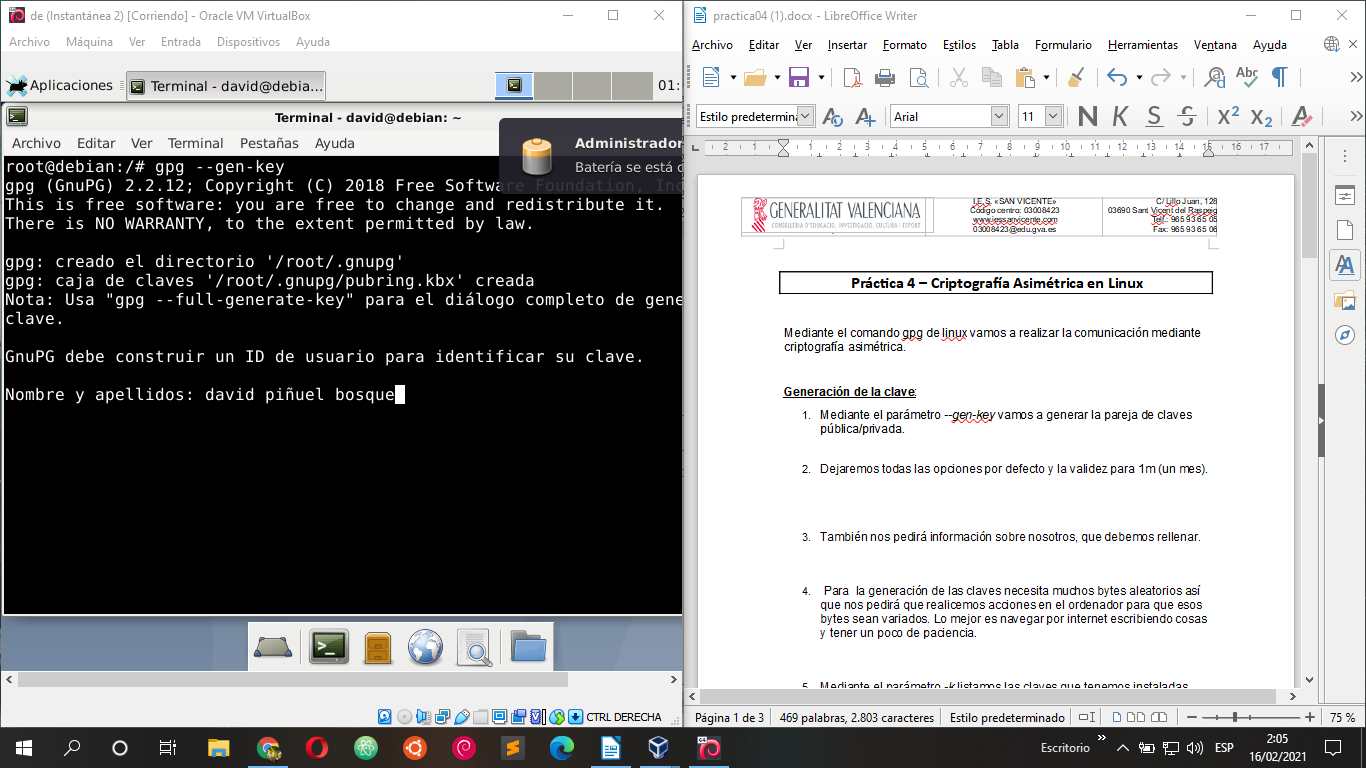
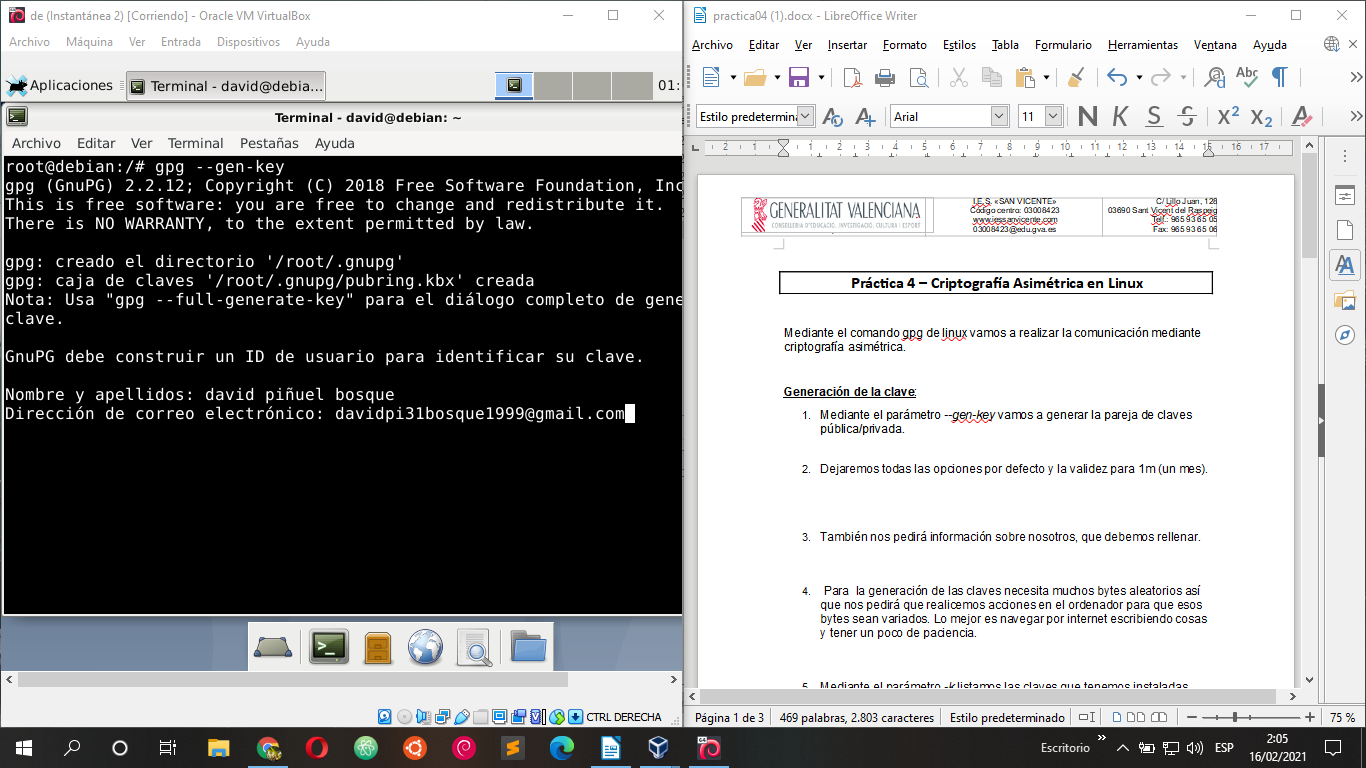
**Práctica 4 – Criptografía Asimétrica en Linux**

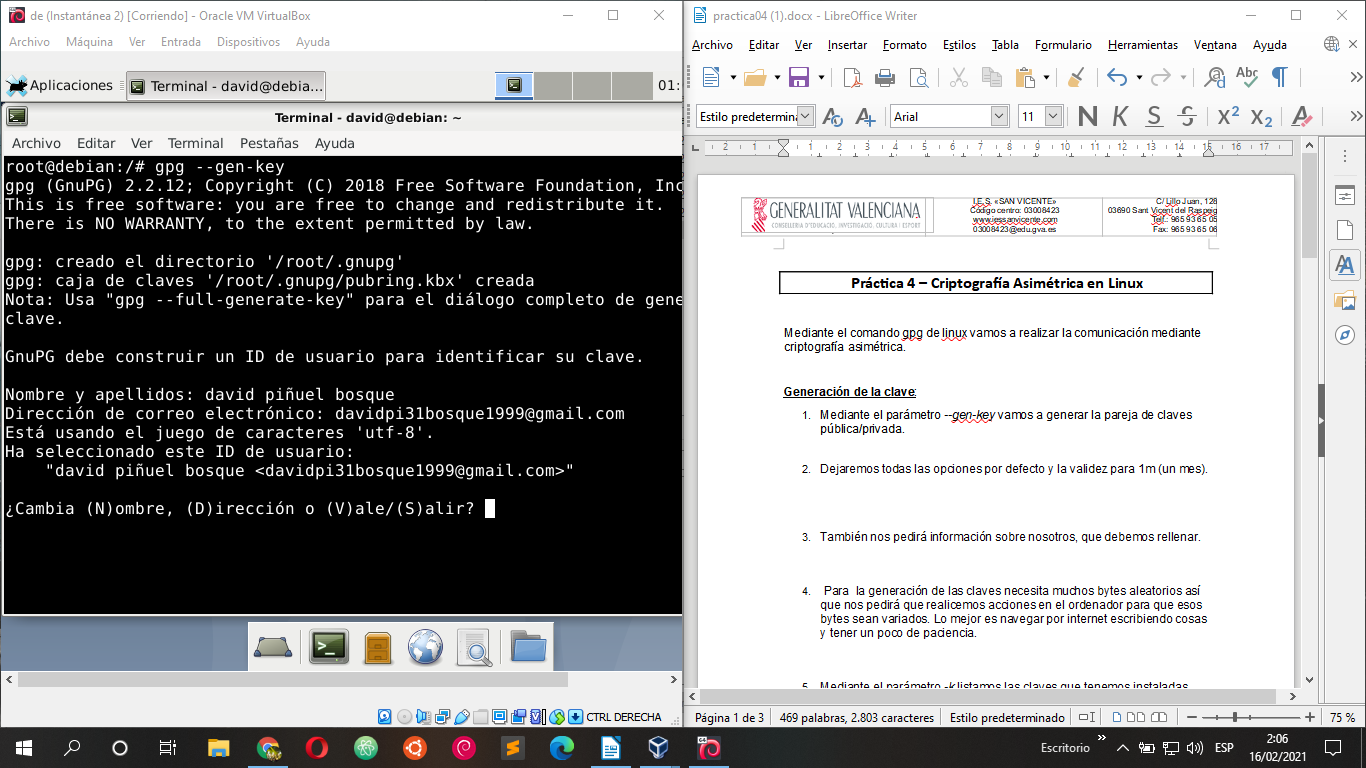
Mediante el comando gpg de linux vamos a realizar la comunicación mediante criptografía asimétrica.

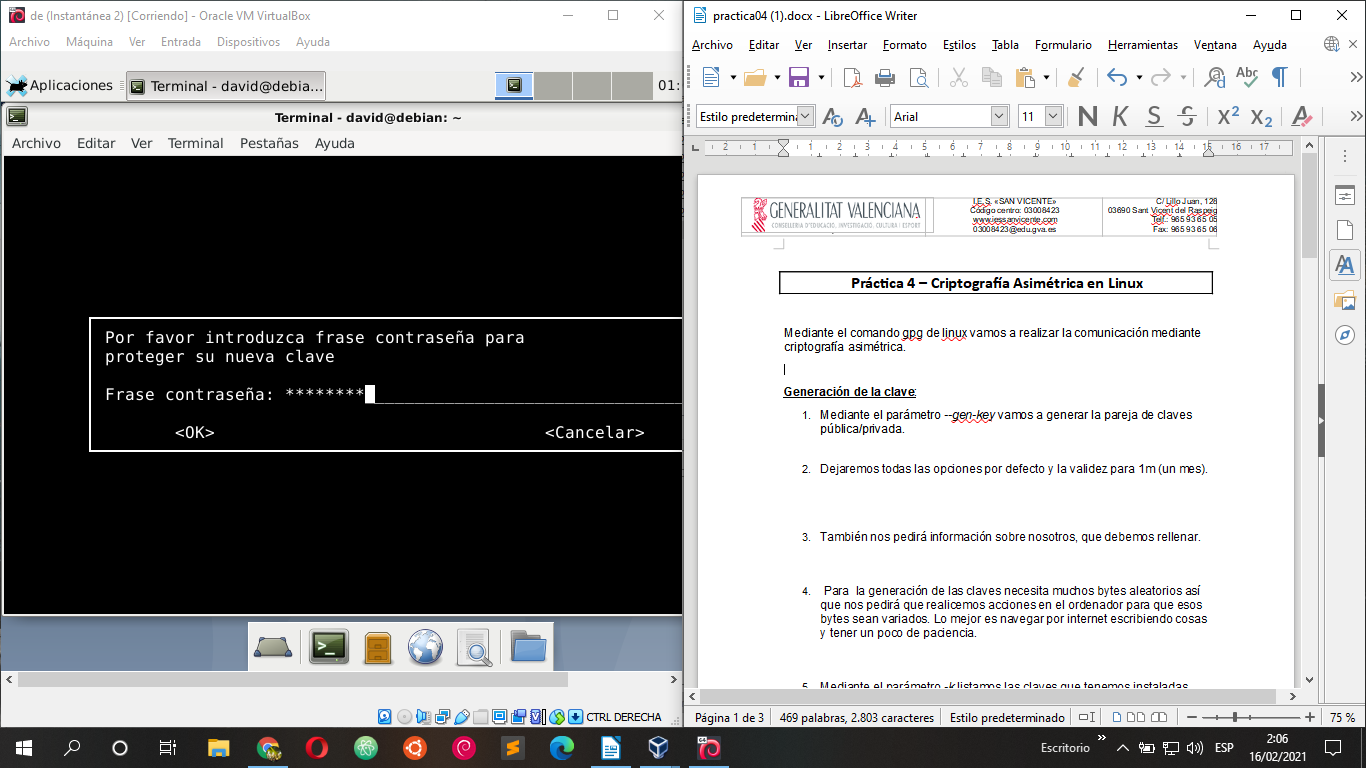
**Generación de la clave**:

1. Mediante el parámetro *--gen-key* vamos a generar la pareja de claves pública/privada.

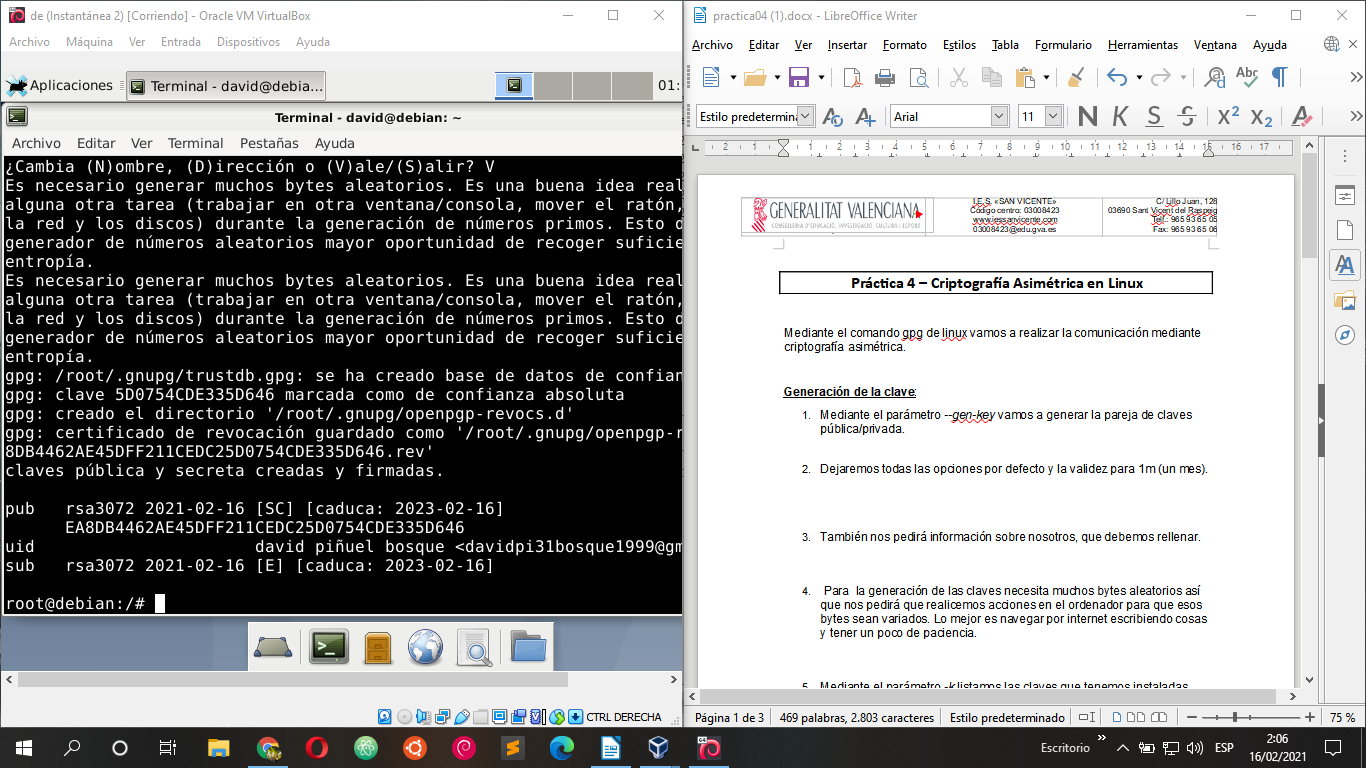




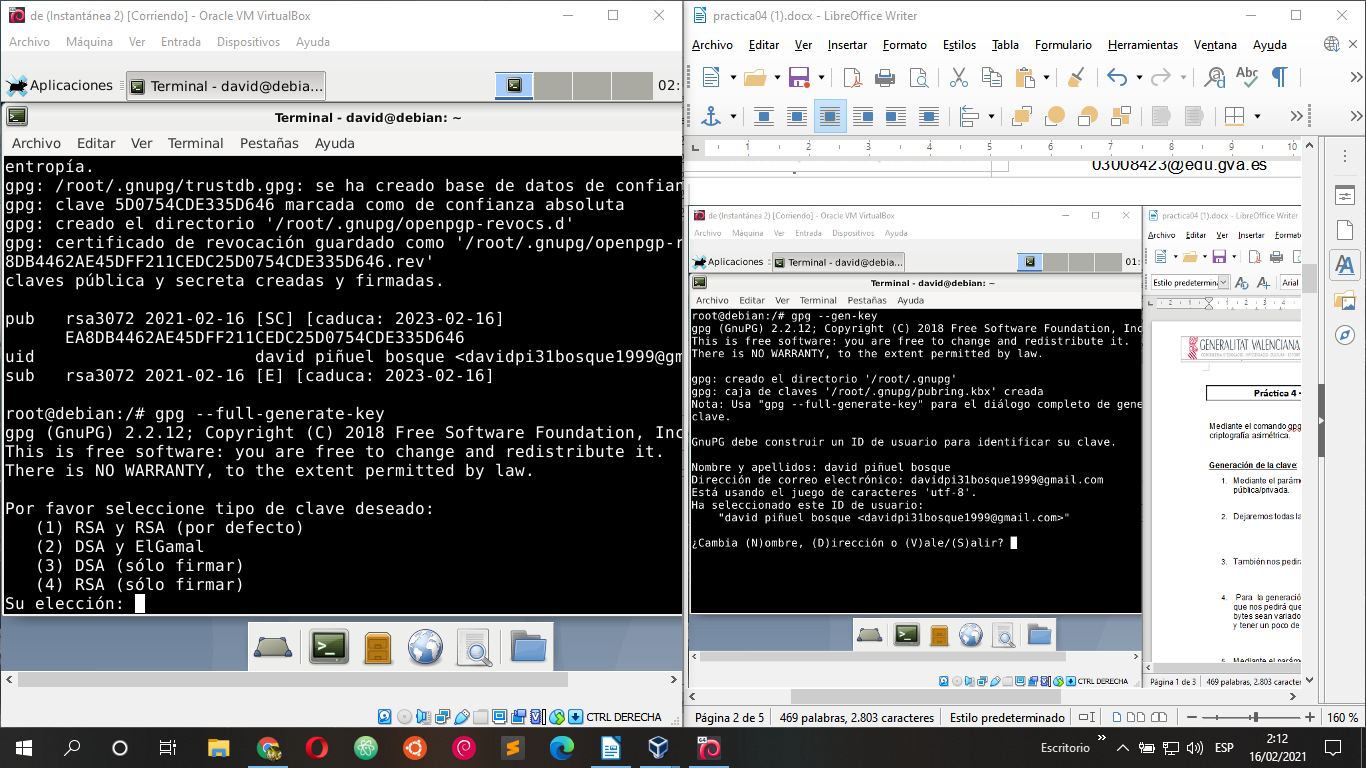


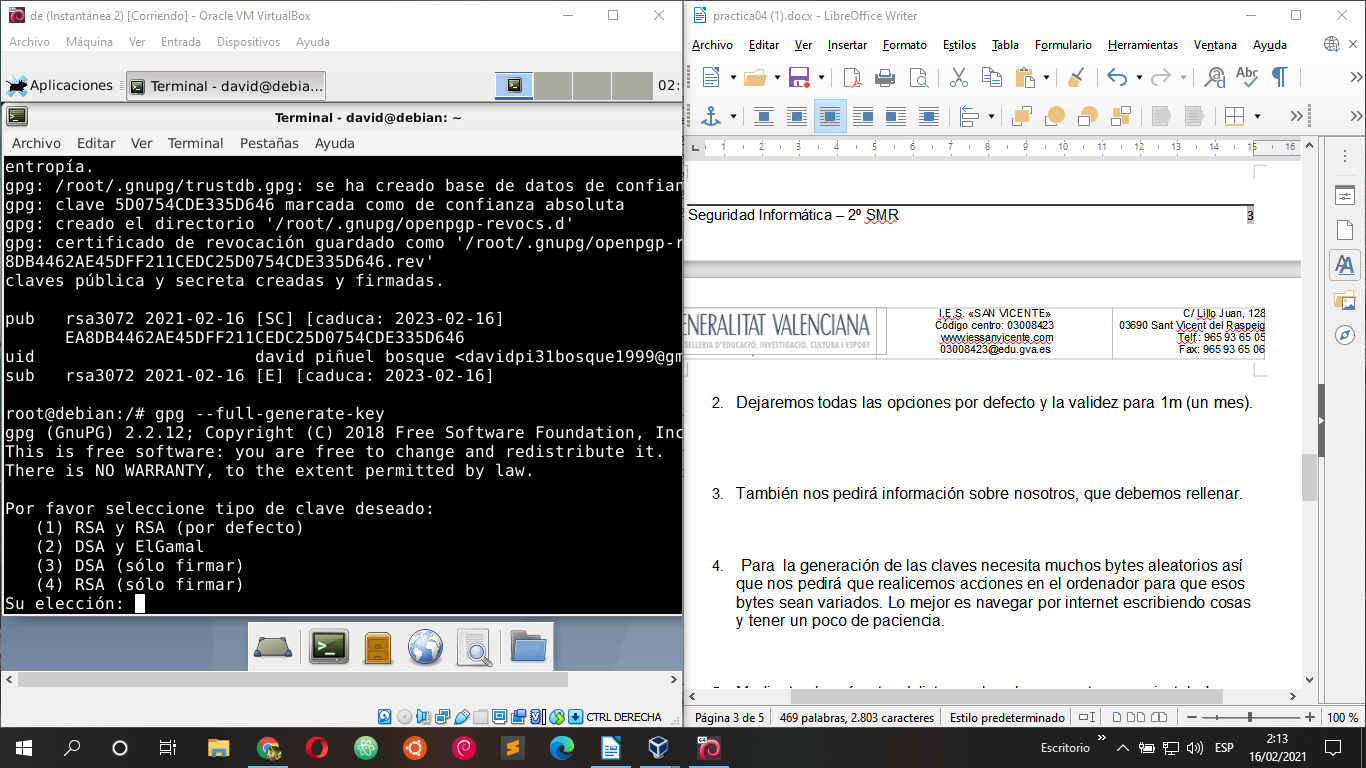


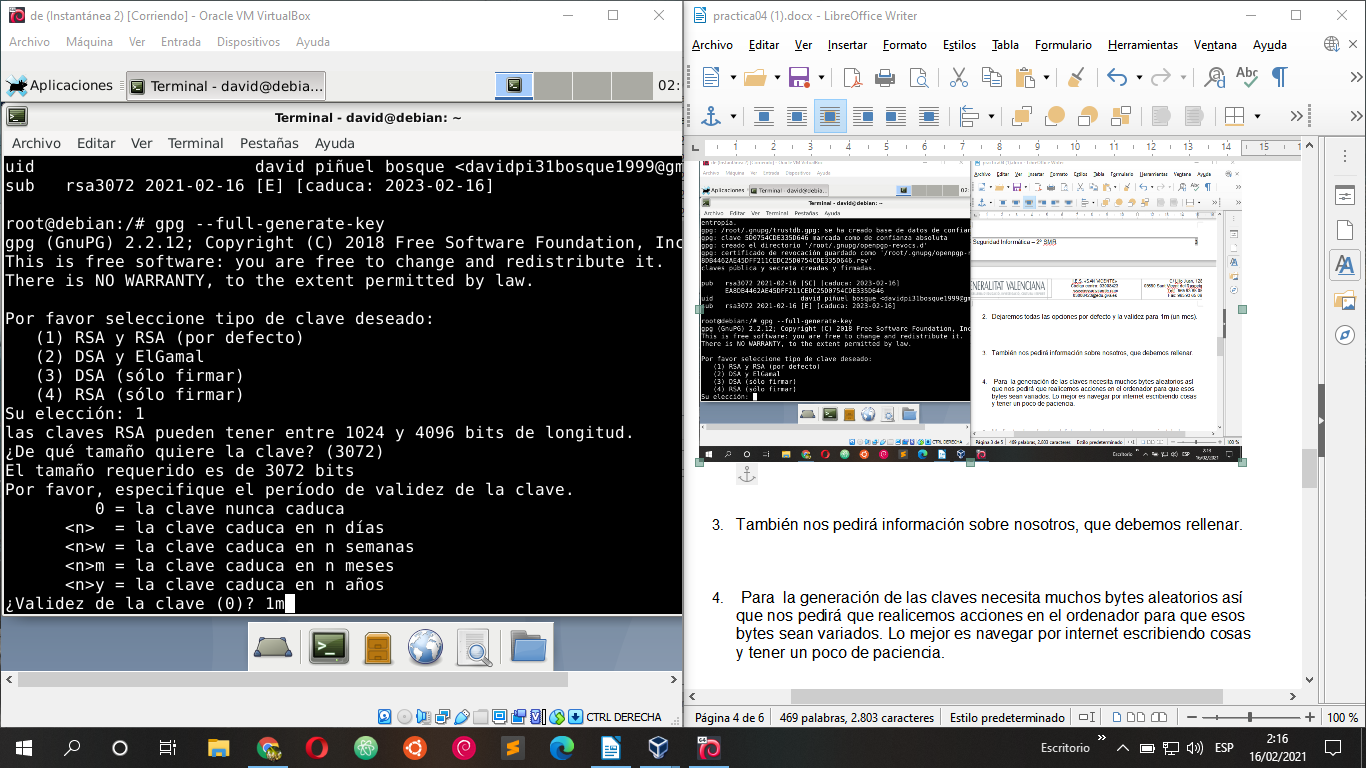




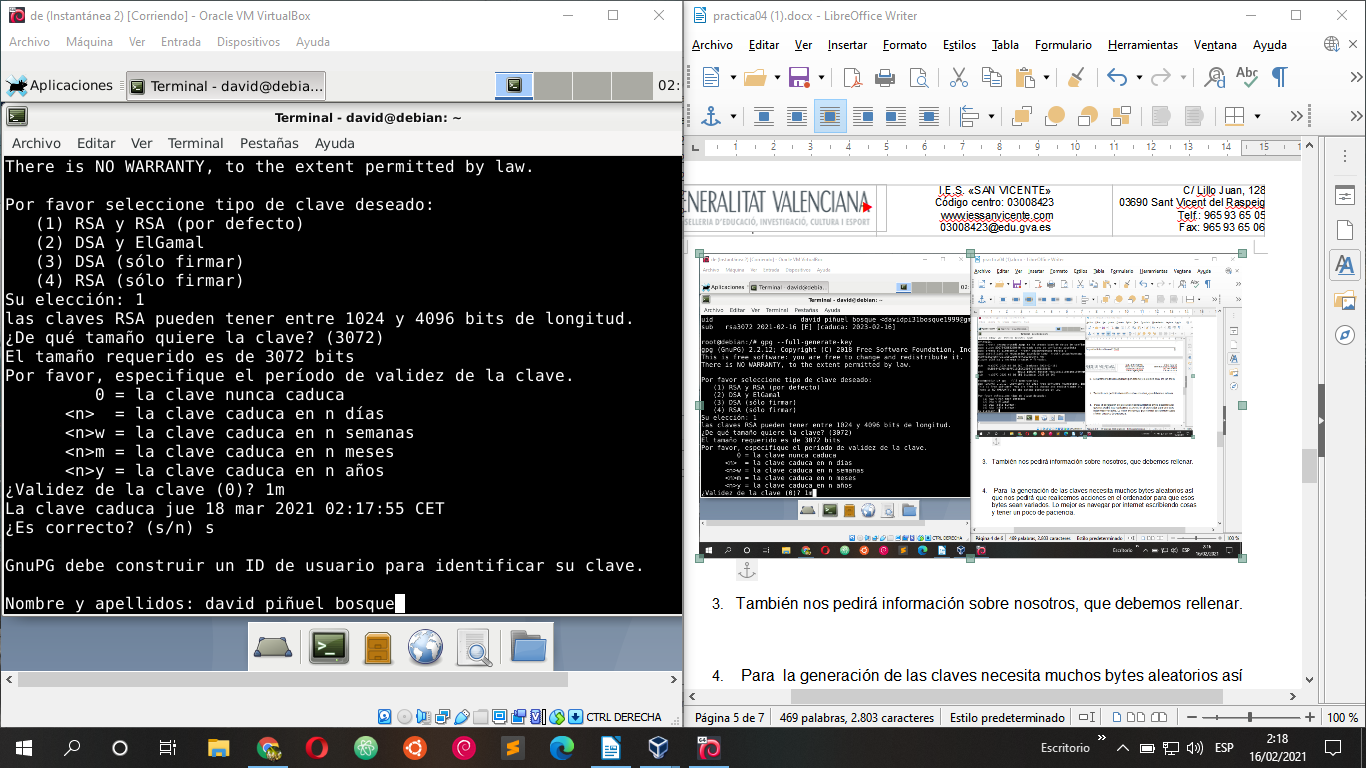
1. Dejaremos todas las opciones por defecto y la validez para 1m (un mes).

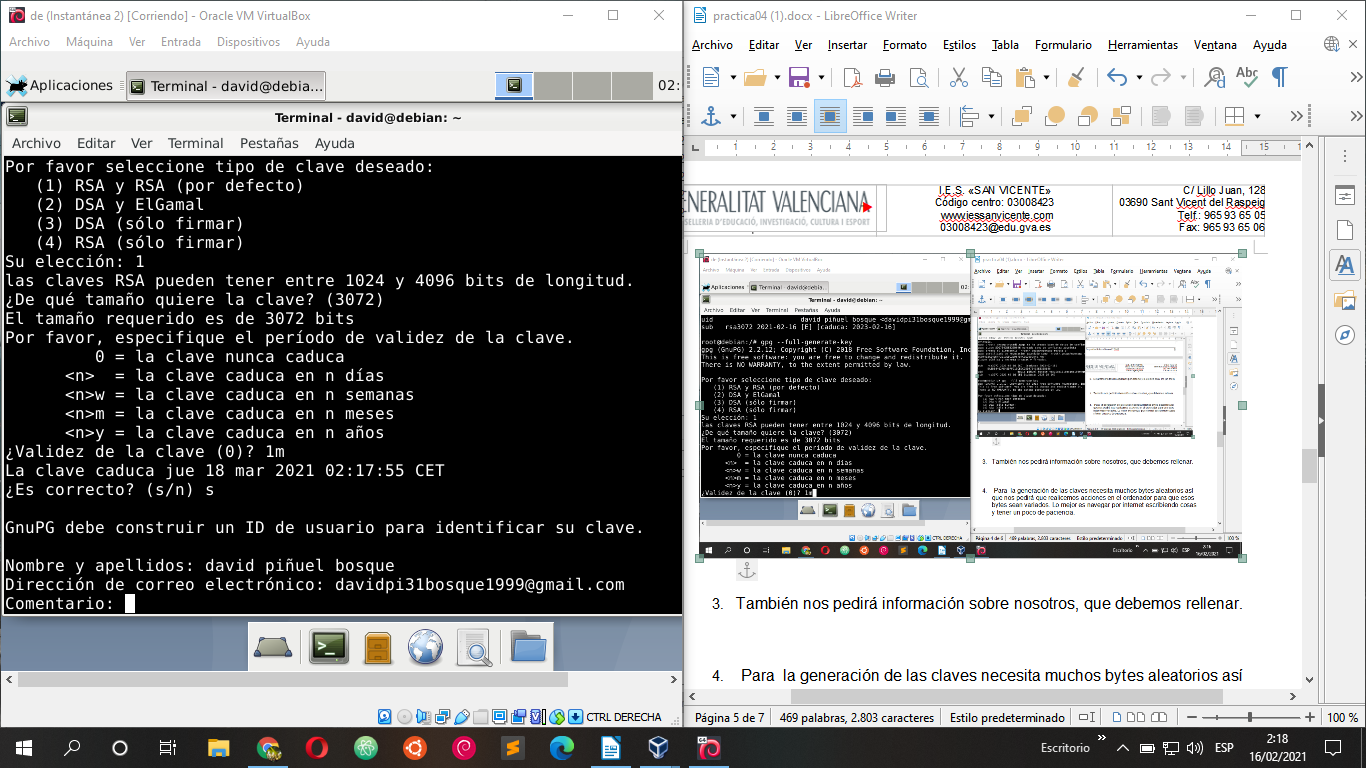




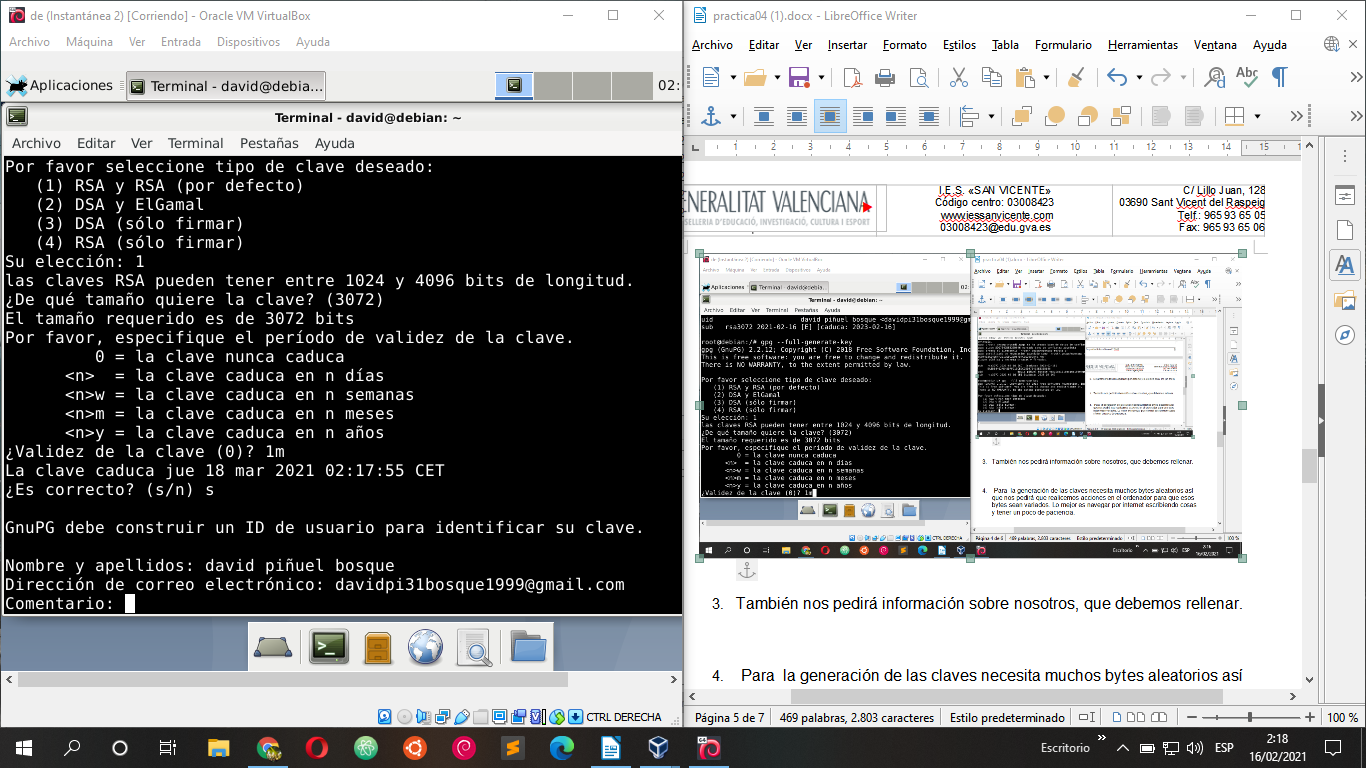


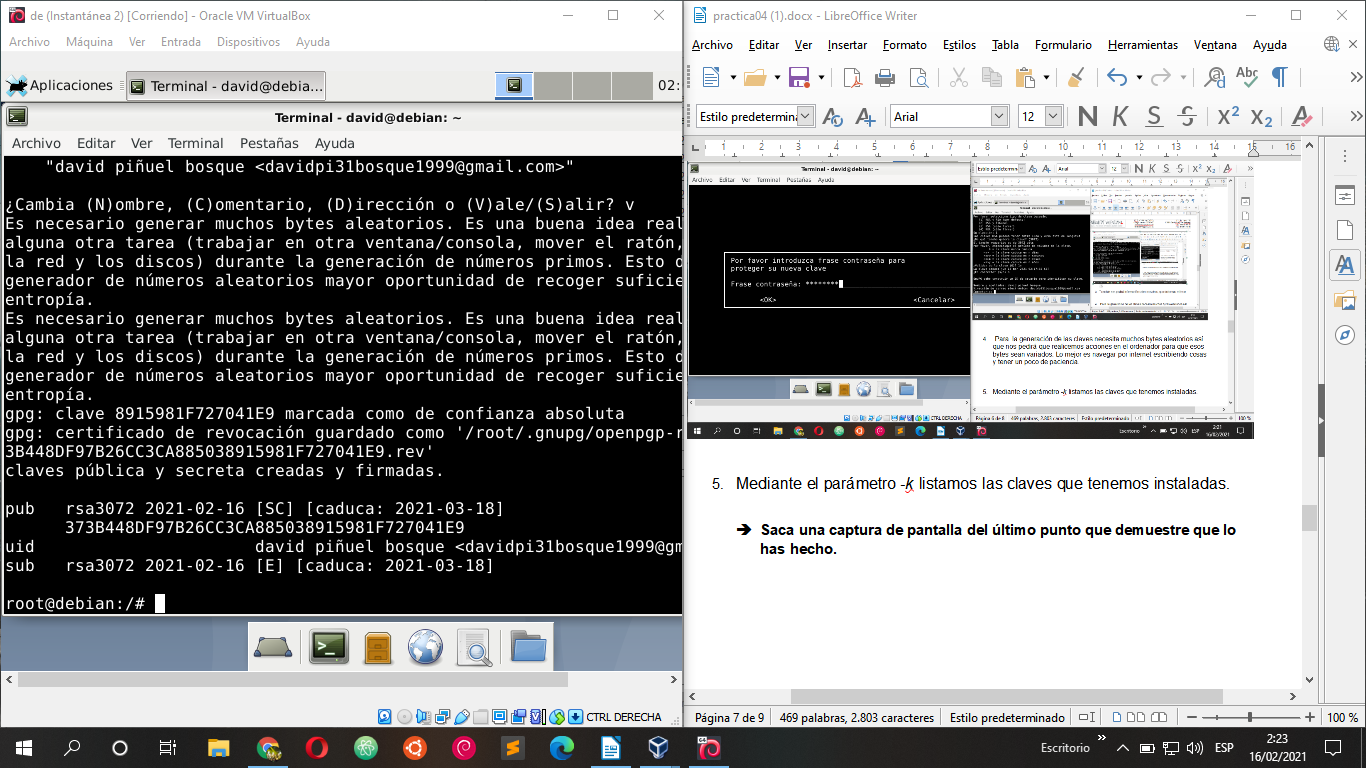
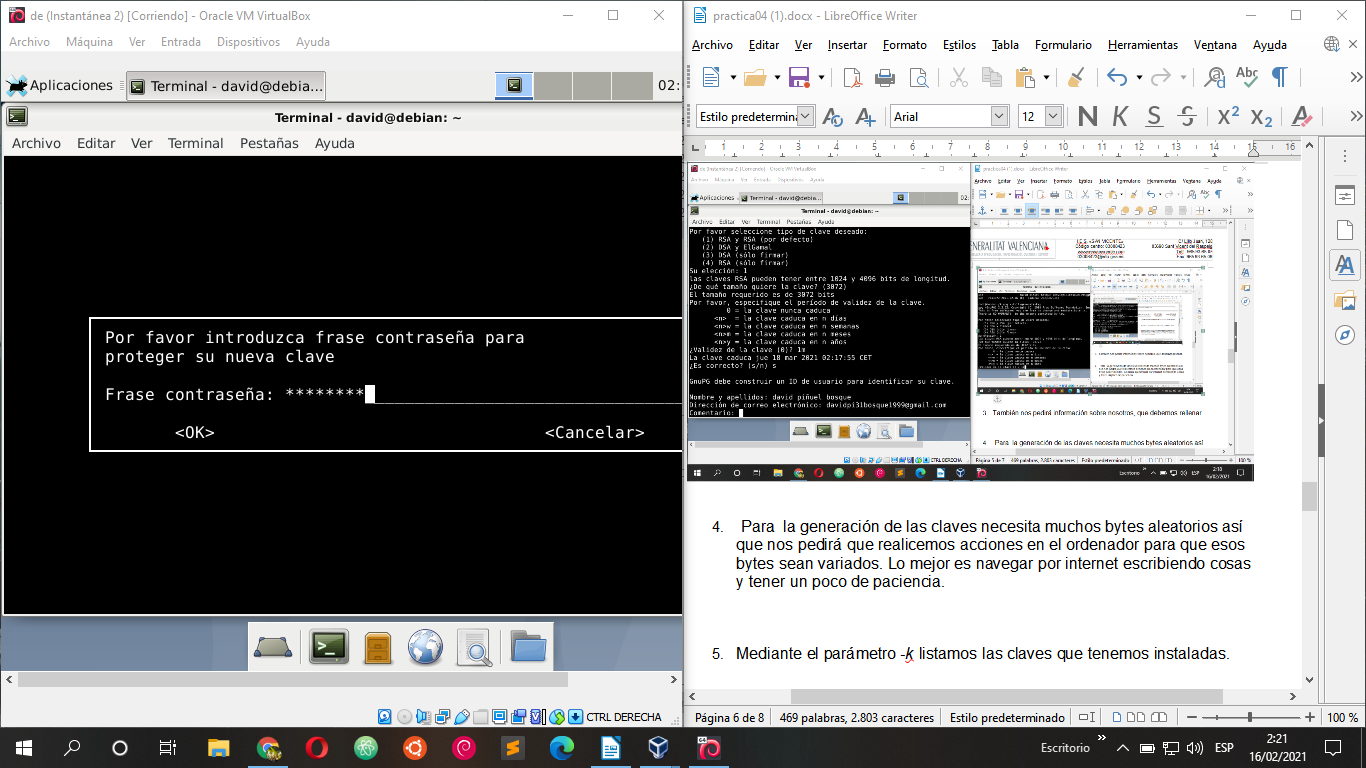
1. También nos pedirá información sobre nosotros, que debemos rellenar.



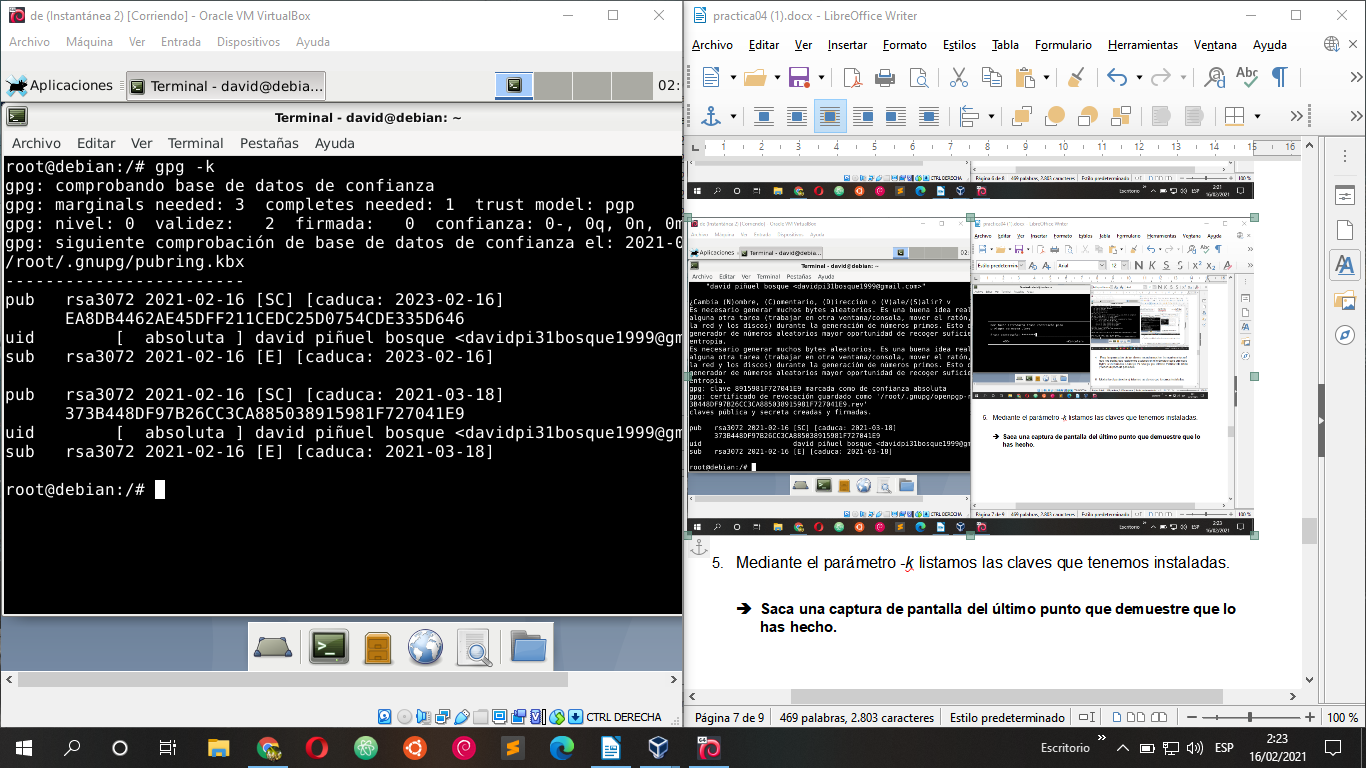


1. Para la generación de las claves necesita muchos bytes aleatorios así que nos pedirá que realicemos acciones en el ordenador para que esos bytes sean variados. Lo mejor es navegar por internet escribiendo cosas y tener un poco de paciencia.





1. Mediante el parámetro *-k* listamos las claves que tenemos instaladas.

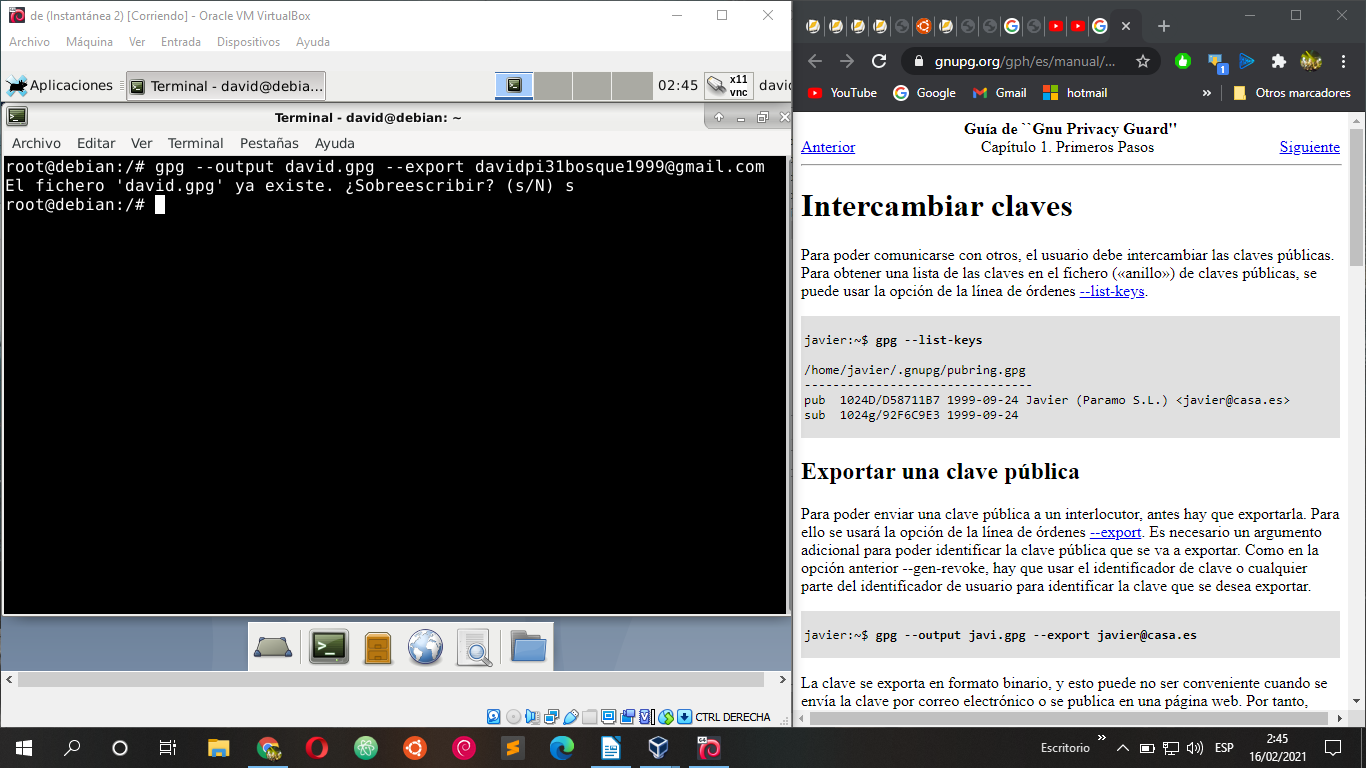
* **Saca una captura de pantalla del último punto que demuestre que lo has h****echo.**

**Intercambio de claves**:

1. Primero debemos exportar nuestra clave pública para poder pasarla a las personas con las que nos queramos comunicar. Se realizará con el comando –export

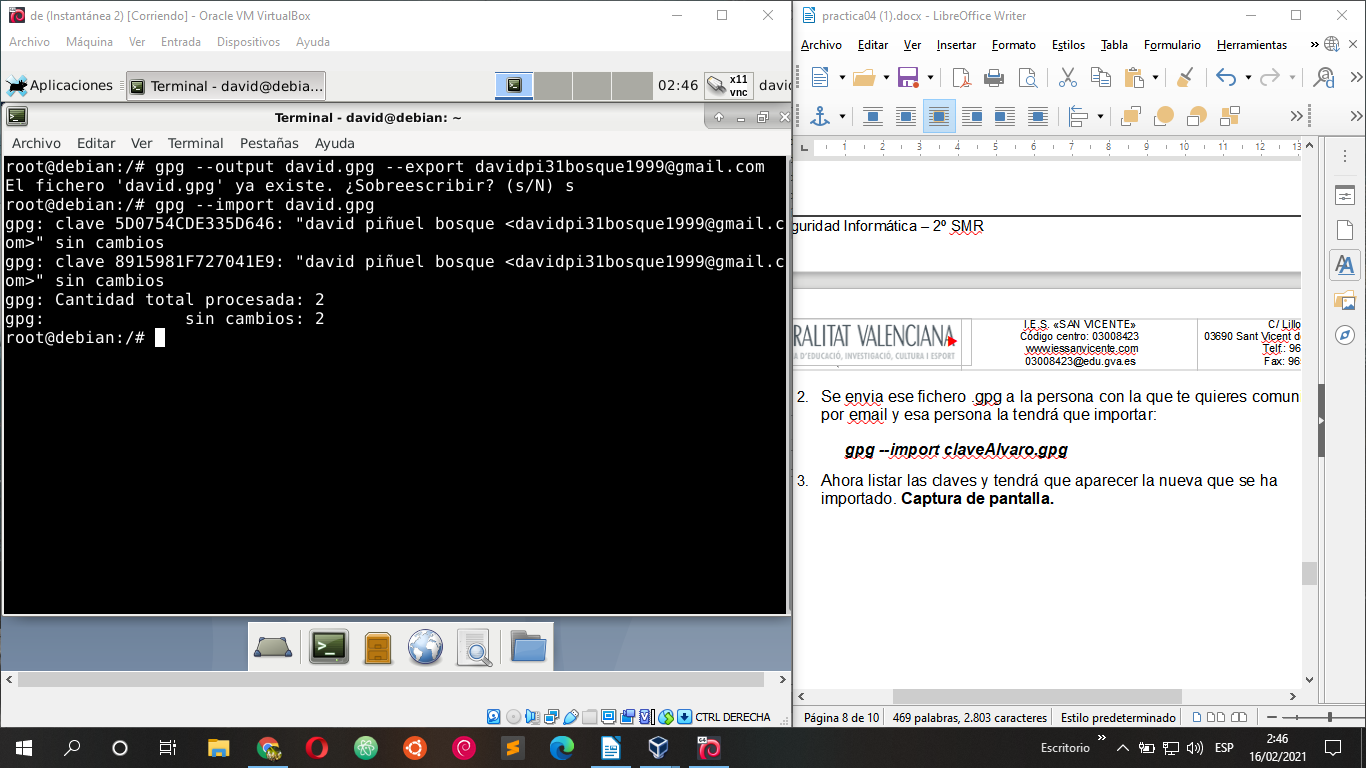
***gpg --output claveAlvaro.gpg --export IDClave***

**NOTA: la opción –armor sirve para exportar la clave en ASCII**

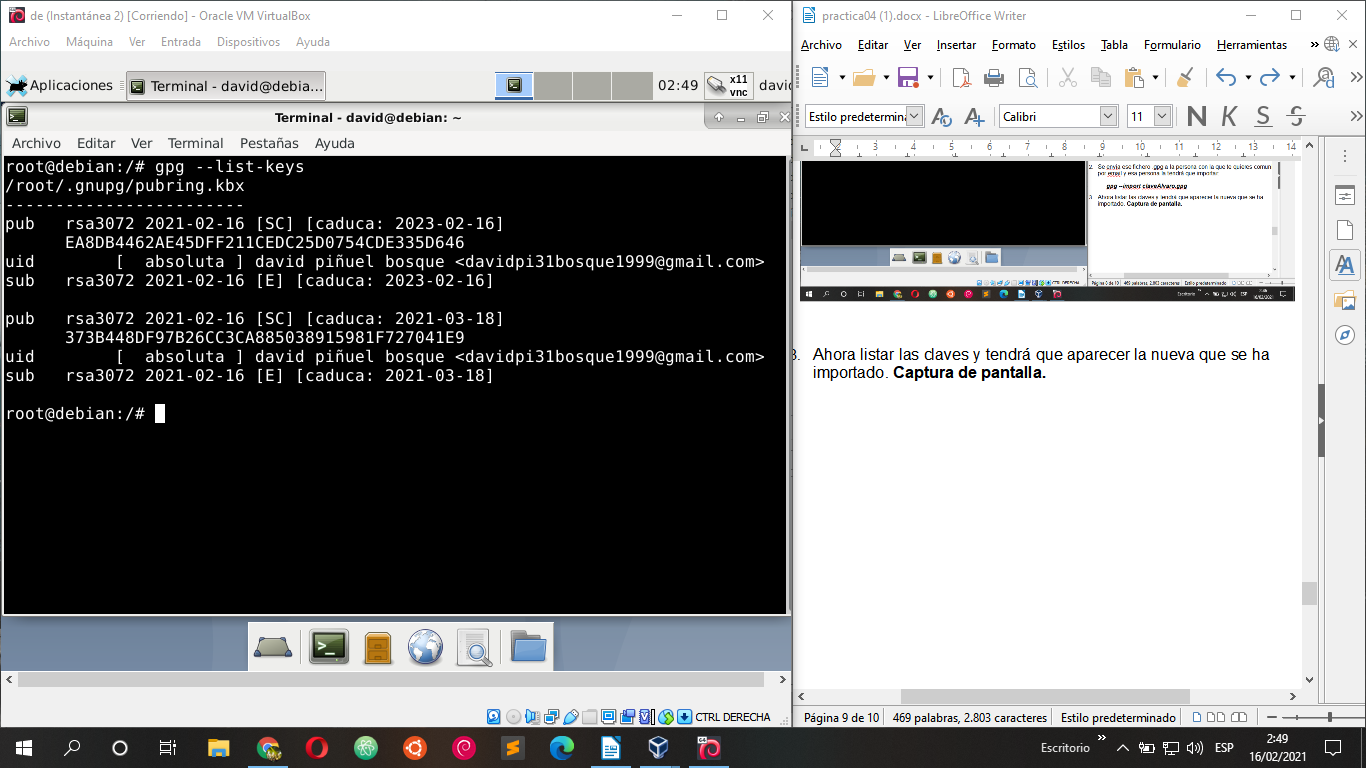
******

1. Se envia ese fichero .gpg a la persona con la que te quieres comunicar por email y esa persona la tendrá que importar:

***gpg --import claveAlvaro.gpg***



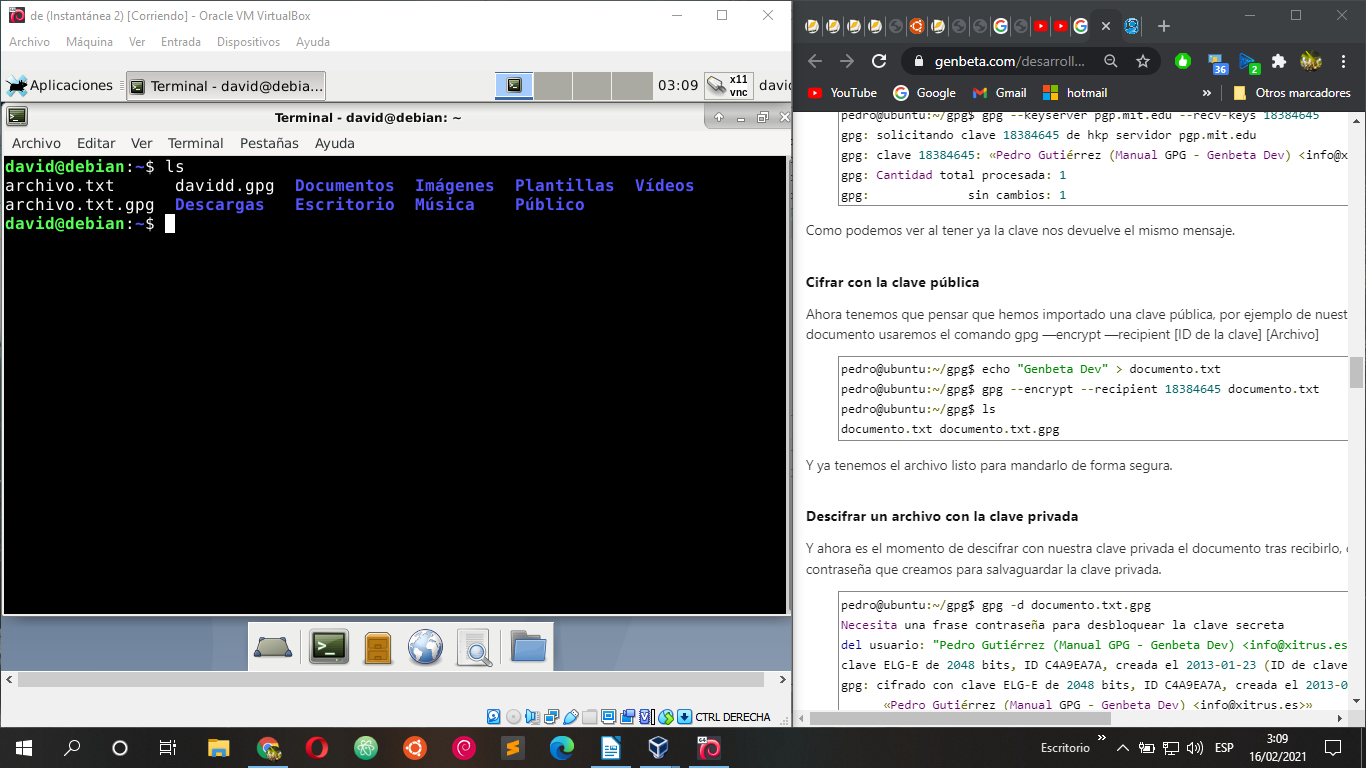
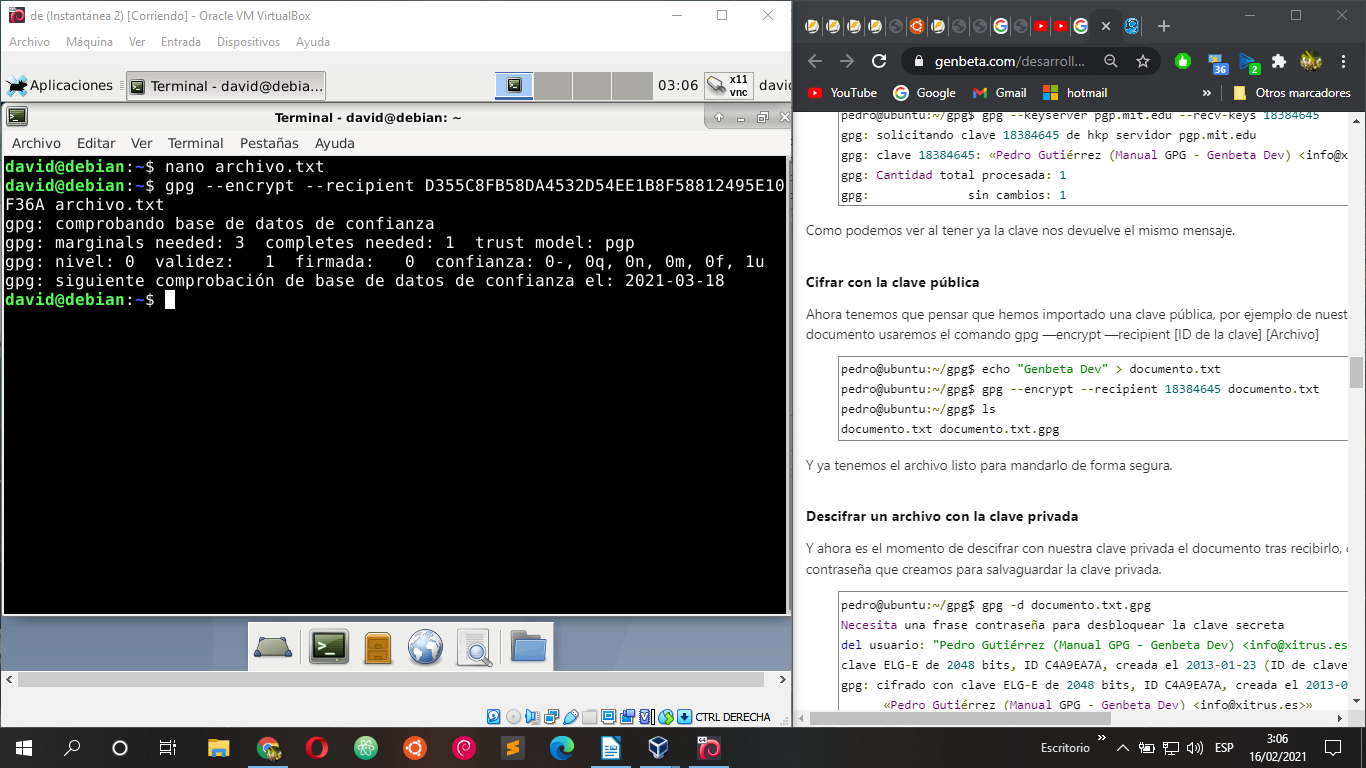
1. Ahora listar las claves y tendrá que aparecer la nueva que se ha importado. **Captura de pantalla.**



**Cifrar con la clave pública**

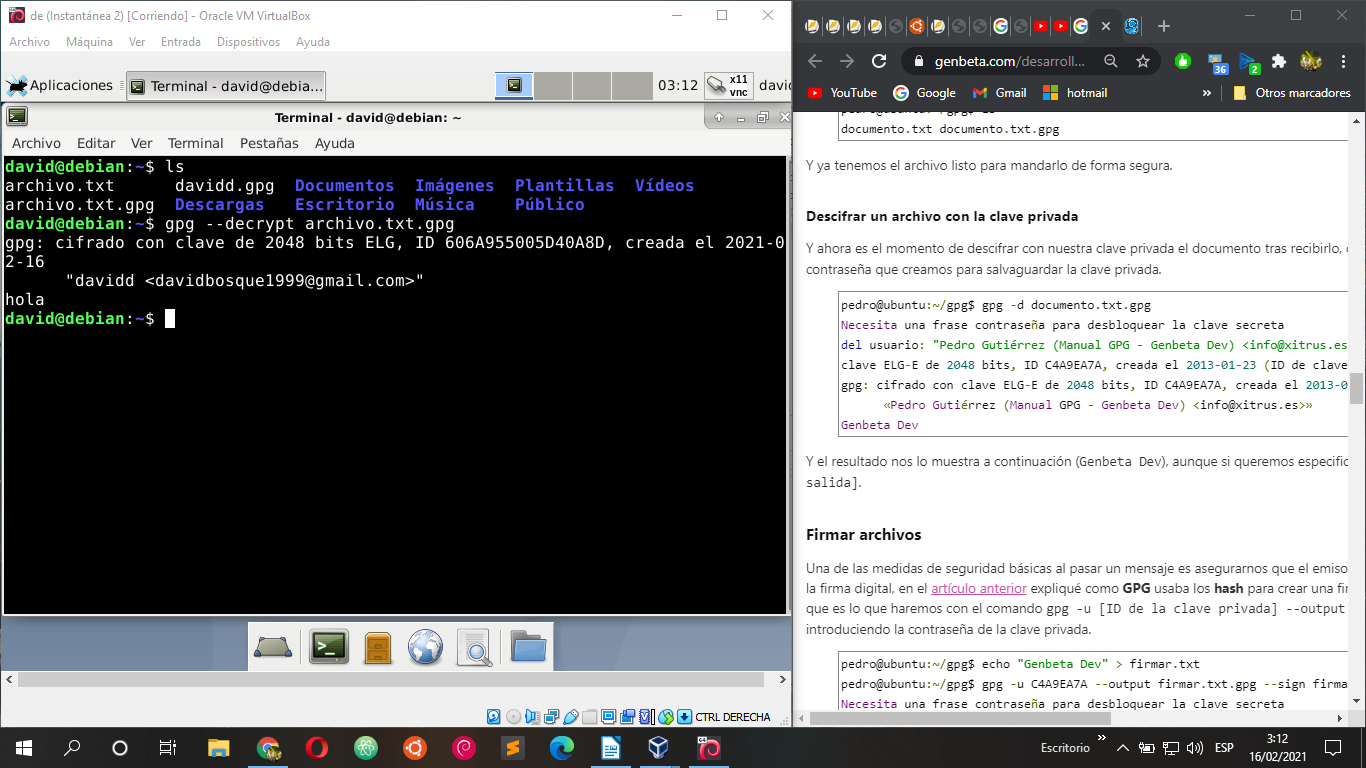
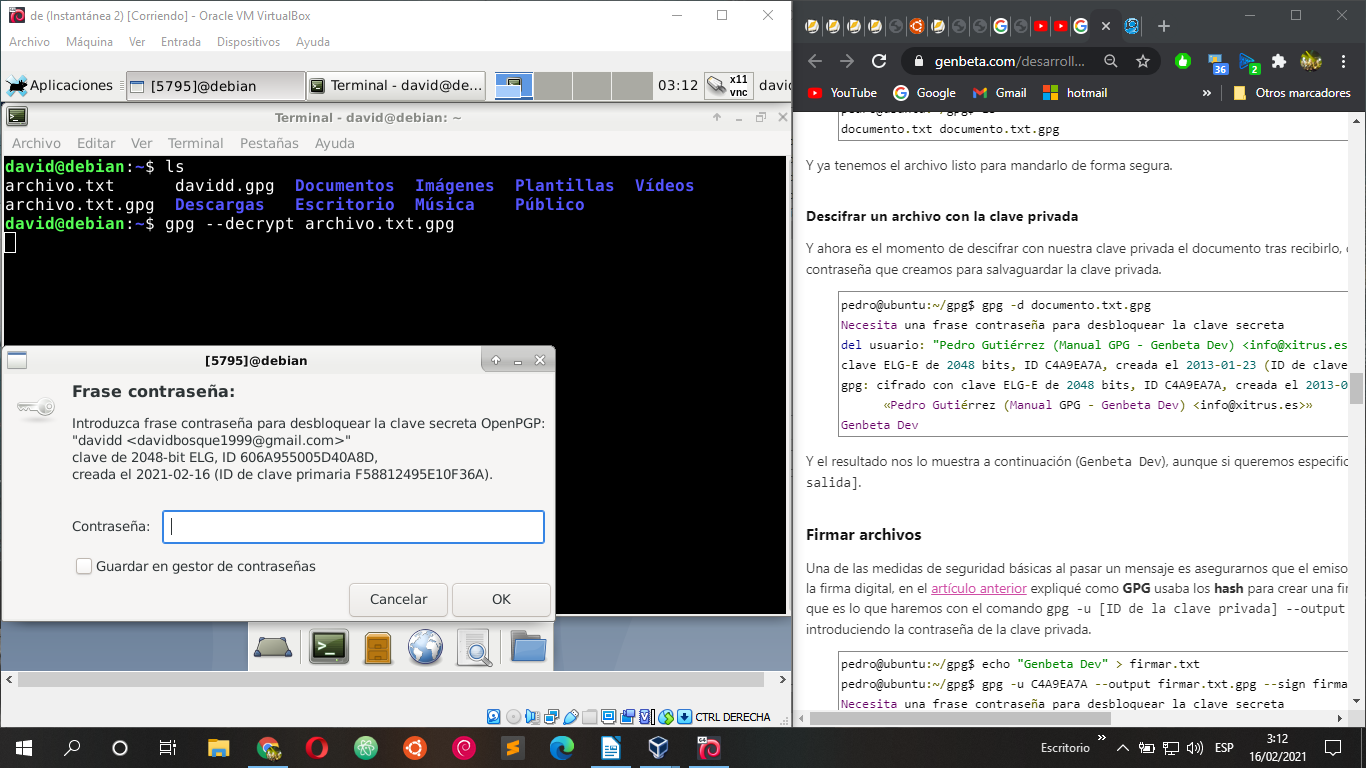
1. Ahora encriptaremos un fichero usando la clave pública que nos ha mandado el compañero con el siguiente comando:

***gpg --encrypt --recipient IDClave documento.txt***

******

1. Ahora vamos a desencriptar el fichero que nos ha mandado el compañero. Para ello usamos:

***gpg -d [Archivo encriptado] –o [Fichero de salida]***

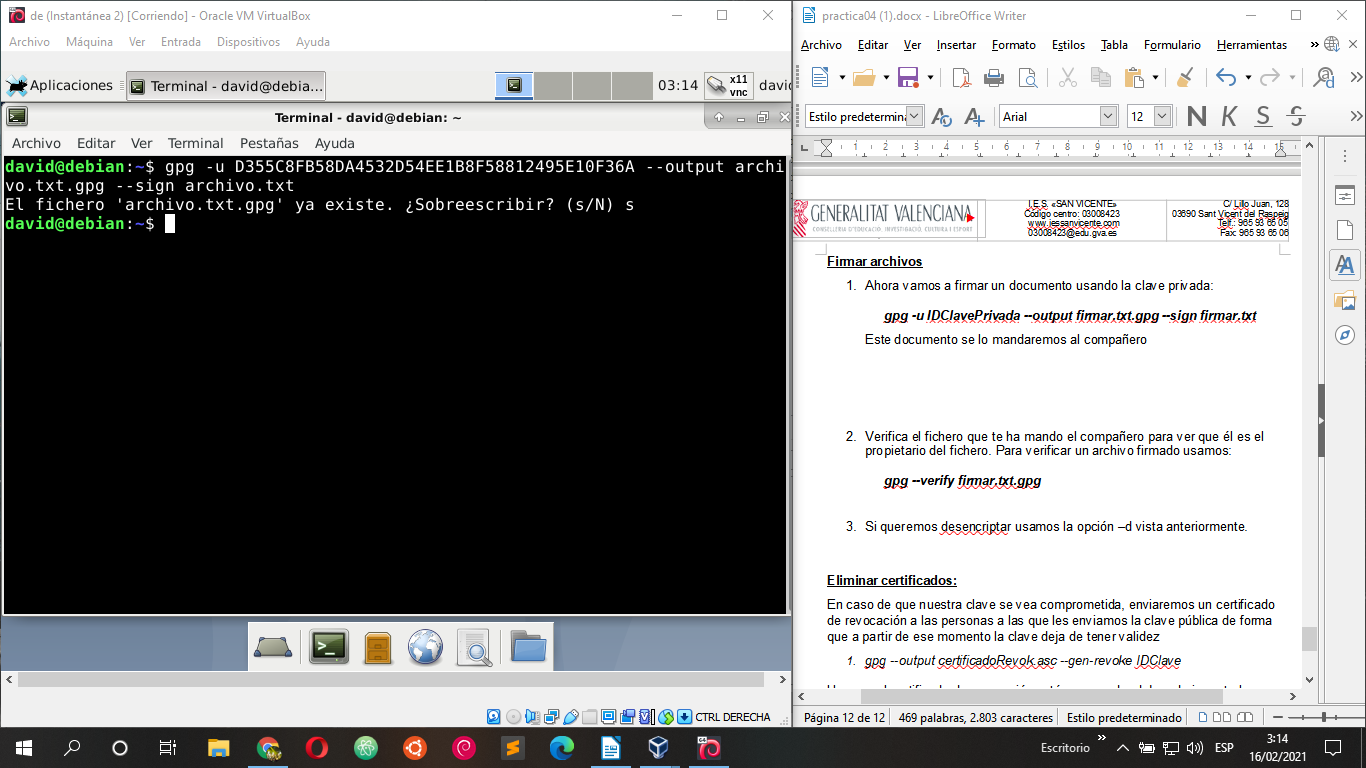
******

**Firmar archivos**

1. Ahora vamos a firmar un documento usando la clave privada:

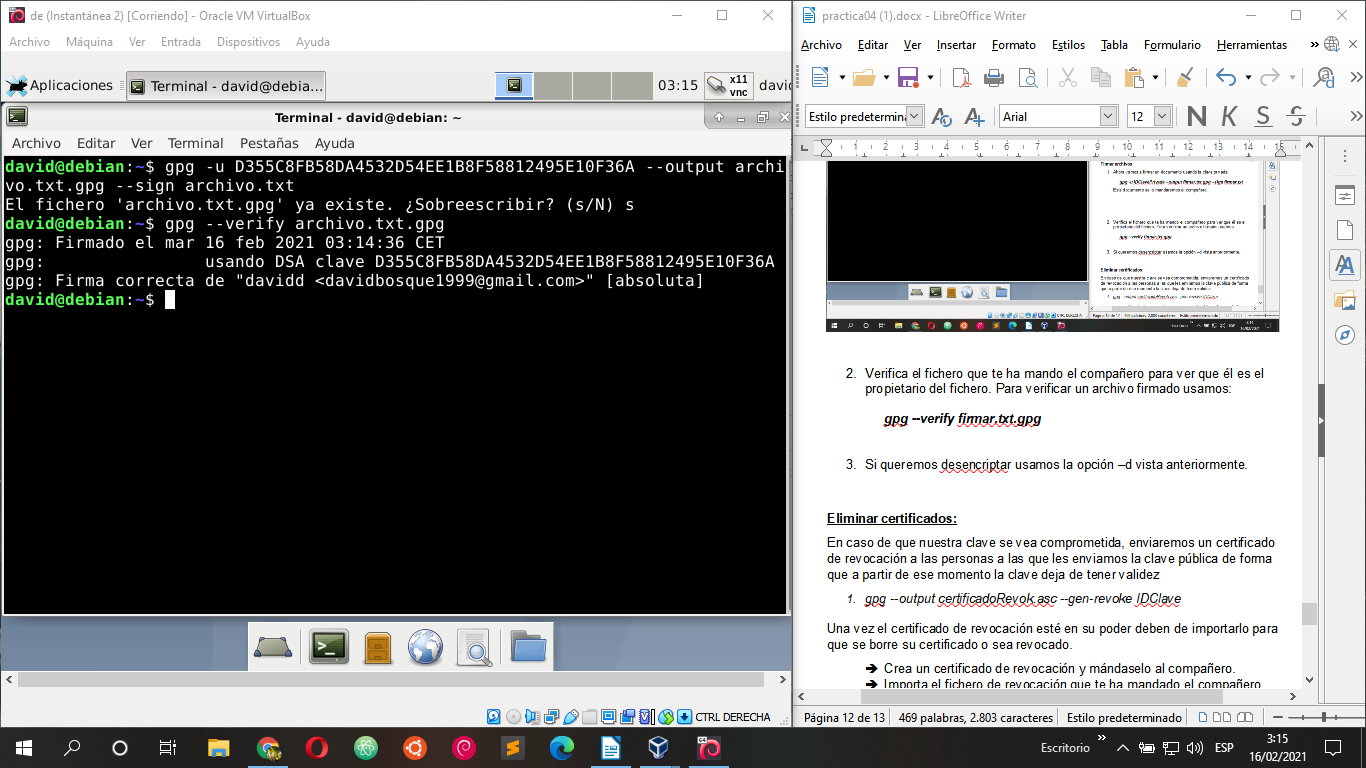
***gpg -u IDClavePrivada --output firmar.txt.gpg --sign firmar.txt***

Este documento se lo mandaremos al compañero

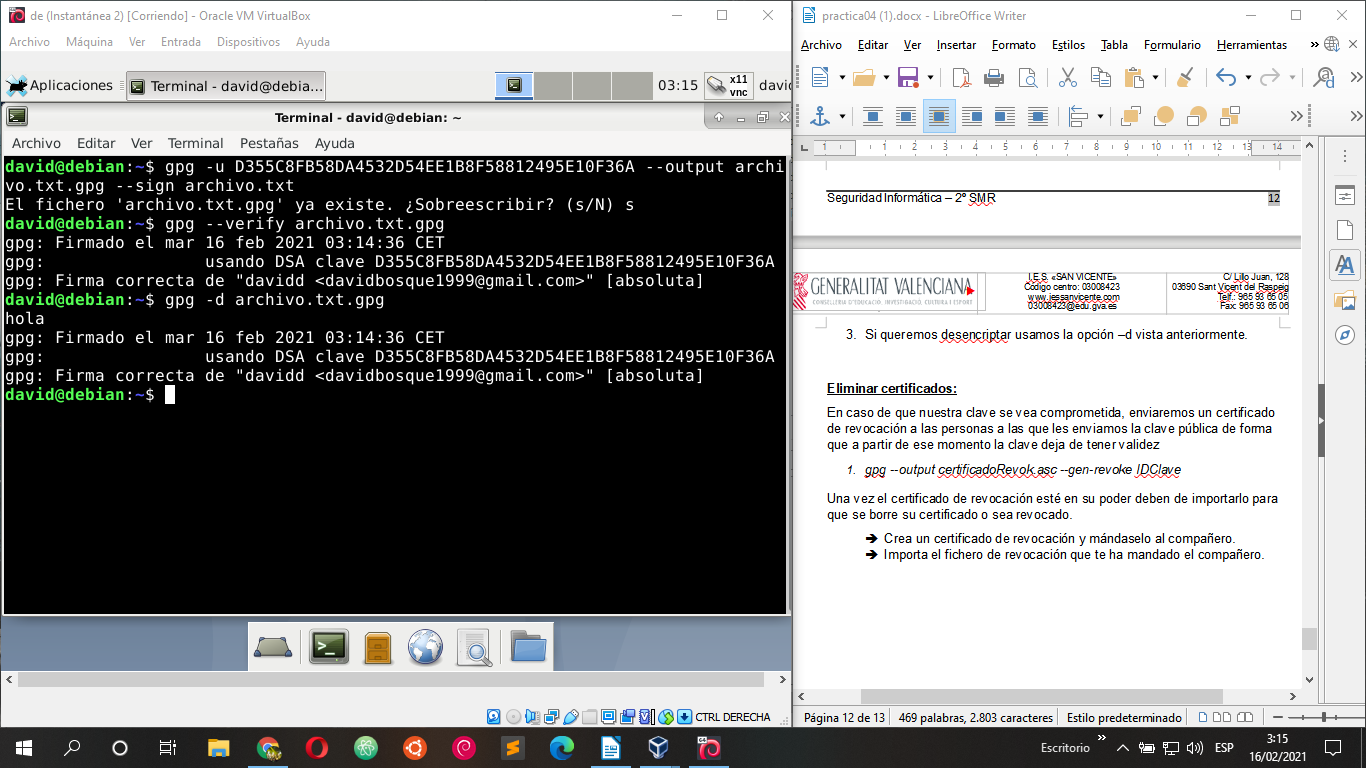


1. Verifica el fichero que te ha mando el compañero para ver que él es el propietario del fichero. Para verificar un archivo firmado usamos:

***gpg --verify firmar.txt.gpg***



1. Si queremos desencriptar usamos la opción –d vista anteriormente.

****

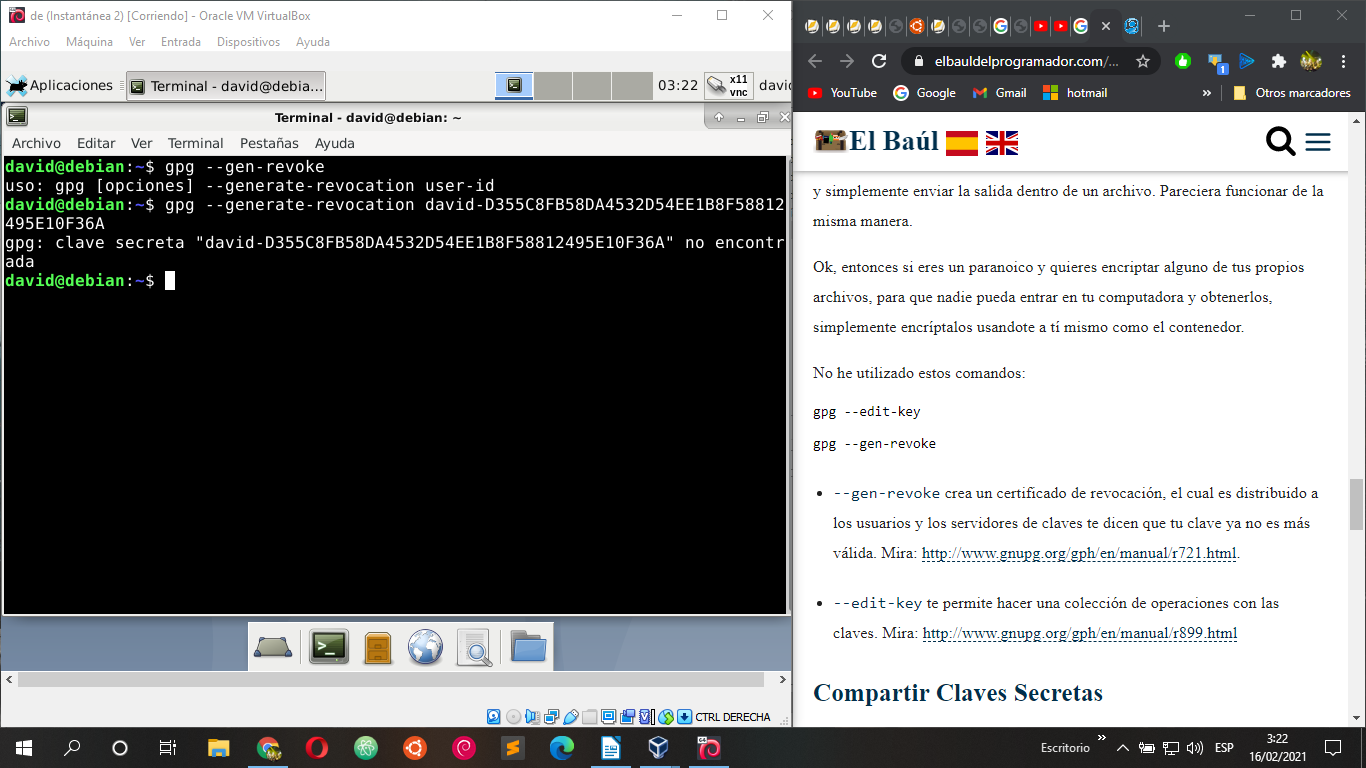
**Eliminar certificados:**

En caso de que nuestra clave se vea comprometida, enviaremos un certificado de revocación a las personas a las que les enviamos la clave pública de forma que a partir de ese momento la clave deja de tener validez

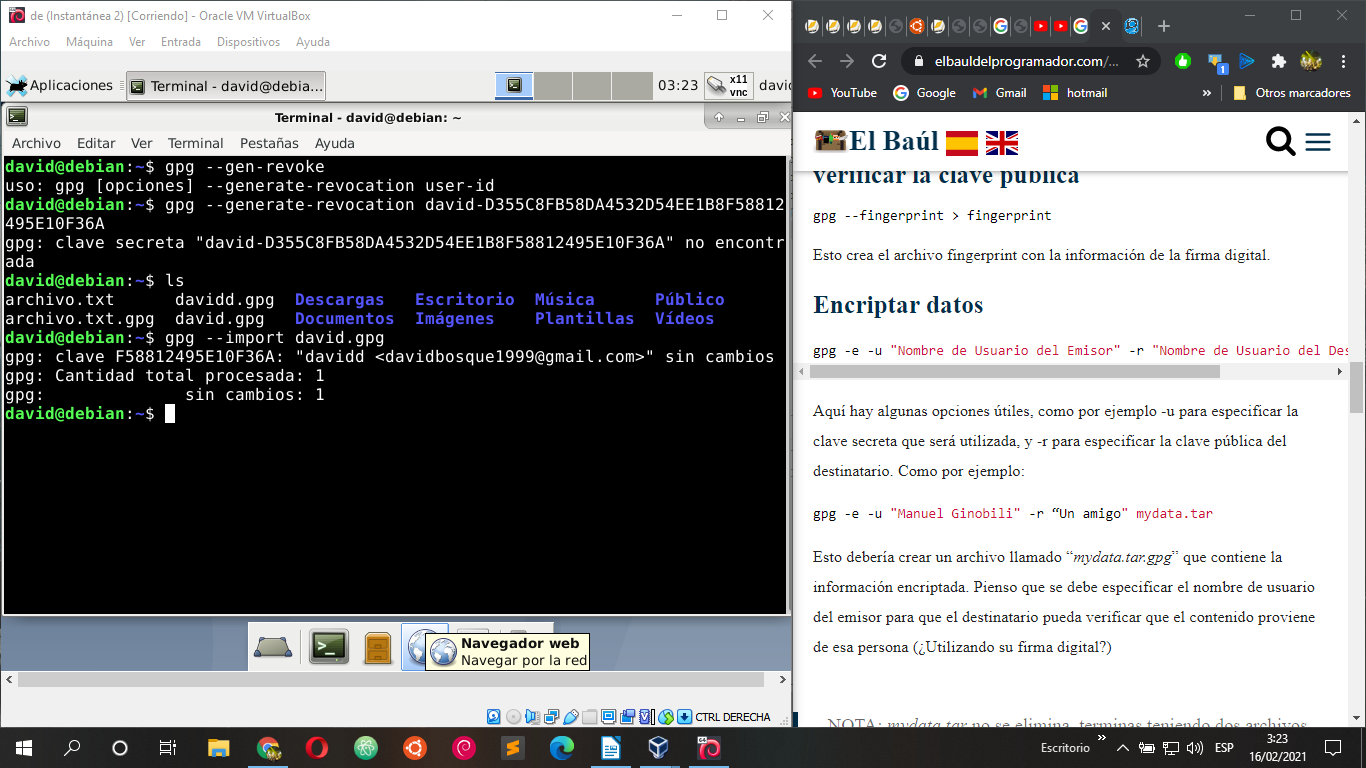
1. *gpg --output certificadoRevok.asc --gen-revoke IDClave*

Una vez el certificado de revocación esté en su poder deben de importarlo para que se borre su certificado o sea revocado.

* Crea un certificado de revocación y mándaselo al compañero.



* Importa el fichero de revocación que te ha mandado el compañero.

**