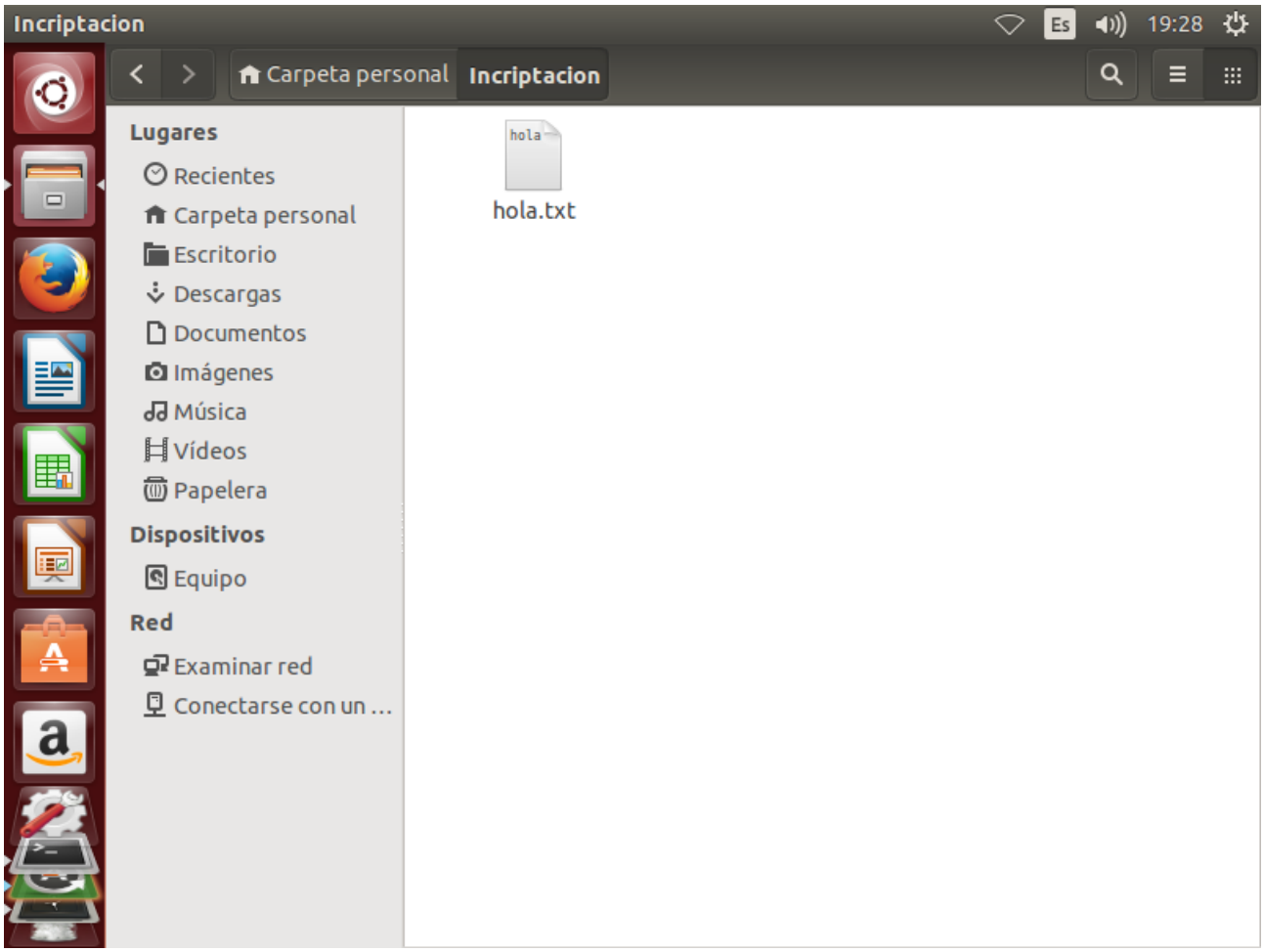
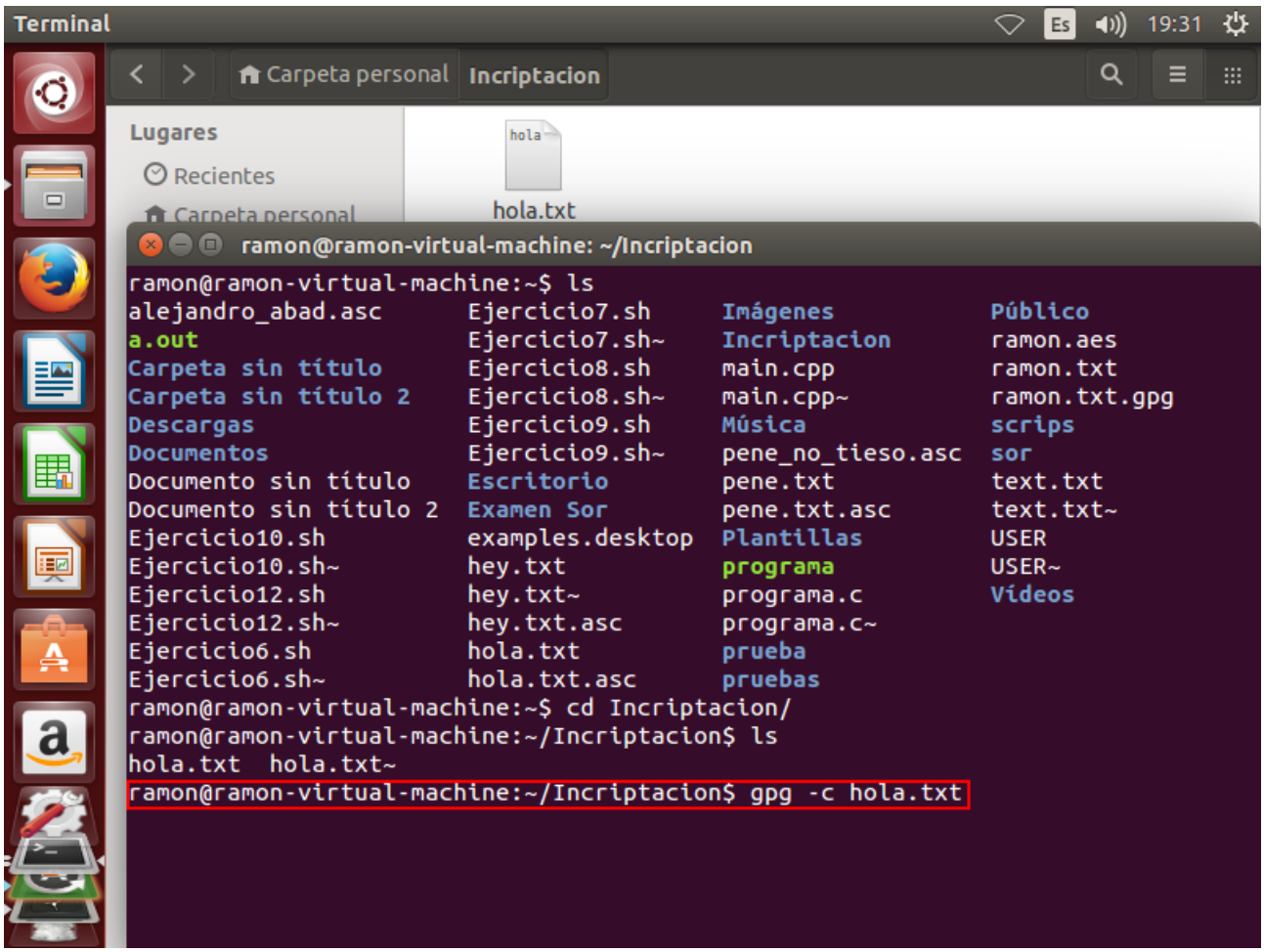
Práctica Encryptación.

Ramón Botella Alfonso.

Primero debemos crear un archivo para encriptar.

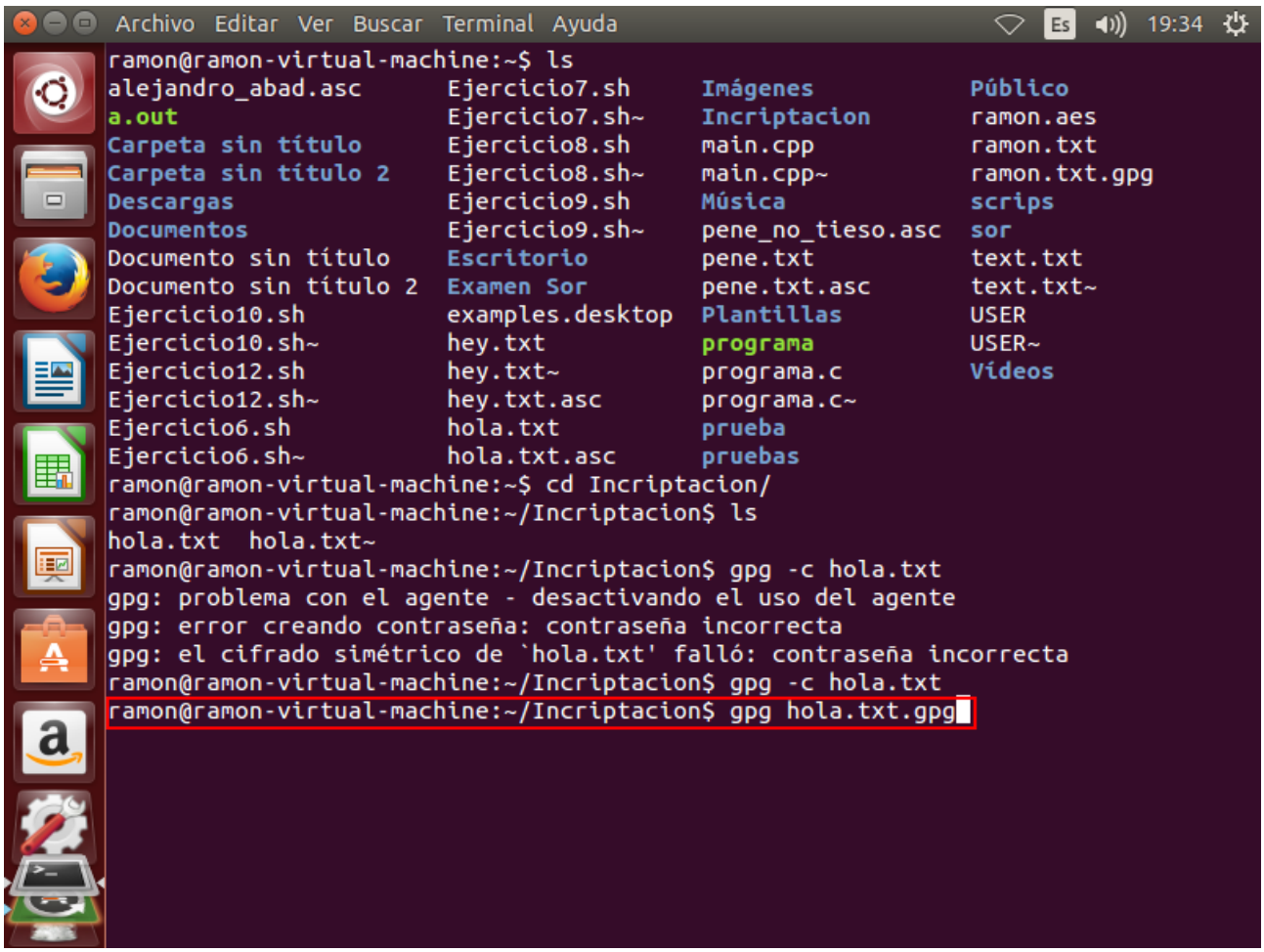


Ahora vamos a la terminal e introducimos el comando.

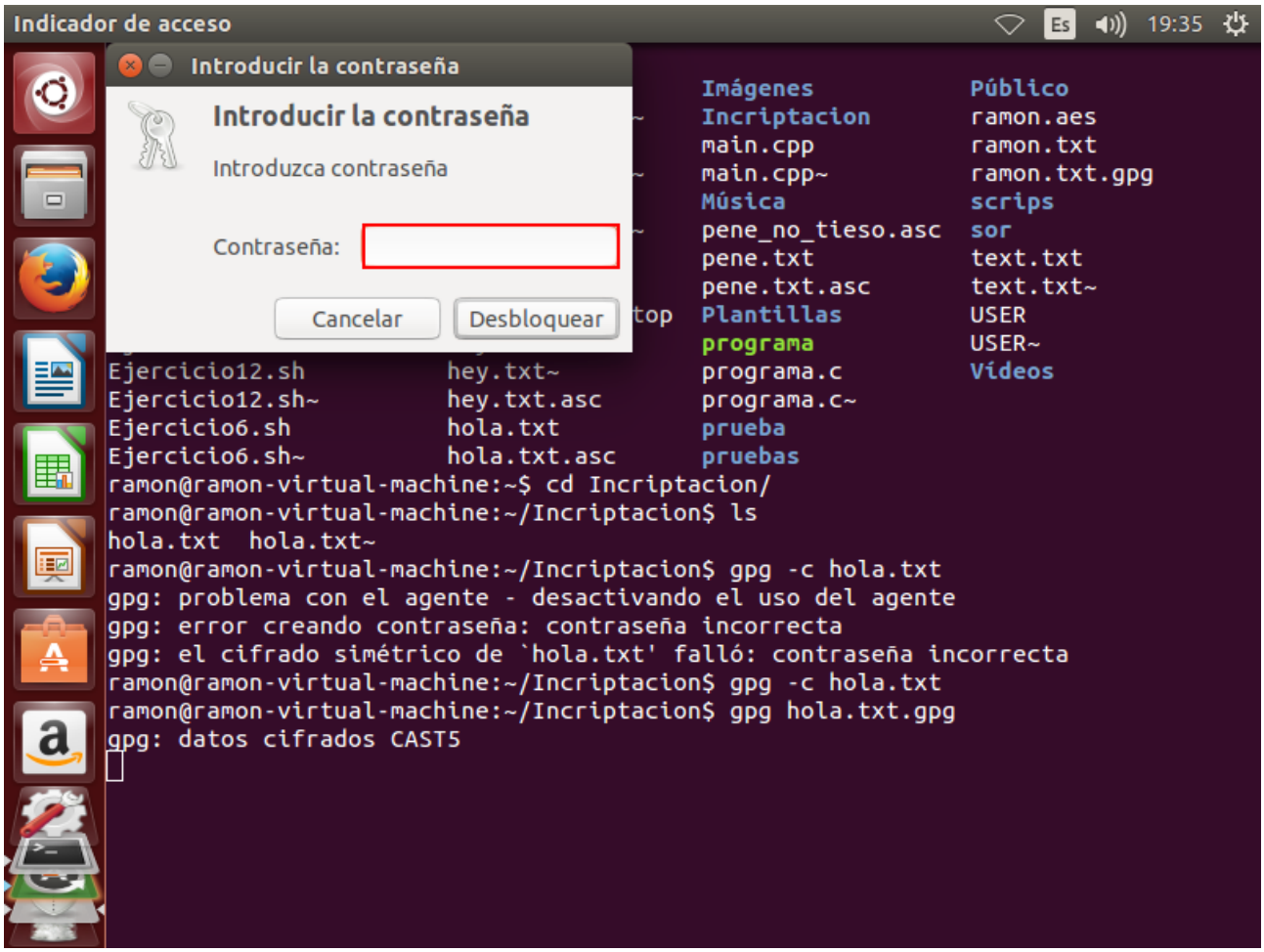


Introducimos una clave.

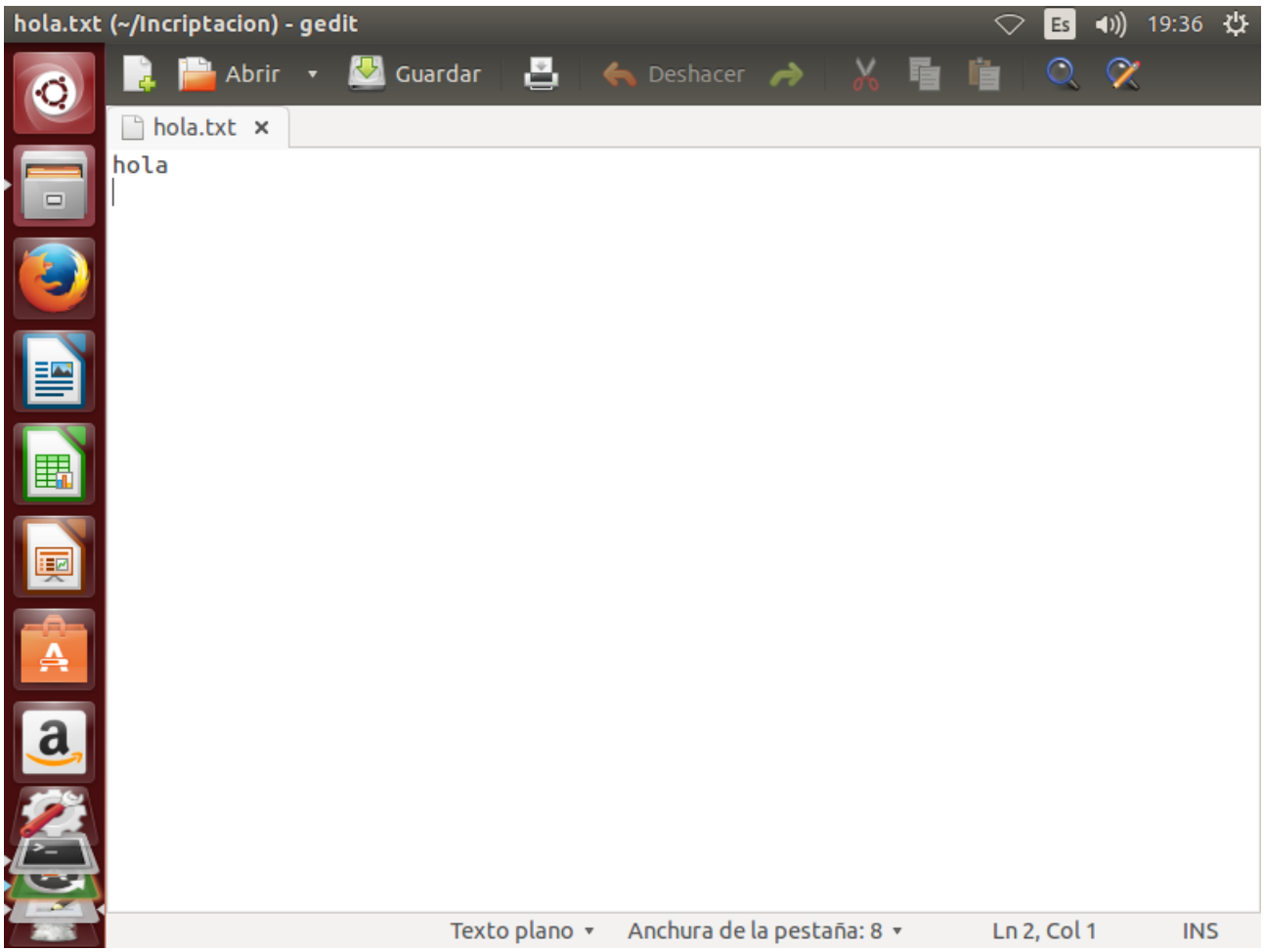
Y para desincriptar debemos introducir el comando:


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~ pene_no_tieso.asc sor
Documento sin título Escritorio pene.txt text.txt
Documento sin título 2 Examen Sor pene.txt.asc text.txt~
Ejercicio10.sh examples.desktop Plantillas USER
Ejercicio10.sh~ hey.txt programa USER~
Ejercicio12.sh hey.txt~ programa.c Vídeos
Ejercicio12.sh~ hey.txt.asc programa.c~
Ejercicio6.sh hola.txt prueba
Ejercicio6.sh~ hola.txt.asc pruebas
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

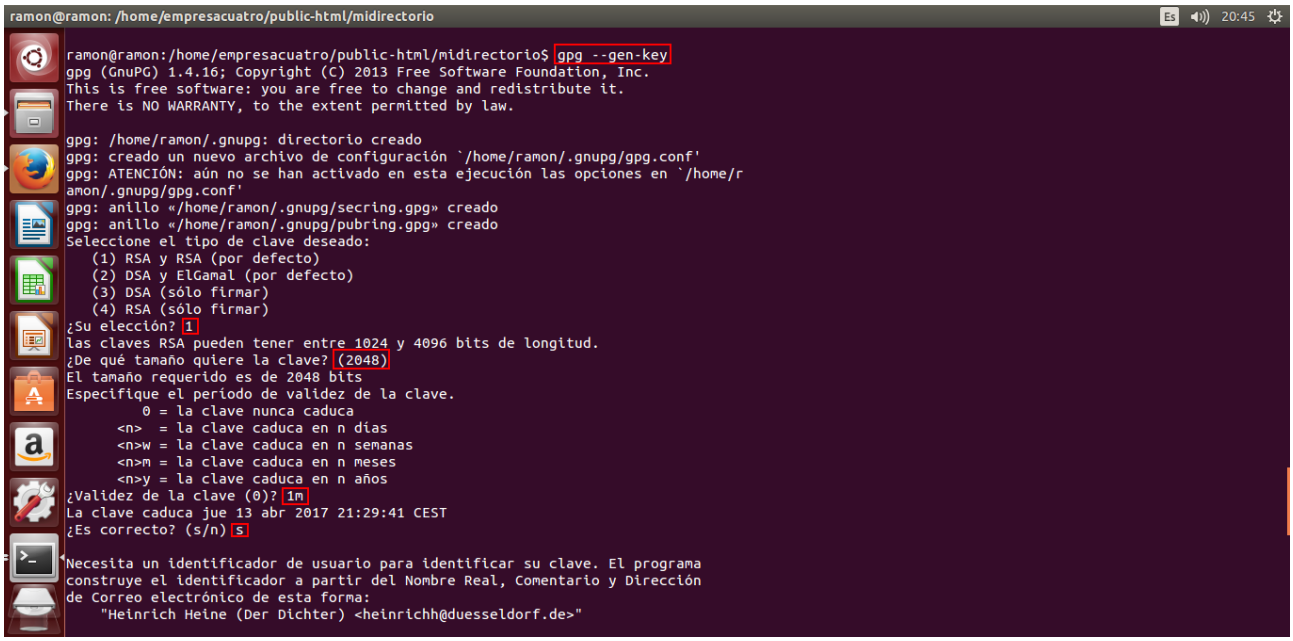
Introduciremos la contraseña del archivo

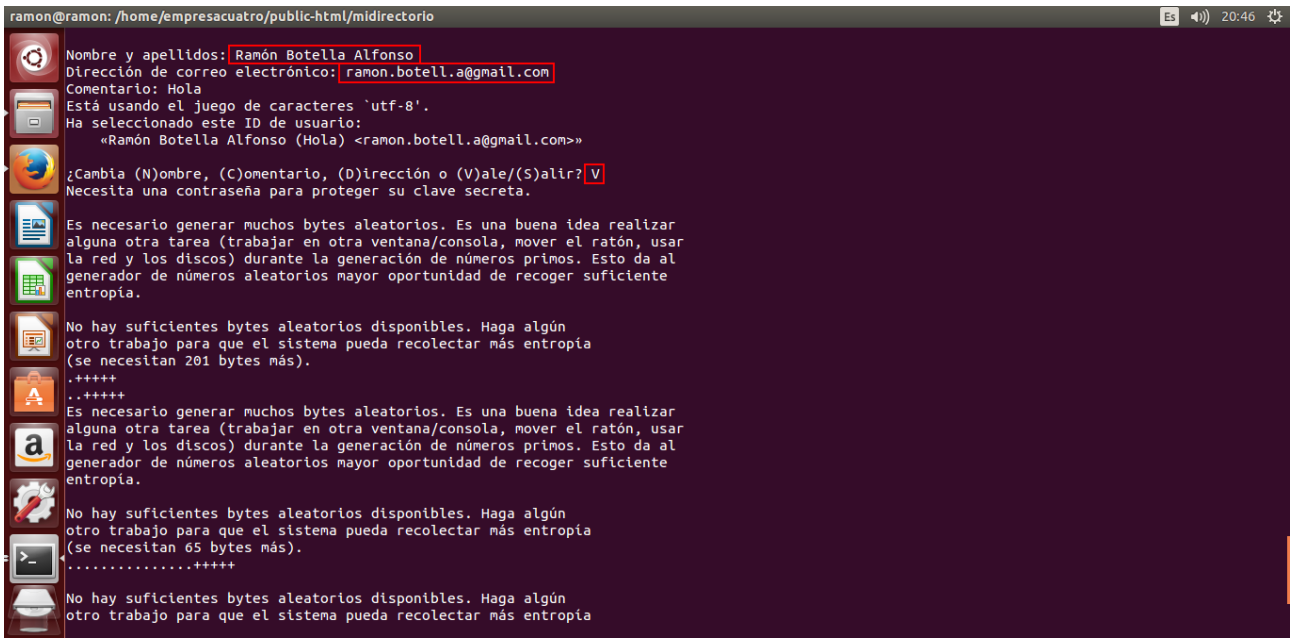


Y nos generara el archivo original.

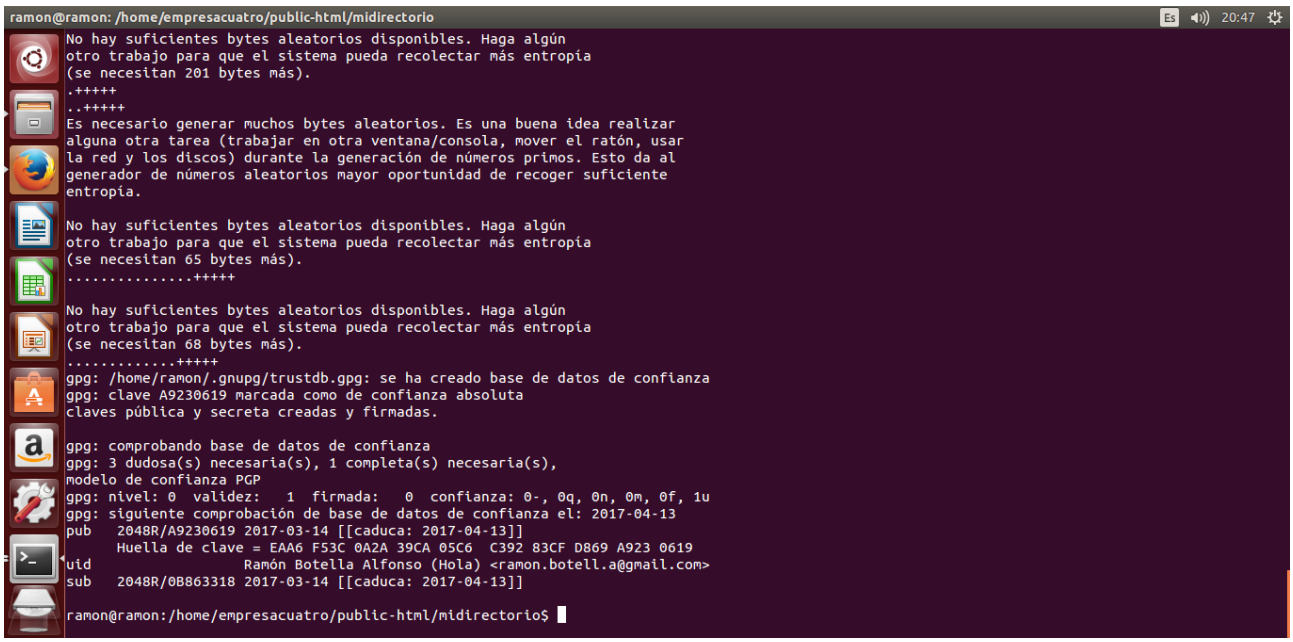


Ahora generaremos un par de claves para la encriptación simetrica, para eello introduciremos:





Una vez introducidos estos parametros se nos creara un par de claves simetricas, es posbile 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~~ paginas web inofensivas.



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>»
```

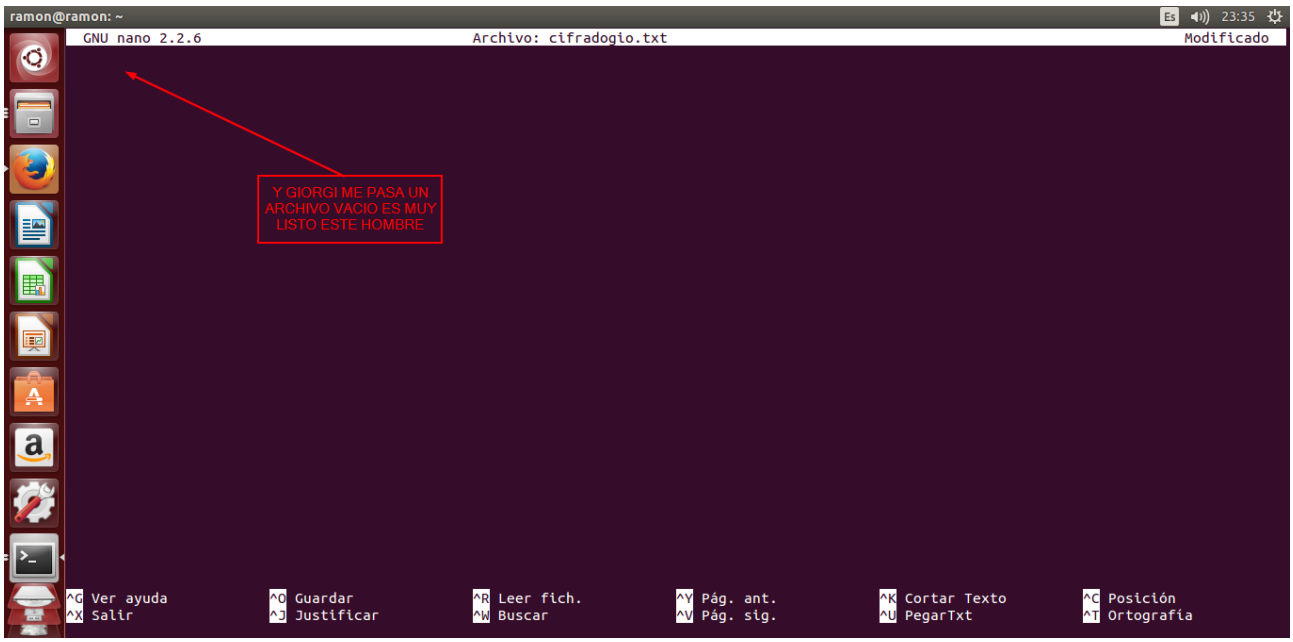
Desencriptamos el archivo de Giorgi.

```
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.botell.a@gmail.com>"
clave RSA de 2048 bits, ID A9230619, creada el 2017-03-14
```

Para verificar la firma deberiamos 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.botell.a@gmail.com>»
```

Y si altereamos 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>»
```