Practica 3

francisco javier lópez calderón

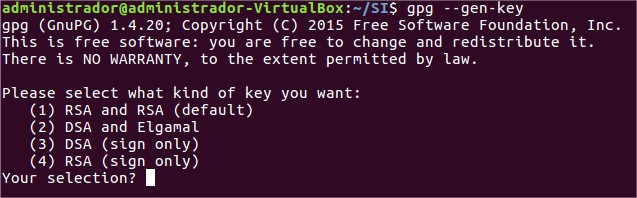
2021

UT 6. Criptografía y Sistemas Identificación

**P6.3 – Cifrado Asimétrico Generación Claves**

**Desarrollo de la práctica**

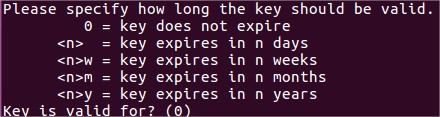
1. Genera el par de claves pública/privada, según el proceso descrito anteriormente. Utiliza los siguientes datos para generar el identificador de clave (**ClaveID**): nombre y apellidos, **comentario** = alumno2SMR-2020, y **dirección de correo electrónico del alumno**.



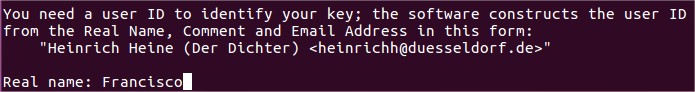
**Tras utilizar “–gen-key” comienza el proceso de creación de clave**



**Se ha utilizado 1024 bits**



**Se ha elegido 5 meses ya que en ese periodo finaliza el curso**



**He insertado el nombre Francisco**

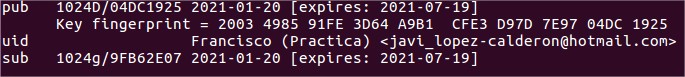


**El correo también**



**Se ha introducido la clave requerida**

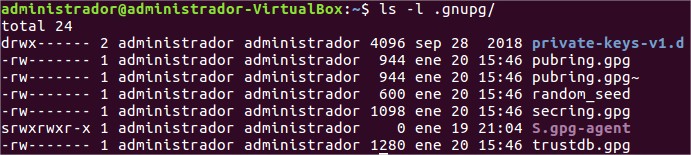
**Se ha completado la generación de la clave**



**IMPORTANTE**: en esta práctica cada alumno genera sus claves y entrega la práctica por separado.

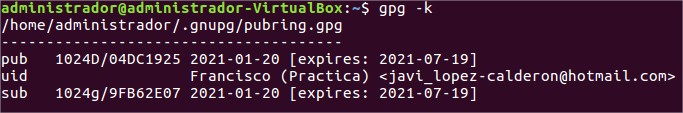
En el proceso se genera el directorio **/home/usuario/.gnupg** donde se encuentran los archivos de claves públicas y privadas, **pubring.gpg** y **secring.gpg** respectivamente. Los archivos en los que se guardan las claves públicas y las privadas se llaman anillos (KeyRings).

Para ver este directorio ponemos: ls -l .gnupg/



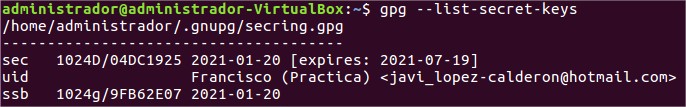
1. Para ver las claves públicas que hay disponibles dentro del fichero **pubring.gpg**. Vemos que se genera una clave primaria (pub) y una clave subordinada (sub).

gpg --list-keys o gpg -k



1. Para ver las claves privadas disponibles dentro del fichero **secring.gpg**

gpg --list-secret-keys



Vemos que se genera una clave primaria (pub) y una clave subordinada (sub).

1. Las claves se identifican por su ClaveID. Deberás buscar la ClaveID para DSA (D) y para el Gamal (g).



ID DSA---------- **04DC1925**

ID egamal------- **9FB62E07**

Una vez generadas las claves, para que el resto de las personas y entidades puedan comprobar nuestros mensajes firmados, tenemos que **darles nuestra clave pública**. Esto se puede hacer de varias maneras:

* **Servidor de claves públicas**: Los servidores de claves suelen estar interconectados, es decir, que, subiendo la clave a un servidor, el resto ya tiene conocimiento de su existencia. Por ejemplo, podemos usar el servidor pgp de la RedIris (http://www.rediris.es/servicios/identidad/pgp/)
* **Distribución directa**: se distribuye el fichero que la contiene, por correo o utilizando un soporte físico (USB, CD/DVD, etc.). En este caso debemos exportar la clave.

Operaciones más usuales:

* Publicar clave en el servidor:

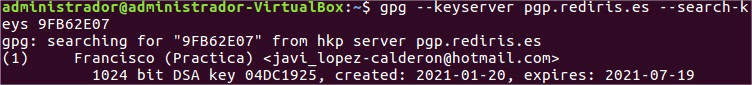
gpg --send-keys --keyserver pgp.rediris.es ClaveID





* Buscar clave pública en el servidor:

gpg --keyserver pgp.rediris.es --search-keys ClaveID



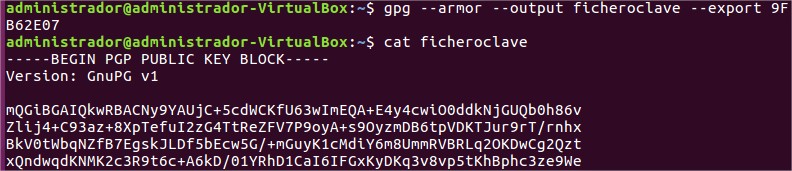
* Bajar una clave pública:

gpg --keyserver pgp.rediris.es --recv-keys ClaveID



* Exportar la clave pública a un fichero:

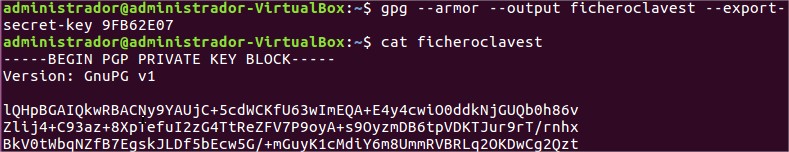
gpg --armor --output ficherodeclave --export ClaveID



Es importante tener una copia de nuestra clave privada, para que en caso de pérdida de datos podamos recuperarla:

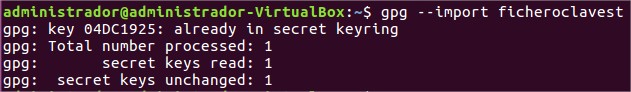
* Para exportar la clave privada a un fichero y poder tener una copia de seguridad:

gpg --armor --output ficherodeclave --export-secret-key ClaveID



* Para importar una clave volcada en un fichero:

gpg --import ficherodeclave



1. Envía tu clave al servidor de RedIris. Comprueba en la página de RedIris (http://www.rediris.es/servicios/identidad/pgp/) que está publicada.

**El envío de la clave se ha realizado anteriormente.**

1. Busca con la opción --search-keys tu clave pública (ClaveID **FCF9A9B5**)
2. Exporta tu clave pública a un archivo llamado NombreApellidoClave.

Rediris está caído…pero, anteriormente hemos comprobado la funcionalidad del servicio con comandos

****