Enunciado de la Práctica - Uso del GPG

1. Material.

Para la realización de esta práctica, los alumnos deberán de contar con un ordenador con distribución libre de S.O. (p.ej.: Ubuntu, Guadalinex o similares), así como tener instalado el paquete GPG. Asismismo, puede consultarse la ayuda disponible en el sistema del GPG con el comando man, y la búsqueda en Internet sobre sus opciones más extendidas.

2. Trabajo previo.

Para la correcta realización de la presente práctica, es recomendable que los alumnos visiten y lean la documentación ofrecida en los siguientes enlaces:

http://www.tribulinux.com/guia-rapida-gpg-crear-borrar-importar-y-exportar-claves.html

http://www.slideshare.net/berrueta/gnupg-criptografa-para-todos

http://www.slideshare.net/ulisesiet/cifrar-archivos-y-directorios-en-gnulinux

3. Trabajo práctico.

Desde la línea de comandos, invoca el comando gpg junto a sus parámetros necesarios para llevar a cabo las siguientes opciones (puede consultarse la ayuda disponible en el sistema del GPG con el comando man, y la búsqueda en Internet sobre sus opciones más extendidas). Se aconseja seguir el orden de las opciones establecido para una correcta realización de todos los puntos:

a. Opción para cifrar de formar simétrica un fichero (incluir tanto la forma del comando que permite la salida en binario como en ascii).
b. Opción para generar nuestro par de claves pública/privada.
c. Opción para exportar nuestra clave pública (para ser transmitida a un compañero, que podrá enviarnos información cifrada con nuestra clave pública).
d. Opción para importar la clave pública de un compañero.
e. Opción para verificar el estado de nuestro anillo de confianza de claves (para comprobar tanto los pares de clave pública/privada que hemos generado, como que las importaciones de claves a nuestro sistema se han realizado correctamente).
f. Opción para cifrar un fichero con la clave pública de un compañero (se asume que ya debe tenerse importada la clave pública del compañero en nuestro sistema).
g. Opción para descifrar con nuestra clave privada, la información cifrada con nuestra clave pública, que nos envía un compañero.
h. Opción para firmar un documento con nuestra clave privada y generar como resultado un fichero que contiene el documento original sin cifrar junto con la firma digital obtenida.
i. Opción para comprobar la veracidad de la firma digital del fichero firmado (incluir comprobación que muestre tanto que la firma digital es correcta como que no lo es, tras la

manipulación del fichero correspondiente).

4. Resultados/entregables.

Los alumnos deberán entregar un documento que incluya la descripción de cómo han realizado la práctica incluyendo algunas capturas significativas del proceso, que demuestren que se ha llevado a cabo. Dicho documento debe presentarse en formato PDF.

- Autores de esta práctica:

Manuel Rodríguez Jiménez

Lidia García Pérez

MAES curso 2012/2013

Aprendizaje y enseñanza de las materias de Informática

Profesor: Jorge Juan Chico