Uso del GPG - Guía Docente

1. Entorno de la práctica:

El entorno de aplicación de la presente práctica correspondería a dar cobertura a los temas relacionados con la criptografía de la siguiente lista de módulos:

- "Seguridad informática", perteneciente al 2º curso del Ciclo Formativo de Grado Medio de Administración de Sistemas Microinformáticos y Redes.
- "Seguridad y alta disponibilidad", perteneciente al 2º curso del Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos y Redes.
- "Programación de Servicios y Procesos", perteneciente al 2º curso del Ciclo Formativo de Grado Superior de Desarrollo de Aplicaciones Multiplataforma.

Identificando los objetivos descritos en el BOJA núm. 142, 21 de Julio de 2011, a esta práctica le corresponderían los siguientes objetivos:

- Conocimiento de las principales aplicaciones criptográficas.
- Conocimiento de los principales protocolos criptográficos.
- Definición y aplicación de criptográfica de claves pública y privada.
- Uso y difusión de información encriptada.
- Transmisión de información de forma segura en canales de comunicación de uso público.

2. Objetivos de la práctica

Con la presente práctica se pretende reforzar y hacer más accesibles y prácticos los conceptos teóricos relacionados con la criptografía, el cifrado y el uso de técnicas de encriptado y desencriptado, así como su uso en certificados, firmas digitales y mecanismos de autenticación.

3. Contenidos detallados

En esta práctica, se van a tratar los aspectos relacionados con el cifrado simétrico y asímetrico, la generación de pares de claves pública/privada, y su empleo tanto para el cifrado como para su uso en certificados y firmas de documentos. Así, con ayuda del GPG, de forma detallada, se va a tratar de forma práctica aspectos de:

- Cifrado simétrico de documentos.
- Descifrado simétrico de documentos.
- Generación de claves pública/privada.
- Exportación y difusión de clave pública.
- Cifrado con clave pública de otro usuario.
- Descifrado con clave privada.
- Firma de documentos con clave privada.
- Comprobación de documento firmado, con clave pública de otro usuario.
- Etc..

4. Herramientas

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.

5. Evaluación

Para la evaluación de esta práctica se propone la realización del siguiente ejercicio:

- 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).

Para la evaluación de esta práctica se tendrán en cuenta los siguientes criterios:

- Nivel de corrección en los parámetros utilizados.
- Grado de completud del total de puntos incluidos realizados correctamente.
- Nivel de detalle de las respuestas dadas (se han incluido capturas significativas del proceso, necesarias para entender adecuadamente el proceso seguido, explicaciones relevantes, etc).
- Asimismo, se penalizará un uso incorrecto de los parámetros del GPG que no sean aplicables a los requerimientos del enunciado donde se apliquen, y también, el uso incorrecto de las reglas gramaticales y de ortografía.

6. Justificación

Creemos que es muy importante que los alumnos conozcan las herramientas de cifrado, autenticación y firma digital que nos suministra el software libre, por una parte, para difundir el uso de estas herramientas de software libre y por otra, para concienciarlos de la importancia de utilizar los mecanismos adecuados para transmitir y recibir información cifrada en los medios actuales de comunicación no seguros, inculcarles un espíritu crítico frente a las decisiones de elección de los algoritmos criptográficos y claves seleccionados, preocupación por la necesaria labor de investigación y aprendizaje continuos para estar al tanto de las novedades en el campo de la seguridad informática, y por supuesto, implicarlos en una tarea de trabajo cooperativo con sus compañeros (ya que la práctica propuesta implica la colaboración entre varios compañeros para llevarla a cabo correctamente, a través de la investigación, búsqueda, participación y aportaciones de todos los integrantes del grupo que realiza la práctica).

Asimismo, creemos que esta práctica influirá positivamente en la repercusión que tiene su actitud en la vida cotidiana frente al uso de las múltiples tecnologías que tenemos a nuestra disposición, donde interviene la seguridad y se aplican técnicas criptográficas (por ejemplo, uso de las tarjetas bancarias, uso del dni electrónico tanto para autenticarnos en procesos de consulta de información confidencial como de firma digital para dar nuestro consentimiento en acciones primordiales como operaciones bancarias, envío de información crítica frente a entidades de la administración usando certificados digitales, etc).

- 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