

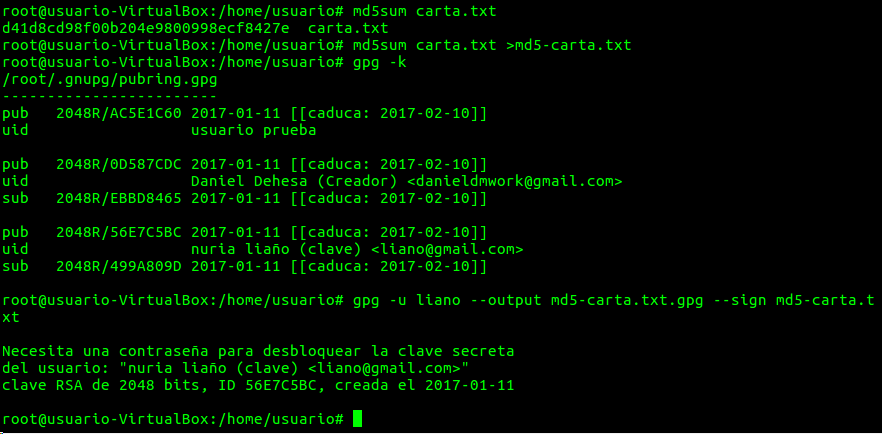
|  |  |
| --- | --- |
| **SEGURIDAD INFORMÁTICA** – 2º SMR | |
| UT5: Sistemas de identificación. Criptografía. | Práctica 3: Firmas digitales. |
| Nombre: | |
| Nota: | Observaciones: |

En la teoría hemos visto que la pareja de claves pública privada podía ser usada para asegurar:

* Confidencialidad de la comunicación: si enviamos nuestra clave pública al resto del mundo, podrán usar esa clave para cifrar documentos que sólo nosotros podremos descifrar usando nuestra clave privada.
* Autenticación y no repudio: si usamos nuestra clave privada para firmar un documento a otra persona. Esa persona podrá usar nuestra clave pública para descifrar la firma y asegurarse de que solo nosotros podemos haber hecho dicho documento.

Hemos estado trabajando el primer uso en la práctica anterior. Ahora vamos a realizar una práctica para comprobar como funciona la segunda aplicación.

1. Averigua cuáles son las opciones para ejecutar gpg en Ubuntu que permiten firmar documentos de la siguiente manera:
   1. Creando la firma junto con el documento.



Clave password

* 1. Creando la firma separada del documento.

1. Firma digitalmente algún documento sencillo, que tengo un tamaño pequeño.
   1. ¿Qué tipo de firma crees que será la más adecuada? Fírmalo según esa firma.
   2. Intenta abrir el documento y observa si es legible.
   3. Envía el documento firmado al menos a dos compañeros. Asegúrate de que tengan tu clave pública. ¿Podrán todos descifrar tu documento? ¿Es esa comunicación confidencial?
   4. Al mismo tiempo tú deberás recibir algún documento de algún compañero que esté firmado digitalmente. Descifra el documento utilizando la clave pública de tu compañero. Si un hacker interceptara el documento, ¿podría descifrarlo? ¿hay algún problema en ello? ¿cuál es la única cosa de la que puedes estar seguro?
2. Ahora firma digitalmente alguno de los archivos DOC usados para el módulo.
   1. ¿Qué tipo de firma crees que será la más adecuada? Fírmalo según esa firma.
   2. Envía el documento y la firma a un compañero para que la verifique.

En caso de que ejecutaras el comando anterior con un archivo con firma no separada, lo que te solicita es el nombre del archivo que generará al quitar la firma:

* 1. Al mismo tiempo tú deberás recibir el documento y la firma de otro. Verifica dicha firma.
  2. ¿Qué característica de seguridad queda garantizada?
  3. Modifica el documento que has recibido, introduciendo y borrando algún carácter y comprueba si se sigue verificando la firma.

Links

https://www.genbetadev.com/seguridad-informatica/manual-de-gpg-cifra-y-envia-datos-de-forma-segura