**ANEXO III**

**Práctica 3:** **Cifrado y firma digital con el uso de GPG**

**Trabajo preparatorio**

* **Explicar la diferencia entre cifrado simétrico y asimétrico. También entre clave pública y clave privada.**

En el cifrado simétrico, se emplea una sola clave secreta compartida para llevar a cabo tanto el cifrado como el descifrado de los datos. Esto requiere que ambas partes acuerden y mantengan la clave en estricta confidencialidad. Este método destaca por su rapidez y eficiencia, siendo adecuado para manejar grandes volúmenes de datos. Sin embargo, su mayor desafío es garantizar la distribución segura de la clave, ya que, si un tercero logra obtenerla, podría acceder a la información protegida [46].

En cambio, en el cifrado asimétrico utiliza un par de claves interrelacionadas: una pública y una privada. La clave pública, que se puede compartir libremente, se emplea para cifrar los datos, mientras que la clave privada, mantenida en secreto, se utiliza para descifrarlos. Este enfoque elimina la necesidad de compartir una clave secreta entre las partes, lo que refuerza la seguridad de las comunicaciones. Sin embargo, es menos eficiente que el cifrado simétrico, por lo que generalmente se utiliza para el intercambio seguro de claves simétricas o en aplicaciones donde la velocidad no es un factor crucial [46].

En la criptografía asimétrica, las claves pública y privada cumplen funciones específicas:

* Clave Pública: Esta clave se puede compartir libremente y se utiliza para cifrar información o verificar firmas digitales. Aunque cualquiera puede acceder a ella, no permite descifrar los datos encriptados [47].
* Clave Privada: Mantiene su confidencialidad y se emplea para descifrar información cifrada con la clave pública correspondiente o para generar firmas digitales. La seguridad de todo el sistema se basa en la protección de esta clave [47].
* **Consultar que es una firma digital, su utilidad, proceso de verificación y su importancia en la seguridad en dispositivos Linux.**

Una firma digital es una técnica criptográfica que asegura la autenticidad, integridad y no repudio de un documento o mensaje electrónico. A diferencia de una firma manuscrita, utiliza algoritmos matemáticos para crear un vínculo único entre el firmante y el contenido firmado, garantizando que no ha sido modificado y que proviene de una fuente confiable. [48]

Una firma digital es un valor numérico representado como una secuencia de caracteres, generado mediante un proceso matemático avanzado que solo puede realizar un ordenador. Las firmas digitales se fundamentan en la criptografía de clave pública, también conocida como criptografía asimétrica. Este sistema utiliza algoritmos como RSA para generar un par de claves matemáticamente vinculadas: una clave privada y una clave pública.

El funcionamiento se basa en la autenticación mutua mediante estas dos claves criptográficas. El creador de la firma utiliza su clave privada para cifrar los datos asociados a la firma, asegurando su autenticidad. Para validar la firma, se utiliza la clave pública correspondiente, ya que es la única capaz de descifrar la información cifrada. Este proceso garantiza la autenticidad de la firma digital y del contenido relacionado.

En sistemas Linux, las firmas digitales tienen un papel fundamental en los siguientes aspectos:

* Verificación de Software: Los paquetes y actualizaciones están firmados digitalmente para garantizar que provienen de fuentes legítimas y no han sido alterados, protegiendo al sistema contra software malicioso. [48]
* Cifrado y Autenticación: Herramientas como GnuPG emplean firmas digitales para cifrar información y autenticar comunicaciones, asegurando la privacidad y seguridad de los datos transmitidos. [48]
* Acceso Seguro:La autenticación mediante certificados digitales facilita conexiones seguras, como en redes privadas virtuales (VPN), donde se utilizan certificados para verificar la identidad de los usuarios. [48]
* **Describir que es GPG y su utilidad, así como la forma de instalar y configurar en Linux.**

GPG (GNU Privacy Guard) es una herramienta de cifrado y firma digital basada en el estándar OpenPGP. Permite a los usuarios garantizar la confidencialidad e integridad de sus datos y comunicaciones mediante la criptografía de clave pública. Con GPG, los datos se cifran para que solo los destinatarios autorizados puedan acceder a ellos, y se firman digitalmente para confirmar su autenticidad y origen. [49]

Utilidad de GPG:

* Cifrado de Datos: Permite proteger archivos y mensajes, asegurando que solo los destinatarios que posean la clave correspondiente puedan acceder al contenido.
* Firmas Digitales: Ofrece la posibilidad de firmar digitalmente documentos y correos electrónicos, garantizando su autenticidad y confirmando que no han sido modificados.
* Gestión de Claves: Facilita la generación, distribución y revocación de claves públicas y privadas, elementos esenciales en la criptografía asimétrica.

Para instalar se usa el comando sudo apt install gnupg. Luego de se genera el par de claves, pública y privada, con el comando gpg --full-generate-key. Este comando da una serie de preguntas para configurar tus claves, como el tipo de clave, tamaño, duración, nombre y correo electrónico asociados.

Luego se exporta la clave pública con el comando gpg --export --armor tu\_correo@example.com > clave\_publica.asc, se la comparte con otros usuarios para poder cifrar y descifrar archivos dependiendo del caso de uso. Además, también es necesario poseer claves públicas de otros usuarios para poder cifrar con dicha clave y que los usuarios puedan descifrar el archivo con su clave privada en su dispositivo.