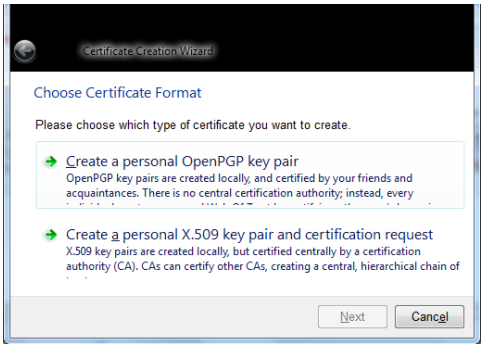
ACTIVIDAD 3 – TÉCNICAS DE CIFRADO – TEMA 2 –SAD

a) Cifrado simétrico: Uso de PGP y GPG.

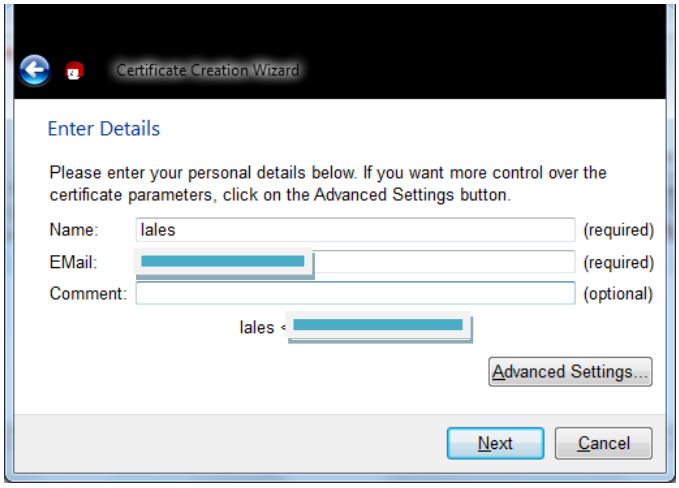
Instalamos GPG en Windows

Esta página la dejamos por defecto

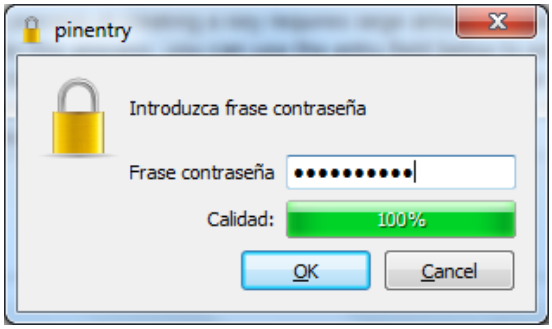
Elegimos crear un nuevo certificado



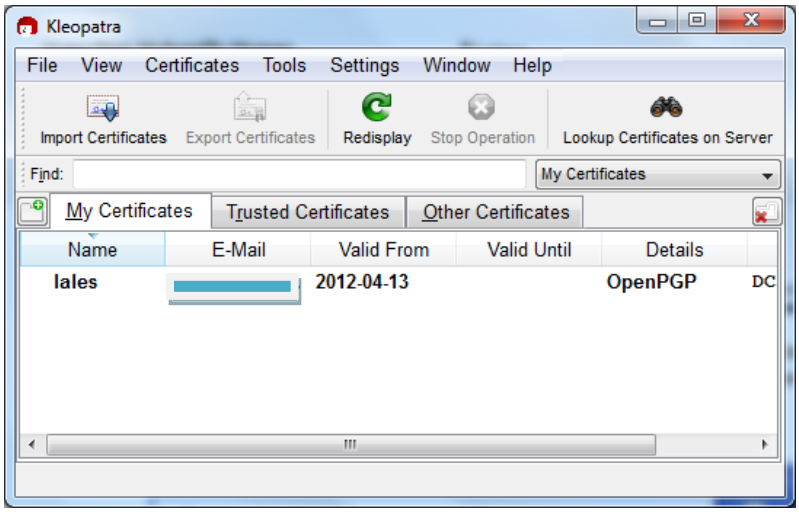
Ahora ponemos nuestros datos



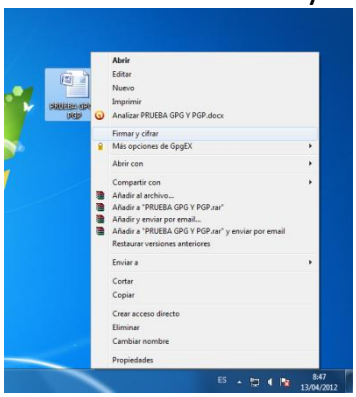
Nos pide que creemos una contraseña



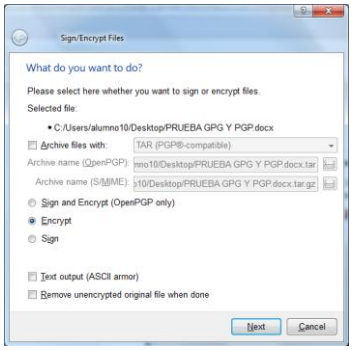
Y aquí vemos como se ha creado el certificado



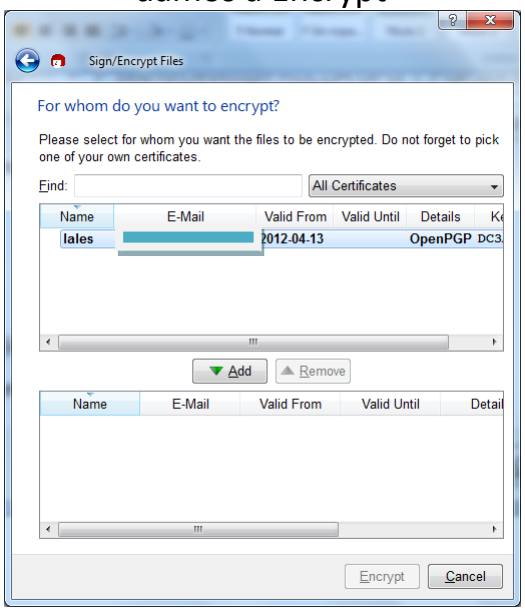
Ahora vamos a crear un documento en el escritorio y le damos con el botón derecho a firmar y cifrar



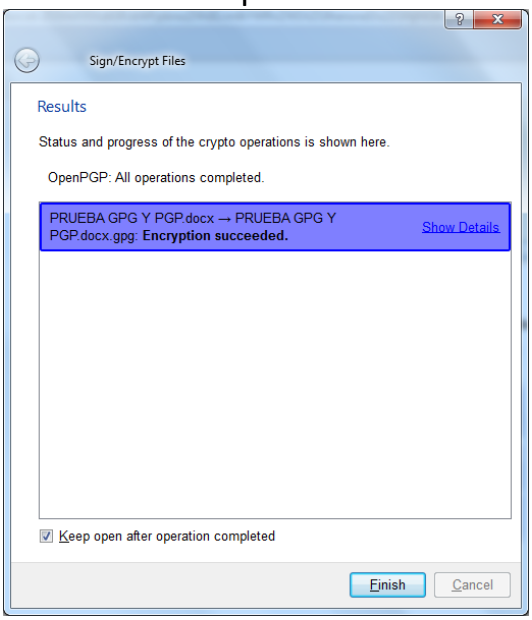
Le damos a Next y continuamos



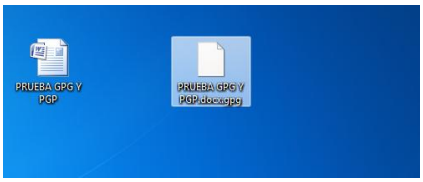
Le damos a añadir y nos lo añade al certificado que hemos creado y le damos a Encrypt



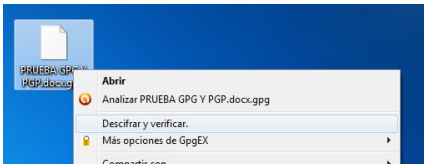
Ya tenemos Encriptado el documento



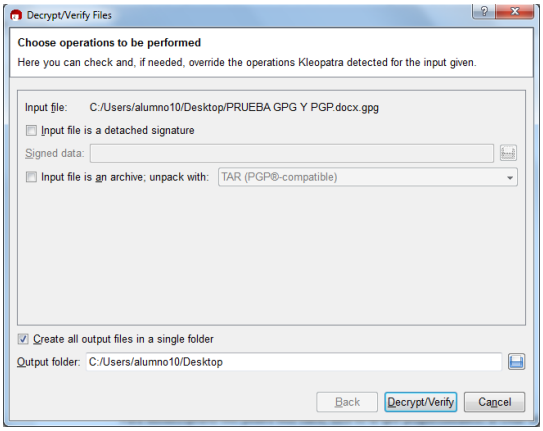
Aquí lo vemos encriptado



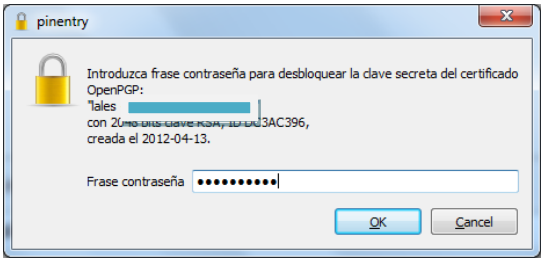
Ahora vamos a descifrarlo, le damos a botón derecho descifrar y verificar



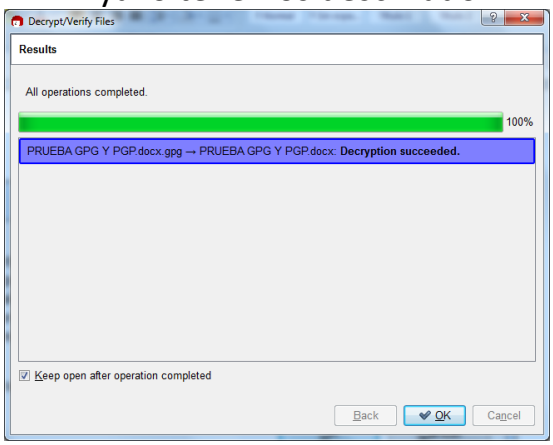
Le damos a Decrypt/Verify en esta ventana



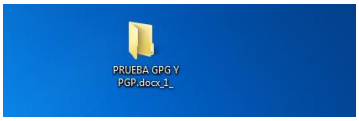
Y nos pide la contraseña que hemos puesto anteriormente



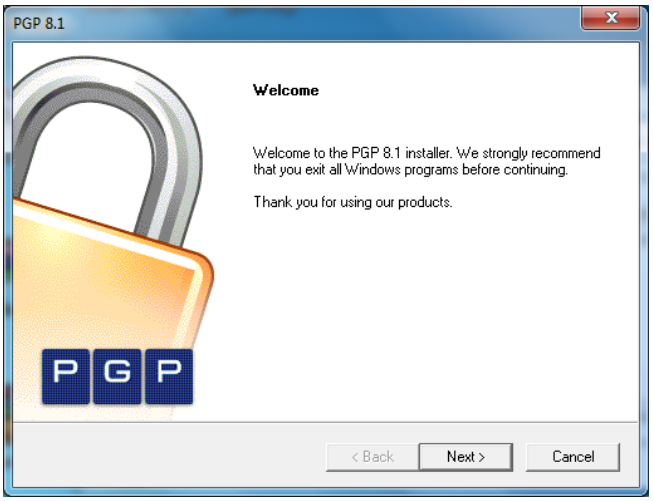
Y ya lo tenemos descifrado



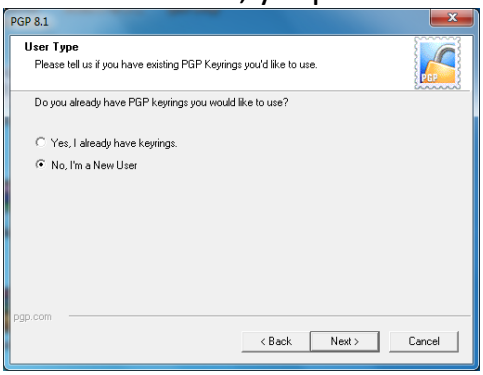
Aquí nos aparece la carpeta que nos ha creado con el documento descifrado

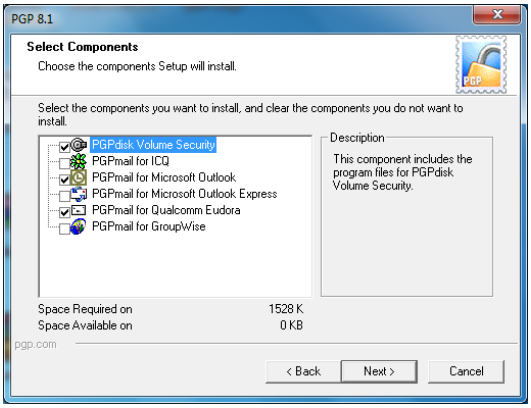


INSTALAMOS PGP EN WINDOWS

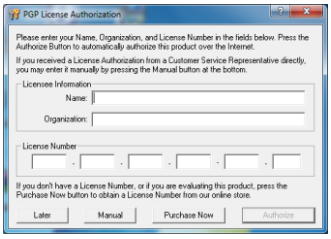


Aquí le damos a No, ya que eres nuevo

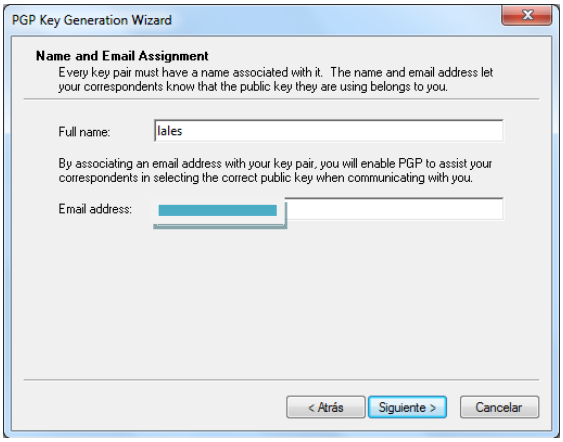




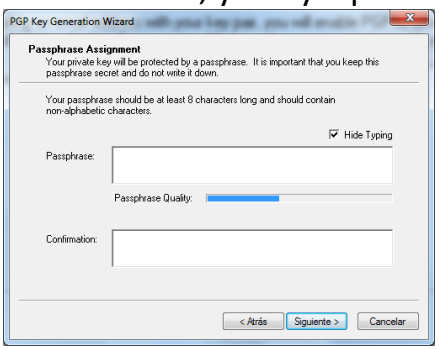
Aquí le damos a Later



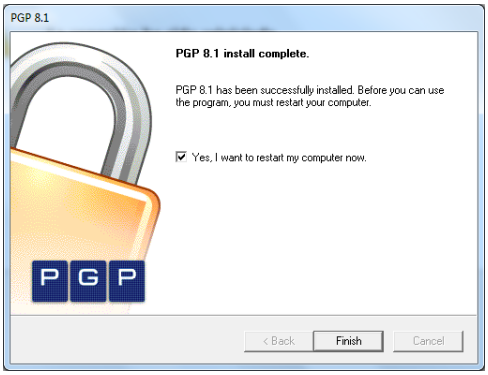
Y aquí ponemos nuestros datos

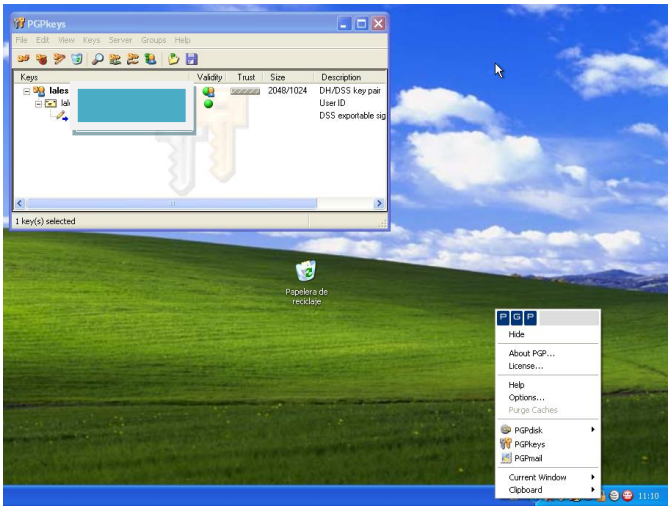


Aquí ponemos una frase, yo voy a poner invesinves

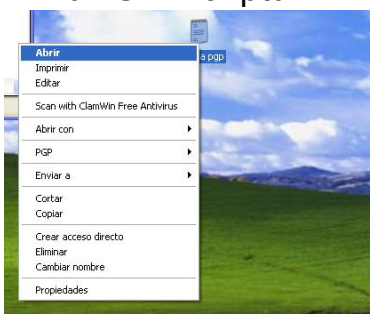


Ya tenemos instalado PGP

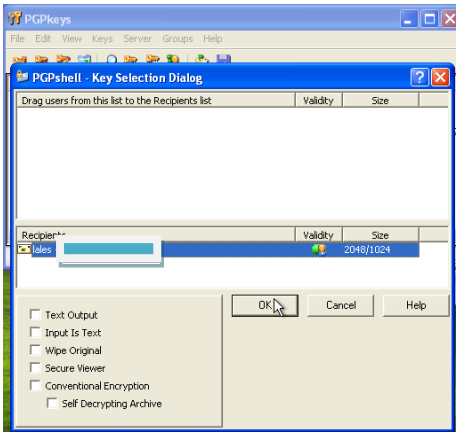




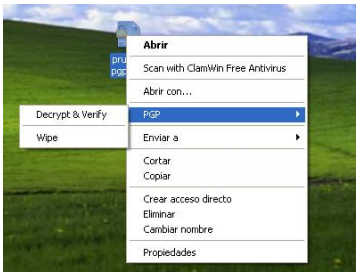
Creamos ahora un fichero en el escritorio y con el botón derecho le damos a PGP Encriptar



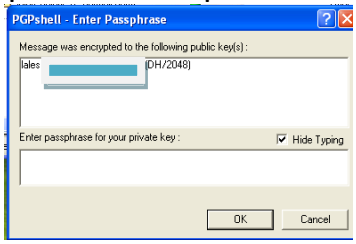
Le damos a Ok y nos aparece en el escritorio el archivo encriptado



Ahora vamos a descifrarlo, le damos con el botón derecho al archivo cifrado y le damos a Decrypt Verify



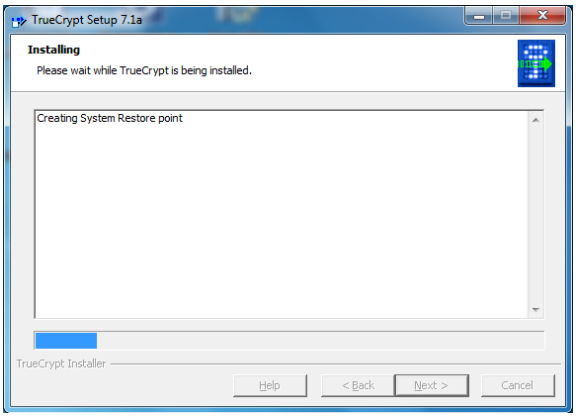
Nos pide la clave para descifrar



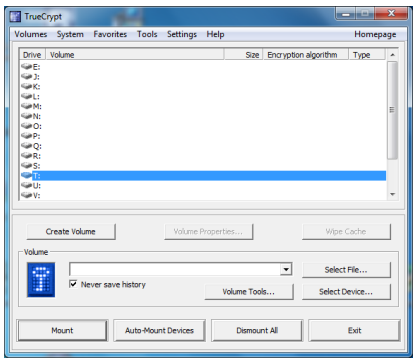
Y ya lo tenemos descifrado

b) Cifrado de datos y particiones: En Windows: Uso de TrueCrypt.

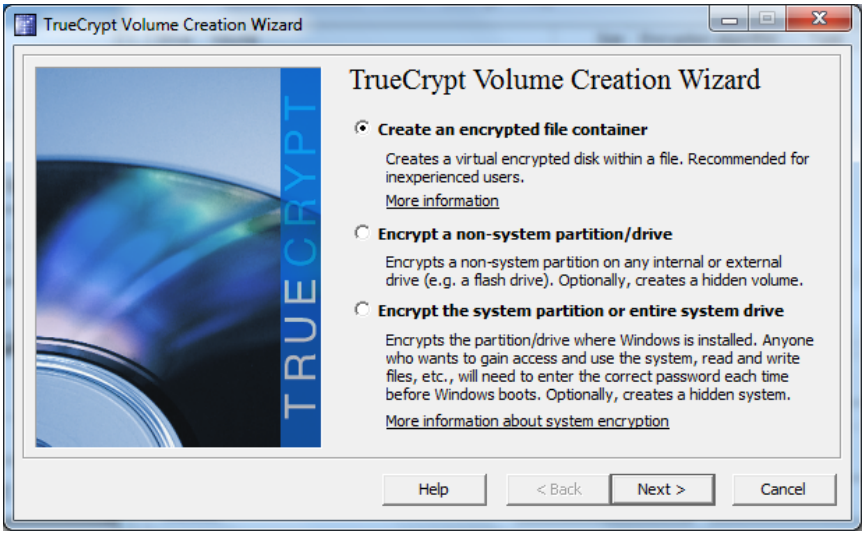
Vamos a descargar TrueCrypt



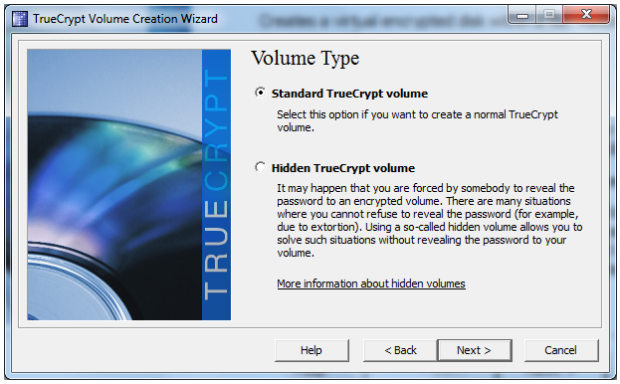
Una vez hecho esto vamos a elegir una unidad



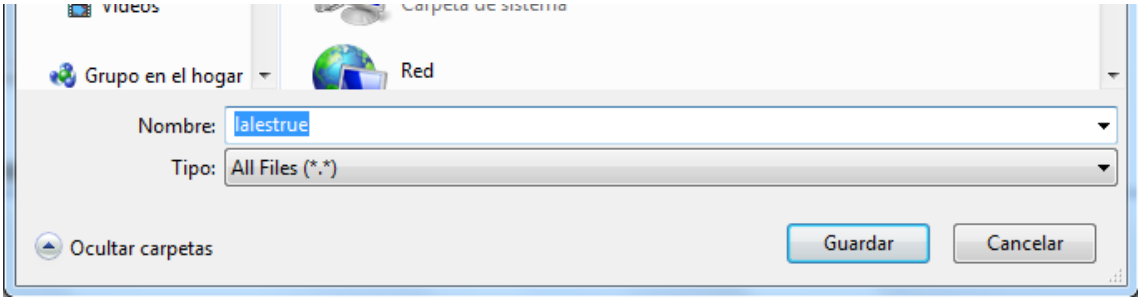
Elegimos la opción que viene por defecto

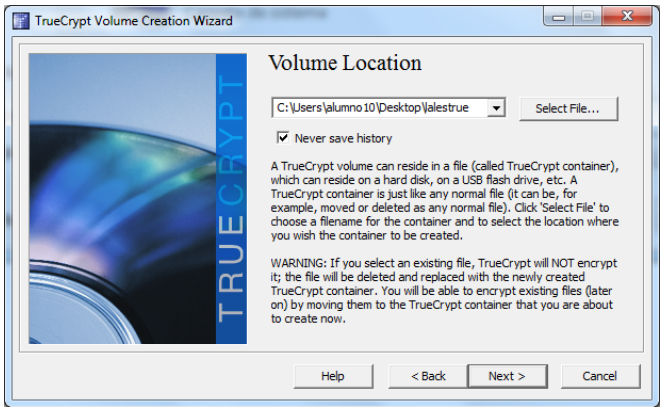


Y esta opción la dejamos igual



Elegimos el sitio donde lo vamos a guardar y un nombre, lalestrue



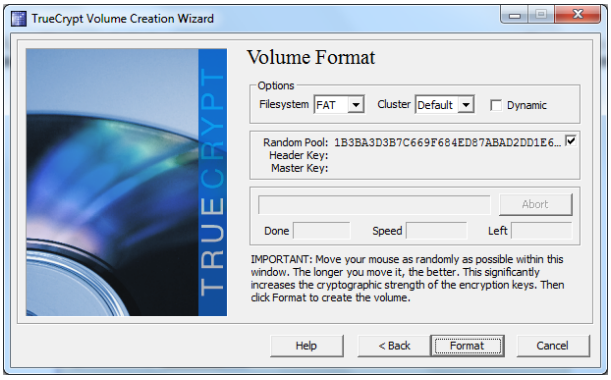


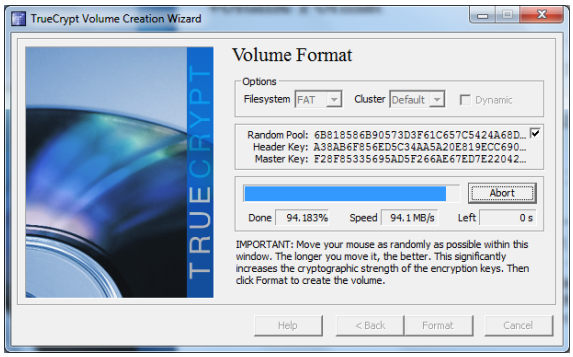
Dejamos la siguiente por defecto

En el volumen elegimos 300 MB

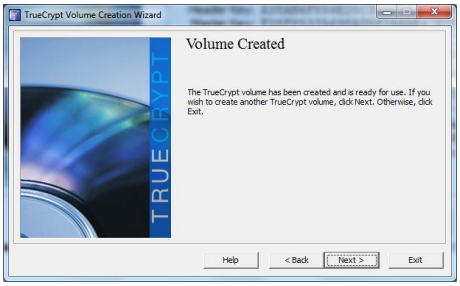
Y ahora ponemos la contraseña que queremos tener para el volumen

Le damos a Format y formatea el volumen

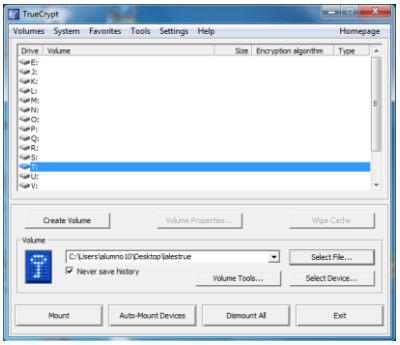




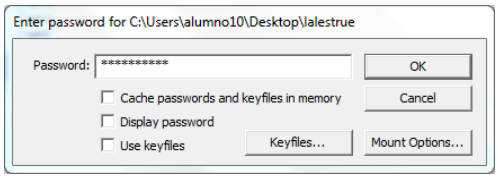
Ya hemos creado el volumen



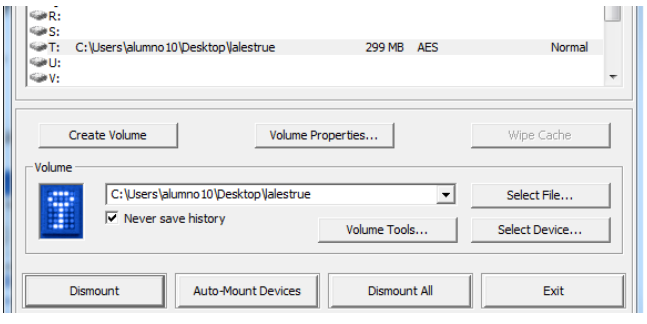
Ahora vamos a abrirlo, elegimos donde lo guardamos, en mi caso en el escritorio

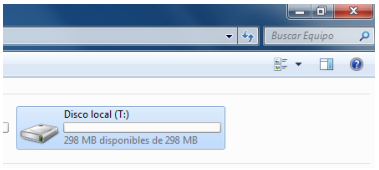


Y ponemos la contraseña que pusimos



Ya lo tenemos montado, vamos a comprobarlo

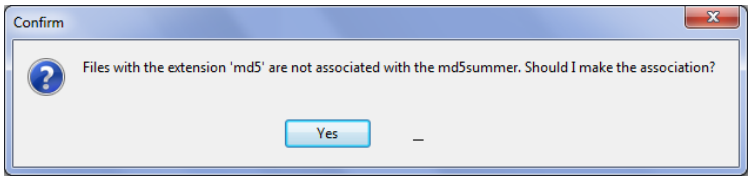




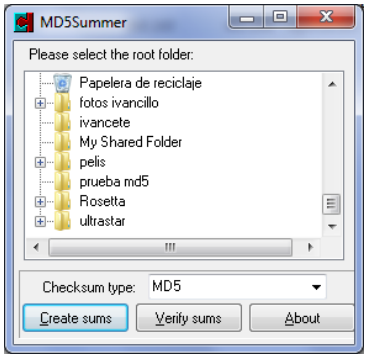
c) Funciones HASH: En Windows: md5sum. En GNU/Linux: md5sum.

En Windows: md5sum

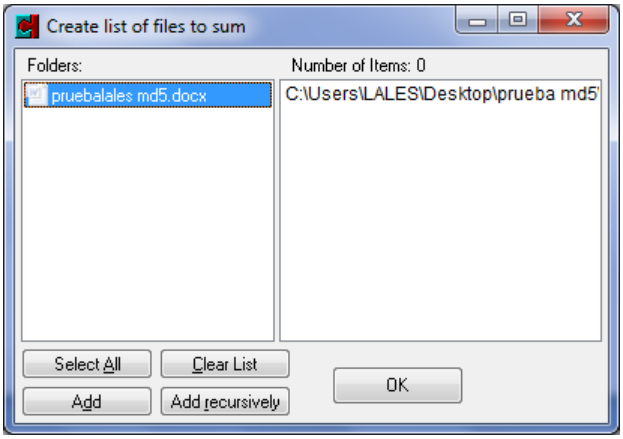
Nos descargamos el programa md5summer y es un ejecutable, le damos a yes y empieza el programa



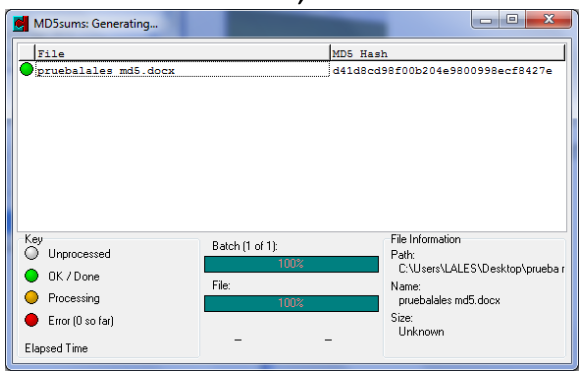
Ahora vamos a elegir una carpeta que hemos creado con el nombre prueba md5 y le damos a Create sums



Ahora elegimos un fichero que tenemos dentro de esta carpeta y lo seleccionamos y le damos a OK

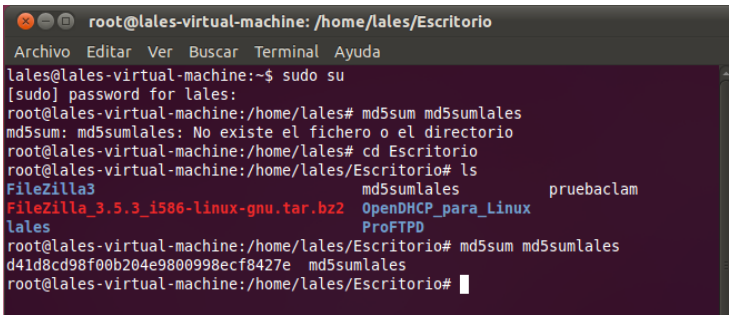


Y nos da el proceso como correcto, nos ha certificado el documento



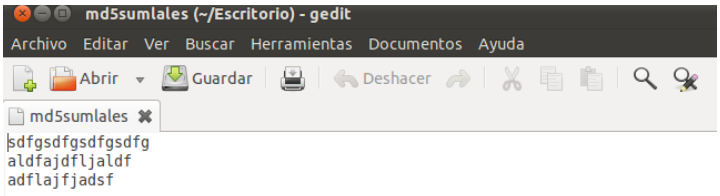
En Linux: md5sum

En Linux lo único que tenemos que hacer es poner en el terminal md5sum y el nombre de un archivo que queramos certificar en este caso md5sumlales

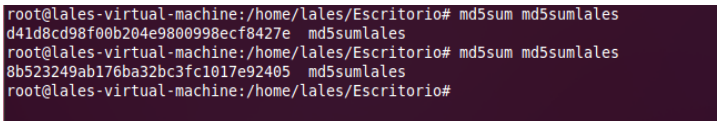


El resultado es una serie de números que es el certificado de ese archivo

A continuación vamos a abrir el archivo y vamos a ponerle unas líneas

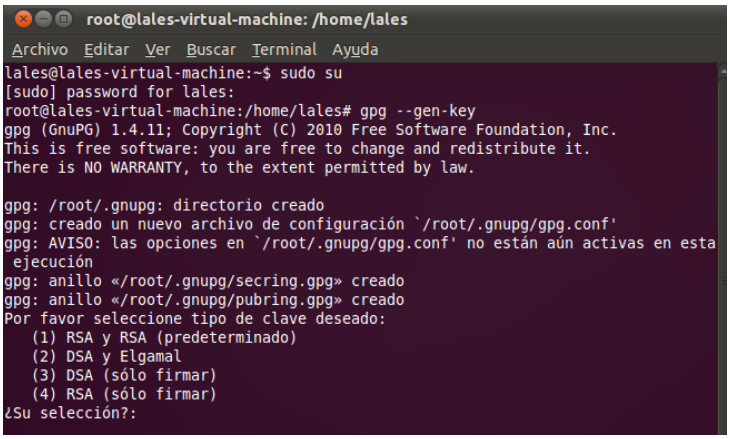


Si ahora volvemos a hacer lo mismo que antes, con el comando, vemos que la serie de números es diferente, ya que hemos añadido información al archivo

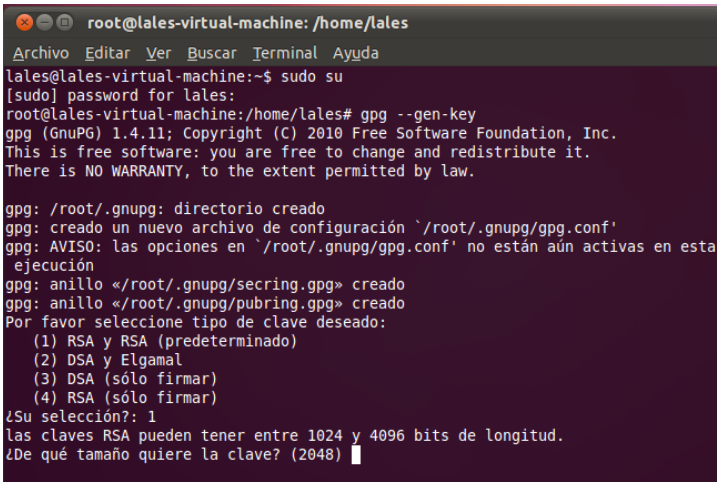


d) Cifrado asimétrico: En GNU/Linux: gpg.

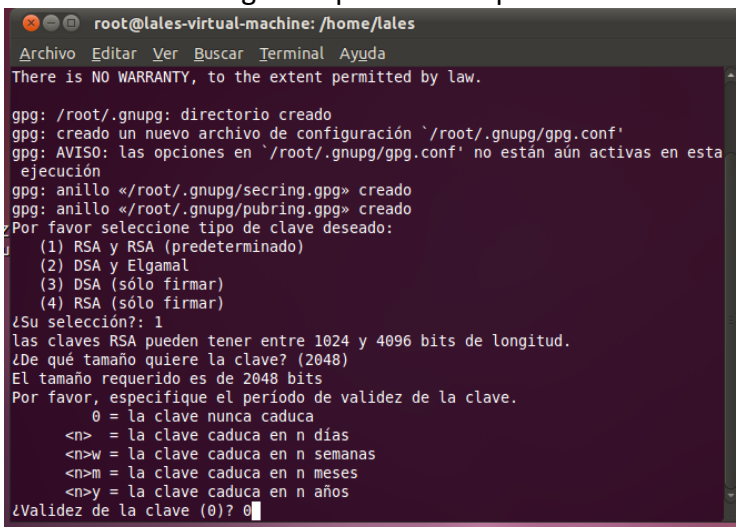
Vamos a ir a un terminal en Linux y vamos a poner el siguiente comando:
Gpg - -gen-key
Nos pide a continuación que elijamos una opción, le damos a 1 para encriptar



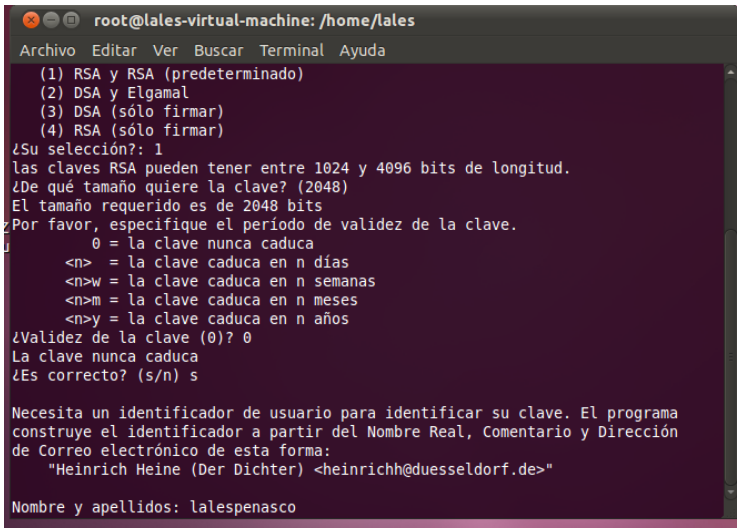
Ahora elegimos el tamaño, dejamos lo que viene por defecto que son 2048 bits



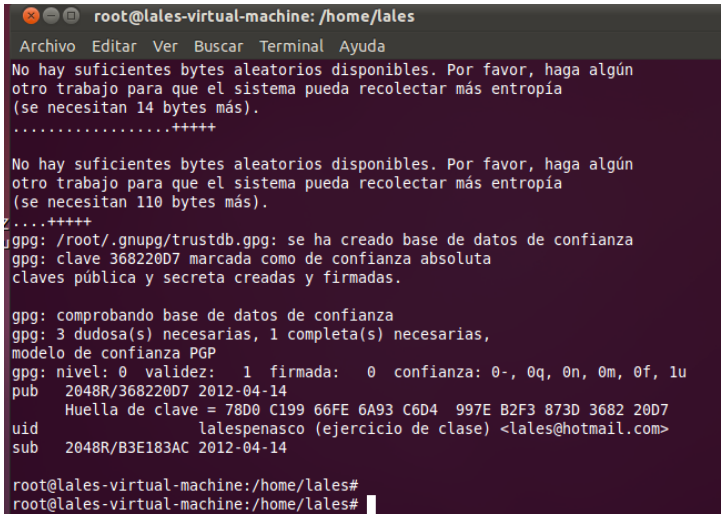
Ahora elegimos que no caduque nunca



Y vamos rellenando nombre y apellidos y dirección y nos pide también una contraseña, pongo invesinves



Aquí nos pone ya que nos ha dado la clave privada y pública y se ha cifrado correctamente



Ahora podemos ver las claves que tenemos poniendo el comando:
Gpg - - list-keys