

1. PGP (Pretty Good Privacy)

PGP (Pretty Good Privacy) fue uno de los primeros sistemas de encriptación de clave pública que fueron lanzados al mercado (Junio de 1991). Esta aplicación es un sistema de encriptación híbrido que utiliza RSA como algoritmo de encriptación de clave pública para el tratamiento de claves e IDEA como algoritmo de cifrado simétrico para el tratamiento del texto. Esta primera parte de la práctica consiste en la instalación y utilización de los comandos básicos de PGP.

1.1. Obtención e Instalación de PGP

La instalación de la aplicación PGP podrá realizarse en cualquier plataforma linux disponible, recomendándose las que hay instaladas en los laboratorios docentes. En caso de utilizar alguna distribución no presente en los laboratorios, los alumnos deberán proporcionar la infraestructura para realizar las pruebas. A través de la página web de la asignatura se proporciona PGP para la distribución Debian y su instalación se realiza siguiendo los siguientes pasos:

- Conectarse a la página web:
`http://www.debian.org/`
- Obtener el fichero DEB con la última versión de disponible de PGP:
`pgp_2.6.3a-9_i386.deb`
- Desde la cuenta de root instalar la aplicación del siguiente modo:
`dpkg -i pgp_2.6.3a-9_i386.deb`
- En el caso que la aplicación PGP requiera otros paquetes deberán ser instalados previamente del mismo modo que el anteriormente detallado.

1.2. Utilización de los Comandos Básicos de PGP

El objetivo principal del alumno es descubrir el modo de utilizar las funcionalidades básicas que proporciona PGP y comprobar su correcto funcionamiento. De este modo, es necesario realizar las siguientes tareas:

- **Generar la pareja clave privada/clave pública**
Se generará una clave secreta y su correspondiente clave pública. Al ejecutar esta función es posible que se pida cierta información adicional (algoritmo de encriptación, número de bits de la clave privada, identificador del usuario, palabra de paso).
- **Extraer una clave pública**
Se buscará en el fichero de claves públicas y se extraerá una clave determinada indicada por el identificador del usuario.
- **Añadir una clave pública**
Se añadirá al fichero de claves públicas la clave pública indicada.
- **Encriptar**
Se encriptará un fichero con una clave pública determinada indicada por el identificador del usuario, obteniendo un fichero encriptado.
- **Firmar**
Se firmará un fichero con una clave privada indicada con el identificador del usuario obteniendo un fichero firmado.
- **Desencriptar y/o Autenticar**
Se desencriptará y/o autenticará los ficheros anteriormente encriptados y/o firmados. La aplicación debería reconocer con que clave se encriptó y/o firmó el documento y buscará en el directorio de claves si existe su pareja. En caso de encriptación se validará la clave privada a través de la introducción de la palabra de paso.

En el directorio raíz del usuario existe un subdirectorio `.pgp/` donde aparecen todos los archivos que utiliza la aplicación pgp. Son importantes los archivos:
 - `Pubring.pbk`: Aquí se almacenan las claves públicas de los usuarios conocidos.
 - `Secring.srg`: Aquí se almacenan las claves privadas del usuario del sistema.

2. Servidor Apache con Certificados

La práctica consiste en la instalación del servidor web *Apache* y su posterior configuración para poder utilizar certificados digitales. Apache HTTP Server es un servidor web robusto, de múltiples características y funcionalidades y de código libre que forma parte del llamado *Apache Project*. (<http://www.apache.org/>).

Los diferentes pasos que se deben realizar se pueden resumir en los siguientes puntos:

- Instalación y configuración del servidor web Apache en cualquiera de las distribuciones linux existentes. El alumno debe tener en cuenta que en la entrevista se comprobará el correcto funcionamiento del servidor, por lo que si utiliza una distribución distinta a las proporcionadas en los laboratorios deberá montar la infraestructura necesaria. En los laboratorios docentes se dispone de la distribución Debian.
- Comprobación de la correcta instalación y funcionamiento del servidor web Apache. Un prueba sencilla tras la configuración, aunque sea de forma básica, consiste en teclear en el navegador la dirección "http://localhost" para controlar que Apache contesta. Se realizará también la prueba desde un host diferente al que tiene instalado el servidor Apache. Obviamente, la petición desde el navegador se realizará indicando su nombre de dominio: "http://nombre_dominio_servidor/". En este caso se obtendrá también la página de prueba del servidor Apache.
- Configuración del servidor Apache como servidor seguro. Existen distintos métodos para realizarlo. Uno de ellos consiste en la combinación de los módulos Apache, OpenSSL y Mod_SSL. Para ello, si no lo están ya, se deberán acoplar estas funcionalidades a nuestra distribución linux. A través de la página web de la asignatura se puede obtener los paquetes necesarios así como información de su funcionamiento.
- Una vez instalados los módulos necesarios, es importante saber que un servidor seguro necesita un certificado digital para identificarse a los browser de la Web. Para ello, el primer paso es crear un certificado utilizando claves pública y privada propias. Posteriormente será necesario o crear una petición de un certificado (CSR) para mandar a una CA (Autoridad Certificadora) o crear el propio certificado self-signed.
- Una forma sencilla de crear un certificado digital es la siguiente:

```
openssl req -new -nodes -keyout myserver.key -out server.csr
```
- **IMPORTANTE:** En esta práctica, se creará un certificado que posteriormente será autenticado por una autoridad certificadora. A través de la página web de la asignatura se proporciona información, así como enlaces a alguna de las muchas autoridades certificadoras, que proporcionan certificados autenticados gratuitos y por

un periodo de vida limitado. En el caso que la obtención de un certificado gratuito no fuera posible, cabe la posibilidad de utilizar alguno de los certificados de pruebas que estas autoridades proporcionan.

- A continuación y tras configurar nuestro servidor web con el nuevo certificado, se comprobará su correcto funcionamiento. Para ello se accederá al servidor instalado, desde un browser y se comprobará que nos informa que se está accediendo a una zona segura. El modo de acceder al servidor es análogo al ya utilizado anteriormente con la salvedad que ahora el protocolo utilizado es HTTPS. De este modo se utilizará: "https://localhost" para controlar que Apache contesta. De igual manera se comprobará su funcionamiento desde un host remoto. Es importante saber que HTTP y HTTPS utilizan puertos diferentes por lo cual los dos servicios estarán activos. Comprobar también el funcionamiento de Apache mediante una conexión no segura, utilizando http.
- Finalmente, se modificará la configuración del servidor web apache seguro, para que funcione en un puerto diferente al especificado por defecto (por ejemplo el 8080).
- Todos los paquetes necesarios para la instalación del servidor apache seguro y no seguro, pueden obtenerse a través de la pagina: (<http://www.debian.org/>)

3. Notaciones

- Las prácticas se realizarán individualmente o en grupos de dos personas como máximo.
- Se realizará una entrevista y prueba de la aplicación con todos los miembros del grupo.
- Mejoras y funcionalidades adicionales se tendrán en cuenta en la nota final.

4. Documentación a entregar

Informe detallado con TODOS los pasos realizados en:

- Instalación y comprobación de las todas las funcionalidades de PGP requeridas en esta práctica.
- Instalación del servidor Apache tanto en modo seguro como en modo no seguro, obtención del certificado digital y pruebas realizadas para la comprobación del correcto funcionamiento.