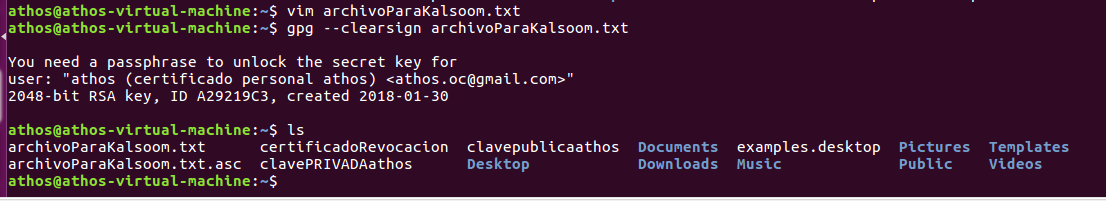
# Firma digital

En esta práctica vamos a firmar un documento, para poder verificar más tarde que fue precisamente el remitente el que realmente envió ese archivo.

Para esto, vamos a crear un archivo, y vamos a firmarlo con el comando gpg –clearsign nombredearchivo

Tras esto, nos pedirá la contraseña (si es que la tiene) de nuestra clave publica.

Creamos una archivo y lo firmamos



Esto nos generara otro archivo. Este archivo añade al archivo original un hash del archivo original, firmado con nuestra clave privada. El archivo tiene extensión asc. Es precisamente este archivo el que enviaremos para que mas tarde puedan comprobar que realmente fuimos nosotros quien lo envió.

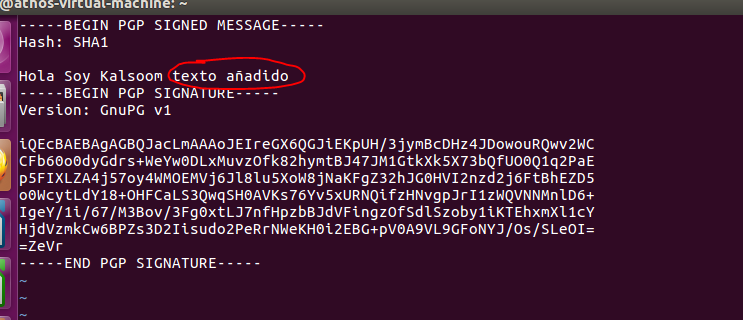
Hemos recibido un archivo de un compañero, y vamos a verificar que fue el el que nos mando el archivo. Para poder comprobar que la firma corresponde con nuestro compañero, primero deberemos tener la clave publica de este. Puede enviárnosla por correo, o subirlo a un repositorio de los que hay para esta tarea.

Comprobamos si el archivo que hemos recibido corresponde al remitente con el comando gpg –verify nombre de archivo.

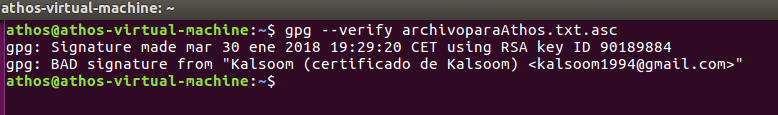


Como vemos en la imagen anterior, la firma corresponde con kalsoom, aunque nos sale una advertencia que nos indica que el certificado no ha sido expedido por una entidad certificadora (ca) con lo cual, en realidad no podemos verificar que fue realmente kalsoom el que emitió el certificado, ya que cualquiera podría haber creado un certificado auto firmado con los datos de kalsoom

No obstante, modificamos el archivo para comprobar, que después de modificado, si volvemos a comprobar la firma, esta nos da un error.



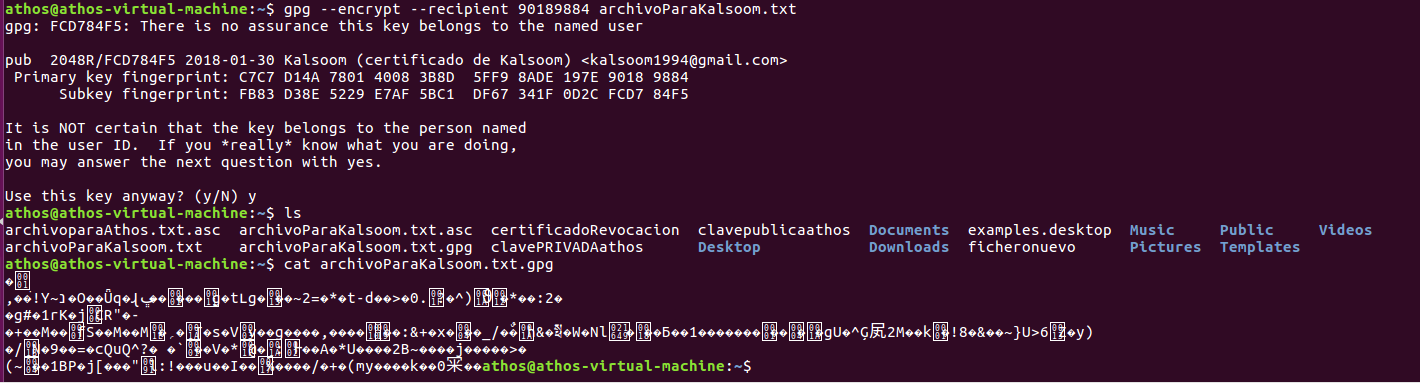
Vemos que ahora no lo verifica bien



# Encriptación:

Ya hemos visto como podemos firmar un documento. Pero esto no impide a un usuario no autorizado a leer el contenido del archivo. Para esto vamos a usar la encriptación. Este proceso consiste en cifrar el mensaje con la clave publica del destinatario, ya que ese archivo cifrado solo podrá descifrarlo el con su clave privada.

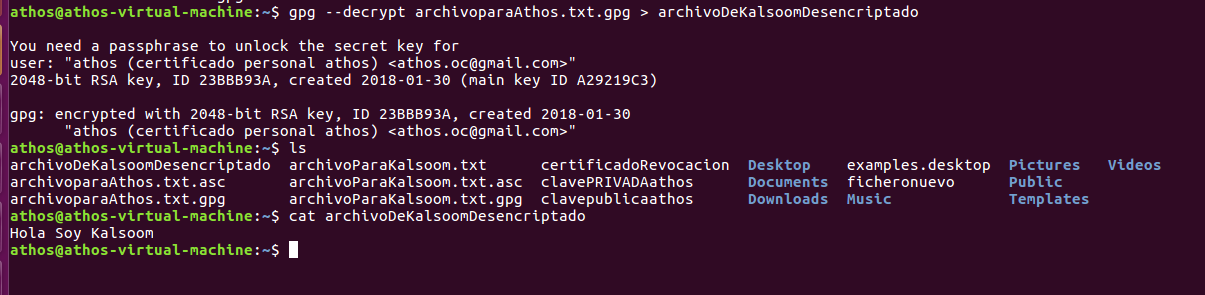
Como hemos visto anteriormente, necesitamos la clave publica del destinatario. Una vez la tenemos, la encriptamos con el comando gpg –encript –recipient (identificador de la clave publica del destinatario) nombredearchivo



Como podemos ver en la imagen anterior, el archivo queda totalmente ilegible y solo podrá desencriptarlo el que posea la clave privada correspondiente a la clave publica con la que ciframos el archivo.

# Desencriptar el archivo

Para desencriptar el archivo, lo haremos con el comando gpg –decrypt nombredearchivo > otronombredearchivo

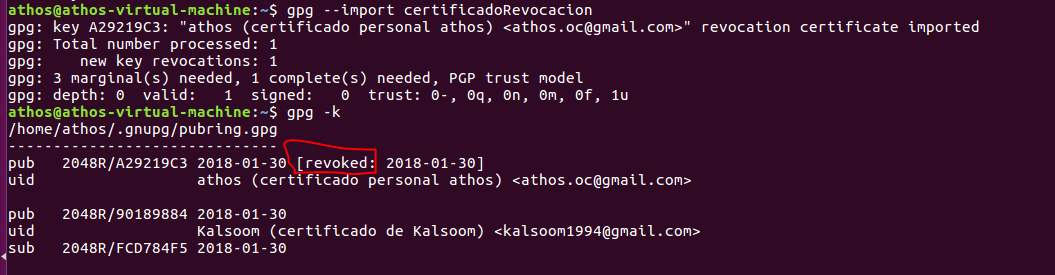


Vemos que después de esto, podemos ver el contenido del mensaje.

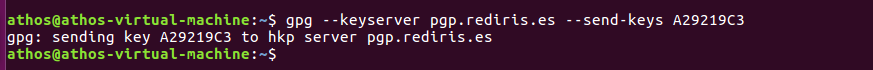
# Revocar certificado:

Si por algún motivo vemos que nuestra clave privada ha sido comprometida, podemos revocar el certificado. Para esto solo tendremos que mandar al servidor el certificado que hemos creado anteriormente (en otra practica) con el comando gpg –import nombredelcertificadoderevocacion

Como vemos en la segunda parte de la siguiente imagen, con el comando gpg –k que sirve para listar las claves, vemos que nuestra clave ha sido revocada



Y con el siguiente comando enviamos la información al servidor de certificados ya que de alguna manera tenemos que informarlo.



Si después de esto, alguien revisase mi clave publica en el servidor, vería que está revocado como vamos a comprobar ahora.

Comprobar certificado revocado de kalsoom

Con el comando de la siguiente imagen, buscamos la clave con el id del compañero y vemos que es de kalsoom y que está revocado.

