GnuPG: cifrando y firmando

Curso 2017-2018

1 Introducción

En esta práctica vamos a utilizar *GnuPG* para realizar cifrado y firmado de documentos. Además nos familiarizaremos con el manejo de claves asimétricas, lo que se conoce como infraestructura de clave pública o PKI. La herramienta GnuPG implementa el OpenPGP, que proviene a su vez del famoso y conflictivo software desarrollado por Phill Zimmerman.

Toda la información necesaria la puedes encontrar en la *Guía de GnuPG*. Como repositorio de claves puedes utilizar el *Servidor de claves de RedIris*

Como resultado de esta práctica debes generar un informe, para ello ponte de acuerdo con un compañero tuyo para realizarlo conjuntamente. No es necesario que entreguéis este informe, pero sí os resultará útil el día del examen.

2 Cifrar y descifrar un fichero mediante clave simétrica

Se trata de cifrar un fichero mediante clave simétrica y enviarlo a un compañero para que lo descifre.

3 Generar una pareja de claves asimétricas con su certificado de revocación.

Debes generar una pareja de claves pública-privada, exportarlas para que tu compañero las pueda importar. Por el momento no vamos a utilizar un servidor de claves, por lo que lo haremos mediante transferencia de ficheros. Entiende bien porqué es importante generar el certificado de revocación en el momento de la creación de la claves.

4 Cifrar y descifrar un documento

Una vez compartidas las claves necesarias ya puedes cifrar con clave asimétrica un fichero y enviárselo a tu compañero para que lo descifre.

5 Firmar y verificar firmas

Ahora tu objetivo es firmar un documento para que tu compañero verifique que es tuyo. Existen diversas forma de hacerlo, ilústralas mediante ejemplos.

6 Gestión de claves

Tanto las claves privadas como las públicas incluyen una serie de componentes. Se trata de realizar las siguientes tareas:

1. Analizar las propiedades de las claves (Identificador, huella, tipo de algoritmo, fecha de creación, fecha de caducidad y fortaleza).
2. Ver la confianza de una clave
3. Mediante el comando *help* revisar las opciones que ofrece la edición de claves.
4. Activar y desactivar claves
5. Modificar la fecha de caducidad
6. Añadir identificadores a la clave
7. Añadir una fotografía
8. Cambiar la contraseña

Dado que el sistema de confianza en PGP es anárquico ahora se trata de descargarte una clave pública del un repositorio de claves, firmarla y volver a subirla, verificando que está firmada. Para ilustrar eso podéis plantear el siguiente caso. Tenemos 3 usuarios, Anacleta, Bonifacio y Juan Tenorio.

1. Juan firma el fichero *te_amo.txt* y se lo manda a Anacleta.
2. Anacleta verifica la firma de Juan, ya que se ha descargado la clave pública de un tal Juan Tenorio de un repositorio de claves. Pero no está muy segura de que ese sea su deseado Tenorio.
3. Anacleta le pide a Bonifacio que termine su labor de celestino, ya que fue él quien le presentó a Juan. Para ello Bonifacio debe descargar la clave de Juan - ya que él si sabe que es la suya- validarla y volver a subirla al repositorio.
4. Anacleta que confía en la clave de Bonifacio debe realizar los pasos necesarios para convencerse de la que carta de amor de Juan es realmente de su Juan.