

Taller de OpenSSL

Contenido

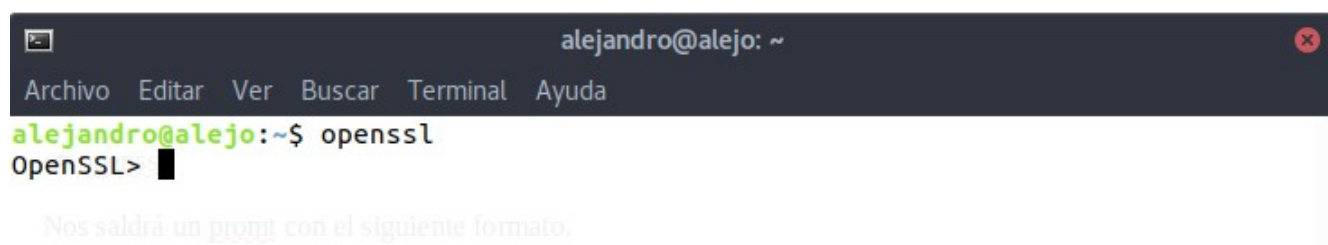
Introducción a openssl:.....	2
Uso de openssl:.....	2
Cifrado simétrico:.....	3
Cifrar.....	3
Descifrar:.....	4
Cifrado asimétrico.....	5
Generación de llaves:.....	5
Cifrar.....	7
Descifrar:.....	8
Practica recomendada:.....	9

Introducción a openssl:

OpenSSL es un proyecto de software libre que provee un conjunto de herramientas para TSL, (Transport Layer Security) y SSL (Secure Sockets Layer). También provee una librería de criptografía de propósito general y que es el objeto de este taller.

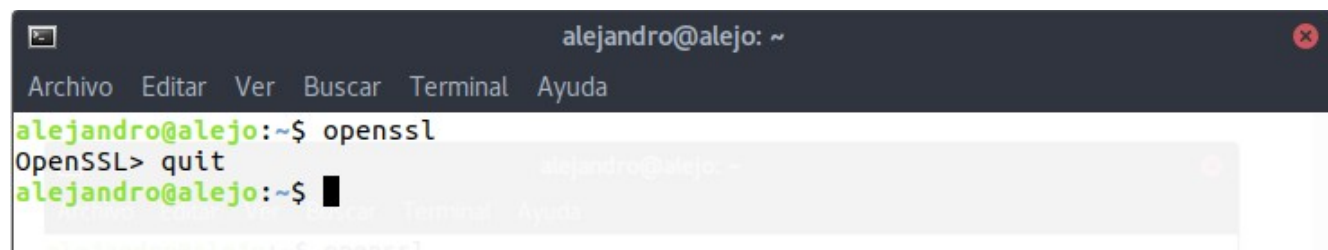
Uso de openssl:

Acceder a openssl:



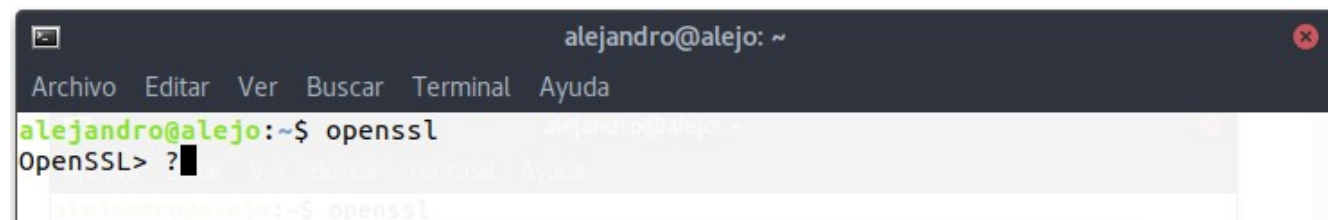
```
alejandro@alejo: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
alejandro@alejo:~$ openssl  
OpenSSL>   
  
Nos saldrá un promt con el siguiente formato,
```

Salir de openssl:



```
alejandro@alejo: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
alejandro@alejo:~$ openssl  
OpenSSL> quit  
alejandro@alejo:~$
```

Ayuda:



```
alejandro@alejo: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
alejandro@alejo:~$ openssl  
OpenSSL> ?  
alejandro@alejo:~$ openssl
```

Nos mostrará una lista de los comandos disponibles.

```
alejandro@alejo: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Standard commands
asn1parse      ca              ciphers         cms
crl            crl2pkcs7      dgst            dh
dhparam        dsa            dsaparam        ec
ecparam        enc            engine          errstr
gendh          gendsa         genpkey         genrsa
nseq           ocs            passwd          pkcs12
pkcs7          pkcs8          pkey            pkeyparam
pkeyutl        prime          rand            req
rsa            rsautl         s_client        s_server
s_time         sess_id        smime           speed
spkac          srp            ts              verify
version        x509

Message Digest commands (see the 'dgst' command for more details)
md4            md5            rmd160          sha
sha1

Cipher commands (see the 'enc' command for more details)
aes-128-cbc    aes-128-ecb    aes-192-cbc    aes-192-ecb
aes-256-cbc    aes-256-ecb    base64          bf
bf-cbc         bf-cfb         bf-ecb          bf-ofb
camellia-128-cbc camellia-128-ecb camellia-192-cbc camellia-192-ecb
camellia-256-cbc camellia-256-ecb cast            cast-cbc
```

Cifrado simétrico:

Cifrar

Para cifrar vamos a usar un archivo con el siguiente contenido:

```
alejandro@alejo: ~/practica_openssl
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

nano 2.6.3      Archivo: entrada.txt

Un archivo para cifrar en la práctica de openssl
Para cifrar vamos a usar un archivo con el siguiente contenido:
```

DES:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> enc -des -in entrada.txt -pass pass:miClave -out salidaDes.txt
```

el resultado:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
nano 2.6.3 Archivo: salidaDes.txt
Salted__  
OpenSSL> enc -des -in entrada.txt -pass pass:miClave -out salidaDes.txt
```

AES:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> enc -aes128 -in entrada.txt -pass pass:miClave -out salidaAES.txt
OpenSSL>
```

el resultado:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
nano 2.6.3 Archivo: salidaAES.txt
Salted__  
fS^DmK33u`^TdE
```

Descifrar:

DES:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> enc -d -des -in salidaDes.txt -pass pass:miClave -out descifradoDES.txt
OpenSSL> █
```

el resultado:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
nano 2.6.3 Archivo: descifradoDES.txt
Descifrar:
Un archivo para cifrar en la práctica de openssl
```

AES:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> enc -d -aes128 -in salidaAES.txt -pass pass:miClave -out descifradosAES.txt
OpenSSL> █
```

el resultado:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
nano 2.6.3 Archivo: descifradosAES.txt
Descifrar:
Un archivo para cifrar en la práctica de openssl
```

Cifrado asimétrico

Generación de llaves:

Generar llave del algoritmo asimétrico RSA: Vamos a generar una llave privada de 1020 bits

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> genrsa -out privada1.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
OpenSSL> █
```

Resultado:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
nano 2.6.3 Archivo: privada1.key
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDG5Ui/jsHUGx83704WwvdmYlv1nF64FT7jGaaPe1N2e6i0fCsI
/ss+yPU4zMZP09drMathA9GPSPUpl98+Aj00n919Q3kBPn7cXQGV/ENnExD3SwoT
uSxI6hPeIHSaWwsQKs8qsU2It6ofPg0fLE/G0AozRl4MTgT/L+1J552sIQIDAQAB
AoGACn9d0ZfqV7ysksmzvuwQyrvQLyp2dnFYJvk/lN2gF/VFYGe25Hv0S8UvpPRQ
9lY3ghXF9GB+ZJo6x0fw4PfUuy7z7kiJ5a2mwr0+mGLZoTms0y0tmd9us0y9reda
havDYJmN8odLKU37Yj8THR9h/xacX/SnM70lHbwLPZbbBgECQQD/VIqtqz4q7mwg
d6hbATajBx9xQbLrAHP/kBMf3r02bhSLGrQDRgCwG11v2jhw6ep0r9k4FgC1wVIW
ou7fvAaJAKEAx2rYgiTjWRTeVxJVU+6xKIaWpLGymS0f3UDs1T7vilbR572hpmQL
yNxXyYlTZ+DjchqhTbkJhwXfa7eKGPkS2QJAbWafz+ltriLAOuBHRESuzQN+GpwU
MssM5csoBhz6XNinADE+KTDRlp8CVanbPJATiQWXPYlfYHyh14SQY1M+UQJABDrB
6NC7ebI1nQcohCU14LQqEcgrD5Bv3ZN48nTotoxs20tsWEkbfA0gV4fwGu3sJQCU
1z8rco+vU2uLJEhQ0QJASRC/fl9BLZGpXEaX0TAKnAlS9EEDjHn7huJ2qdBaSoEa
XPXyYllHFnzYhwFjUTFvJWo7+fC0hqw3Nq6dj4uGxMg==
-----END RSA PRIVATE KEY-----
```

Cifrar la clave privada con DES para evitar su uso fraudulento:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> genrsa -out privada2.key -passout pass:miClave -des 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
OpenSSL> █
```

Resultado:


```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
nano 2.6.3 Archivo: privada2.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,A916BF908F473D02
VNWFYHailk90DHfJG5QS8nhpc/xMKVf3NZoSamrcBGcaCdQFA990mfJxGh+xARK/
Ks2Wb7wVhzErXs/USv6Rrs0VNNHdbt7P/UDqfHeoskci6HhZKghI1WoEL5SwBCBg
HiTvGbzmFYfOMW6rMMxGIqX6w+rXpy7ICLV2wtUwcdGug4kqm2NuJ7hGpXi9mX75
Jh0iKprFJhW7Grpum1svLbRJhZpuU78lZp8LLdtlZE6q678SWatso1RePRCTEwaLZ
8ENcWswRCB9GLEsQsz9kPaHjhV3uP15jeCXeckYx0y0TWEEH50wfPQcfXW2IJWn7
oCqvMvUI511nD0IcCX/8I8dYt2BMk3AEi+T9vaSKzcX5EOY4epdf+9MfmK7/00QP
i/TD5WiJ0CPMSm/MaW4EEcCg/fSaxqtbcJtt50QapVBNZ3/pLQ92z+jDh+tt1qlU
D1Yu3HVEQaH/KnsqACNbyDkkfln06UWGRpP/7ZrFeuDEcWGqMa+YZpMWjiDKfFgL
9VNdtxFX+vRDs08UewjK6kwozEqFeT19IQPgs5ovntvaEg9Z+nkDjwVXUE3Y83p
tQgfPsrkbs0t1V7kUcU5skk2Kxkv27biBSbQ12QdHiYsM5M5OR1cnZ1RIT0R3XYa
10jQfuXt0V6KRMcLOZn9ArBpAR1u8ZP9gq5rNY1UoJJkUMCgMnI2I8kp5vtXZ5BT
KBXMMxLTGVhvzQL7rM183AK2eY8kuCdu+jlZN3i+RGjipF+/FGsCnDr5B6sV4lrB
fTATYIUwMOJ0NE4FFLKuRvcNiSZVJ5QXclaf8F7YlqZf3eZm9f98mw==
-----END RSA PRIVATE KEY-----
```

Se realiza este cifrado porque la clave privada se genera como un fichero de texto que cualquiera podría leer, para evitar esto la ciframos.

Generar claves públicas derivadas:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> rsa -in privada1.key -pubout -out publica1.key
writing RSA key
OpenSSL> rsa -in privada2.key -pubout -out publica2.key -passin pass:miClave
writing RSA key
OpenSSL> █
```

Cifrar

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> rsautl -pubin -encrypt -in entrada.txt -out salidaRSA.txt -inkey publica1.key
OpenSSL> █
```

Resultado:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
nano 2.6.3 Archivo: salidaRSA.txt
U!^U;r01^Y00,0z00^LR?;U0'00^G0fu00d^Ew0!00)|00^@^_A0^R0Q-lp0^V0I0B0ZY0s00^S0^]Lr1$
^Q0^ER-00wp00K^G000$0n
```

Descifrar:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> rsautl -decrypt -in salidaRSA.txt -out descifradoRSA.txt -inkey privada1.key
OpenSSL> █
```

Resultado:

```
alejandro@alejo: ~/practica_openssl
Archivo Editar Ver Buscar Terminal Ayuda
nano 2.6.3 Archivo: descifradoRSA.txt
Un archivo para cifrar en la práctica de openssl
alejandro@alejo:~/practica_openssl$ openssl
OpenSSL> rsautl -decrypt -in salidaRSA.txt -out descifradoRSA.txt -inkey privada1.key
█
```


Practica recomendada:

1. Genere un archivo que contenga información acerca de los integrantes del grupo, la información debe contener:
 - Código del estudiante.
 - Nombre completo.
 - Cita de algún personaje histórico con el que se identifique.
 - Texto de la cita.
 - Nombre del personaje.
2. Cifre el archivo usando RSA según se indico en el ejemplo, usando una llave privada cifrada.
3. Intercambie los archivos exclusivamente necesarios con otro grupo para intercambiar dicha información. (justifique que archivos compartió)
4. Relacione la información referida por el otro grupo.