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 3 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 local o externa se les entregara el día de la práctica o 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 se realizará en la semana del 16 al 20 de **octubre 2023 en hora clase, en caso de no terminar se activara el servidor por la noche.** 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: Julio_Torres_**GIDS4073-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 (putty) y el link con la firma digital de la aplicación. • Sintaxis y uso adecuados de los comandos para dar respuesta a las preguntas especificadas en el anexo de práctica. • Mostrar el contenido de cada uno de los archivos encriptados.
Resultado	3		• 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	1		• Conexión y acceso al servidor por ssh sin que se pida contraseña.
Total	**4**	**6**	

Anexo (hoja práctica)

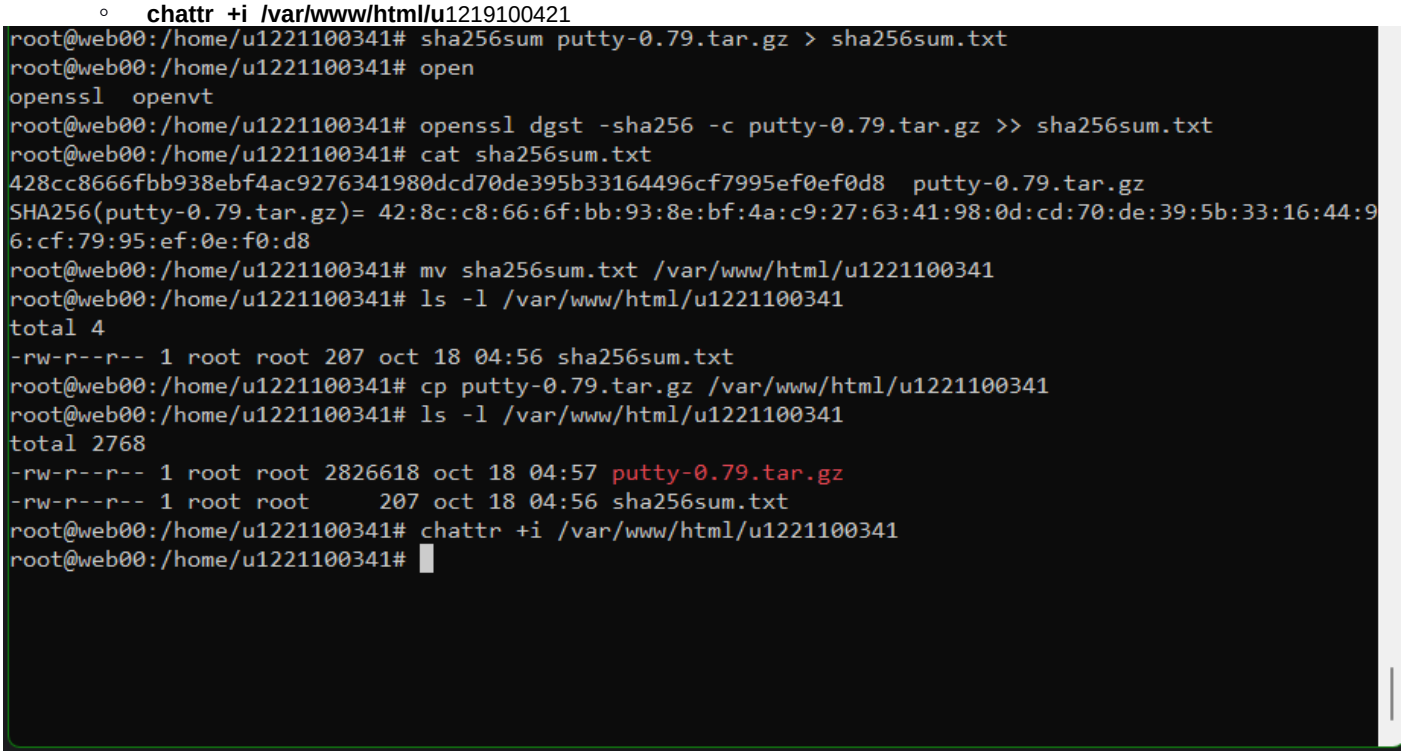
Instrucciones:

- 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: **u**1221100352
- 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:

- Ingresar como modo administrador, la contraseña es linux (contraseña insegura solo para las prácticas).
- Verifica que se encuentre en tu carpeta personal la aplicación putty.
- Crea la firma digital (openssl y sha256sum) del software anterior en un archivo llamado sha256sum.txt y colócalo en /var/www/html/u_tu_número_control. Nota: Debe haber dos lineas, una de openssl y otra de sha256sum.
- Con el comando **cp** copia el archivo **putty-0.79.tar.gz** a /var/www/html/u_tu_número_control
- Verificar el resultado en el navegador, ejemplo: *http://187.140.159.26/***u1220100050**
- Se deberá agregar un candado a la carpeta personal en /var/www/html, ejemplo:
  - **chattr +i /var/www/html/u**1219100421



1 Punto

Ocultar archivos en Linux

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

- **Comprimir y encriptar (en Linux)** con **rar** el archivo **pagina.tar.gz,** el archivo final debe ser **pagina.rar**

```
root@web00:/home/u1221100341# 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
```

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

```
root@web00:/home/u1221100341# cat boom_a_windows.jpeg pagina.rar > linux_alan.jepg
root@web00:/home/u1221100341# ls -l
total 7212
-rw-r--r-- 1 u1221100341 u1221100341     139 oct 11 17:21 archivo1.txt
-rwxr-xr-x 1 u1221100341 u1221100341   29677 oct 11 16:55 boom_a_windows.jpeg
-rw-r--r-- 1 root        root        1519722 oct 18 05:22 linux_alan.jepg
-rw-r--r-- 1 root        root        1490045 oct 18 05:19 pagina.rar
-rwxr-xr-x 1 u1221100341 u1221100341 1493467 oct 11 16:55 pagina.tar.gz
-rw-r--r-- 1 u1221100341 u1221100341     325 oct 11 17:21 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1221100341 u1221100341     256 oct 11 17:21 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1221100341 u1221100341 2826618 oct 11 16:55 putty-0.79.tar.gz
root@web00:/home/u1221100341#
```

- 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**.

```
root@web00:/home/u1221100341# cp linux_alan.jepg /var/www/html/u1221100341/
root@web00:/home/u1221100341# ls -l /var/www/html/u1221100341/
total 4256
-rw-r--r-- 1 root root 1519722 oct 18 05:25 linux_alan.jepg
-rw-r--r-- 1 root root 2826618 oct 18 04:57 putty-0.79.tar.gz
-rw-r--r-- 1 root root     207 oct 18 04:56 sha256sum.txt
root@web00:/home/u1221100341#
```

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.

```
root@web00:/home/u1221100341# echo napolitano | openssl passwd -stdin -salt NO
NOHAjsDqpVhVc
```

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

```
root@web00:/home/u1221100341# ls -l
total 7212
-rw-r--r-- 1 u1221100341 u1221100341     139 oct 11 17:21 archivo1.txt
-rwxr-xr-x 1 u1221100341 u1221100341   29677 oct 11 16:55 boom_a_windows.jpeg
-rw-r--r-- 1 root        root        1519722 oct 18 05:22 linux_alan.jepg
-rw-r--r-- 1 root        root        1490045 oct 18 05:19 pagina.rar
-rwxr-xr-x 1 u1221100341 u1221100341 1493467 oct 11 16:55 pagina.tar.gz
-rw-r--r-- 1 u1221100341 u1221100341     325 oct 11 17:21 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1221100341 u1221100341     256 oct 11 17:21 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1221100341 u1221100341 2826618 oct 11 16:55 putty-0.79.tar.gz
```

  - 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.

```
root@web00:/home/u1221100341# echo napolitano | openssl passwd -stdin -salt NO
NOHAjsDqpVhVc
root@web00:/home/u1221100341# openssl aes-256-cbc -d -a -salt -in prueba01_aes-256.tar.gz.enc -out a
rchivo_final01.tar.gz
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
root@web00:/home/u1221100341# ls -l
total 7216
-rw-r--r-- 1 u1221100341 u1221100341     139 oct 11 17:21 archivo1.txt
-rw-r--r-- 1 root        root            209 oct 18 05:37 archivo_final01.tar.gz
```

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

```
root@web00:/home/u1221100341# tar zxf archivo_final01.tar.gz
root@web00:/home/u1221100341# ls -l
total 7220
-rw-r--r-- 1 u1221100341 u1221100341     139 oct 11 17:21 archivo1.txt
-rw-r--r-- 1 root        root            209 oct 18 05:37 archivo_final01.tar.gz
-rwxr-xr-x 1 u1221100341 u1221100341   29677 oct 11 16:55 boom_a_windows.jpeg
-rw-r--r-- 1 root        root        1519722 oct 18 05:22 linux_alan.jepg
-rw-r--r-- 1 root        root        1490045 oct 18 05:19 pagina.rar
-rwxr-xr-x 1 u1221100341 u1221100341 1493467 oct 11 16:55 pagina.tar.gz
-rw-r--r-- 1 root        root            112 oct 11 17:00 prueba01_aes-256
-rw-r--r-- 1 u1221100341 u1221100341     325 oct 11 17:21 prueba01_aes-256.tar.gz.enc
-rw-r--r-- 1 u1221100341 u1221100341     256 oct 11 17:21 prueba02_des3.tar.gz.enc
-rw-r--r-- 1 u1221100341 u1221100341 2826618 oct 11 16:55 putty-0.79.tar.gz
root@web00:/home/u1221100341# cat prueba01_aes-256

El mundo no está en peligro por las malas personas sino por aquellas que permiten la maldad (Albert
Einstein)
root@web00:/home/u1221100341#
```

- 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.

```
root@web00:/home/u1221100341# echo neptuno | openssl passwd -stdin -salt NE
NEo/nJ82b1JIo
```

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

  - 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.

```
root@web00:/home/u1221100341# 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.
```

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

```
root@web00:/home/u1221100341# tar zxf archivo_final02.tar.gz
root@web00:/home/u1221100341# cat prueba02_des3

Estar preparado es importante, saber esperarlo es aún más, pero aprovechar el momento adecuado es la
 clave de la vida (Arthur Schnitzler)
root@web00:/home/u1221100341#
```

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.**

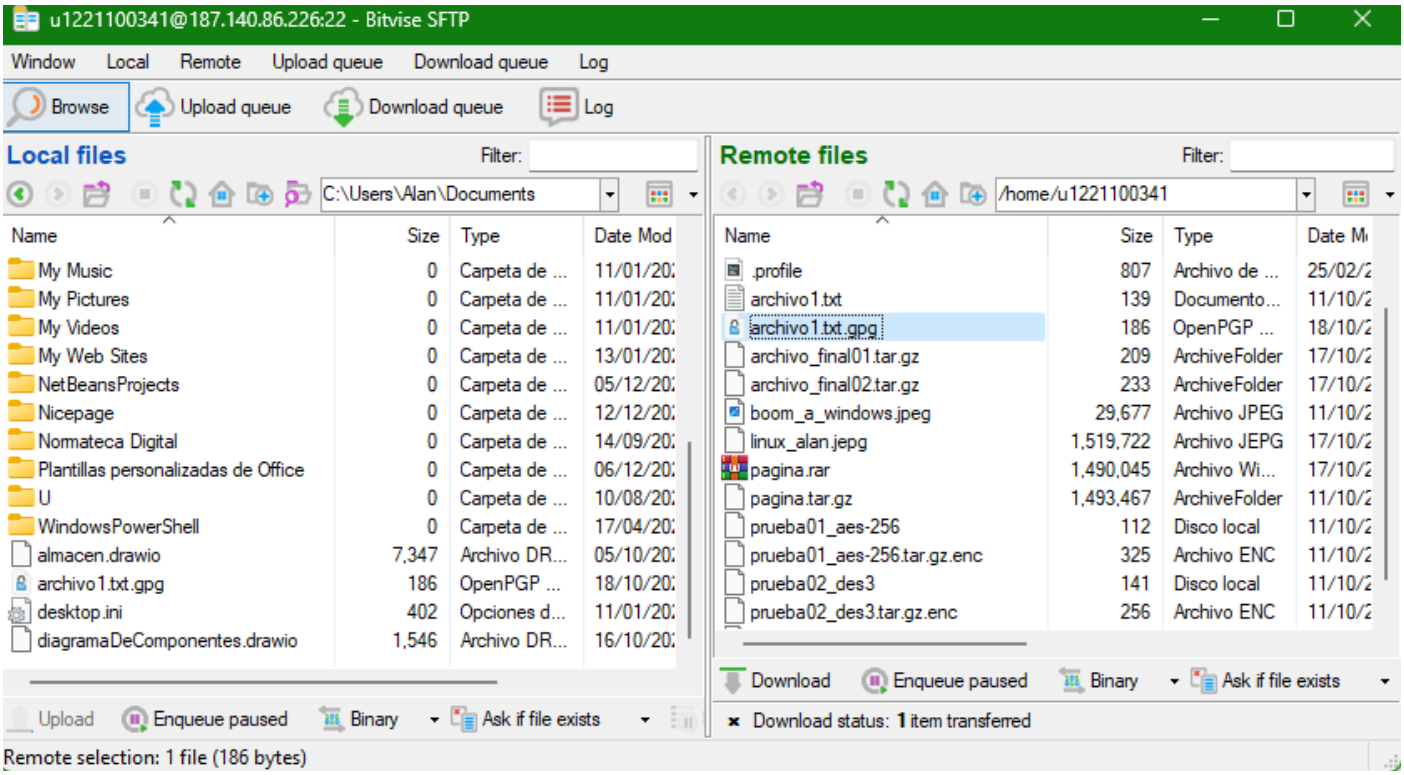
1 Con el comando **echo palabra | openssl passwd -stdin -1** crea una contraseña segura, tu eliges la palabra mágica en el comando.

```
root@web00:/home/u1221100341# echo paleton | openssl passwd -stdin -1
$1$PeEvXC6U$Bf2u5CjQGPjNBuu6prm8E0
root@web00:/home/u1221100341#
```

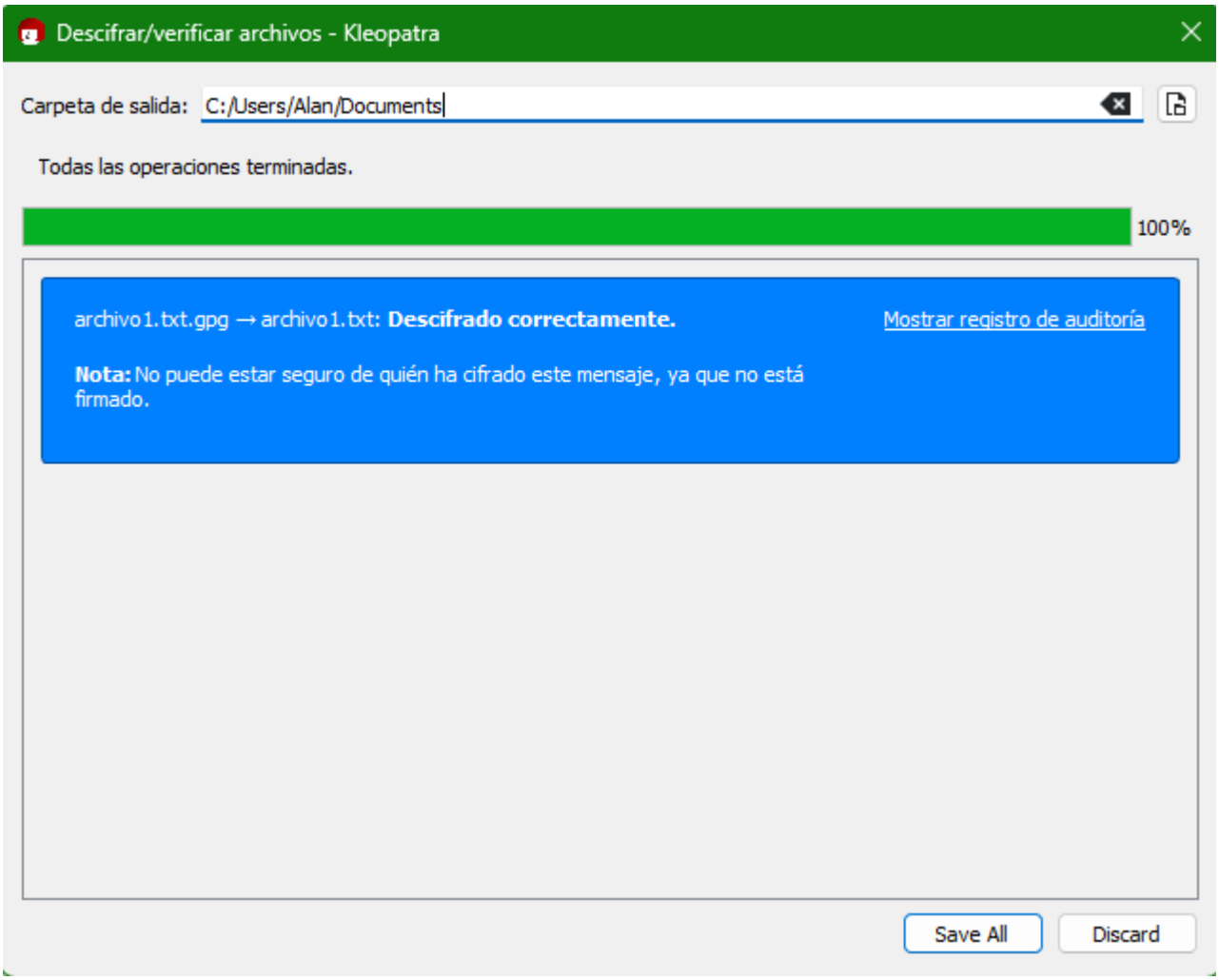
2 **Encripta** el archivo **archivo1.txt** con el algoritmo CAMELLIA256 en el comando openssl -c --cipher-algo.

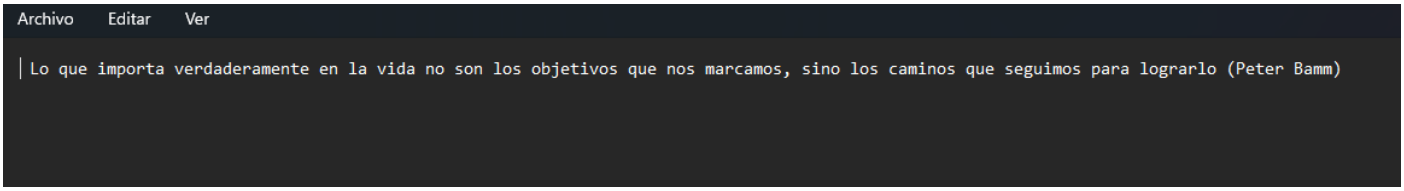
```
root@web00:/home/u1221100341# gpg -c --cipher-algo CAMELLIA256 archivo1.txt
root@web00:/home/u1221100341#
```

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.


Descifrar/verificar archivos - Kleopatra
Carpeta de salida: C:/Users/Alan/Documents
Todas las operaciones terminadas.
100%
archivo1.txt.gpg → archivo1.txt: Descifrado correctamente.
Mostrar registro de auditoría
Nota: No puede estar seguro de quién ha cifrado este mensaje, ya que no está firmado.
Save All
Discard


Archivo
Editar
Ver
Lo que importa verdaderamente en la vida no son los objetivos que nos marcamos, sino los caminos que seguimos para lograrlo (Peter Bamm)

X

Cumplimiento de tareas 1 punto:

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.

- 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:

1. Desde una terminal desde tu aplicación bitvise, linux o cualquier aplicación que estés utilizando para conectarte al **servidor remoto**, ingresa con ssh a un **servidor local** (temporal) del profesor (usuario jrubio, contraseña linux e IP Local (192.168.1.121).

2. Ingresa como administrador (su) y crea tu usuario con tu nombre, ejemplo: # useradd -d /home/pedro -m -s /bin/bash pedro Nota: No crear a pedro (si no te llamas así).

```
root@serv01:/home/jrubio# useradd -d /home/alan -m -s /bin/bash alan
```

3. Agregar la contraseña insegura solo para práctica (linux) al usuario, ejemplo: # passwd pedro ;y después salte de la cuenta de root y jrubio. Conéctate nuevamente al servidor local (paso 1), pero con la cuenta creada, ejemplo: ssh pedro@192.168.1.121.

```
root@serv01:/home/jrubio# passwd alan
New password:
Retype new password:
passwd: password updated successfully
root@serv01:/home/jrubio#
```

4. Mostrar: La creación de una carpeta llamada **keys** en tu directorio personal, ejemplo: **/home/pedro/keys** y **la copia** de las llaves de **/home/pedro/.ssh/*** a la carpeta **keys/.**

```
alan@web00:~$ ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/home/alan/.ssh/id_rsa):
Created directory '/home/alan/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alan/.ssh/id_rsa
Your public key has been saved in /home/alan/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:NFLOIpHzKaeoUNwnutja0OpR+Sdr4IZbanKbng1v6aY alan@web00.utng.edu.mx
The key's randomart image is:
+---[RSA 2048]----+
|    ..  .        |
|    o. +         |
| . ..oo.=        |
|  o =.=+ .       |
| . = *  S        |
|..+.o            |
|o==o.+ .         |
|+*BO+.+          |
|*BE*=.           |
+----[SHA256]-----+
alan@web00:~$ ls -l /home/alan/.ssh/*
-rw------- 1 alan alan 1831 oct 18 06:39 /home/alan/.ssh/id_rsa
-rw-r--r-- 1 alan alan  404 oct 18 06:39 /home/alan/.ssh/id_rsa.pub
alan@web00:~$ cp /home/alan/.ssh/* /home/alan/keys/
alan@web00:~$ ls -l  /home/alan/keys/
total 8
-rw------- 1 alan alan 1831 oct 18 06:41 id_rsa
-rw-r--r-- 1 alan alan  404 oct 18 06:41 id_rsa.pub
alan@web00:~$
```

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

```
alan@serv01:~/keys$ ssh-copy-id u1221100341@187.140.86.226
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/alan/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
u1221100341@187.140.86.226's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'u1221100341@187.140.86.226'"
and check to make sure that only the key(s) you wanted were added.
```

6. Evidenciar: el ingreso a tu cuenta del servidor remoto con el comando **ssh -i keys/llave** usuario@ip_externa **Nota: el comando debe indicar la ruta de la carpeta, además de que al conectarse a el servidor remoto no debe pedir contraseña.**

```
alan@serv01:~/keys$ ssh -i id_rsa u1221100341@187.140.86.226
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 as of mié 18 oct 2023 07:14:54 UTC

  System load:             0.09
  Usage of /home:          2.5% of 19.56GB
  Memory usage:            51%
  Swap usage:              4%
  Processes:               625
  Users logged in:         45
  IPv4 address for enp0s3: 192.168.1.120
  IPv6 address for enp0s3: 2806:102e:11:2008:a00:27ff:fea9:4908

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Wed Oct 18 07:14:04 2023 from 187.140.86.226
```