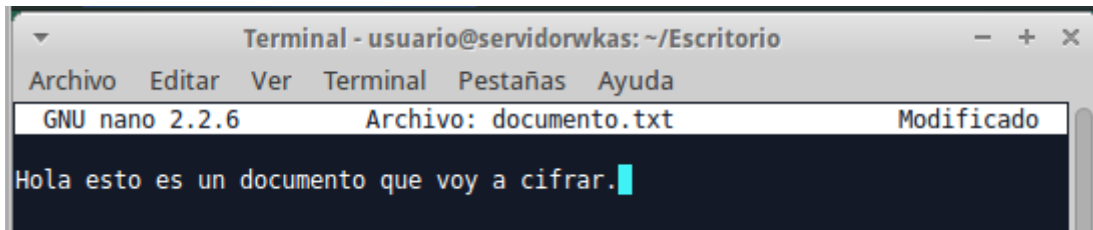
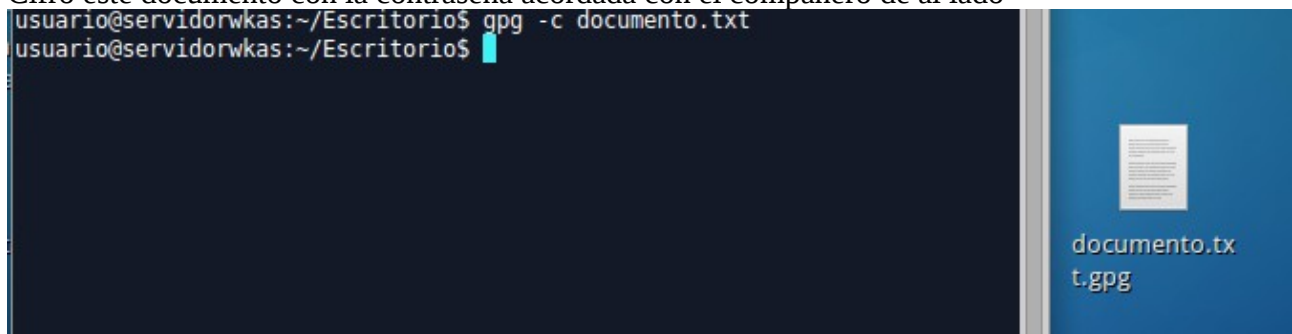


## Ejercicio 1: Cifrado simétrico de un documento

Voy a crear un documento de texto usando el editor nano desde el terminal



Cifro este documento con la contraseña acordada con el compañero de al lado



Voy a descifrar el documento que me ha hecho llegar mi compañero Jorge. El fichero se llama cifrado.gpg

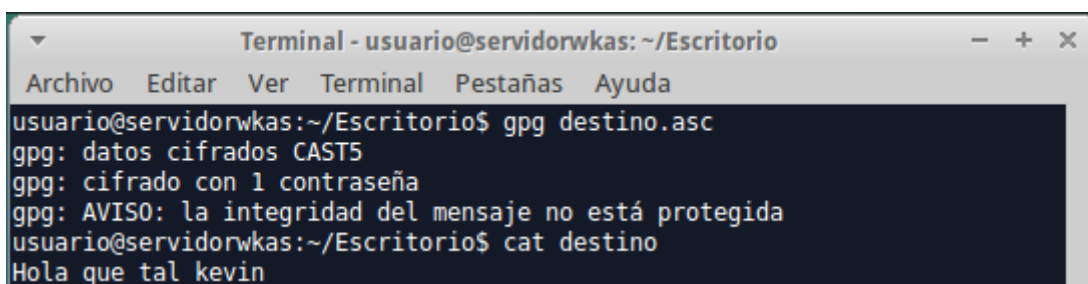
```
usuario@servidorwkas:~/Escritorio$ gpg cifrado.gpg
gpg: datos cifrados CAST5
gpg: cifrado con 1 contraseña
gpg: AVISO: la integridad del mensaje no está protegida
usuario@servidorwkas:~/Escritorio$
```

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@servidorwkas:~/Escritorio$ gpg -ca cifrado
usuario@servidorwkas:~/Escritorio$ cat cifrado.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

jA0EAwMC00D0mL1xzghgyS+r/kmKmNVK5pmK6qBLzUCfDTSHlKT3EM4+CvMHRMsJ
K7BtEBEklSs+zLD5iUl3ZQ==
=N6Rl
-----END PGP MESSAGE-----
usuario@servidorwkas:~/Escritorio$
```

Jorge me ha mandado por correo el contenido de su cifrado.asc, ahora voy a añadirlo a un fichero y a descifrar lo que me acaba de mandar. Al descifrarlo voy también a mostrar su contenido.



## **Ejercicio 2: Creación de nuestro par de claves publica-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.

```
usuario@servidorwkas:~/Escritorio$ 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.

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
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
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 21:01:01 CEST
¿Es correcto? (s/n) s
```

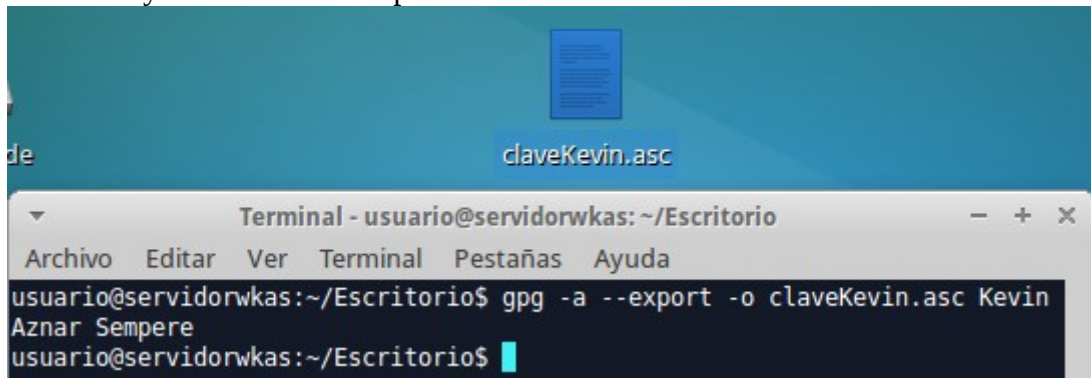
He seguido todos los pasos hasta que finalmente la he creado correctamente

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

El ID de usuario que he introducido es Kevin Aznar Sempere y la contraseña a utilizar es 123

### Ejercicio 3: Exportar e importar claves públicas

He exportado mi clave pública en forma ASCII y guardado en un archivo denominado ClaveKevin.asc y enviado a un compañero



A continuación voy a importar la clave pública que he recibido de Jorge.

```
usuario@servidorwkas:~$ 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)
```

Compruebo que las claves se han incluido correctamente en el keyring

```
usuario@servidorwkas:~$ gpg -kv
/home/usuario/.gnupg/pubring.gpg
-----
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]]

pub  2048R/21E673D4 2017-03-07 [[caduca: 2017-04-06]]
uid  Kevin Aznar Sempere <rvnmondead@gmail.com>
sub  2048R/09822E46 2017-03-07 [[caduca: 2017-04-06]]

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]]

usuario@servidorwkas:~$
```

## Ejercicio 4: Cifrado y descifrado de un documento

Voy a cifrar un archivo cualquiera y lo enviaré por email a mi compañero jorge que nos proporcionó su clave publica anteriormente


```
usuario@servidorwkas:~/Escritorio$ gpg -a -r Jorge --encrypt documento.txt
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>
Huellas de clave primaria: ED5E CFBA ACAF D23A 77C0 AF5E 8C3B 606B B3AB 27
47
Huellas de subclave: C03E 4017 FEFD 490E E15B A929 CE0C 4464 C423 020
F

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
usuario@servidorwkas:~/Escritorio$
```

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



cifrado.asc    clavejorge.asc

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

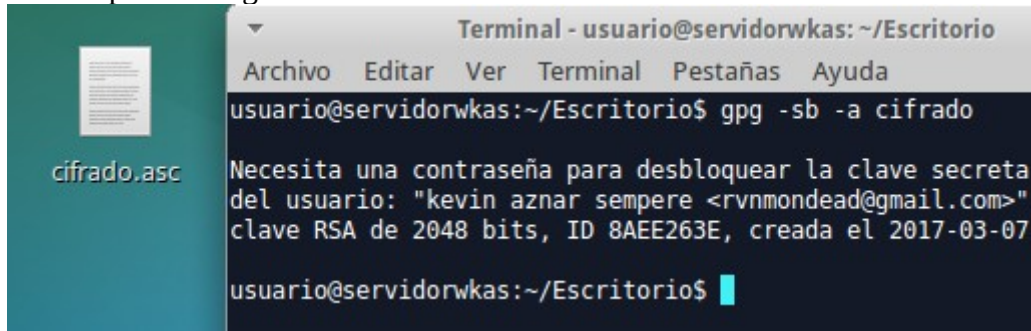
```
usuario@servidorwkas:~$ gpg cifrado.asc

Necesita una contraseña para desbloquear la clave secreta
del usuario: "kevin aznar sempere <rvnmondead@gmail.com>"
clave RSA de 2048 bits, ID D09CDA86, creada el 2017-03-07 (identificador de
clave primaria 8AEE263E)

gpg: cifrado con clave RSA de 2048 bits, ID D09CDA86, creada el 2017-03-07
«kevin aznar sempere <rvnmondead@gmail.com>»
usuario@servidorwkas:~$ cat cifrado
Hola que tal kevin
usuario@servidorwkas:~$
```

## Ejercicio 5: Firma digital de un documento

He creado la firma digital de un archivo de texto cualquiera y enviado éste junto al documento con la firma a mi compañero Jorge



```
Terminal - usuario@servidorwkas: ~/Escritorio
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
usuario@servidorwkas:~/Escritorio$ gpg -sb -a cifrado
Necesita una contraseña para desbloquear la clave secreta
del usuario: "kevin aznar sempere <rvnmondead@gmail.com>"
clave RSA de 2048 bits, ID 8AEE263E, creada el 2017-03-07
usuario@servidorwkas:~/Escritorio$
```

Voy a verificar que la firma recibida del documento es correcta.

```
usuario@servidorwkas:~/Escritorio$ gpg --verify cifrado.asc
gpg: Firmado el mar 07 mar 2017 20:38:54 CET usando clave RSA ID 8AEE263E
gpg: Firma correcta de «kevin aznar sempere <rvnmondead@gmail.com>»
usuario@servidorwkas:~/Escritorio$
```

Ahora modificaré el archivo ligeramente, insertando un carácter, en concreto una A y he vuelto a comprobar si la firma se verifica.

```
usuario@servidorwkas:~/Escritorio$ gpg --verify cifrado.asc
gpg: error de redundancia cíclica: B3C168 - E78A76
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.
usuario@servidorwkas:~/Escritorio$
```