

ACTIVIDAD 3 – TÉCNICAS DE CIFRADO – TEMA 2 –SAD

a) Cifrado simétrico: Uso de PGP y GPG.

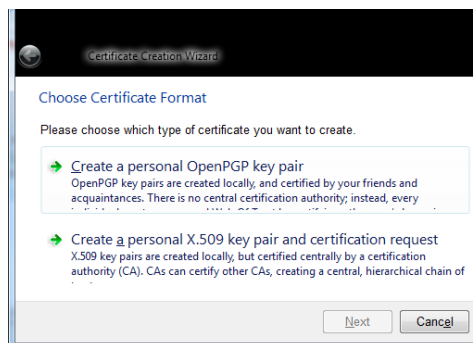
Instalamos GPG en Windows



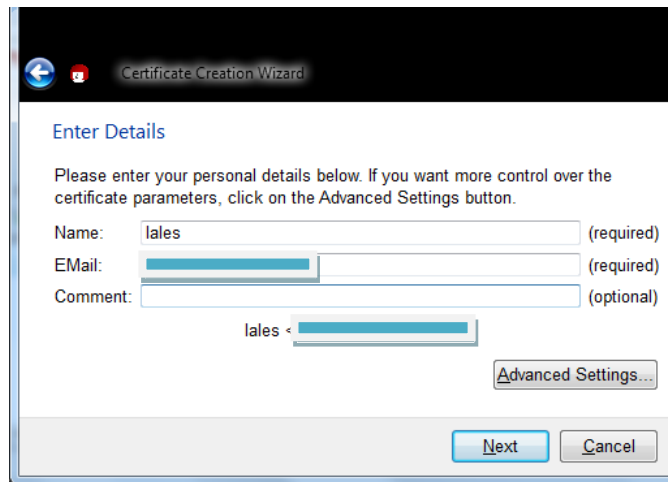
Esta página la dejamos por defecto



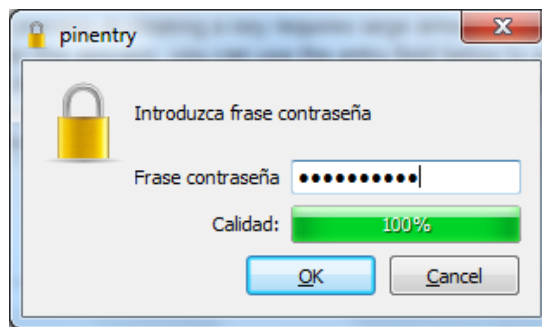
Elegimos crear un nuevo certificado



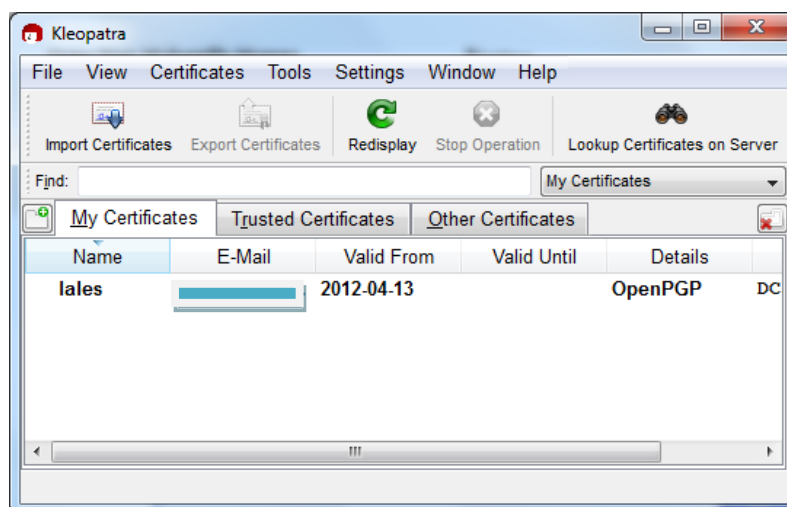
Ahora ponemos nuestros datos



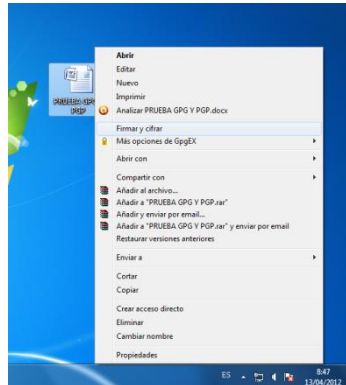
Nos pide que creamos una contraseña



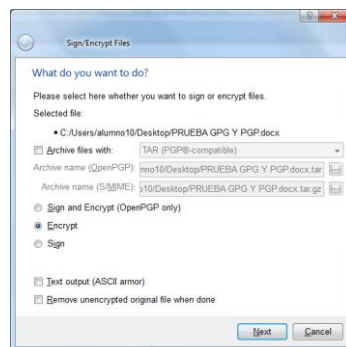
Y aquí vemos como se ha creado el certificado



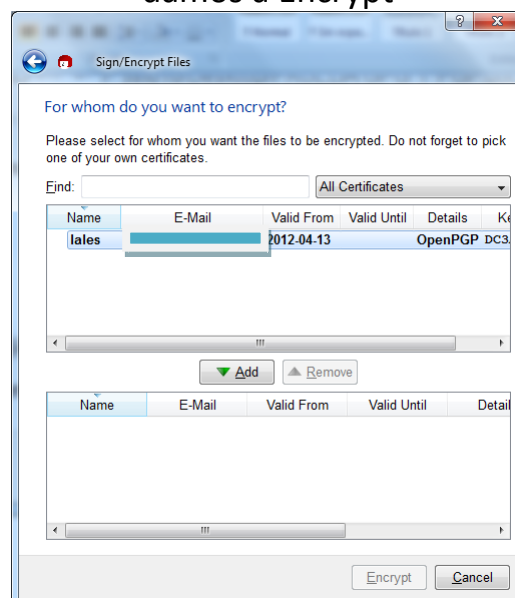
Ahora vamos a crear un documento en el escritorio y le damos con el botón derecho a firmar y cifrar



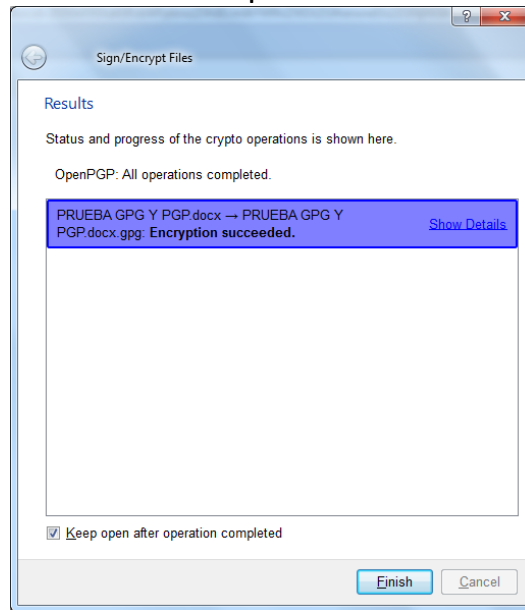
Le damos a Next y continuamos



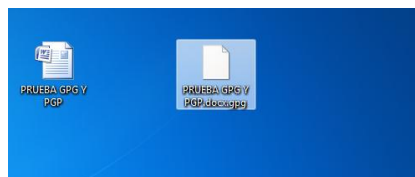
Le damos a añadir y nos lo añade al certificado que hemos creado y le damos a Encrypt



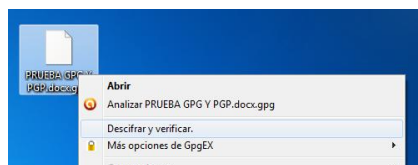
Ya tenemos Encriptado el documento



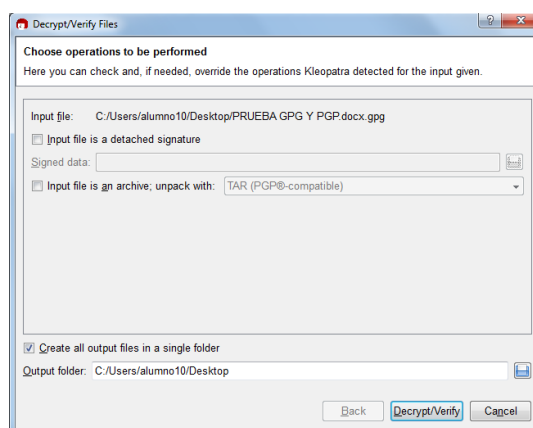
Aquí lo vemos encriptado



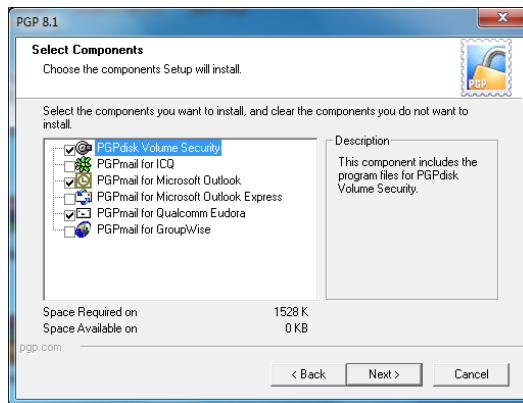
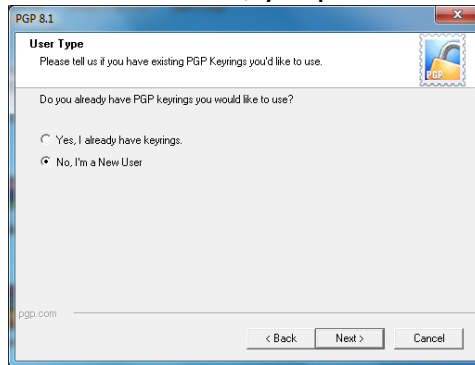
Ahora vamos a descifrarlo, le damos a botón derecho descifrar y verificar



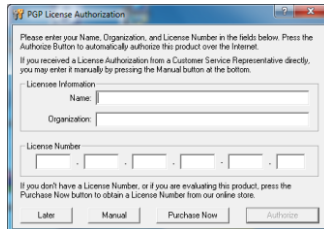
Le damos a Decrypt/Verify en esta ventana



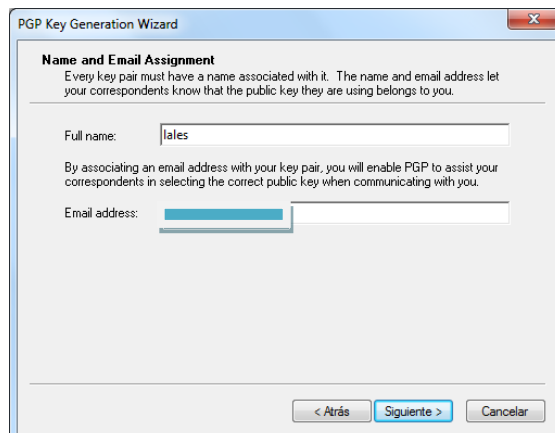
Aquí le damos a No, ya que eres nuevo



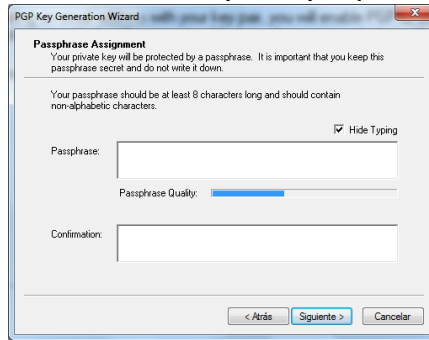
Aquí le damos a Later



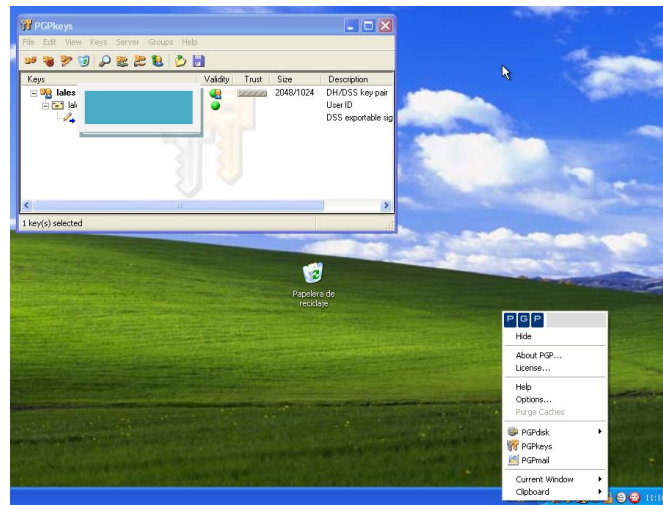
Y aquí ponemos nuestros datos



Aquí ponemos una frase, yo voy a poner invesinves



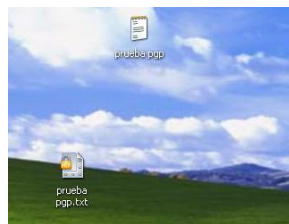
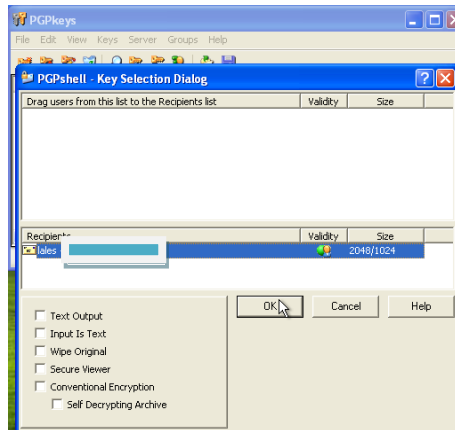
Ya tenemos instalado PGP



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

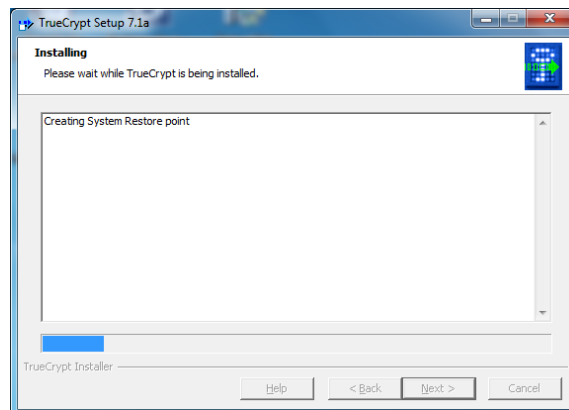


Y ya lo tenemos descifrado

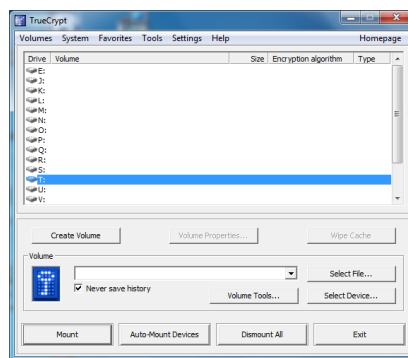


b) Cifrado de datos y particiones: En Windows: Uso de TrueCrypt.

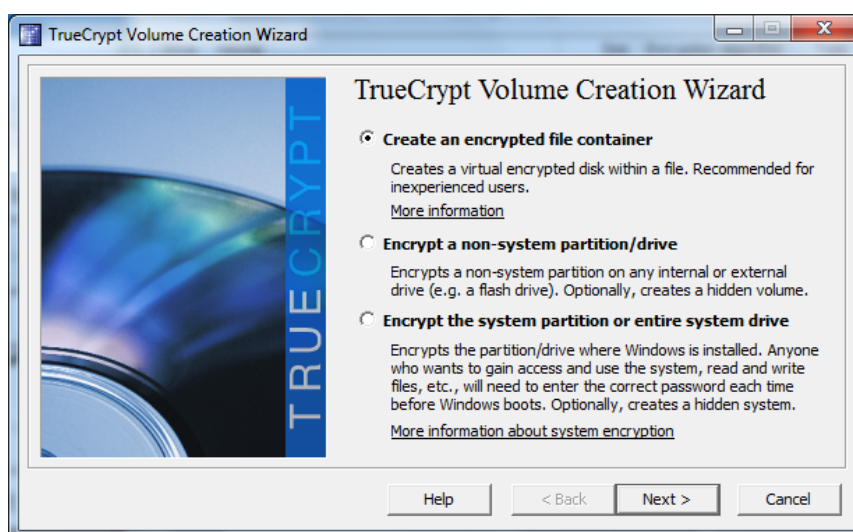
Vamos a descargar TrueCrypt



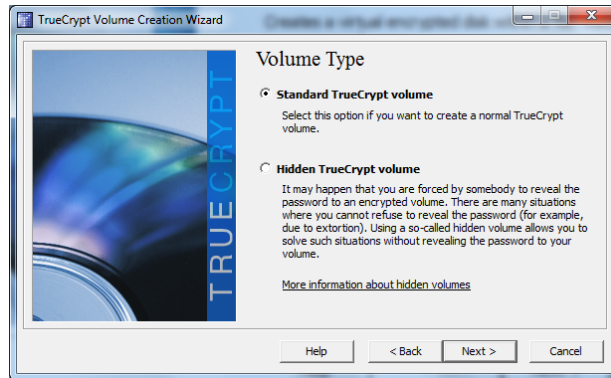
Una vez hecho esto vamos a elegir una unidad



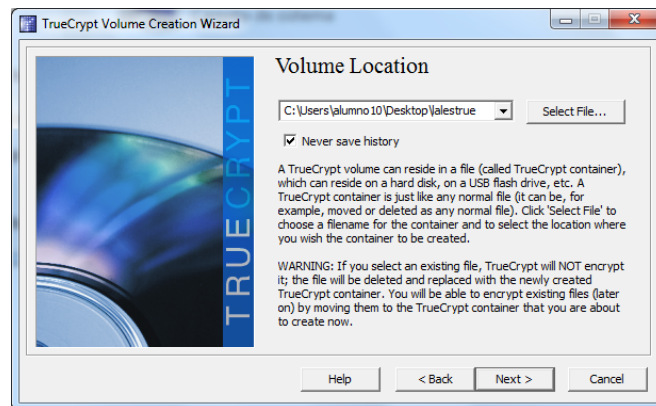
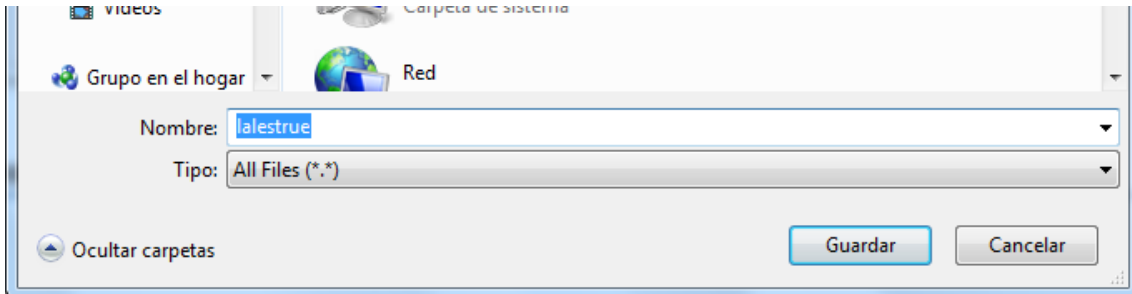
Elegimos la opción que viene por defecto



Y esta opción la dejamos igual



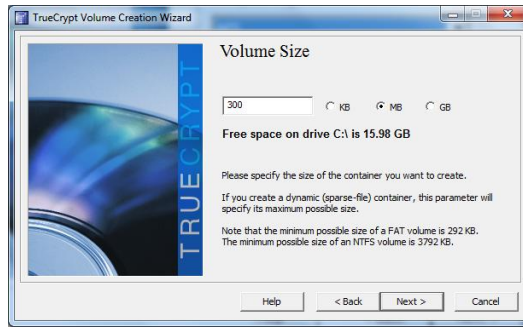
Elegimos el sitio donde lo vamos a guardar y un nombre, lalestrue



Dejamos la siguiente por defecto



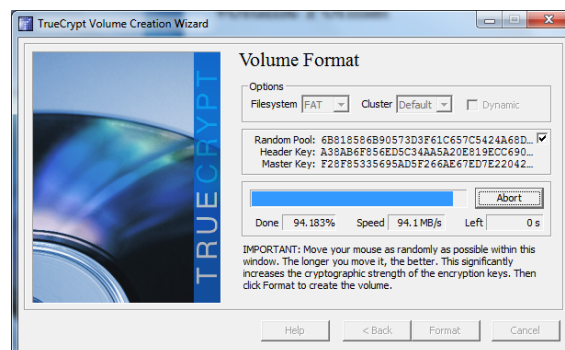
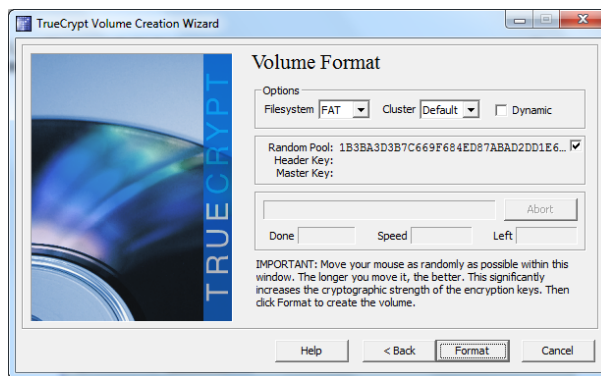
En el volumen elegimos 300 MB



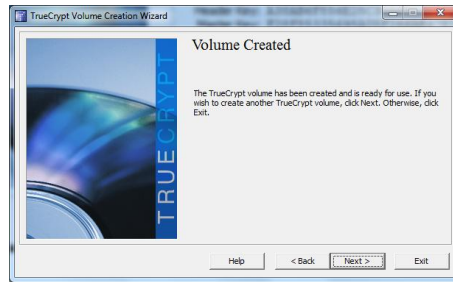
Y ahora ponemos la contraseña que queremos tener para el volumen



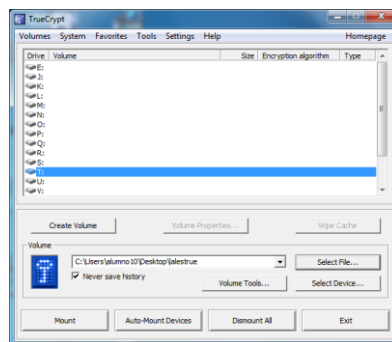
Le damos a Format y formatea el volumen



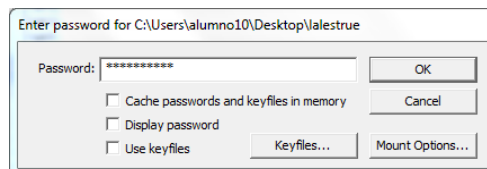
Ya hemos creado el volumen



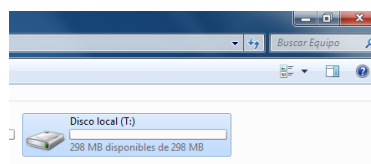
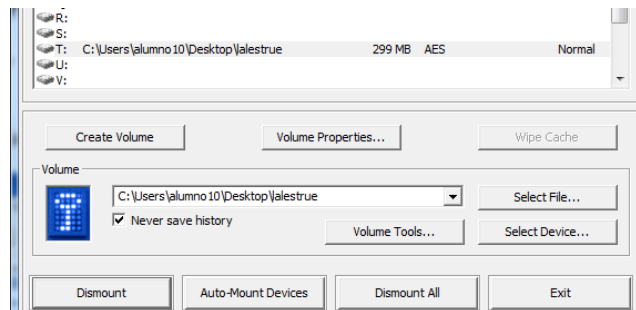
Ahora vamos a abrirlo, elegimos donde lo guardamos, en mi caso en el escritorio



Y ponemos la contraseña que pusimos



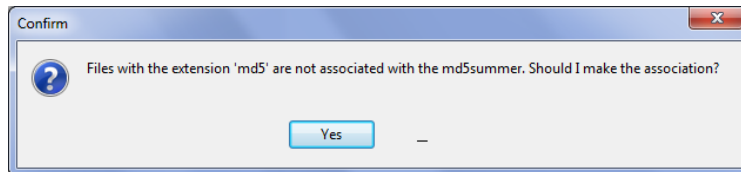
Ya lo tenemos montado, vamos a comprobarlo



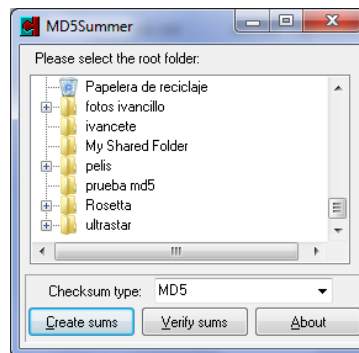
c) Funciones HASH: En Windows: md5sum. En GNU/Linux: md5sum.

En Windows: md5sum

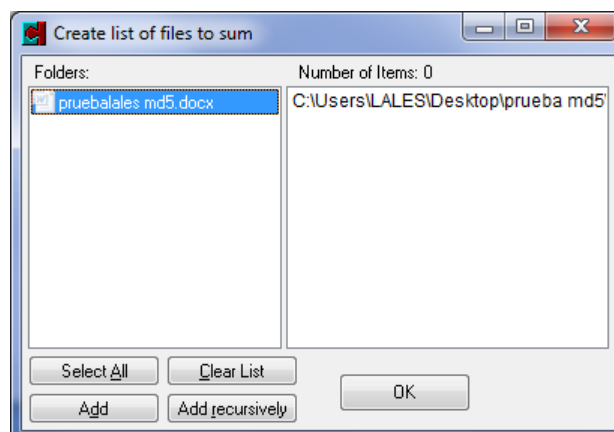
Nos descargamos el programa md5summer y es un ejecutable, le damos a yes y empieza el programa



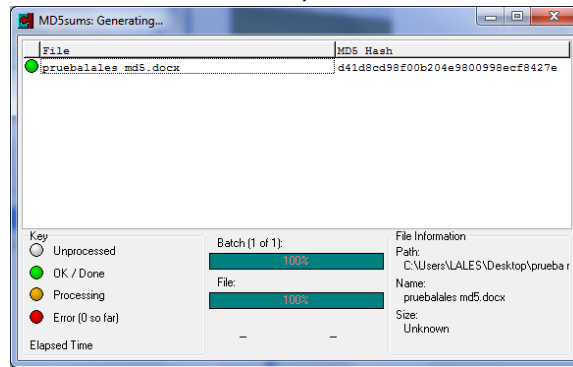
Ahora vamos a elegir una carpeta que hemos creado con el nombre prueba md5 y le damos a Create sums



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



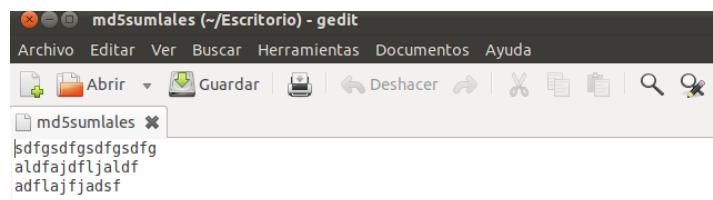
En Linux: md5sum

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

```
root@lales-virtual-machine: /home/lales/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
lales@lales-virtual-machine:~$ sudo su
[sudo] password for lales:
root@lales-virtual-machine:/home/lales# md5sum md5sumlales
md5sum: md5sumlales: No existe el fichero o el directorio
root@lales-virtual-machine:/home/lales# cd Escritorio
root@lales-virtual-machine:/home/lales/Escritorio# ls
FileZilla3 md5sumlales pruebaclam
FileZilla 3.5.3_i586-linux-gnu.tar.bz2 OpenDHCIP_para_Linux
lales ProFTP
root@lales-virtual-machine:/home/lales/Escritorio# md5sum md5sumlales
d41d8cd98f00b204e9800998ecf8427e md5sumlales
root@lales-virtual-machine:/home/lales/Escritorio#
```

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

```
root@lales-virtual-machine:/home/lales/Escritorio# md5sum md5sumlales
d41d8cd98f00b204e9800998ecf8427e md5sumlales
root@lales-virtual-machine:/home/lales/Escritorio# md5sum md5sumlales
8b523249ab176ba32bc3fc1017e92405 md5sumlales
root@lales-virtual-machine:/home/lales/Escritorio#
```

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

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
lales@lales-virtual-machine:~$ sudo su
[sudo] password for lales:
root@lales-virtual-machine:/home/lales# gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: /root/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración `root/.gnupg/gpg.conf'
gpg: AVISO: las opciones en `root/.gnupg/gpg.conf' no están aún activas en esta
ejecución
gpg: anillo «root/.gnupg/secring.gpg» creado
gpg: anillo «root/.gnupg/pubring.gpg» creado
Por favor seleccione tipo de clave deseado:
(1) RSA y RSA (predeterminado)
(2) DSA y Elgamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
¿Su selección?:
```

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

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
lales@lales-virtual-machine:~$ sudo su
[sudo] password for lales:
root@lales-virtual-machine:/home/lales# gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: /root/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración `root/.gnupg/gpg.conf'
gpg: AVISO: las opciones en `root/.gnupg/gpg.conf' no están aún activas en esta
ejecución
gpg: anillo «root/.gnupg/secring.gpg» creado
gpg: anillo «root/.gnupg/pubring.gpg» creado
Por favor seleccione tipo de clave deseado:
(1) RSA y RSA (predeterminado)
(2) DSA y Elgamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
¿Su selección?: 1
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048) █
```

Ahora elegimos que no caduque nunca

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
There is NO WARRANTY, to the extent permitted by law.

gpg: /root/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración '/root/.gnupg/gpg.conf'
gpg: AVISO: las opciones en '/root/.gnupg/gpg.conf' no están aún activas en esta
ejecución
gpg: anillo «/root/.gnupg/secring.gpg» creado
gpg: anillo «/root/.gnupg/pubring.gpg» creado
¿Por favor seleccione tipo de clave deseado:
(1) RSA y RSA (predeterminado)
(2) DSA y Elgamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
¿Su selección?: 1
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
El tamaño requerido es de 2048 bits
Por favor, especifique el periodo de validez de la clave.
  0 = la clave nunca caduca
  <n> = la clave caduca en n días
  <n>w = la clave caduca en n semanas
  <n>m = la clave caduca en n meses
  <n>y = la clave caduca en n años
¿Validez de la clave (0)? 0
```

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

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
(1) RSA y RSA (predeterminado)
(2) DSA y Elgamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
¿Su selección?: 1
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
El tamaño requerido es de 2048 bits
Por favor, especifique el periodo de validez de la clave.
  0 = la clave nunca caduca
  <n> = la clave caduca en n días
  <n>w = la clave caduca en n semanas
  <n>m = la clave caduca en n meses
  <n>y = la clave caduca en n años
¿Validez de la clave (0)? 0
La clave nunca caduca
¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
Nombre y apellidos: lalespenasco
```

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
(2) DSA y Elgamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
¿Su selección?: 1
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
El tamaño requerido es de 2048 bits
Por favor, especifique el periodo de validez de la clave.
  0 = la clave nunca caduca
  <n> = la clave caduca en n días
  <n>w = la clave caduca en n semanas
  <n>m = la clave caduca en n meses
  <n>y = la clave caduca en n años
¿Validez de la clave (0)? 0
La clave nunca caduca
¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
Nombre y apellidos: lalespenasco
Dirección de correo electrónico: lales@hotmail.com
```



```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
0 = la clave nunca caduca
<n> = la clave caduca en n días
<n>w = la clave caduca en n semanas
<n>m = la clave caduca en n meses
<n>y = la clave caduca en n años
¿Validez de la clave (0)? 0
La clave nunca caduca
¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: lalespenasco
Dirección de correo electrónico: lales@hotmail.com
Comentario: ejercicio de clase
Ha seleccionado este ID de usuario:
«lalespenasco (ejercicio de clase) <lales@hotmail.com>»

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Necesita una frase contraseña para proteger su clave secreta.
Repita frase contraseña:
```

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

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
No hay suficientes bytes aleatorios disponibles. Por favor, haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 14 bytes más).
.....+++++

No hay suficientes bytes aleatorios disponibles. Por favor, haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 110 bytes más).
Z.....+++++
gpg: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 368220D7 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
pub 2048R/368220D7 2012-04-14
Huella de clave = 78D0 C199 06FE 6A93 C6D4 997E B2F3 873D 3682 20D7
uid lalespenasco (ejercicio de clase) <lales@hotmail.com>
sub 2048R/B3E183AC 2012-04-14

root@lales-virtual-machine: /home/lales#
root@lales-virtual-machine: /home/lales#
```

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

```
root@lales-virtual-machine: /home/lales#
root@lales-virtual-machine: /home/lales# gpg --list-keys
/root/.gnupg/pubring.gpg
-----
pub 2048R/368220D7 2012-04-14
uid lalespenasco (ejercicio de clase) <lales@hotmail.com>
sub 2048R/B3E183AC 2012-04-14
```

MARÍA ÁNGELES PEÑASCO SÁNCHEZ – ACTIVIDAD 3 – TEMA 2 - SAD