Manejar claves asimétricas

En este [enlace](https://www.dropbox.com/s/35onav07t3frrwu/parejas asimétrica.ods?dl=0) puedes buscar cuál es tu pareja para hacer esta práctica.

**Importante:** Debes ir poniendo las capturas de pantalla que consideres importantes para lo que se te va pidiendo.

Importante: Para crear claves utiliza **gpg - -full-gen-key** en vez de **gpg –gen-key.**

**Haz capturas de pantalla de todo el proceso**. Aprenderás a:

* Crear tus propios par de claves (pública y privada).
* Exportar tu clave pública para darla a otra persona.
* Importar una clave pública de otra persona en tu anillo de confianza para poder cifrar.
* Encriptar y desencriptar un documento usando las claves apropiadas.
* Revocar tu clave para que no se pueda usar más.

**¿Qué se debe tener al final en la práctica?**

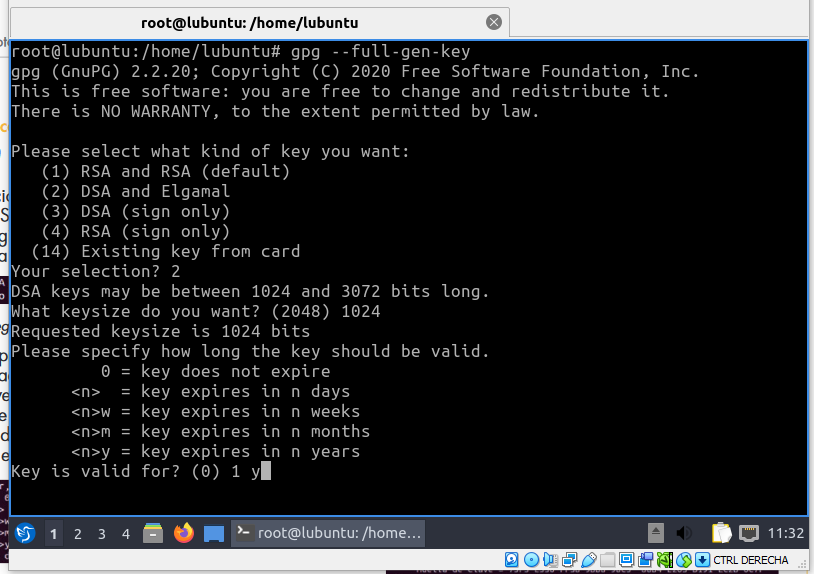
* Tu clave pública, esta deberá estar revocarla, y tu clave privada.
* Has encriptado un archivo para un compañero/a
* Has desencriptado un archivo que te han enviado a ti, cifrado con tu clave pública.

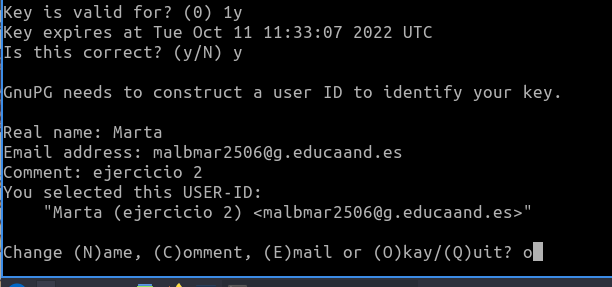
1. Para ayudarte en esta práctica tienes el caso práctico 3 del tema 2, un manual en formato pdf en la plataforma (***manual.pdf)*** y un fichero .doc (***Publicar, importar y revocar claves públicas***), también en la plataforma. También puedes ayudarte de internet si esos documentos no te gustan.
2. (**2 ptos**) Crea tu clave privada y pública (debe expirar en un año), siguiendo las instrucciones que vienen en ***manual.pdf*** o bien caso práctico 3 del tema. Es muy importante que rellenes los datos de forma correcta!!!!. **Importante:** cuidado con la clave que eliges para la clave privada, si la olvidas **TENDRÁS QUE EMPEZAR TODO EL PROCESO!!!**.

Comenzamos usando el comando “gpg --full -gen -key”, nos pedirá que tipo de llave queremos crear, y seleccionaremos la opción 2 “(2) DSA and Elgamal”.

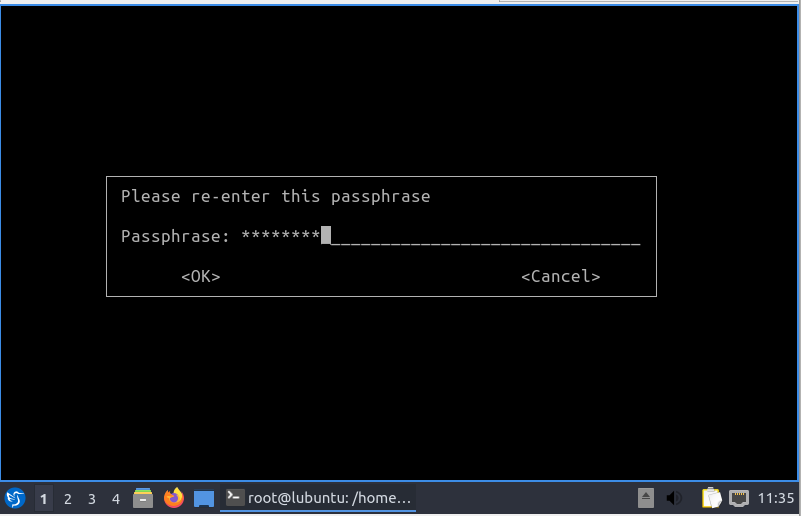
Una vez seleccionamos el tipo, nos preguntará el tamaño de llave que queremos crear (de cuantos bits), pondremos el tamaño de 1024 bits.

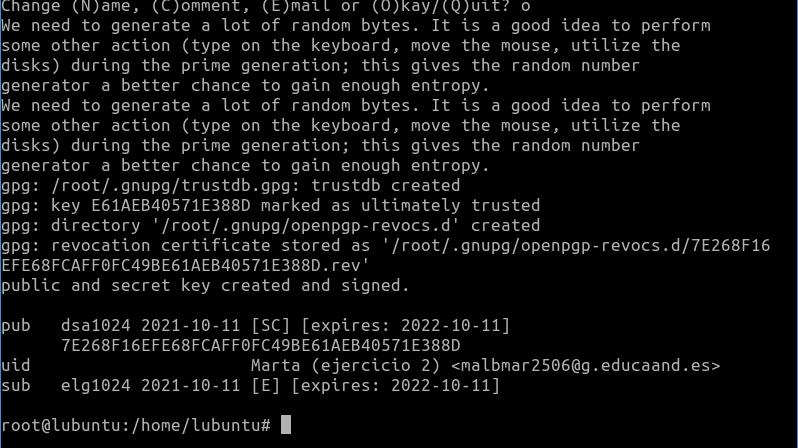
Ahora nos pedirá en cuanto tiempo queremos que expire, seleccionaremos 1 año, poniendo “1y”.

Confirmamos, y ahora necesita confirmar el usuario ID de la llave, para ello pondremos nuestro nombre, correo y el asunto o comentario de la llave, nos mostrará los datos introducidos para que confirmemos los datos, escribiremos “o” para confirmar.

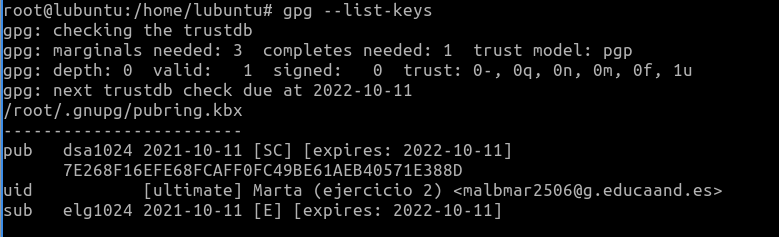


Una vez confirmado nos pedirá introducir una contraseña privada para la llave privada, saldrá una ventana así. Introducimos la clave, y es importante recordarla y no perderla, porque si no no podremos recuperarla

Una vez acabe de crearse, nos dará los datos finales de nuestra clave



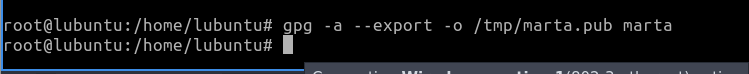
Ya se habrá creado correctamente la llave, si usamos el comando “gpg --list-keys” podremos ver nuestra lista de llaves, y ahí nos aparecerá nuestra llave recién creada con todos sus datos

****

1. **(2 ptos)** **EXPORTAR TU CLAVE PUBLICA:** Exporta tu clave pública a un archivo de tipo ascii.

**Opcional:** envía el archivo tipo ascii a tu compañero/a por email para que él lo importe. Ilustra esto con capturas de pantalla.

Para exportar la llave en formato ascii, podemos usar el comando “gpg -a --export -o /tmp/marta.pub marta”

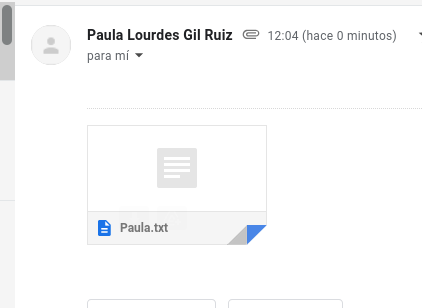
Ya tenemos nuestra clave exportada en formato ascii, podemos ver la clave a continuación usando el comando “head /tmp/marta.pub”

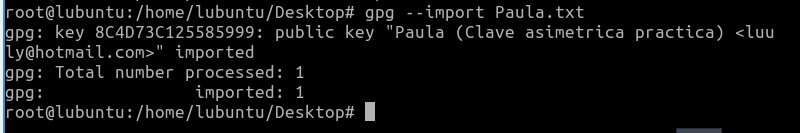


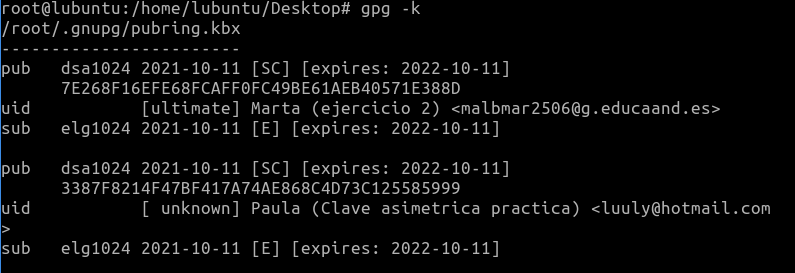
Ahora ya podemos mandarle nuestra clave pública a nuestro compañero, simplemente enviando el archivo por email

1. **(2 ptos)** **IMPORTAR CLAVE COMPAÑERO:** Elige un compañero, pon el nombre del compañero, y bájate su clave pública (que te la debe haber enviado por email). Después deberás importar esa clave a tu sistema, debes buscar el comando que hace eso, y comprobar, usando **gpg -k** que lo tienes en el sistema.

Cuando recibamos el correo de nuestro compañero con su clave pública, lo descargamos y lo importamos

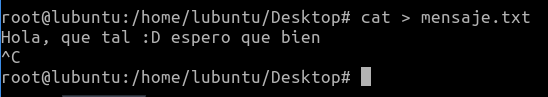
Para importar la llave, lo único que tendremos que hacer será usar el comando “gpg --import Paula.txt” y ya la tendríamos en nuestra lista de claves

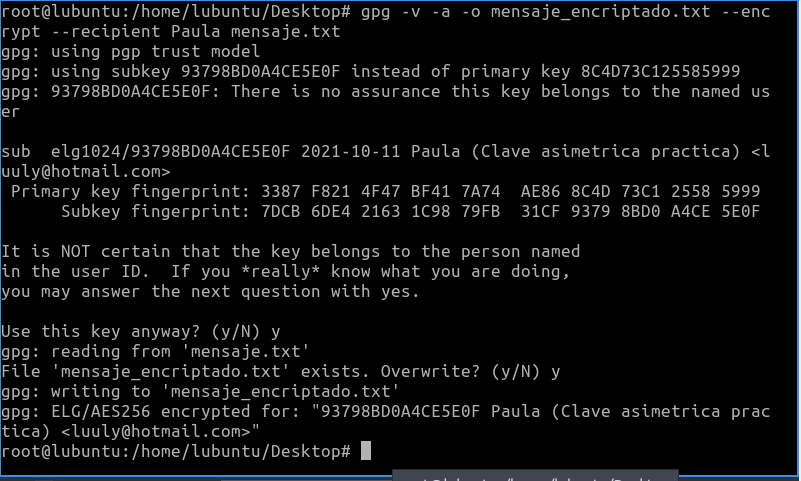
Si usamos el comando “gpg -k” podremos ver nuestra lista de claves disponibles:



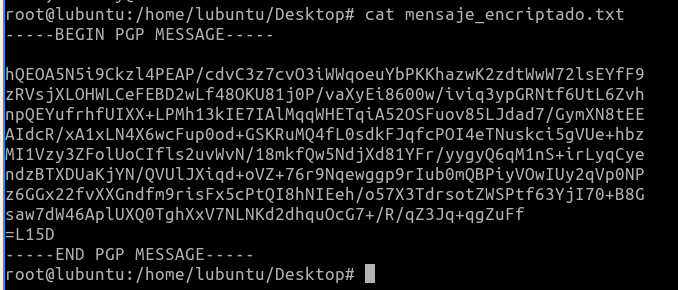
1. **(3 ptos)** **ENCRIPTACIóN:** Deberás enviar un mensaje cifrado a tu compañero con su clave pública y él a ti. Después descifraréis lo que os habéis enviado.

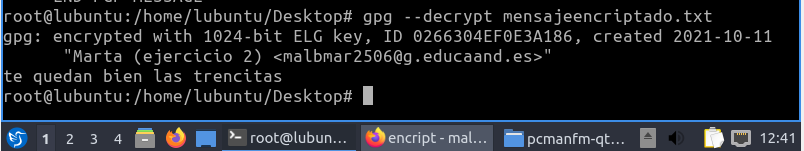
Para encriptar un archivo de texto, lo primero que tenemos que hacer es crear ese archivo de texto con nuestro mensaje dentro usando el comando “cat > NombreFichero.txt” y a continuación escribiremos el mensaje que queramos poner.

Para encriptar el mensaje que acabamos de crear, usaremos el comando “gpg -v -a -o mensaje\_encriptado.txt --ecrypt --recipient Paula mensaje.txt”, con este comando, le habremos especificado en que formato queremos que se guarde, el nombre del archivo que se va a crear, que mensaje queremos encriptar y qué clave queremos usar para encriptar el mensaje. Confirmamos y listo



Ahora, si usamos el comando “cat mensaje\_encriptado.txt” podremos ver el contenido el fichero de texto, y podemos comprobar que nuestro mensaje se ha encriptado.

Le enviamos el mensaje encriptado a nuestro compañero, y es momento de desencriptar el fichero que hemos recibido de nuestro compañero. Una vez descargado el fichero, podremos desencriptar el mensaje con nuestra clave, usando el comando “gpg --decrypt mensajeencriptado.txt” usará automáticamente la clave necesaria, y nos da el mensaje del fichero encriptado



1. **Llama a tu profesor para mostrar la práctica y que vea que has revocado la clave.**