GnuPG Gnu Privacy Guard

Curso de privacidad y protección de las comunicaciones.

Para utilizar GnuPG de forma gráfica y no tener que estar escribiendo los comandos podemos encontrar para KDE el programa **KGPG** y para Gnome el programa **SeaHorse**.

Hay algunos clientes de correo que también soportan GnuPG como **Evolution** o Mozilla Thunderbird al que hay que ponerle el plugin Enigmail para que tenga soporte de GnuPG.

Cifrar y descifrar en ubuntu

Otras opciones para Windows:

7zip	cifrado simétrico, compresión
Bitlocker	cifrado de volúmenes
gpg4win	cifrado asimétrico y generación de certificados
VeraCrypt	cifrado simétrico, cifrado de volúmenes y del sistema operativo.

RESUMEN DE COMANDOS

man gpg	Ayuda
gpg –h	Muestra ayuda
gpg --gen-key	Generar par de llaves pública y privada
gpg --list-key	Lista las llaves del anillo de llaves
gpg --delete-key id_usuario	Borra una llave pública del anillo de llaves
gpg -a --export [id_usuario] > llave_pub	Extrae la llave pública para exportarla en formato ascii
gpg --export [id_usuario] **>** llave_pub	Extrae la llave pública para exportarla
gpg --import llave_pub	Incluye una llave pública al anillo de llaves
gpg -r id_usuario **--encrypt** mensaje **(salida gpg)** **gpg -a -r** id_usuario **--encrypt** mensaje **(salida asc)**	Encriptar un mensaje
gpg --decrypt mensaje_enc **>** mensaje_claro	Desencriptar un mensaje
gpg -s mensaje_enc **(salida gpg)** **gpg -a -s** mensaje_enc **(salida asc)**	Firmando un mensaje
gpg --verify mensaje_firmado	Verifica la firma de un mensaje
gpg --decrypt mensaje_firmado **|** **gpg --decrypt**	Desencriptar un mensaje encriptado y firmado
gpg -u id_remitente **-r** id_destinatario **-sea** mensaje_para_destinatario	Encriptar y firmar un mensaje
gpg mensaje_para_destinatario**.asc**	Desencriptar y validar un mensaje firmado
gpg --edit-key id-usuario **(check=verificar firmas de la llave pub)** **(sign=firmar la llave pub)**	Editar llave pública
gpg --sign-key id-usuario **gpg --list-sigs** [id-usuario]	Firmar una llave pública Lista las llaves públicas del anillo de llaves y sus firmas

CIFRADO SIMÉTRICO

gpg –c *nombrededocumento*	Genera un *nombrededocumento.**gpg*** cifrado con una clave que nos pide. Comentar elección correcta de la clave. **–o** para controlar la salida
gpg –c -a *nombrededocumento*	*nombrededocumento.**asc*** cifrado en ascii
gpg --symmetric *nombrededocumento*	Genera un *nombrededocumento.**gnu*** cifrado con una clave que nos pide. Comentar elección correcta de la clave.
gpg –d *nombrededocumento.gpg*	Para descifrar el documento

¿podemos cifrar un directorio?

ENTROPIA

Solución del problema de producción de entropía para la generación del certificado

fuente - *Ayudar al generador de números aleatorios a generar suficiente entropía.*

Instalación del paquete:

apt-get install rng-tools *(**r n g** - tools)*

Modificación del fichero de configuración: ***/etc/default/rng-tools*** *(**r n g** - tools)*

HRNGDEVICE = /dev/urandom

Lanzamos el servicio ing-tools:

/etc/init.d/rng-tools start

Generamos la clave:

gpg --gen-key

CIFRADO ASIMÉTRICO

GENERACIÓN DE CLAVES

gpg --gen-key	crea un par de claves

DSA y El Gamal

DSA

RSA

Tamaño

Periodo de validez

Datos personales

Password de protección

sec	**secret key**	**pub**	**public key**
ssb	**secret subkey**	**sub**	**public subkey**

LISTADO DE CLAVES

gpg -k	Muestra las claves públicas
gpg -K	Muestra las claves privadas
gpg --list-keys nuestro@correo	lista nuestra/s clave/s
gpg --list-secret-keys	lista nuestra/s clave/s privadas
gpg --fingerprint nro_clave	muestra "finger print" nuestra huella digital)

¿Dónde se guardan las claves? **/root/.gnupg/**

/home/alumno/.gnupg/

pubring.gpg

secring.gpg

Anillo de claves privadas – anillo de claves públicas.

Usuarios – claves de usuario

REVOCACIÓN DE CLAVES

gpg --output FicheroRevocacion **--gen-revoke** id-clave	Revocar clave, por ejemplo si ha sido robada Genera el certificado de revocación que publicaremos cuando sea necesario. Se recomienda hacerlo al crear la clave.
gpg – import FicheroRevocacion	Para revocar la clave… ya no podremos cifrar ni firmar con esta clave

BORRADO DE CLAVES

gpg --delete-secret-key id-clave	Borra la clave privada
gpg --delete-key id-clave	Borra la clave pública

INTERCAMBIO DE CLAVES

gpg --export [identificador de usuario]	exportar una clave pública **-- output** nombrefichero.gpg
gpg --import [archivo]	importa una clave
gpg --keyserver keyserver.ubuntu.com **--send-keys** nro_clave	sube nuestra key a un servidor público, por ejemplo el de Ubuntu
gpg --armor --output	Exportar la clave pública

fichoeDeSalida **--export** ClaveID	
gpg --armor --output fichoeDeSalida **--export-secret-key** ClaveID	Exportar la clave privada

FIRMA

gpg --clearsign documento	Firma al final del documento
gpg -s documento	Firma y genera un fichero comprimido **-o** nombreficherosalida
gpg -b documento	La firma aparece en un fichero separado
gpg -a documento	Para abrir un fichero cifrado con –s
gpg --verify fichero	Para verificar ficheros firmados

CIFRAR Y DESCIFRAR

gpg -e nombre_archivo	Cifrar
gpg --encrypt nombre_archivo	Cifrar
gpg -d nombre_archivo	Descifrar
gpg --decrypt nombre_archivo	Descifrar
gpg --armor --recipient ClaveID **--encrypt** nombre_archivo	Cifrar un fichero

EJERCICIO

1. Cifrado **simétrico** – descifrar el fichero cifrado – estudiar distintos tipos de cifrado simétrico.

2. Generar un **certificado**.

    a. Opciones de generación.

    b. Donde se guarda.

    c. Como podemos ver los certificados almacenados: anillo de claves privadas, anillo de claves públicas.

    d. Revocación de certificado.

    e. Borrado de certificado.

3. Cifrado **asimétrico** – descifrar el fichero cifrado – estudiar distintos tipos de cifrado asimétrico.

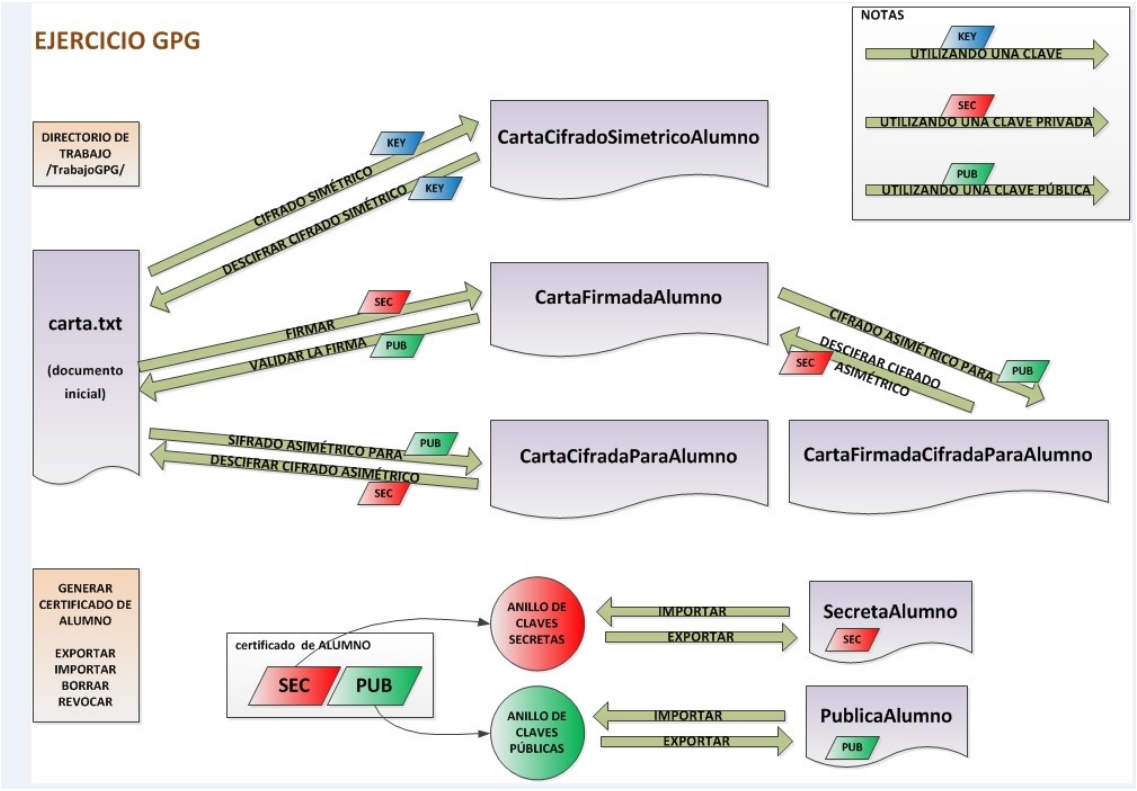
4. **Firma** de un documento – comprobar la firma de un documento – estudiar distintos tipos de firma – Comprobar la firma cuando el documento ha sido modificado.

5. **Firmar y cifrar** – descifrar y comprobar la firma.

6. (**Equipos distintos**) **Exportar e importar** un certificado – descifrar y comprobar la firma del documento de un compañero.

7. (**Usuarios distintos** de root) Jefe1 y Jefe2 utilizan sus certificados en la misma máquina para intercambiarse documentos firmados y cifrados.

8. Utilizar los certificados creados en el **correo electrónico** entre Jefe1 y Jefe2.


EJERCICIO GPG
NOTAS
KEY
UTILIZANDO UNA CLAVE
SEC
UTILIZANDO UNA CLAVE PRIVADA
PUB
UTILIZANDO UNA CLAVE PÚBLICA
DIRECTORIO DE TRABAJO /TrabajoGPG/
CartaCifradoSimetricoAlumno
CIFRADO SIMÉTRICO
DESCIFRAR CIFRADO SIMÉTRICO
carta.txt
(documento inicial)
CartaFirmadaAlumno
FIRMAR
VALIDAR LA FIRMA
CIFRADO ASIMÉTRICO PARA
DESCIFRAR CIFRADO ASIMÉTRICO
SIFRADO ASIMÉTRICO PARA
DESCIFRAR CIFRADO ASIMÉTRICO
CartaCifradaParaAlumno
CartaFirmadaCifradaParaAlumno
GENERAR CERTIFICADO DE ALUMNO
EXPORTAR
IMPORTAR
BORRAR
REVOCAR
certificado de ALUMNO
SEC
PUB
ANILLO DE CLAVES SECRETAS
ANILLO DE CLAVES PÚBLICAS
IMPORTAR
EXPORTAR
SecretaAlumno
PublicaAlumno