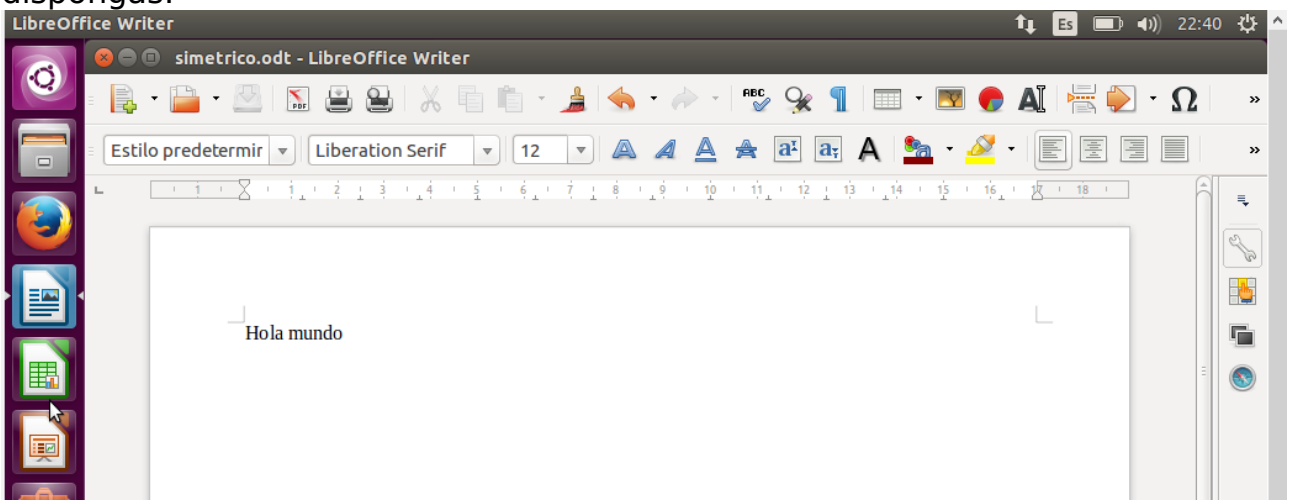
Cifrado simétrico de un documento

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



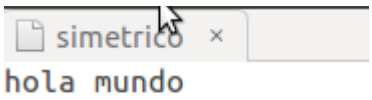
2. Cifra este documento con alguna contraseña acordada con el compañero de al lado.

```
root@aaron-VirtualBox:/home# gpg -c simetrico
gpg: el agente gpg no esta disponible en esta sesión
El archivo «simetrico.gpg» ya existe. ¿Sobreescribir? (s/N) s
root@aaron-VirtualBox:/home# ls
aaron  simetrico  simetrico.gpg
root@aaron-VirtualBox:/home#
```

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

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

```
root@aaron-VirtualBox:/home/aaron/Descargas# gpg simetrico.gpg
gpg: datos cifrados CAST5
gpg: el agente gpg no esta disponible en esta sesión
gpg: cifrado con 1 frase contraseña
gpg: AVISO: la integridad del mensaje no está protegida
root@aaron-VirtualBox:/home/aaron/Descargas#
```

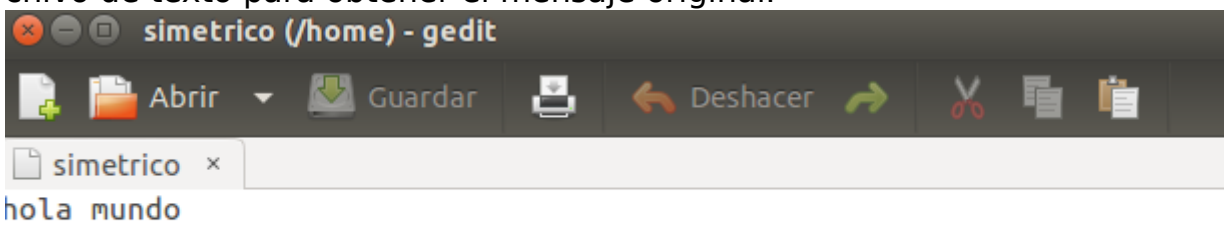


5. Repite el proceso anterior, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.

```
root@aaron-VirtualBox:/home/aaron/Descargas# gpg -a simetrico.gpg
gpg: datos cifrados CAST5
gpg: el agente gpg no esta disponible en esta sesión
gpg: cifrado con 1 frase contraseña
El archivo «simetrico» ya existe. ¿Sobreescribir? (s/N) s
gpg: AVISO: la integridad del mensaje no está protegida
root@aaron-VirtualBox:/home/aaron/Descargas# cat simetrico.gpg
[illegible] root@aaron-VirtualBox:/h
```

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

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



Creación de nuestro par de claves publicas-privadas

1.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.

```
root@aaron-VirtualBox:/home# gpg --gen-key
gpg (GnuPG) 1.4.18; Copyright (C) 2014 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: anillo «/root/.gnupg/secring.gpg» creado
Por favor seleccione tipo de clave deseado:
   (1) DSA y ElGamal (por defecto)
   (2) DSA y ElGamal (por defecto)
   (3) DSA (sólo firmar)
   (4) RSA (sólo firmar)
¿Su selección?: 1
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
Por favor, 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)? m
valor inválido
¿Validez de la clave (0)? 1m
La clave caduca jue 06 abr 2017 21:30:41 CEST
¿Es correcto? (s/n) s

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:
```

```
No hay suficientes bytes aleatorios disponibles. Por favor, haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 92 bytes más).
...+++++

No hay suficientes bytes aleatorios disponibles. Por favor, haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 100 bytes más).
+++++
gpg: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 8A72C4D7 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
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/8A72C4D7 2017-03-07 [[caduca: 2017-04-06]]
      Huella de clave = 9FDE 1CCA CD3C AE3B 29BF  9903 B8E7 1996 8A72 C4D7
uid                  aaron
sub   2048R/63AFAD6E 2017-03-07 [[caduca: 2017-04-06]]
```

Exportar e importar claves publicas

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

```
root@aaron-VirtualBox:/home/aaron/Escritorio# gpg -a --export -o Aaron_Agullo.asc aaron
root@aaron-VirtualBox:/home/aaron/Escritorio# ls
Aaron_Agullo.asc  simetrico.odt
```

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

```
aaron@aaron-VirtualBox:~/Descargas$ gpg -a --import Aaron_Agullo.asc
gpg: /home/aaron/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración `/home/aaron/.gnupg/gpg.conf'
gpg: AVISO: las opciones en `/home/aaron/.gnupg/gpg.conf' no están aún activas e
n esta ejecución
gpg: anillo «/home/aaron/.gnupg/secring.gpg» creado
gpg: anillo «/home/aaron/.gnupg/pubring.gpg» creado
gpg: /home/aaron/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 8A72C4D7: clave pública "aaron" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1  (RSA: 1)
```

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

```
aaron@aaron-VirtualBox:~$ gpg -kv
/home/aaron/.gnupg/pubring.gpg
------------------------------
pub   2048R/8A72C4D7 2017-03-07 [[caduca: 2017-04-06]]
uid                  aaron
sub   2048R/63AFAD6E 2017-03-07 [[caduca: 2017-04-06]]
```

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.

```
root@aaron-VirtualBox:/home/aaron/Escritorio# gpg -a -r aaron --encrypt simetrico.odt
root@aaron-VirtualBox:/home/aaron/Escritorio# ls
Aaron_Aguilo.asc  simetrico.odt  simetrico.odt.asc
```

2.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.

```
gpg: cifrado con clave RSA, ID 63AFAD6E
gpg: descifrado fallido: clave secreta no disponible
```

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.

```
root@aaron-VirtualBox:/home/aaron/Escritorio# gpg -sb -a hola.txt

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "aaron"
clave RSA de 2048 bits, ID 8A72C4D7, creada el 2017-03-07
```

2.Verifica que la firma recibida del documento es correcta.

```
root@aaron-VirtualBox:/home/aaron/Escritorio# gpg --verify hola.txt.asc
gpg: asumiendo que hay datos firmados en «hola.txt»
gpg: Firmado el mar 07 mar 2017 23:22:45 CET usando clave RSA ID 8A72C4D7
gpg: Firma correcta de «aaron»
```

3.Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.

```
root@aaron-VirtualBox:/home/aaron/Escritorio# gpg --verify hola.txt.asc
gpg: asumiendo que hay datos firmados en «hola.txt»
gpg: Firmado el mar 07 mar 2017 23:22:45 CET usando clave RSA ID 8A72C4D7
gpg: Firma INCORRECTA de «aaron»
```