Tema VI: Cifrado de Información

Nicolás A. Ortega Froysa

12 de mayo de 2022

Índice

1. Introducción

A menudo es necesario cifrar información para que sólo aquellas personas privilegiadas puedan accederla. Para esto, se ha usado históricamente el cifrado, y en nuestra época digital tecnológica, esto no ha cambiado, sino que se ha visto potenciado aún más, hasta el punto de que hoy día el cifrado de información es algo de lo más cotidiano. Simplemente con acceder a una página con el protocolo HTTPS ya estás usando cifrado.

2. GNU Privacy Guard (GPG)

En los sistemas GNU/Linux, la forma más normal de cifrar archivos es usando la herramienta de *GNU Privacy Guard* (GPG). Esto se usa tanto para cifrado simétrico como asimétrico. Vamos a revisar cómo cifrar un archivo usando esta herramienta de forma simétrica: es decir, que se usa la misma contraseña para cifrar y descifrar.

2.1. Cifrado

En primer lugar, tendremos que juntar todos los archivos que queremos cifrar en un solo archivo. Esto se puede hacer usando cualquier herramienta de compresión o unión de archivos. Para nuestro ejemplo, usaremos la herramienta `tar`, aunque también se podría usar ZIP.

Creamos un directorio con todos los archivos que queremos comprimir, y luego los juntamos usando el comando de `tar` siguiente:

```
$ tar cvf secreto.tar secreto/
```

Una vez que tengamos todos los archivos dentro de un mismo archivo, podemos cifrarlo usando el comando `gpg` (o en algunos sistemas de GNU/Linux es `gnupg`). Usamos el comando siguiente:

```
$ gpg --symmetric --cipher-algo <cipher> secreto.tar
```

En este caso `<cipher>` se reemplaza con el tipo de cifrado que se quiere hacer. En nuestro caso queremos usar el cifrado `AES256`. Pedirá también una contraseña para el cifrado en este paso. Esto producirá un archivo denominado `secreto.tar.gpg`. A partir de aquí podemos borrar los archivos originales de `secreto.tar` y el contenido del directorio `secreto/`. Dicho lo cual, como acabamos de cifrar los archivos es más seguro borrarlos usando el comando `shred` de GNU/Linux, que no sólo borrará los archivos, sino que antes de borrarlos reemplazará todo su contenido con caracteres aleatorios.

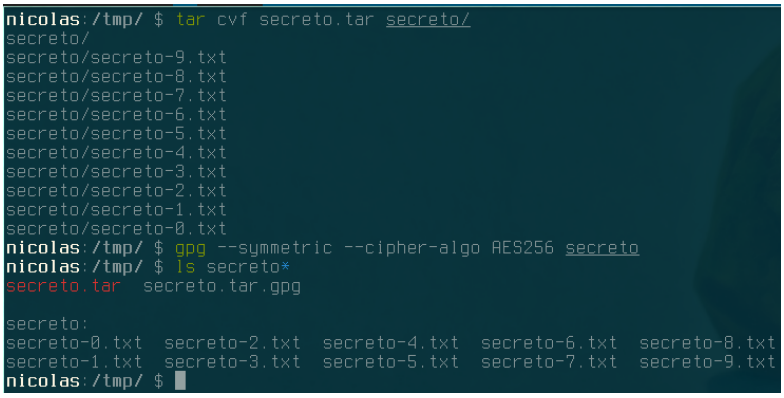

Figura 1: Cifrado de un archivo con GPG.

2.2. Descifrado

Para descifrar el mismo archivo, hacemos lo que sería el mismo proceso, pero a la inversa. Primero, lo desciframos usando GPG, e introduciendo la contraseña establecido anteriormente:

```
$ gpg -o secreto.tar -d secreto.tar.gpg
```

Esto producirá de nuevo nuestro archivo de `secreto.tar`. Posteriormente queremos desjuntar los archivos contenidos en ese *tarball*. Esto lo hacemos igualmente con el comando `tar`:

```
$ tar xvf secreto.tar
```

Esto nos extraerá del archivo el directorio original y los archivos contenidos en él. Con esto, ya habremos descifrado y recuperado los datos.

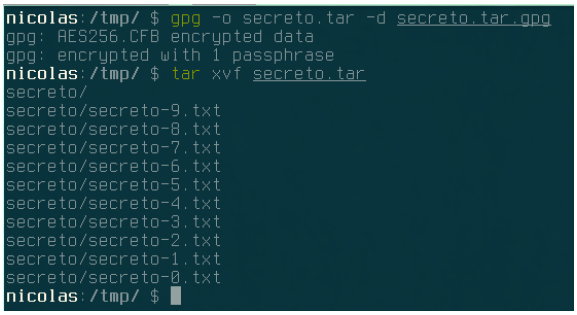

Figura 2: Descifrado con GPG.

3. Conclusión

El cifrado por línea de comando en GNU/Linux usando la herramienta GPG de GNU es una tarea bastante sencilla, aunque se tiene que dividir en sub-pasos si se quiere hacer con varios archivos. Mas esto forma parte de lo que sería la mentalidad de UNIX – que cada herramienta haga una sola cosa, y que lo haga bien.

4. Derechos de Autor y Licencia