Dibujo de una persona

Descripción generada automáticamente con confianza baja

Encriptación de mensajes





**Achraf El mahjouby Sourour**

ÍNDICE

Contenido

[Introducción 3](#_Toc180495016)

[¿Para qué se usa la encriptación? 3](#_Toc180495017)

[¿Qué son las Claves pública y privada? 3](#_Toc180495018)

[¿Para qué sirve generar un par de Claves? 3](#_Toc180495019)

[Encriptación en Linux 4](#_Toc180495020)

[Encriptación con kleopatra en Windows 12](#_Toc180495021)

# Introducción

En la siguiente práctica vamos a encriptar y desencriptar menajes o archivos entre una máquina de Ubuntu y otra máquina de Windows con diferentes usuarios

## ¿Para qué se usa la encriptación?

La encriptación es como un candado invisible que protege tu información y te permite compartirla con confianza.

Encriptación en Windows

Lo primero que vamos a hacer en Linux Ubuntu es crearnos un par de claves con el comando gpg – gen-key y ¿para qué sirve?

“gpg” Es un programa que utiliza la criptografía para proteger tus datos.

“--gen-key” es un comando específico de GPG que se utiliza para generar un par de llaves: una pública y otra privada.

## ¿Qué son las Claves pública y privada?

Clave pública: Es como una tarjeta de presentación digital que puedes compartir con quien quieras. Si alguien quiere enviarte un mensaje secreto, utilizará tu llave pública para cifrarlo. Clave privada: Es tu llave secreta, como la llave de tu diario. Solo tú debes conocerla y guardarla muy bien. Esta llave es la única que puede descifrar los mensajes que fueron cifrados con tu llave pública.

## ¿Para qué sirve generar un par de Claves?

Cifrar tus mensajes: Puedes usar tu llave pública para cifrar un mensaje y enviárselo a alguien. Solo la persona que tenga tu llave privada podrá leerlo.

Firmar digitalmente tus mensajes: Cuando firmas digitalmente un mensaje, estás demostrando que eres tú quien lo ha escrito y que no ha sido modificado.

Esto es muy útil para verificar la autenticidad de documentos importantes.

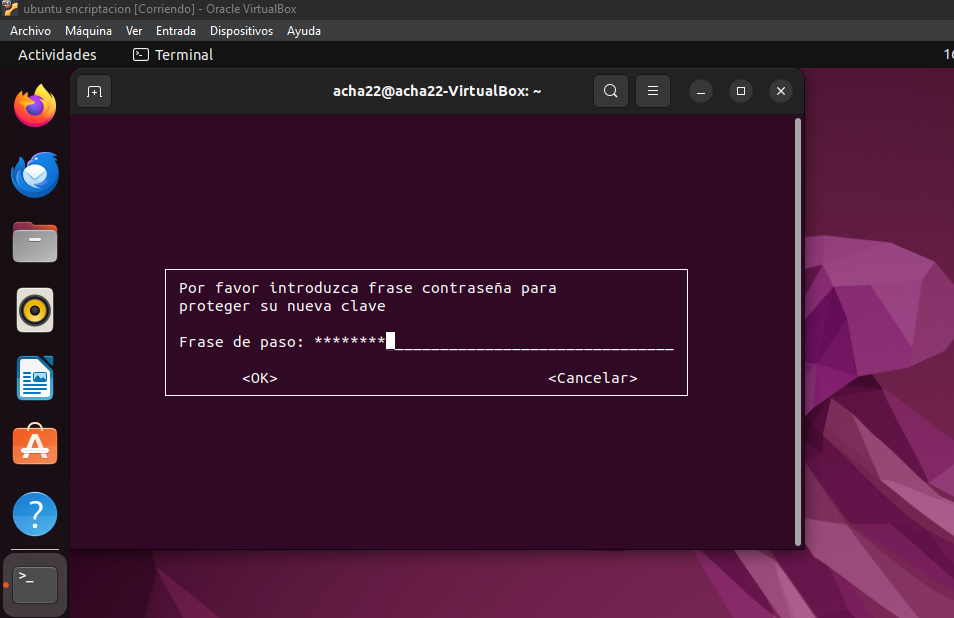
En resumen, GPG --gen-key te permite crear tu propio sistema de cifrado personal para proteger tus datos. Es como tener tu propio código secreto para comunicarte de forma segura con otras personas.

Como podemos observar en la siguiente imagen lo ejecutamos y nos da a elegir nombre y dirección de correo

# Encriptación en Linux

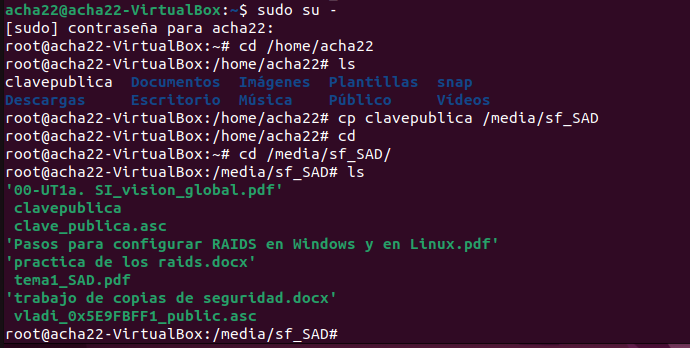
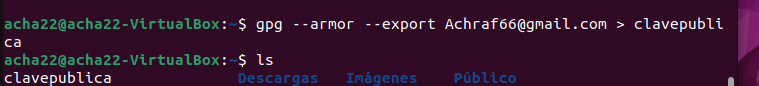


Nos dará para poner una contraseña y poner que es muy importante para importar y exportar con seguridad.

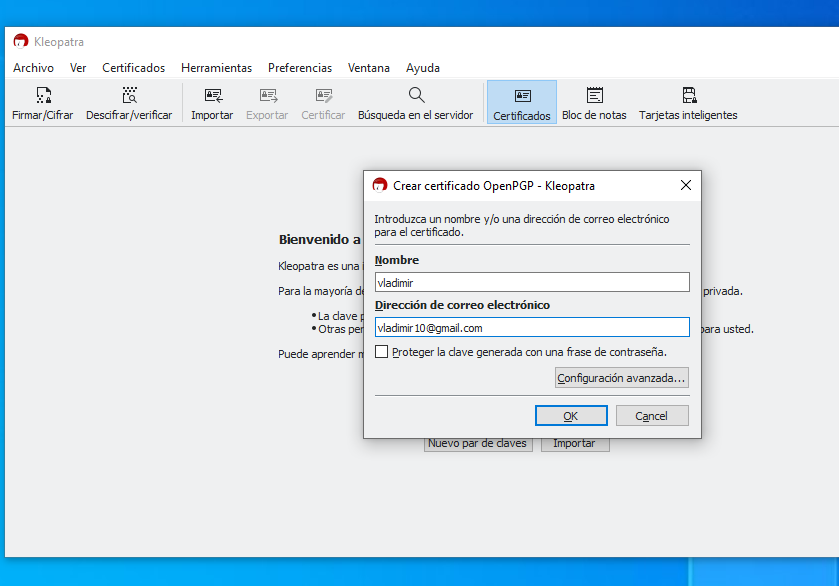


En la siguiente imagen vamos a observar una serie de cosas. Lo siguiente que tenemos que hacer es crearnos la clave pública que tendremos que importar en la otra máquina.

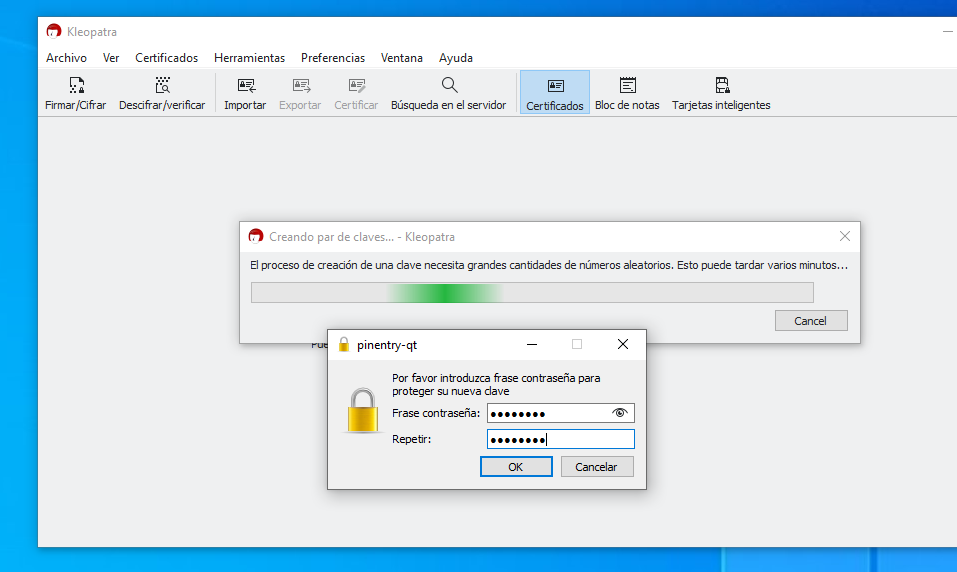
Nosotros no podemos desde nuestro propio usuario copiar en otra máquina archivos /carpetas por lo que lo haremos desde el usuario “root”, ya que anteriormente creamos una carpeta compartida entre las dos máquinas y como se puede observar creamos la clave pública



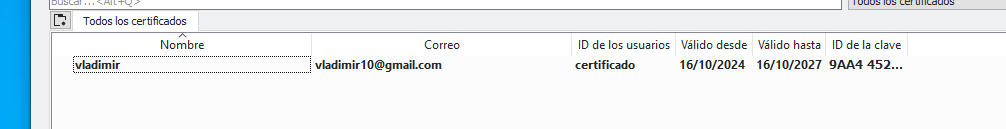
En la siguiente imagen nos dirigimos a la otra máquina y nos creamos también nuestro par de claves



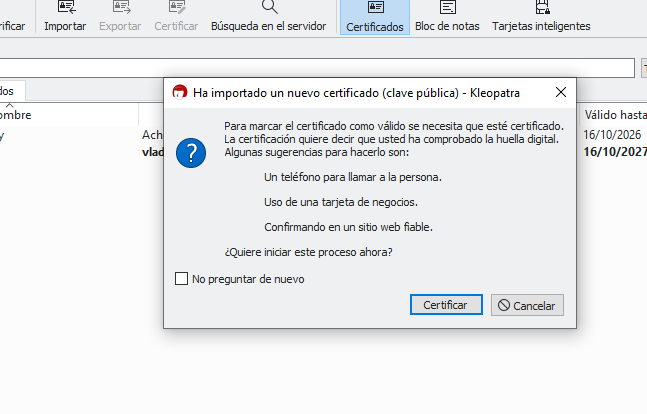
Y también lo aseguramos con una contraseña



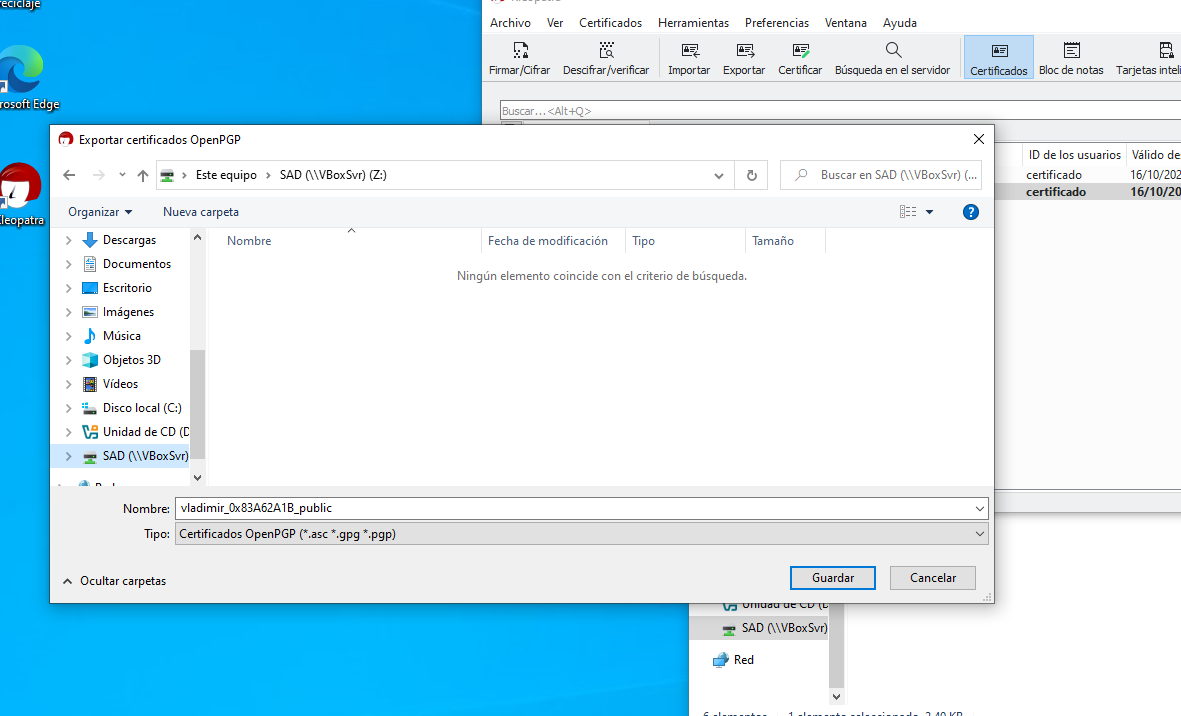
Aquí ya tendríamos creado a nuestro usuario Vladimir con su email y su par de claves que tendremos que compartir la publica en la máquina de Ubuntu con el otro usuario.



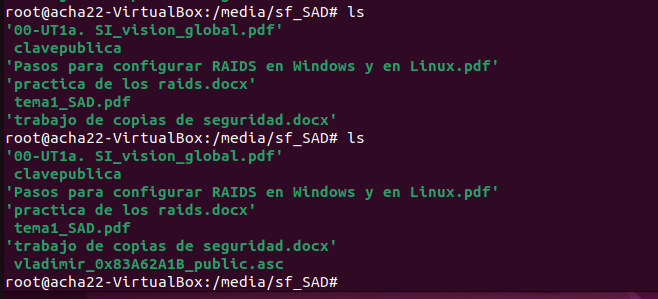
Luego importaremos la clave pública de nuestro usuario creado en la otra máquina y ya estarían listos para enviarse mensajes



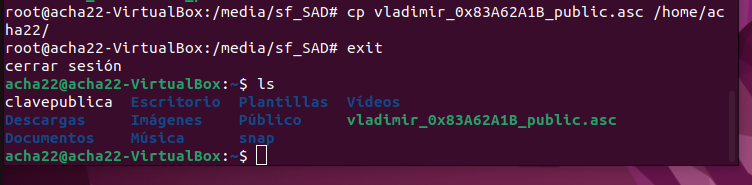
Aquí ya estaríamos exportando la clave pública de validimir10 para achraf66



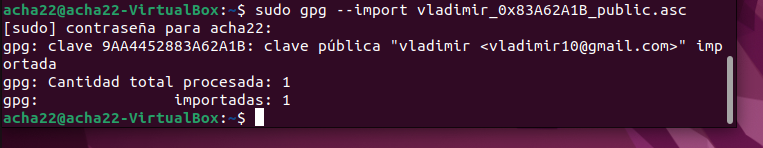
En la siguiente imagen podemos ver cunado realizamos un “ls” al principio que no teníamos la clave pública y al actualizar ya la tendríamos lista para importarla.



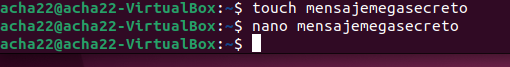
Lo que tendríamos que hacer para trabajar con nuestro usuario de la máquina es copiarla al archivo madre /home



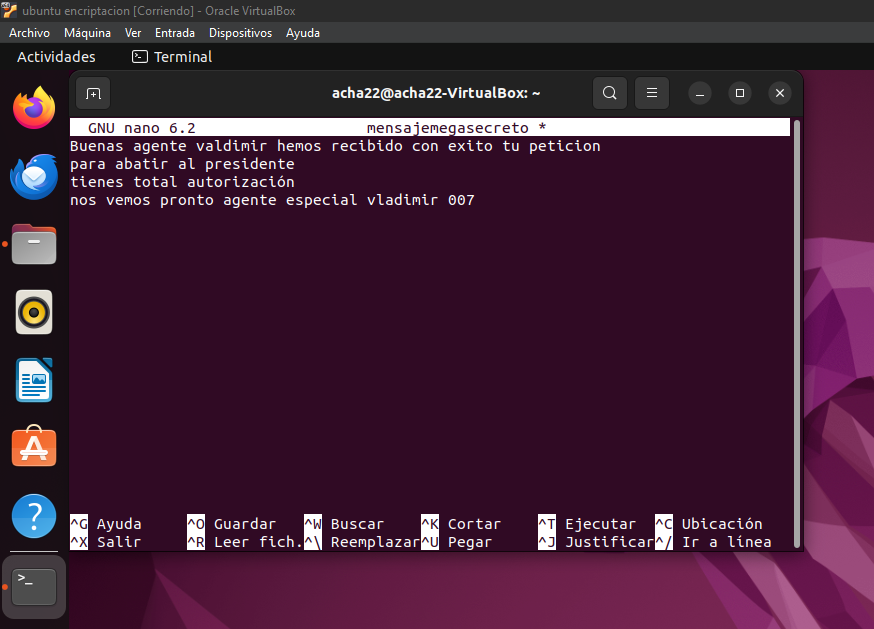
Como podemos observar en la siguiente imagen ya pudimos importar la clave pública de Vladimir para poder mandarle mensajes.



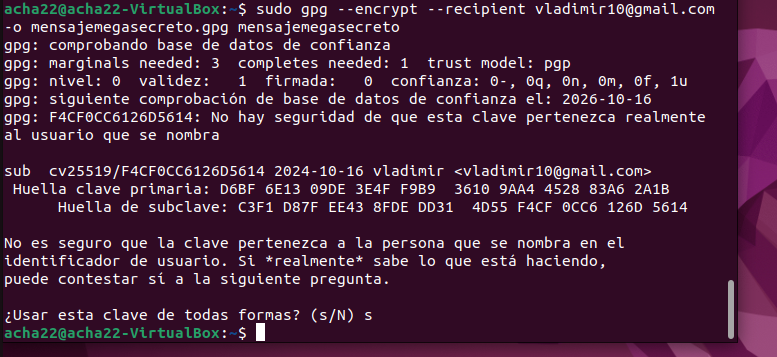
El siguiente paso sería crearnos un fichero de texto con un mensaje para Vladimir.



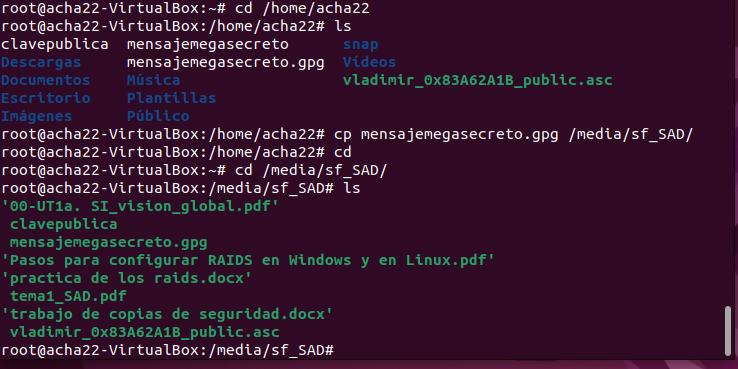
Y como se puede observar ya tendríamos el mensaje creado con éxito



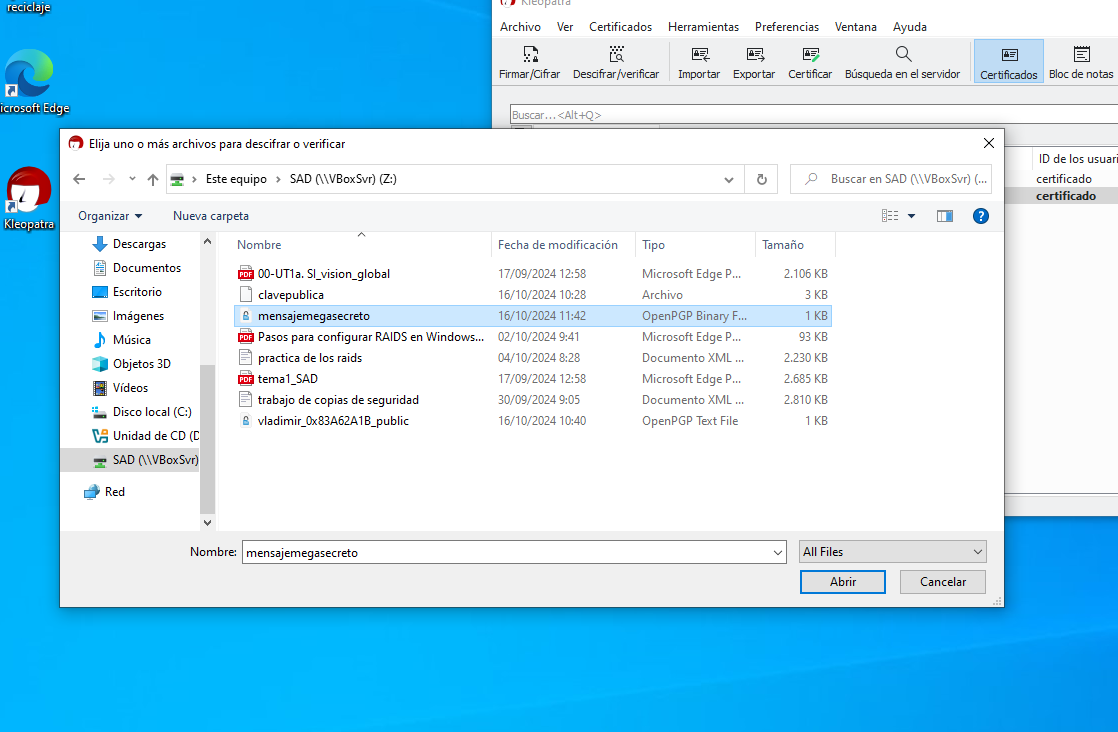
El siguiente paso sería encriptar el mensaje con el siguiente comando “” y convertirlo en “gpg” para poder mandárselo a Vladimir



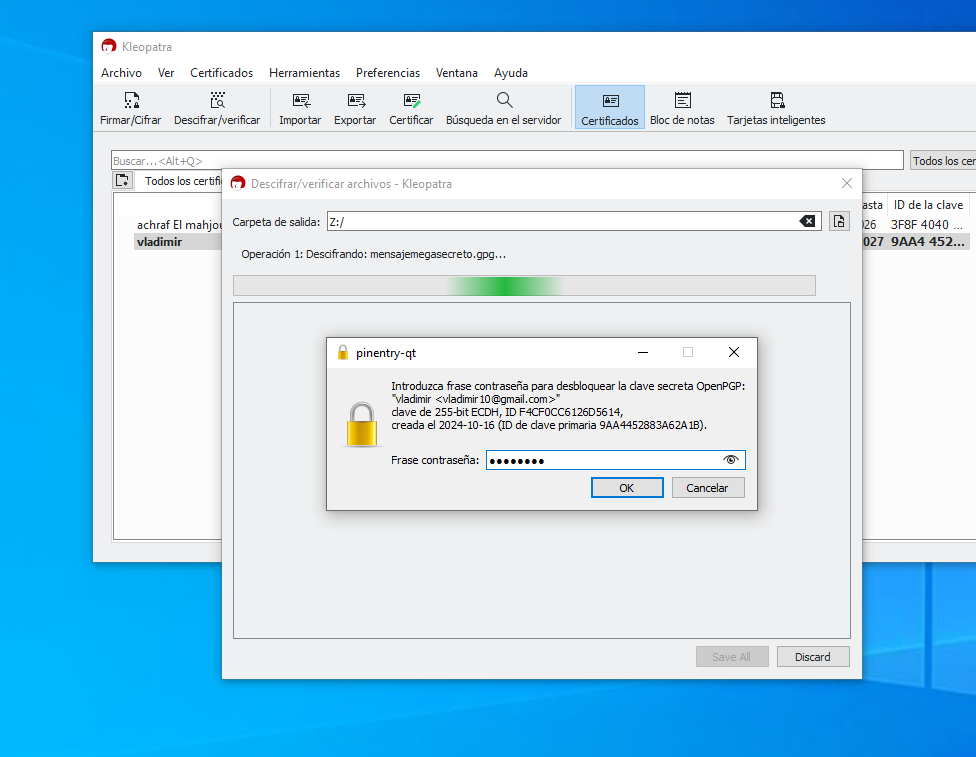
Ahora el siguiente paso es coger ese mensaje y pasarlo por la carpeta compartida a la otra maquina



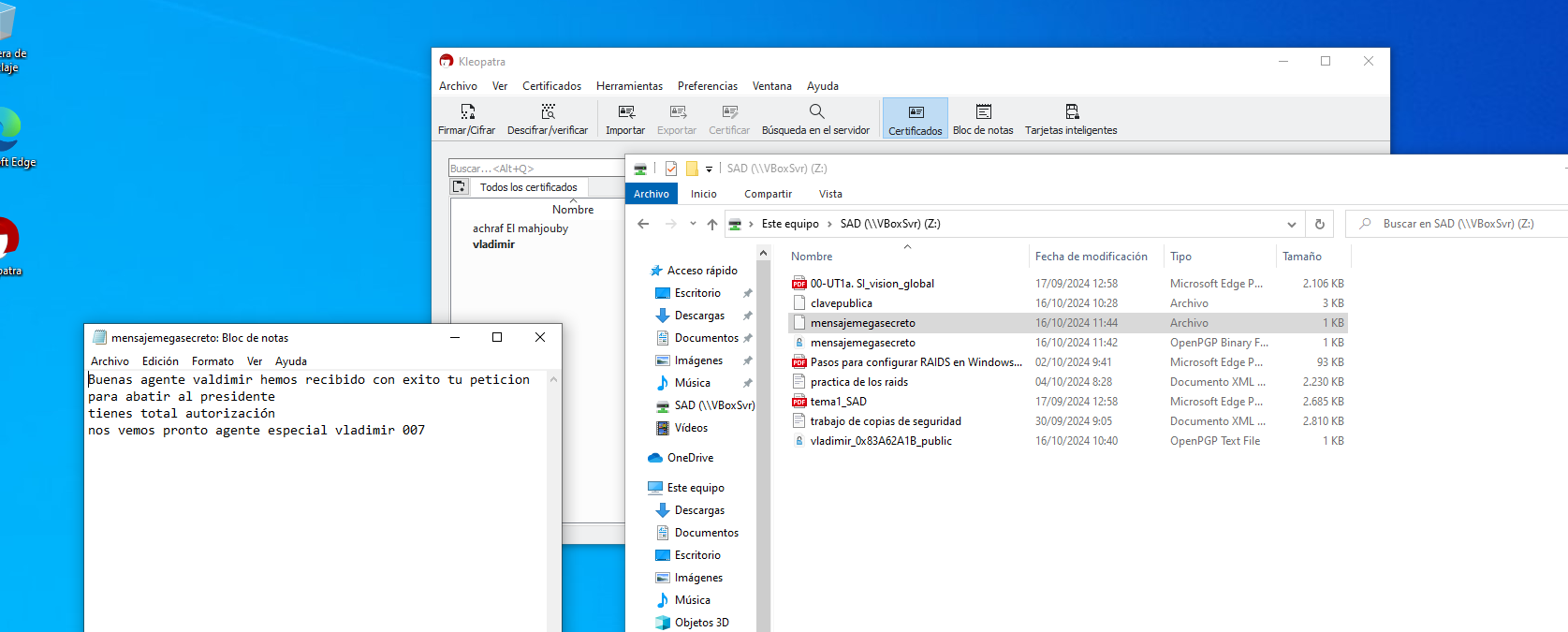
Después en la App de kleopatra nos daba la opción de descifrar archivos por lo que elegimos el que le ha mandado achraf66 a Vladimir 10



En este paso ya estaríamos descifrándolo y nos pedía la contraseña para desbloquear la clave privada de Vladimir y descifrar el mensaje.

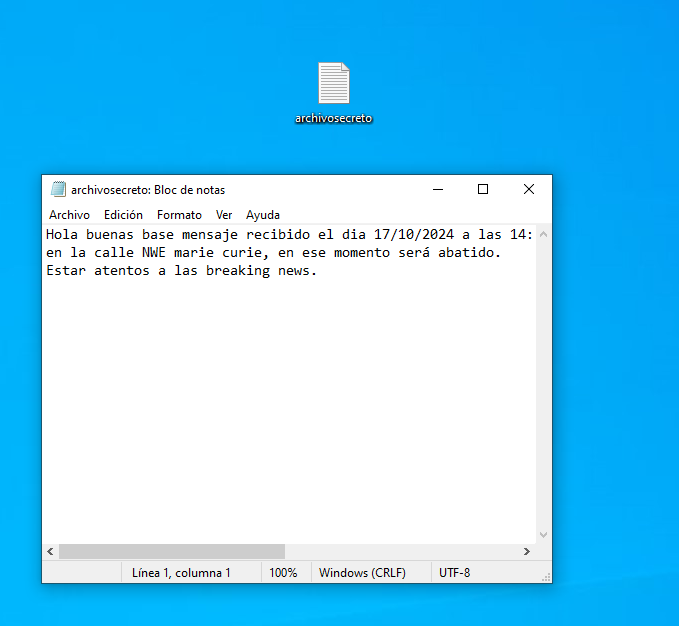


Como podemos observar en la siguiente imagen ya podríamos observar el mensaje.

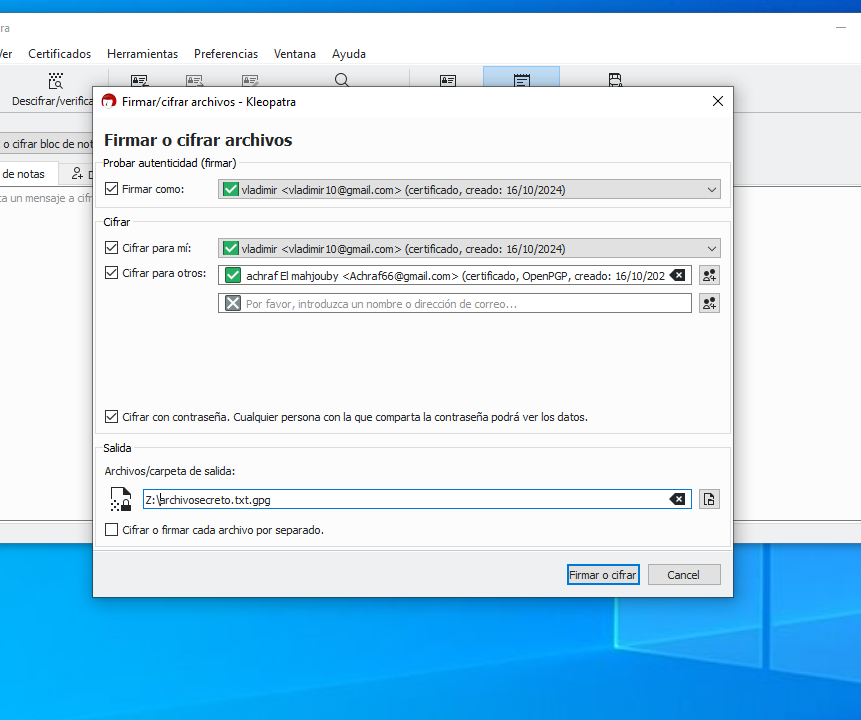


# Encriptación con kleopatra en Windows

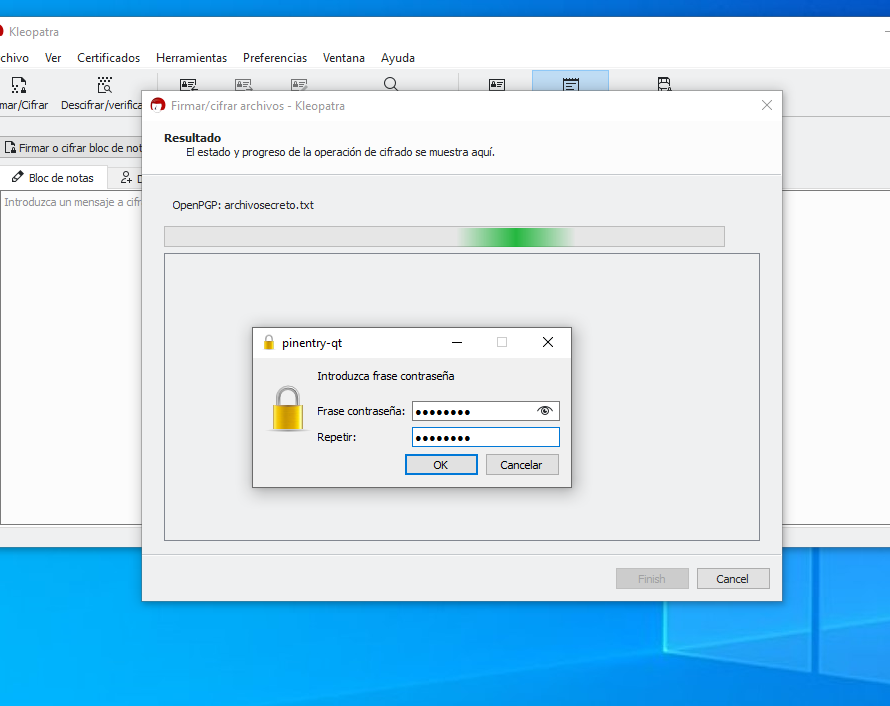
Para la siguiente práctica de la practica haremos lo mismo, pero para el usuario de la máquina de Linux para ellos previamente hemos tenido que crear un archivo con un mensaje par pode cifrarlo o encriptarlo como podemos observar en la siguiente imagen



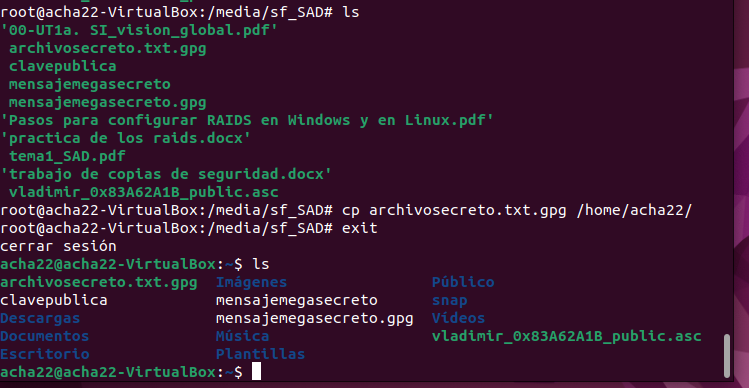
Ahora ya podríamos cifrar y firmar el mensaje y meterlo en la carpeta de salida, también le tenemos que asignar el usuario al que también se lo quiero cifrar que en este caso es Achraf66 el de Ubuntu



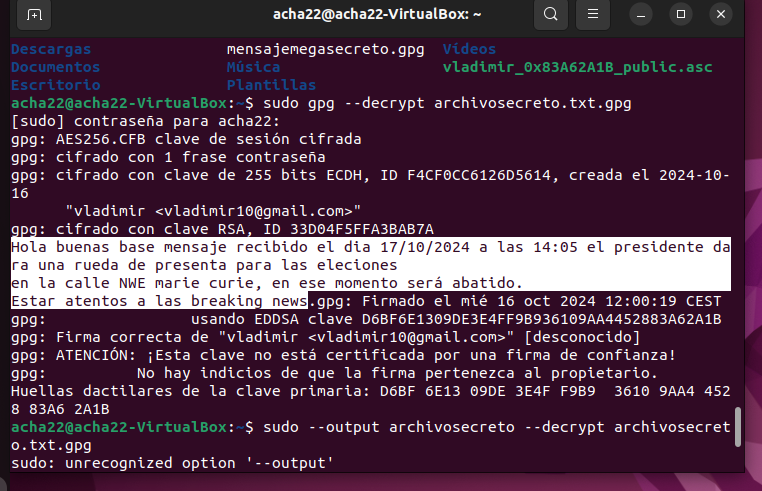
Para cifrar nos pide la contraseña de la clave privada de vladimir10 para cifrar esos mensajes.



En el siguiente paso nos iríamos a la máquina de Ubuntu y con el usuario “root” copiaríamos el “archviosecreto.gpg” a nuestra Shell propia par luego después poder desencriptarlo



En el siguiente paso lo que tenemos que hacer es descifrar el mensaje con el siguiente comando y cómo podemos observar funcionaria correctamente, pero para hacerlo más profesional lo pasamos a un archivo.txt.



Y por último en la siguiente imagen hemos podido desencriptar el archivo y transformarlo a txt para poder visualizarlo correctamente.

