



CENTRE ESPECÍFIC
D'EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

ACTIVIDAD EVALUA

K

SEGURIDAD Y ALTA DISPONIBILIDAD

Cifrado con GnuGP en Linux Ubuntu

Alejandro Almagro Torregrosa.

Licencia Creative Commons



Reconocimiento – NoComercial – CompartirIgual (by-nc-sa): No se permite el uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Cifrado con GnuPG en Linux Ubuntu

GnuPG es una herramienta de cifrado y firmas digitales. Ubuntu escritorio
Para instalar GnuPG debes abrir una terminal de Linux y escribir:

```
sudo apt-get update
```

```
sudo apt-get install gnupg
```

```
root@dislexia-VirtualBox:/home/dislexia# aptitude install gnupg
gnupg ya está instalado en la versión solicitada (2.4.4-2ubuntu17)
gnupg ya está instalado en la versión solicitada (2.4.4-2ubuntu17)
No se instalará, actualizará o eliminará ningún paquete.
0 paquetes actualizados, 0 nuevos instalados, 0 para eliminar y 3 sin actualizar
.
Necesito descargar 0 B de ficheros. Después de desempaquetar se usarán 0 B.

root@dislexia-VirtualBox:/home/dislexia#
```

Para obtener ayuda sobre los comandos disponibles para GnuPG escribe en la terminal `gpg -h`

```
Necesito descargar 0 B de ficheros. Después de desempaquetar se usarán 0 B.

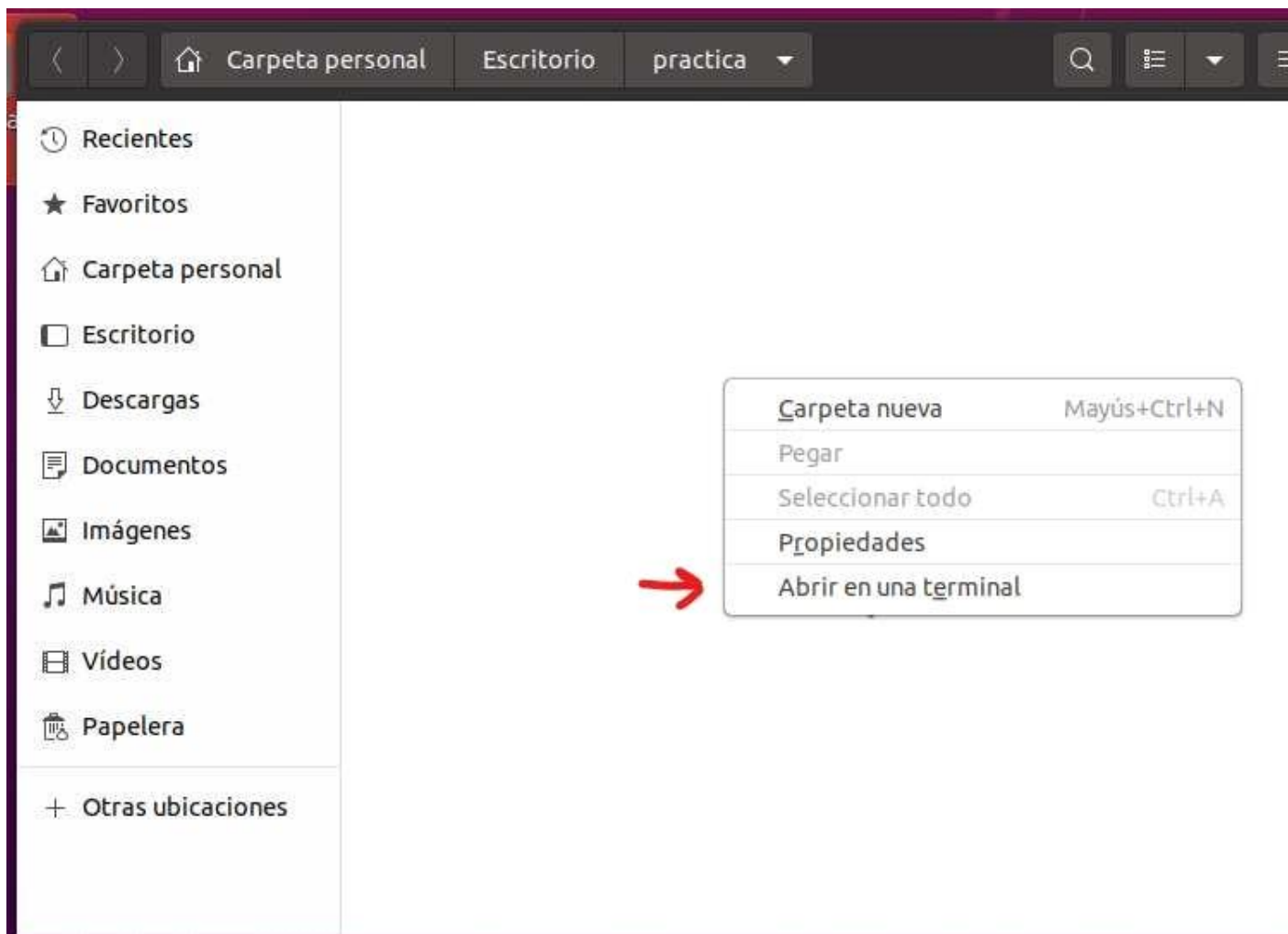
root@dislexia-VirtualBox:/home/dislexia# gpg -h
gpg (GnuPG) 2.4.4
libgcrypt 1.10.3
Copyright (C) 2024 g10 Code GmbH
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /root/.gnupg
Algoritmos disponibles:
Clave pública: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cifrado: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
CAMELLIA128, CAMELLIA192, CAMELLIA256
Resumen: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compresión: Sin comprimir, ZIP, ZLIB, BZIP2

Sintaxis: gpg [opciones] [ficheros]
firma, comprueba, cifra o descifra
la operación por defecto depende de los datos de entrada
```

Una vez instalado puedes cerrar la terminal.

Para esta práctica debes crear una carpeta y dentro de la carpeta llamada “practica cifrado simétrico” abrir una nueva terminal de Linux. Para ello, dentro de la carpeta en el explorador de archivos, haz *click derecho* y pulsa e *Abrir en una terminal*. Esto abrirá una terminal de Linux localizada en la carpeta que hemos creado.

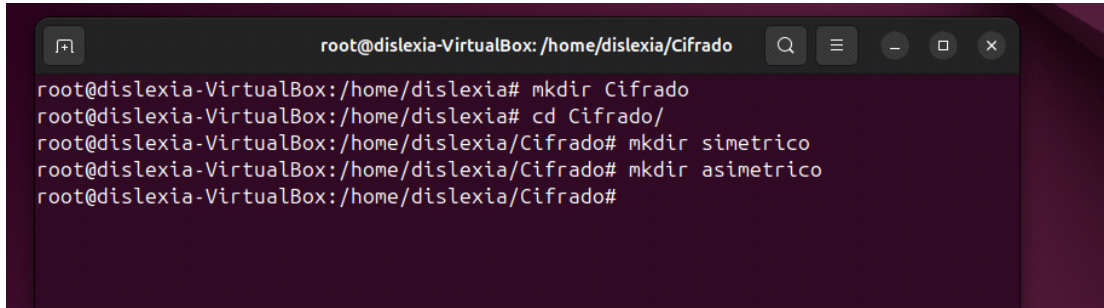


Práctica 1 – Cifrado simétrico

Crear un fichero, cifrarlo y descifrarlo con cifrado simétrico.

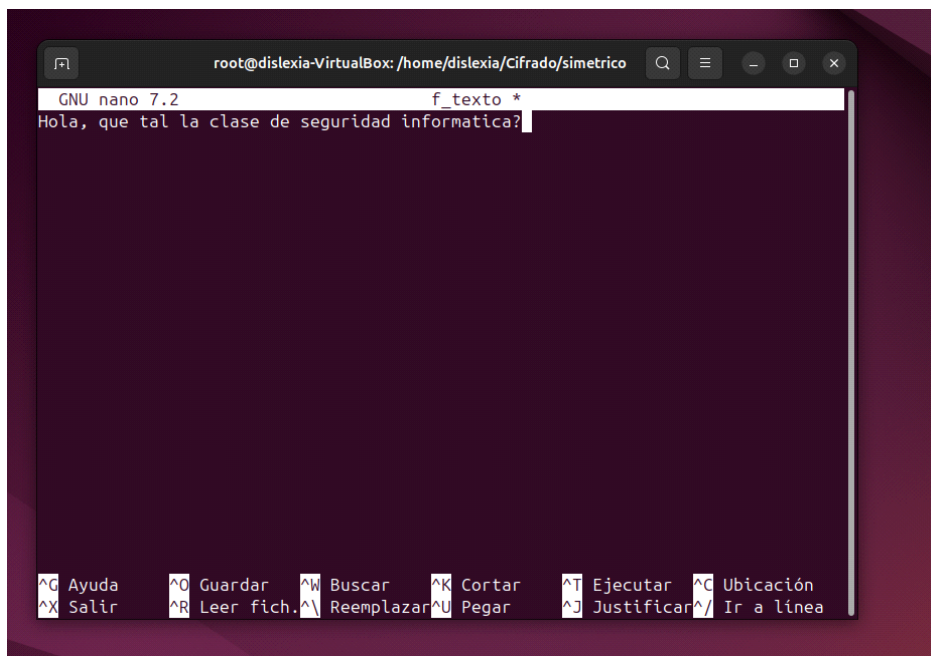
- Crea un fichero llamado **f_texto** con el comando *touch*.

`touch f_texto`

A terminal window titled 'root@dislexia-VirtualBox: /home/dislexia/Cifrado' showing the following commands and output:

```
root@dislexia-VirtualBox:/home/dislexia# mkdir Cifrado
root@dislexia-VirtualBox:/home/dislexia# cd Cifrado/
root@dislexia-VirtualBox:/home/dislexia/Cifrado# mkdir simetrico
root@dislexia-VirtualBox:/home/dislexia/Cifrado# mkdir asimetrico
root@dislexia-VirtualBox:/home/dislexia/Cifrado#
```

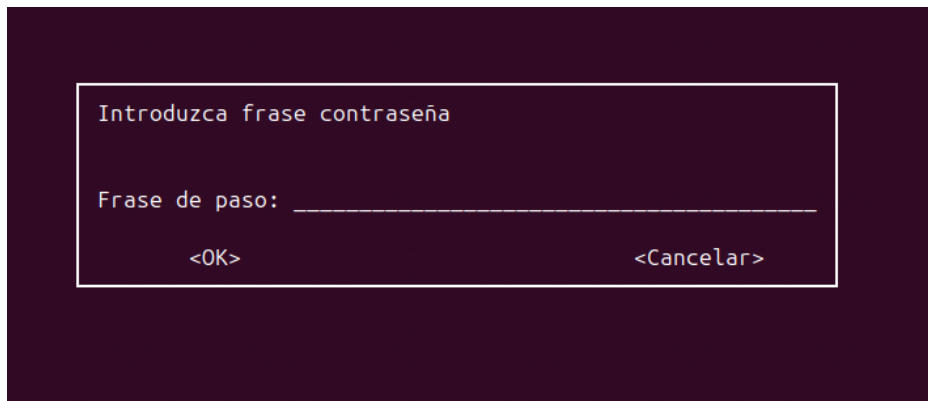
- Abre el fichero haciendo doble click y **escribe “Hola, que tal la clase de seguridad informática?” dentro de él**. Guarda el fichero y cierra el editor de texto.

A terminal window titled 'root@dislexia-VirtualBox: /home/dislexia/Cifrado/simetrico' showing the nano 7.2 editor. The file 'f_texto *' is open, and the text 'Hola, que tal la clase de seguridad informática?' is entered. The bottom status bar shows various keyboard shortcuts like '^G Ayuda', '^O Guardar', etc.

```
GNU nano 7.2 f_texto *
Hola, que tal la clase de seguridad informática?
```

- Vamos a cifrar el fichero utilizando una clave de paso. La clave debe ser *clave123*. Para cifrar vamos a utilizar el comando de GnuPG: *gpg*. Cifra el fichero *f_texto* utilizando la opción de comando *-c*.

`gpg -c f_texto`



Se habrá creado un fichero f_texto.gpg. Es el fichero cifrado.

```
root@dislexia-VirtualBox:/home/dislexia/Cifrado/simetrico# gpg -c f_texto
root@dislexia-VirtualBox:/home/dislexia/Cifrado/simetrico# ls
f_texto  f_texto.gpg
root@dislexia-VirtualBox:/home/dislexia/Cifrado/simetrico#
```

- Descripta el fichero encriptado. Ahora, vamos a limpiar la cache de contraseñas para simular loque le sucedería a una persona que recibe el fichero cifrado y quiere descifrarlo.

Limpiar cache:

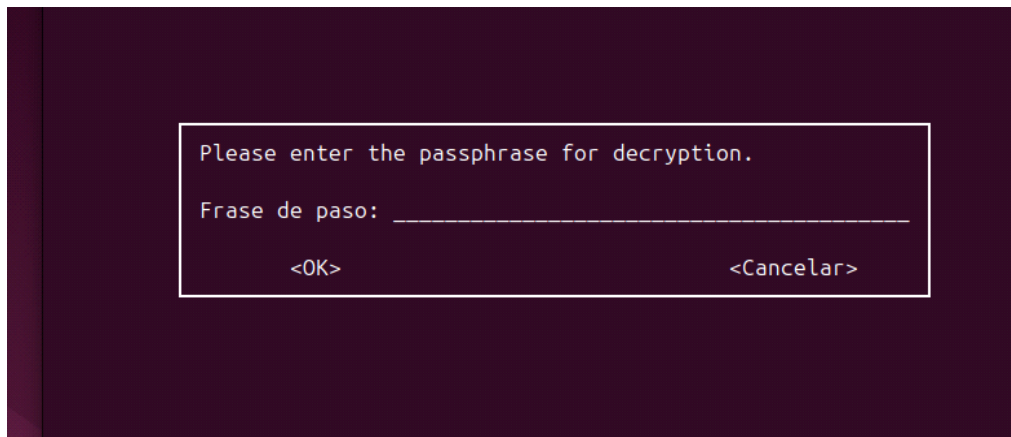
gpg-connect-agent reloadagent /bye

```
root@dislexia-VirtualBox:/home/dislexia/Cifrado/simetrico# gpg-connect-agent reloadagent /bye
OK
```

Para descriptar un fichero debes indicar dónde se va a guardar el resultado de descriptarutilizando la opción -o y el fichero que quieres descriptar utilizando -d.

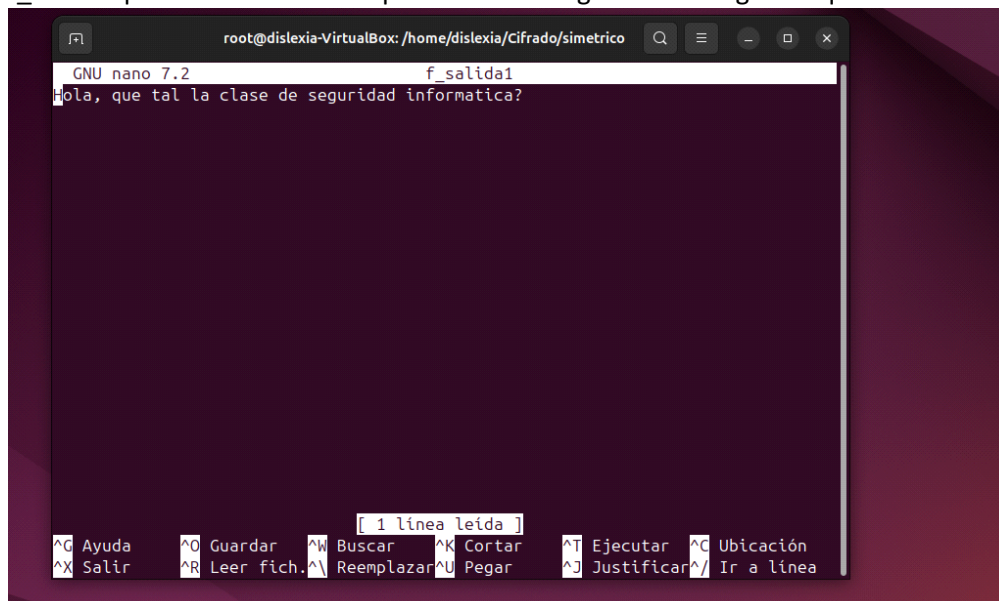


gpg -o f_salida1 -d f_texto.gpg



```
root@dislexia-VirtualBox:/home/dislexia/Cifrado/simetrico# gpg -o f_salida1 -d f_texto.gpg
gpg: AES256.CFB encrypted data
gpg: cifrado con 1 frase contraseña
root@dislexia-VirtualBox:/home/dislexia/Cifrado/simetrico# ls
f_salida1 f_texto f_texto.gpg
root@dislexia-VirtualBox:/home/dislexia/Cifrado/simetrico#
```

Si te ha pedido una contraseña para desencriptar y se ha creado un fichero con el nombre `f_salida1` que contiene el texto que escribiste originalmente significa que has hecho todo bie





Práctica 2 – Cifrado asimétrico

Descripción de la práctica.

En el cifrado asimétrico las claves públicas y privadas se guardan en un llavero que gestiona Ubuntu. Al ser claves muy complejas e irrecordables por una persona estas deberán estar correctamente identificadas a través de la descripción, el nombre y el email de propietario.

En esta práctica deberás crear una dupla de claves (la pública y la privada), encriptar un fichero con tu clave pública (cualquier persona a la que le des tu clave pública puede encriptar un fichero) y posteriormente, desencriptar el fichero usando tu clave privada. Es importante no pasar tu clave privada a nadie pues de lo contrario cualquier persona podría leer los ficheros encriptados con la clave pública y solo tú quieres poder leerlo.

- Genera una dupla de claves para el cifrado simétrico:

```
gpg --full-generate-key
```

La clave deberá ser de 3072 bits de longitud y el algoritmo de cifrado “*DSA y ElGamal*”.

Las claves caducarán en 5 días.

Te pedirá una manera de identificar ese par de claves con tu nombre, un email y una descripción.

```
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico# gpg --full-generate-
key
gpg (GnuPG) 2.4.4; Copyright (C) 2024 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.

Por favor seleccione tipo de clave deseado:
(1) RSA and RSA
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
(9) ECC (sign and encrypt) *default*
(10) ECC (sólo firmar)
(14) Existing key from card
Su elección: 2
las claves DSA pueden tener entre 1024 y 3072 bits de longitud.
¿De qué tamaño quiere la clave? (2048) 3072
El tamaño requerido es de 3072 bits
Por favor, especifique el período de validez de la clave.
  0 = la clave nunca caduca
 <n> = la clave caduca en n días
```



```

root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico# gpg --list-keys
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: 2024-11-05
/root/.gnupg/pubring.kbx
-----
pub   dsa3072 2024-10-31 [SC] [caduca: 2024-11-05]
      8CF4125426BB54F28D69AE916BB7A80147554FF6
uid   [ absoluta ] Alejandro Almagro (Clave para asimetricas) <sr.panceto@gmail.com>
sub   elg3072 2024-10-31 [E] [caduca: 2024-11-05]

```

Por favor introduzca frase contraseña para proteger su nueva clave

Frase de paso: _____

<OK>

<Cancelar>

Posteriormente te pedirá una clave de paso que será *clave123*. Esta clave servirá como contraseña para poder acceder a la clave privada cuando queramos. Para acceder a la clave pública no será necesario introducir ninguna clave de paso pues es pública y puede acceder quien quiera.

- Tras generar las claves, podemos listar las claves (sin mostrarlas) que tenemos en el llavero usando el siguiente comando:

gpg --list-keys

```

root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico# gpg --list-keys
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: 2024-11-05
/root/.gnupg/pubring.kbx
-----
pub   dsa3072 2024-10-31 [SC] [caduca: 2024-11-05]
      8CF4125426BB54F28D69AE916BB7A80147554FF6
uid   [ absoluta ] Alejandro Almagro (Clave para asimetricas) <sr.panceto@gmail.com>
sub   elg3072 2024-10-31 [E] [caduca: 2024-11-05]

```

Cuidado: este comando no te muestra las claves, únicamente te las lista mostrando el ID que las identifica y

la información proporcionada anteriormente. ID NO es la clave.

ID

```

pub   rsa3072 2021-11-15 [SC] [caduca: 2023-11-15]
      E23DB57E9F4B1323F056BA01BA14B6861AFFF70F
uid   Paco Gimenez <PacoGimenez@gmail.com>
sub   rsa3072 2021-11-15 [E] [caduca: 2023-11-15]

```

- Exporta la clave pública en un fichero para poder pasársela a alguien en caso de que fueran necesario.

`gpg -a -o f_clave_publica --export KEY_ID`

```
pub dsa3072 2024-10-31 [SC] [caduca: 2024-11-05]
    8CF4125426BB54F28D69AE916BB7A80147554FF6
uid [ absoluta ] Alejandro Almagro (Clave para asimetricas) <sr.panceto@gmail.com>
sub elg3072 2024-10-31 [E] [caduca: 2024-11-05]

root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico# gpg -a -o f_clave_publica --export sr.panceto@gmail.com
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico# ls
f_clave_publica
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico#
```

Cuidado: debes sustituir `KEY_ID` por el ID del par de claves o el email de esta.

Se habrá creado un fichero con la clave pública. Comprobar en carpeta archivo con logo candado.

Si quieres que alguien cifre un fichero que solo puedas leer tú puedes pásale esa clave y esa persona deberá cifrar con la clave.

```
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico
GNU nano 7.2 f_clave_publica
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQSuBGCjwNoRDACu9oTYTC+vzV6nUjx32W9GpPux2liTCZajcxuq0n50kua32miE
pAXDqIQ7LCC2826Si1sWuBJscA4QqL9YEpZ6Kn1vdXvh/Qo0CYbH8wrB5tVNxcGL
UpZy0fAB7C0QeXIL1mj5emXAofnsYTXsGB3Yry3yHQJbsgK6Vpod+p1VnIshB3t3
vH0Gcw1lfr/ht15qPmNU39meHNMpCFqr5F4G37VXwvxVEDXbH/oN/j8I9ngTEfTG
Ci1A56C1xQd+yerG0ktrA5IA/8MpmKpVtFyMW1iUubzac8H743cs0/gh6Ij0gepV
hlTRuwk6E1q3uJhMRkiTBk/dYfXjl02hkpcdbLcIp/WmGY/qZEykyMxY2LDSBwZd
YzBE2kVns/AwRCA/S+Gxt0sXM+67QI9xmYpaZF8ZUE5Tvqid00SVhlBdjNU4BY/3
5W4xMuKkciyqbyrkF+CbtW4xgMmCXWBN9z3M3Z7kdpclFdB8N5iNWqMxGs4dBMP
Ux+XARjuTJkAH0sBAKb/ZzxSVcNW5SKqdmFdoQAJXzTjSt54c4KbdXSG7aS/C/9h
iOzzPsULk58P0mnZnPN0fA3yMWIt0yGakCKM4C9Eg5mgUhxk/c/ZH4eG8ksLt3Zr
nBUy6l4qqlsXqzv7svZQzyk8vFVP7fC7+B32cbKnKZDAv+cquLK4PoPgmRVfAKg3
d03LswMh2QEiCk22Q70yRGpcdvjPkqyNZoKiBalB6cmxmVUcy+7EAEhIyVfkWjd
K/aNRNNbN9qy6vk42/urI2x9fGe+baq5SLNCE3/E7xaLz1Y0kgm+Uaob/YD8P3HJ
D80vJI3ua6B96mIXUwm14xeGrk9yxtarQPEoXwsljvmX9X+T6NZCFm7TW/FRX9uv
xUo6fpU/AiIX0qXIV1dg9IX7Elhm4LC164xSETZmSxB4pT0DN4H6CS0/x40RBrAu
dABk+U7CbnRWCkr6dHQb0mLD2rTC696qZ6+M+aJcHIeYkfcD3yqrJB/GHLLBb5D
rjGQZ/CVS6PzTtD92pTGWdhq15bBKI+4hBXsstYw12LZnUo7roE+JraWSl03sIoL
/3UCfkUvh0sQdth0horG6ti12FkBP6a+jdZ6B+YkiRc3vnT99B4YLUNIR8nNMmoL

[ 53 líneas leídas ]
^G Ayuda      ^O Guardar   ^W Buscar    ^K Cortar    ^T Ejecutar  ^C Ubicación
^X Salir      ^R Leer fich.^_ Reemplazar ^U Pegar     ^J Justificar^_/ Ir a línea
```

- Vamos a simular que somos una persona ajena que nos quiere mandar un mensaje cifrado. Debemos primero importar la clave pública ajena para poder cifrar con ella.

`gpg --import f_clave_publica`

```
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico# gpg --import f_clave_publica
gpg: clave 6BB7A80147554FF6: "Alejandro Almagro (Clave para asimetricas) <sr.panceto@gmail.com>" sin cambios
gpg: Cantidad total procesada: 1
gpg: sin cambios: 1
```

En el caso de que no existiera en nuestro llavero ahora aparecería un nuevo elemento en la lista de claves, se trata de la clave pública. En nuestro caso no se añade ninguna pues ya la teníamos porque la hemos creado nosotros.

- Cifrar con la clave pública.

`gpg -r KEY_ID -a -o f_cifrado2 --encrypt f_texto`

Cuidado: debes sustituir KEY_ID por el ID de la clave que quieres usar para cifrar.

```
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico# gpg -r sr.panceto@gmail.com -a -o f_cifrado2 --encrypt f_texto
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico#
```

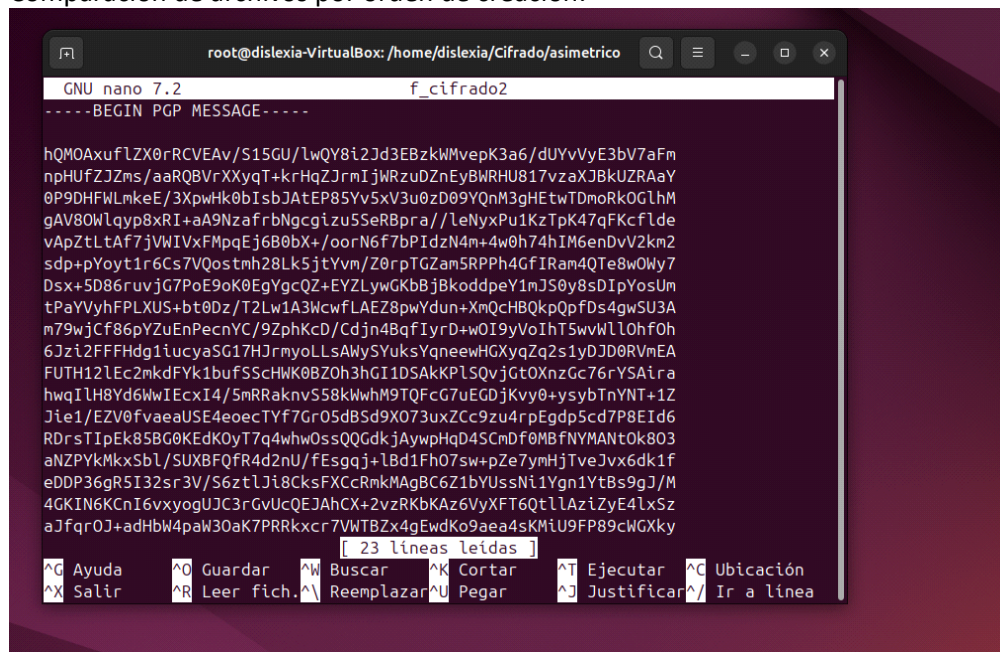
-a Encipta en ASCII para poder ser legible y no tener problemas de envío de paquete. F_Cifrado2 es el nombre del archivo que vamos a crear encriptado

```
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico# gpg -r sr.panceto@gmail.com -a -o f_cifrado2 --encrypt f_texto
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico# ls
f_cifrado2 f_clave_publica f_texto
```

KEY (mail ó ID) designa la contraseña publica que vamos a utilizar para encriptar “Prueba a hacer el mismo ejercicio sin -a (Binario)” y comprueba qué pasa.

```
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico# gpg -r sr.panceto@gmail.com -o f_cifrado3 --encrypt f_texto
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico#
```

Comparacion de archivos por orden de creacion:



The screenshot shows a terminal window titled 'root@dislexia-VirtualBox: /home/dislexia/cifrado/asimetrico'. Inside, the GNU nano 7.2 editor is open, editing a file named 'f_cifrado2'. The editor displays a PGP message starting with '-----BEGIN PGP MESSAGE-----' followed by a large block of base64-encoded text. The text is wrapped at 76 characters per line. At the bottom of the editor, a status bar indicates '[23 lineas leidas]'. Below the editor, a keyboard shortcuts menu is visible, listing various actions like Ayuda, Guardar, Buscar, Cortar, Ejecutar, Ubicación, Salir, Leer fich., Reemplazar, Pegar, Justificar, and Ir a línea.

```
root@dislexia-VirtualBox: /home/dislexia/cifrado/asimetrico
GNU nano 7.2 f_cifrado2
-----BEGIN PGP MESSAGE-----

hQMOAxuflZX0rRCVEAv/S15GU/lwQY8i2Jd3EBzkWMvepK3a6/dUYvVyE3bV7aFm
npHUfZJZms/aaRQBvRXXyqT+krHqZJrmIjWRzuDZnEyBWRHU817vzaXJBkUZRAaY
0P9DHFwLmkeE/3XpwHk0bIsbJAtEP85Yv5xV3u0zD09YQnM3gHEtwTDmoRkOGlhM
gAV80Wlqyp8xRI+aA9NzafRbNgcgizu5SeRBpra//leNyxPu1KzTpK47qFKcflde
vApZtLtAf7jVWIVxFMpqEj6B0bX+/oorN6f7bPIdzN4m+4w0h74hIM6enDv2km2
sdp+pYoyt1r6Cs7VQostmh28Lk5jtYvm/Z0rpTGZam5RPPH4GfIRam4QTe8w0Wy7
Dsx+5D86ruvjG7PoE9oK0EgYgcQZ+EYZLwGKbBjBkoddpeY1mJS0y8sDipYosUm
tPaVvyhFPLXUS+bt0Dz/T2Lw1A3WcwfLAEZ8pwYdun+XmQcHBQkpQpFDs4gwSU3A
m79wjCf86pYZuEnPecNYC/9ZphKcD/Cdjn4BqfIyrd+wOI9yVoIhT5wvWllohf0h
6Jzi2FFFHdg1iucyaSG17HJrmyoLLsAWySYuksYqneewHGXYqZq2s1yDJD0RVmEA
FUTH12lEc2mkdFYk1bufSScHWK0B20h3hGI1DSAKPLSqvJgtOXnzGc76rYSAira
hwqILH8Yd6WwIEcxI4/5mRRaknvS58kWhM9TQFcG7uEGDjKvy0+ysybTnYNT+1Z
Jie1/EZV0fvaeeUSE4eoecTYf7Gr05dBsd9X073uxZCc9zu4rpEgdpScd7P8EId6
RDrsTIpEk85BG0KedK0yT7q4whw0ssQQGdkjAypwHqD4ScmDf0MBfNYMANTok803
aNZPYkMxSbL/SUXBFQFR4d2nU/fEsqgj+lBd1Fh07sw+pZe7ymHjTveJvx6dk1f
eDDP36gR5I32sr3V/S6ztLJi8CksFXCcRmkMAgBC6Z1bYUssNi1Ygn1YtBs9gJ/M
4GKIN6KcNI6vxyogUJC3rGvUcQEJAhCX+2vzRKbKAz6VyXFT6QtllAziZyE4lxSz
aJfqr0J+adHbW4paW30aK7PRRkxcr7VNTBZx4gEwdKo9aea4sKMiU9FP89cWGXky

[ 23 lineas leidas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^_ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea
```

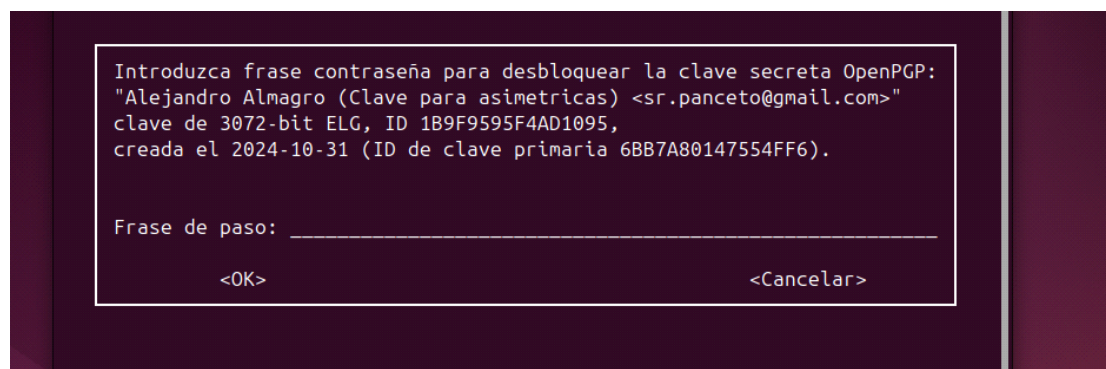


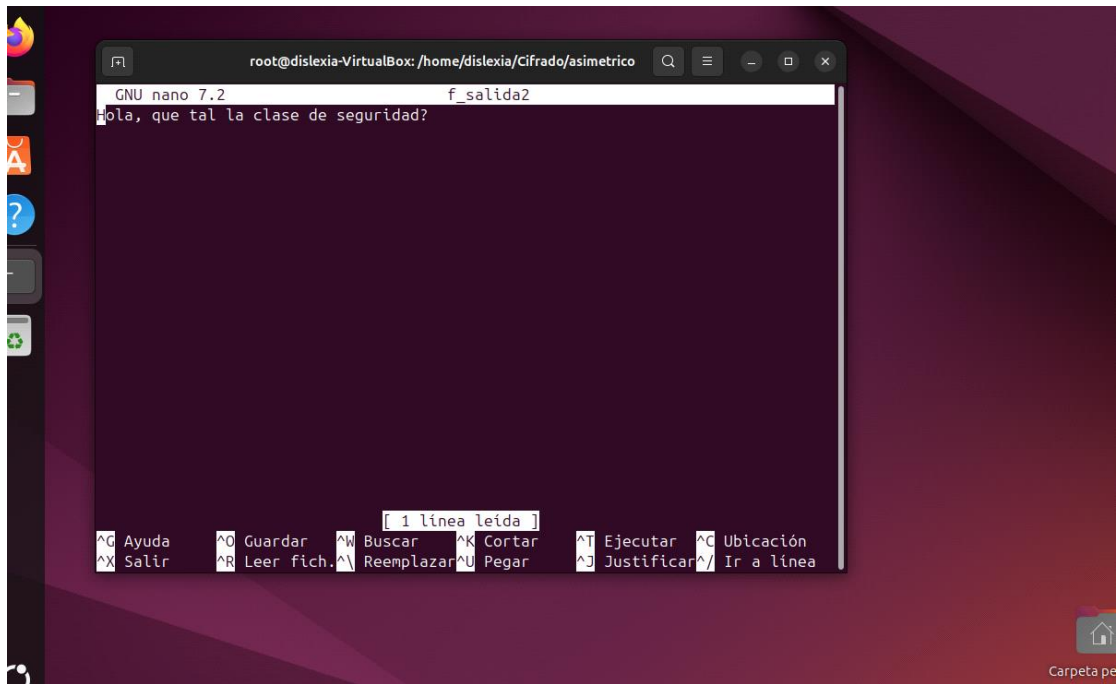
```
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico
GNU nano 7.2 f_cifrado3
^C^N^C^  ^P^P^L^@^y
a40er$^U=^i^Y5_läF^P^? (w^Z^A^V: _Q^0'^^?; z!i^q^0Q
^Q`^0^R^P^u& ^M*^)^m+^[^@_*(b^B^;{Häh^<^ K^@^P^iHQ^tx
^#^9^>]^^^^^] ^X.^i^W= d^X,^
^W&^[W^B6j-X$fe~^X^B^X06^A^C^C^Q^Q^Y}^H^[^W^^^^\^;)^^^^^|K^W^zT^nc^
R^c^i^S^@^Tz;^N(N^V^d^m^H-^&Z^=====^i^ ^/^S^t^u%^P^^\$^j^e^C^o^k^e^0^6p_
^$^n^e^\/^/+0q^i^D^A^0^M^s^L^Hm[])^^^^Y`^M^o)^^\^~^-%^

[ 7 líneas leídas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar      ^J Justificar ^/ Ir a línea
```

- Desencripta el fichero cifrado.

gpg -r KEY_ID -o f_salida2 --decrypt f_cifrado2





KEY_ID: Id del llavero que contiene la clave privada a utilizar.

Te pedirá la clave de paso. Esto se debe a que para descryptar un fichero debemos acceder a la clave privada.



Práctica 3 – Cifrado asimétrico

Los criptosistemas asimétricos pueden emplear diferentes longitudes de clave y diferentes algoritmos de cifrado. Mayores longitudes de clave harán que la generación y el cifrado sean más lentos.

Crea una pareja de claves de manera similar a lo realizado anteriormente utilizando el comando.

`gpg --full--generate-key`

```

las claves DSA pueden tener entre 1024 y 3072 bits de longitud.
¿De qué tamaño quiere la clave? (2048) 3072
El tamaño requerido es de 3072 bits
Por favor, especifique el período de validez de la clave.
    0 = la clave nunca caduca
    <n> = la clave caduca en n días
    <n>w = la clave caduca en n semanas
    <n>m = la clave caduca en n meses
    <n>y = la clave caduca en n años
¿Validez de la clave (0)? 3
La clave caduca dom 03 nov 2024 18:53:54 CET
¿Es correcto? (s/n) s

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

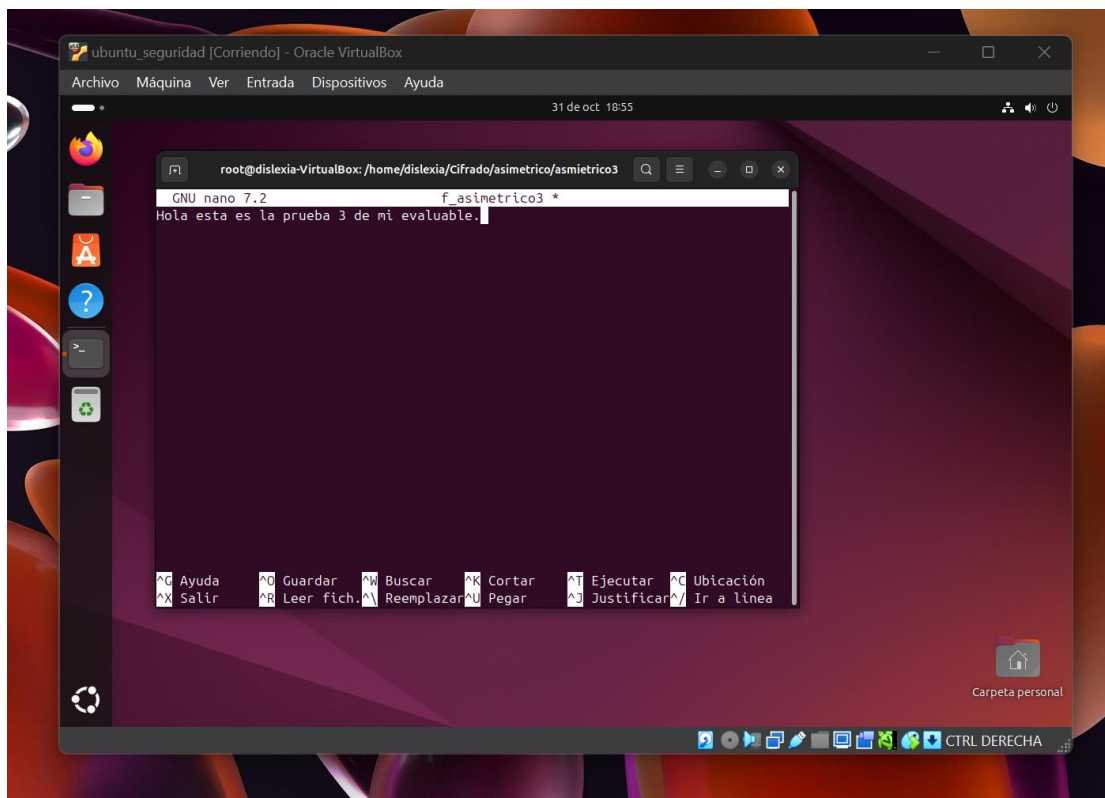
Nombre y apellidos: Alex Almagro
Dirección de correo electrónico: clasedeseguridad@gmail.com
Comentario: esta es la clave del ejercicio 3
Ha seleccionado este ID de usuario:
    "Alex Almagro (esta es la clave del ejercicio 3) <clasedeseguridad@gmail.com
>"

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

```

La clave deberá ser de 3072 bits de longitud y el algoritmo de cifrado “DSA y ElGamal”.

Cifra un fichero con la clave pública generada (no hace falta que la exportes y la importes pues la has creado tú y ya la tienes).




```

root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3# gpg -r c
lasedeseguridad@gmail.com -a -o f_cifrado3 --encrypt f_asimetrico3
gpg: comprobando base de datos de confianza
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: nivel: 0 validez: 2 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 2u
gpg: siguiente comprobación de base de datos de confianza el: 2024-11-03
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3# ls
f_asimetrico3 f_cifrado3
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3#

```

```

GNU nano 7.2 f_cifrado3
-----BEGIN PGP MESSAGE-----

hQMOA/xcHte1Cs1+EAWAvMfDDut7aGf0S19QNKhaZGoN5riPm53ajPAA4rxuZLq
5UBYr1XG91cnONZCZOjSMLuT4Zt90y+K/aRuXeHbFjIEPvAveRMVb7eA0ZkB0iah
PdiJYksDY/ghn3sbpxB9f+zES7Q14PDf49qyGbsZEESNSZ1dgLYnTJoIyIoJ4U7J
26iQ+e4HUKUxGzpBqHJLA2E3Btlw37zVSE60bKxjghWC3mX8nHRWpdLPdF2udDM
k1A9FrGUJ+d/pdLmAW5mvE9woPEww2KZeux1IDxPUcNvZKYlpTM80BeRMw1cN8Kd
cxTVTIKeRmUG27hhZjsR0rYkVpwUuZuNo1pkUDgvzVZfAmaJYw1jWoxJeCBZ3juM
Rfd/63oX2PNYjeG+lglyxRsMI+CERmMnWaoc5qnY6WeTN7X66PkVDiIxtE7T72i
DU7o2jSmpvHLxy4iKNPRSGZZfpQ4D3rzDeGczKXzItsTMTYrvmOwc0oPBIUL1R3l
58LDF+UhmQ239upU0K7kC/wKdRWCjwnma0DkRKe7WigEibplyI62/P0bRG4L5+dK
3fdoQ9WJuavKyQJ1PdLyHSvZRFVnHENmSWyDh00e1MvqkzmRYGVAdW30NH5Gd83
05bjvgIgiImIoKJJYhTo71MznMBj8SGdqLvDpUVFPwYE7uf0i8rTFR5cW0kAXSLf
wgaKMKMwS5j6cpTbQUyRuo40stk7LQSHmW0MXkb0L4sMdFxbwn1XjEbl/CGhor2
jYKtz3gTurHiJTGMMQB5sIav0WecoKF2ERpZ79+GXWGTJXg4Lu6t6o1g1HsnUK2
x830HyTdeSCftn2Es2ZX1U+S/T5Ap44sb5Mv4foZzV5CT5UQ5sq2Qq70Dyl010U2
bBLMdMfScB8XJWGCi/3aJDiSaKn/waZ7Bndvg+kPqgdDZBSLEfYQRoPUFZEZ9fY
QtsLDBq8Z03V9+X0y6on3G4Sv2+i3T1Zs2HkgkGCHccde3N8G1MZjk6skPdByKR6
z99yczeFjcchutM6iaM1k23UeAEJAAR7hSKEmdLbmK/eK3FIkBXeKtJNV0JS3Uk
oCcFZShE0tEiAa4WKEvADQYjsJI59jE001XHJhjkyzfsVpH1y3w0Wo9hcAjrDS3R

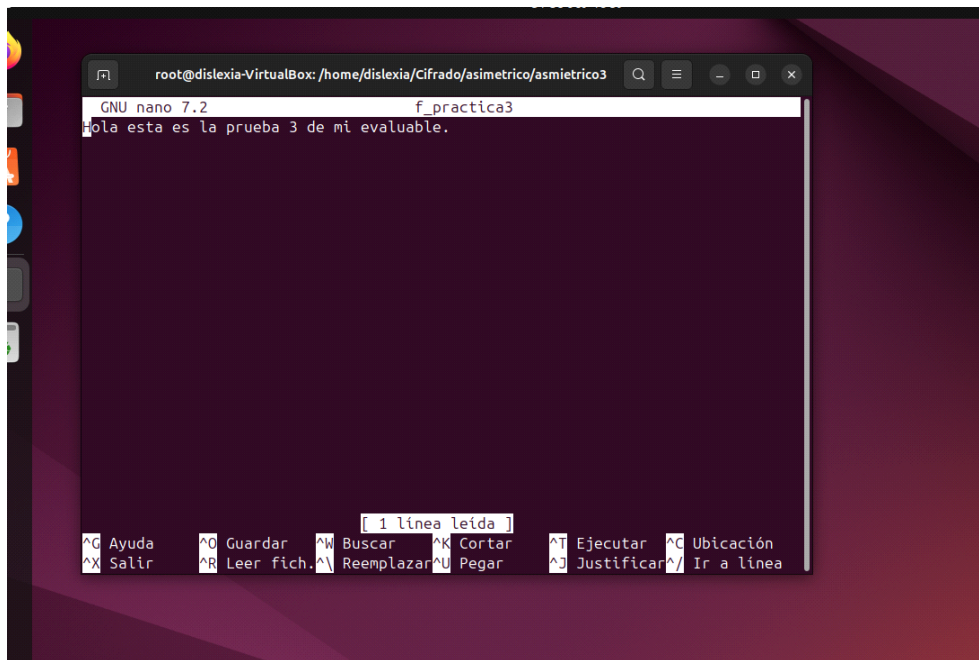
[ 23 líneas leídas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^_ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea

```

```

root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3# gpg -r c
lasedeseguridad@gmail.com -o f_practica3 --decrypt f_cifrado3
gpg: encrypted with elg3072 key, ID FC5C1ED7B50AC97E, created 2024-10-31
"Alex Almagro (esta es la clave del ejercicio 3) <lasedeseguridad@gmail.c
om>"
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3#

```



Descifra el fichero.

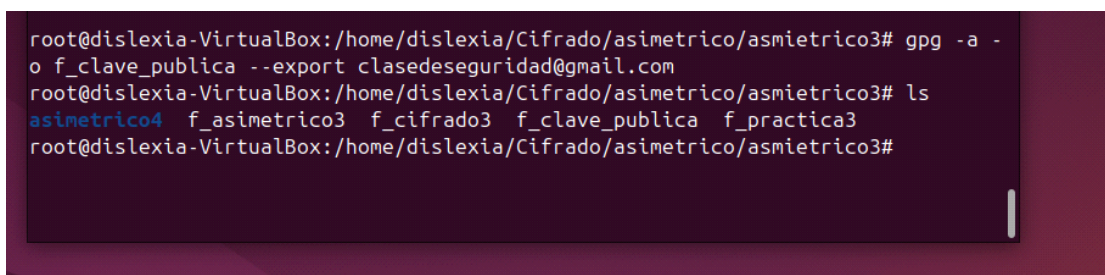
Comprueba que el contenido es el mismo que el original.

Práctica 4 – Cifrado asimétrico

Cifra un fichero con la clave publica proporcionada y envíaselo al dueño del par de claves para que pueda descifrarlo.

Recuerda que para importar la clave pública debes usar el siguiente comando:

```
gpg --import fichero_con_la_clave_publica
```



```
root@dislexia-VirtualBox: /home/dislexia/Cifrado/asimetrico/asmietrico3
GNU nano 7.2 f_nombre *
Alejandro Almagro Torregrosa.

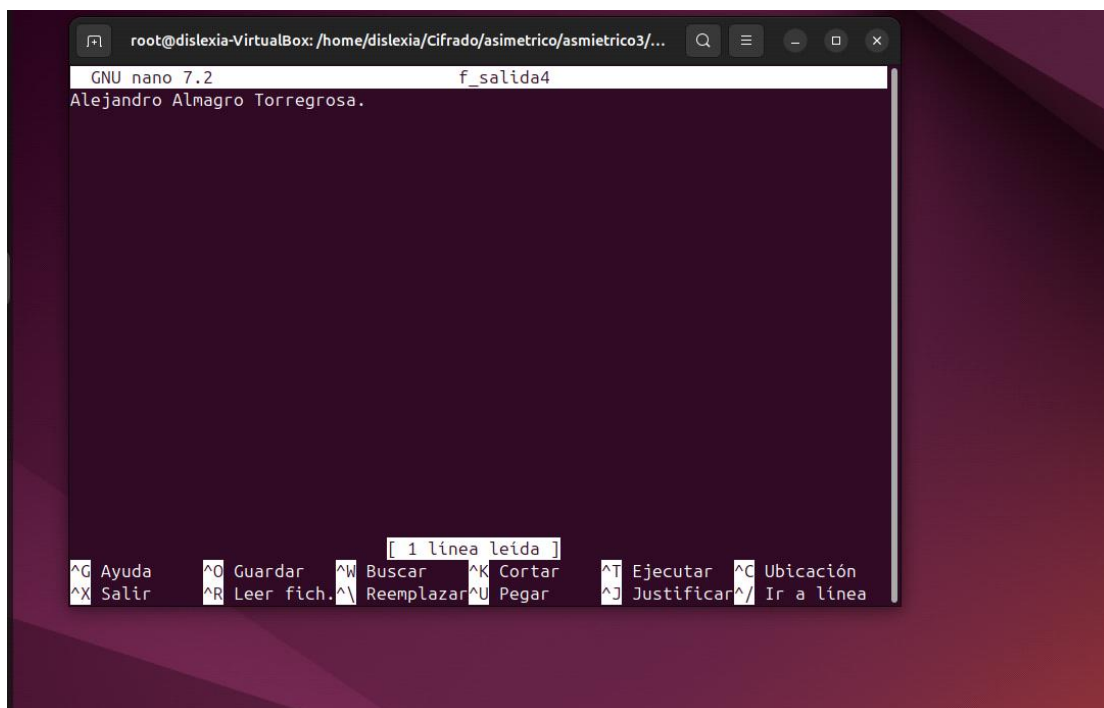
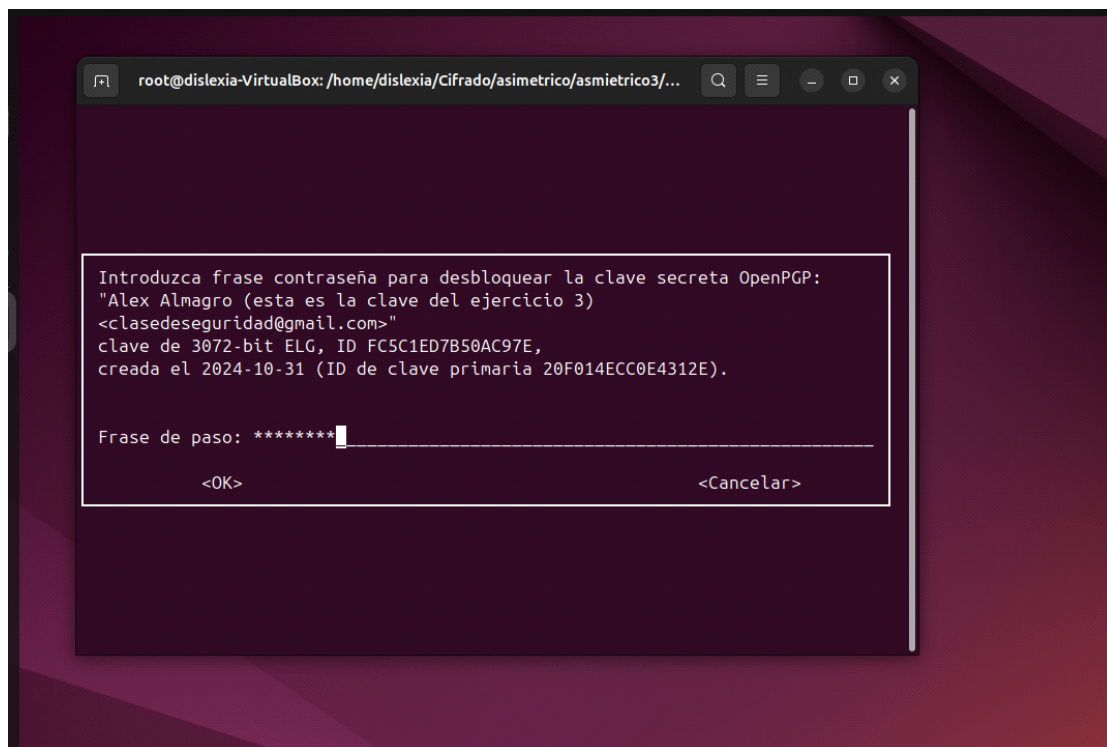
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar      ^J Justificar ^_ Ir a línea

root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3# gpg -r c
lasedeseguridad@gmail.com -a -o f_practica4 --encrypt f_nombre
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3# ls
asimetrico4  f_cifrado3    f_nombre      f_practica4
f_asimetrico3 f_clave_publica f_practica3
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3#
```

Simulación de envío, mediante el comando cp.

```
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3# ls
asimetrico4  f_cifrado3    f_nombre      f_practica4
f_asimetrico3 f_clave_publica f_practica3
root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3# cp f_practica4 f_clave_publica /home/dislexia/Cifrado/asimetrico/asmietrico3/asimetrico4
/

root@dislexia-VirtualBox:/home/dislexia/Cifrado/asimetrico/asmietrico3/asimetrico4# ls
f_clave_publica  f_practica4
```

El documento a cifrar debe tener como mensaje tu nombre y apellidos.

Una vez cifrado mándaselo al dueño del par de claves para que lea el mensaje.