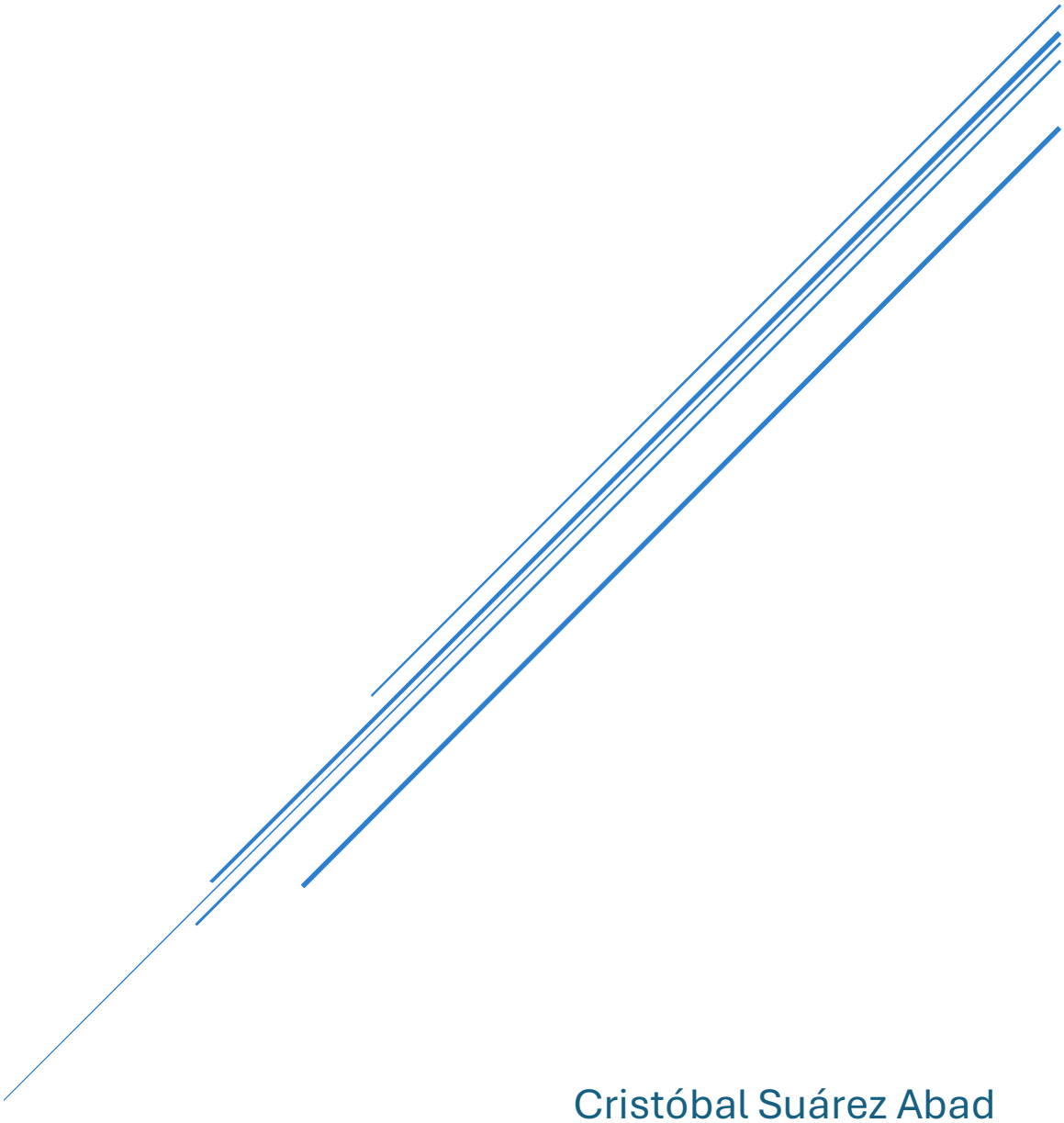
CRIPTOGRAFÍA

Actividad 3



Cristóbal Suárez Abad
Seguridad y alta disponibilidad – 2º ASIR

Índice

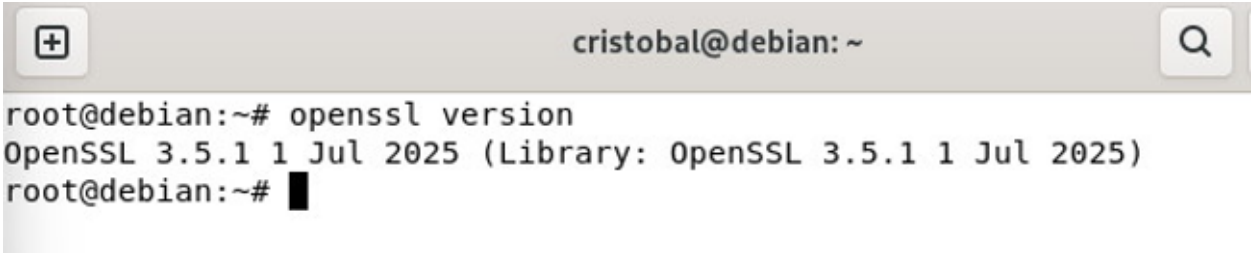
Instalar OpenSSL:

apt update

apt install openssl -y

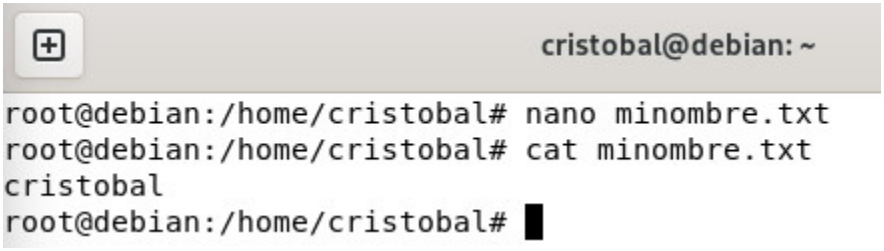
openssl versión

```
root@debian:~# apt update
Obj:1 http://security.debian.org/debian-security trixie-security InReleas
e
Obj:2 http://deb.debian.org/debian trixie InRelease
Obj:3 http://deb.debian.org/debian trixie-updates InRelease
Se pueden actualizar 132 paquetes. Ejecute «apt list --upgradable» para v
erlos.
root@debian:~# sudo apt update
sudo apt install openssl -y
^C
root@debian:~# apt install openssl
openssl                  openssl-provider-legacy
openssl-provider-fips
root@debian:~# apt install openssl
openssl                  openssl-provider-legacy
openssl-provider-fips
root@debian:~# apt install openssl -y
```



TAREA 1: Clave Simétrica con OpenSSL

a) Crea un archivo de texto llamado mensaje.txt con un mensaje breve: tu nombre.

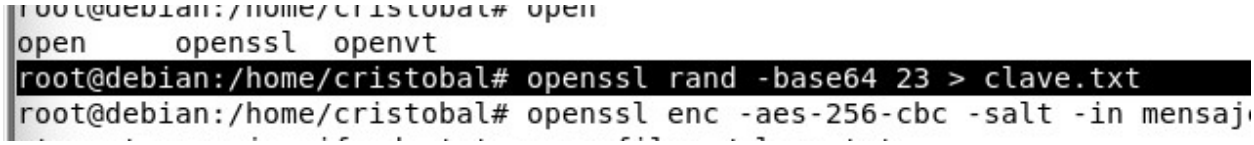


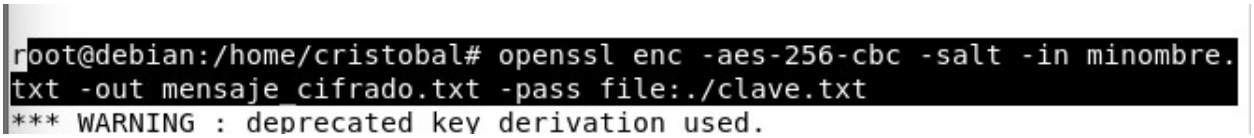
b) Usa el comando openssl para cifrar este archivo con el algoritmo AES-256. El mensaje cifrado debe llamarse mensaje_cifrado.txt Has debido de crear una clave de cifrado. Guárdala en un archivo llamado clave.txt

Primero guardamos la clave: **openssl rand -base64 23 > clave.txt**

Luego creamos el archivo cifrado usando la clave:

openssl enc -aes-256-cbc -salt -pbkdf2 -in minombre.txt -out mensaje_cifrado.txt -pass file:./clave.txt





c) Descifra el mensaje generando un archivo llamado mensaje_descifrado.txt

openssl enc -d -aes-256-cbc -pbkdf2 -in mensaje_cifrado.txt -out mensaje_descifrado.txt -pass file:./clave.txt

```
root@debian:/home/cristobal# openssl enc -d -aes-256-cbc -in mensaje_cifr
ado.txt -out mensaje_descifrado.txt -pass file:./clave.txt
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
root@debian:/home/cristobal#
```

```
-rw-rw-r-- 1 root      root        10 oct 31 17:40 mensaje_descifrado.txt
-rw-rw-r-- 1 root      root        10 oct 31 17:28 minombre.txt
drwxr-xr-x 2 cristobal cristobal 4096 ago 30 17:48 Música
drwxr-xr-x 2 cristobal cristobal 4096 ago 30 17:48 Plantillas
drwxr-xr-x 2 cristobal cristobal 4096 ago 30 17:48 Público
drwxr-xr-x 2 cristobal cristobal 4096 ago 30 17:48 Vídeos
root@debian:/home/cristobal# cat mensaje_descifrado.txt
cristobal
root@debian:/home/cristobal#
```

¿Por qué es necesario proteger la clave de cifrado?

Porque cualquiera que obtenga la clave podrá descifrar los datos cifrados.

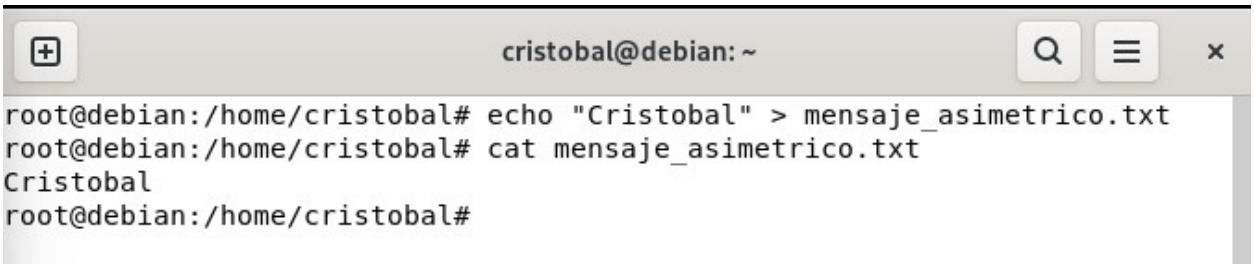
En el cifrado simétrico, la misma clave sirve para cifrar y descifrar, por lo tanto es el punto más vulnerable.

¿Qué sucede si la clave se pierde o es interceptada?

Si se pierde no podremos descifrar los mensajes encriptados. Y si es interceptada nuestros mensajeres estará a merced del atacante.

TAREA 2: Cifrado asimétrico con OpenSSL.

a) Crea un archivo de texto llamado mensaje_asimétrico.txt con un mensaje breve: tu nombre.



b) Genera un par de claves RSA (pública y privada). Para ello, usa el comando genpkey para generar la clave privada, y, a partir de esta, genera la clave pública. Obtendrás 2 archivos con extensión .pem

clave privada:

openssl genpkey -algorithm RSA -out clave_privada.pem -pkeyopt rsa_keygen_bits:2048

clave publica: openssl rsa -pubout -in clave_privada.pem -out clave_publica.pem

```
root@debian:/home/cristobal/clave_asimetrica# openssl rsa -pubout -in cla
ve_privada.pem -out clave_publica.pem
writing RSA key
root@debian:/home/cristobal/clave_asimetrica#
```

c) Cifra el archivo mensaje_asimétrico.txt usando la clave pública, generando un archivo que se llame mensaje_asimétrico_cifrado.txt.

openssl pkeyutl -encrypt -pubin -inkey clave_publica.pem -in mensaje_asimetrico.txt -out mensaje_asimetrico_cifrado.txt

```
oot@debian:/home/cristobal/clave_asimetrica# openssl rsautl -encrypt -pu
in -inkey clave_publica.pem -in mensaje_asimetrico.txt -out mensaje_asim
trico_cifrado.txt
he command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
oot@debian:/home/cristobal/clave_asimetrica# ls -l
otal 16
rw------- 1 root root 1704 oct 31 17:50 clave_privada.pem
rw-rw-r-- 1 root root  451 oct 31 17:51 clave_publica.pem
rw-rw-r-- 1 root root  256 oct 31 17:54 mensaje_asimetrico_cifrado.txt
rw-rw-r-- 1 root root   10 oct 31 17:49 mensaje_asimetrico.txt
oot@debian:/home/cristobal/clave_asimetrica#
```

d) Descifra el archivo usando la clave privada, generando un archivo llamado mensaje_asimétrico_descifrado.txt

openssl pkeyutl -decrypt -inkey clave_privada.pem -in mensaje_asimetrico_cifrado.txt -out mensaje_asimetrico_descifrado.txt

```
root@debian:/home/cristobal/clave_asimetrica# openssl rsautl -decrypt -in
key clave_privada.pem -in mensaje_asimetrico_cifrado.txt -out mensaje_asi
metrico_descifrado.txt
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
root@debian:/home/cristobal/clave_asimetrica# ls -l
total 20
-rw------- 1 root root 1704 oct 31 17:50 clave_privada.pem
-rw-rw-r-- 1 root root  451 oct 31 17:51 clave_publica.pem
-rw-rw-r-- 1 root root  256 oct 31 17:55 mensaje_asimetrico_cifrado.txt
-rw-rw-r-- 1 root root   10 oct 31 17:56 mensaje_asimetrico_descifrado.tx
t
-rw-rw-r-- 1 root root   10 oct 31 17:49 mensaje_asimetrico.txt
root@debian:/home/cristobal/clave_asimetrica# cat mensaje_asimetrico_desc
ifrado.txt
Cristobal
root@debian:/home/cristobal/clave_asimetrica#
```

¿Por qué el cifrado asimétrico es más seguro para la transmisión de datos entre dos partes desconocidas?

Porque no hay que compartir la clave privada, solo es necesario distribuir la pública. En este caso hemos encriptado con la pública y desencriptado con la privada.

Ejemplo: "Francisco" me ha dado su clave pública para que yo pueda cifrar un mensaje solo para él y mandárselo. Una vez que le llega a "Francisco", el, con su clave privada lo desencripta. Solo él puede desencriptarla.

Otra función sería la de "**no repudio**": Usas tu propia clave privada para cifrar un mensaje, se lo mandas a alguien a quien le hayas dado tu clave pública. Al solo poder ser descifrado con esa clave, el destinatario sabe con certeza que eres tú y nadie más quien ha mandado ese mensaje.

¿Qué ventaja tiene este método en comparación con el cifrado simétrico?

Al necesitar dos claves, no es necesario compartir la clave privada (con la cuál certificas que eres tú quien encripta y envía el mensaje). Solo se comparte la clave pública, la cual solo permite al destinatario descifrar los mensajes del remitente.