d/E0043A2A66A59D4B84
411D2BE450542138A94B23.rev'
claves pública y secreta creadas y firmadas.

pub   rsa3072 2023-09-26 [SC] [caduca: 2025-09-25]
      E0043A2A66A59D4B84411D2BE450542138A94B23
uid                      Nicolas Ballesteros <nicolasballesteros@gmail.com>
sub   rsa3072 2023-09-26 [E] [caduca: 2025-09-25]

root@ubuntu:~#
```

Comando gpg –list-secret-keys –keyid-format LONG

```
root@ubuntu:~# gpg --list-secret-keys --keyid-format LONG
gpg: comprobando base de datos de confianza
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: nivel: 0  validez:   1  firmada:   0  confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2025-09-25
/root/.gnupg/pubring.kbx
------------------------
sec   rsa3072/E450542138A94B23 2023-09-26 [SC] [caduca: 2025-09-25]
      E0043A2A66A59D4B84411D2BE450542138A94B23
uid              [  absoluta ] Nicolas Ballesteros <nicolasballesteros@gmail.com>
ssb   rsa3072/16ECA701D5A7F12B 2023-09-26 [E] [caduca: 2025-09-25]

root@ubuntu:~#
```

Es para listar claves secretas

Exportamos la Clave publica

Exportamos la clave publica, **aquí no nos pide contraseña**

```
root@ubuntu:~# gpg --armor --export E450542138A94B23
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGUTDHIBDAC7vvESV/r9r1SgvkuB3EDEBA5tX1NNmdYBw8B23GNUKzzpLzRT
mm42uJNyc/QAr4RC+OFyW4TZeMb9niRHd2WpyR/pqvQ7pb1T0M1f2URybWhGHr8o
2ilD+KIPIJvAE1HmCO8Ha33YJK+NsJ1m7sfNxy0TT5pLkAAjV///YtzhQ6EvDgLn
/HiMIQk+Ygcyg0/Yqrwh4nV5yYGFEN4rUrCH3TglX6ww4ml/ewECsroj7XAheVkw
lvnGr4Fz/rJkk8KCfpDiyvLiiFK6r9ijwC5Q3bNSDbQbhvdpuKfZS8qPaJaUX2yO
wEHiLRu1RktfA98VSitKCm3ZrCKK08ODXUUupGOZiheJDUzu+jSl4Rauv9vshIjv
hlflz/RBLFCCWGdSPBwlK2/KpAeFgVjPCiR/yuN60dUlyaWHndxzObWF9yVth9P3
NlEfyTlP+SZYjWkfkVnOYaJLO9oukaTBXl3lSgqGXExj5UeDLI33naElqhfLNS0P
6k//Bur7RPTx7gsAEQEAAbQyTmljb2xhcyBCYWxsZXN0ZXJvcyA8bmljb2xhc2Jh
bGxlc3Rlcm9zQGdtYWlsLmNvbT6JAdQEEwEKAD4WIQTgBDoqZqWdS4RBHSvkUFQh
OKlLIwUCZRMMcgIbAwUJA8JnAAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRDk
UFQhOKlLIlLpC/0SN9I0w/gWH0AsTYIQhOVuAHNjJvgwQ6az5T60FKrvsOGzkNOB
KaWlBZ9xgyhnsuLp7zxr5etFsQT4KHsj/vYl+uxOwXw24Ca3aGgeSaViFLWmGMwD
HeSKgdboTsAt+lFRRdn6QZvE1GMhwbwdw0GxtX2XIkj2319VdkdkRYxAtYSUeZeh
UXi7bdwLI0aGp8QhluAgZBOHivBwSzKrHv1tiG3+e+98oGChzkc0D26EOVyxAJaC
Iwe21/287cWdira3Wlll DU0z5y/m3LWlmn0K5SpzXRmqs+QO+UGIBTf1/RsfGTfC
LfHD8yMfQq9WIOn+wcyFX1uDy73I0NbRnUQsCID+79oyPG3hK/ynvD8SLIF2V2WF
YB0/PyQKV6NovAV8cz5liJ6IqdpSrstk1sz7OyTbDlTnJd2DsZ6Vpu6QAFAK12cO
LtIyVJ0/byNGhLTGM2YYH9ETYCMYVCsa+HE9Tlb3vKJ3JoKfuFFnHlSSMKRlmA0P
GERrukQiMXObq4u5AY0EZRMMcgEMALAmhbr79gqL84dNSypXsR/uMogomGj/JZ7k
TVz37maUNqRAj+nrUUzEgoLVzWziJogwZjH3Wbs42hkLqG6OmvqU+aoUNIi0AYfN
vefcRtMqhYxsTLj/gdnTkK8aAUpGR+fODUKJW9MR+u7vCX4Zu72sy+0Qtq+GgbH9
4/E3cGvDLIdbZGpfntdqBzkWzAZmUOvFT//2gALcdNZ4xy0qEDNcuJc0ztErg7Z6
GX0fcBpleYjo99Vglilx2GdOE2E804S43mP3KylurP4rfmZyJsKiIlBLDLDFP5u9
UGLMr9HlQuV8rrKu8aqwACE6IrMTYCkBz9PsYJ3xzltYmwjHugsMA9BIWST3rtwc
GQnzfMzKsiKQb0XWcNohmLSLyBZGsmPnew9YaGvr4ykHM9thiMP8f34fiwzc1WeH
c/JLCfGi590aRydRBGd1/n7gA/Dpz+qtoxDfUPRnF4cscXXcXseUl4IJ3Uz3ylGo
oZYuQsGKphIhYHPo9EOj6TUlJfkpgQARAQABiQG8BBgBCgAmFiEE4AQ6KmalnUuE
QR0r5FBUITipSyMFAmUTDHICGwwFCQPCZwAACgkQ5FBUITipSyPkgQv7BJehFVnT
5+mFW3bVKZR2/l58lbHumw9Qf9/yj0vf/Gub61O9EIn5wb2ZO3usawBIx69/2JZe
0j5aVdbmmo9bMebv01NhgGru3S9O6fWx0pAHap8tBUuC/7CJAyaro72mWDw463H0
xZh/3LofJHIQRk/D5S0svM26c3hivLoDKOlSaXAw4pNnecbD67KRWcqT+G0N3i+X
WC0LNAWPuMqbnAgFFWBwcXK02Y6Wjep3IhVHMLtyIT+0MVeTPWg/cxvtEX92sIt4
UBLiABOwydTJeEzAglWTd8ROXWelh05U0+SxWuOCk0fNBRdUhPUi33D9BkAmPnlR
f8J5kg2SUFWENNTYBX7cMK6YauciJ4JsF/ZsFa0vc/SvDPTzXag35KFwhq2R/4j2
u//0FeIHPKj8zc2v5JICaGCrHHHSK4Ha/cGWjkiQk2AHfSw5zCRyQ/YZ8IGGFTw1
y/iH31NZyPOLqTaoM4SiGIdP03ZYRsawoZRSHABA2a5VEgrnm6Jtn4Oe
=MQtH
-----END PGP PUBLIC KEY BLOCK-----
root@ubuntu:~#
```

Nos vamos a escritorio para crear una carpeta que guardaremos todas las claves

```
root@ubuntu:~/Escritorio# mkdir claves
root@ubuntu:~/Escritorio# ls -l
total 4
drwxr-xr-x 2 root root 4096 sep 26 19:16 claves
root@ubuntu:~/Escritorio#
```

```
root@ubuntu:~/Escritorio# mkdir claves
root@ubuntu:~/Escritorio# ls -l
total 4
drwxr-xr-x 2 root root 4096 sep 26 19:16 claves
root@ubuntu:~/Escritorio# cd claves/
root@ubuntu:~/Escritorio/claves# ls
root@ubuntu:~/Escritorio/claves# ls -l
total 0
root@ubuntu:~/Escritorio/claves#
```

Y ahí pondremos un comando que creara un fichero donde se exportara la clave en el fichero

```
root@ubuntu:~/Escritorio/claves# gpg --armor --export E450542138A94B23 >> Archivo.asc
root@ubuntu:~/Escritorio/claves# ls -l
total 4
-rw-r--r-- 1 root root 2476 sep 26 19:21 Archivo.asc
root@ubuntu:~/Escritorio/claves#
```

Vemos que se nos ha creado el fichero

Ponemos este comando para exportar la clave secreta

```
root@ubuntu:~/Escritorio/claves# gpg --export-secret-key --armor E450542138A94B23
```

Nos pide la contraseña para poder acceder ella

Ya hemos accedido porque la hemos exportado

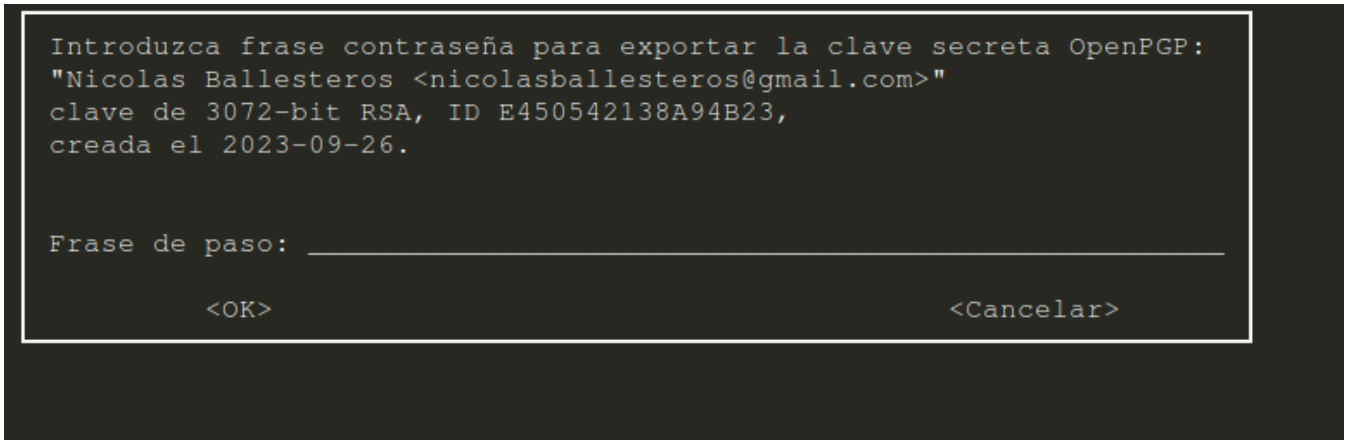
```
root@ubuntu:~/Escritorio/claves# gpg --export-secret-key --armor E450542138A94B23
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQWGBGUTDHIBDAC7vvESV/r9r1SgvkuB3EDEBA5tX1NNmdYBw8B23GNUKzzpLzRT
mm42uJNyc/QAr4RC+OFyW4TZeMb9niRHd2WpyR/pqvQ7pb1T0M1f2URybWhGHr8o
2ilD+KIPIJvAE1HmCO8Ha33YJK+NsJ1m7sfNxy0TT5pLkAAjV///YtzhQ6EvDgLn
/HiMIQk+Ygcyg0/Yqrwh4nV5yYGFEN4rUrCH3TglX6ww4ml/ewECsroj7XAheVkw
lvnGr4Fz/rJkk8KCfpDiyvLiiFK6r9ijwC5Q3bNSDbQbhvdpuKfZS8qPaJaUX2yO
wEHiLRulRktfA98VSitKCm3ZrCKK08ODXUUupGOZiheJDUzu+jSl4Rauv9vshIjv
hlflz/RBLFCCWGdSPBwlK2/KpAeFgVjPCiR/yuN60dUlyaWHndxzObWF9yVth9P3
NlEfyT1P+SZYjWkfkVnOYaJLO9oukaTBXl31SgqGXExj5UeDLI33naElqhfLNS0P
6k//Bur7RPTx7gsAEQEAAf4HAwKEFbGKTxbNPuUjDyCKU6Aiqko11R54dZMDJVco
sQjlObRVBFSb2GndPJf6WW6dboM42bhjQh394P88zo7CEZX6yh8LVA0ydUrI4P1k
WCeNEEHWs8TSn71zsXc6pCJTGli0q1TFfFKc5IkHtCNRTxTqKALBRA9Qk+RtXb4h
GYE6ANlcVxT8nrm9xsmpo/i881MIJgyx2TB+bUOjz3++OZs03q+9UiAuJge+//Yk
v2zD+crC/0MLL1F+ah4F+uKh8i6h2XoSqXX9TSwXwc+NT9I07KVT5RJy4JNTdXNw
WxfSmlZn9t78RuSgAjPyICrkrqexbf65uqmfCbznMJilBiPRT+CWChlUjOWht1Ss
tLJukNnLm/babM6X/rP0Eb9dASQwlh+JcMisfmYtA/W/TIXkHns5g8AbVqP3yG1P
nyJ2/CFIryA580ikdDkazXgBD5A8/eYaSOE6OTwZAgf5RBcYBWjKChA4YRdF1rdF
76Rz0hWR2U1zLanA47JzeBsCJ4ZfSgVUJdRuAtGATErFzj2aAqr7r5i7y5kPjhf1
yTLLP5bu0E1l+cKOlteEOaGOy7PnSZ1CPoDSZM1KKG5Ljr0wrd8a3VYh2QMQPq3M
ifIM2juLxNt/+pQbp41SPu5TtYJH9t9+YhIMWkPZcxFUaXjL/dYN8N6Sz1RWzdp2
AHEyWyAbI76q2tCWxC0VZyq+SD3hCkKKyZ3nZJ3tQxu+PWXtwCQnMOTxWQ0i3xtb
/3mDSYzwYa5+q3MzHr9MEofSGU5pcP7t4QL2vHeQFY5gpOjMm8yAYje6yGhLYOWc
UIMPk4rCBM+4Zz6OzwQG5a6vGTvqgq0TbF7edr45UxT+R7e53ZqlaY5oLq2LbILi
xUYmRHkk6p22HFL8tJA3YBPizbIJhltmQ1AT6anz1FfU0uq7clpm5r7Rq2GR7eXa
lMSVkJs85dMgLU4Dm8koMohafIkGil6wQePfgI+VPF2uY9LR0SytWKNcMOHM+Ebn
LJBshBvAJ4spr91+RF+FWuktkj8qKqbF5C40rZMSdzchQwInIFleDnR0KTmwMs76
dNRyoN8ZcsL52a3R97OI/5sbO4XgV4+ij6xAKSyCdB0+F8wA1bedn6PpLznjwpZ+
T1Xl8XyVdFQJAeXLnxgohJWmoCmG+OQXdhKsmUYTdT4+t+41O3oyloQjp6KKtoNm
XNW8xr95RQB33/EutM4zLn36OhU9PeMpczlkwImsQFUNxPnl9ONT4G3ItXwUc8wm
9hDB1TEqMggAOCUG1LwuGRoKESL+hGq9tc9OG8Q8AOF6mpz3gos5cljOJHTK2LpL
8ZNrLqFGUemGWfiGGFjyrZ89ToSoUTs/jbQyTmljb2xhcyBCYWxsZXN0ZXJvcyA8
bmljb2xhc2JhbGxlc3Rlcm9zQGdtYWlsLmNvbT6JAdQEEwEKAD4WIQTgBDoqZqWd
S4RBHSvkUFQhOKlLIwUCZRMMcgIbAwUJA8JnAAULCQgHAgYVCgkICwIEFgIDAQIe
AQIXgAAKCRDkUFQhOKlLI1LpC/0SN9IOw/gWH0AsTYIQhOVuAHNjJvgwQ6az5T60
FKrvsOGzkNOBKaWlBZ9xgyhnsuLp7zxr5etFsQT4KHsj/vYl+uxOwXw24Ca3aGge
SaViFLWmGMwDHeSKgdboTsAt+lFRRdn6QZvE1GMhwbwdw0GxtX2XIkj2319Vdkdk
RYxAtYSUeZehUXi7bdwLI0aGp8QhluAgZBOHivBwSzKrHv1tiG3+e+98oGChzkc0
D26EOVyxAJaCIwe21/287cWdira3Wl1lDU0z5y/m3LW1mn0K5SpzXRmqs+QO+UGI
BTfl/RsfGTfCLfHD8yMfQq9WIOn+wcyFX1uDy73I0NbRnUQsCID+79oyPG3hK/yn
```

Exportamos la clave privada

```
root@ubuntu:~/Escritorio/claves# gpg --export-secret-key --armor E450542138A94B23 >> ArchivoPr
ivado.asc
```

Ponemos ese comando y acto seguido nos pide la contraseña



Y ya esta en fichero dentro de la carpeta

```
root@ubuntu:~/Escritorio/claves# ls -l
total 12
-rw-r--r-- 1 root root 2476 sep 26 19:21 Archivo.asc
-rw-r--r-- 1 root root 5233 sep 26 19:31 ArchivoPrivado.asc
root@ubuntu:~/Escritorio/claves#
```

Como encriptar un fichero con GPG.

Listamos las claves que tenemos

```
root@ubuntu:~/Escritorio/claves# gpg --list-keys
/root/.gnupg/pubring.kbx
------------------------
pub   rsa3072 2023-09-26 [SC] [caduca: 2025-09-25]
      E0043A2A66A59D4B84411D2BE450542138A94B23
uid           [  absoluta ] Nicolas Ballesteros <nicolasballesteros@gmail.com>
sub   rsa3072 2023-09-26 [E] [caduca: 2025-09-25]

root@ubuntu:~/Escritorio/claves#
```

Importamos la clave publica

```
root@ubuntu:~/Escritorio/claves# gpg --import Archivo.asc
gpg: clave E450542138A94B23: "Nicolas Ballesteros <nicolasballesteros@gmail.com>" sin cambios
gpg: Cantidad total procesada: 1
gpg:               sin cambios: 1
root@ubuntu:~/Escritorio/claves#
```

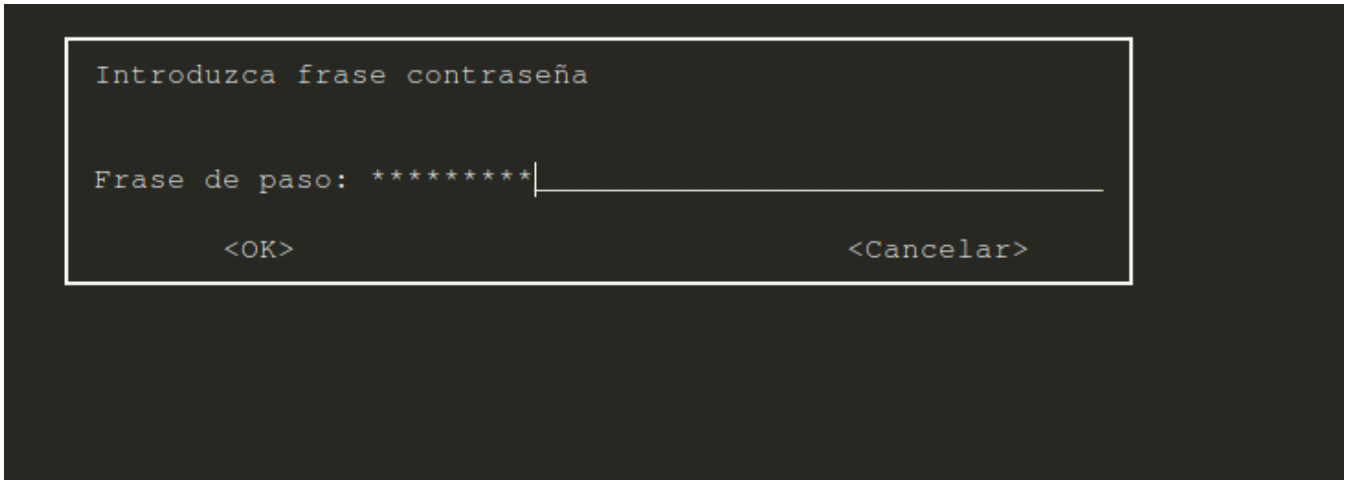
Encriptamos el archivo

```
root@ubuntu:~/Escritorio/claves# gpg --encrypt --recipient E450542138A94B23 --output Archivoen
criptado.gpg documentoencriptado.txt
El fichero 'Archivoencriptado.gpg' ya existe. ¿Sobreescribir? (s/N) S
root@ubuntu:~/Escritorio/claves# ls -l
total 16
-rw-r--r-- 1 root root 2476 sep 26 19:21 Archivo.asc
-rw-r--r-- 1 root root  483 sep 26 19:53 Archivoencriptado.gpg
-rw-r--r-- 1 root root 5233 sep 26 19:31 ArchivoPrivado.asc
-rw-r--r-- 1 root root    0 sep 26 19:53 documentoencriptado.txt
root@ubuntu:~/Escritorio/claves#
```

Especificamos una contraseña

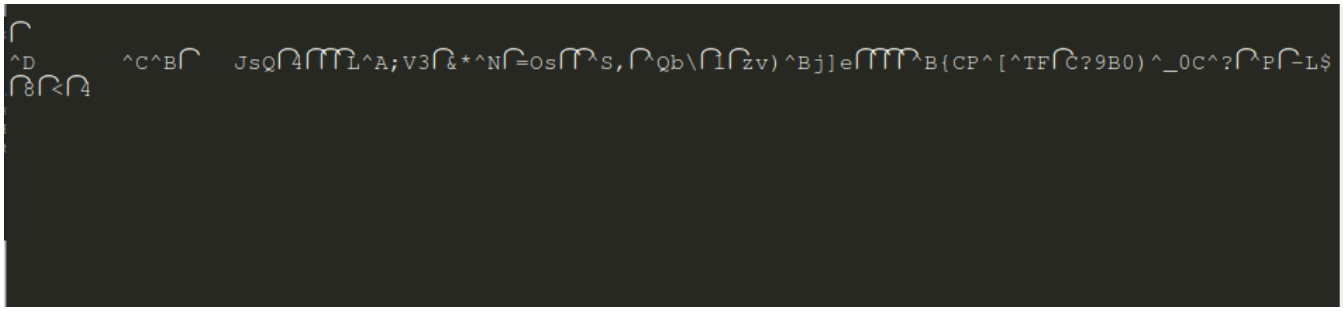
```
root@ubuntu:~/Escritorio/claves# gpg --symmetric --output Archivoencriptado.gpg documentoencri
ptado.txt
```

Le ponemos la contraseña



Le cambiamos el nombre del fichero Archivoencriptado2.gpg

```
root@ubuntu:~/Escritorio/claves# gpg --symmetric --output Archivoencriptado.gpg documentoencri
ptado.txt
El fichero 'Archivoencriptado.gpg' ya existe. ¿Sobreescribir? (s/N) N
Introduzca nuevo nombre de fichero: Archivoencriptado2.gpg
```



Vemos que esta encriptado