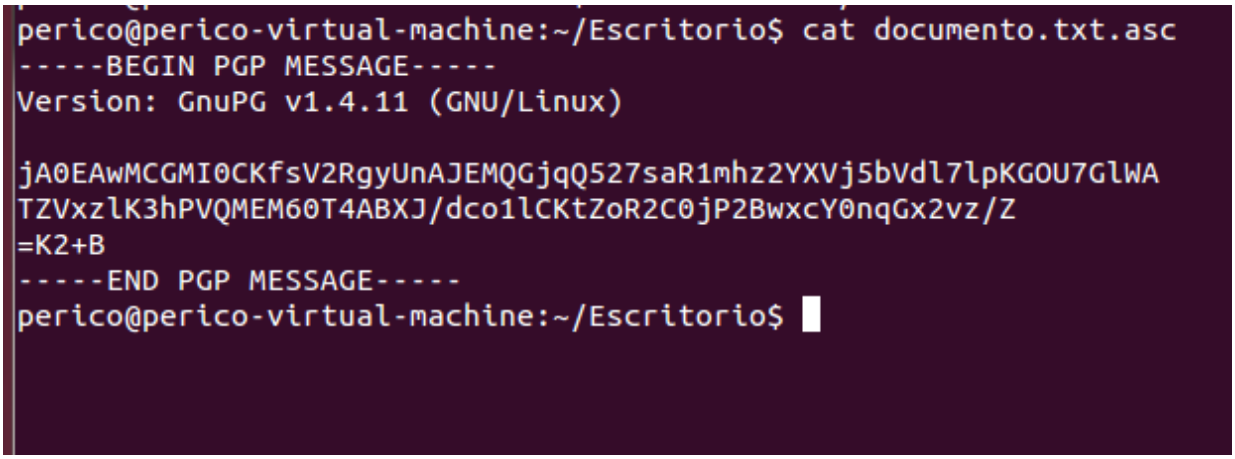
Ejercicio: Cifrado simétrico de un documento

1. Crea un documento de texto con cualquier editor o utiliza uno del que dispongas.
   Lo hice con click derecho crear documento.Lo llame documento.txt
2. Cifra este documento con alguna contraseña acordada con el compañero de al lado.
   Contraseña: documento.txt
3. Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar. Por USB.
4. Descifra el documento que te ha hecho llegar tu compañero de al lado.
   Antoniosoler.txt contraseña antoniosoler123
5. Repite el proceso anterior, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.



6. Copia y pega el contenido del archivo cifrado anteriormente y envíalo por mail a tu compañero para que lo descifre. Enviado a Antonio Soler
7. Una vez has recibido el mensaje de tu compañero en tu mail, copialo en un archivo de texto para obtener el mensaje original.

   #gpg 1234.txt
   mensaje original HOLA

Ejercicio:Creación de nuestro par de claves publica-privada

1. Siguiendo las indicaciones de este epígrafe, crea tu par de claves pública y privada. La clave que vas a crear tendrá una validez de 1 mes.
   #gpg -–gen-key
   Luego elegimos la opcion 1
   Seleccionamos la longitud de las claves (2048)
   Periodo de validez: ponemos 1m
   Nos aparecerá un mensaje que nos indica cuando caduca la clave.
   Ahora introducimos :
   Nombre y Apellidos:(Javier Triguero)
   Correo electrónico:(javi997@gmail.com)
   Comentario:(gj gl wp honor me)
   Nos aparecerá un mensaje de que si todo esta bien le decimos que si ponemos una V.
   Nos saldrá un recuadro para poner la contraseña (hola)
   Una vez se haya completado los bytes necesarios ya estará lista

2. Recuerda el ID de usuario de tu clave y la contraseña de paso utilizada. Anotala en un lugar seguro si lo consideras necesario.

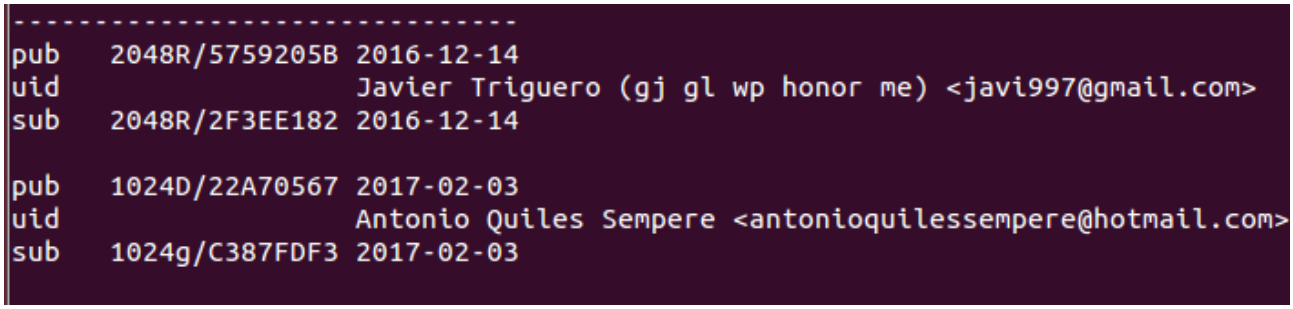
Ejercicio: Exportar e importar claves públicas.

1. Exporta tu clave pública en formato ASCII y guardalo en un archivo nombre_apellido.asc y envíalo a un compañero/a.
   #gpg -a --export -o miclavejavier.asc key_id
   #gpg -a --export --output miclavejavier.asc key_id

   #gpg -a --export key_id > miclavejavier.asc

2. Importa las claves públicas recibidas de vuestros/as compañeros/as.
   #gpg –import claveantonio.asc
3. Comprueba que las claves se han incluido correctamente en vuestro keyring.

   Para comprobarlo:
   #gpg -kv



Ejercicio: Cifrado y descifrado de un documento.

1. Cifraremos un archivo cualquiera y lo remitiremos por email a uno de nuestros compañeros que nos proporcionó su clave pública.
   #gpg -aer documentov2.txt
   Archivo cifrado documentov2.txt.asc
   Para descifrarlo tiene que gpg documentov2.txt
2. Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos. archivoantonio.asc
3. Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.
   Hemos podido descifrarlo porque conocemos entre nosotros nuestras claves publicas
4. Por último, enviaremos el documento cifrado a alguien que no estaba en la lista de destinatarios y comprobaremos que este usuario no podrá descifrar este archivo.

   José,al no estar en mi lista de destinatarios no puede ver el contenido del archivo documentov2.txt.asc Porque no conoce mi clave

Ejercicio: Firma digital de un documento.

1. Crea la firma digital de un archivo de texto cualquiera y envíale éste junto al documento con la firma a un compañero.
   #gpg -sb -a documentofirmado
   #gpg documentoformado.asc

2. Verifica que la firma recibida del documento es correcta.

   Gpg –verify documentofirmado.asc

3. Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica. Si se verifica.