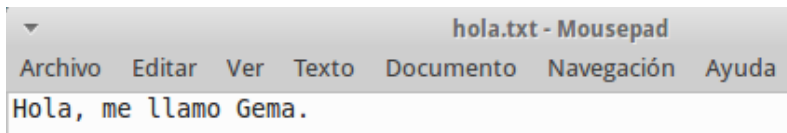


## CIFRADO

### Ejercicio1: Cifrado simétrico de un documento.

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



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

```
usuario@servidorglr:~/Escritorio$ gpg -c hola.txt
```

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

```
usuario@servidorglr:~/Escritorio$ scp /home/usuario/Escritorio/hola.txt.gpg usua
rio@192.168.3.64:/home/usuario/Escritorio/hola.txt.gpg
The authenticity of host '192.168.3.64 (192.168.3.64)' 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 '192.168.3.64' (ECDSA) to the list of known hosts.
usuario@192.168.3.64's password:
hola.txt.gpg                                100% 66    0.1KB/s  00:00
```

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




```
usuario@servidorglr:~/Escritorio$ gpg hola.gpg
gpg: datos cifrados CAST5
gpg: cifrado con 1 contraseña
gpg: AVISO: la integridad del mensaje no está protegida
usuario@servidorglr:~/Escritorio$ cat hola
Hola gema
```

- 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@servidorglr:~/Escritorio$ cat hola.txt.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

jA0EAwMCW8SnxqDum6BgyTExb6KL3UmEJmCCADpx5cYTzYQXZPxndpFOM7n9LHHe
V1H2PTq2tqGTUuS3FUKVJLm1
=7SWV
-----END PGP MESSAGE-----
```

- Copia y pega el contenido del archivo cifrado anteriormente y envíalo por mail a tu compañero para que lo descifre.

 **Gema Lara Rubio** <gemalaru@gmail> 18:58 (l)  
para jorgeboix72 ▾

-----BEGIN PGP MESSAGE-----  
Version: GnuPG v1

jA0EAwMCW8SnxqDum6BgyTExb6KL3U  
mEJmCCADpx5cYTzYQXZPxndpFOM7n9LHHe  
V1H2PTq2tqGTUuS3FUKVJLm1  
=7SWV  
-----END PGP MESSAGE-----

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

```
usuario@servidorglr:~/Escritorio$ gpg Jorge.txt
gpg: datos cifrados CAST5
gpg: cifrado con 1 contraseña
gpg: Jorge.txt: sufijo desconocido
Introduzca nuevo nombre de archivo [hola]: hola
El archivo «hola» ya existe. ¿Sobreescribir? (s/N) s
gpg: AVISO: la integridad del mensaje no está protegida
usuario@servidorglr:~/Escritorio$ cat hola
Hola gema
```

## Ejercicio2: Creación de la pareja de 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. Anotala en un lugar seguro si lo consideras necesario.

Ponemos el comando **gpg --gen-key**.

```
usuario@servidorglr:~$ 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.
```

Nos da 4 opciones a elegir, entre ellas elegimos la 1, RSA y RSA (por defecto)

```
gpg: anillo «/home/usuario/.gnupg/secring.gpg» creado
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
```

Elegimos el tamaño de la clave, en este caso elegimos 2048.

```
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
```

Especificamos el período de validez, en este caso nos pide un mes, por lo cual ponemos 1m.

```
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 vie 07 abr 2017 19:28:49 CEST
¿Es correcto? (s/n) s
```

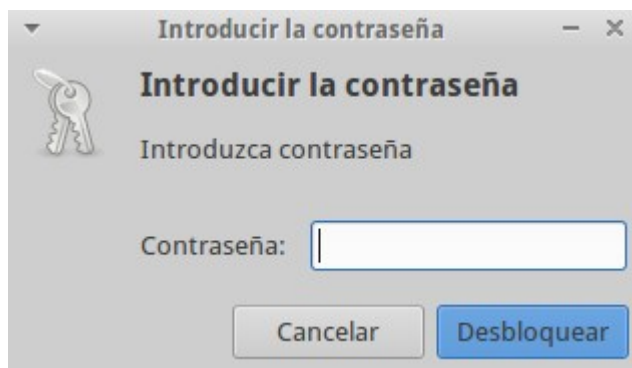
Ponemos nuestro nombre, nuestro correo y un comentario.

```
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: Gema Lara
Dirección de correo electrónico: gemalara@gmail.com
Comentario: Holi mi nombre es Gema
Ha seleccionado este ID de usuario:
    «Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>»
```

Introducimos

una contraseña. Yo he puesto 1234.



Y por último nos indica que se ha creado.

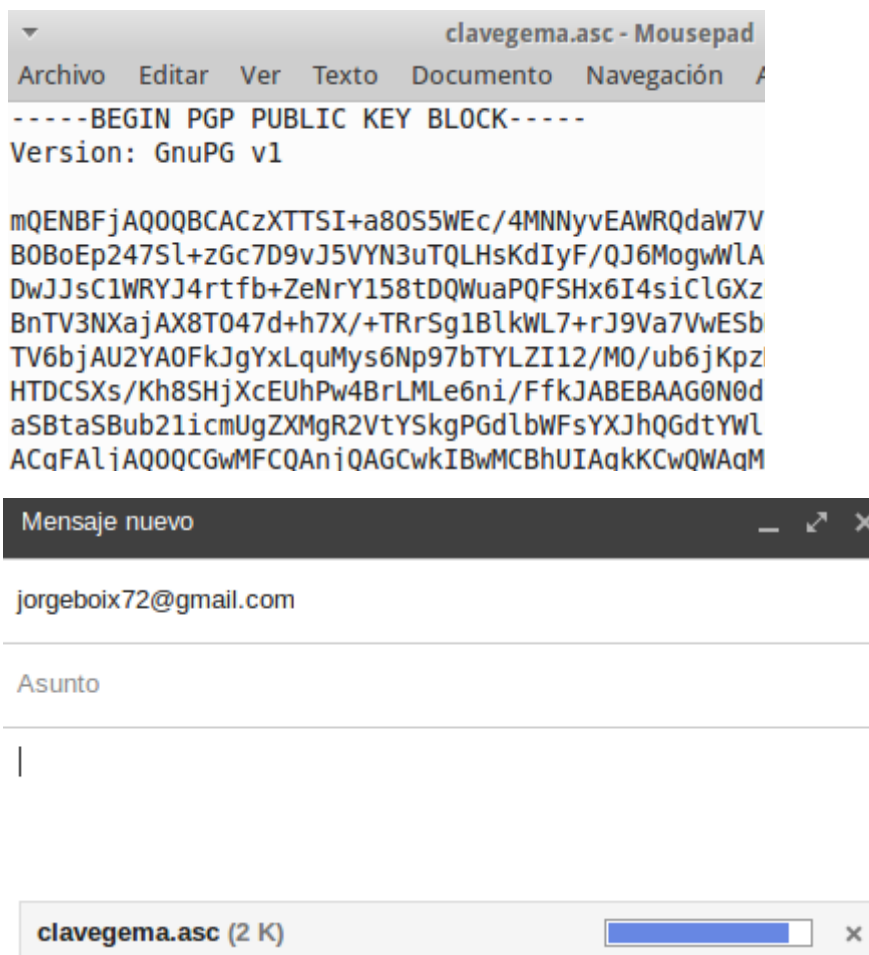
```
gpg: /home/usuario/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave C5035B37 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

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: 2017-04-07
pub 2048R/C5035B37 2017-03-08 [[caduca: 2017-04-07]]
    Huella de clave = 1553 B6DA D463 2A0E 412A F25E 6922 7E44 C503 5B37
uid      Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>
sub 2048R/2BB50C8C 2017-03-08 [[caduca: 2017-04-07]]
```

### Ejercicio3: Exportar e importar claves públicas.

- Exporta tu clave pública en formato ASCII y guárdalo en un archivo nombre\_apellido.asc y envíalo a un compañero/a.

```
usuario@servidorglr:~/Escritorio$ gpg -a --export -o clavegema.asc Gema Lara
```



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

```
usuario@servidorglr:~/Escritorio$ gpg --import clavejorge.asc
gpg: clave B3AB2747: clave pública "Jorge Boix Vilella <jorgeboix72@gmail.com>"
importada
gpg: Cantidad total procesada: 1
gpg: importadas: 1 (RSA: 1)
```

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

```
usuario@servidorglr:~/Escritorio$ gpg -kv
/home/usuario/.gnupg/pubring.gpg
-----
pub  2048R/C5035B37 2017-03-08 [[caduca: 2017-04-07]]
uid          Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>
sub  2048R/2BB50C8C 2017-03-08 [[caduca: 2017-04-07]]

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]]
```

### Ejercicio4: Cifrado y descifrado de un documento.

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

```
usuario@servidorglr:~/Escritorio$ gpg -a -r Jorge --encrypt cifrado
gpg: C423020F: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

pub 2048R/C423020F 2017-03-07 Jorge Boix Vilella <jorgeboix72@gmail.com>
Huella de clave primaria: ED5E CFBA ACAF D23A 77C0 AF5E 8C3B 606B B3AB 2747
Huella de subclave: C03E 4017 FEFD 490E E15B A929 CE0C 4464 C423 020F

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
```

- Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos.

```
usuario@servidorglr:~/Escritorio$ gpg hola.asc

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>"
clave RSA de 2048 bits, ID 2BB50C8C, creada el 2017-03-08 (identificador de clave
primaria C5035B37)

gpg: cifrado con clave RSA de 2048 bits, ID 2BB50C8C, creada el 2017-03-08
«Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>»
```

- Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.

```
usuario@servidorglr:~/Escritorio$ cat hola
hola gema
```

- 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.

```
Terminal - usuario@servidorwabc: ~/Descargas
Archivo Editar Ver Terminal Pestañas Ayuda
usuario@servidorwabc:~/Descargas$ gpg hola.asc
gpg: cifrado con clave RSA de 2048 bits, ID C423020F, creada el 2017-03-07
«Jorge Boix Vilella <jorgeboix72@gmail.com>»
gpg: descifrado fallido: clave secreta no disponible
usuario@servidorwabc:~/Descargas$
```



### Ejercicio5: Firma digital de un documento.

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

```
usuario@servidorglr:~/Escritorio$ gpg -sb -a documentofirmar

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>"
clave RSA de 2048 bits, ID C5035B37, creada el 2017-03-08

gpg: Frase contraseña incorrecta; inténtelo de nuevo. ...

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>"
clave RSA de 2048 bits, ID C5035B37, creada el 2017-03-08

gpg: Frase contraseña incorrecta; inténtelo de nuevo. ...

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>"
clave RSA de 2048 bits, ID C5035B37, creada el 2017-03-08
```

```
usuario@servidorglr:~/Escritorio$ gpg documentofirmar.asc
gpg: Firmado el vie 10 mar 2017 18:11:35 CET usando clave RSA ID C5035B37
gpg: Firma correcta de «Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>»
```

```
usuario@servidorglr:~/Escritorio$ gpg --verify documentofirmar.asc
gpg: Firmado el vie 10 mar 2017 18:11:35 CET usando clave RSA ID C5035B37
gpg: Firma correcta de «Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>»
```

```
usuario@servidorglr:~/Escritorio$ gpg -a --sign documentofirmar

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>"
clave RSA de 2048 bits, ID C5035B37, creada el 2017-03-08

El archivo «documentofirmar.asc» ya existe. ¿Sobreescribir? (s/N) s
```

```
usuario@servidorglr:~/Escritorio$ gpg --verify documentofirmar.asc
gpg: Firmado el vie 10 mar 2017 18:15:27 CET usando clave RSA ID C5035B37
gpg: Firma correcta de «Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>»
usuario@servidorglr:~/Escritorio$ gpg --decrypt -o documentooriginal documentofirmar.asc
gpg: Firmado el vie 10 mar 2017 18:15:27 CET usando clave RSA ID C5035B37
gpg: Firma correcta de «Gema Lara (Holi mi nombre es Gema) <gemalara@gmail.com>»
```