Ejercicio1

Creo el documento

Lo cifro

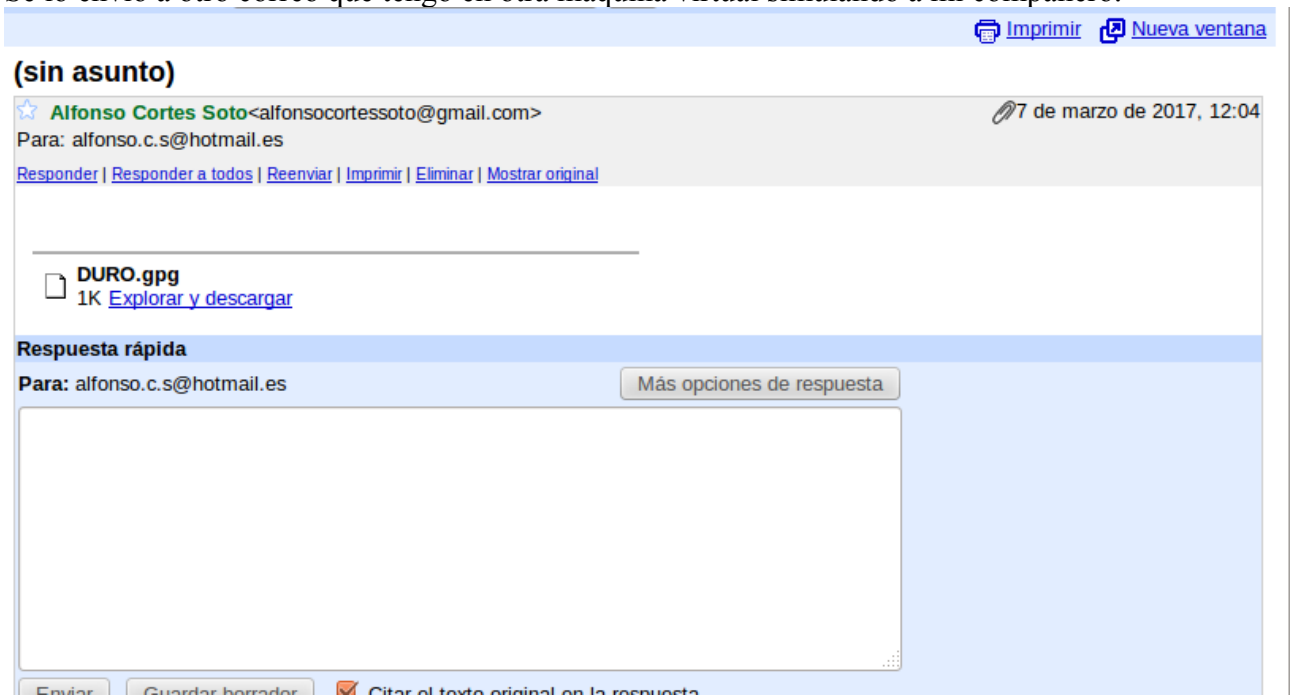
```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -c DURO
```

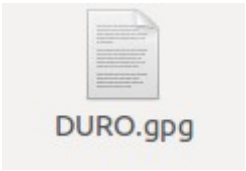
Le asigno una contraseña que es 123

```
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#
```

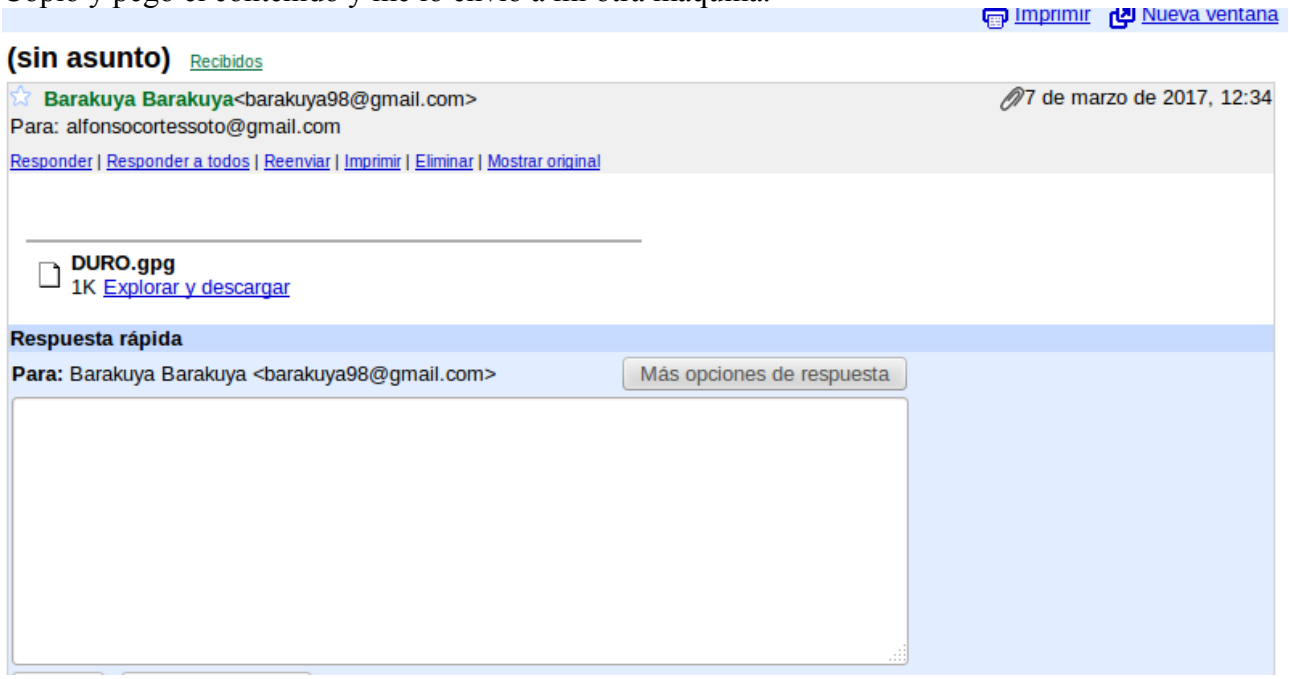
Lo descifro pe añado -a

```
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#
```

Y ejecuto con el comando cat

```
root@alfonso-VirtualBox:/home/alfonso/Descargas# cat DURO.gpg
[illegible]ux` [illegible]J)3ġ[illegible]!*=0{[illegible]sV[illegible]proot@alfonso-VirtualBox:/home/alfonso/
Descargas#
```

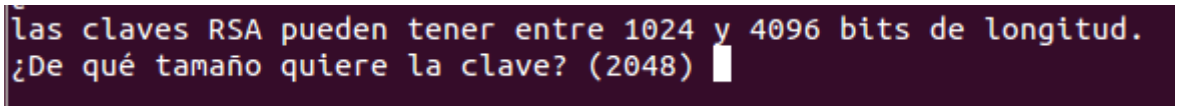
Copio y pego el contenido y me lo envió a mi otra maquina.



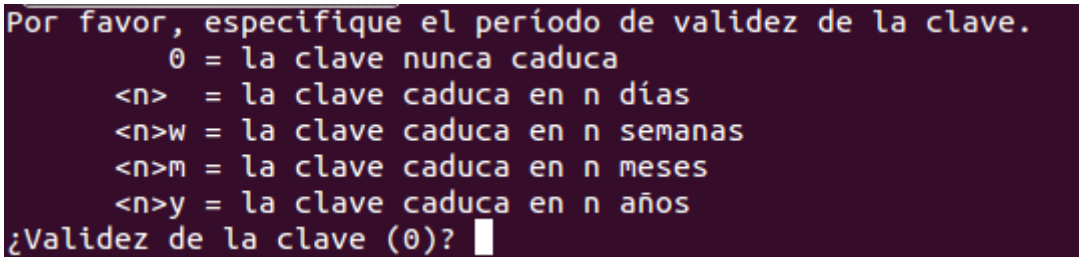
Ejercicio2

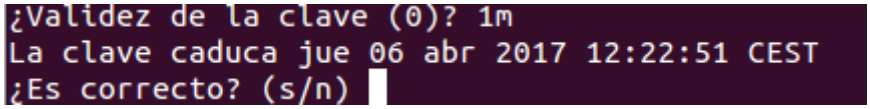
Creo una calve publica elijo la primera la predeterminada.

Le añado una longitud 2028

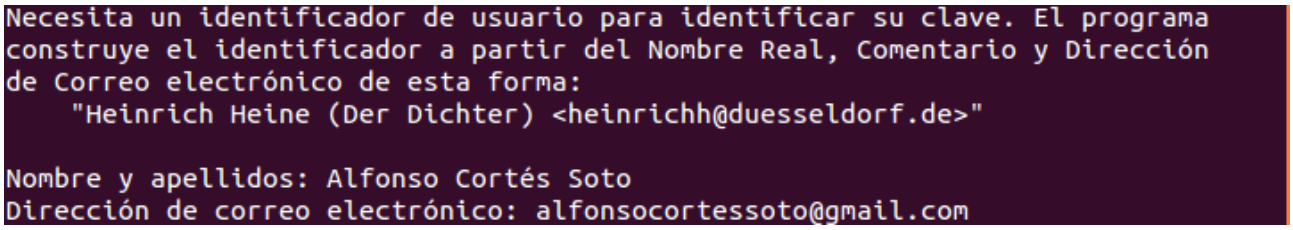


Elijo el periodo de un mes poniendo 1m





Creo un identificador de usuario



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

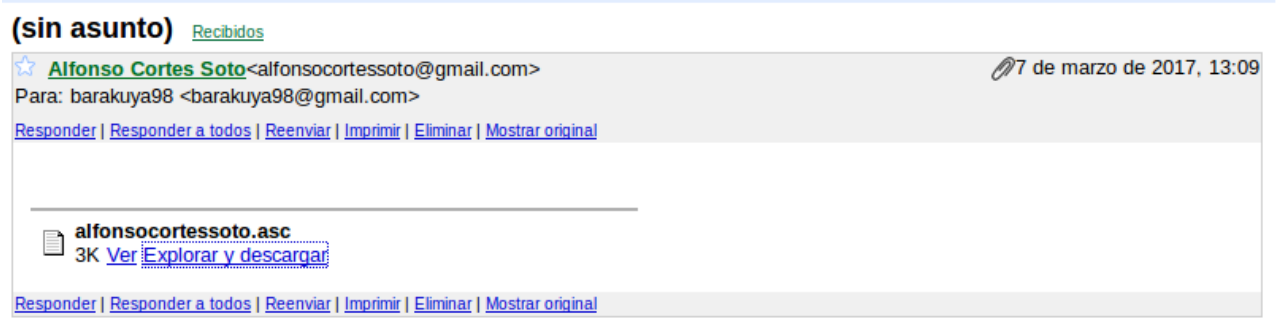
```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg -a --export Alfonso Cortés
 Soto
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQENBFi+i5sBCADV4ugRtOgCbJ2bK28rD3gN6auf8b0x8Kfsr0lGZGjDiP+TsmvR
ARqyPsVYCQrvX7kNG4ASgoQW3MG0iXLjVyPqTXgx3XDqSIWPcNtEvyjOwkpmlBKS
+ZRmvqEdnajRxmI+y2ybLHpRMmxwv/P/x41NU3HoDbvgqfEFowbMnf7dJO6M5Zel
SIg/wEq/Wivvsm5FRBlq62napxnpENBFEg70oHJ2Z1gylKNwWAZQM+xFa+eWlJjK
jQ7ojkngqF+So4NL/stJmTZto2k8XkqysRJJ3IRK7Z7bhl1DPE0bTHzHjSrZTlLx
/c2mL/OIzIl1gMi2v9DuSKsqT9cHb96li3FLABEBAAG0QEFsZm9uc28gQ29ydMOp
cyBTb3RvIChEdXJvIEJsYW5kbykgPGFsZm9uc29jb3J0ZXNzb3RvQGdtYWlsLmNv
bT6JAT4EEwECACgFAli+i5sCGwMFCQAnjQAGCwkIBwMCBhUIAgkKCwQWAgMBAh4B
AheAAAoJEMXo2hD5uG8OhtkIAMuXSYpd1mSYtEPpTimhlh3DttvVzG6Ot8jdhPQe
tZ9Lvg5VJmd46xR1SHK5L4HHodCILqPHdL4A/OWTUbuqmpSTLUcNkt0d/PQOeWWs
xkAp1170TWYk/sNmdy3qBgHQcICIH3tz1OQQTpSJr+IcFJR5zQ8juPdavC1Ng5YJ
vzMOpdiLccLjBtU7WwE4lyFYHxH3Y5zZmcE178Nsx9sPnebCqt6i3mo0JLY2UzIb
tLoTs3LTdaPVuHgnvSQnuazUjqsYfNNngF9xOdX6tiYeJCcqRUkIUblaj1MU7nlj
ZtPmGab6ImTJXN87N7g0IlHl+O+Jy36/iIBptVAHtOUzpqa5AQ0EWL6LmwEIAK6F
Lm3tA2CVKa41oTxnwsOCo63MznVOTH5VdbGBiTvmLvHG1h1tvNkoHvPsqRFmsb3p
lJmsN6qlhYR+0LKiXLWwYYniO4/LBBcD2RNFe3c7HaiFEl/psu9aFBsTOb78P53h
egVuqdn574kuqdrJU8OjUy8bGtbAADaN82vx+cwagY9W5wfw+FCtwosjWId0DfmC
CNYhEhDSwpg/mIlh/8MmStjYE1YP/LINq89YRsD5q5jrTI7smNWkSgEkFKGnvu+n
2vYJHnhLeMZO8+9MWV/LojbabMQS/Gpmt9n3Hm4OUV17YyyFCcdRX+5yhIasKK/t
oU02I8ZF1iBQ0mfYcH0AEQEAAYkBJQQYAQIADwUCWL6LmwIbDAUJACeNAAAKCRDF
6NoQ+bhvDkepB/95w75mtVUIhDh95n+S16vDEwUBdNiUYUiYQMZjkfBmB1uhaQ31
NyXJIJo/Slji7QMYu0+V0hhXGg4KddFhkPsNujrrJzkY8l71czBZg2zu8eZfRwbU
9ITwf82KNWtltzBh+6yDGP7cDRiCYUqyShCdjHnTlp2zm5PApBiRFpPryaj/+JyQ
m3HbDegua849d0nUGOX7/UB3TASbpGBG/lNqPkSC3y2kLAwW01jNFm88Ttnb4iVi
igvjw0TMvb7pb/tnjWe1Tn4utcqbi8RRDgBPnGrzAz7E6Yot/kW9zq/ie7/gpsCu
KAjDoShYeeTB9ufqDae3JD2AneYN4sboG8RnmI0EWL85wQEEAKzgCkV0bL2q+v00
9YR1xp9mditnDzMCrJZvNOpzlA8Z9Iq679bHaOTbhNvrqAoQUXtRyj2lTS0nFAtG
njHxT/Flx5yDl7Ha29P15XUaHPgPD/EA49cfNiOpOjtnIRA1vCMbddbJmx8bqzXo
FGnOOQdYLgxU22JgrlbXTp2gueSdABEBAAG0LkFsZm9uc28gQ29ydMOpcyAoZHVy
bykgPGFsZm9uc28uYy5zQGdtYWlsLmNvbT6IvgQTAQIAKAUCWL85wQIbAwUJACeN
```

Lo exporto

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

Lo envió 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 alfonsocortessoto.acs
```

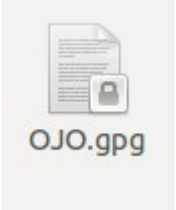
Compruebo que se a incluido en mi keyring

```
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>
```

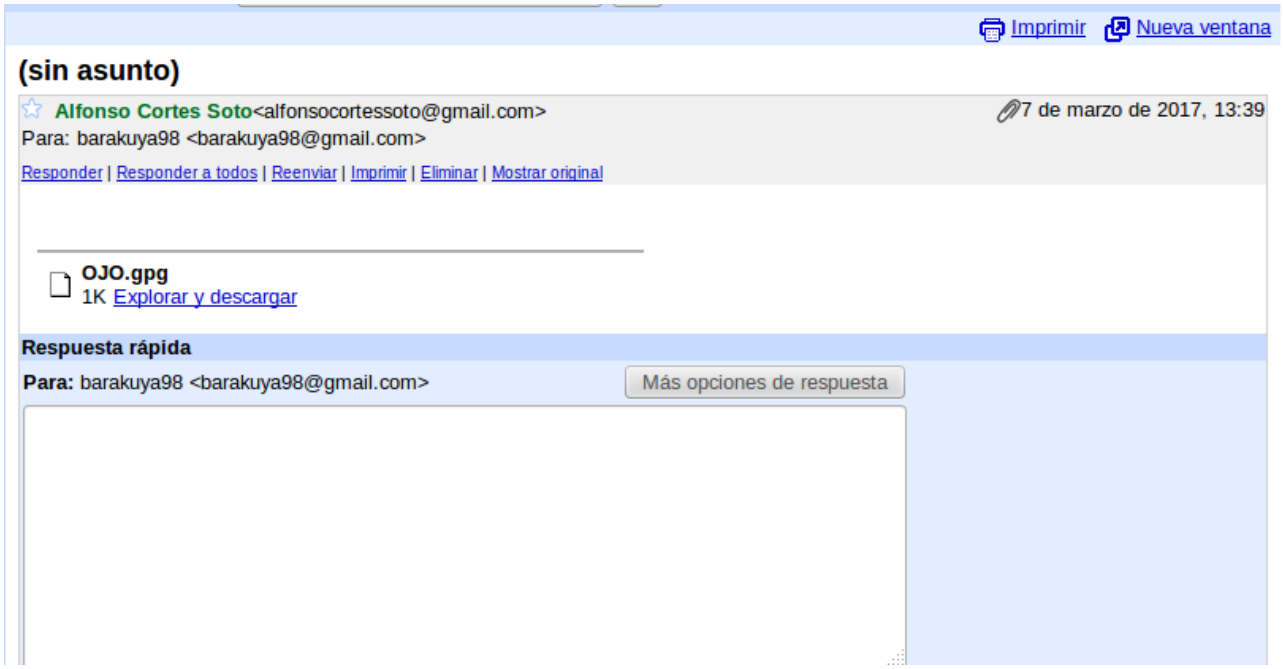
Ejercicio4

Cifro un archivo

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



Se lo envióa mi otra cuenta de email que esta activa en otra maquina virtual.

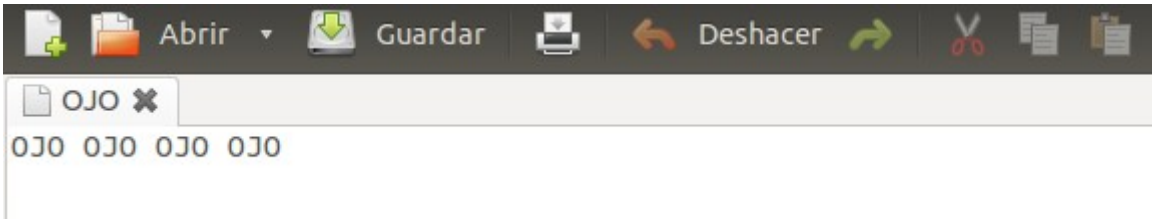


Lo descifro

```
root@alfonso-VirtualBox:/home/alfonso/Escritorio# gpg OJO.gpg
gpg: datos cifrados CAST5
gpg: el agente gpg no esta disponible en esta sesión
Introduzca frase contraseña:
```

Y introduzco la contraseña que le e puesto.

Y me deja ver lo que contiene.



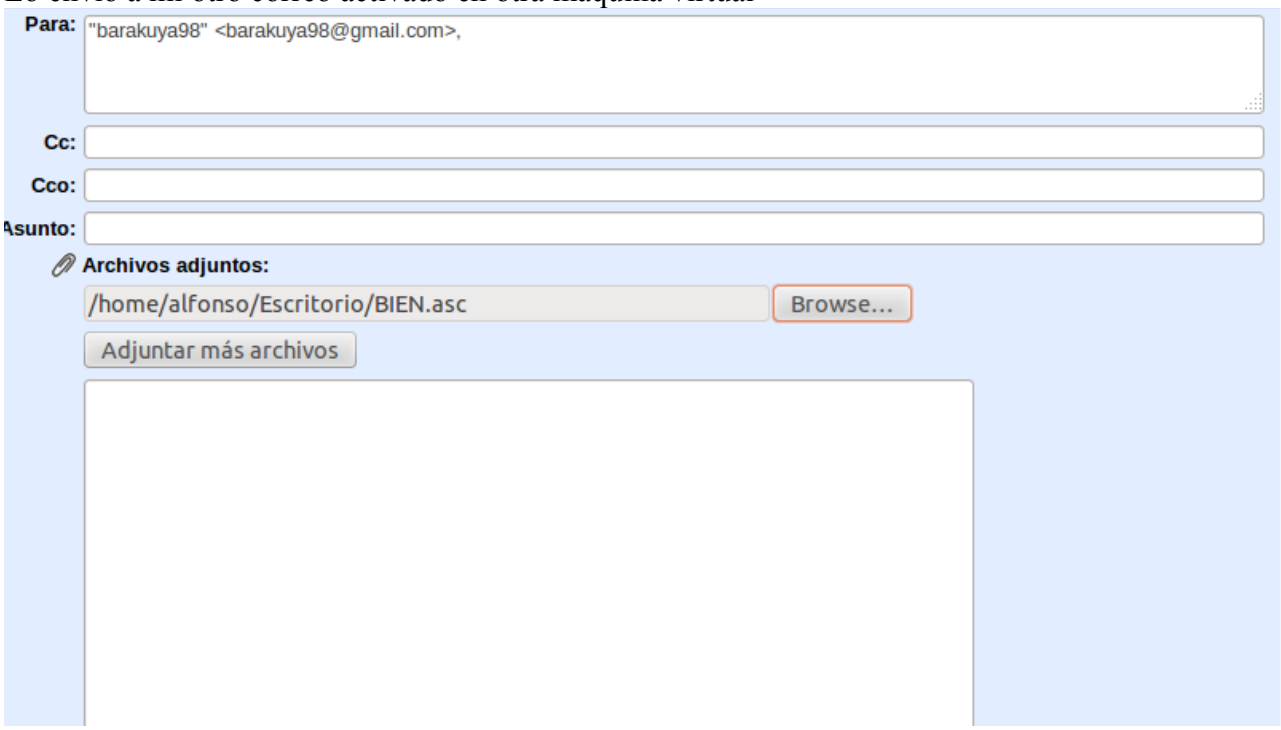
Ejercicio5

Creo un documento

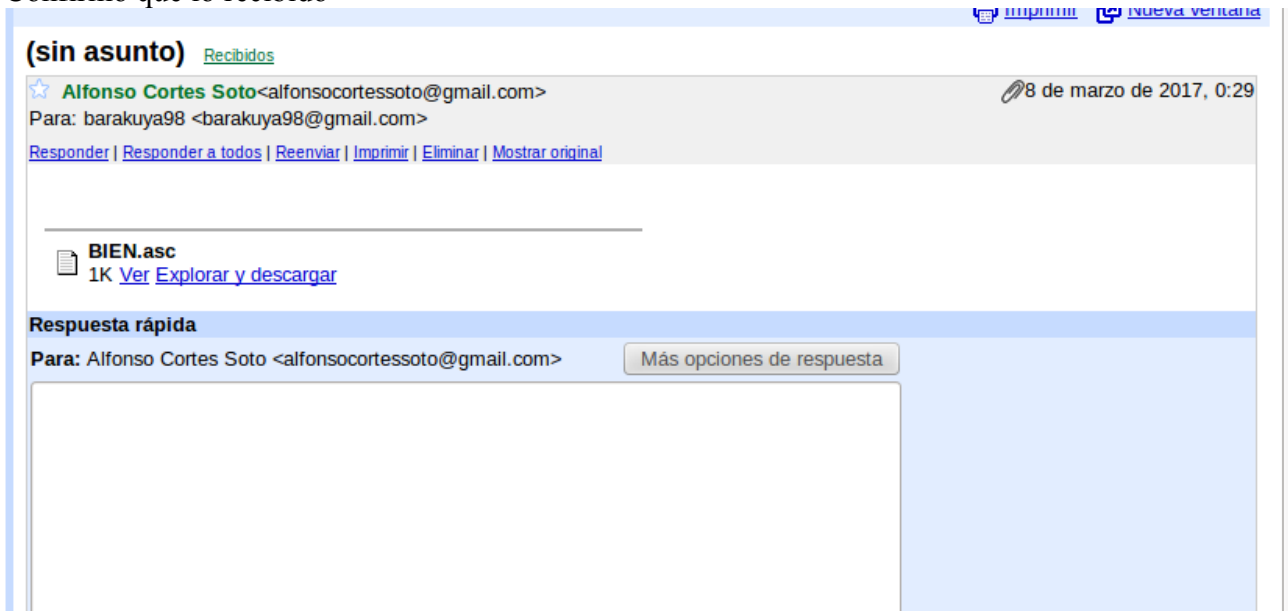
Le creo una firma

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

Lo envió a mi otro correo activado en otra maquina virtual



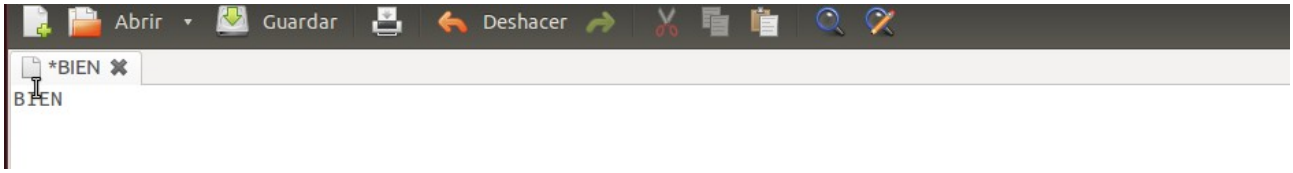
Confirmo que lo recibido



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.



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>»
```