**ANEXO III**

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

**Informe**

* **Documentar las configuraciones aplicadas.**

Las configuraciones realizadas se encuentran en la parte procedimiento de la práctica.

* **Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados. Además, indicar el impacto en la seguridad.**

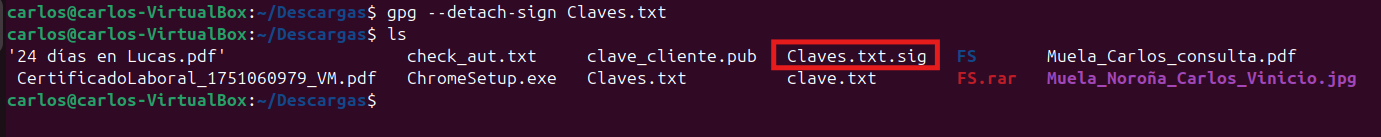
Los resultados obtenidos de la práctica con la debida explicación se muestran en la parte de resultados de la práctica. Y también el impacto que tiene en la seguridad de los dispositivos.

* **Realizar el proceso de firma separada y explicar sus casos de uso. Además, las diferencias que tiene con firma adjunta.**

La firma digital separada como se nombre lo dice, se guarda en un archivo independiente del documento original. Este archivo de firma almacena la información criptográfica necesaria para validar la autenticidad del documento sin alterar su contenido. Se utiliza con frecuencia en entornos donde es fundamental preservar la integridad del archivo original, como en sistemas gubernamentales y transacciones electrónicas, asegurando que los documentos no sean alterados y mantengan su validez.

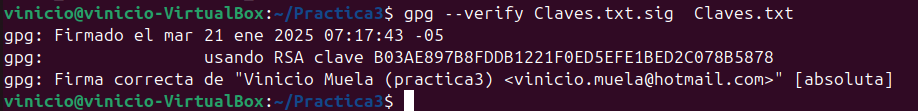
Por lo tanto, Se emplea una **firma adjunta** cuando se requiere un archivo autocontenido, lo que facilita su distribución y uso sin necesidad de archivos adicionales. Por otro lado, se utiliza una **firma separada** cuando es necesario firmar documentos sin alterarlos, especialmente en situaciones donde la integridad del archivo original es crucial, como en entornos gubernamentales o transacciones seguras.

De esta forma firmar un archivo con firma separada, primero se genera el archivo firmado por parte del emisor con su clave privada. Para el caso se obtiene el archivo Claves.txt.sig.



**Figura 5.19.** Firma de archivo por parte del emisor.

De esta forma el archivo formido .sig y el archivo original se envían al receptor para que pueda verificar la autenticidad del archivo utilizando la clave pública del emisor. Para ello se usa el comando gpg --verify mensaje.txt.sig mensaje.txt.



**Figura 5.20.** Verificación de la firma por parte del receptor.

En consecuencia, se observa que el archivo fue firmado por el emisor de forma correcta por el receptor, es decir, el documento no fue alterado y la firma es válida. Además, se puede ver que para el rececptor la firma del emisor es confiable completamente dado que se presenta el mensaje “absoluta”

Por otro lado, los casos de uso son los siguientes:

**Garantizar integridad sin modificar el archivo original**

* Se emplea cuando es necesario verificar la autenticidad de un archivo sin alterar su contenido.
* Es especialmente útil en auditorías de seguridad y en la protección de documentos oficiales.

**Distribución de Software Seguro**

* Muchos proyectos de código abierto utilizan archivos .sig junto con sus paquetes para que los usuarios puedan validar su autenticidad.
* Ejemplo: Distribuciones como Debian, Fedora y Arch Linux publican firmas digitales separadas para garantizar la integridad de los paquetes antes de su instalación.

**Mensajes Firmados sin Cifrar**

* Permite que cualquier persona acceda al contenido sin requerir una clave privada, pero manteniendo la capacidad de verificar la autenticidad del mensaje.

**Verificación de Archivos Grandes**

* Evita la necesidad de modificar archivos de gran tamaño, facilitando su verificación sin afectar su estructura o contenido.