

CRIPTOGRAFIA

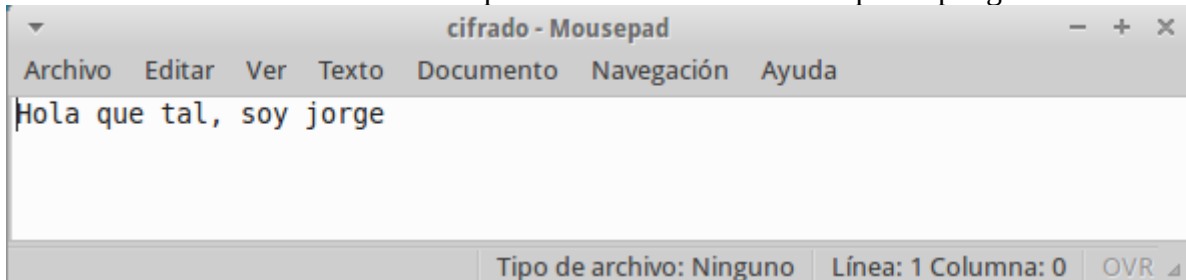
Nombre: Jorge
Apellidos: Boix Vilella
Curso: 2ºF

INDICE

Ejercicio 1: Cifrado simetrico de un documento.....	Página 3
Ejercicio 2: Creación de nuestro par de claves pública-privada.....	Página 5
Ejercicio 3: Exportar e importar claves públicas.....	Página 7
Ejercicio 4: Cifrado y descifrado de un documento.....	Página 8
Ejercicio 5: Firma digital de un documento.....	Página 9

Ejercicio 1: Cifrado simétrico de un documento

- 1.- Crea un documento de texto con cualquier editor o utiliza uno del que dispongas.



- 2.- Cifra este documento con alguna contraseña acordada con el compañero de al lado.

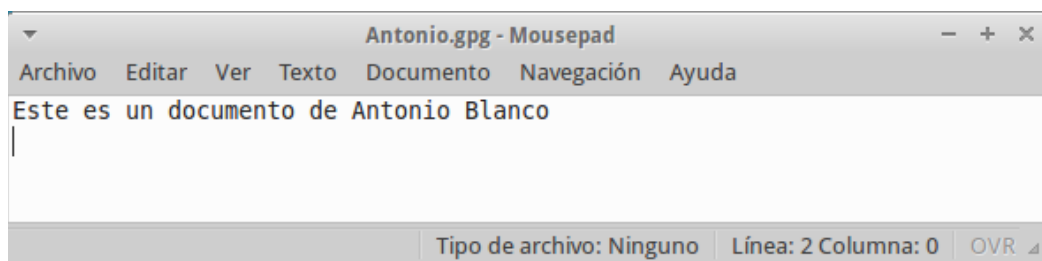
```
root@servidorwjbv:/home/usuario/Escritorio# gpg -c cifrado
gpg: el agente gpg no esta disponible en esta sesión
```

- 3.- Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar.

```
root@servidorwjbv:/home/usuario/Escritorio# scp /home/usuario/Escritorio/cifrado.gpg usuario@192.168.3.63:/home/usuario/Escritorio/cifrado.gpg
The authenticity of host '192.168.3.63 (192.168.3.63)' can't be established.
ECDSA key fingerprint is 91:19:d8:c0:4e:96:fa:ac:38:da:60:93:1c:cb:35:e7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.3.63' (ECDSA) to the list of known hosts.
usuario@192.168.3.63's password:
cifrado.gpg                                100% 70   0.1KB/s   00:00
root@servidorwjbv:/home/usuario/Escritorio#
```

- 4.- Descifra el documento que te ha hecho llegar tu compañero de al lado.

El documento lo he descifrado con **gpg Antonio.gpg**



- 5.- Repite el proceso anterior, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.

```
usuario@servidorwjbv:~/Escritorio$ sudo gpg -ca cifrado
gpg: AVISO: propiedad insegura del archivo de configuración '/home/usuario/.gnupg/gpg.conf'
gpg: el agente gpg no esta disponible en esta sesión
```

```
usuario@servidorwjbv:~/Escritorio$ cat cifrado.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

jA0EAWMCSTS0ll10HGNgYtUEKnJxJfVZZG0mkfFXb4kHfBQBI0XI8Pw0NKlYW8EG
e25lCW8aFZIiwXGxZrg3ZJcfAzfKQ==
=KQRt
-----END PGP MESSAGE-----
```

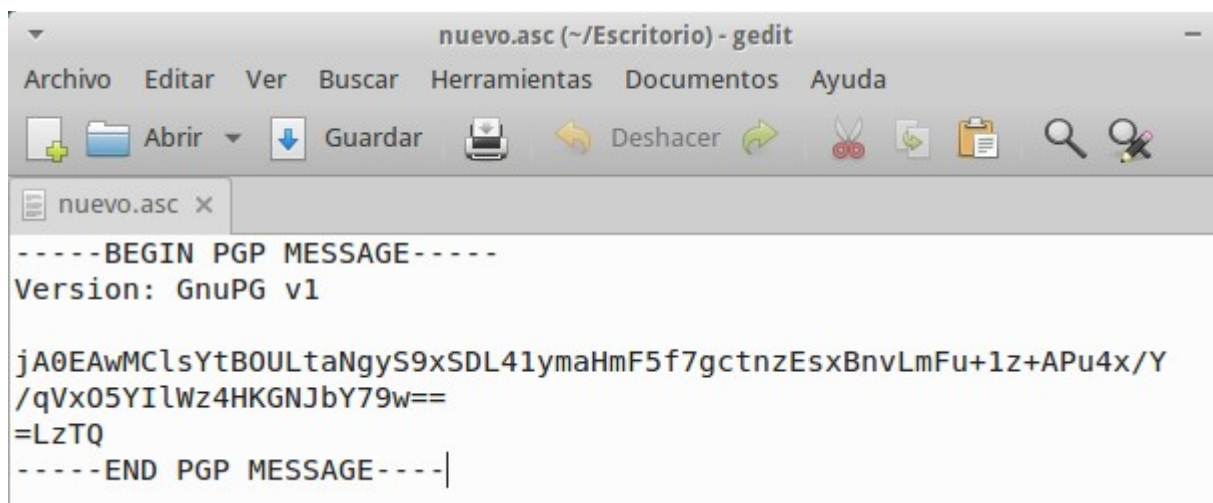
6.- Una vez has recibido el mensaje de tu compañero en tu mail, copialo en un archivo de texto para obtener el mensaje original.

Este es el correo que he recibido de Kevin



```
-----BEGIN PGP MESSAGE-----  
Version: GnuPG v1  
  
jA0EAwMCIsYtBOULtaNgyS9xSDL41ymaHmF5f7gctnzEsxBnvLmFu+1z+  
APu4x/Y  
/qVxO5YIIWz4HKGNJbY79w==  
=LzTQ  
-----END PGP MESSAGE-----
```

Luego el mensaje recibido lo he copiado en un texto y lo he llamado nuevo.asc



A continuación he descifrado el archivo

```
usuario@servidorwjbv:~/Escritorio$ gpg nuevo.asc  
gpg: datos cifrados CAST5  
gpg: cifrado con 1 contraseña  
gpg: AVISO: la integridad del mensaje no está protegida
```

Y por ultimo hago **cat** al archivo que se ha creado para ver su contenido

```
usuario@servidorwjbv:~/Escritorio$ cat nuevo  
Hola que tal Jorgeusuario@servidorwjbv:~/Escritorio$
```

Ejercicio 2: Creación de nuestro par de claves pública-privada

Para este ejercicio hay que crear una clave pública y privada y esto lo hacemos todo con el comando **gpg --gen-key**.

```
usuario@servidorwjbv:~$ gpg --gen-key
gpg (GnuPG) 1.4.16; Copyright (C) 2013 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.

gpg: /home/usuario/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración '/home/usuario/.gnupg/gpg.conf'
gpg: ATENCIÓN: aún no se han activado en esta ejecución las opciones en '/home/usuario/.gnupg/gpg.conf'
gpg: anillo «/home/usuario/.gnupg/secring.gpg» creado
gpg: anillo «/home/usuario/.gnupg/pubring.gpg» creado
```

Una vez ejecutamos el comando nos pide varias cosas

1.- Primero nos pide que seleccionemos el tipo de clave, que en nuestro caso hemos seleccionado la clave por defecto que es la 1

```
Seleccione el tipo de clave deseado:
(1) RSA y RSA (por defecto)
(2) DSA y ElGamal (por defecto)
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
¿Su elección? 1
```

2.- Después tenemos que indicar la longitud de la clave, he seleccionado la por defecto la 2048, ya que a mayor longitud de la clave, más seguridad tendremos

```
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048) 2048
El tamaño requerido es de 2048 bits
```

3.- A continuación debemos indicar el periodo de validez, esto es necesario para que pasado un cierto tiempo, la clave que vamos a crear deje de ser válida. Esto se hace debido a que pasado un tiempo nuestras claves se ven comprometidas por que pueden haber intentado descubrirlas. Nosotros tenemos que indicarle un mes de validez.

```

Especifique el período de validez de la clave.
  0 = la clave nunca caduca
  <n> = la clave caduca en n días
  <n>w = la clave caduca en n semanas
  <n>m = la clave caduca en n meses
  <n>y = la clave caduca en n años
¿Validez de la clave (0)? 1m
La clave caduca jue 06 abr 2017 19:39:59 CEST
¿Es correcto? (s/n) s

```

4.- Cuando hayamos indicado la validez de la clave nos pide que nos identifiquemos poniendo nuestro nombre y nuestro correo y finalmente nos pide una contraseña en mi caso como es una práctica con una máquina virtual he puesto como contraseña “123”

```

Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Jorge Boix Vilella
Dirección de correo electrónico: jorgeboix72@gmail.com
Comentario:
Ha seleccionado este ID de usuario:
  «Jorge Boix Vilella <jorgeboix72@gmail.com>»

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Necesita una contraseña para proteger su clave secreta.

```

5.- Finalmente deberemos hacer procesos aleatorios para que genere nuestra clave y utilice una combinación de bits aleatorias

```

****
gpg: /home/usuario/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave B3AB2747 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: 2017-04-06
pub 2048R/B3AB2747 2017-03-07 [[caduca: 2017-04-06]]
    Huella de clave = ED5E CFBA ACAF D23A 77C0 AF5E 8C3B 606B B3AB 2747
uid                               Jorge Boix Vilella <jorgeboix72@gmail.com>
sub 2048R/C423020F 2017-03-07 [[caduca: 2017-04-06]]

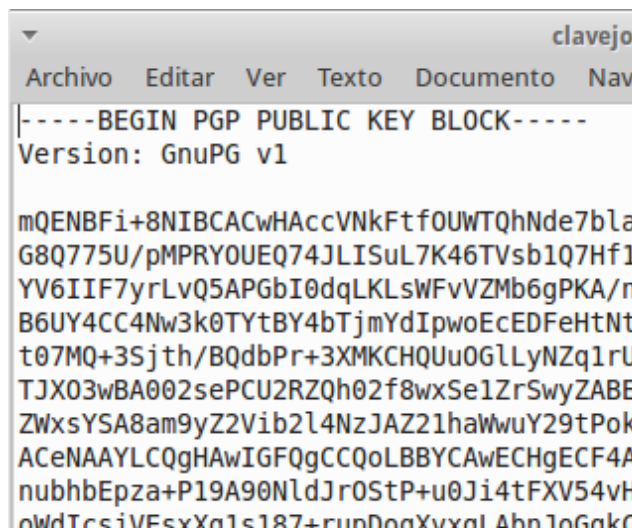
```

Ejercicio 3: Exportar e importar claves públicas.

Lo primero que he hecho ha sido exportar mi clave a un archivo al que he llamado “clavejorge.asc”

```
usuario@servidorwjbv:~$ gpg -a --export -o clavejorge.asc Jorge Boix Vilella
```

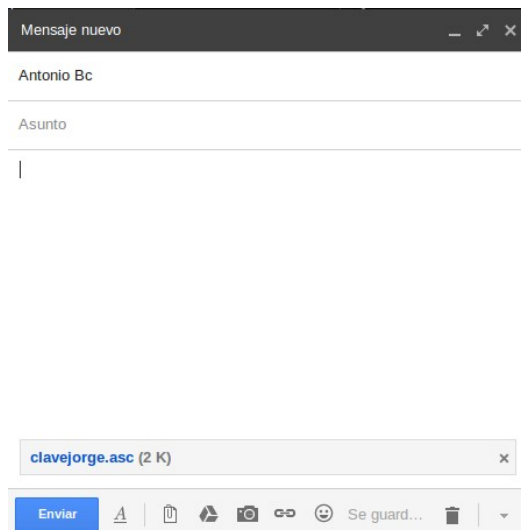
El contenido del fichero contiene lo siguiente (He recortado la imagen para que se vea todo en la misma página)



```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBFi+8NIBCACwHAccVNkFtf0UWTQhNde7b1a
G8Q775U/pMPRY0UEQ74JLISuL7K46TVsb1Q7Hf1
YV6IIF7yrLvQ5APGbI0dqLKLsWFvVZMb6gPKA/r
B6UY4CC4Nw3k0TYtBY4bTjmYdIpwoEcEDFeHtNt
t07MQ+3Sjth/BQdbPr+3XMKCHQUu0GLLyNZq1rL
TJX03wBA002sePCU2RZQh02f8wxSe1ZrSwyZABE
ZWxsYSA8am9yZ2Vib2l4NzJAZ21haWwY29tPok
ACeNAAYLCQgHAWIGFQgCCQoLBBYCAwECHgECF4A
nubhbEpza+P19A90NldJr0StP+u0Ji4tFXV54vH
owdTsivF5xXo1s187+runDooXvxo1Ahn1oGokr
```

A continuación he enviado mi clave en ASCII a un compañero de clase en mi caso se lo he enviado ha Antonio



Un compañero en este caso Kevin me ha enviado su clave pública por correo me he descargado el archivo y lo he importado a mi keyring

```
usuario@servidorwjbv:~$ gpg --import clavekevin.asc
gpg: clave 8AEE263E: clave pública "kevin aznar sempere <rvnmondead@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg: importadas: 1 (RSA: 1)
```


Y por ultimo muestro mi keyring indicando ambas claves

```
usuario@servidorwjbv:~$ gpg -kv
/home/usuario/.gnupg/pubring.gpg
-----
pub   2048R/B3AB2747 2017-03-07 [[caduca: 2017-04-06]]
uid           Jorge Boix Vilella <jorgeboix72@gmail.com>
sub   2048R/C423020F 2017-03-07 [[caduca: 2017-04-06]]

pub   2048R/8AEE263E 2017-03-07 [[caduca: 2017-04-06]]
uid           kevin aznar sempere <rvnmondead@gmail.com>
sub   2048R/D09CDA86 2017-03-07 [[caduca: 2017-04-06]]
```

Ejercicio 4: Cifrado y descifrado de un documento.

Primero he cifrado un archivo en el que dentro ponía un mensaje que solo debe leer Kevin, y lo he cifrado con su clave publica

```
usuario@servidorwjbv:~$ gpg -a -r kevin --encrypt cifrado
gpg: D09CDA86: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

pub   2048R/D09CDA86 2017-03-07 kevin aznar sempere <rvnmondead@gmail.com>
Huella de clave primaria: 3733 871A 6FCE 4117 A1A3 A45D 598A 5C71 8AEE 263E
Huella de subclave: 23BE 6151 3079 461B 8C81 5E25 F470 C702 D09C DA86

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
```

Despues Kevin ha hecho un mensaje parecido al mio y lo ha cifrado con mi clave y me lo ha enviado para luego yo descifrarlo y ver el mensaje

```
usuario@servidorwjbv:~/Descargas$ gpg Cifradojorge.asc

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Jorge Boix Vilella <jorgeboix72@gmail.com>"
clave RSA de 2048 bits, ID C423020F, creada el 2017-03-07 (identificador de clave primaria B3AB2747)

gpg: cifrado con clave RSA de 2048 bits, ID C423020F, creada el 2017-03-07
«Jorge Boix Vilella <jorgeboix72@gmail.com>»
usuario@servidorwjbv:~/Descargas$ cat Cifradojorge
Hola jorge
```

Y por ultimo como se puede observar al otro compañero que he enviado el mensaje cifrado con mi clave al no tenerla no puede descifrarlo

```
usuario@servidorwabc:~/Descargas$ gpg Cifradojorge.asc
gpg: /home/usuario/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración `/home/usuario/.gnupg/gpg.conf'
gpg: ATENCIÓN: aún no se han activado en esta ejecución las opciones en `/
home/usuario/.gnupg/gpg.conf'
gpg: anillo «/home/usuario/.gnupg/secring.gpg» creado
gpg: anillo «/home/usuario/.gnupg/pubring.gpg» creado
gpg: cifrado con clave RSA, ID C423020F
gpg: descifrado fallido: clave secreta no disponible
usuario@servidorwabc:~/Descargas$
```


Ejercicio 5: Firma digital de un documento

Primero he firmado un fichero con un mensaje

```
usuario@servidorwjbv:~$ gpg -sb -a firma  
  
Necesita una contraseña para desbloquear la clave secreta  
del usuario: "Jorge Boix Vilella <jorgeboix72@gmail.com>"  
clave RSA de 2048 bits, ID B3AB2747, creada el 2017-03-07
```

A continuación se lo he enviado a un compañero para que verifique que he sido yo el que ha enviado el fichero y indica que lo he enviado yo

```
usuario@servidorwjbv:~$ gpg --verify firma.asc  
gpg: Firmado el mar 07 mar 2017 20:39:34 CET usando clave RSA ID B3AB2747  
gpg: Firma correcta de «Jorge Boix Vilella <jorgeboix72@gmail.com>»
```

Y después de escribir un carácter aleatorio en el documento firma.asc que es el que contiene mi firma después no se puede verificar

```
usuario@servidorwjbv:~$ gpg firma.asc  
gpg: error de redundancia cíclica: 1DEE1A - B3C083  
gpg: mpi too large for this implementation (26655 bits)
```