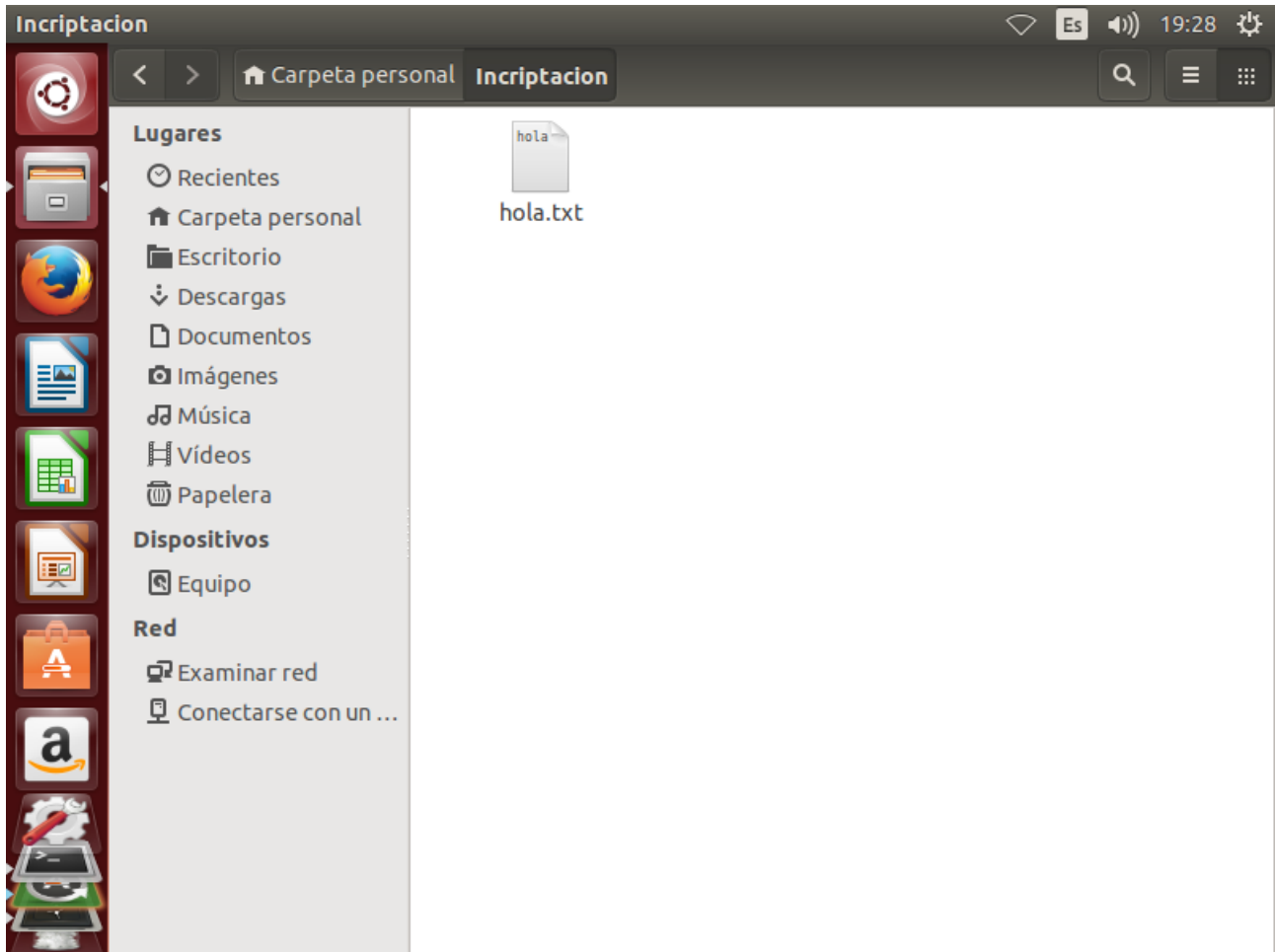


# Práctica Encryptación.

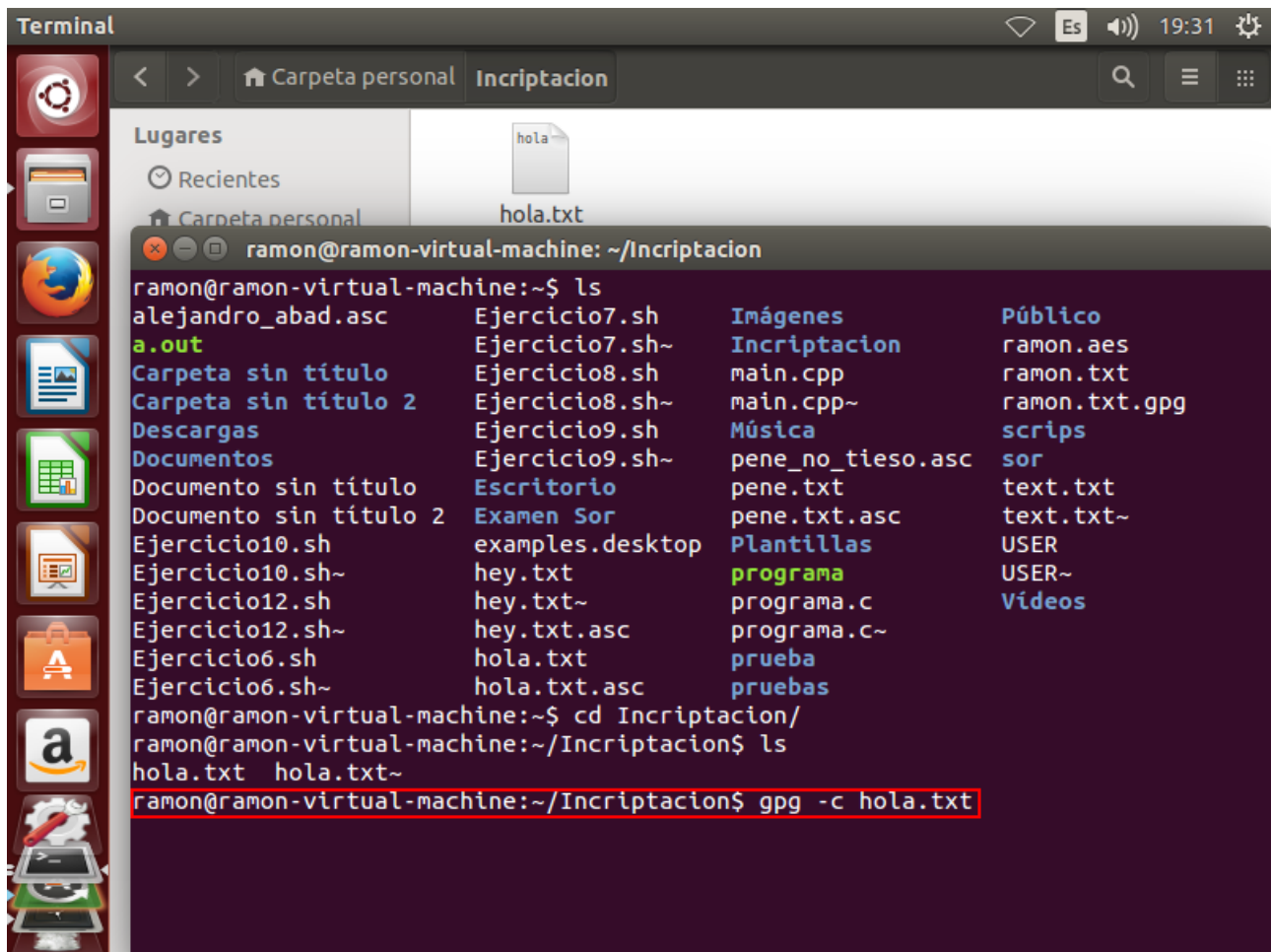


Ramón Botella Alfonso.

Primero debemos crear un archivo para encriptar.



Ahora vamos a la terminal e introducimos el comando.



Introducimos una clave.

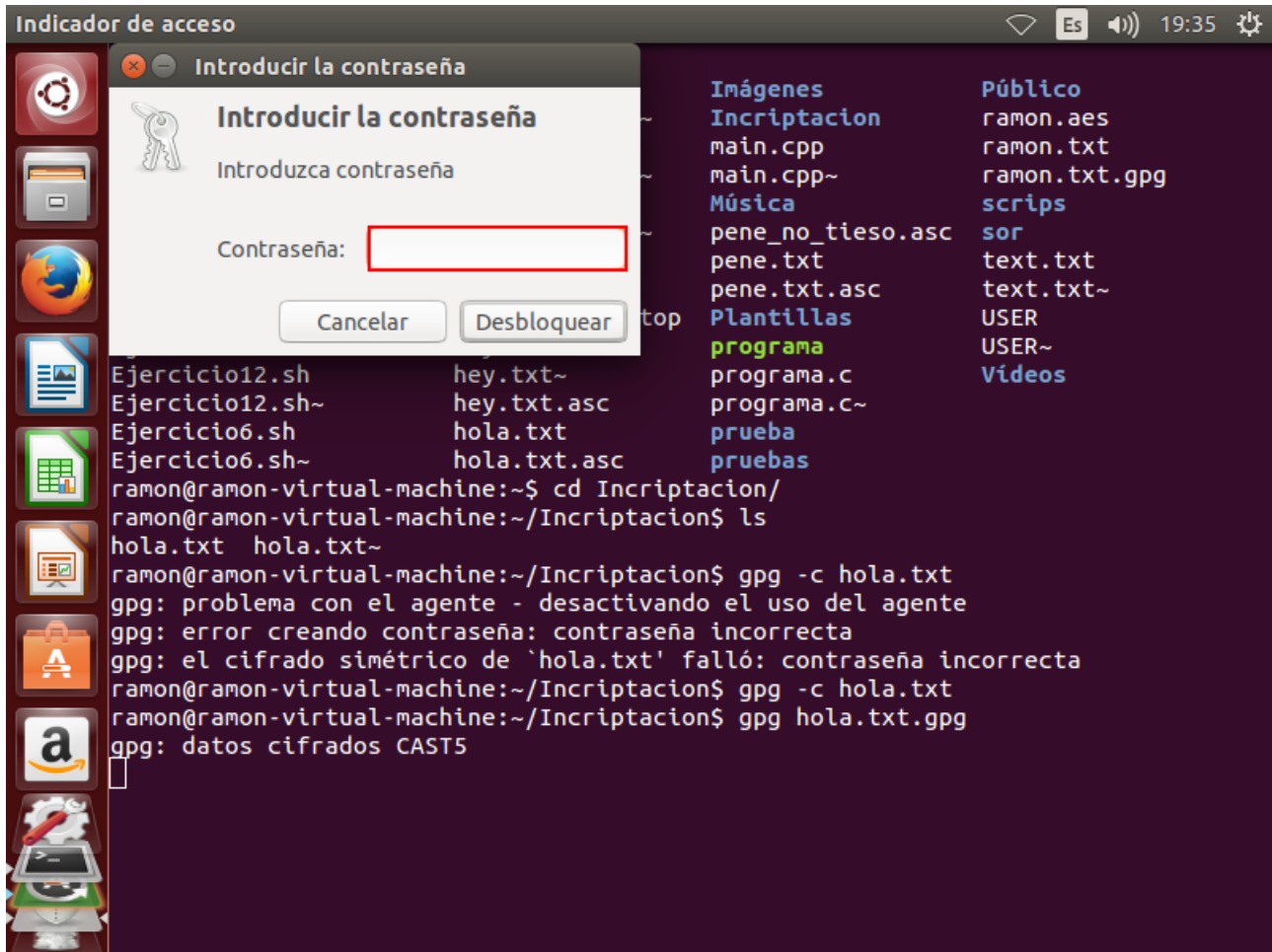


Y para desincryptar debemos introducir el comando:

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  Es  19:34

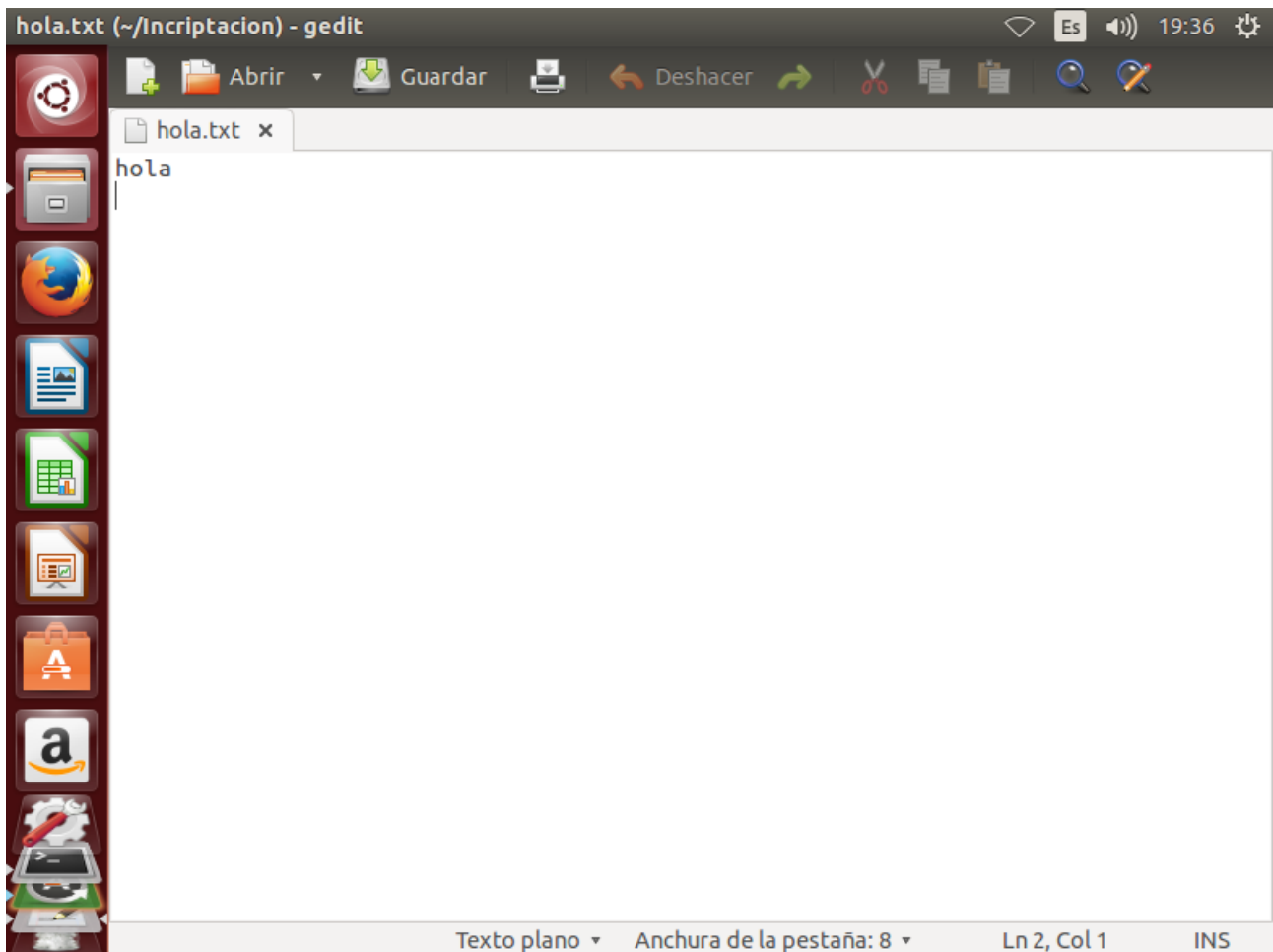
ramon@ramon-virtual-machine:~$ ls
alejandro_abad.asc  Ejercicio7.sh  Imágenes  Público
a.out              Ejercicio7.sh~ Incriptacion  ramon.aes
Carpeta sin título  Ejercicio8.sh  main.cpp    ramon.txt
Carpeta sin título 2 Ejercicio8.sh~ main.cpp~   ramon.txt.gpg
Descargas           Ejercicio9.sh  Música      scrips
Documentos          Ejercicio9.sh~ Escritorio   sor
Documento sin título Ejercicio10.sh Examenes Sor text.txt
Documento sin título 2 Ejercicio10.sh~ examples.desktop text.txt~
Ejercicio10.sh       Ejercicio12.sh hey.txt      USER
Ejercicio10.sh~      Ejercicio12.sh~ hey.txt~     USER~
Ejercicio12.sh       Ejercicio12.sh~ hey.txt.asc  Videos
Ejercicio12.sh~      Ejercicio6.sh  hola.txt    pene_no_tieso.asc
Ejercicio6.sh        Ejercicio6.sh~ hola.txt.asc pene.txt
Ejercicio6.sh~       ramon@ramon-virtual-machine:~$ cd Incriptacion/
ramon@ramon-virtual-machine:~/Incriptacion$ ls
hola.txt  hola.txt~
ramon@ramon-virtual-machine:~/Incriptacion$ gpg -c hola.txt
gpg: problema con el agente - desactivando el uso del agente
gpg: error creando contraseña: contraseña incorrecta
gpg: el cifrado simétrico de 'hola.txt' falló: contraseña incorrecta
ramon@ramon-virtual-machine:~/Incriptacion$ gpg -c hola.txt
ramon@ramon-virtual-machine:~/Incriptacion$ gpg hola.txt.gpg
```

Introduciremos la contraseña del archivo

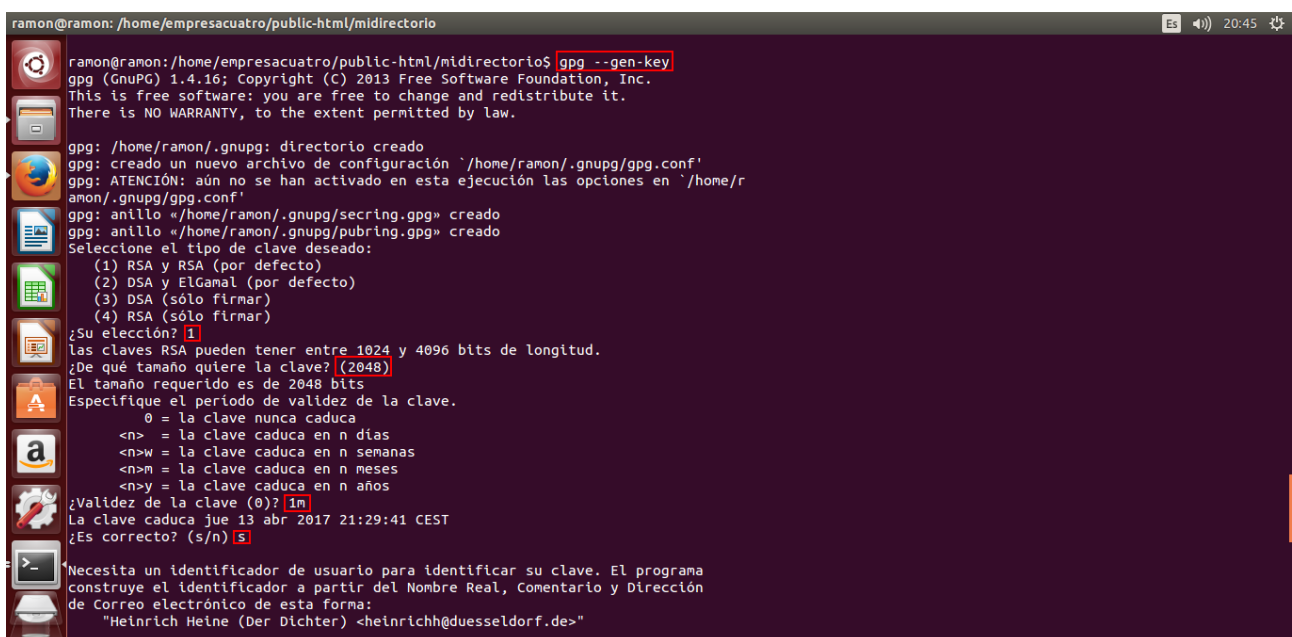


Y nos generara el archivo original.





Ahora generaremos un par de claves para la encriptación simétrica, para ello introduciremos:



```
ramon@ramon: /home/empresacuatro/public-html/midirectorio
Nombre y apellidos: Ramón Botella Alfonso
Dirección de correo electrónico: ramon.botell.a@gmail.com
Comentario: Hola
Está usando el juego de caracteres 'utf-8'.
Ha seleccionado este ID de usuario:
«Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>»

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

Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.

No hay suficientes bytes aleatorios disponibles. Haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 201 bytes más).
.....+++++
..+++++
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.

No hay suficientes bytes aleatorios disponibles. Haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 65 bytes más).
.....+++++

No hay suficientes bytes aleatorios disponibles. Haga algún
otro trabajo para que el sistema pueda recolectar más entropía
```

Una vez introducidos estos parametros se nos creara un par de claves simetricas, es posible que nos diga que generemos bytes aleatorios de informacion para que la cree, para ello iremos al buscador e introduciremos paginas web como [WWW.CHOLO-LOVERS/24/7/365.COM](http://WWW.CHOLO-LOVERS/24/7/365.COM) paginas web inofensivas.

```
ramon@ramon: /home/empresacuatro/public-html/midirectorio
No hay suficientes bytes aleatorios disponibles. Haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 201 bytes más).
.....+++++
..+++++
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.

No hay suficientes bytes aleatorios disponibles. Haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 65 bytes más).
.....+++++

No hay suficientes bytes aleatorios disponibles. Haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 68 bytes más).
.....+++++
gpg: /home/ramon/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave A9230619 marcada como de confianza absoluta
claves publica 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: 2017-04-13
pub 2048R/A9230619 2017-03-14 [[caduca: 2017-04-13]]
HueLLa de clave = EAA6 F53C 0A2A 39CA 05C6 C392 83CF D869 A923 0619
uid Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>
sub 2048R/0B863318 2017-03-14 [[caduca: 2017-04-13]]

ramon@ramon: /home/empresacuatro/public-html/midirectorio$
```

Una vez creadas las exportaremos con el comando.

```
ramon@ramon:~$ gpg -a --export -o Ramón Botella Alfonso.asc ramon.botell.a@gmail.com
```

Se pueden verificar la capturas en el trabajo de Giorgi

```
perico@giorgimegutnishvili:~$ gpg --import ramon
gpg: clave A9230619: clave pública "Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg: importadas: 1 (RSA: 1)
```

E importamos la clave del compañero con.

```
ramon@ramon:~$ gpg --import miclave.asc
gpg: clave 465AEA40: clave pública "giorgimegut (Soy giorgi) <giorgimegut@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg: importadas: 1 (RSA: 1)
```

Y encriptamos el archivo con:

```
ramon@ramon:~$ gpg -a -r giorgimegut@gmail.com --encrypt fin.txt
```

Se confirma con Giorgi.

```
perico@giorgimegutnishvili:~$ gpg fin.txt.asc

Necesita una contraseña para desbloquear la clave secreta
del usuario: "giorgimegut (Soy giorgi) <giorgimegut@gmail.com>"
clave RSA de 2048 bits, ID 3A082AA1, creada el 2017-03-14 (identificador de clave
primaria 465AEA40)

gpg: cifrado con clave RSA de 2048 bits, ID 3A082AA1, creada el 2017-03-14
«giorgimegut (Soy giorgi) <giorgimegut@gmail.com>»
```

Desencriptamos el archivo de Giorgi.

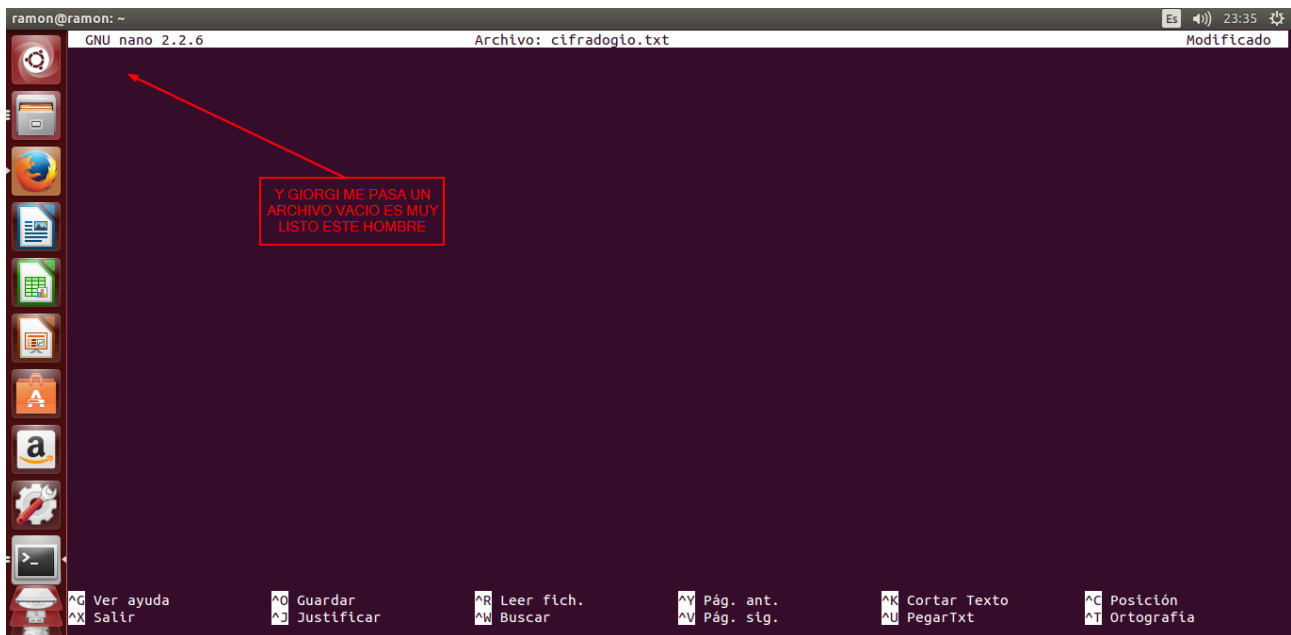
```
ramon@ramon:~$ gpg cifradogio.txt.asc

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>"
clave RSA de 2048 bits, ID 0B863318, creada el 2017-03-14 (identificador de clave primaria A9230619)
```

Nos pedira nuestra clave privada.

Y ya lo tenemos.





Ahora vamos crear un documento y firmarlo para ello introduciremos:

```
ramon@ramon:~$ gpg -sb -a firmar.txt
```

```
Necesita una contraseña para desbloquear la clave secreta
del usuario: "Ramón Botella Alfonso (Hola) <ramon.botella@gmail.com>"
clave RSA de 2048 bits, ID A9230619, creada el 2017-03-14
```

Para verificar la firma deberíamos introducir este comando, a mi no me ha salido correctamente.

```
perico@giorgimegutnishvili:~$ gpg --verify firmaramon.txt.asc
gpg: Firmado el mié 15 mar 2017 00:19:09 CET usando clave RSA ID 465AEA40
gpg: Firma correcta de «giorgimegut (Soy giorgi) <giorgimegut@gmail.com>»
perico@giorgimegutnishvili:~$
```

El compañero comprueba que le funciona correctamente.

```
perico@giorgimegutnishvili:~$ gpg firmar.txt.asc
gpg: Firmado el mié 15 mar 2017 00:00:26 CET usando clave RSA ID A9230619
gpg: Firma INCORRECTA de «Ramón Botella Alfonso (Hola) <ramon.botella@gmail.com>»
```

Y si alteramos el archivo esto es lo que nos muestra.

```
ramon@ramon:~$ gpg firmaramon.txt.asc
gpg: Firmado el mié 15 mar 2017 00:19:09 CET usando clave RSA ID 465AEA40
gpg: Firma INCORRECTA de «giorgimegut (Soy giorgi) <giorgimegut@gmail.com>»
```