Anexo de la Unidad 2: Criptografía

Objetivo:	El alumnado aplicará aplicaciones de software integrando algoritmos criptográficos para mantener la confidencialidad de la información.
Modalidad:	**Individual**
Descripción:	1.- Analiza y comprende la información sobre la unidad temática Criptografía **(saber 2 puntos),** realizando el Quiz de conocimientos mediante la plataforma institucional. Curso de DH-Seguridad Informática ING con su usuario y contraseña de la plataforma elearning.utng.edu.mx 2. Los alumnos y las alumnas deberán agregar en /var/www/html/u_su_numero_control el software (entregado por el profesor) y la **firma digital** del software putty.7z • Los alumnos y alumnas deberán ingresar vía remota con el cliente Bitvise o con linux a el servidor con el servicio WEB Apache. La IP externa se les enviara vía correo electrónico. • Los alumnos y alumnas utilizaran su número de control como usuario y contraseña. Nota: Agregar una letra **u** al principio del número de control. • Se deberá agregar un candado a la carpeta personal en /var/www/html al final de la práctica, ejemplo: ◦ chattr +i /var/www/html/u1219100421 3. - Los alumnos y las alumnas deben leer y comprender las preguntas indicadas (anexo hoja práctica) por el profesor e identificar que comandos y aplicaciones se van a utilizar de acuerdo a cada pregunta. • El profesor entregara el archivo en .doc con las preguntas el día de la práctica. • Utilizar los apuntes (prácticos) tomados en clases de la unidad 2 de Criptografía. • Al saber la respuesta y verificarla, deberán recortar la imagen (con una aplicación de Windows o Linux) de la respuesta escrita en la terminal. **Nota:** Deben recorta la imagen donde viene la respuesta, pero no deben agregar toda la pantalla.
Especificaciones de realización y entrega:	1.- Se entregará al alumnado el anexo de la práctica y contestaran las preguntas utilizando el sistema operativo Linux. La práctica de realizará el **martes 25 de octubre 2022.** 3. El alumnado subirá el archivo con las respuestas en formato .pdf, en la plataforma moodle (elearning.utng.edu.mx) unidad 2. El archivo deber llevar tu nombre_apellido__grupo_practica_unidad2.pdf. Ejemplo: Gustavo_Garcia_**GDGS3071-E_practica_unidad2.pdf** **Nota: Acomodar lo mejor posible las respuestas y las figuras.**
Evaluación:	Esta actividad se evaluará de acuerdo con la siguiente rúbrica:

Concepto	Saber	Hacer	Criterios de evaluación que determinan el puntaje a obtener
Procedimiento		5	• Mostrar con la IP externa del servidor del profesor el software y el link de la firma digital. • Sintaxis y uso adecuados de los comandos para dar respuesta a las preguntas especificadas en el anexo de práctica.
Resultado	2		• Evidenciar el saber (quiz) de la unidad a través de la plataforma moodle.
Ser		1	• Asistencia en clase, actitud y apuntes completos de la unidad.
Cumplimiento de tareas	2		• Mostrar el contenido de cada uno de los archivos encriptados. • Conexión y acceso al servidor por ssh sin que se pida contraseña.
Total	**4**	**6**	

Anexo (hoja práctica)

Instrucciones:

- Para realizar la siguiente práctica las alumnas y los alumnos deberán conectarse con la IP externa, utilizando su número de control como usuario y contraseña. Nota: agregar la letra **u** al principio de tu numero de control, ejemplo: **u1220100050**
- Al conectarse a su cuenta, deberán verificar con el comando **ls -l** los archivos que contiene su directorio. En caso de no encontrar archivos, deberán enviar un correo al profesor (joserubio@utng.edu.mx) indicando que no tienen archivos para realizar su práctica.

Procedimiento

1 punto:

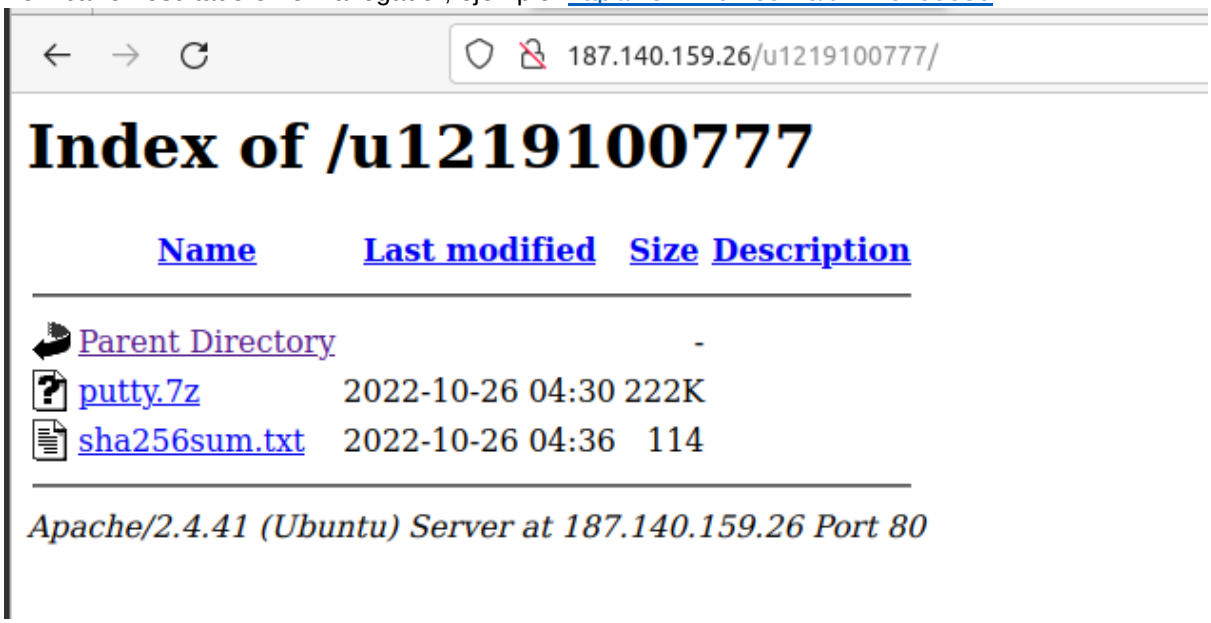
1. Ingresar como modo administrador, la contraseña es linux (contraseña insegura solo para las prácticas).
   (En la imagen de abajo están ambos procedimientos)
2. Con el comando **cp** copia el archivo **putty.7z** a /var/www/html/u_tu_número_control

```
u1219100777@web00:~$ ls
archivo1.txt         pagina.tar.gz               prueba02_des3.tar.gz.enc
boom_a_windows.jpeg  prueba01_aes-256.tar.gz.enc  putty.7z
u1219100777@web00:~$ ls -l
total 1728
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
u1219100777@web00:~$ su
Password:
root@web00:/home/u1219100777# cp putty.7z /var/www/html/html/u1219100777
cp: cannot create regular file '/var/www/html/html/u1219100777': No such file or directory
root@web00:/home/u1219100777# cp putty.7z /var/www/html/u1219100777
root@web00:/home/u1219100777#
```

3. Crea la firma digital del software anterior en un archivo llamado sha256sum.txt y colócalo en /var/www/html/u_tu_número_control.

```
root@web00:/home/u1219100777#  openssl sha256 -c putty.7z>sha256sum.txt
root@web00:/home/u1219100777# dir
archivo1.txt  boom_a_windows.jpeg  pagina.tar.gz  prueba01_aes-256.tar.gz.enc  prueba02_des3.tar.gz.enc  putty.7z  sha256sum.txt
root@web00:/home/u1219100777# exit
exit
u1219100777@web00:~$ ls -l
total 1732
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
-rw-r--r-- 1 root        root            114 oct 26 04:33 sha256sum.txt
u1219100777@web00:~$ cat sha256sum.txt
SHA256(putty.7z)= f9:78:8b:07:e8:cb:57:f8:cd:25:16:fe:30:47:14:60:7f:b9:1e:ba:a3:ad:57:b9:70:ea:9d:86:5a:98:fc:8a
u1219100777@web00:~$ su
Password:
root@web00:/home/u1219100777# cp sha256sum.txt  /var/www/html/u1219100777
root@web00:/home/u1219100777#
```

4. Verificar el resultado en el navegador, ejemplo: http://187.140.159.26/**u1220100050**



1 Punto

Ocultar archivos en Linux

1. Al Ingresar al servidor remoto del profesor, verifica la dirección IP local del servidor **(ip a) y** ejecuta el comando **cat /etc/hosts.**

```
u1219100777@web00:/var/www/html/u1219100777$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:89:52:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.120/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 2806:102e:11:1d8d:a00:27ff:fe89:52fd/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591759sec preferred_lft 2591759sec
    inet6 fe80::a00:27ff:fe89:52fd/64 scope link
       valid_lft forever preferred_lft forever
u1219100777@web00:/var/www/html/u1219100777$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 web00

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
u1219100777@web00:/var/www/html/u1219100777$
```

2. Comprimir y encriptar con **rar** el archivo **pagina.tar.gz,** el archivo final debe ser **pagina.rar**

```
u1219100777@web00:~$ rar a pagina.rar pagina.tar.gz

RAR 5.50   Copyright (c) 1993-2017 Alexander Roshal   11 Aug 2017
Trial version             Type 'rar -?' for help

Evaluation copy. Please register.

Creating archive pagina.rar

Adding    pagina.tar.gz                                           OK
Done
u1219100777@web00:~$ ls -l
total 3188
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 1490045 oct 26 06:27 pagina.rar
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
-rw-r--r-- 1 root        root            114 oct 26 04:33 sha256sum.txt
```

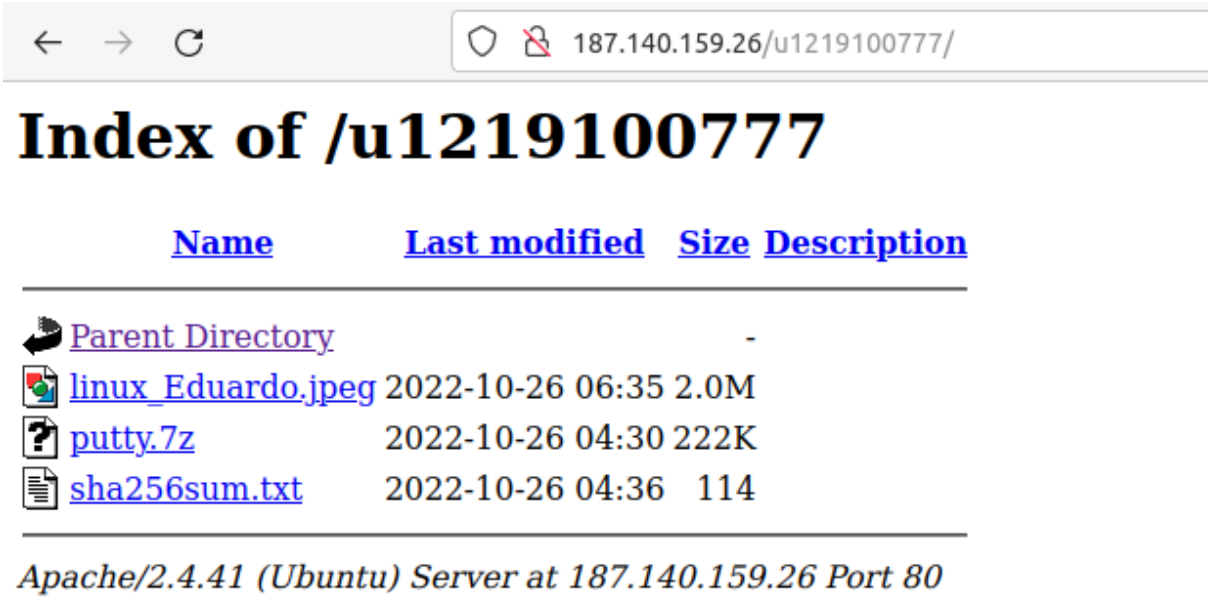
```
u1219100777@web00:~$ openssl aes-256-cbc -a -salt -in pagina.rar -out pagina.rar.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
u1219100777@web00:~$ ls -l
total 5160
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 1490045 oct 26 06:27 pagina.rar
-rw-rw-r-- 1 u1219100777 u1219100777 2017795 oct 26 06:29 pagina.rar.enc
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
-rw-r--r-- 1 root        root            114 oct 26 04:33 sha256sum.txt
```

3. Colocar el archivo **pagina.rar** dentro de la figura llamada **boom_a_windows.jpeg**, pero indicando al final tu nombre, ejemplo: linux_pedro.jpeg.

```
u1219100777@web00:~$ cat boom_a_windows.jpeg pagina.rar.enc > linux_Eduardo.jpeg
u1219100777@web00:~$ ls -l
total 7160
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 2047472 oct 26 06:31 linux_Eduardo.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 1490045 oct 26 06:27 pagina.rar
-rw-rw-r-- 1 u1219100777 u1219100777 2017795 oct 26 06:29 pagina.rar.enc
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
-rw-r--r-- 1 root        root            114 oct 26 04:33 sha256sum.txt
u1219100777@web00:~$
```

```
u1219100777@web00:~$ su
Password:
root@web00:/home/u1219100777# cp linux_Eduardo.jpeg /var/www/html/u1219100777
root@web00:/home/u1219100777#
```

4. Con el comando **cp** copia el archivo linux_pedro.jpeg a /var/www/html/u_tu_número_control y verifica el resultado en el navegador, ejemplo: http://187.140.159.26/**u1220100050**.



1.5 Puntos

Desencriptar archivos con openssl

- Para realizar la desencriptación del siguiente archivo, se requiere obtengas la contraseña con la palabra mágica: **napolitano** y utilizando las **dos** ultimas **letras** de la palabra mágica como parte del comando.

1. Verifica con el comando ls -l si se encuentra un archivo llamado **prueba01_aes-256**.tar.gz.enc

```
u1219100777@web00:~$ echo napolitano | openssl passwd -stdin -crypt -salt NO
NOHAjsDqpVhVc
```

(Si estaba en el archivo solo que el ls -l se ve en la parte de abajo)

2. Con el algoritmo adecuado y con la contraseña obtenida desencripta el archivo enviándolo a uno nuevo. El nuevo archivo se debe llamar archivo_final01.tar.gz.

```
u1219100777@web00:~$ openssl aes-256-cbc -d -a -salt -in prueba01_aes-256.tar.gz.enc -out archivo_final01.tar.gz
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
u1219100777@web00:~$ ls -l
total 7164
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-rw-r-- 1 u1219100777 u1219100777     284 oct 26 07:48 archivo_final01.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 2047472 oct 26 06:31 linux_Eduardo.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 1490045 oct 26 06:27 pagina.rar
-rw-rw-r-- 1 u1219100777 u1219100777 2017795 oct 26 06:29 pagina.rar.enc
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
-rw-r--r-- 1 root        root            114 oct 26 04:33 sha256sum.txt
```

3. Con ayuda del comando **tar zxf**: descompacta y descomprime el archivo anterior. Muestra con el comando **cat** el contenido del archivo.

```
u1219100777@web00:~$ tar zxf archivo_final01.tar.gz
u1219100777@web00:~$ ls -l
total 7168
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-rw-r-- 1 u1219100777 u1219100777     284 oct 26 07:48 archivo_final01.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 2047472 oct 26 06:31 linux_Eduardo.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 1490045 oct 26 06:27 pagina.rar
-rw-rw-r-- 1 u1219100777 u1219100777 2017795 oct 26 06:29 pagina.rar.enc
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-rw-r-- 1 u1219100777 u1219100777     210 oct 24 21:49 prueba01_aes-256
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
-rw-r--r-- 1 root        root            114 oct 26 04:33 sha256sum.txt
u1219100777@web00:~$ cat prueba01_aes-256
Si no sabes, te enseño. Si no puedes, te ayudo. Pero si no quieres, lo siento, pero nada puedo hacer por ti.

La única diferencia entre el éxito y el fracaso es la capacidad de actuar. Alexander Graham Bell
```

- Para realizar la desencriptación del siguiente archivo, se requiere obtengas la contraseña con la palabra mágica: **neptuno** y utilizando las **dos** primeras **letras** de la palabra mágica como parte del comando.

```
u1219100777@web00:~$ echo neptuno | openssl passwd -stdin -crypt -salt NE
NEo/nJ82b1JIo
```

1. Verifica con el comando ls -l si se encuentra un archivo llamado **prueba02_des3**.tar.gz.enc

(Si estaba en el archivo solo que el ls -l se ve en la parte de abajo)

2. Con el algoritmo adecuado y con la contraseña obtenida desencripta el archivo enviándolo a uno nuevo. El nuevo archivo se debe llamar archivo_final02.tar.gz.

```
u1219100777@web00:~$ openssl des3 -d -in prueba02_des3.tar.gz.enc -out archivo_final02.tar.gz
enter des-ede3-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
u1219100777@web00:~$ tar zxf archivo_final02.tar.gz
u1219100777@web00:~$ ls -l
total 7176
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-rw-r-- 1 u1219100777 u1219100777     284 oct 26 07:48 archivo_final01.tar.gz
-rw-rw-r-- 1 u1219100777 u1219100777     297 oct 26 07:52 archivo_final02.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 2047472 oct 26 06:31 linux_Eduardo.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 1490045 oct 26 06:27 pagina.rar
-rw-rw-r-- 1 u1219100777 u1219100777 2017795 oct 26 06:29 pagina.rar.enc
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-rw-r-- 1 u1219100777 u1219100777     210 oct 24 21:49 prueba01_aes-256
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-rw-r-- 1 u1219100777 u1219100777     219 oct 24 22:00 prueba02_des3
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
-rw-r--r-- 1 root        root            114 oct 26 04:33 sha256sum.txt
```

3. Con ayuda del comando **tar zxf**: descompacta y descomprime el archivo anterior. Muestra con el comando **cat** el contenido del archivo.

```
u1219100777@web00:~$ cat prueba02_des3
"La vida es como montar en bicicleta. Para mantener el equilibrio tienes que avanzar." Albert Einstein

"Nunca digas nunca, porque a menudo los límites, como los miedos, son solo ilusiones" – Michael Jordan
```

1.5 puntos

(**Simétrica**). Encriptar con **gpg** los archivos en el Servidor Ubuntu 20.04 remoto del profesor y **desencriptar en windows (tu equipo de escritorio)** con **gpg (kleoptra)**. **Nota: Crea una contraseña segura con openssl.**

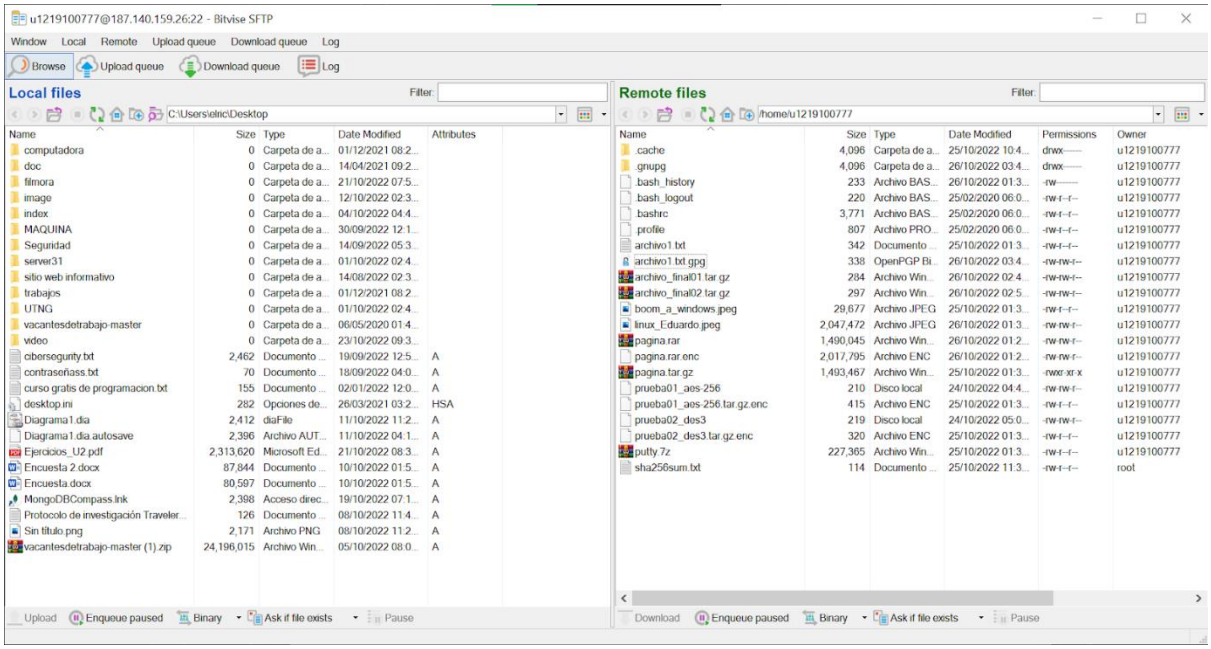
1. Con el comando **echo palabra | openssl passwd -stdin -1** crea una contraseña segura, tu eliges la palabra mágica en el comando.

(En la imagen de abajo están ambos procedimientos)

2. **Encripta** el archivo **archivo1.txt** con el algoritmo CAMELLIA256 en el comando openssl -c --cipher-algo.

```
u1219100777@web00:~$ echo lalo44m | openssl passwd -stdin -1
$1$Dv2ua1ad$X4zlqDtVsJM9DYM4PT.13.
u1219100777@web00:~$ gpg -c --cipher-algo CAMELIA256 archivo1.txt
gpg: selected cipher algorithm is invalid
u1219100777@web00:~$ gpg -c --cipher-algo CAMELLIA256 archivo1.txt
gpg: directory '/home/u1219100777/.gnupg' created
gpg: keybox '/home/u1219100777/.gnupg/pubring.kbx' created
u1219100777@web00:~$ ls -l
total 7180
-rw-r--r-- 1 u1219100777 u1219100777     342 oct 25 18:33 archivo1.txt
-rw-rw-r-- 1 u1219100777 u1219100777     338 oct 26 08:42 archivo1.txt.gpg
-rw-rw-r-- 1 u1219100777 u1219100777     284 oct 26 07:48 archivo_final01.tar.gz
-rw-rw-r-- 1 u1219100777 u1219100777     297 oct 26 07:52 archivo_final02.tar.gz
-rw-r--r-- 1 u1219100777 u1219100777   29677 oct 25 18:33 boom_a_windows.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 2047472 oct 26 06:31 linux_Eduardo.jpeg
-rw-rw-r-- 1 u1219100777 u1219100777 1490045 oct 26 06:27 pagina.rar
-rw-rw-r-- 1 u1219100777 u1219100777 2017795 oct 26 06:29 pagina.rar.enc
-rwxr-xr-x 1 u1219100777 u1219100777 1493467 oct 25 18:33 pagina.tar.gz
-rw-rw-r-- 1 u1219100777 u1219100777     210 oct 24 21:49 prueba01_aes-256
-rw-r--r-- 1 u1219100777 u1219100777     415 oct 25 18:33 prueba01_aes-256.tar.gz.enc
-rw-rw-r-- 1 u1219100777 u1219100777     219 oct 24 22:00 prueba02_des3
-rw-r--r-- 1 u1219100777 u1219100777     320 oct 25 18:33 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1219100777 u1219100777  227365 oct 25 18:33 putty.7z
-rw-r--r-- 1 root        root            114 oct 26 04:33 sha256sum.txt
u1219100777@web00:~$
```

3. Desde la maquina con windows y con la herramienta Bitvise obtén el archivo **archivo1.txt.gpg** en tu directorio de **Documentos.**



4. **Desencriptar** el archivo1.txt.gpg con **gpg (kleopatra)** en tu maquina con windows y muestra el contenido.

Cumplimiento de tareas 2 puntos:

Llaves públicas y privadas. El alumno debe evidenciar el proceso y la conexión remota segura de el Sistema Operativo Cinnamon (Maquina de Escritorio) o cualquiera otra distribución Linux al servidor remoto Ubuntu Server 20.04 del profesor (IP indicada el día de la práctica) con claves públicas y privadas.

1. Mostrar: La creación de las llaves públicas y privadas (2048 bits) en la maquina con el sistemas operativo Linux Mint, ubuntu o cualquier otra distribución que permita realizar crear las llaves.

```
richard@richard-VirtualBox:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/richard/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/richard/.ssh/id_rsa
Your public key has been saved in /home/richard/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Ns3FIULLymDSjZTlOzwdF9/61sInXAIoad45Fj6lzrc richard@richard-VirtualBox
The key's randomart image is:
+---[RSA 3072]----+
|    .o..o o .    |
|   o.+ . + * o   |
|  . = o B + * .  |
|   o + * O * o   |
|      B S @ . . .|
|       + = o + + |
|          o . B o|
|           . o + |
|            E    |
+----[SHA256]-----+
```

2. Mostrar: La **creación** de la carpeta llamada **keys** en /home/usuario/Documentos y **la copia** de las llaves de /home/usuario/.ssh/* a la carpeta **keys/.**

```
richard@richard-VirtualBox:~$ cp .ssh/* Documentos/keyslalo
```

3. **Mostrar: C**on **ssh-copy-id** copiar la llave pública a la cuenta en el servidor remoto (indicado por el profesor).

```
richard@richard-VirtualBox:~$ ssh-copy-id u1219100777@187.140.159.26
The authenticity of host '187.140.159.26 (187.140.159.26)' can't be established.
ED25519 key fingerprint is SHA256:b7dpLmJ/8SMaf5i5rQ2h9euEsmc9WzvKWyvrn2o2d8Q.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
u1219100777@187.140.159.26's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'u1219100777@187.140.159.26'"
and check to make sure that only the key(s) you wanted were added.
```

4. Evidenciar: el ingreso a tu cuenta del servidor remoto con el comando ssh -i y la llave privada que se encuentra en la carpeta **keys/ Nota: el comando debe indicar la** ruta de la carpeta.

```
richard@richard-VirtualBox:~$ ssh -i Documentos/keyslalo/id_rsa u1219100777@187.140.159.26
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 1.0

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

53 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Wed Oct 26 08:39:11 2022 from 189.169.121.0
```