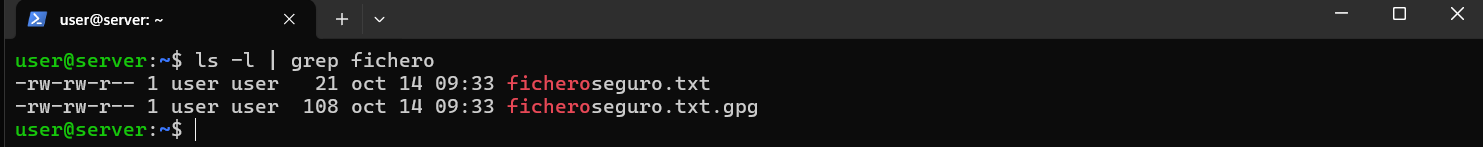
Para la realización de este ejercicio, se procede a la creación de un fichero llamado: “ficheroseguro.txt”. Esto lo haremos con el comando “nano ficheroseguro.txt”. Pondremos nuestro nombre y apellidos. Con el atajo “Ctl + O - Enter” guardamos el fichero.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Con el comando “gpg -c ficheroseguro.txt” procedemos a cifrar nuestro fichero. Se creará otro fichero llamado “ficheroseguro.txt.gpg”.

Con el comando “ls -l | grep ficheroseguro” nos muestra el fichero que hemos creado con el “nano” y el fichero “.gpg”.



Con el comando “cat ficheroseguro.txt.gpg” nos muestra el fichero con lenguaje cifrado.



Probamos a desencriptar el fichero previamente cifrado. Si lo hacemos desde nuestra terminal, lo desencripta sin problema.



Sin embargo, si lo hacemos desde otra terminal, nos pide la contraseña.

Texto

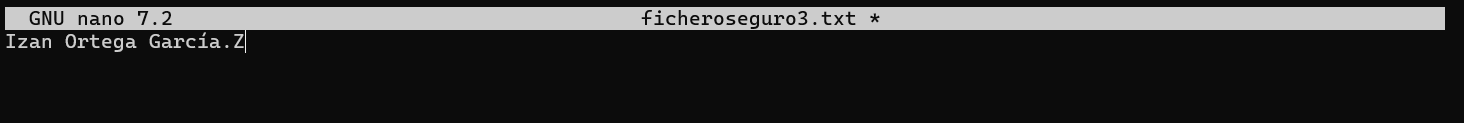
Descripción generada automáticamente

Con el comando “gpg –version” podemos ver la versión de “GPG” que tenemos. Soporta varias técnicas de cifrado, de hecho, se puede usar para funciones de “hashing”. Se puede hacer con otras versiones de GPG.

Texto

Descripción generada automáticamente

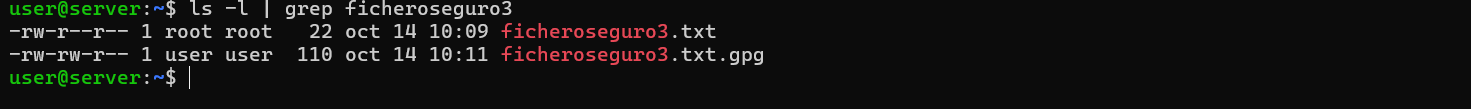
Ahora, procederemos a crear un fichero llamado “ficheroseguro3.txt” el cual, procederemos a cifrar con TWOFISH.



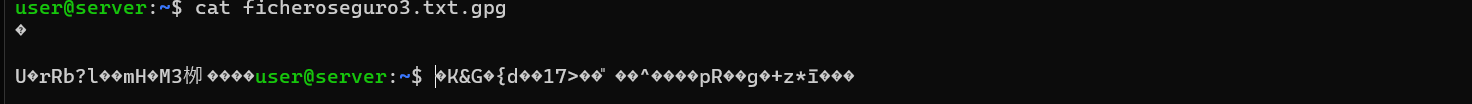
Con el siguiente comando, ciframos el fichero en TWOFISH: “gpg -c --cipher-algo TWOFISH ficheroseguro3.txt”. El parámetro que permite seleccionar el algoritmo con el que queremos cifrar es “—cipher-algo TWOFISH”.



Comprobamos que se ha creado un fichero “.gpg” y que está cifrado.



Con el comando “cat” comprobamos que el fichero está cifrado.



Para el siguiente paso, procederemos a instalar las “Guest Additions”.

# Desencriptación del fichero “secreto.txt”.

Texto

Descripción generada automáticamente