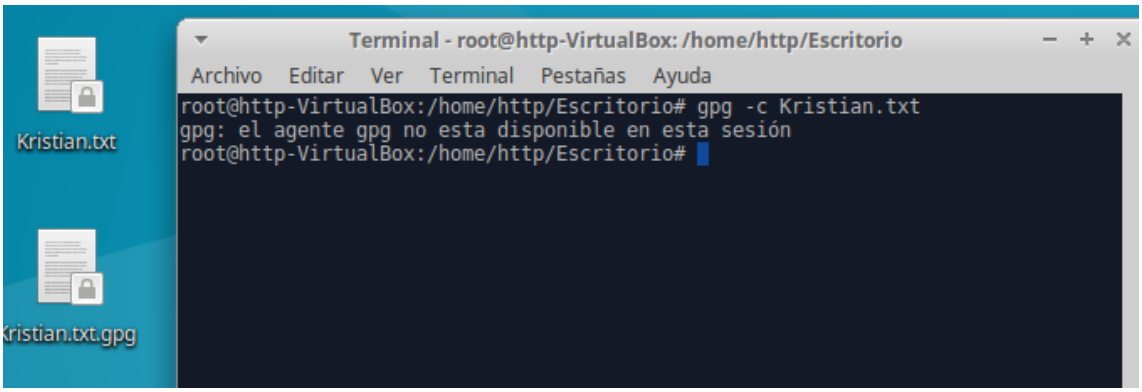
EJERCICIO 1 . CIFRADO SIMETRICO DE UN DOCUMENTO

1. Crea un documento de texto con cualquier editor o utiliza uno del que dispongas.

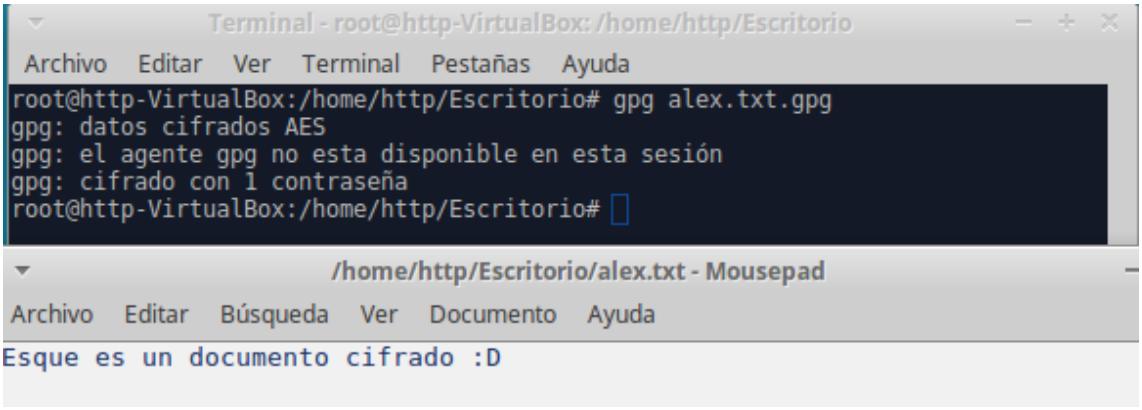
```
root@http-VirtualBox:/home/http/Escritorio# touch Kristian.txt
root@http-VirtualBox:/home/http/Escritorio# nano Kristian.txt
root@http-VirtualBox:/home/http/Escritorio# cat Kristian.txt
Este documento va cifrado ^^
root@http-VirtualBox:/home/http/Escritorio#
```

2. Cifra este documento con alguna contraseña acordada con el compañero de al lado.

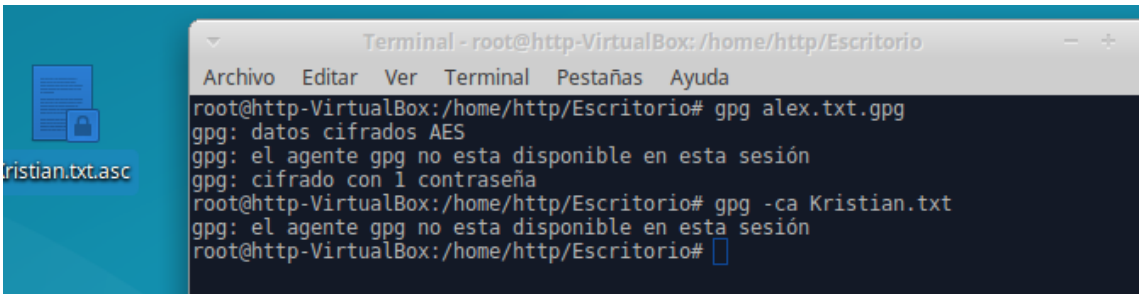


3. Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar.

4. Descifra el documento que te ha hecho llegar tu compañero de al lado.

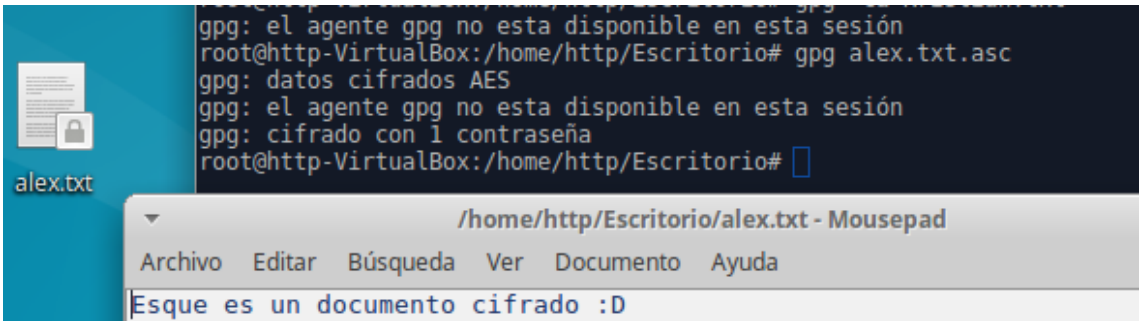


5. Repite el proceso anterior, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.



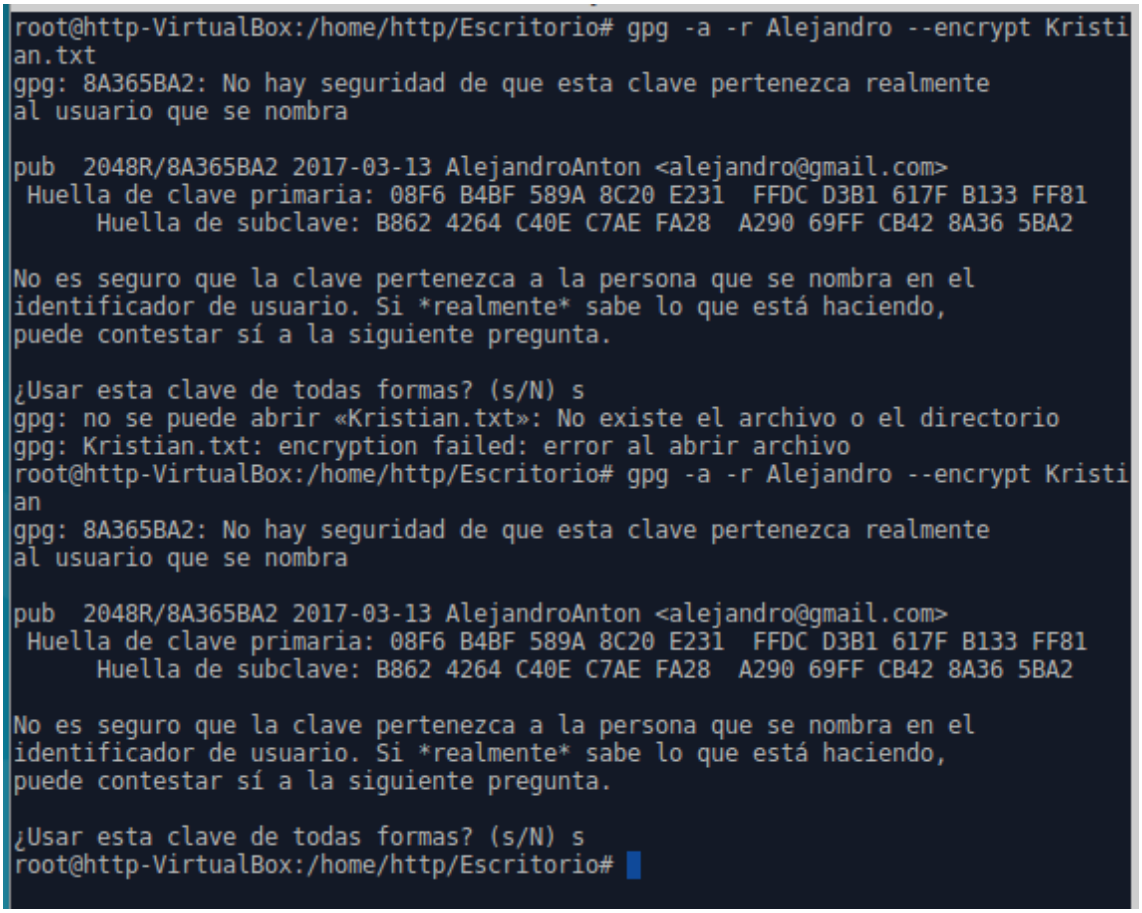
6. Copia y pega el contenido del archivo cifrado anteriormente y envíalo por mail a tu compañero para que lo descifre.

7. Una vez has recibido el mensaje de tu compañero en tu mail, copialo en un archivo de texto para obtener el mensaje original.



EJERCICIO 2 . CREACION DE NUESTRO PAR DE CLAVES PUBLICA-PRIVADA

1. Siguiendo las indicaciones de este epígrafe, crea tu par de claves pública y privada. La clave que vas a crear tendrá una validez de 1 mes.ç



2. Recuerda el ID de usuario de tu clave y la contraseña de paso utilizada. Anotala en un lugar seguro si lo consideras necesario.

Kris Tomas y contraseña 123

EJERCICIO 3 . EXPORTAR E IMPORTAR CLAVES PUBLICAS

1. Exporta tu clave pública en formato ASCII y guardalo en un archivo nombre_apellido.asc y envíalo a un compañero/a.

```
root@http-VirtualBox:/home/http/Escritorio# gpg -a --export -o KristianKey.asc K
ris Tomas
```

2. Importa las claves públicas recibidas de vuestros/as compañeros/as.

```
root@http-VirtualBox:/home/http/Escritorio# gpg --import alexkey.asc
gpg: clave B133FF81: clave pública "AlejandroAnton <alejandro@gmail.com>" import
ada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1  (RSA: 1)
root@http-VirtualBox:/home/http/Escritorio#
```

3. Comprueba que las claves se han incluido correctamente en vuestro keyring

```
root@http-VirtualBox:/home/http/Escritorio# gpg -kv
/root/.gnupg/pubring.gpg
------------------------
pub   2048R/8DDDFA4E 2017-03-13 [[caduca: 2017-04-12]]
uid                  Tomas <lala@gmail.com>
sub   2048R/3F2D99DC 2017-03-13 [[caduca: 2017-04-12]]

pub   2048R/B133FF81 2017-03-13 [[caduca: 2017-04-12]]
uid                  AlejandroAnton <alejandro@gmail.com>
sub   2048R/8A365BA2 2017-03-13 [[caduca: 2017-04-12]]

root@http-VirtualBox:/home/http/Escritorio#
```

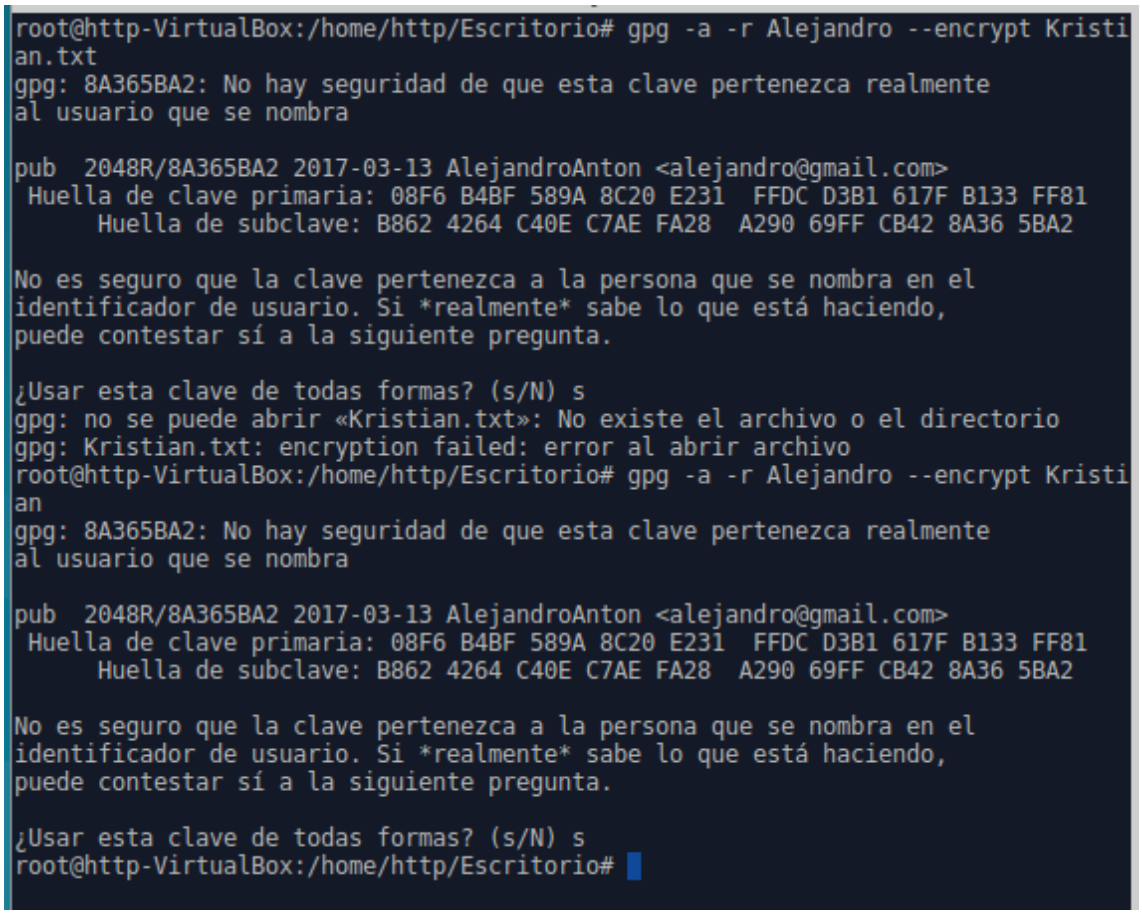
EJERCICIO 4 . CIFRADO Y DESCIFRADO DE UN DOCUMENTO

1. Cifraremos un archivo cualquiera y lo remitiremos por email a uno de nuestros compañeros que nos proporcionó su clave pública.

2. Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos.

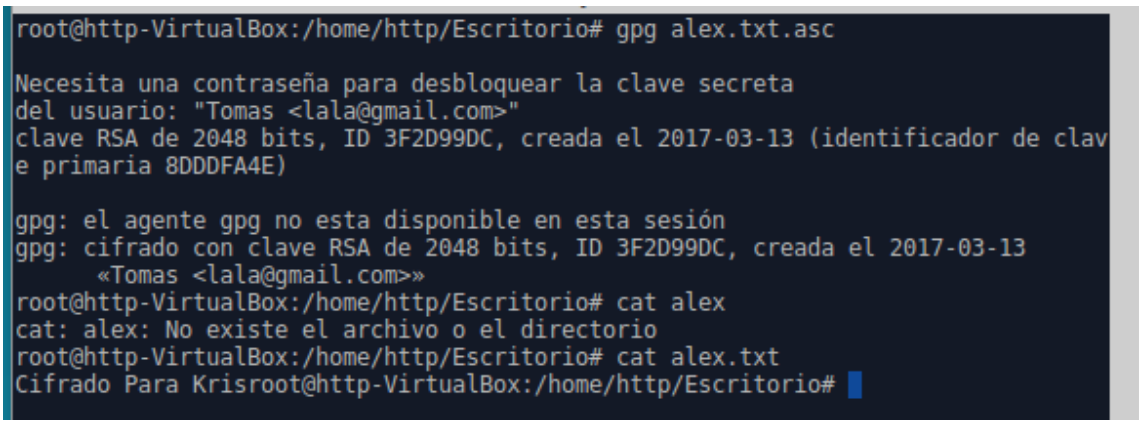
3. Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.

4. Por último, enviaremos el documento cifrado a alguien que no estaba en la lista de destinatarios y comprobaremos que este usuario no podrá descifrar este archivo.



EJERCICIO 5. FIRMA DIGITAL DE UN DOCUMENTO

1. Crea la firma digital de un archivo de texto cualquiera y envíale éste junto al documento con la firma a un compañero.



2. Verifica que la firma recibida del documento es correcta.

3. Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.