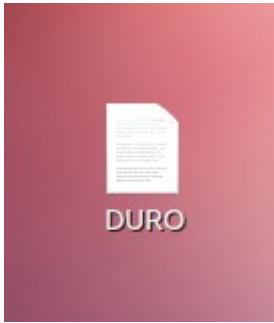


Ejercicio1

Creo el documento



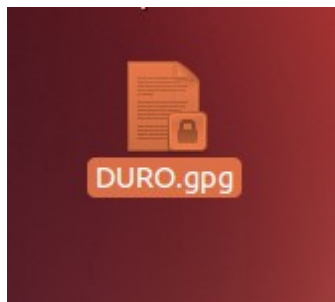
Lo cifro

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -c DURO
```

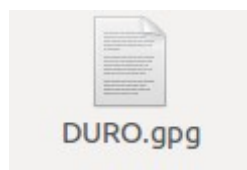
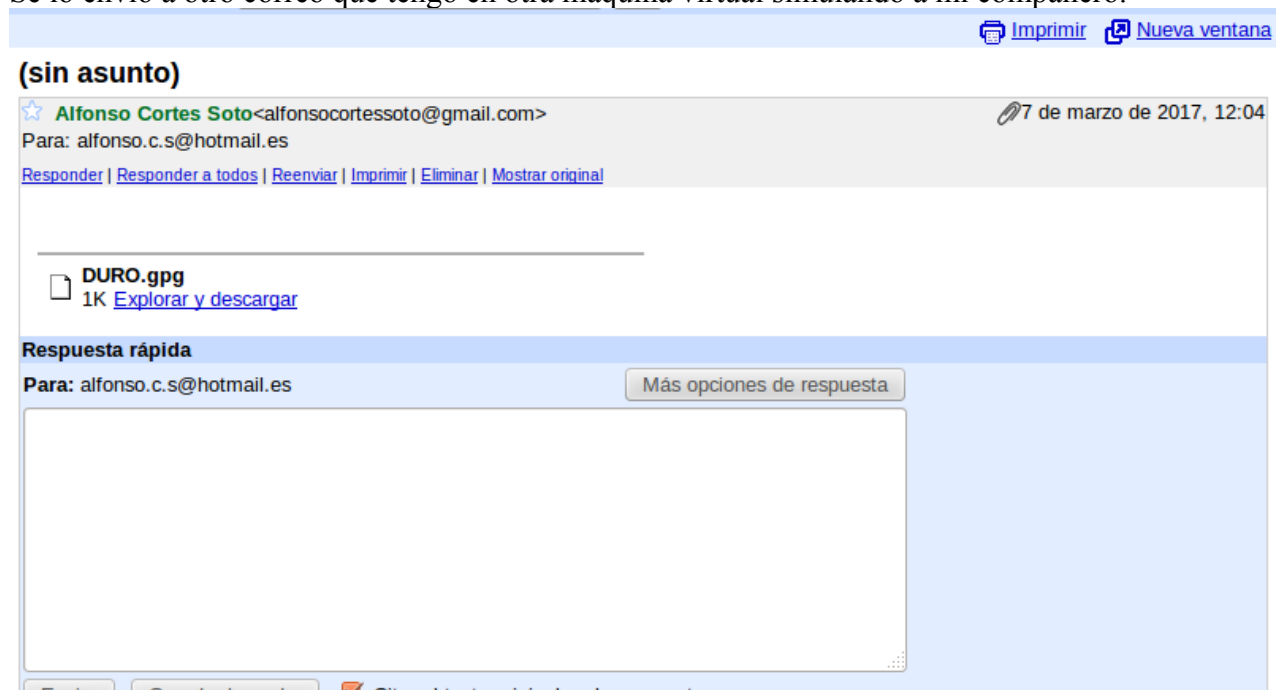
Le asigno una contraseña que es 123

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -c DURO
gpg: el agente gpg no esta disponible en esta sesión
Introduzca frase contraseña: 
```

Me aparecerá el documento encriptado



Se lo envió a otro correo que tengo en otra maquina virtual simulando a mi compañero.



Descifro el documento que e enviado ami otra maquina.

```
root@alfonso-VirtualBox:/home/alfonso/Descargas# gpg DURO.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@alfonso-VirtualBox:/home/alfonso/Descargas#
```



Lo descifro pe añado -a

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

```
root@alfonso-VirtualBox:/home/alfonso/Descargas# cat DURO.gpg
```

 [Imprimir](#)  [Nueva ventana](#)

Barakuya Barakuya<barakuya98@gmail.com>
Para: alfonso cortessoto@gmail.com

7 de marzo de 2017, 12:34

[Responder](#) | [Responder a todos](#) | [Reenviar](#) | [Imprimir](#) | [Eliminar](#) | [Mostrar original](#)

DURO.gpg
1K [Explorar y descargar](#)

Respuesta rápida

Para: Barakuya Barakuya <barakuya98@gmail.com>

Más opciones de respuesta

Ejercicio2

Creo una calve publica elijo la primera la predeterminada.

```
root@alfonso-VirtualBox: /home/alfonso
alfonso@alfonso-VirtualBox:~$ sudo su
[sudo] password for alfonso:
root@alfonso-VirtualBox:/home/alfonso# gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 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: /root/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración '/root/.gnupg/gpg.conf'
gpg: AVISO: las opciones en '/root/.gnupg/gpg.conf' no están aún activas en esta
ejecución
gpg: anillo «/root/.gnupg/secring.gpg» creado
gpg: anillo «/root/.gnupg/pubring.gpg» creado
Por favor seleccione tipo de clave deseado:
  (1) RSA y RSA (predeterminado)
  (2) DSA y Elgamal
  (3) DSA (sólo firmar)
  (4) RSA (sólo firmar)
¿Su selección?:
```

Le añado una longitud 2028

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

Elijo el periodo de un mes poniendo 1m

```
Por favor, especifique el periodo 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)?
```

```
¿Validez de la clave (0)? 1m
La clave caduca jue 06 abr 2017 12:22:51 CEST
¿Es correcto? (s/n)
```

Creo un identificador de usuario

```
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: Alfonso Cortés Soto
```

```
Dirección de correo electrónico: alfonso cortessoto@gmail.com
```

Y le añado la contraseña para proteger la clave.

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

Ejercicio3

Mi clave publica

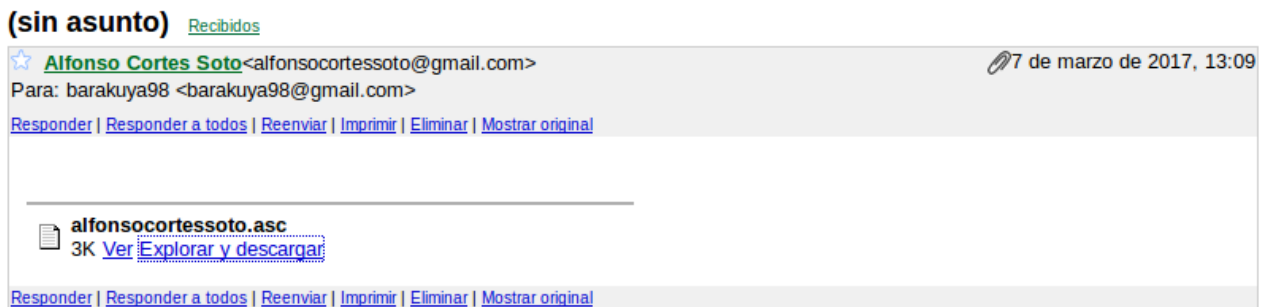
```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -a --export Alfonso Cortés
Soto
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQENBFi+i5sBCADV4ugRtOgCbJ2bK28rD3gN6auf8b0x8Kfsr0LGZGjDiP+TsmvR
ARqyPsVYCQrvX7kNG4ASgoQW3MG0iXLjVYPqTXgx3XDqSIWPCntEvYjOwkpmLBKS
+ZRMvqEdnajRxmI+y2ybLHpRMmxwv/P/x41NU3H0DbvgqfEFowbMnf7dJO6M5Zel
SIg/wEq/Wlvvsm5FRBlq62napxnpENBFeg70oHJ2Z1gyLKNwWAZQM+xFa+eWlJjK
jQ7ojkngqF+So4NL/stJmTZto2k8XkqysRJJ3IRK7Z7bhl1DPE0bTHzHjSrZTLx
/c2mL/OIzIl1gMi2v9DuSKsqT9cHb96li3FLABEBAAG0QEFsZm9uc28gQ29ydM0p
cyBTb3RvIChEdXJvIEJsYW5kbykgPGFsZm9uc29jb3J0ZXNzb3RvQGdtYWlsLmNv
bT6JAT4EEwECACgFali+i5sCGwMFCQAnjQAGCwkIBwMCBhUIAgkKCwQWAgMBAh4B
AheAAAOJEMXo2hd5uG80htkIAMuXSYpd1mSYtEPpTimhLh3DttvVzG60t8jdhPQe
tZ9Lv95VJmd46xR1SHK5L4HHodCILqPHdL4A/OWTUbuqmpSTLUCNkt0d/PQ0ewWs
xkAp1170TWYk/sNmody3qBgHQcICIH3tz10QQTpSJr+IcFJR5zQ8juPdavC1Ng5YJ
vzM0pdilLccLjBTu7WwE4lyFYHxH3Y5zZmcE178Nsx9sPnebCqt6i3mo0JLY2UzIb
tLoTs3LTdaPVuHgnvSQnuazUjqsYfNNngF9x0dX6tiYeJCcqRUKIUbLaj1MU7nlj
ZtPmGab6ImTJXN87N7g0iLhL+0+Jy36/iIBptVAht0UzpqA5AQ0EwL6LmwEIAK6F
Lm3tA2CVKa41oTxnws0Co63MznV0TH5VdbGBiTvmLvHG1h1tvNkoHvPsqRFmsb3p
lJmsN6qlhYR+0LKIXLWwYYni04/LBBcD2RNFe3c7HaifEL/psu9aFBsTOb78P53h
egVuqdn574kuqdrJU80jUy8bGtbAADaN82vx+cwagY9W5wfw+FctwosjWId0DfmC
CNYhEhDSwpg/mIlh/8MmstjYE1YP/LINq89YRsD5q5jrTI7smNwkSgEkFKGnvu+n
2vYJHnhLeMZ08+9MWV/LojbabMQS/Gpmt9n3Hm40UV17YyyFCcdRX+5yhIasKK/t
oU02I8ZF1iBQ0mfYcH0AEQEAAyKBjJQQAQIADwUCWL6LmwIbDAUJACeNAAAKCRDF
6NoQ+bhvDkepB/95w75mtVUIhDh95n+S16vDEwUBdNiUYUiYQMZjkfBmB1uhaQ31
NyXJIJo/Slji7QMYu0+V0hhXGg4KddFhkPsNujrrJzkY8l71czBZg2zu8eZfRwbU
9ITwf82KNWtltzBh+6yDGP7cDRiCYUqyShCdjhNtLp2zm5PApBiRFpPryaj/+JyQ
m3HbDegua849d0nUGOX7/UB3TASbpGBG/lNqPkSC3y2kLAWw01jNFm88Ttnb4iVi
lgvjw0TMvb7pb/tnjWe1Tn4utcbi8RRDgBPnGrzAz7E6Yot/kW9zq/ie7/gpsCu
KAjDoShYeeTB9ufqDae3JD2AneYN4sboG8RnmI0EWL85wQEEAKzgCkV0bL2q+v00
9YR1xp9mditnDzMcrJZvN0pzlA8Z9Iq679bHa0TbhNvrqAoQUXtRyj2LTS0nFAtG
njHxT/Flx5yDl7Ha29P15XUaHPgPD/EA49cfNiOp0jtnIRA1vCMbddbJmx8bqzXo
FGn00QdYlgxU22JgrlbXTp2gueSdABEBAAG0LkFsZm9uc28gQ29ydM0pcyAoZHVy
bykgPGFsZm9uc28uYy5zQGdtYWlsLmNvbT6IvgQTAQIAKAUCWL85wQIbAwUJACeN
```

Lo exporto

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -a --export -o alfonsocortes.acs Alfonso Cortés Soto
```

Lo envié a mi otro correo que lo tengo abierto en otra maquina virtual simulando la de mi compañero.



Lo e recibido



Lo importo

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg --import alfonso cortessoto.asc
```

Compruebo que se a incluido en mi keyring

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -kv
/root/.gnupg/pubring.gpg
-----
pub 2048R/F9B86F0E 2017-03-07 [[caduca: 2017-04-06]]
uid Alfonso Cortés Soto (Duro Blando) <alfonsocortessoto@gmail.com>
```

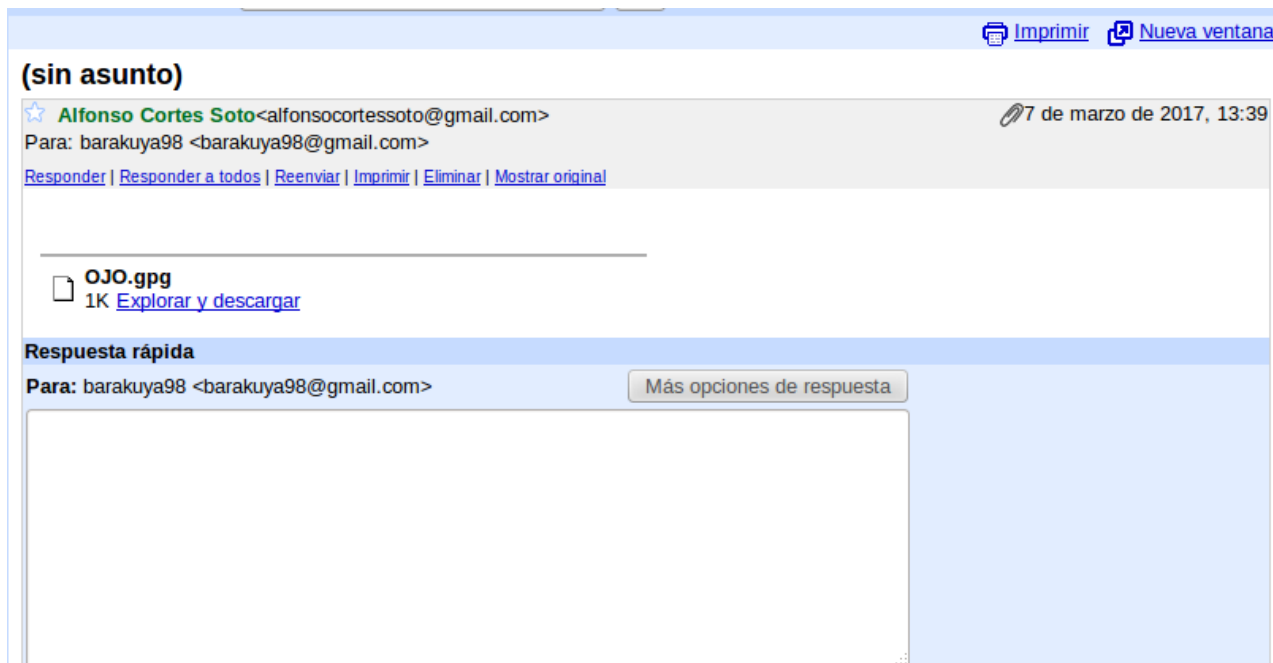
Ejercicio4

Cifro un archivo

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -c OJO
```



Se lo envi a mi otra cuenta de email que esta activa en otra maquina virtual.

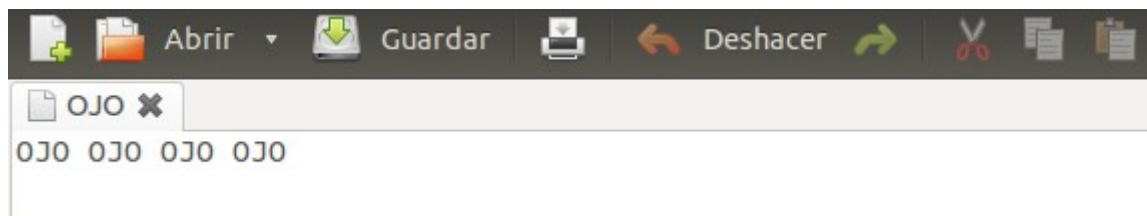


Lo descifro

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg OJO.gpg
gpg: datos cifrados CAST5
gpg: el agente gpg no esta disponible en esta sesi n
Introduzca frase contrase a:
```

Y introduzco la contrase a que le e puesto.

Y me deja ver lo que contiene.



Ejercicio5

Creo un documento



Le creo una firma

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -sb -a BIEN
```


Lo envié a mi otro correo activado en otra maquina virtual

Para: "barakuya98" <barakuya98@gmail.com>

Cc:

Cco:

Asunto:

Archivos adjuntos:

/home/alfonso/Escritorio/BIEN.asc [Browse...](#)

[Adjuntar más archivos](#)

Confirmo que lo recibido

[Imprimir](#) [Nueva ventana](#)

(sin asunto) [Recibidos](#)

★ **Alfonso Cortes Soto** <alfonsocortessoto@gmail.com> 8 de marzo de 2017, 0:29

Para: barakuya98 <barakuya98@gmail.com>

[Responder](#) | [Responder a todos](#) | [Reenviar](#) | [Imprimir](#) | [Eliminar](#) | [Mostrar original](#)

BIEN.asc
1K [Ver](#) [Explorar y descargar](#)

Respuesta rápida

Para: Alfonso Cortes Soto <alfonsocortessoto@gmail.com> [Más opciones de respuesta](#)

Verifico si el documento va firmado.

```
root@alfonso-VirtualBox:/home/alfonso/Descargas# gpg --decrypt -o BIEN BIEN.asc
El archivo «BIEN» ya existe. ¿Sobreescribir? (s/N) s
gpg: Firmado el mar 07 mar 2017 14:37:22 CET usando clave RSA ID F9B86F0E
gpg: Firma correcta de «Alfonso Cortés Soto (Duro Blando) <alfonsocortessoto@gmail.com>»
root@alfonso-VirtualBox:/home/alfonso/Descargas#
```

Modifico el documento.

[Abrir](#) [Guardar](#) [Imprimir](#) [Deshacer](#) [Recortar](#) [Copiar](#) [Pegar](#) [Buscar](#) [Editar](#)

*BIEN x

BIEN

Verifico que después de modificarlo sigue la firma.

```
root@alfonso-VirtualBox:/home/alfonso/Descargas# gpg --decrypt -o BIEN BIEN.asc
El archivo «BIEN» ya existe. ¿Sobreescribir? (s/N) s
gpg: Firmado el mar 07 mar 2017 14:37:22 CET usando clave RSA ID F9B86F0E
gpg: Firma correcta de «Alfonso Cortés Soto (Duro Blando) <alfonsocortessoto@gmail.com>»
```