INTRODUCCIÓN A LA CRIPTOGRAFÍA DE CLAVE PÚBLICA GNUPG

INTRODUCCIÓN A LA CRIPTOGRAFÍA DE LLAVE PÚBLICA

Encriptación simétrica y asimétrica

Existen dos tipos de encriptación

Encriptación simétrica consiste en el uso de una única llave para encriptar y desencriptar mensajes y documentos

Encriptación asimétrica consiste en el uso de dos llaves, una **pública** para encriptar y una **privada** para desencriptar
En la encriptación asimétrica la desencriptación de mensajes o documentos solo puede ser realizada utilizando la **clave privada**

Encriptación asimétrica. Llaves públicas y privadas

En la **encriptación asimétrica** se usa un sistema de llaves públicas lo que viene a decir que cada usuario tiene una clave privada y una clave pública

La **llave privada** es la que usamos para desencriptar mensajes o documentos encriptados con nuestra llave pública. Obviamente esta llave solo debe conocerla el propietario de dicha llave

La **llave pública** es la que compartimos con las personas para que mediante esta llave pública puedan enviarnos mensajes o documentos cifrados

Funciones hash

Las funciones **hash** son algoritmos matemáticos que permiten calcular un valor resumen de los datos para ser firmados digitalmente
Funciona en una sola dirección, esto es, no es posible a partir del valor resumen calcular los datos originales

Cuando la fuente es un documento, el resultado de la función **hash** es un número que identifica inequívocamente a dicho documento, así el destinatario puede aplicar de nuevo la función y comprobar el resultado con el que ha recibido

Las operaciones con funciones **hash** no están pensadas para que las lleven a cabo los usuarios, sino que se utiliza software tanto para automatizar el cálculo del valor **hash** como su verificación posterior

GnuPG

GPG GNU ***P***rivacy ***G***uard es un software de encriptación utilizado para cifrar y firmar mensajes y documentos que utiliza criptografía híbrida, esto es, combina **criptografía simétrica**, por su rapidez, con **criptografía asimétrica** por no necesitar compartir claves secretas

GPG viene a reemplazar a ***PGP P***retty ***G***ood ***P***rivacy bajo licencia GPL utilizando el estándar ***OpenPG***

Mediante ***GPG*** se puede crear claves públicas y privadas, administrar dichas claves, encriptar datos usando las llaves públicas y desencriptar datos usando las llaves privadas

INSTALACIÓN GPG EN UBUNTU

Ubuntu viene con ***GPG*** y la interfaz gráfica ***Seahorse*** instalados. Si no se encontrara instalado se puede instalar desde los repositorios mediante el comando *sudo apt-get install gnupg* y *sudo apt-get install seahorse*

NOTA Si queremos integrar ***Seahorse*** con el explorador de archivos ***Nautilus*** instalamos el paquete *seahorse-plugins* con el comando *sudo apt-get install seahorse-plugins* y reiniciamos ***Nautilus*** ejecutando *sudo killall nautilus*

GENERAR NUESTRA LLAVE Y AGREGAR LLAVES PÚBLICAS A NUESTRO ANILLO DE LLAVES

Crear nuestra llave

Para generar nuestra propia llave ejecutamos el comando *gpg --gen-key*. La primera vez que ejecutemos esta orden, ***GPG*** creará algunos archivos y directorios en el directorio *.gnupg* normalmente alojado en el directorio *home* del usuario que ejecuta el comando

Crear un certificado de revocación

NOTA Esta parte es muy importante y se tiene que hacer AHORA

Como precaución, es posible que en el futuro queramos invalidar las llaves creadas ya sea por el simple hecho de olvidarnos de la frase de paso o porque tanto la llave privada como la frase de paso hayan sido comprometidas

Para crear un certificado de revocación ejecutaremos *gpg --output archivo_revocación.asc --gen-revoke id_llave*

Para conocer el identificador de la llave podemos usar el comando *gpg --list-keys* que muestra las claves públicas de nuestro anillo de claves. Estas claves se encuentran en el archivo *pubring.gpg*

Exportar llaves

Para exportar nuestra **llave pública** tenemos que ejecutar *gpg --armor --output archivo_llave.asc --export id_llave*

Tras la opción *--export* podemos indicar cualquier dato que identifique a la llave como el mail o la id de la llave. Ahora tenemos un archivo *archivo_llave.asc* que podemos enviar a otras personas para que puedan comunicarse con nosotros de forma segura

Para exportar nuestras **llaves privadas** tenemos que ejecutar *gpg --armor --output archivo_llave_privada.asc --export-secret-keys id_llave*

Para listar y conocer el identificador de las llaves privadas que se encuentran en el archivo *secring.gpg*, podemos ejecutar el comando *gpg --list-secret-keys*

Importar llaves públicas a nuestro anillo de llaves

Para añadir llaves públicas a nuestro anillo de llaves, primero tendremos que importarlas, luego comprobar la huella digital de la llave para validarla y después de verificar dicha huella validar la llave

Estos comandos hacen esto importar la llave pública, mostrar la huella de dicha llave que tendremos que confirmar con el dueño de dicha llave y finalmente firmar la llave

gpg --import llave_publica.asc

gpg --fingerprint id_llave

gpg --sign-key id_llave

Borrar llaves de nuestro anillo de llaves

Los anillos de claves son los archivos en los que se guardan las llaves públicas **pubring.gpg** y privadas **secrimg.gpg**. Para eliminar las llaves de estos archivos hay que eliminar primero las llaves privadas y luego las públicas

Para borrar las llaves privadas ejecutamos *gpg --delete-secret-keys id_clave*

Para borrar las llaves públicas ejecutamos *gpg --delete-keys id_clave*

Utilizar servidores web de llaves públicas

Una de las mejores formas de poner a disposición de otras personas nuestras claves públicas es utilizando servidores web de llaves, los cuales nos permiten exportar nuestras llaves públicas, importar llaves de otras personas y buscar llaves dentro de su depósito. Los comandos que nos permiten exportar una llave a un servidor, buscar una llave determinada en el servidor e importar una llave son respectivamente

gpg --keyserver nombre_servidor --send-keys id_llave

gpg --keyserver nombre_servidor --search-keys id_llave

gpg --keyserver nombre_servidor --recv-keys id_llave

NOTA como servidor de llaves usaremos *hkp://keys.gnupg.net* que escucha en el puerto *11371*

NOTA en algunos servidores habrá que buscar las llaves de forma *0xid_llave*

TRABAJAR CON DOCUMENTOS

Cifrar y firmar

Digamos que tenemos un archivo que queremos enviar a otra persona. Podemos cifrarlo, firmarlo o cifrarlo y firmarlo. Cifrarlo significa que solo el receptor del archivo podrá abrirlo. La firma le dirá al receptor que fuimos realmente nosotros quien creamos el archivo

Estos 3 comandos harán esto, cifrar, firmar y cifrar-firmar

gpg --armor --output archivo_cifrado.txt --encrypt --recipient usuario@correo.com archivo_original

gpg --clearsign --output archivo_firmado.txt --sign --recipient usuario@correo.com archivo_original

gpg --armor --output archivo_cifrado_firmado.txt --encrypt --sign --recipient usuario@correo.com archivo_original

Firmar archivos por separado

En algunos casos, puede interesarnos que la firma electrónica vaya separada del archivo original en un fichero aparte, para ello ejecutamos el comando *gpg --armor --output firma.txt --detach-sign archivo_original*

NOTA ten en cuenta que a la hora de verificar la firma del archivo tendremos que tener tanto el archivo con la firma electrónica como el propio archivo firmado. El comando que verifica la firma digital es *gpg --verify firma.txt archivo_original*

Descifrar y verificar firmas

Para descifrar un documento cifrado tenemos que ejecutar *gpg --output archivo --decrypt archivo_cifrado.txt*. Esto descifrará el archivo y verificará la firma si la hay

Si solo queremos verificar la firma de un archivo ejecutaremos *gpg --verify archivo_firmado.txt*

Cifrar y descifrar archivos sin llaves

GPG permite cifrar documentos usando contraseñas en lugar de llaves. La contraseña funcionará como clave y será utilizada como **encriptado simétrico**. Se puede cifrar el archivo con el parámetro *--symmetric* del comando *gpg*; el descifrado usa el parámetro ***–decrypt***

gpg --armor --output archivo_cifrado.txt --symmetric archivo_original

MODIFICAR PROPIEDADES DE LAS LLAVES

GnuPG subshell

Para modificar parámetros de nuestras llaves tales como su frase de paso, fecha de expiración o firmar llaves públicas de otras personas ***GPG*** instala una *shell* que permite, desde la línea de comandos, ejecutar estas operaciones

Para iniciar **gpg subshell** ejecutamos el comando *gpg --edit-key id_llave*

COMANDOS BÁSICOS GPG SUBSHELL

COMANDO	DESCRIPCIÓN
?	Lista y describe los comandos disponibles
list	Muestra los datos de la llave desde el archivo *secring.gpg*
fpr	Muestra la huella, *fingerprint*, de la llave
sing	Permite firma la llave
trust	Establece o cambia el nivel de confianza a la llave
expire	Permite cambiar la fecha de expiración de la llave