2021

Practica 3

FRANCISCO JAVIER LÓPEZ CALDERÓN

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

```
administrador@administrador-VirtualBox:~/SI$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection?
```

```
Your selection? 2
DSA keys may be between 1024 and 3072 bits long.
What keysize do you want? (2048) 1024
```

Se ha utilizado 1024 bits

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

```
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
```

```
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Francisco
```

He insertado el nombre Francisco

El correo también

```
Comment: Practica
You selected this USER-ID:
    "Francisco (Practica) <javi_lopez-calderon@hotmail.com>"
```

```
Enter passphrase:
```

Se ha introducido la clave requerida

Se ha completado la generación de la clave

```
pub   1024D/04DC1925 2021-01-20 [expires: 2021-07-19]
      Key fingerprint = 2003 4985 91FE 3D64 A9B1  CFE3 D97D 7E97 04DC 1925
uid                  Francisco (Practica) <javi_lopez-calderon@hotmail.com>
sub   1024g/9FB62E07 2021-01-20 [expires: 2021-07-19]
```

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/

```
administrador@administrador-VirtualBox:~$ ls -l .gnupg/
total 24
drwx------ 2 administrador administrador 4096 sep 28  2018 private-keys-v1.d
-rw------- 1 administrador administrador  944 ene 20 15:46 pubring.gpg
-rw------- 1 administrador administrador  944 ene 20 15:46 pubring.gpg~
-rw------- 1 administrador administrador  600 ene 20 15:46 random_seed
-rw------- 1 administrador administrador 1098 ene 20 15:46 secring.gpg
srwxrwxr-x 1 administrador administrador    0 ene 19 21:04 S.gpg-agent
-rw------- 1 administrador administrador 1280 ene 20 15:46 trustdb.gpg
```

2. 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
```

```
administrador@administrador-VirtualBox:~$ gpg -k
/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]
```

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

```
gpg --list-secret-keys
```

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

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

4. 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**

```
pub   1024D/04DC1925
uid
sub   1024g/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`

```
administrador@administrador-VirtualBox:~$ gpg --send-keys --keyserver pgp.rediris.e
s 04DC1925
gpg: sending key 04DC1925 to hkp server pgp.rediris.es
```

```
administrador@administrador-VirtualBox:~$ gpg --send-keys --keyserver pgp.rediris.e
s 9FB62E07
gpg: sending key 04DC1925 to hkp server pgp.rediris.es
```

- Buscar clave pública en el servidor:
  `gpg --keyserver pgp.rediris.es --search-keys ClaveID`

```
administrador@administrador-VirtualBox:~$ gpg --keyserver pgp.rediris.es --search-k
eys 9FB62E07
gpg: searching for "9FB62E07" from hkp server pgp.rediris.es
(1)     Francisco (Practica) <javi_lopez-calderon@hotmail.com>
          1024 bit DSA key 04DC1925, created: 2021-01-20, expires: 2021-07-19
```

- Bajar una clave pública:
  `gpg --keyserver pgp.rediris.es --recv-keys ClaveID`

```
administrador@administrador-VirtualBox:~$ gpg --keyserver pgp.rediris.es --recv-keys 9F
B62E07
gpg: requesting key 9FB62E07 from hkp server pgp.rediris.es
gpg: key 04DC1925: "Francisco (Practica) <javi_lopez-calderon@hotmail.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
```

- Exportar la clave pública a un fichero:
  `gpg --armor --output ficherodeclave --export ClaveID`

```
administrador@administrador-VirtualBox:~$ gpg --armor --output ficheroclave --export 9F
B62E07
administrador@administrador-VirtualBox:~$ cat ficheroclave
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQGiBGAIQkwRBACNy9YAUjC+5cdWCKfU63wImEQA+E4y4cwiO0ddkNjGUQb0h86v
Zlij4+C93az+8XpTefuI2zG4TtReZFV7P9oyA+s9OyzmDB6tpVDKTJur9rT/rnhx
BkV0tWbqNZfB7EgskJLDf5bEcw5G/+mGuyK1cMdiY6m8UmmRVBRLq2OKDwCg2Qzt
xQndwqdKNMK2c3R9t6c+A6kD/01YRhD1CaI6IFGxKyDKq3v8vp5tKhBphc3ze9We
```

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`

```
administrador@administrador-VirtualBox:~$ gpg --armor --output ficheroclavest --export-
secret-key 9FB62E07
administrador@administrador-VirtualBox:~$ cat ficheroclavest
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v1

lQHpBGAIQkwRBACNy9YAUjC+5cdWCKfU63wImEQA+E4y4cwiO0ddkNjGUQb0h86v
Zlij4+C93az+8XpïefuI2zG4TtReZFV7P9oyA+s9OyzmDB6tpVDKTJur9rT/rnhx
BkV0tWbqNZfB7EgskJLDf5bEcw5G/+mGuyK1cMdiY6m8UmmRVBRLq2OKDwCg2Qzt
```

- Para importar una clave volcada en un fichero:
  `gpg --import ficherodeclave`

```
administrador@administrador-VirtualBox:~$ gpg --import ficheroclavest
gpg: key 04DC1925: already in secret keyring
gpg: Total number processed: 1
gpg:       secret keys read: 1
gpg:  secret keys unchanged: 1
```

5. 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.

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

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