

# **Práctica**

# **Cifrado Simétrico GnuPG**

**Franco Larrea**

2º SMR-A  
(Prof. Fernando Albert González)  
Instituto IES SAN VICENTE

# Índice

Teoría.....	Pag. 3
Tareas y cuestiones.....	Pag. 4
1.....	Pag. 3
2.....	Pag. 3
3.....	Pag. 5
4.....	Pag. 6
5.....	Pag. 10
6.....	Pag. 12
7.....	Pag. 13
8.....	Pag. 14
9.....	Pag. 17
Problemas encontrados.....	Pag. 18
Fuentes.....	Pag. 18

# Teoría

Para realizar esta practica es conveniente saber algunos conceptos:

## **Cifrado Simétrico**

### **¿Que es?**

La criptografía de clave simétrica (en inglés symmetric key cryptography), también llamada criptografía de clave secreta, es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor.

### **Funcionamiento**

Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y este lo descifra con la misma clave.

## **GnuPG**

### **¿Que es?**

GNU Privacy Guard (GnuPG o GPG) es una herramienta de cifrado y firmas digitales desarrollado por Werner Koch. Es software libre licenciado bajo la GPL.

GPG utiliza el estándar del IETF denominado OpenPGP.

# Tareas y cuestiones

**Cifrado simétrico con GnuPG sobre la distribución GNU/Linux**

**Mediante el comando gpg cifraremos un par de mensajes (uno normal y otro ASCII) que enviaremos por correo a un compañero y él nos tendrá que contestar también cifrado.**

**Opciones de gpg que utilizaremos:**

**gpg -c documento → encriptación**

**gpg -ca documento → encriptación en ASCII**

**gpg -d documento.gpg/asc > documento2 → desencriptación**

**Se deberá realizar como siempre un informe con todas las partes necesarias.**

Para poder cifrar dos mensajes y enviarlos primero necesitamos un par de mensajes.

Así que abrimos el nano desde una terminal y creamos dos mensajes.

```
fmol107@machine103: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3      mensaje_encriptado_Franco      Modificado
Este es un mensaje cifrado simetrico mediante GnuPG de Franco Larrea para Fran.
2SMRA
Cosas randoms por aqui escritas.
```

```
fmol107@machine103: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3      mensaje_encriptado_Franco_ASCII      Modificado
Este es otro mensaje encriptado y este otro mensaje totalmente aleatorio.
```



Ya tenemos dos mensajes creados para cifrar.

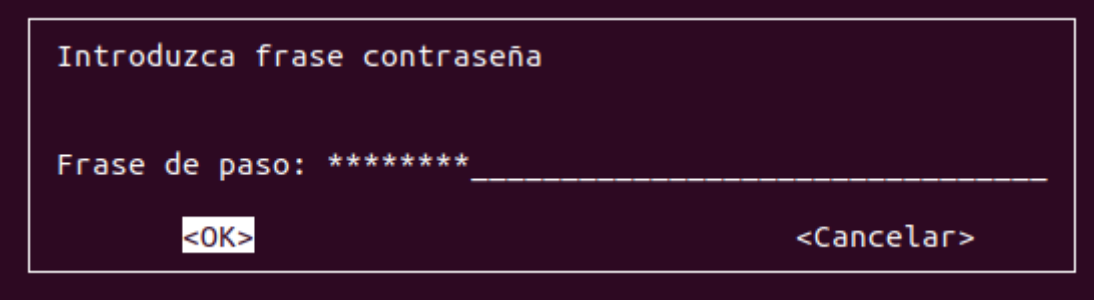
Vamos a encriptar el primer mensaje. Para ello ejecutaremos el siguiente comando:

**gpg -c <Ruta-del-archivo-a-encriptar>**

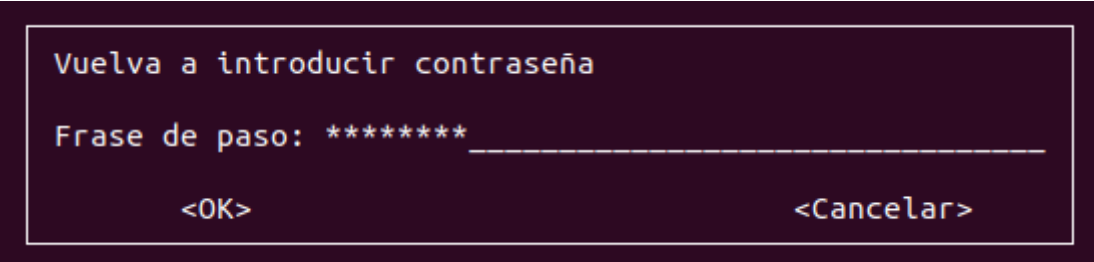
En caso de que nos de problemas de permisos lo ejecutaremos con **sudo** delante.

```
fmol107@machine103:~/Escritorio$ sudo gpg -c mensaje_encriptado_Franco
```

Nos solicitará una contraseña.

A dark-themed dialog box with a white border. It contains the text "Introduzca frase contraseña" at the top. Below it is "Frase de paso: \*\*\*\*\*" followed by a dashed line for input. At the bottom, there are two buttons: "<OK>" on the left and "<Cancelar>" on the right.

Después de poner una contraseña nos pedirá confirmación de la misma.

A dark-themed dialog box with a white border. It contains the text "Vuelva a introducir contraseña" at the top. Below it is "Frase de paso: \*\*\*\*\*" followed by a dashed line for input. At the bottom, there are two buttons: "<OK>" on the left and "<Cancelar>" on the right.

Después de introducir la contraseña nos generará el fichero encriptado.

Ahora vamos a encriptar el segundo mensaje. Este lo encriptaremos en ASCII.

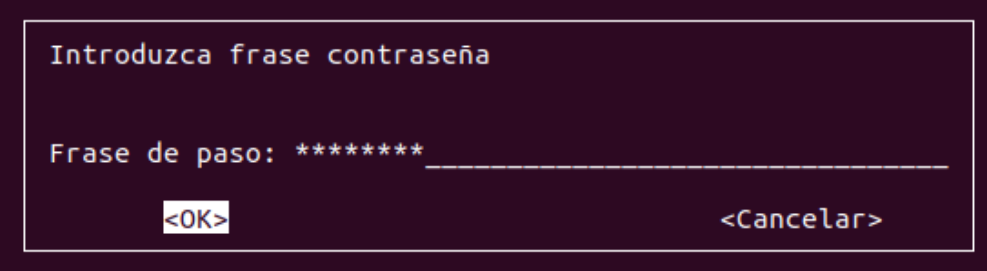
Para ello ejecutaremos el siguiente comando:

**gpg -c -a <Ruta-del-archivo-a-encriptar>**

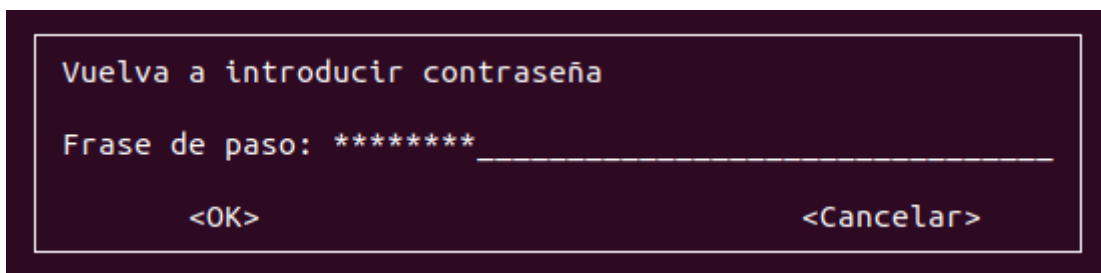
En caso de que nos de problemas de permisos lo ejecutaremos con **sudo** delante.

```
fmol107@machine103:~/Escritorio$ sudo gpg -ca mensaje_encriptado_Franco_ASCII
```

Volverá a pedirnos una contraseña. Puede ser una diferente o la misma, para esta práctica he puesto la misma que para el anterior cifrado.

A dark-themed dialog box with a white border. It contains the text "Introduzca frase contraseña" at the top. Below it is "Frase de paso: \*\*\*\*\*" followed by a dashed line for input. At the bottom, there are two buttons: "<OK>" on the left and "<Cancelar>" on the right.

Y nuevamente tendremos que confirmar la contraseña.

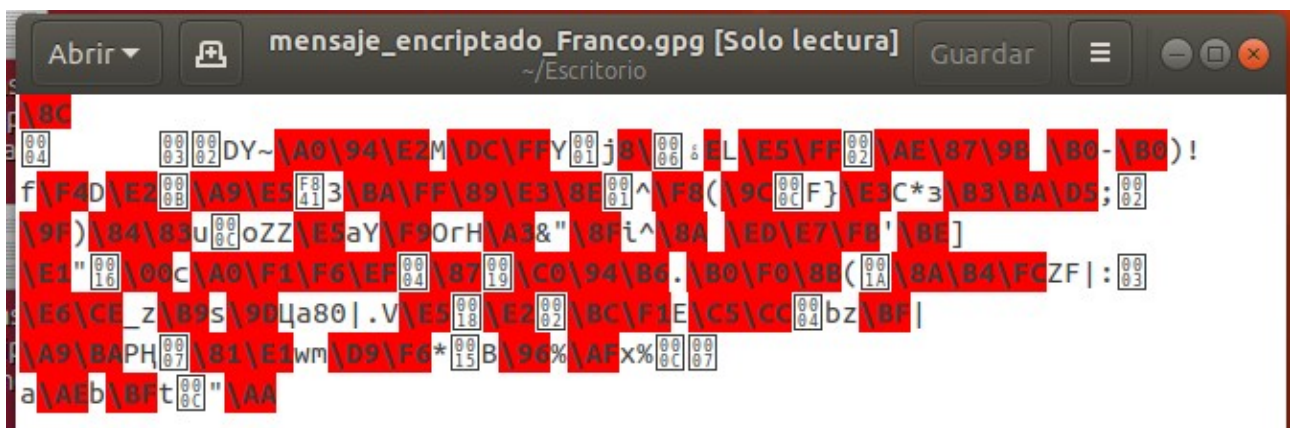


Después de introducir la contraseña nos generará el otro fichero encriptado.

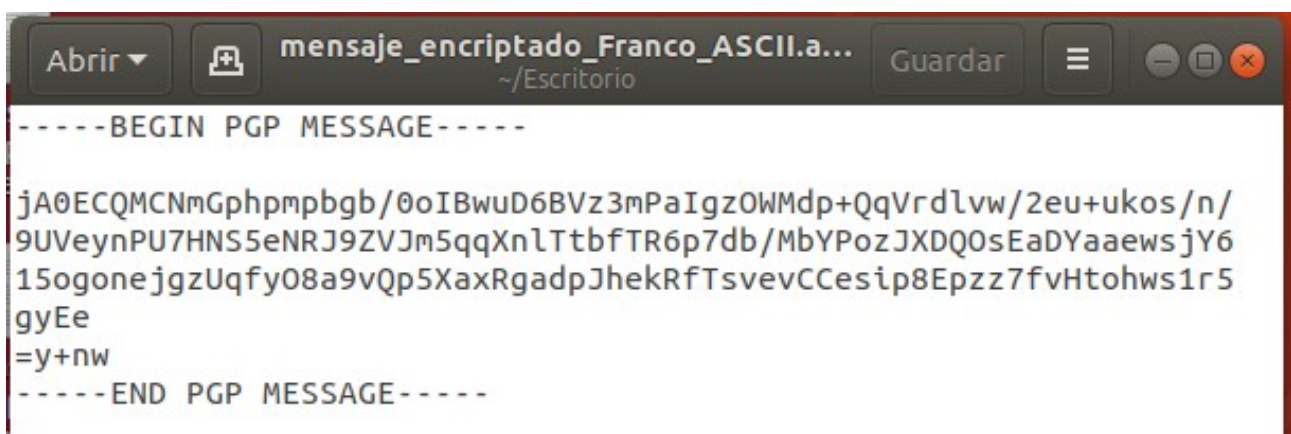
Después de esto ya tendremos los dos archivos encriptados.



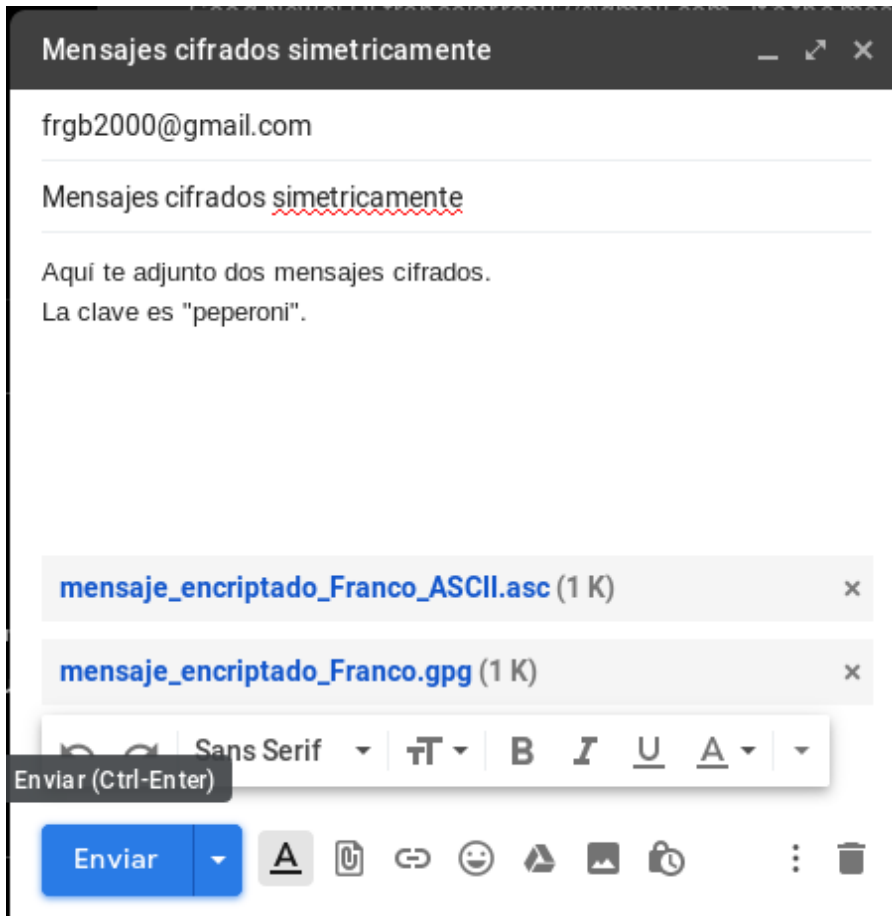
Si abrimos los archivos cifrados podemos ver que el texto es ilegible.



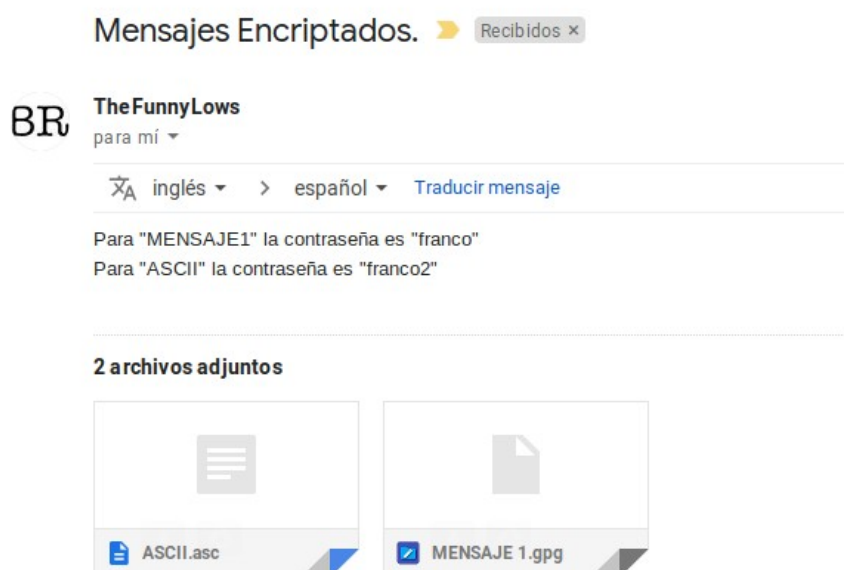
Al menos el archivo que hemos encriptado con ASCII tiene letras entendibles por el editor.



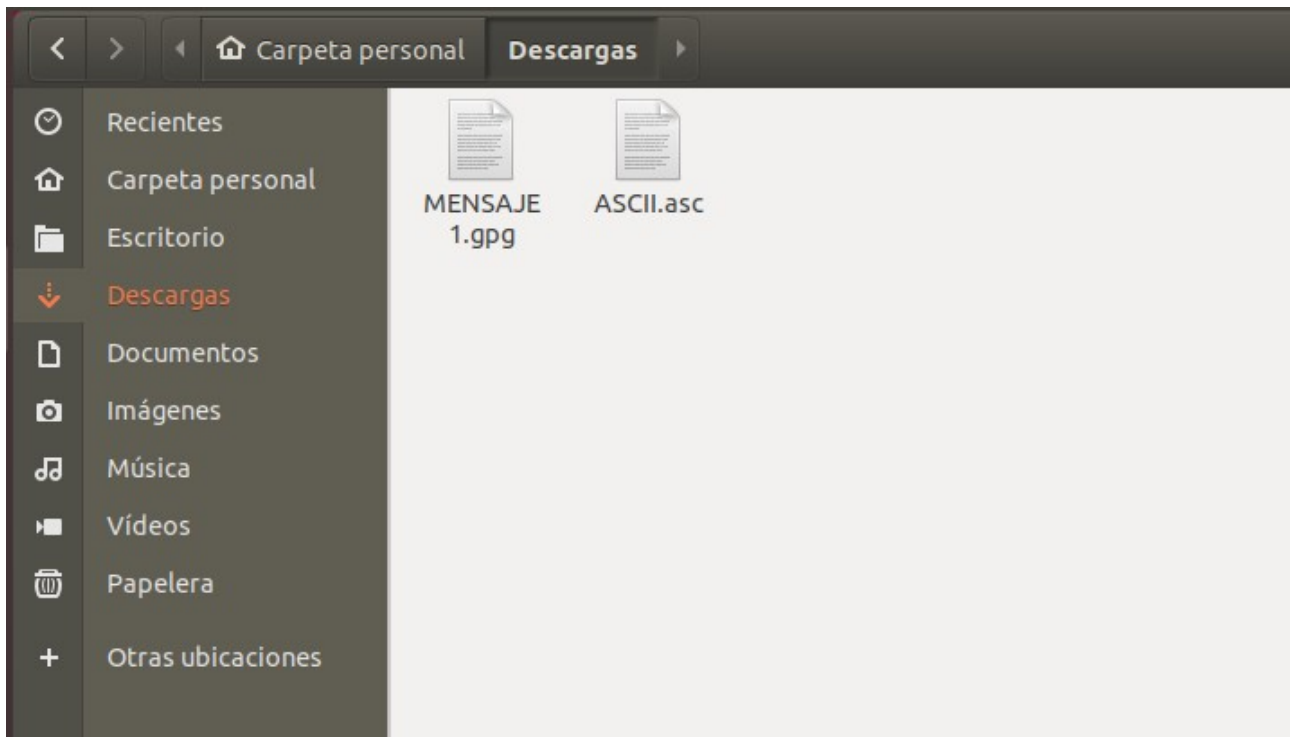
Ahora mandaré los dos mensajes encriptados a mi compañero Fran Gomez.



De la misma forma que he hecho yo, Fran ha encriptado dos archivos y me los ha mandado por correo junto a las claves de encriptación.



Descargaré los dos archivos encriptados que me ha mandado mi compañero.



Ahora voy a proceder a descriptarlos.

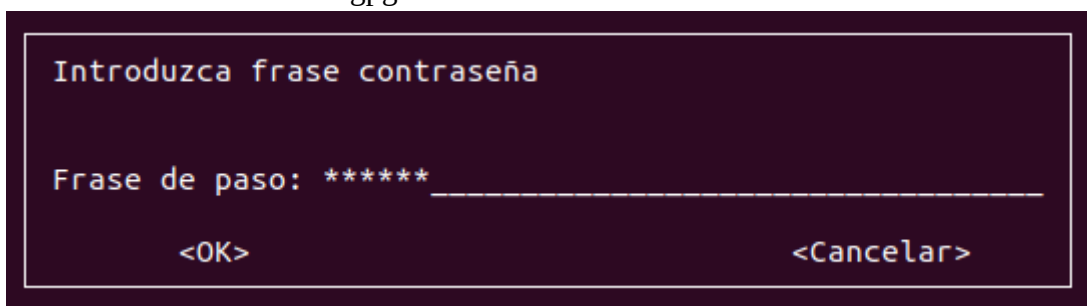
Para ello ejecutaremos el siguiente comando:

```
gpg -d <Ruta-del-archivo-a-desencriptar> > <nombre-mensaje-desencriptado>
```

En caso de que nos de problemas de permisos lo ejecutaremos con **sudo** delante.

```
fmol107@machine103:~/Descargas$ sudo gpg -d MENSAJE\ 1.gpg > MENSAJE1desencriptado
gpg: AVISO: propiedad insegura del directorio personal '/home/fmol107/.gnupg'
gpg: datos cifrados AES256
gpg: cifrado con 1 frase contraseña
```

Nos solicitará la contraseña con la que nuestro compañero ha encriptado el archivo. En el caso del documento “MENSAJE 1.gpg” la contraseña es “franco”.



Después de introducir la contraseña nos generará el fichero desencriptado.



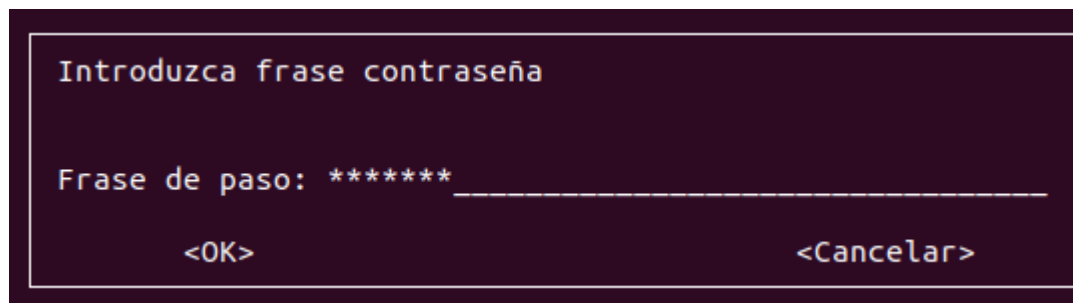
El otro mensaje se descripta igual. Con el comando:

**gpg -d <Ruta-del-archivo-a-descriptar> > <nombre-mensaje-descriptado>**

**En caso de que nos de problemas de permisos lo ejecutaremos con sudo delante.**

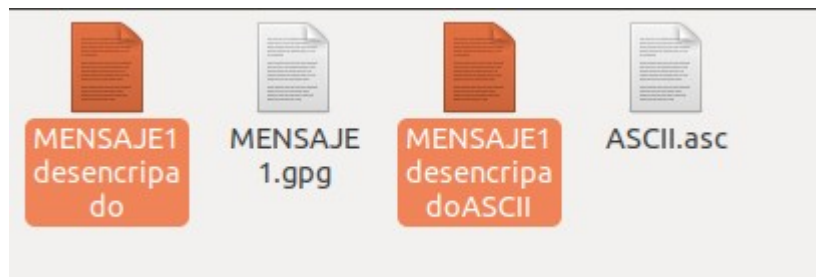
```
fmol107@machine103:~/Descargas$ sudo gpg -d ASCII.asc > MENSAJE1desencriptadoASCII
gpg: AVISO: propiedad insegura del directorio personal '/home/fmol107/.gnupg'
gpg: datos cifrados AES256
gpg: cifrado con 1 frase contraseña
```

Nos solicitará la contraseña con la que nuestro compañero ha encriptado el archivo. En el caso del archivo llamado “ASCII.asc” la contraseña es “franco2”.

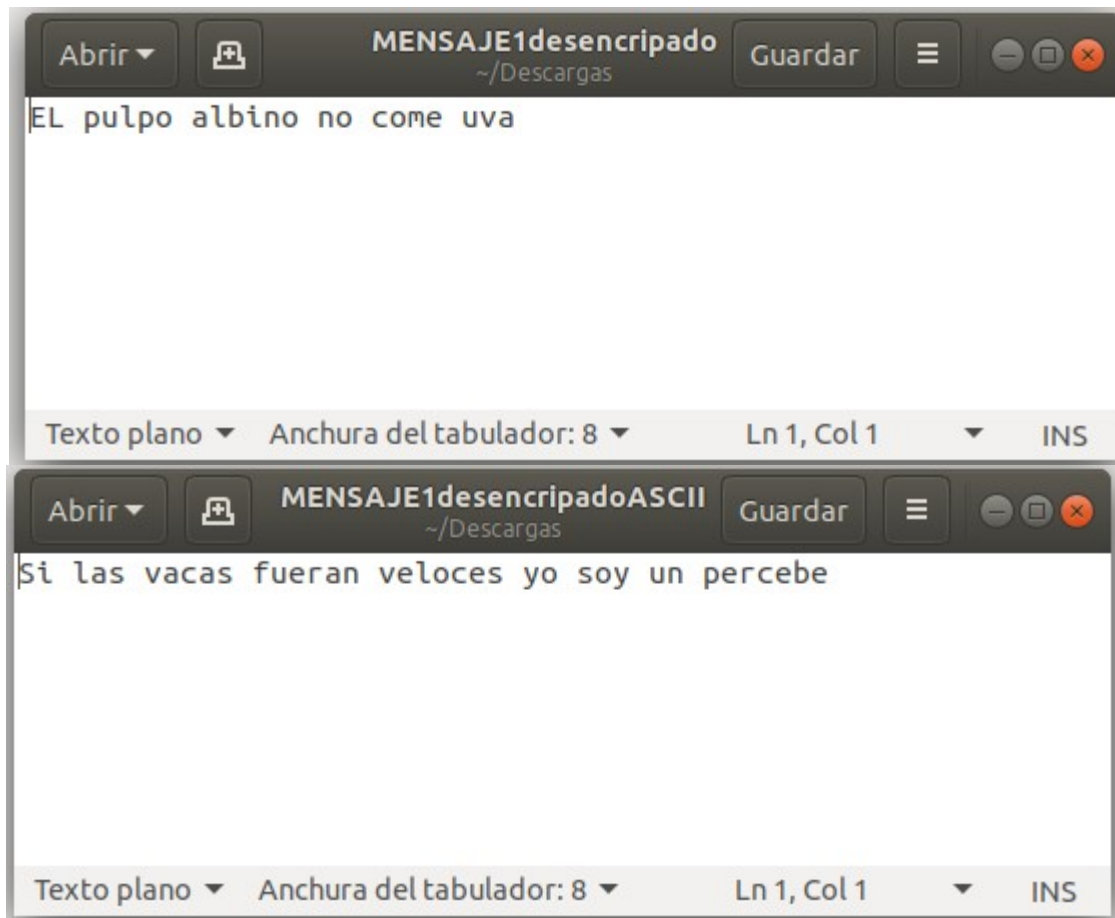


Después de introducir la contraseña nos generará el fichero desencriptado.

Ya tendríamos los dos archivos desencriptados.



Como podemos observar, los mensajes de mi compañero son legibles.



# Problemas encontrados:

Esta práctica se ha realizado sin dificultades.

# Fuentes:

- [https://es.wikipedia.org/wiki/GNU\\_Privacy\\_Guard](https://es.wikipedia.org/wiki/GNU_Privacy_Guard)
- [https://es.wikipedia.org/wiki/Criptograf%C3%ADa\\_sim%C3%A9trica](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica)