



Módulo 2.2 La secrecía de la información

Actividad Práctica: Aplicaciones criptográficas.

Cursante (nombre completo):

Objetivo:

- Conocer distintas aplicaciones de los algoritmos criptográficos.

Material y equipo necesario:

- Máquinas virtuales (proporcionadas en la carpeta de materiales en Classroom).

Aspectos a considerar:

Realizará una serie de actividades referentes a temas de criptografía, en varios casos se le solicitará que agregue capturas de pantalla por lo cual se le pide que por favor agregue las capturas lo más legible posibles y en donde solo se visualice la parte del ejercicio solicitado.

Para un correcto llenado de su práctica favor de utilizar el visualizador de archivos Adobe Acrobat Reader DC o Foxit Reader, evite usar Google docs. para la edición ya que éste modifica la estructura del archivo.

Actividad 1: Creación de script (Usar máquina virtual Cliente)

Cree un script en el lenguaje de programación de su preferencia, el cual debe realizar el método de cifrado y descifrado , tanto para un algoritmo simétrico moderno (DES, 3DES o AES) como para un algoritmo asimétrico (RSA o ELGAMMAL), esto es, deberá realizar la programación de ambos algoritmos, y que el script sea capaz de cifrar y descifrar cualquier tipo de archivo.



Debe comentar todas las líneas que contenga su script, lo que realice cada función o módulo utilizado si es el caso.

Debe considerar todos los posibles errores que este pueda generar y evitar que sean visualizados por el usuario, es decir, en caso de que no se encuentre el archivo a cifrar el programa debe mostrar un mensaje personalizado y no el mensaje de error que se da por defecto.

En el siguiente recuadro coloque una captura de pantalla en donde se visualice el uso de su programa para el cifrado.

En el siguiente recuadro coloque una captura de pantalla en donde se visualice el uso de su programa para el descifrado.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Debe entregar tanto el script como el archivo utilizado para el cifrado y descifrado colocado en las capturas anteriores.

Actividad 2: Creación de sitio web (Usar máquina virtual Cliente)

Debe realizar un sitio web sencillo en donde se explique el funcionamiento del script creado en la actividad 1, considere que será un sitio de carácter informativo para que otro usuario pueda hacer uso correcto de su programa, por lo cual debe considerar colocar la información que usted considere necesaria a fin de que quede lo más claro posible.

En el siguiente recuadro coloque una captura de pantalla donde se visualice su sitio web

Actividad 3: Búsqueda de archivo y conexión por SSH mediante certificados (Usar máquina virtual Cliente y Servidor)

Busque un archivo cuyo nombre sea el resultado de obtener el hash de la palabra «Criptografía». El archivo está en la máquina cliente.

El hash que debe usar es aquel que fue revisado y actualizado en 1995 y fue publicado como FIPS 180-1, ¿De qué hash se está hablando?

Utilice el hash de la respuesta anterior para obtener el nombre del archivo a buscar, ¿Cuál es el resultado al obtener el hash de la palabra «Criptografía»? Coloque una captura de pantalla de su procedimiento. Tenga mucho cuidado en escribir correctamente los caracteres.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Busque un archivo cuyo nombre sea el resultado obtenido anteriormente, este debe ser un archivo oculto con extensión jpg. Coloque en el recuadro siguiente el proceso utilizado.

Visualice la imagen, puede hacer uso del comando *shotwell «nombre del archivo»*

¿Ve algo raro en ella? En el siguiente recuadro escriba su propia definición de Esteganografía.

La imagen encontrada previamente fue sometida a esteganografía por lo cual debe conseguir el texto oculto. Para eso, se hará uso del comando *steghide* y una contraseña se podrá obtener el texto.

La contraseña es la contraseña número 29 de las contraseñas más utilizadas del año 2020

Ejecute el comando: *steghide extract -sf «nombre del archivo»* al ejecutarlo le pedirá una contraseña ingrese la correspondiente.

El archivo encontrado es un certificado, visualice dicho certificado con el comando *«ssh-keygen -Lf nombre del certificado»*

Como podrá darse cuenta el certificado esta expirado, por lo cual debe crear un nuevo certificado para conectarse, pero lo hará desde un nuevo usuario.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Lo primero que debe hacer, es crear un usuario en el **servidor**, el cual debe estar compuesto por la primera letra de su nombre y su apellido paterno completo, es decir si su nombre es Patricia Flores su usuario debe ser **pflores**. Para crear su usuario haga uso del comando *sudo adduser «nombre de usuario»*

- **Creación de certificados.**

En la máquina **cliente**, cree un par de claves, para eso primero verifique que su usuario tenga el directorio **.ssh**, para esto posíñese en el directorio home de su usuario con el comando *cd /home/«nombre de usuario»* para visualizar qué archivos se encuentran en dicho directorio, ejecute el comando *ls -a* , se hace uso de este comando ya que el directorio **.ssh** es un directorio oculto, y el **-a** permite visualizar los archivos y directorios con estas características.

Como se observa, el directorio **.ssh** no se encuentra, por lo cual se crea con el comando **«mkdir .ssh»** y finalmente se muestra nuevamente que el directorio ya se encuentra.

Si usted si cuenta con este directorio, omita lo anterior.

La creación de las claves las puede realizar con el comando **«ssh-keygen -t rsa -b 4096 -C ssh_usuario -f /home/usuario/.ssh/usuario_key»** donde, **-t** indica el tipo de cifrado a usar, en este caso RSA, **-b** la longitud de las claves, en este caso será de 4096 bits, **-C** es un comentario, se recomienda colocar el nombre de usuario, y por último **-f**, donde además de indicar la ruta a seguir para guardar las claves en el directorio **.ssh**, se coloca el nombre con el que se van a guardar. En este caso como ya se encuentra en el directorio **.ssh** solo basta con indicar el nombre del archivo, es decir **«ssh-keygen -t rsa -b 4096 -C ssh_usuario -f usuario_key»**

Si se omite la opción **-f** las claves se crearán por defecto en el directorio **.ssh** con los nombres *id_rsa* y *id_rsa.pub*.

En la Figura N° 1 se muestra la creación de las claves para el usuario **twellick**,

ATENCIÓN: Cuando cree las claves se le pedirá una contraseña (Passphrase) esta es la que protege a sus claves, por lo cual **NO** la olvide.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

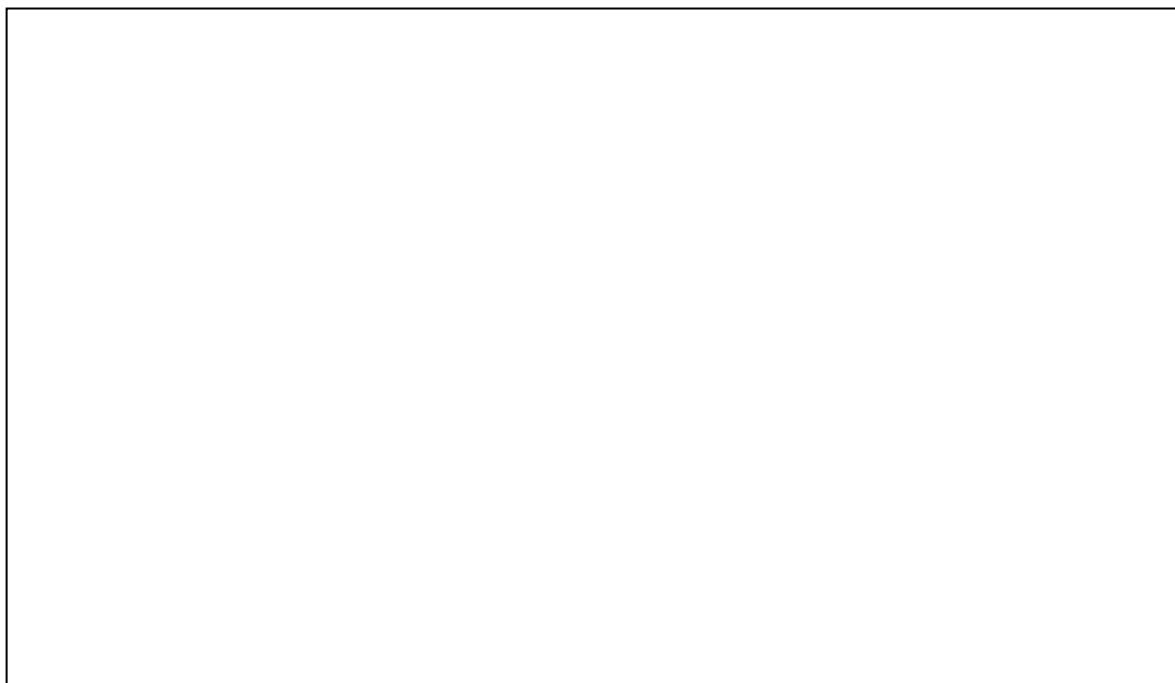
CiberSEG
Diplomado en Ciberseguridad



```
twellick@crypto:~/.ssh$ ssh-keygen -t rsa -b 4096 -C ssh_twellick -f twellick_key
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in twellick_key.
Your public key has been saved in twellick_key.pub.
The key fingerprint is:
SHA256:79HGeQ10f+XPkDeI+r6cnWFvyvTGG8LgaWy6oloI6u4 ssh_twellick
The key's randomart image is:
+---[RSA 4096]----+
|          .         |
|          .         |
|          .         |
|          S . o o   |
|          .oo++ *+  |
|          . . . o*o*B*|
| . . o . .+o +==#  |
|=E . . . .oo .=%0  |
+---[SHA256]-----+
twellick@crypto:~/.ssh$
```

Figura N° 1: El cliente crea sus nuevas claves

Coloque una captura de pantalla en donde se visualice la creación de sus claves.



Ahora, el **cliente** debe enviar la clave que puede compartir con el **servidor**, para eso haremos uso de **netcat**, un comando que nos permite realizar un pequeño canal de comunicación cliente-servidor, pero también nos permite intercambiar archivos, esto puede suceder siempre y cuando se encuentren en la misma red.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Para esto debe saber cuál es la IP del servidor, puede verificarlo con el comando *ip add* tal como se muestra en la Figura N° 2:

```
elliottcrypto:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:94:62:b3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.133.140/24 brd 192.168.133.255 scope global dynamic noprefixroute ens33
        valid_lft 1665sec preferred_lft 1665sec
    inet6 fe80::20c:29ff:fe94:283/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
elliottcrypto:~$
```

Figura N° 2: Revisión de IP del equipo.

En el siguiente recuadro coloque la IP del cliente y su servidor.

IP máquina Cliente

IP máquina Servidor

En el servidor se encuentra un directorio en el home de *darllene* llamado *CUsuarios*, aquí coloque la clave que será compartida.

Para hacer el intercambio del archivo con la clave, **el servidor** (*darllene*) quien será el **receptor** abrirá el canal de comunicación, para eso debe ejecutar: «*nc -l -p N° de puerto > nombre a guardar el archivo*»

Por su lado **el cliente** quien será el *emisor* debe ejecutar: «*nc ip del servidor -q 0 N° de puerto < nombre del archivo a enviar*»

El proceso se muestra en la Figura N° 3:

```
darllene@crypto:~/CUsuarios$ nc -l -p 1707 > twellick_key.pub
darllene@crypto:~/CUsuarios$ ls -la
total 12
drwxr-xr-x  2 darllene darllene 4096 May 11 01:18 .
drwxr-xr-x 16 darllene darllene 4096 May 10 21:41 ..
-rw-r--r--  1 darllene darllene  738 May 11 01:18 twellick_key.pub
darllene@crypto:~/CUsuarios$
```



```
twellick@crypto:~/.ssh$ nc 192.168.133.141 -q 0 1707 < twellick_key.pub
twellick@crypto:~/.ssh$
```

Figura N° 3: Conexión mediante netcat entre servidor y cliente



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Ahora, el **servidor** debe firmar la clave pública del cliente, esto se realiza con el comando:
«`ssh-keygen -s clave_privada_del_servidor -I ID_usuario -V tiempo_de_vida_para_el_certificado -n Usuario clave_pública_del_usuario`»

En donde, **-s** indica la clave privada del servidor, **-I** es un ID para identificar el certificado, puede usar algún alias, **-V** indica el periodo de tiempo en que el certificado será válido, en **-n** se indica el usuario que hará uso de este certificado, en este caso *twellick* y la clave pública de dicho usuario.

La creación del certificado puede visualizarla en la Figura N° 4, en este caso al certificado se le dio una validez de 30 días.

```
darllene@crypto:~/C Usuarios$ ssh-keygen -s ../../ssh/darllene_key -I user_twellick -V +30d  
-n twellick twellick_key.pub  
Enter passphrase:  
Signed user key twellick_key-cert.pub: id "user_twellick" serial 0 for twellick valid from 2021-05-11T01:30:00 to 2021-06-10T01:31:14  
darllene@crypto:~/C Usuarios$
```

Figura N° 4: Conexión mediante netcat entre servidor y cliente

Ahora, el servidor debe regresar el certificado al cliente, ¿De qué manera lo realizaría? Describa el proceso en el siguiente recuadro

NOTA: El cliente debe tener alojado el certificado en el mismo directorio en donde se encuentren sus claves pública y privada.

La clave pública del servidor debe encontrarse en el directorio /etc/ssh/ del servidor, realice la copia de dicho archivo, para lo cual debe realizarlo con permisos de administrador, el comando sería: «`sudo cp archivo /etc/ssh`» tal como se muestra en la Figura N° 5

```
darllene@crypto:~/.ssh$ sudo cp darllene_key.pub /etc/ssh  
darllene@crypto:~/.ssh$ ls -la /etc/ssh/darllene_key*  
-rw-r--r-- 1 root root 738 May 11 23:06 /etc/ssh/darllene_key.pub  
darllene@crypto:~/.ssh$
```

Figura N° 5: Copia de certificado de cliente a directorio /etc/ssh

Ahora, el **servidor** debe realizar algunas modificaciones para que el cliente logre conectarse haciendo uso del certificado.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



El archivo de configuración de SSH es `/etc/ssh/sshd_config`, se debe realizar una copia de este archivo, ya que, si se llega a cometer algún error, se tendrá un respaldo disponible. Puede copiarlo en el mismo directorio, y solo agregando al final del nombre del archivo, la fecha en que se realizó la copia.

Ahora, se realizan las modificaciones al archivo `sshd_config`, ingresando a él, la edición la debe realizar como administrador por lo cual debe anteponer `sudo`, e indicar el editor a usar, es decir debe usar el comando «`sudo vim/nano sshd_config`»

Las modificaciones que encontrará ya realizadas son:

PasswordAuthentication: Se coloca en **no**, esto evitará conexiones mediante credenciales, es decir, el uso de una contraseña.

PermitRootLogin: Se coloca en **no**, para evitar ataques de fuerza bruta y que usuarios no autorizados quieran ingresar. De esta manera se bloquea la opción para ingresar ya sea con usuario y contraseña o con claves asimétricas.

PubKeyAuthentication: Se coloca en **yes**, para permitir el inicio haciendo uso de claves o certificado.

AllowUser: Para asegurar que los usuarios tienen permiso de ingresar al servidor, se crea una lista blanca, esto quiere decir, que se colocan los nombres de los usuarios permitidos, estos deben encontrarse separados por un espacio.

TrustedUserCaKeys: Aquí, se debe indicar la ruta en donde se encuentra la clave pública del servidor, ya que esta es la que verificará si el certificado usado para realizar la conexión es válido.

Tal como se muestran en la Figura N° 6

Realice las modificaciones pertinentes y guarde el archivo, ejecute «`sudo service ssh reload`», esto para que se guarden los cambios que acaba de realizar. Revise que el nombre del usuario lo ingresa correctamente, así como las demás configuraciones para evitar errores al realizar la autenticación.

Adicionalmente se le pide que cambie el número de puerto por otro, este debe ser distinto al rango de puertos bien conocidos.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



```
PermitRootLogin no
PubkeyAuthentication yes

# To disable tunneled clear text passwords, change to "no"
PasswordAuthentication no
#PermitEmptyPasswords no

#Usuarios permitidos
AllowUsers elliot twellick

#Clave pública del servidor
TrustedUserCAKeys /etc/ssh/darlene_key.pub
```

Figura N° 6: Configuraciones en sshd_config

Describa en el siguiente recuadro cuales fueron las modificaciones realizadas y por qué se realizaron.

Con las modificaciones que acaba de realizar, **el cliente** podrá ingresar al **servidor**. Como el puerto cambió, se debe especificar el puerto en la línea de comandos, es decir: «*ssh -i ruta_de_clave_privada usuario@IP_Servidor -p puerto*»

Ingrese una captura de pantalla donde se visualice de la conexión realizada.

En el servidor, puede checar el archivo *auth.log*, localizado en el directorio */var/log*. El archivo, es un archivo en donde se muestran todos los inicios de sesión o intentos de inicio al servidor, puede consultarla ya sea con *cat*, *more* o *less*, El comando completo usando *cat* es: «*sudo cat /var/log/auth.log*»



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



En la Figura N° 7, puede visualizar el fragmento de archivo *auth.log*, donde se indica que el usuario **twellick** inicio sesión haciendo uso de su certificado y las comparaciones con el certificado para validar que es el mismo.

```
twellick@crypto:~/ssh$ ssh-keygen -Lf twellick_key-cert.pub
twellick_key-cert.pub:
    Type: ssh-rsa-cert-v01@openssh.com user certificate
    Public key: RSA-CERT SHA256:79HGeQ10f+XPkDe1+r6cnWFvyvTGG8LgaWy6oloi6u4
      Signing CA: RSA SHA256:S0imQVomRsBG9WAqEmvhLRDqr5S66MLrHrvScBt0Ys
    Key ID: "user_twellick"
    Serial: 0
    Valid: from 2021-05-11T01:30:00 to 2021-06-10T01:31:14
    Principals:
        twellick
    Critical Options: (none)
    Extensions:
        permit-X11-forwarding
        permit-agent-forwarding
        permit-port-forwarding
        permit-pty
        permit-user-rc

May 11 23:23:22 crypto sshd[2509]: Accepted publickey for twellick from 192.168
.133.140 port 52016 ssh2: RSA-CERT SHA256:79HGeQ10f+XPkDe1+r6cnWFvyvTGG8LgaWy60
loiu4 ID user_twellick (serial 0) CA RSA SHA256:S0imQVomRsBG9WAqEmvhLRDqr5S66
MLrHrvScBf0Ys
May 11 23:23:22 crypto sshd[2509]: pam_unix(sshd:session): session opened for u
ser twellick by (uid=0)
May 11 23:23:22 crypto systemd-logind[421]: New session 21 of user twellick.
May 11 23:23:22 crypto systemd: pam_unix(systemd-user:session): session opened
for user twellick by (uid=0)
May 11 23:23:28 crypto sudo: darllene : TTY=pts/1 ; PWD=/home/darllene ; USER=r
oot ; COMMAND=/usr/bin/cat /var/log/auth.log
May 11 23:23:28 crypto sudo: pam_unix(sudo:session): session opened for user ro
ot by (uid=0)
```

Figura N° 7: Uso de certificado para la conexión mediante SSH

En el siguiente recuadro coloque una captura de la comparativa de la conexión tal como se realizó en la figura N° 7, debe entregar el certificado obtenido para realizar la conexión.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Y, ¿Qué paso con el usuario Elliot? ¿Puede o no realizar la conexión?

Intente realizar la conexión del usuario Elliot al servidor, ¿La conexión se realizó con éxito?
Coloque una captura de pantalla en donde se visualice si se realizo o no la conexión.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Módulo 2.2 La secrecía de la información

¿Por qué sucedió lo anterior? Explíquelo en el recuadro de abajo

Actividad 4: Certificado en sitios web (Usar máquina virtual Cliente y Servidor)

Un sitio con el acrónimo HTTPS crea más confianza en los usuarios que uno con simplemente HTTP por lo cual la creación de certificados HTTPS en los últimos días se ha vuelto sumamente importante.

La creación de un certificado se realiza cuando una autoridad certificadora firma con su clave privada una clave pública de su cliente, siempre y cuando tenga plena confianza en él, tal como sucedió en la actividad pasada.

Sin embargo, de tal modo que la creación de certificados sea más seguro, el firmar se compone de: la autoridad certificadora raíz, es un equipo aislado que se encarga de designar a una autoridad intermedia a la firma de los certificados finales, creando así una cadena de confianza, así si en algún momento la autoridad intermedia se ve comprometida, la autoridad raíz elimina dicha confianza y se crea una nueva autoridad intermedia.

En esta actividad va a crear el certificado para su sitio web, creado en la Actividad 2, esto debe realizarlo en la máquina cliente con el usuario que crearon en la actividad anterior, ya que la máquina servidor es la autoridad intermedia.

El proceso es el siguiente: Los tres componentes: ca raíz, ca intermedia y sitio web deben crear un par de claves y el certificado en esta ocasión se realizará usando OpenSSL, pero cada una con su archivo correspondiente, como usted solo creará las claves para su sitio debe modificar el archivo openssl.cnf en donde colocará el nombre de su sitio, este será su nombre de usuario tal como lo creo en la actividad 3, es decir primera letra del nombre con el apellido, seguido del dominio *dipciber.unam.mx*, es decir quedaría www.twellick.dipciber.unam.mx

El archivo openssl se encuentra en el directorio */sitio_web*



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Antes de crear las claves y el certificado cree un directorio en donde alojara las claves y los archivos creados, para los ejemplos se crea el directorio *web_twellick* y dentro de este directorio cree los directorios *private*, *cert* y *csr*. Al directorio *private* cambie los permisos de modo que solo el dueño del archivo tenga todos los permisos, del mismo modo, copie el archivo *openssl.cnf* al directorio creado, en este caso a *web_twellick*

El directorio se vería algo como lo mostrado en la Figura N° 8

```
twellick@crypto:~/web_twellick$ ls  
certs  csr  openssl.cnf  private  
twellick@crypto:~/web_twellick$
```

Figura N° 8: Directorio creado para realización de claves y certificado

Para crear sus claves utilice el siguiente comando:

```
openssl genrsa -out private/SITIO_USUARIO.key.pem 4096
```

Donde la palabra USUARIO debe cambiarla por su correspondiente usuario y SITIO por el nombre de su sitio, el resultado será algo parecido a lo mostrado en la Figura N° 9, aquí se está creando una clave de tipo RSA de 4096 bits que se guarda en el directorio *private*

```
twellick@crypto:~/web_twellick$ openssl genrsa -out private/www.twellick.dipcibe  
r.unam.mx_twellick.key.pem 4096  
Generating RSA private key, 4096 bit long modulus (2 primes)  
.....++++  
.....  
.....  
.....  
.....  
.....  
e is 65537 (0x010001)  
twellick@crypto:~/web_twellick$
```

Figura N° 9: Creación de claves

Ahora, debe crear la solicitud de firma del certificado, para eso antes debe modificar algunas líneas en el archivo *openssl.cnf*, las líneas a modificar son las mostradas en la Figura N° 10



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



```

[ CA_default ]
# Directory and file locations.
dir          = /certificado_server
certs        = $dir
crl_dir      = $dir
new_certs_dir = $dir
database    = $dir/index.txt
serial       = $dir/serial
RANDFILE     = $dir/private/.rand

# The root key and root certificate.
private_key   = $dir/www.usuario.dipciber.unam.mx.key.pem
certificate   = $dir/www.usuario.dipciber.unam.mx.cert.pem

```

Figura N° 10: Líneas a modificar el archivo openssl.cnf

En donde *dir* debe cambiarlo por la ruta absoluta del directorio que creo, y *private_key* y *certificate* solo debe cambiar usuario por su nombre de usuario, guarde los cambios realizados.

Ahora sí, para crear la solicitud de firma de certificado debe ejecutar lo siguiente:

```
openssl req -config openssl.cnf -key private/SITIO_USUARIO.key.pem -new -sha256 -out
               csr/SITIO_USUARIO.csr.pem
```

El resultado debe ser algo parecido a lo mostrado en la Figura N° 11:

```

twellick@crypto:~/web_twellick$ openssl req -config openssl.cnf -key private/www
._twellick.dipciber.unam.mx_twellick.key.pem -new -sha256 -out csr/www.twellick.d
ipciber.unam.mx_twellick.csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [MX]:MX
State or Province Name [Mexico]:Mexico
Locality Name [Facultad de Ingenieria]:Facultad de Ingenieria
Organization Name [Diplomado en Ciberseguridad]:Diplomado en Ciberseguridad
Organizational Unit Name [Secrecia de la informacion]:Secrecia de la informacion
Common Name [www.usuario.dipciber.unam.mx]:www.twellick.dipciber.unam.mx
Email Address []:
twellick@crypto:~/web_twellick$ 
```

Figura N° 11: Creación de petición de firma para certificado



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Coloque en el siguiente recuadro una captura de su resultado parecido a la Figura N° 11:

Comparta su petición a la autoridad intermedia (*Servidor*), el servidor debe guardarla en el directorio *csr* ¿De qué manera enviará el archivo?

Ahora, la autoridad intermedia firmará y creará el certificado, para eso, el sitio web enviará su petición.

La autoridad intermedia hará uso del siguiente comando para realizar la firma:

```
openssl ca -config openssl.cnf -extensions server_cert -days 375 -notext -md sha256 -in  
csr/SITIO_USUARIO.csr.pem -out certs/SITIO_USUARIO.cert.pem
```

Recuerde cambiar INICIALES por las iniciales del usuario correspondiente y SITIO por el nombre de su sitio web, además le pedirá la contraseña, esta es: la contraseña es la contraseña número 11 de las contraseñas más usadas en el 2020 el resultado será como el mostrado en la Figura N° 12:



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



```

darllene@crypto:~/intermedia_darllene$ openssl ca -config openssl.cnf -extensions server_cert -days 375 -notext -md sha256 -in csr/www.twellick.dipciber.unam.mx_twellick.csr.pem -out certs/www.twellick.dipciber.unam.mx_twellick.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for /home/darllene/intermedia_darllene/private/intermedia_darllene.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 4096 (0x1000)
    Validity
        Not Before: May 14 05:11:00 2021 GMT
        Not After : May 24 05:11:00 2022 GMT
    Subject:
        countryName                = MX
        stateOrProvinceName         = Mexico
        localityName               = Facultad de Ingenieria
        organizationName           = Diplomado en Ciberseguridad
        organizationalUnitName      = Secceria de la informacion
        commonName                 = www.twellick.dipciber.unam.mx
X509v3 extensions:

```

Figura N° 12: Creación de certificado para sitio web

Del mismo modo puede verificar su certificado con el comando `openssl x509 -noout -text -in certs/SITIO_USUARIO.cert.pem`, el resultado se muestra en la Figura N° 13, donde vemos que darllene fue quien firmó el certificado y fue firmado para twellick.

```

Certificate:
Data:
    Version: 3 (0x2)
    Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = MX, ST = Mexico, O = Diplomado en Ciberseguridad, OU = "Secceria de la informacion ", CN = darllene
    Validity
        Not Before: May 14 05:11:00 2021 GMT
        Not After : May 24 05:11:00 2022 GMT
    Subject: C = MX, ST = Mexico, L = Facultad de Ingenieria, O = Diplomado en Cibers
eguridad, OU = Secceria de la informacion, CN = www.twellick.dipciber.unam.mx
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public-Key: (4096 bit)
        Modulus:
            00:bb:94:b5:5f:78:60:f9:98:83:9e:24:f7:3b:21:
            d0:8b:99:35:f7:9c:ff:29:36:f0:91:2e:33:0d:5f:
            18:33:01:1e:d1:68:f3:00:4c:1d:1b:f8:8d:1c:48:
            80:a1:25:7f:0d:12:57:8d:c9:bd:22:63:2b:51:d5:
            ba:4c:70:2f:17:e4:9a:96:38:fe:ea:9f:dc:af:f2:
            f2:99:ac:cb:84:42:0f:e6:89:a2:f9:13:d2:6a:6e:
            25:7f:e8:9a:59:0f:ae:f5:4b:2d:fe:11:ae:e6:fd:
            23:67:4c:d5:26:2e:a9:1e:23:ba:30:10:be:59:c4:
            62:cd:a2:51:80:e9:12:e3:ef:e7:1d:fb:cb:89:0b:
            1d:d1:b1:ff:8b:be:5f:ea:82:03:78:35:cd:5c:7d:
--More--

```

Figura N° 13: Verificación de sitio web



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Coloque una captura de pantalla donde se observe la información de su certificado tal como se muestra en la Figura N° 13



Así mismo puede verificar la confianza de su certificado, para esto debe usar el archivo *ca-chain.cert.pem* que se encuentra en el directorio *certs*, este archivo, representa la cadena de confianza que se creó entre la autoridad raíz (*mrobot*) y la intermedia (*darllene*), ejecute el comando: *openssl verify -CAfile certs/ca-chain.cert.pem certs/SITIO_USUARIO.cert.pem* recuerde cambiar STIO y USUARIO por los correspondientes a su caso.

Si existe confianza obtendrá como respuesta un *Ok* como se muestra en la Figura N° 14

```
darllene@crypto:~/intermedia_darllene$ openssl verify -CAfile certs/ca-chain.cert.pem certs/www.twellick.dipciber.unam.mx_twellick.cert.pem
certs/www.twellick.dipciber.unam.mx_twellick.cert.pem: OK
darllene@crypto:~/intermedia_darllene$
```

Figura N° 14: Verificación de confianza del certificado

El servidor debe enviar el certificado y el archivo *ca-chain.cert.pem* al sitio web para poder hacer uso de estos, el sitio debe guardar dichos archivos en su directorio *certs*.



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Uso del certificado en el sitio web.

Para hacer uso del certificado, se hará uso del servidor apache, por lo cual se deben realizar los siguientes pasos como superusuario:

1. Copiar todos los archivos `*.cert.pem` al directorio `/etc/ssl/certs`
2. Copiar el archivo `*.key.pem` al directorio `/etc/ssl/private`
3. Cambiar el propietario de los archivos anteriores por `root:ssl-cert`
4. Cambie los permisos para los archivos en el directorio `/etc/ssl/certs` de modo que queden: lectura y escritura para el dueño, y solo escritura para grupos y otros.
5. Cambie los permisos para los archivos en el directorio `/etc/ssl/private` de modo que queden: lectura y escritura para el dueño, solo escritura para grupos ningún permiso para otros.

Lo anterior debe quedar como se muestra en la Figura N° 15:

```
root@crypto:/etc/ssl# ls -la certs/*.cert.pem
-rw-r--r-- 1 root ssl-cert 4317 May 14 01:35 certs/ca-chain.cert.pem
-rw-r--r-- 1 root ssl-cert 2516 May 14 01:35 certs/www.twellick.dipciber.unam.mx_twellick.cert.pem
root@crypto:/etc/ssl# ls -la private/*.key.pem
-rw-r----- 1 root ssl-cert 3243 May 14 01:36 private/www.twellick.dipciber.unam.mx_twellick.key.pem
m
root@crypto:/etc/ssl#
```

Figura N° 15: Modificaciones para uso de certificado en sitio web

Ahora, debe realizar las modificaciones en el archivo de configuración de apache que es `/etc/apache2/sites-available/default-ssl.conf`, edítelo y agregue las siguientes líneas realizando las modificaciones pertinentes:

SSLEngine on

SSLCertificateFile ruta_donde_se_encuentra_el_certificado

SSLCertificateKeyFile ruta_donde_se_encuentra_la_clave_privada

SSLCertificateChainFile ruta_donde_se_encuentra_el_certificado_de_confianza



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Además, agregue:

ServerName *dominio_de_su_pagina_web*

Y de ser el caso, realice la modificación

DocumentRoot *ruta_de_los_archivos_de_su_página_web*

Al finalizar las modificaciones pertinentes en el archivo *default-ssl.conf* guarde el archivo y debe activar el módulo SSL, para esto, ejecute primero *su* – despues el siguiente comando:

a2enmod ssl

Debe activar el archivo de configuración *default-ssl.conf*, para esto ejecute:

a2ensite default-ssl.conf

Finalmente aplicar los cambios con el comando: *systemctl reload apache2*

Ahora, edite el archivo */etc/hosts* y agregue la IP de su servidor, o bien solo coloque la *IP 127.0.0.1* seguido del dominio de su sitio, esto para que pueda ver su página web en el navegador. La línea debe quedar:

Ejemplo: 127.0.0.1 www.twellick.dipciber.unam.mx

Guarde el archivo con los cambios.

Reinic peace nuevamente el servidor para guardar los cambios, para esto tambien puede ejecutar el comando: */etc/init.d/apache2 restart*

Importe el certificado en el navegador, para evitar que se indiquen problemas con su sitio.

Para esto, en su navegador, en este caso Firefox, vaya a Preferencias → Privacidad y Seguridad → Certificados → Ver

Certificados → Autoridades → Importar

Y seleccione el archivo *ca_chain.cert.pem*, y seleccione la casilla Confiar en esta CA para identificar sitios web.

Cierre el navegador y vuélvalo a abrir para que se apliquen los cambios.

Intente ingresar a su sitio y debe poder realizarlo con éxito, el ejemplo se muestra en la Figura N° 16



Universidad Nacional Autónoma de México
Facultad de Ingeniería

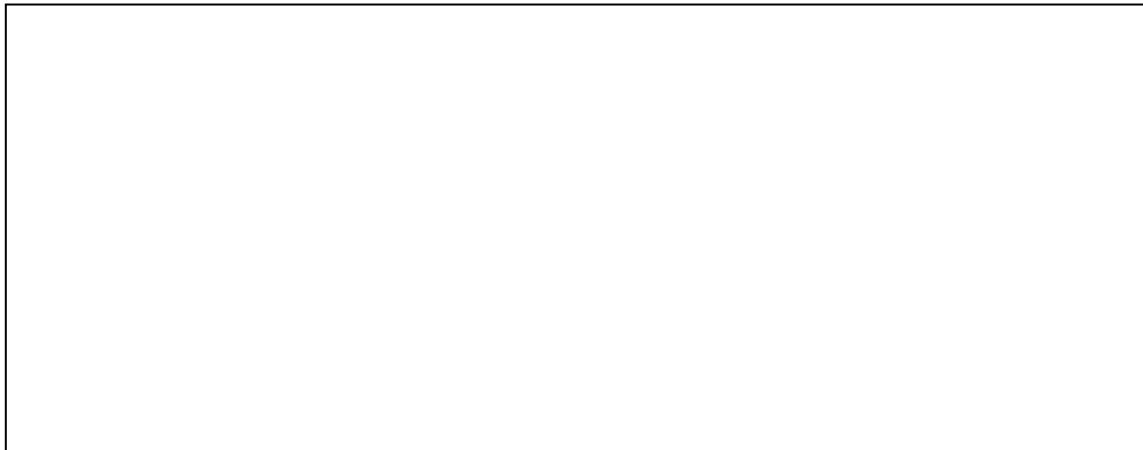
CiberSEG
Diplomado en Ciberseguridad





Figura N° 16: Uso de certificado en sitio web

Coloque una captura de pantalla en donde se visualice el uso del certificado en su sitio web



Al dar clic en el candado de aparece la opción de *ver los detalles de la conexión* y posteriormente *ver información*, esto le abrirá una nueva ventana, de clic en el botón que dice *Ver certificado* esto le abrirá una nueva pestaña en el navegador, en donde mostrará la información de su certificado, tal como se muestra en la Figura N° 17

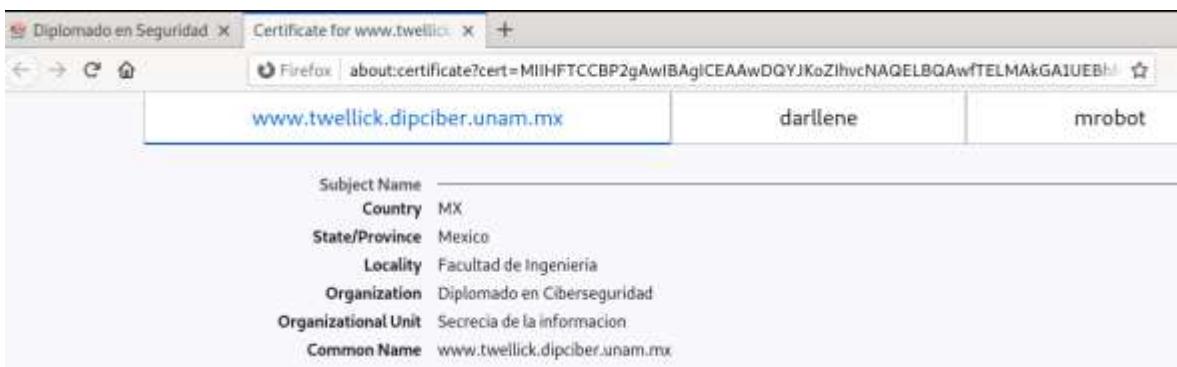


Figura N° 17: Detalles del certificado en sitio web



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Coloque una captura de pantalla en donde se visualice los detalles de su certificado en el sitio web. De esta actividad debe entregar el certificado usado en su sitio.

Actividad 5: Criptografía en la vida diaria.

Hasta ahora se han mostrado algunas formas de usar la criptografía en el día a día, pero ¿En dónde más podemos ver a la criptografía?

Llene el siguiente recuadro de 3 a 5 ejemplos del uso de la criptografía, en la vida diaria.

Ejemplo	Definición	Elementos de la criptografía



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Actividad 6: Entrega de práctica:

Para cada uno de los elementos a entregar debe realizar lo siguiente:

En un archivo .txt coloque nombre del elemento a entregar, obtenga el HASH SHA256 de cada uno de los elementos, teniendo en cuenta que es del elemento mas no del nombre de dicho elemento.

Lo puede realizar desde la máquina cliente con el comando *sha256sum nombre_del_archivo* coloque cada uno de los resultados hash, debe obtenerlo incluso de esta práctica.

Cifre el archivo .txt con el script que creo en la actividad 1, con el algoritmo simétrico utilizado, llama al archivo txt con el cifrado ROT13 de la contraseña utilizada, es decir si la contraseña es QWERTY obtenga el ROT13 de QWERTY y llame a su archivo de esa manera, tome en cuenta que para ROT13 solo se utiliza el alfabeto, esto tambien lo puede hacer desde la máquina cliente, utilizando el comando *echo contraseña / rot13*



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad



Los elementos a entregar son:

- Script de actividad 1
- Archivo que uso para cifrar y descifrar en actividad 1
- Certificado utilizado para conexión en actividad 3
- Certificado utilizado en sitio web actividad 4
- Archivo pdf de la práctica
- Archivo txt cifrado que contiene los hash de los archivos mencionados anteriormente.

CONCLUSIÓN

1. ¿Qué es la criptografía?

2. ¿Cuál es la diferencia entre la criptografía simétrica y asimétrica?

3. ¿Cuáles son sus aprendizajes generales con esta práctica?



Universidad Nacional Autónoma de México
Facultad de Ingeniería

CiberSEG
Diplomado en Ciberseguridad

