Practica 4

Francisco javier lópez calderón

2021

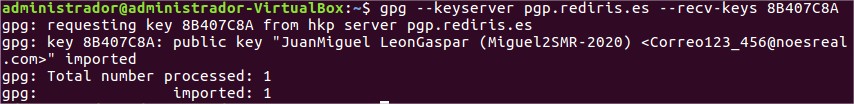
UT 6. Criptografía y Sistemas Identificación

**P6.4 – Cifrado Asimétrico Cifrado Documentos**

**Desarrollo de la práctica**

1. Importa la clave pública de un compañero y la clave pública del profesor. Las claves se importan desde el repositorio de claves públicas utilizando el ID correspondiente

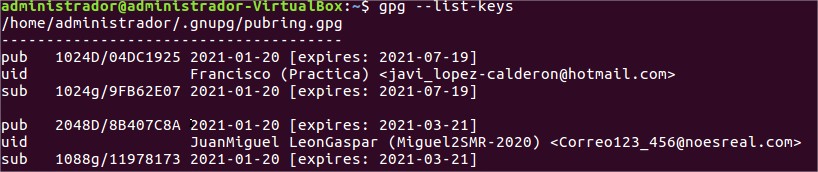
gpg --keyserver pgp.rediris.es --recv-keys ID



1. Comprueba las claves que tienes instaladas en tu anillo de claves

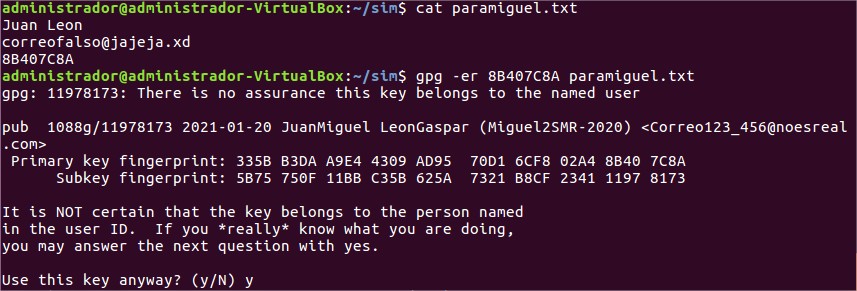
gpg --list-keys o gpg -k

**Como se puede comprobar, actualmente poseo la clave pública de Juan Miguel**



1. Crea un documento de texto que contenga el nombre y los apellidos del alumno, la dirección de email y el ID de la clave pública. Cifra el documento anterior con la clave pública del alumno. Entrega el documento a un alumno vía email.

Utilizamos -e para encriptar y -r para introducir la clave del compañero



1. Por parejas: cifra un documento con la clave pública del compañero. Él deberá comprobar que puede descifrarlo con su clave privada. Igualmente, tú debes comprobar que puedes descifrar con tu clave privada el que tu compañero ha cifrado.

**Utilizando nuestra propia contraseña, podemos abrir el documento cifrado del compañero**

