**A1 - Ocultación**



Daniel Escaño Hernández

# **1. Índice**

[**1. Índice**](#_9x9j6eds8olc) **2**

[**2. Encriptación**](#_n1rbsuh1kvz7) **3**

[2.1 Encriptado simétrico](#_fszwzgqam2po) 3

[Captura de la creación del fichero y encriptación:](#_rsji5ad5fkni) 3

[Captura del desencriptado:](#_xlrv4tpetyy9) 4

[2.2 Encriptado asimétrico](#_s47c6tsmvzmz) 4

[Captura de la consulta de las claves:](#_x2v4xwn3pjr8) 5

[Captura del directorio oculto (.gnugp):](#_i118eo3iadhh) 5

[Captura de la exportación de la clave pública:](#_fsgmj2me13s8) 6

[Captura de la encriptación asimétrica:](#_7frpus2f093a) 7

[**2. Firma**](#_h5cpoadae74n) **7**

[Captura de la creación de la firma:](#_gbat2bl6r5oi) 8

[Captura de la modificación de la firma y comprobación:](#_161vdyox4g36) 8

[**3. Esteganografía**](#_nn6z52pki6ca) **9**

[Captura del proceso de estenografía:](#_hr26e9oudtrb) 10

[Captura de la extracción del archivo oculto:](#_i0km0vhfbbku) 11

[**4. Partición encriptada**](#_4f1yuy67n4ym) **12**

[4.1 Teoría: contenedor encriptado](#_35h93jj30gx9) 12

[4.2 Proceso: partición encriptada](#_h2p5u28jy6df) 12

[Captura de la creacion y montado de la partición cifrada:](#_2wbbjdcl0j7g) 12

[Captura de la comprobación de montado:](#_pjcy63towvaw) 13

# **2. Encriptación**

## **2.1 Encriptado simétrico**

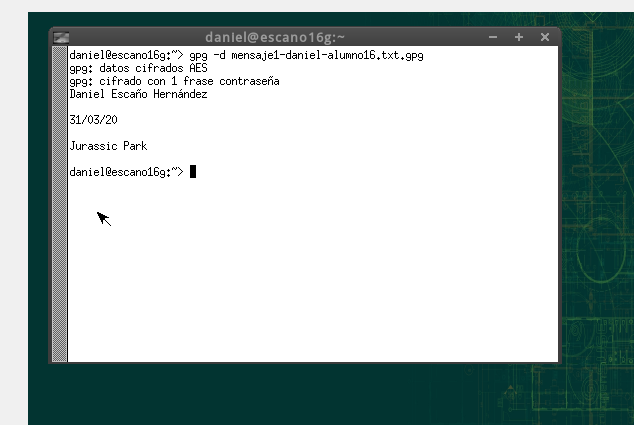
* Asegurarnos de tener instalado GPG (zypper info gpg2).
* Trabajaremos con nuestro usuario habitual. No usar root.
* Crear un fichero de texto /home/nombre-alumno/mensaje1-nombre-alumnoXX.txt.
  + Escribir dentro el nombre del alumno, la fecha de hoy y un título de una película.
* Hacer una encriptación simétrica con GPG.
  + gpg -c mensaje1-nombre-alumnoXX.txt

### Captura de la creación del fichero y encriptación:

## 

* Enviar fichero encriptado al compañero (alumno2) para que lo desencripte.
  + gpg -d mensaje1-nombre-alumnoXX.txt.gpg

### Captura del desencriptado:

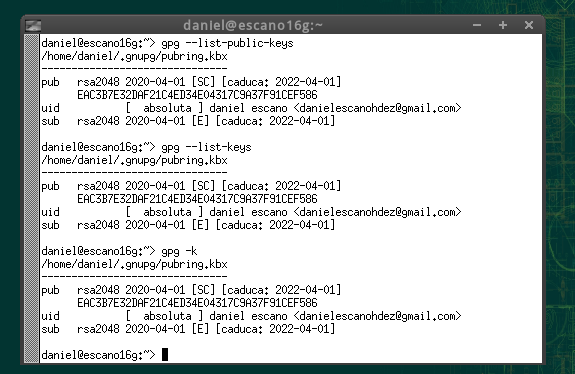


## **2.2 Encriptado asimétrico**

Alumno1(Nosotros):

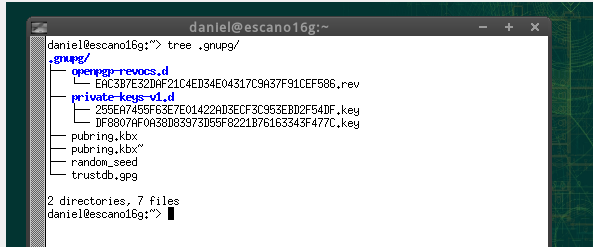
* Alumno1 genera un par de claves pública/privada.
  + gpg --gen-key, genera un par de claves pública/privada.
  + Consultar las claves públicas con alguno de los siguientes comandos gpg --list-public-keys, gpg --list-keys o gpg -k. La línea pub 2048R/IDNUMBER, muestra la información con el identificador de la clave pública.

### Captura de la consulta de las claves:



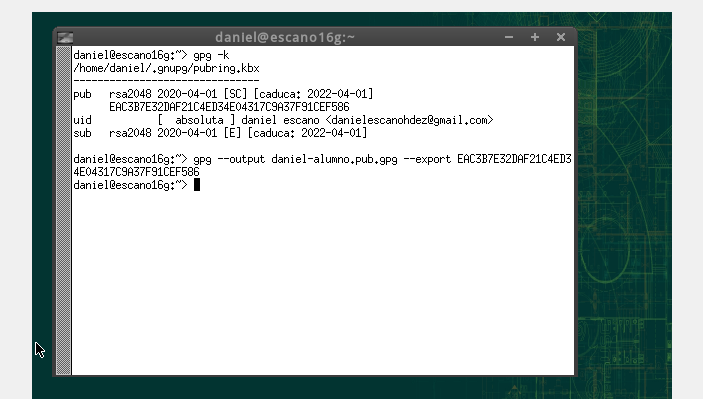
* + tree .gnupg, Comprobaremos que se crea un directorio oculto, dentro del home de nuestro usuario con el nombre .gnugp. Ahí es donde se guarda la información de claves de GPG para nuestro usuario.

### Captura del directorio oculto (.gnugp):



* Alumno1 exporta la clave pública para pasarla al compañero.
  + gpg --output nombre-alumnoXX.pub.gpg --export PUBLIC\_KEY\_IDNUMBER
  + El valor PUBLIC\_KEY\_IDNUMBER lo obtenemos al consultar la salida del comando anterior (gpg -k).

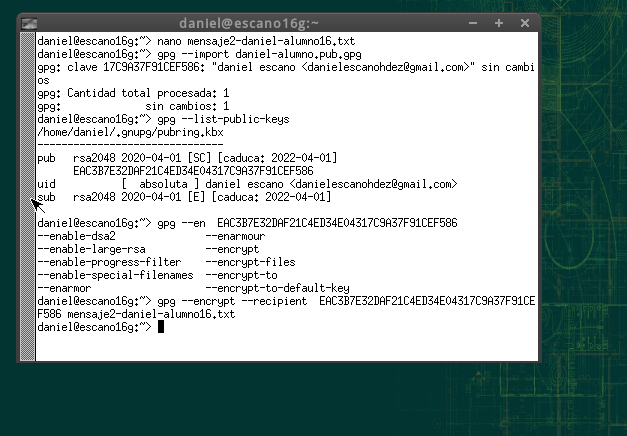
### Captura de la exportación de la clave pública:



Alumno2(Nuestro compañero):

* Alumno2 crea un fichero de texto /home/nombre-alumno/mensaje2-nombre-alumnoXX.txt.
  + Escribir dentro el nombre del alumno, la fecha de hoy y una frase/mensaje.
* Alumno2 importa la clave pública del compañero (alumno1).
  + gpg --import nombre-alumnoXX.pub.gpg
* Alumno2 hace una encriptación asimétrica con GPG con la clave pública recibida.
  + gpg --list-public-keys, para ver las claves públicas que tenemos.
  + gpg --encrypt --recipient PUBLIC\_KEY\_IDNUMBER mensaje2-nombre-alumnoXX.txt

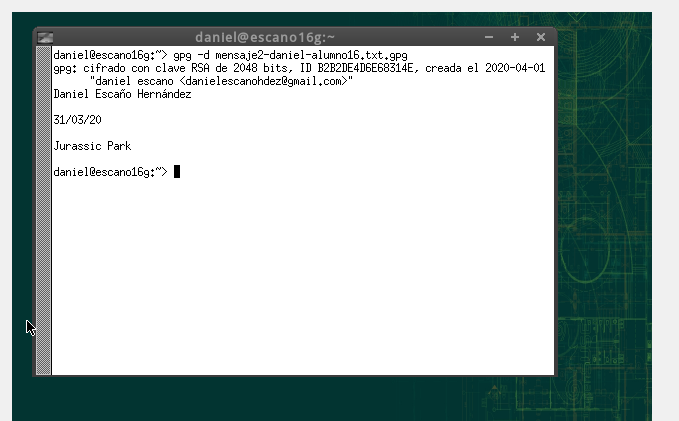
### Captura de la encriptación asimétrica:



* Alumno2 envía el fichero a alumno1 para que lo desencripte.

Alumno1(Nosotros):

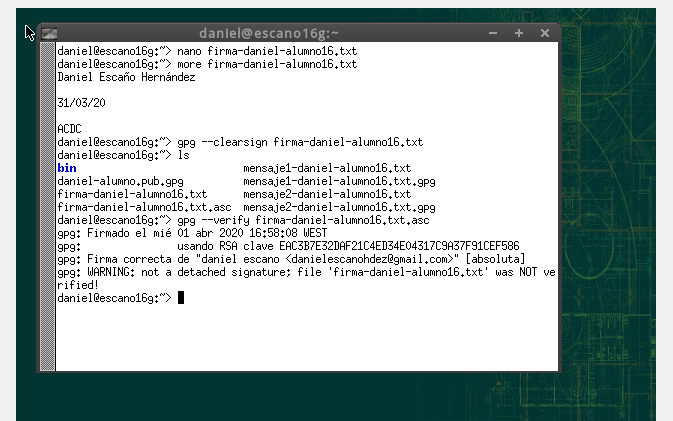
* Alumno1 desencripta el fichero gpg -d mensaje2-nombre-alumnoXX.txt.gpg.



# **2. Firma**

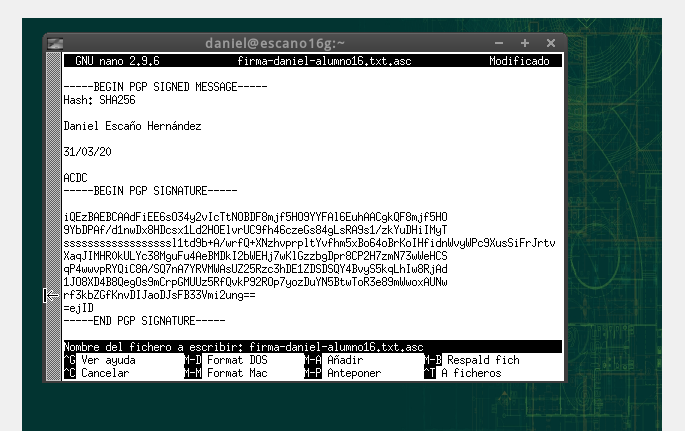
* Crear documento firma-nombre-alumnoXX.txt.
  + Escribir dentro el nombre del alumno, la fecha de hoy y un grupo de música.
* Vamos a firmar digitalmente el documento en modo ASCII.
  + gpg --clearsign firma-nombre-alumnoXX.txt
* Consultar el fichero que se ha generado con la firma firma-alumnoXX.txt.asc
* Comprobar que la firma es correcta.
  + gpg --verify firma-nombre-alumnoXX.txt.asc

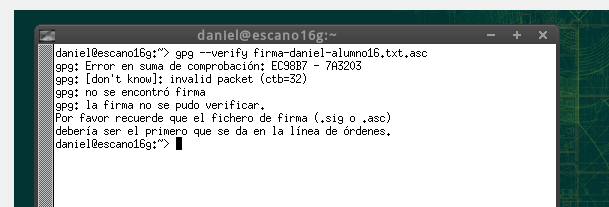
### Captura de la creación de la firma:



* Modificar el documento firma-nombre-alumnoXX.txt.asc.
* Comprobar que ahora el fichero tiene la firma incorrecta.

### Captura de la modificación de la firma y comprobación:

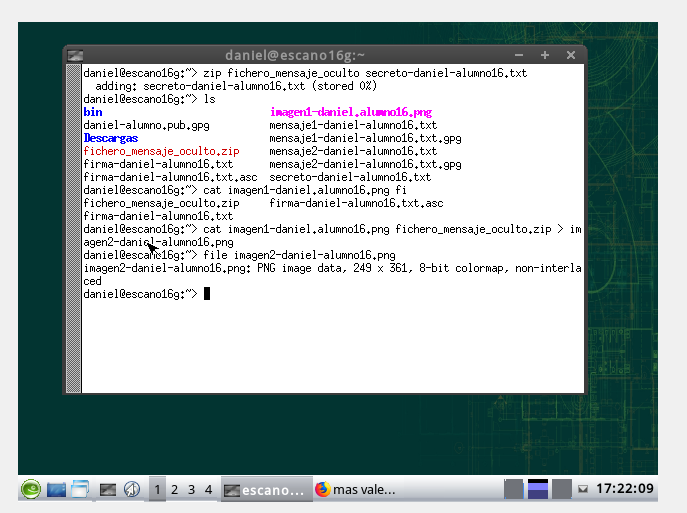


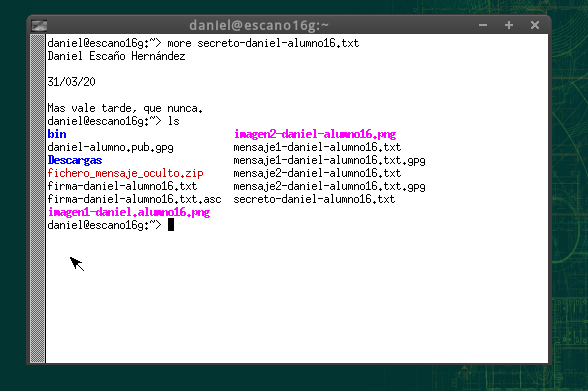


# **3. Esteganografía**

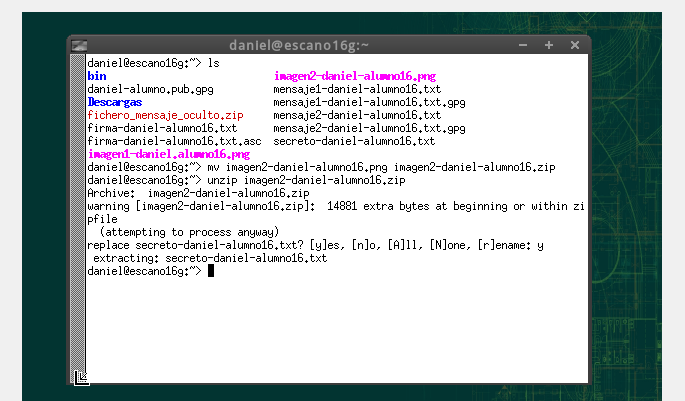
* Consultar enlace sobre estenografía de "Andar por casa (zip y cat)".
* Crear un fichero de texto con un mensaje oculto (secreto-nombre-alumnoXX.txt).
  + Escribir dentro el nombre del alumno, la fecha de hoy y un refrán o frase famosa.
* Crear un fichero zip con el mensaje oculto.
* Descargar una imagen1-nombre-alumnoXX.png que nos guste.
* Incrustar el fichero zip dentro de la imagen1-nombre-alumnoXX.png, obteniendo un fichero imagen2-nombre-alumnoXX.png.
* Pasar el fichero imagen2-nombre-alumnoXX.png al compañero.
* Verificar el formato de las imágenes, bien usando el comando file o capturando vista de la misma.
* El compañero debe aplicar el proceso necesario para extraer el mensaje oculto dentro de la imagen2-nombre-alumnoXX.png.

### Captura del proceso de estenografía:





### Captura de la extracción del archivo oculto:



# **4. Partición encriptada**

## **4.1 Teoría: contenedor encriptado**

Es posible crear un fichero encriptado, que a su vez puede contener directorios y ficheros manteniendo los datos de forma confidencial. La ventaja de usar un contenedor encriptado sobre encriptar particiones es que se pueden añadir sin tener que reparticionar el disco. Se montan en un dispositivo Loop y se comportan como si fueran particiones normales.

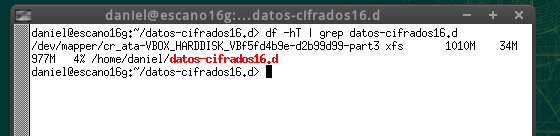
## **4.2 Proceso: partición encriptada**

* Por seguridad, vamos a hacer una instantánea de la MV antes de empezar con este apartado.
* Crear directorio /home/nombre-alumno/datos-cifradosXX.d.
* Ir a Yast -> Particionador. Crear una partición encriptada.
* Montar partición encriptada en la carpeta anterior.
* Reiniciar la MV para que active los cambios que hemos realizado.
* Escribir el password del contenedor para poder activarlo.

### Captura de la creacion y montado de la partición cifrada:

* df -hT | grep datos-cifradosXX.d, comprobamos que hay un dispositivo montado.
* Poner archivos dentro del contenedor.

### Captura de la comprobación de montado:



* Reiniciar la MV.
* Comprobar a acceder a los ficheros del contenedor cuando se pone la contraseña correcta y cuando no.

Al no introducir correctamente la contraseña de la partición cifrada al iniciar el sistema operativo, no nos aparecen los archivos ni nos permite abrirlos por consecuente.