2021

Practica 4

FRANCISCO JAVIER LÓPEZ CALDERÓN

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
   ```

```
administrador@administrador-VirtualBox:~$ gpg --keyserver pgp.rediris.es --recv-keys 8B407C8A
gpg: requesting key 8B407C8A from hkp server pgp.rediris.es
gpg: key 8B407C8A: public key "JuanMiguel LeonGaspar (Miguel2SMR-2020) <Correo123_456@noesreal
.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

2. 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

```
administrador@administrador-VirtualBox:~$ gpg --list-keys
/home/administrador/.gnupg/pubring.gpg
---------------------------------------
pub   1024D/04DC1925 2021-01-20 [expires: 2021-07-19]
uid                  Francisco (Practica) <javi_lopez-calderon@hotmail.com>
sub   1024g/9FB62E07 2021-01-20 [expires: 2021-07-19]

pub   2048D/8B407C8A 2021-01-20 [expires: 2021-03-21]
uid                  JuanMiguel LeonGaspar (Miguel2SMR-2020) <Correo123_456@noesreal.com>
sub   1088g/11978173 2021-01-20 [expires: 2021-03-21]
```

3. 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

```
administrador@administrador-VirtualBox:~/sim$ cat paramiguel.txt
Juan Leon
correofalso@jajeja.xd
8B407C8A
administrador@administrador-VirtualBox:~/sim$ gpg -er 8B407C8A paramiguel.txt
gpg: 11978173: There is no assurance this key belongs to the named user

pub  1088g/11978173 2021-01-20 JuanMiguel LeonGaspar (Miguel2SMR-2020) <Correo123_456@noesreal
.com>
 Primary key fingerprint: 335B B3DA A9E4 4309 AD95  70D1 6CF8 02A4 8B40 7C8A
      Subkey fingerprint: 5B75 750F 11BB C35B 625A  7321 B8CF 2341 1197 8173

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
```

4. 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