

EJERCICIOS DE CRIPTOGRAFIA

EJERCICIO 1: Cifrado simétrico de un documento.

1. Primero creamos un documento, el que vayamos a compartir.

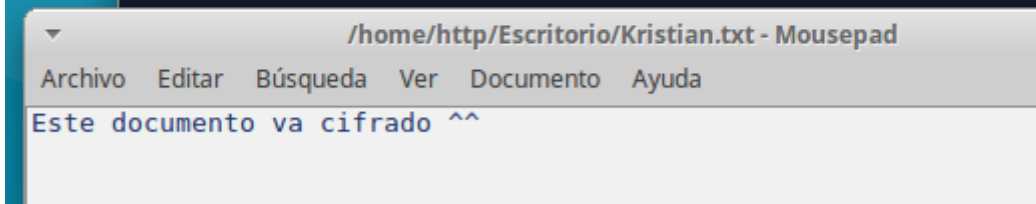
```
http@http-VirtualBox:~/Escritorio$ touch alex.txt
http@http-VirtualBox:~/Escritorio$ nano alex.txt
http@http-VirtualBox:~/Escritorio$ cat alex.txt
Esque es un documento cifrado :D
http@http-VirtualBox:~/Escritorio$
```

2. Ciframos el documento creado

```
http@http-VirtualBox:~/Escritorio$ gpg -c alex.txt
gpg: anillo «/home/http/.gnupg/pubring.gpg» creado
http@http-VirtualBox:~/Escritorio$
```

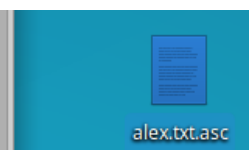
3. Desciframos el documento procedente de nuestro compañero, en este caso es el de Kristian.

```
http@http-VirtualBox:~/Escritorio$ gpg Kristian.txt.gpg
gpg: anillo «/home/http/.gnupg/secring.gpg» creado
gpg: datos cifrados AES
gpg: cifrado con 1 contraseña
http@http-VirtualBox:~/Escritorio$
```



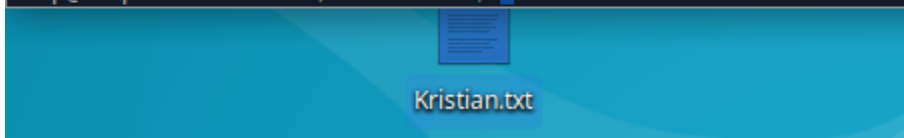
4. Ahora repetimos el comando de antes para cifrarlo, pero con el cambio de -c a -ca, y visualizamos el contenido.

```
http@http-VirtualBox:~/Escritorio$ gpg -ca alex.txt
http@http-VirtualBox:~/Escritorio$
```



5. Kris me mando su cifrado, y vamos a descifrarlo.

```
http@http-VirtualBox:~/Escritorio$ gpg Kristian.txt.asc
gpg: datos cifrados AES
gpg: cifrado con 1 contraseña
http@http-VirtualBox:~/Escritorio$
```



2.Creacion de nuestras claves pública-privada.

Siguiendo las indicaciones de este epígrafe, crea tu par de claves pública y privada. La clave que vas a crear tendrá una validez de 1 mes.

Recuerda el ID de usuario de tu clave y la contraseña de paso utilizada. Anótala en un lugar seguro si lo consideras necesario.

```
tp@http-VirtualBox:~/Escritorio$ 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 the type of key to generate:
(1) RSA and RSA (default)
(2) DSA and ElGamal (default)
(3) DSA (only signing)
(4) RSA (only signing)
Your selection? 1
Keys RSA can have between 1024 and 4096 bits of length.
What size of key do you want? (2048) 2048
Requested size is 2048 bits
Specify the validity of the key.
0 = the key never expires
<n> = the key expires in n days
<n>w = the key expires in n weeks
<n>m = the key expires in n months
<n>y = the key expires in n years
Validity of the key (0)? 1m
Key expires on: 12 Apr 2017 17:02:39 CEST
Is this correct? (y/n) y

You need a user identifier to identify your key. The program
constructs the identifier from the Real Name, Comment and Email Address.
Email address of this form:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name and surnames: AlejandroAnton
Email address of electronic mail: alejandro@gmail.com
Comment:
Selected this ID of user:
«AlejandroAnton <alejandro@gmail.com>»

Change (N)ame, (C)omment, (D)irection or (V)alidity? v
```

```
+++++
gpg: /home/http/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave B133FF81 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

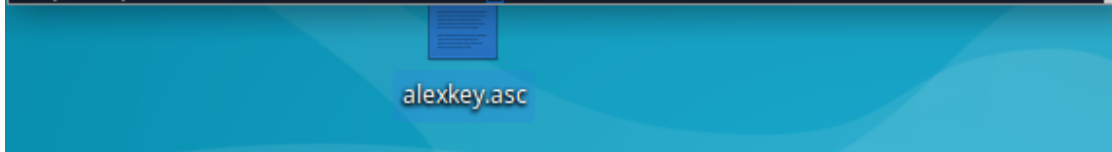
gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesaria(s), 1 completa(s) necesaria(s),
modelo de confianza PGP
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2017-04-12
pub 2048R/B133FF81 2017-03-13 [[caduca: 2017-04-12]]
Huellas de clave = 08F6 B4BF 589A 8C20 E231 FFDC D3B1 617F B133 FF81
uid AlejandroAnton <alejandro@gmail.com>
sub 2048R/8A365BA2 2017-03-13 [[caduca: 2017-04-12]]

tp@http-VirtualBox:~/Escritorio$
```

Ejercicio 3: Exportar e importar claves públicas

1. Exporta tu clave pública en formato ASCII y guárdalo en un archivo nombre_apellido.asc y envíalo a un compañero/a.

```
http@http-VirtualBox:~/Escritorio$ gpg -a --export -o alexkey.asc Alejandro Anton
http@http-VirtualBox:~/Escritorio$
```



2. Importa las claves públicas recibidas de vuestros/as compañeros/as.

```
http@http-VirtualBox:~/Escritorio$ gpg --import KristianKey.asc
gpg: clave 8DDDF4E: clave pública "Tomas <lala@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg:      importadas: 1 (RSA: 1)
http@http-VirtualBox:~/Escritorio$
```

3. Comprueba que las claves se han incluido correctamente en vuestro keyring.

```
http@http-VirtualBox:~/Escritorio$ gpg -kv
/home/http/.gnupg/pubring.gpg
-----
pub   2048R/B133FF81 2017-03-13 [[caduca: 2017-04-12]]
uid           AlejandroAnton <alejandro@gmail.com>
sub   2048R/8A365BA2 2017-03-13 [[caduca: 2017-04-12]]

pub   2048R/8DDDF4E 2017-03-13 [[caduca: 2017-04-12]]
uid           Tomas <lala@gmail.com>
sub   2048R/3F2D99DC 2017-03-13 [[caduca: 2017-04-12]]

http@http-VirtualBox:~/Escritorio$
```

Ejercicio 4: Cifrado y Descifrado de un documento

1. Cifraremos un archivo cualquiera y lo remitiremos por email a uno de nuestros compañeros que nos proporcionó su clave pública.

```
http@http-VirtualBox:~/Escritorio$ gpg -a -r Tomas --encrypt alex.txt
gpg: 3F2D99DC: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

pub 2048R/3F2D99DC 2017-03-13 Tomas <lala@gmail.com>
Huella de clave primaria: 7050 4E9D 880E BB70 97CC 75B8 4B2F AB0F 8DDD FA4E
Huella de subclave: 739A 6E33 61E9 9779 C520 E2F4 718C 824B 3F2D 99DC

No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.

¿Usar esta clave de todas formas? (s/N) s
http@http-VirtualBox:~/Escritorio$
```

2. Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos.
3. Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.
4. Por último, enviaremos el documento cifrado a alguien que no estaba en la lista de destinatarios y comprobaremos que este usuario no podrá descifrar este archivo.

```
http@http-VirtualBox:~/Escritorio$ gpg Kristian.asc

Necesita una contraseña para desbloquear la clave secreta
del usuario: "AlejandroAnton <alejandro@gmail.com>"
clave RSA de 2048 bits, ID 8A365BA2, creada el 2017-03-13 (identificador de clave
primaria B133FF81)

gpg: cifrado con clave RSA de 2048 bits, ID 8A365BA2, creada el 2017-03-13
«AlejandroAnton <alejandro@gmail.com>»
http@http-VirtualBox:~/Escritorio$ cat Kristian
Cifrado del madafink boss Krishttp@http-VirtualBox:~/Escritorio$
```

Ejercicio 5: Firma digital de un documento

1. Crea la firma digital de un archivo de texto cualquiera y envíale éste junto al documento con la firma a un compañero.
2. Verifica que la firma recibida del documento es correcta.
3. Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.

```
http@http-VirtualBox:~/Escritorio$ gpg -sb -a alex.txt
Necesita una contraseña para desbloquear la clave secreta
del usuario: "AlejandroAnton <alejandro@gmail.com>"
clave RSA de 2048 bits, ID B133FF81, creada el 2017-03-13

El archivo «alex.txt.asc» ya existe. ¿Sobreescribir? (s/N) s
http@http-VirtualBox:~/Escritorio$ sudo su
root@http-VirtualBox:/home/http/Escritorio# nano alex.txt.asc
root@http-VirtualBox:/home/http/Escritorio# gpg --verify alex.txt.asc
gpg: error de redundancia cíclica: 260968 - 673279
gpg: no se ha encontrado ninguna firma
gpg: la firma no se pudo verificar.
Por favor recuerde que el archivo de firma (.sig o .asc)
debería ser el primero que se da en la línea de órdenes.
root@http-VirtualBox:/home/http/Escritorio#
```