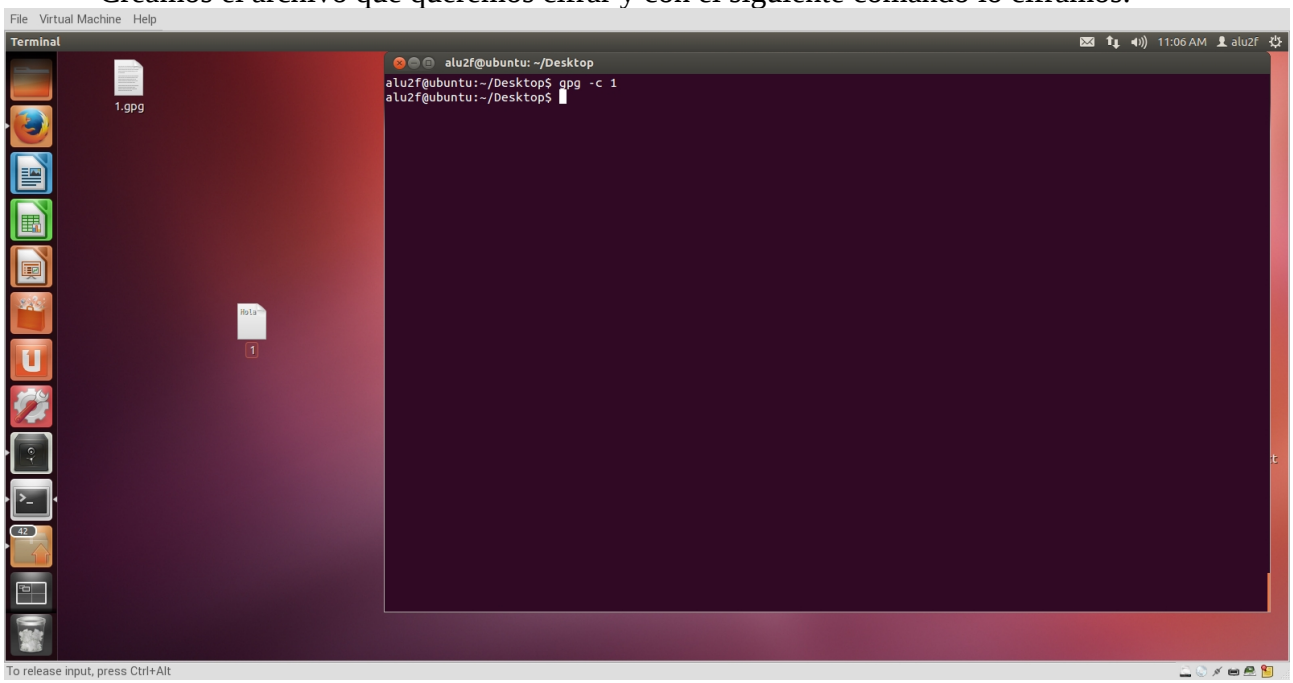
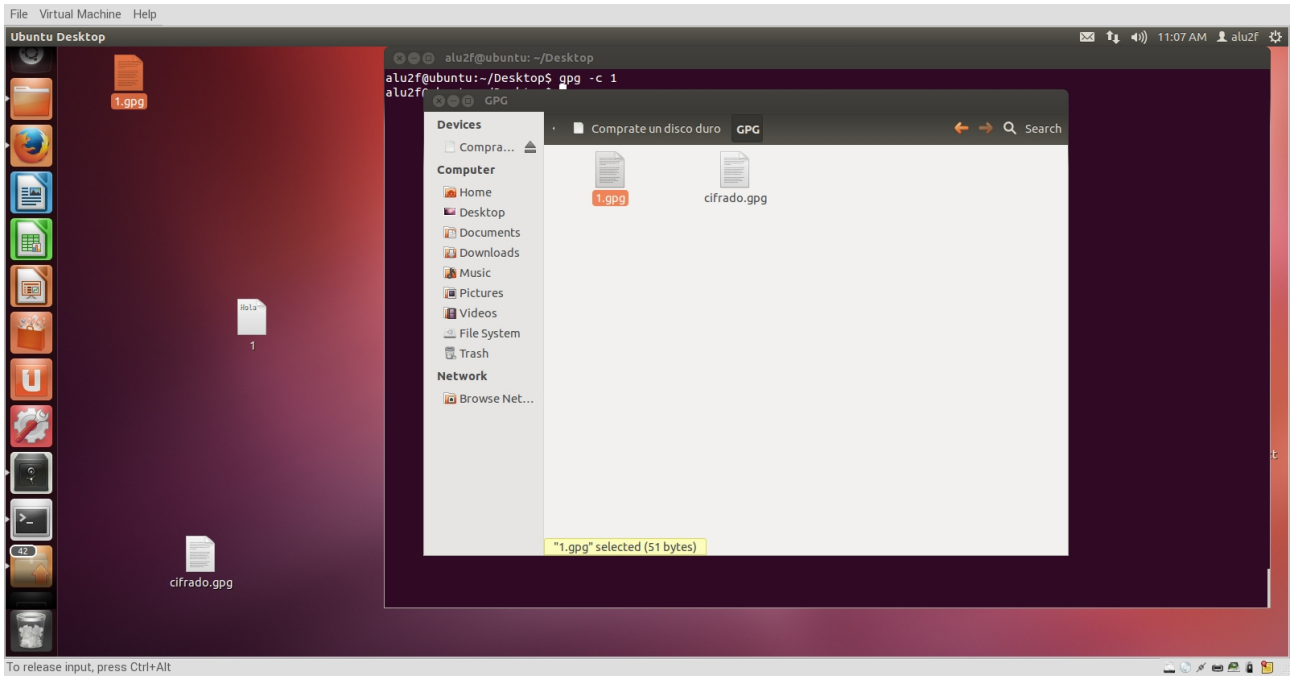
# Práctica Criptografía

## Ejercicio1

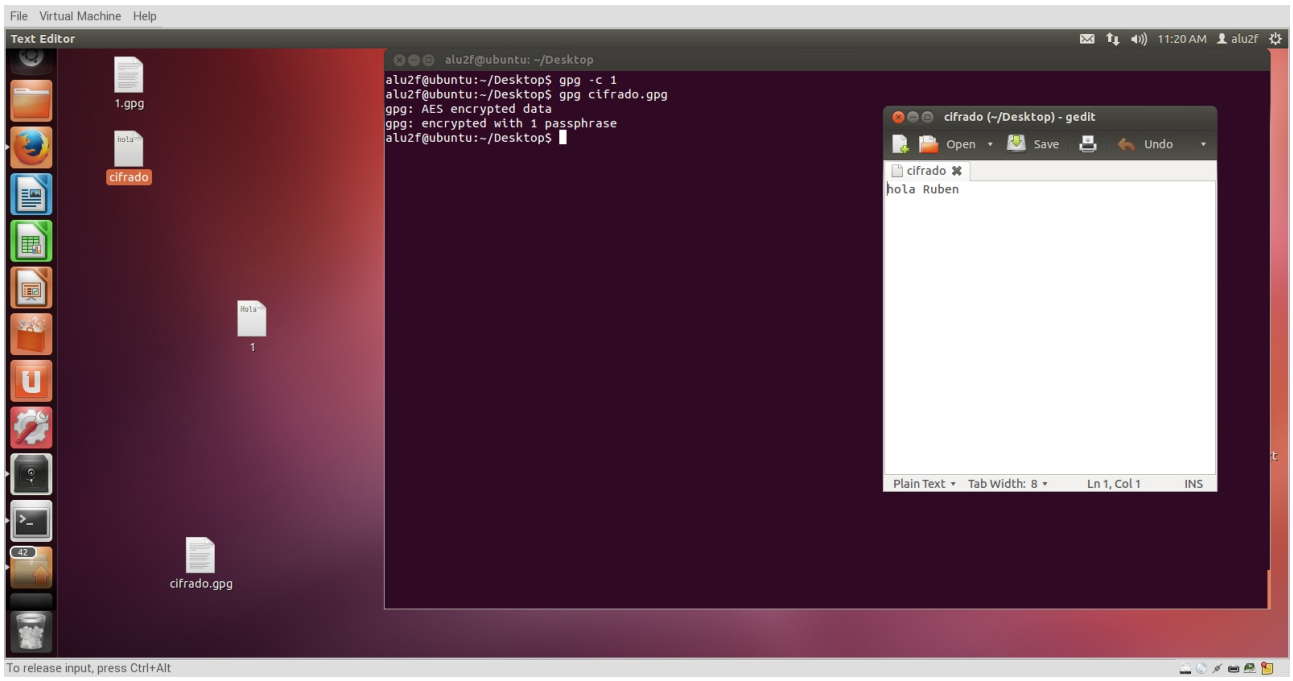
Creamos el archivo que queremos cifrar y con el siguiente comando lo ciframos.



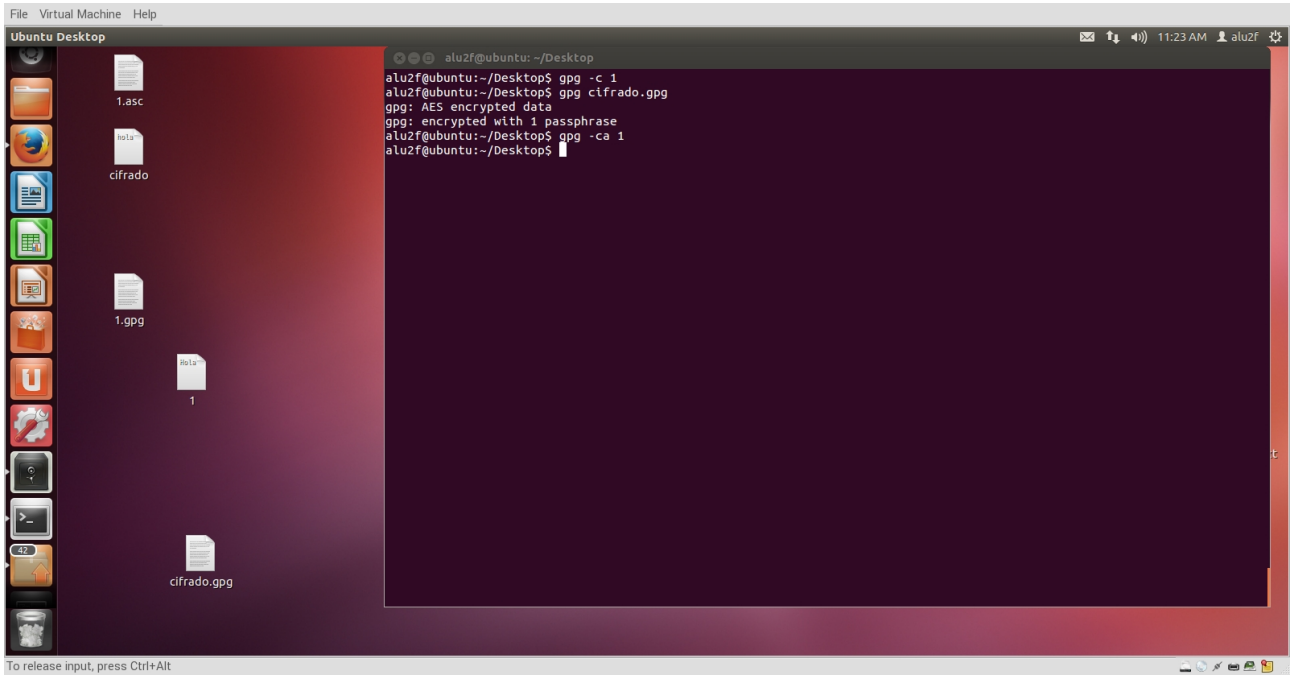

Nos intercambiamos las practicas con nuestro compañero.



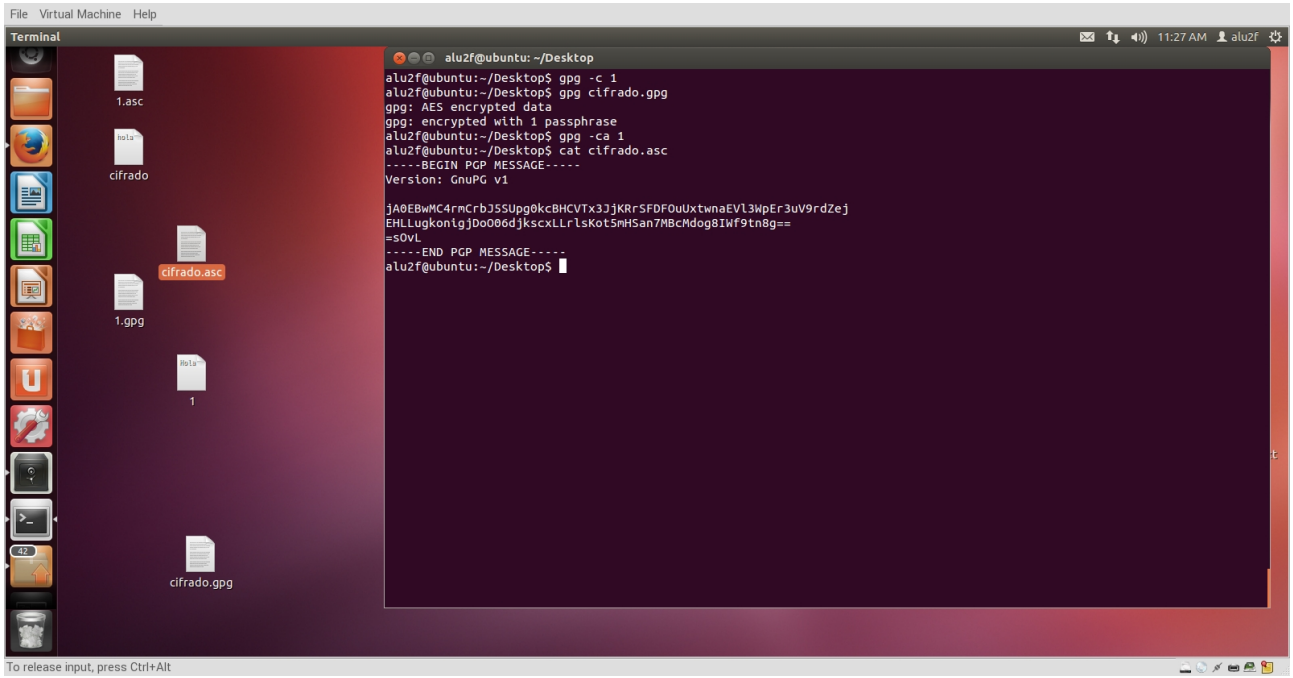
Desciframos el archivo que nos ha pasado el compañero con el siguiente comando. Tras descifrarlo nos aparecerá el contenido.




Con el siguiente comando, añadiendo la opcion “a”, ciframos el archivo de una forma mas segura.

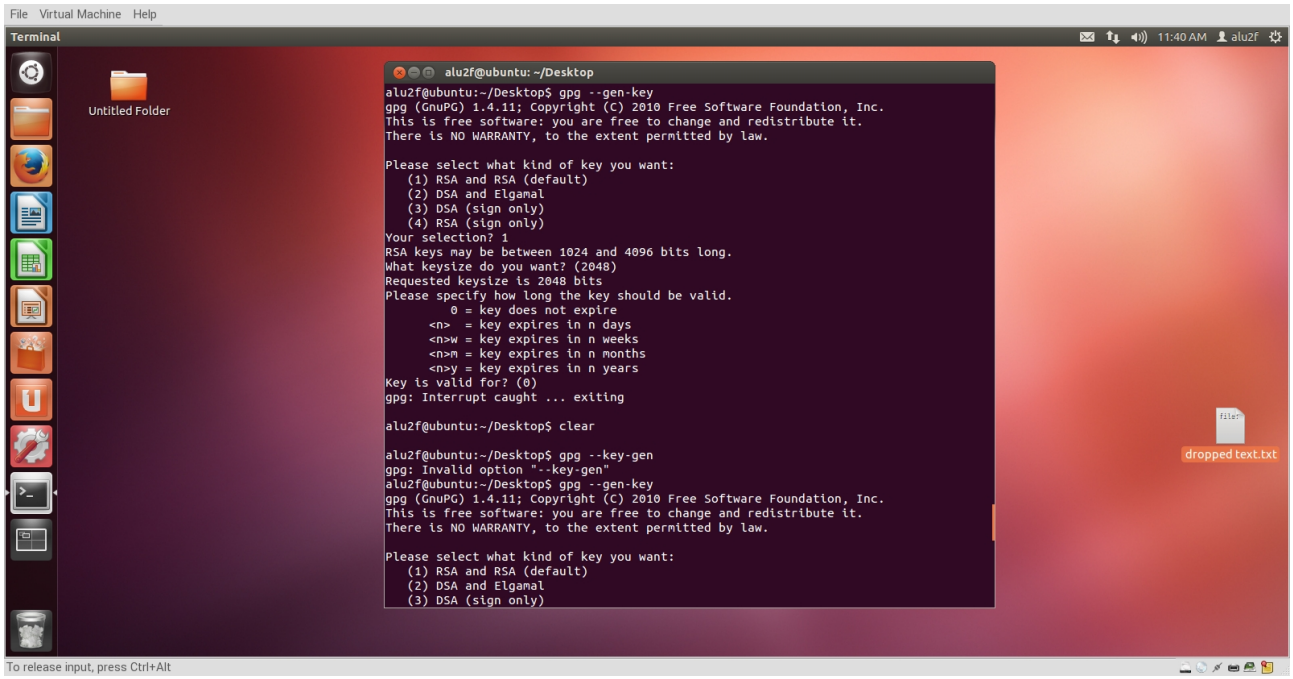


Por ultimo comprobamos que el contenido final de el archivo está cifrado y no podemos acceder a el.

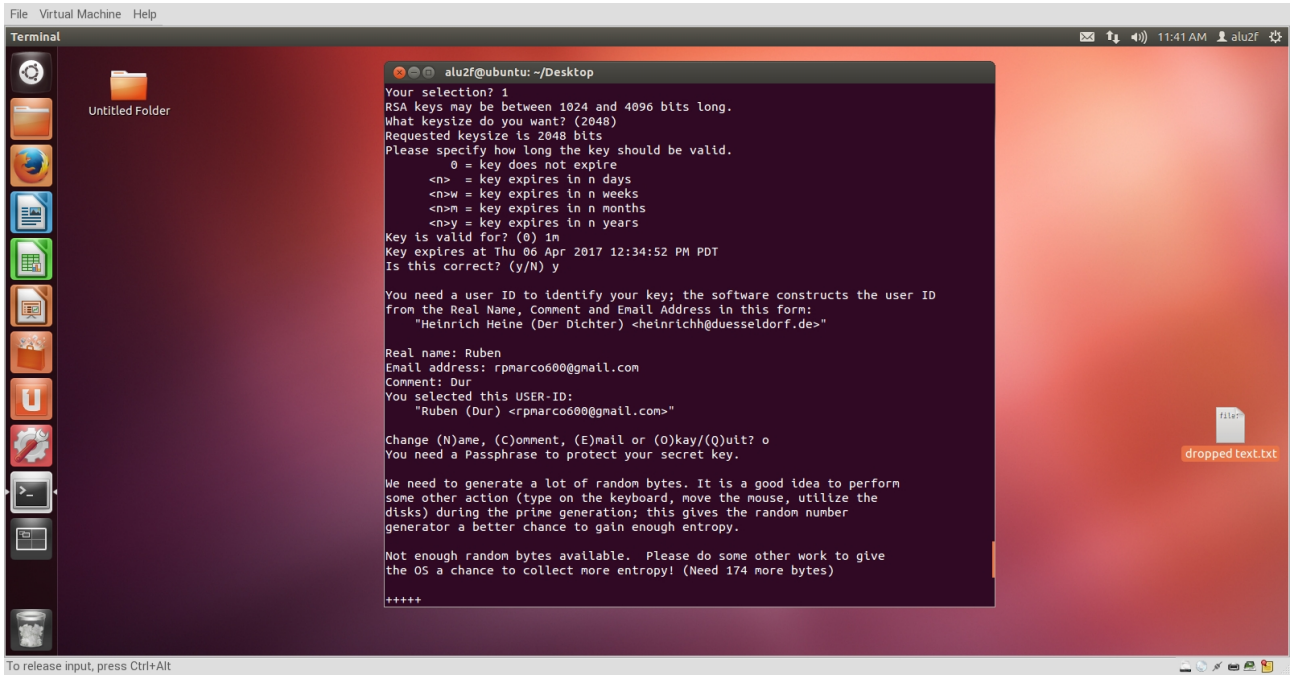


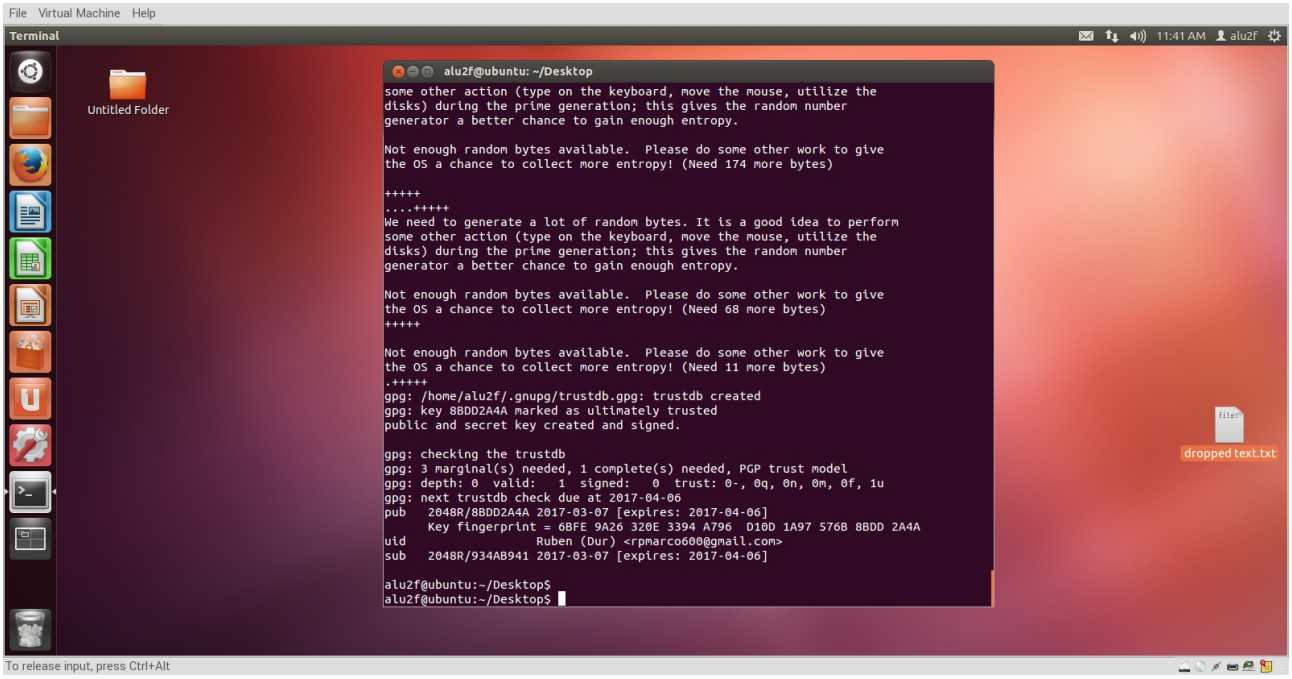
# Ejercicio 2

## Generamos una clave pública.

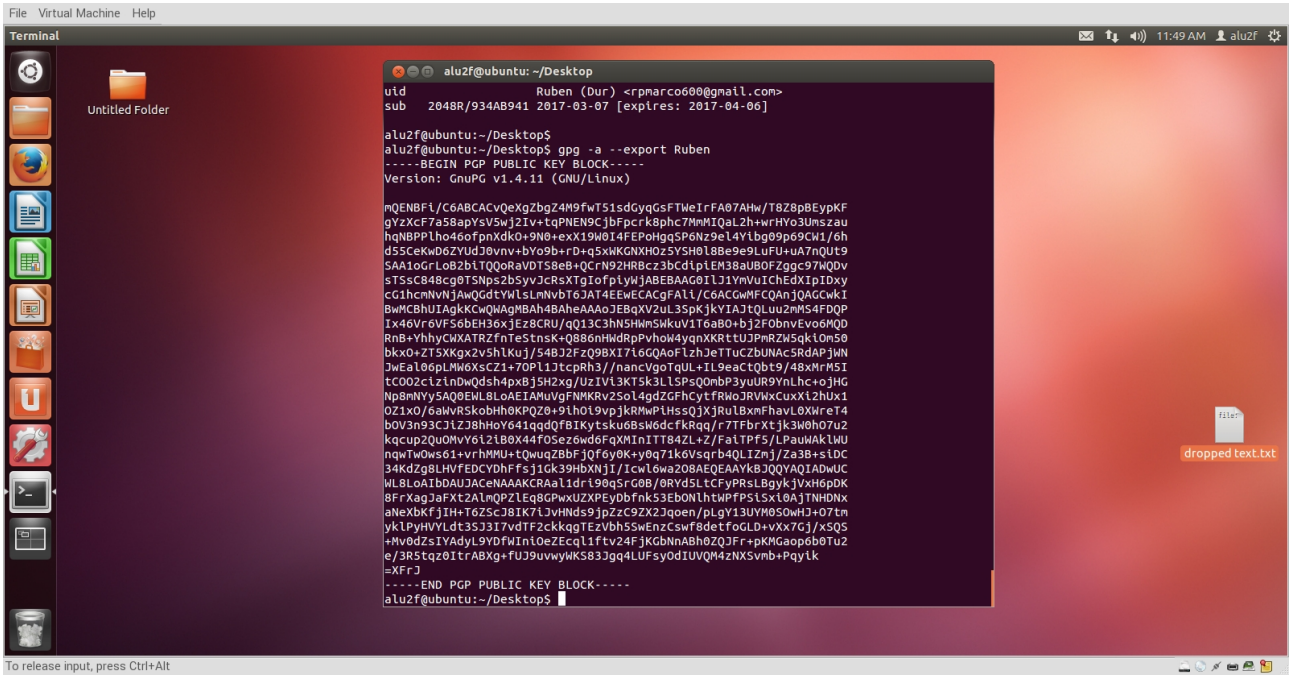



Le damos una longitud a la clave y metemos los datos que se requieran.

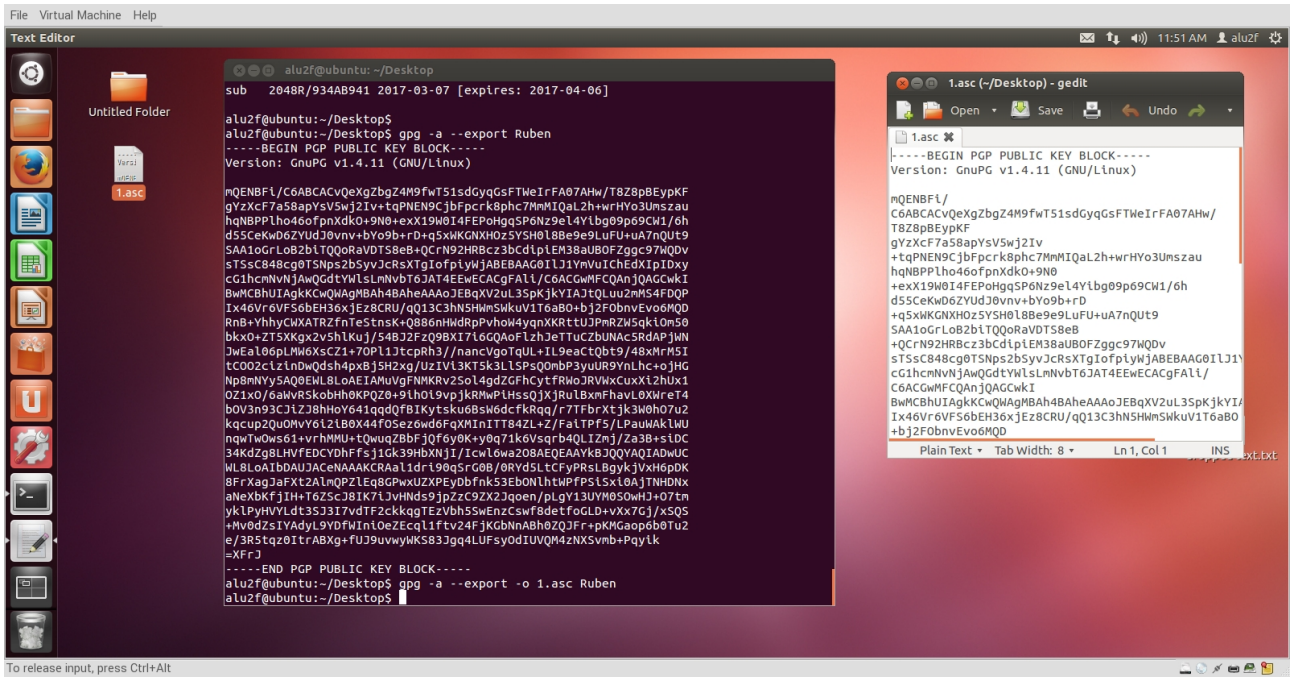





El siguiente paso es exportar la clave que hemos generado y nos saldra en la pantalla del terminal.

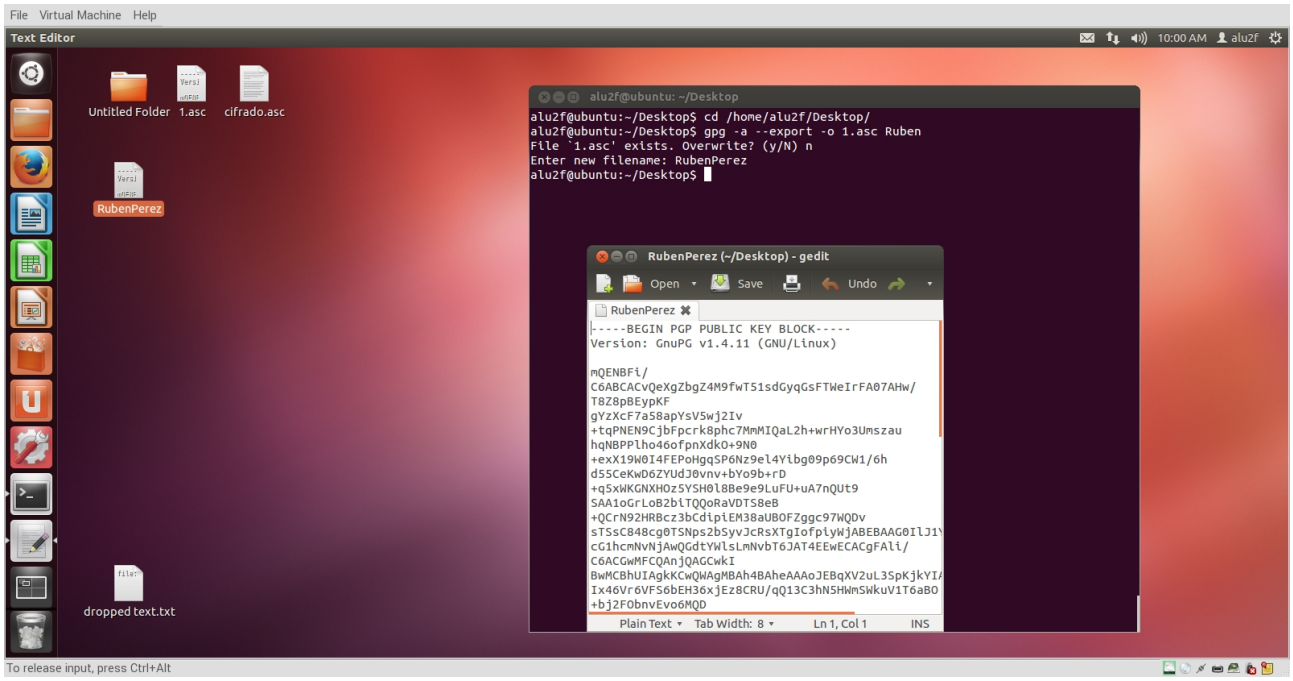


Comprobamos que al abrir el archivo nos sale la información cifrada y que no podemos leerla.



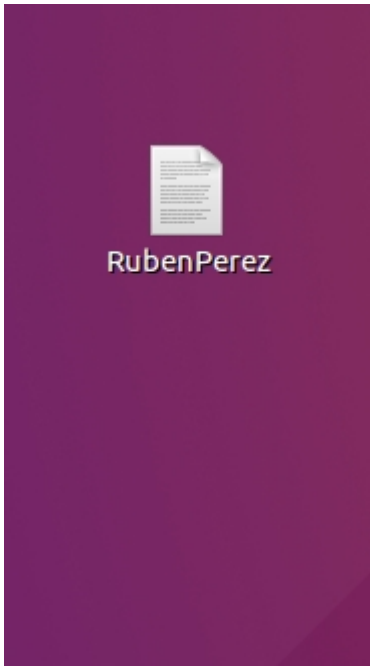
# Ejercicio 3

Exportamos el archivo 1.asc y le cambiamos el nombre.




```
alu2f@ubuntu:~/Desktop$ gpg -a --export -o 1.asc Ruben
```

Este es el archivo con el nuevo nombre.



Importamos el archivo en el ordenador de nuestro compañero

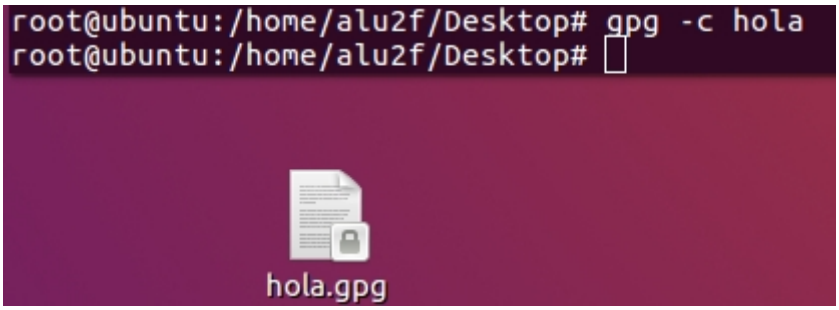
```
alu2f@ubuntu:~/Desktop$ sudo gpg --import 1.asc
[sudo] password for alu2f:
gpg: /home/alu2f/.gnupg/trustdb.gpg: trustdb created
gpg: key 8BDD2A4A: public key "Ruben (Dur) <rpmarco600@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

Con el siguiente comando comprobamos que el archivo se ha importado con éxito.

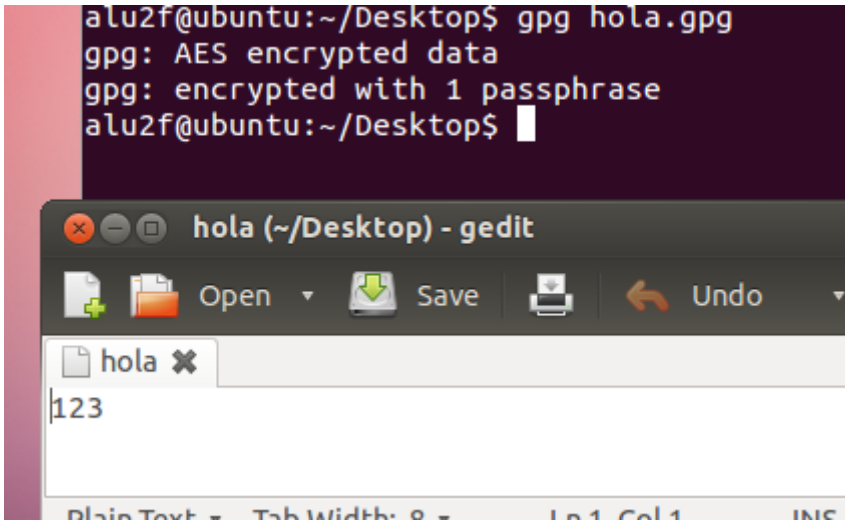
```
root@ubuntu:/home/alu2f/Desktop# gpg -kv
/root/.gnupg/pubring.gpg
------------------------
pub   2048R/8BDD2A4A 2017-03-07 [expires: 2017-04-06]
uid                  Ruben (Dur) <rpmarco600@gmail.com>
sub   2048R/934AB941 2017-03-07 [expires: 2017-04-06]
```

# Ejercicio 4

Creamos un archivo y con el siguiente comando lo ciframos, para que solo podamos acceder a el con la contraseña.

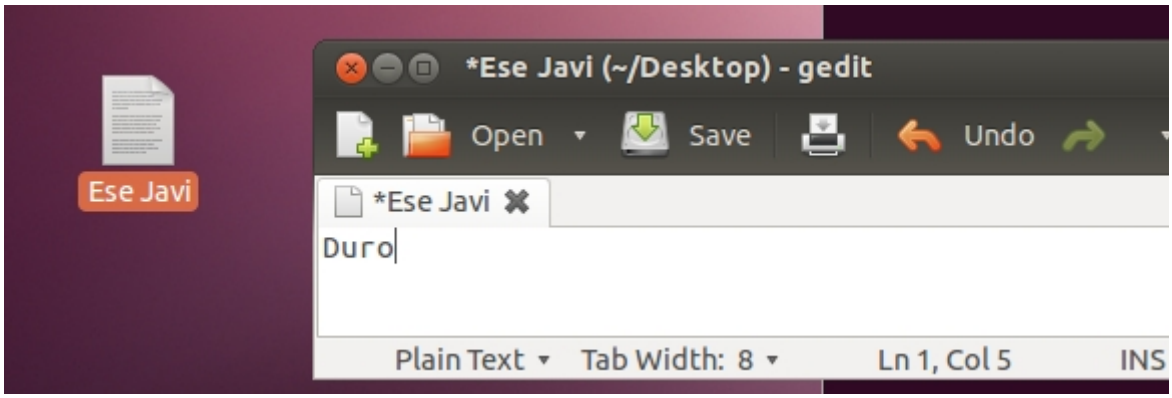



Lo mandamos al otro usuario donde el ya tenia la clave publica por los ejercicios anteriores, lo abrimos y comprobamos que muestra su contenido. Si lo hiciésemos en un ordenador que no tenga la clave no nos mostrara el contenido.

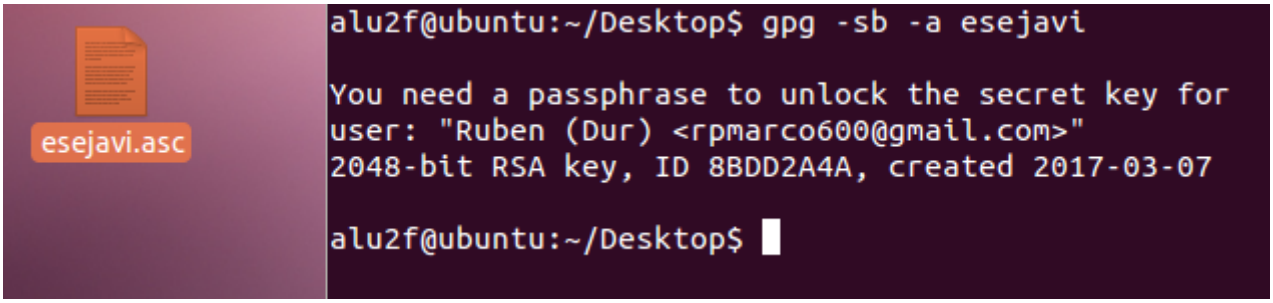


# Ejercicio 5

Creamos un documento con algo escrito dentro, para posteriormente modificarlo.



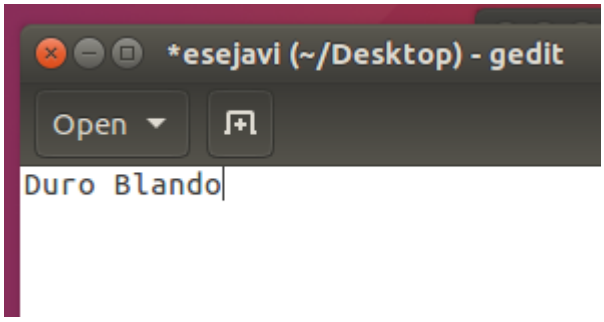

Creamos una clave para el documento.




Ejecutamos el siguiente comando para desencriptar el documento anterior.

```
root@ubuntu:/home/alu2f/Desktop# gpg --decrypt -o esejavi esejavi.asc
gpg: assuming signed data in `esejavi'
gpg: Signature made Mon 13 Mar 2017 08:45:52 AM PDT using RSA key ID 8BDD2A4A
gpg: Good signature from "Ruben (Dur) <rpmarco600@gmail.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 6BFE 9A26 320E 3394 A796  D10D 1A97 576B 8BDD 2A4A
root@ubuntu:/home/alu2f/Desktop#
```

Comprobamos que podemos modificar el archivo cuando introducimos la contraseña que hemos añadido anteriormente.




Con el siguiente comando verificamos si hemos modificado el archivo y comprobamos que si no ponemos la contraseña no nos dejara modificar.

```
root@ubuntu:/home/alu2f/Desktop# gpg --decrypt -o esejavi esejavi.asc
gpg: assuming signed data in `esejavi'
gpg: Signature made Mon 13 Mar 2017 08:45:52 AM PDT using RSA key ID 8BDD2A4A
gpg: BAD signature from "Ruben (Dur) <rpmarco600@gmail.com>"
root@ubuntu:/home/alu2f/Desktop#
```