UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

DEPARTAMENTO DE PROGRAMACIÓN DE COMPUTADORAS

LICENCIATURA EN CIBERSEGURIDAD

CRIPTOGRAFÍA

LABORATORIO#3

PERTENECE A:

POLANCO, OMAR 8-1014-120

PROFESOR:

MORENO, JOSE

GRUPO:

1S3121

II SEMESTRE

2024

Índice

Introducción

En la era digital, la protección de la información es crucial. El cifrado ha emergido como una de las principales herramientas para asegurar la seguridad y la privacidad de los datos. Una de las soluciones más destacadas en este campo es GPG Suite, que permite a los usuarios cifrar y firmar documentos, correos electrónicos y otros tipos de información mediante criptografía de clave pública.

Este informe describe el proceso de instalación de GPG Suite, el intercambio de claves públicas y el uso del cifrado de datos. Se presenta una guía paso a paso para realizar estos procedimientos, enfatizando la importancia de un intercambio seguro de claves y la protección de información sensible. Además, se muestra cómo cifrar un documento con la clave pública del profesor, garantizando que solo él pueda descifrar y acceder al contenido. Este proceso es fundamental en la práctica de ciberseguridad, ya que asegura la confidencialidad y autenticidad de la información transmitida.

Paso#1

El primer paso en la configuración de GPG Suite es crear un nuevo par de claves GPG, que incluye una clave pública y una clave privada. La clave pública se compartirá con otros para que puedan cifrar mensajes destinados a ti, mientras que la clave privada se utilizará para descifrar esos mensajes y firmar digitalmente documentos.

Para generar este par de claves, utiliza el siguiente comando en la terminal:

```
omars@MacBook-Pro-3 ~ % gpg --gen-key
gpg (GnuPG/MacGPG2) 2.2.41; Copyright (C) 2022 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Nota: Usa "gpg --full-generate-key" para el diálogo completo de generac
ión de clave.

GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: Prueba de Omar
Dirección de correo electrónico: pruebadeomar@gmail.com
Ha seleccionado este ID de usuario:
    "Prueba de Omar <pruebadeomar@gmail.com>"
```

Este comando iniciará un asistente interactivo que te solicitará ingresar información como tu nombre, correo electrónicoy una contraseña para proteger la clave privada. Al finalizar, habrás generado un par de claves listo para utilizar en la encriptación y firma de datos.

Paso#2

Después de crear tu par de claves GPG, el siguiente paso es exportar tu clave pública, la cual compartirás con otras personas para que puedan cifrar mensajes dirigidos a ti.

Para exportar la clave pública, ejecuta el siguiente comando:

```
omars@MacBook-Pro-3 ~ % gpg --export Prueba de Omar > pruebadeomar.gpg
```

```
omars@MacBook-Pro-3 ~ % file pruebadeomar.gpg
pruebadeomar.gpg: OpenPGP Public Key Version 4, Created Tue May 16 15:53:58 2023,
RSA (Encrypt or Sign, 4096 bits); User ID; Signature; OpenPGP Certificate
```

El sistema debería indicar que el archivo contiene un "GPG key public ring", lo que confirma que es una clave pública válida.

Si prefieres exportar la clave pública en un formato más legible (ASCII), puedes utilizar el siguiente comando:

```
omars@MacBook-Pro-3 ~ % gpg --armor --export Prueba de Omar > pruebadeomar.asc
```

```
  UW PICO 5.09                          File: pruebadeomar.asc

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGRjpxYBEADLzQw51UGsy+BeACd41wo2lrXFHy3yw3yISAzwKm9dIGSDMv0g
VJZByig3FZS9Pr/P22V3wprNePugmp3PH444UPCsxz6EubQQaH9NRS3R4yD3I045
ZMhwBHLaJ9OT9apyDJ6hfRhS47v2NwLY7qfziCwofQCqrA5R3n4lQ1xJ1Duh7mud
zCptlYg4SGL7uI2KFZ+i2Cvuxg7PfQ+GbPOeVXzNbV+poO0uTAf97gDBdVOiUvzg
dbMUMuWuLQJv8BomDL4u97jJ8pPhOa5LUd9R32AanT+avMssouhNXiMWlAS0GDwi
kwQ2yqNBFm7WpUBxABmt6IO/tUuRAAvFiHojWXxE8uyWFBhzKBO/Z559XG45LnU1
3QamijMzLxKmPaRw1EsrpkxtEDIC0NM5OTtE0f3pjDef5zqHO0tsCUxUZOpA0bgR
E0RSiBB00otUkqt3ROeNLIHh0nOJXJTkObFOoUfO1yaOaNb6Ze1OBNCCAfEvN4YO
uOnTlUxyAHi/bAGM764VvKx1TziOZuUHaXIcdNENlLO9we7OPC5TsPvSwL1PWD0n
+74BoD/zXgCTc6wDlHYOQ9TexmLAdPFzUQqQN/dEXChon2ihDxvR1mFqCabBnuA6
PdOsy3yizjWxUrZQlxc3xWUX1cuE05mR67wxtweTltJ3ss+e8YNWpoIiYQARAQAB
tCZPbWFyIFBvbGFuY28gPHBvbGFuY29vbWFyMThAZ21haWwuY29tPokCVAQTAQgA
PhYhBFe0xLzwgjJGTZtWjVfiqJsM+RzmBQJkY6cWAhsDBQkHhh58BQsJCAcCBhUK
```

Esto generará un archivo llamado ramesh-pub-asc.gpg, que es la versión en texto plano de tu clave pública, ideal para compartir por correo electrónico o mensajes.

Paso#3

El siguiente paso es importar la clave pública de otras personas con las que desees intercambiar información cifrada. Esta clave te permitirá cifrar mensajes específicamente para esa persona y verificar sus firmas digitales.

Para importar una clave pública, utiliza el siguiente comando:

```
omars@MacBook-Pro-3 ~ % gpg --import Alanis\ Zamora_0xA602356F_public.asc
gpg: clave 7AE8CAA2A602356F: "Alanis Zamora <alanis.zamora1@utp.ac.pa>" sin cambio
s
gpg: Cantidad total procesada: 1
gpg:              sin cambios: 1
```

Este comando leerá el archivo y añadirá la clave pública al anillo de claves de tu sistema GPG, permitiéndote usarla para cifrar mensajes o verificar firmas realizadas por esa persona.

Paso#4

Una vez que hayas importado las claves públicas de las personas con las que deseas comunicarte, puedes cifrar mensajes para ellas. A continuación, se muestra cómo cifrar un archivo utilizando la clave pública del destinatario.

Para cifrar un archivo con la clave pública del destinatario, utiliza el siguiente comando:

```
omars@MacBook-Pro-3 ~ % gpg --recipient Alanis\ Zamora --encrypt prueba.txt
gpg: 7DE72EB1A9B5B4D5: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

sub  rsa2048/7DE72EB1A9B5B4D5 2024-08-28 Alanis Zamora <alanis.zamora1@utp.ac.pa>
 Huella clave primaria: 07D6 0260 9157 5C63 8BBC  1114 7AE8 CAA2 A602 356F
      Huella de subclave: 135D 7AE6 1F45 39C1 6FBB  59AF 7DE7 2EB1 A9B5 B4D5

No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.

¿Usar esta clave de todas formas? (s/N)
```

El archivo cifrado solo podrá ser descifrado por el destinatario usando su clave privada, garantizando que el contenido permanezca confidencial durante el intercambio.

Paso#5

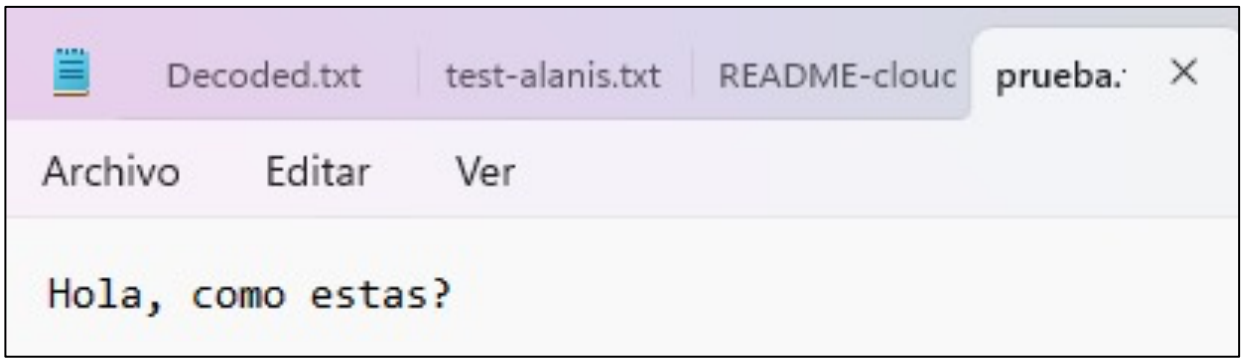
Una vez que el mensaje ha sido cifrado y enviado, el destinatario puede descifrarlo usando su clave privada. A continuación, se explica cómo descifrar un archivo cifrado recibido.

Para descifrar un archivo cifrado, utiliza el siguiente comando:

```
omars@MacBook-Pro-3 ~ % gpg --decrypt prueba.txt.gpg
```

Este comando procesará el archivo cifrado y, si la clave privada correspondiente está disponible, mostrará el contenido descifrado en la terminal o creará un archivo con el contenido descifrado. Así, el destinatario podrá leer el mensaje original enviado de forma segura.

Si el destinatario también desea enviar un mensaje cifrado de vuelta, repetirá el proceso de cifrado utilizando la clave pública del remitente. Como el remitente ya ha compartido su clave pública, el destinatario podrá cifrar el mensaje para devolverlo. De este modo, el intercambio de mensajes cifrados puede continuar, garantizando que la comunicación se mantenga segura y privada.



Conclusión

El uso de GPG Suite para cifrar y descifrar mensajes es esencial para proteger los datos en la comunicación digital. Mediante la generación de pares de claves, el intercambio de claves públicas y el cifrado de mensajes, se garantiza la confidencialidad e integridad de la información transmitida. Este proceso asegura que los mensajes solo sean accesibles para los destinatarios previstos y que cualquier respuesta también sea segura.

El cifrado de mensajes con la clave pública del destinatario y su descifrado con la clave privada correspondiente establece un marco sólido para la protección de datos. Al seguir estos pasos correctamente, se mejora la seguridad de las comunicaciones electrónicas, resguardando la información sensible contra accesos no autorizados y manteniendo la privacidad de los intercambios.