Cifrado simétrico con GPG

Ismael Macareno Chouikh

2024-10-15

Índice

1. Instrucciones

Realizar un cifrado simétrico con la aplicación `GPG`. Esta aplicación está basada en Linux y podemos realizar un cifrado simétrico como asimétrico.

Adjunto fichero PDF

Ejercicio:

- Investigar cuales son los parámetros más importantes de esta herramienta. (2 ptos)
- Crear un archivo de texto con un mensaje y realizar un cifrado simétrico de dicho archivo. (2 ptos)
- Abre el archivo con otro usuario o en otra máquina y descífralo con la contraseña que has introducido. (2 ptos)
- Investiga que otras herramientas existen para realizar un cifrado simétrico y realízala misma prueba. (4 ptos)

Chuleta GPG

NOTA: realiza la documentación paso a paso de la práctica y de los inconvenientes que has tenido y como los has solucionado.

2. Parámetros más importantes de `GPG`

- `-- version`: Este parámetro es bastante importante debido a que `gpg` tiene dos versiones
  - GnuPG 1.x
  - GnuPG 2.x
- `-- help`: Bastante importante para saber como funciona en caso de que no nos acordemos, etc.
- `--dump-options`: Imprime en pantalla una lista de las opciones disponibles
- `-s`: Firma un mensaje. Se puede combinar con las opciones `--encrypt` y a su vez con las opción `--symmetric` para encriptar un mensaje de manera simétrica.
- `-e`: Encripta datos para una o más de una clave pública. Está opción se puede combinar con la opción `-s`
- `-c`: Encripta de manera simétrica usando un parafraseado. Usa por defecto AES-128
- `-d` Desencripta el fichero que le proporcionemos
- `--list-public-keys`: Lista las claves públicas
- `--list-secret-keys`: Lista las claves privadas

Hay muchísimas otras opciones pero considero que estás son las más importantes.

Toda esta información la he obtenido mediante el `man` del comando ejecutando en mi terminal `man gpg`.

También se puede acceder al `man` en la siguiente URL `https://www.gnupg.org/documentation/manpage.html`

3. Cifrado y descifrado de fichero

En este apartado se nos pide que creemos un fichero con X contenido y lo cifremos, seguidamente se nos pide que lo pasemos a otra máquina con otro usuario y lo descifremos con la clave correspondiente.

En mi caso para esté apartado voy a usar lo siguiente:

- Mi máquina real con Fedora 39
- Máquina virtual de Ubuntu 24.04
- La herramienta `gpg` en CLI

3.1. Crear fichero y cifrarlo

En este primer sub-apartado de este apartado lo que haré será crear un fichero con el contenido "Hola mundoçon el comando `echo "Hola mundo» fichero.txt` y luego cifrarlo mediante el comando `gpg -c fichero.txt`

```
maka at magi in ~ 24-10-14 - 17:46:53  cd Desktop
maka at magi in ~/Desktop 24-10-14 - 17:47:09  echo "Hola mundo» fichero.txt
maka at magi in ~/Desktop 24-10-14 - 17:47:19  gpg -c fichero.txt
gpg: directory '/home/maka.gnupg' created
```

3.2. Descifrar desde otra máquina

Para este paso lo que tendremos que hacer será hacer uso de las siguientes funcionalidades:

- `SSH`
  - Lo instalamos mediante los siguientes comandos:
    - *`SSH` Client* En el Ubuntu 24.04 (Cliente): `apt install openssh-client`
    - *`SSH` Server* En mi máquina real en este caso (Servidor): `apt install openssh-server`
- `GPG`
  - Lo instalamos mediante el comando `apt install gpg` en ambas máquinas
- `scp`

Para copiar el fichero `gpg` de la máquina real a la virtual lo que hago es ejecutar el comando

`scp maka@172.20.10.3:/home/maka/Desktop/fichero.txt.gpg .` desde la máquina virtual.

```
maka@makaVB:~$ cd Desktop/
maka@makaVB:~/Desktop$ scp maka@172.20.10.3:/home/maka/Desktop/fichero.txt.gpg .
maka@172.20.10.3's password:
fichero.txt.gpg 100% 92 26.2KB/s 00:00
```

Una vez tenemos el fichero `txt.gpg` lo que tendremos que hacer será descifrarlo mediante `gpg`.

Si intentamos hacer un `cat fichero.txt.gpg` podremos apreciar que no seremos capaces de entender nada.

El comando ejecutado para descrifrar el fichero es `gpg -d fichero.txt.gpg`

¡OJO!: Es necesario hacer el paso de desencriptado en un entorno gráfico.

```
maka@makaVB:~/Desktop$ gpg -d fichero.txt.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
Hola mundo
```

4. Investigación de otras herramientas de cifrado simétrico

Yo en mi caso voy a tratar *gocryptfs* y `ccrypt` que ambos son CLI.

Ambas son herramientas que realizan cifrados simétricos.

4.1. *gocryptfs*

4.1.1. Instalación

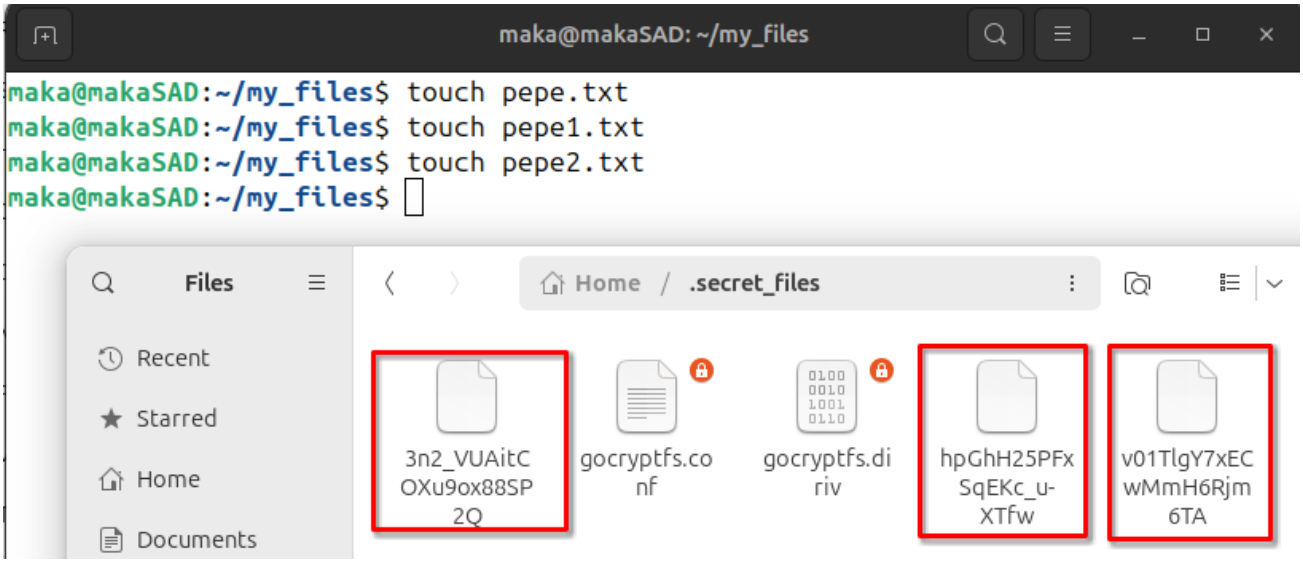
En mi caso voy a instalar *gocryptfs* en una máquina virtual que esta corriendo Ubuntu 24.04.

Para instalar *gocryptfs* lo único que tendremos que hacer es ejecutar el comando `sudo apt install gocryptfs`

4.1.2. Cifrado de fichero

1. Tendremos que crear dos directorios vacíos que nos servirán como puntos de montaje para el *encrypted filesystem*
   - `mkdir ~/.secret_files`
   - `mkdir ~/my_files`
2. Inicializamos *gocryptfs* con una contraseña
   - `gocryptfs -init ~/.secret_files`
3. Motamos el directorio encriptado en el directorio normal
   - `gocryptfs ~/.secret_files ~/my_files`

Después de estos pasos todo lo que pongamos en el directorio normal, automáticamente se encriptará y almacenará en el directorio encriptado



4.2. `ccrypt`

4.2.1. Instalación

¡AVISO! es más sencillo instalarlo en distrubuciones Debian, haciendo esto nos ahorramos el proceso del compilado del código fuente.

Para instalar `ccrypt` lo único que tenemos que hacer es ejecutar el comando: `sudo apt install ccrypt`

4.2.2. Encriptado

Para encriptar un fichero con `ccrypt` lo único que tenemos que hacer es:

1. Crear un fichero con el comando `echo "Hola» cc.txt`
2. Ejecutar el comando `ccrypt cc.txt`
   - Nos pedirá la que introduzcamos dos veces la contraseña
   - Se nos creará un fichero con extensión `.txt.cpt`

```
maka@makaSAD:~$ cd Desktop/
maka@makaSAD:~/Desktop$ echo "Hola" > cc.txt
maka@makaSAD:~/Desktop$ ccrypt cc.txt
Enter encryption key:
Enter encryption key: (repeat)
maka@makaSAD:~/Desktop$ ls -la
total 264
drwxr-xr-x  3 maka maka   4096 Oct 14 21:06 .
drwxr-x--- 16 maka maka   4096 Oct 14 18:36 ..
-rw-r--r--  1 maka maka 242498 Oct  3 17:48 analisisgrafico.svg
-rw-rw-r--  1 maka maka     37 Oct 14 21:06 cc.txt.cpt
-rw-r--r--  1 maka maka     92 Oct 14 18:38 fichero.txt.gpg
drwxrwxr-x  2 maka maka   4096 Sep 23 18:15 siad24
-rw-r--r--  1 root root     80 Sep 23 18:19 siad24.txt.pgp
```

4.2.3. Desencriptado

Para desencriptar lo único que tendremos que hacer será ejecutar el comando `ccrypt -d fichero.X.cpt`

```
maka@makaSAD:~/Desktop$ ls -la | grep -i cc
-rw-rw-r--  1 maka maka     37 Oct 14 21:06 cc.txt.cpt
maka@makaSAD:~/Desktop$ ccrypt -d cc.txt.cpt
Enter decryption key:
maka@makaSAD:~/Desktop$ ls -la | grep -i cc
-rw-rw-r--  1 maka maka      5 Oct 14 21:06 cc.txt
maka@makaSAD:~/Desktop$ cat cc.txt
Hola
```