

 <small>Universidad Tecnológica de México</small>	Practicario de Controles Criptográficos de Seguridad	Clave: MST321
---	---	----------------------

Generales:

Maestría en:	Seguridad de Tecnología de Información
Asignatura:	Controles Criptográficos de Seguridad
Objetivo de la asignatura:	Diseñar aplicaciones de cifrado y descifrado de información considerando los distintos métodos y controles criptográficos, para la evaluación y fortalecimiento de la seguridad de los sistemas, aplicaciones y datos informáticos de las organizaciones.
Nombre del profesor:	Israel Alejandro Herrera Araiza
Nombre del alumno:	Ignacio Ivan Sanchez Pantoja

Datos de la Práctica o Caso Práctico 1

Práctica o caso práctico 1 de 3:	Explorar el cifrado de archivos y datos
Objetivo de la práctica o caso práctico:	Acceder a contenidos cifrados y transferir archivos a través de Internet a un servidor FTP centralizado utilizando los dispositivos cliente en las diferentes regiones geográficas establecidas en la práctica, además, se tendrá que descargar el archivo desde el servidor FTP y descifrar el contenido de los archivos con la finalidad de asimilar los conceptos vistos en clase y su aplicación en un ámbito laboral real, incorporando comandos de cifrado 3DES y AES.
Temas y subtemas asociados:	2. Criptografía de llave privada o cifrados simétricos 2.1. Cifradores de bloque 2.1.1. Estándar de Cifrado Avanzado Advanced Encryption Standar, AES 2.1.2. Estándar de triple cifrado de datos - Triple Data Encryption Standard, TDES 3. Criptografía moderna y llave pública 3.5. Sistema de Rivest, Shamir y Adleman, RSA 5. Soluciones criptográficas en las organizaciones 5.1. Contexto organizacional y arquitectura de la información 5.4. Software de encriptación y des-encriptación 5.8. Aplicaciones de la criptografía en la seguridad tecnológica 5.8.3. Conexión de servidores, Virtual Private Network, VPN 5.8.5. Conectar computadoras, Internet Protocol Secure, IPsec
Fecha:	27/09/2024
Duración (horas):	Una hora

Laboratorio de:	Cómputo
Software requerido:	Sistema operativo Microsoft Windows 10 o superior, MacOS o distribución de Linux, Packet Tracer en su versión 8.2.
Práctica o caso práctico 1 de 3:	Explorar el cifrado de archivos y datos
	<ul style="list-style-type: none"> • Es necesario contar o generar una cuenta de acceso a CISCO en: https://id.cisco.com/signin/register • VirtualBox (https://www.virtualbox.org/wiki/Downloads), VMware (https://www.vmware.com/products/workstation-player.html) o Docker (https://www.docker.com) para virtualizar un sistema operativo. • Distribución de Linux (preferentemente Kali (https://www.kali.org/get-kali/)), con asignación de memoria mínima de 3GB RAM y 100GB en HD.
Equipo necesario en laboratorio:	Computadora con procesador Intel I5 o superior o AMD Ryzen 5 o superior, con 8GB en RAM como mínimo.

Desarrollo o caso práctico 1:

Los corporativos Metrópolis Bank HQ y Healthcare at Home requieren transmitir de manera segura información sensible y valiosa, por ello, han implementado un mecanismo de transmisión vía FTP en el cual es necesario asegurar que los datos enviados a través del medio sean seguros mediante procedimientos criptográficos.

En este sentido, será necesario utilizar credenciales de acceso al medio FTP con la finalidad de enviar y recibir datos entre ambas organizaciones y generar cifrados criptográficos 3DES y AES.

Preguntas del caso práctico 1:

1. ¿Cuál es el nombre de usuario y contraseña encontrados para la autenticación FTP de Mary?
2. ¿Qué datos en texto claro serían descubiertos por algún ciberdelincuente?
3. ¿Cuáles son las credenciales (nombre de usuario y contraseña) de Bob utilizadas en el FTP?
4. ¿Cuáles son los datos que serían vistos por un ciberdelincuente en la transferencia de archivos?
5. ¿Cuál es la clave para descifrar y acceder a la información confidencial del archivo?
6. ¿Cuál es el nombre de la cuenta inicial implícita en el archivo clienteinfo.txt?

Indicaciones de la práctica o caso práctico:

El alumno contará con la infraestructura (ver Figura 1) siguiente, con la finalidad de:

- ubicar las credenciales de la cuenta FTP para la PC portátil de Mary
- cargar datos confidenciales mediante FTP
- ubicar las credenciales de la cuenta FTP para la computadora de Bob
- descargar datos confidenciales mediante FTP
- descifrar el contenido del archivo clienteinfo.txt

Desarrollo o caso práctico 1:

Tabla 1.

Matriz de correspondencia de la infraestructura disponible para el cifrado de archivos y datos.

Dispositivo	Dirección IP privada	Dirección IP pública	Máscara de subred	Sitio
Servidor FTP/web	10.44.1.254	209.165.201.3	255.255.255.0	Metrópolis Bank HQ
Mary	10.44.3.101	No aplica	255.255.255.0	Healthcare at Home
Roberto	10.44.1.3	No aplica	255.255.255.0	Metrópolis Bank HQ

Ejercicio 1

Descargar práctica:



1. Ubicar las credenciales de la cuenta FTP para la PC portátil de Mary.

- Acceda al documento de texto de la PC portátil de Mary.
 - Haga clic en el sitio Healthcare at Home y luego haga clic en la PC portátil Mary.
 - Haga clic en la ficha Escritorio y luego haga clic en Editor de texto.
 - En la ventana del editor de texto, haga clic en Archivo > Abrir.
 - Haga clic en el documento ftplogin.txt y haga clic en Aceptar.
- Descifre la Información de la cuenta de FTP de Mary.
 - Resalte todo el texto del archivo ftplogin.txt y cópielo.
 - Abra un navegador web en su computadora personal y desplácese al sitio web <https://encipher.it>
 - Haga clic en el espacio en blanco a la derecha del sitio web y péguelo el texto cifrado.
 - Haga clic en el botón Descifrarlo y use la contraseña de cifrado maryftp123 para descifrar el texto cifrado. Haga clic en Descifrar.
 - Especificar el nombre de usuario y contraseña encontrados para la autenticación FTP de Mary.

2. Cargar datos confidenciales mediante FTP.

- Vea al documento confidencial en la PC portátil de Mary.
3. Haga clic en el sitio Healthcare at Home y luego haga clic en la PC portátil Mary.



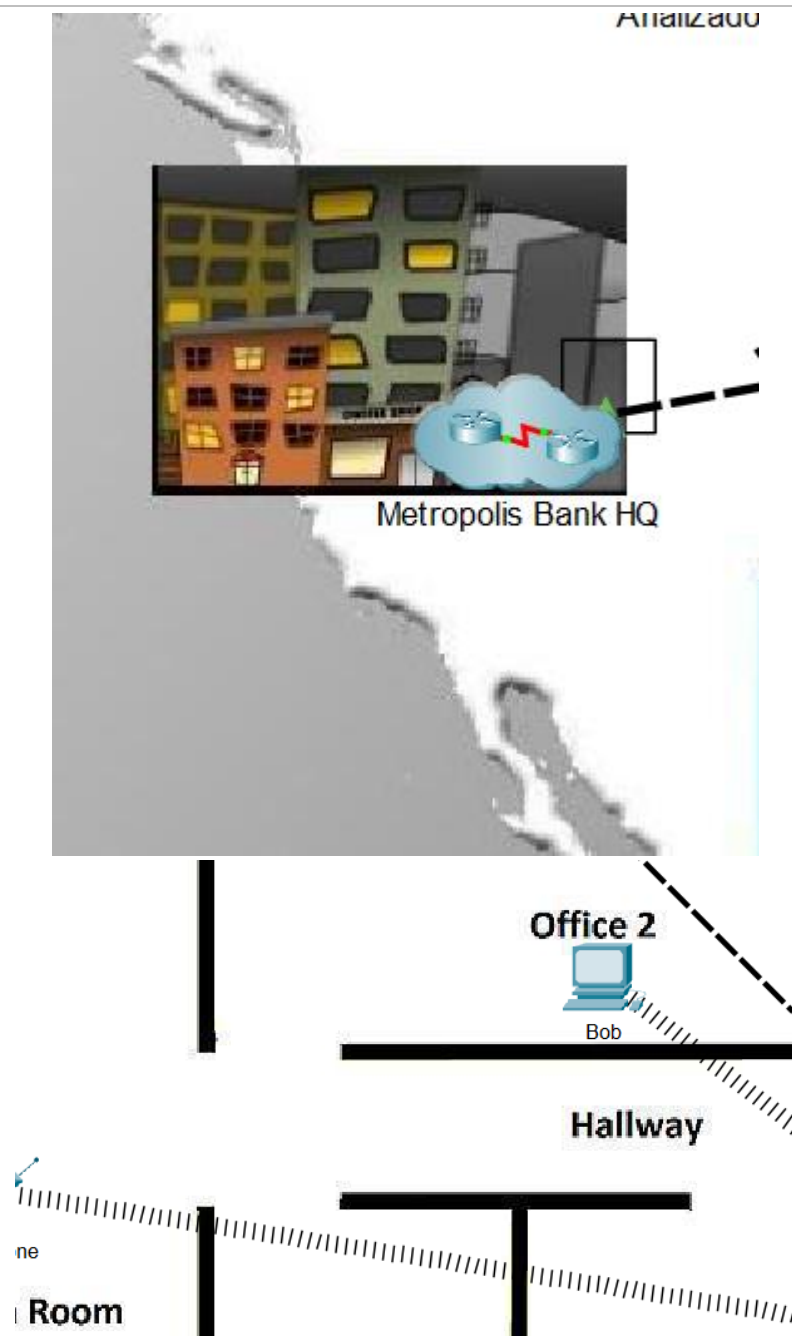
Desarrollo o caso práctico 1:

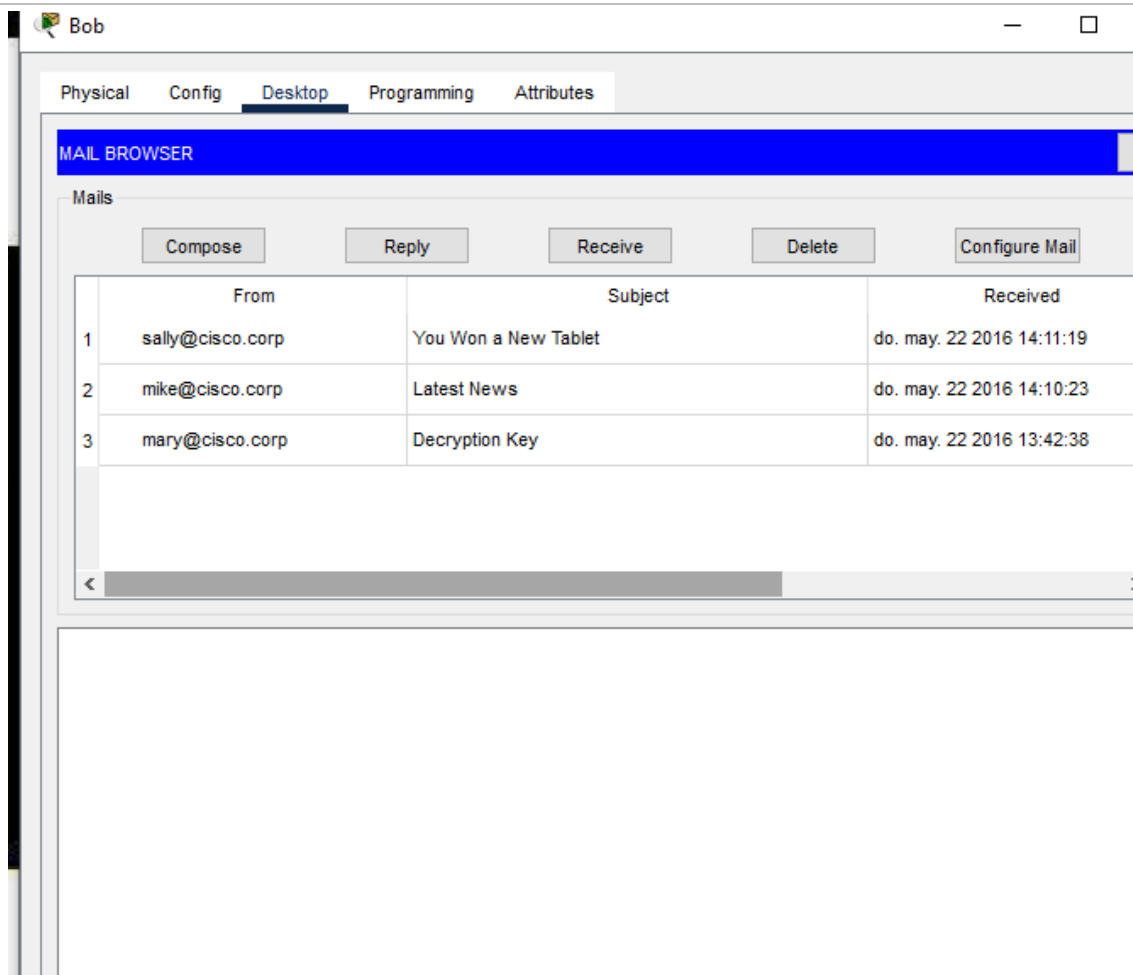
- En el indicador ftp>, introduzca el comando dir para ver los archivos actuales almacenados en el servidor FTP remoto. ○ Mary había cargado el archivo clientinfo.txt que contiene información cifrada sobre los servicios de salud del cliente.
- Descargue el archivo clientinfo.txt en la computadora de Bob al introducir el comando get clientinfo.txt.
- En el indicador ftp>, introduzca el comando quit. ○ En el indicador PC>, introduzca el comando dir y verifique que el archivo clientinfo.txt ahora se encuentre en la computadora de Bob.
- Indique los datos que serían vistos por un ciberdelincuente en la transferencia de archivos.

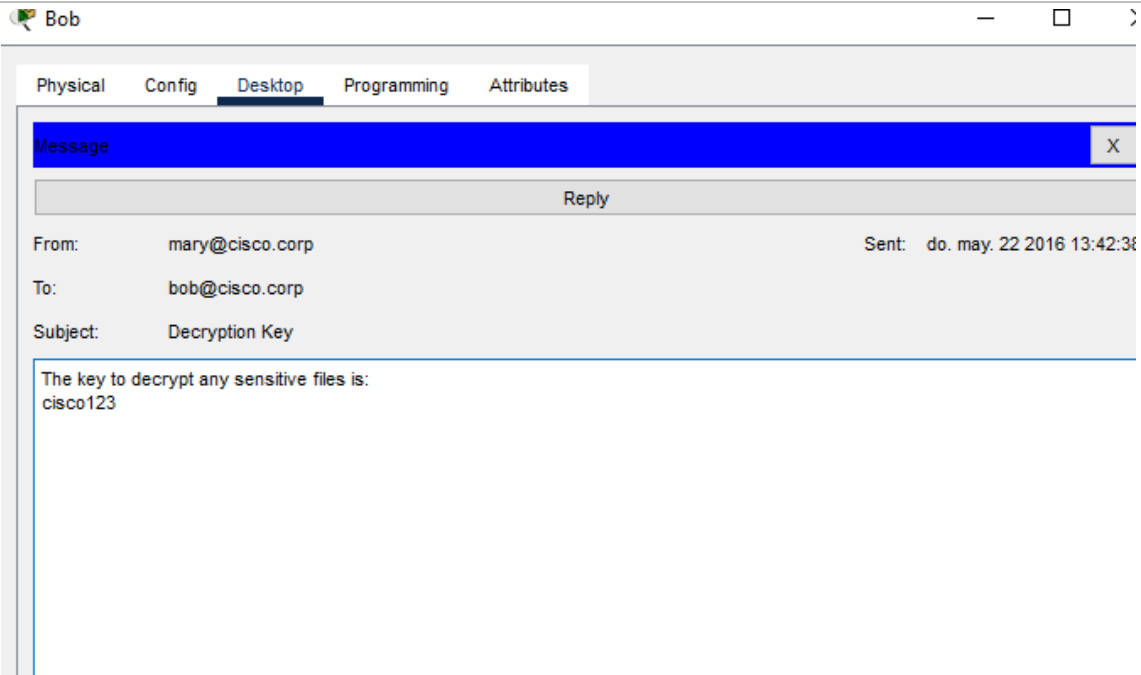
Al ser FTP un protocolo que no cifra los datos en un principio la información estaría en texto plano, sin embargo al estar cifrada haciendo uso de AES 256 es imposible leer el contenido sin la contraseña proporcionada

5. Descifrar el contenido del archivo clientinfo.txt.

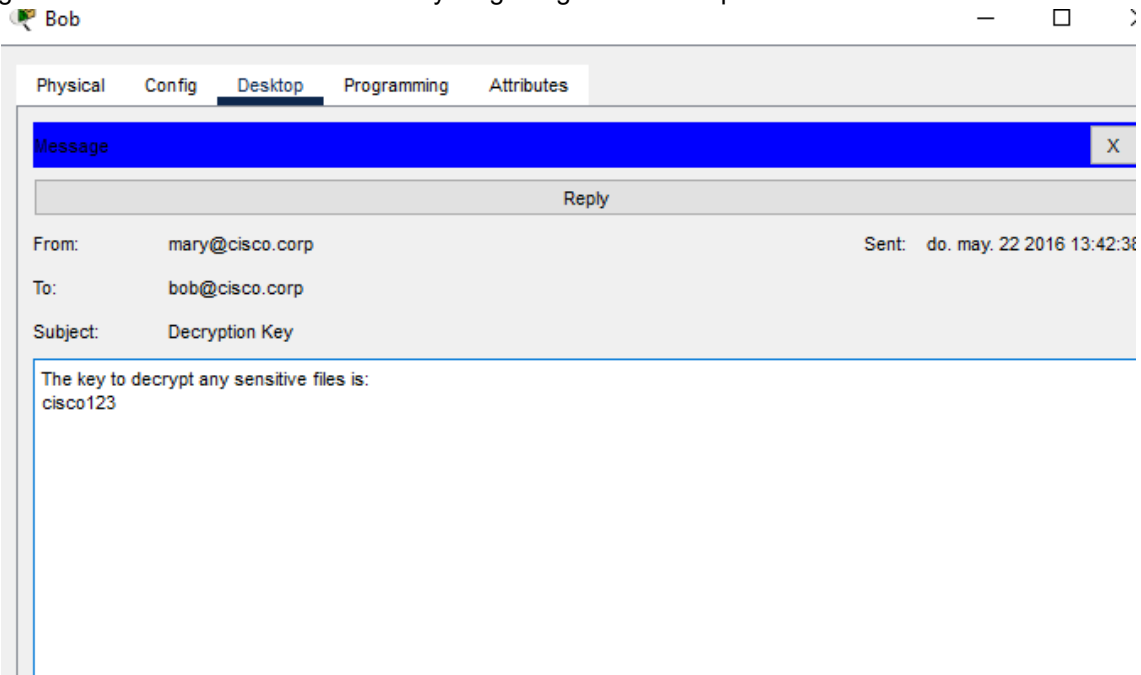
- Reciba la clave de descifrado de Mary.
- En el sitio Metropolis Bank HQ, haga clic en la computadora Bob.
- Haga clic en la ficha Escritorio y luego haga clic en Correo electrónico.
- En la ventana del correo electrónico, haga clic en Recibir
- Haga clic en el correo electrónico con el asunto «clave de descifrado» y registre la clave de descifrado
 - continuación.
 - Indique cuál es la clave para descifrar y acceder a la información confidencial del archivo.







- Descifrar el contenido del archivo clientinfo.txt.
- En el sitio Metropolis Bank HQ, haga clic en la computadora Bob.
- Haga clic en la ficha Escritorio y luego haga clic en Editor de texto.
- En la ventana del editor de texto, haga clic en Archivo > Abrir.
- Haga clic en el documento clientinfo.txt y luego haga clic en Aceptar.



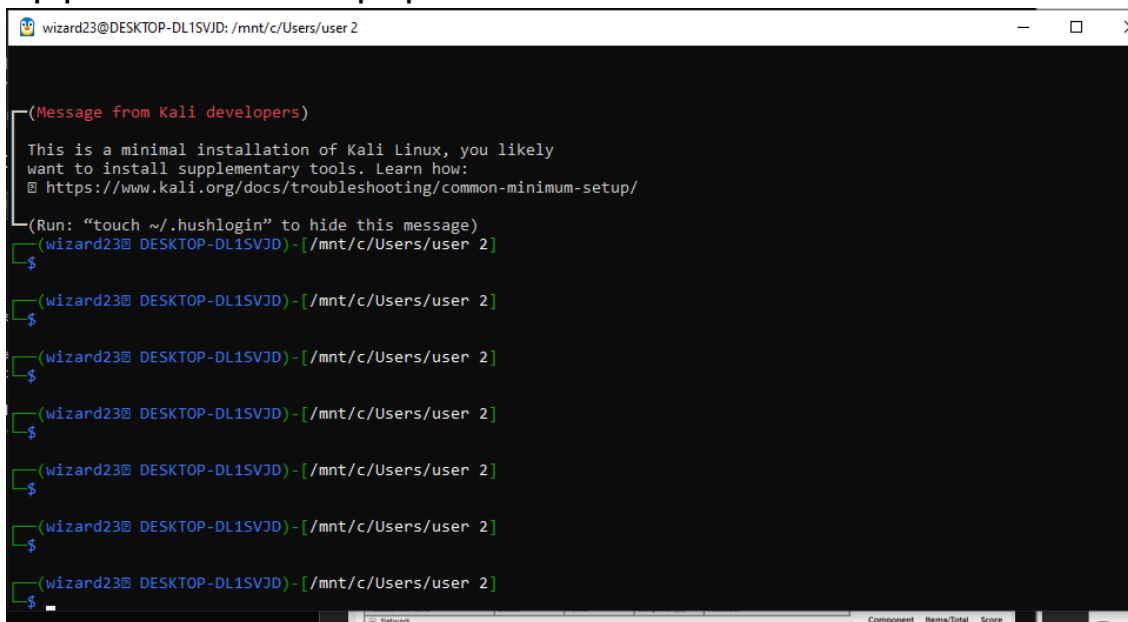
- Resalte todo el texto del archivo clientinfo.txt y cópielo.
 - Abra un navegador web en su computadora personal y desplácese al sitio web
 - <https://encipher.it>
 - Haga clic en el espacio en blanco a la derecha del sitio web y pégue el texto cifrado.
 - Haga clic en el botón Descifrarlo y use la contraseña de cifrado del correo electrónico de Mary para descifrar el texto cifrado. Haga clic en Descifrar.
 - Indique cual es el nombre de la cuenta inicial (clienteinfo.txt).

El nombre de la primera cuenta en el archivo clientinfo.txt es Plato X. Riggs

6. Generar cifrados 3DES y AES en Linux

- En el equipo virtualizado con distribución Linux (Kali), aplicar los siguientes procedimientos desde la terminal.
- Crear un archivo de texto.
- echo Texto dentro del archivo > archivo.txt
- Comprobar el contenido del archivo.
- cat archivo.txt
- Cifrar el texto dentro del archivo generado en el paso anterior, para ello, utilizará un cifrado 3DES.
- openssl enc -des3 -salt -in archivo.txt -out mensajecifrado.bin
- Comprobar el cifrado del contenido en el archivo.
- cat mensajecifrado.bin

Para el equipo de virtualización se opto por utilizar WSL con la distribución Kali Linux



```
wizard23@DESKTOP-DL1SVJD: /mnt/c/Users/user 2

(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
https://www.kali.org/docs/troubleshooting/common-minimum-setup/

(Run: "touch ~/.hushlogin" to hide this message)
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$
```

Desarrollo o caso práctico 1:

- Descifrar el texto dentro del archivo generado en el paso anterior, para ello, utilizará un cifrado 3DES.
 - `openssl enc -des3 -salt -d -in mensajecifrado.bin -out mensajedescifrado.txt`
- Validar que el texto contenido en el archivo se visualiza de manera normal.
 - `cat mensajedescifrado.txt`
- Cifrar el texto dentro del archivo generado en el paso anterior, para ello, utilizará un cifrado AES.
 - `openssl aes-256-cbc -e -in archivo.txt -out mensajecifrado.txt.AES256`
- Comprobar el cifrado del contenido en el archivo.
 - `cat mensajecifrado.txt.AES256`
- Descifrar el texto dentro del archivo generado en el paso anterior, para ello, utilizará un cifrado AES.
 - `openssl aes-256-cbc -e -d -in mensajecifrado.txt.AES256 -out mensajeAES256original.txt`

Resultados obtenidos:

Creación del archivo:

```
(wizard23@ DESKTOP-DL1SVJD) - [/mnt/c/Users/user 2]  
$ echo "Sanchez Pantoja" >> archivo.txt  
  
(wizard23@ DESKTOP-DL1SVJD) - [/mnt/c/Users/user 2]  
$ cat archivo.txt  
Sanchez Pantoja
```

Ahora deberemos cifrar los datos del archivo haciendo uso de 3DES, pero previo a ello comprobaremos si tenemos instalado openssl en la distribución
Eso lo hacemos escribiendo el comando en la línea de comandos

```
(wizard23@ DESKTOP-DL1SVJD) - [ /mnt/c/Users/user 2 ]
$ openssl
help:

Standard commands
asn1parse      ca          ciphers      cmp
cms            crl         crl2pkcs7   dgst
dhparam        dsa         dsaparam    ec
ecparam        enc         engine       errstr
fipsinstall    gendsa     genpkey     genrsa
help           info        kdf          list
mac            nseq       ocsf         passwd
pkcs12         pkcs7      pkcs8       pkey
pkeyparam      pkeyutl    prime       rand
rehash         req        rsa          rsautl
s_client       s_server   s_time      sess_id
smime          speed      spkac       srp
storeutl       ts         verify      version
x509

Message Digest commands (see the `dgst' command for more details)
blake2b512     blake2s256 md4          md5
```

Como podemos observar el comando esta instalado de forma exitosa, por lo cual ejecutaremos el comando de openssl que nos permite cifrar datos con 3des
openssl enc -des3 -salt -in archivo.txt -out mensajecifrado.bin
contraseña usada: R0M30

```
$ cat mensajecifrado.bin
Salted__000JXIqJ15x!
(wizard23@ DESKTOP-DL1SVJD) - [ /mnt/c/Users/user 2 ]
$
```

Ahora procederemos a descifrar el mensaje

```
(wizard23@ DESKTOP-DL1SVJD) - [ /mnt/c/Users/user 2 ]
$ openssl enc -des3 -salt -d -in mensajecifrado.bin -out mensajedescifrado.txt
Enter DES-EDE3-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
din

(wizard23@ DESKTOP-DL1SVJD) - [ /mnt/c/Users/user 2 ]
$ cat mensaje
mensajecifrado.bin  mensajedescifrado.txt
(wizard23@ DESKTOP-DL1SVJD) - [ /mnt/c/Users/user 2 ]
$ cat mensajedescifrado.txt
Sanchez Pantoja
(wizard23@ DESKTOP-DL1SVJD) - [ /mnt/c/Users/user 2 ]
$
```

Ahora cifraremos los datos haciendo uso de AES

```
(wizard23@ DESKTOP-DL1SVJD) - [/mnt/c/Users/user 2]
$ openssl aes-256-cbc -e -in archivo.txt -out mensajecifrado.txt.AES256
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.

(wizard23@ DESKTOP-DL1SVJD) - [/mnt/c/Users/user 2]
$ openssl aes-256-cbc -e -in archivo.txt -out mensajecifrado.txt.AES256
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.

(wizard23@ DESKTOP-DL1SVJD) - [/mnt/c/Users/user 2]
$ openssl aes-256-cbc -e -d -in mensajecifrado.txt.AES256 -out MensajeOriginalAes256.txt
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

(wizard23@ DESKTOP-DL1SVJD) - [/mnt/c/Users/user 2]
$ cat MensajeOriginalAes256.txt
Menú Inicio/
Sanchez Pantoja
```

Conclusiones:

Conclusiones:

La práctica permitió aplicar y comprender los conceptos de cifrado y descifrado de datos mediante la implementación de técnicas de criptografía simétrica y asimétrica, específicamente utilizando 3DES y AES. Durante el desarrollo, se simulaban escenarios corporativos en los cuales se manejó información sensible a través de transferencias seguras de archivos vía FTP y conexiones VPN. Esto ayudó a reforzar la importancia de proteger la información durante la transmisión y almacenamiento, además de resaltar la necesidad de conocer las herramientas y comandos adecuados para asegurar la integridad y confidencialidad de los datos. La experiencia práctica evidenció los riesgos asociados a la transmisión de datos sin cifrar y demostró cómo la criptografía actúa como una barrera eficaz contra accesos no autorizados. Al mismo tiempo, se exploraron las aplicaciones y limitaciones de los métodos criptográficos en un contexto laboral real, lo que subraya la relevancia de estos conocimientos para cualquier profesional en el campo de la ciberseguridad. La importancia de dominar estos mecanismos radica en la capacidad de diseñar soluciones que fortalezcan la seguridad de los sistemas, una habilidad crucial en un entorno donde la protección de los datos es esencial para las operaciones diarias de cualquier organización. Esta práctica contribuye al desarrollo profesional al mejorar la capacidad de identificar vulnerabilidades y aplicar medidas preventivas adecuadas, habilidades que son fundamentales para la gestión segura de la información en un entorno corporativo.

Bibliografía:

- B, M., & M, V. (2021). A novel security mechanism using AES cryptography approach in cloud computing. International Journal of Communication Systems, 34(6), 1–11. doi: 10.1002/dac.4631
- Pattanavichai, S. (2022). Program for Simulation and Testing of Apply Cryptography of Advance Encryption Standard (AES) Algorithm with Rivest-Shamir-Adleman (RSA) Algorithm for Good Performance. International Journal of Electronics & Telecommunications, 68(3), 475–481. doi: 10.24425/ijet.2022.141263
- Shaktawat, R., Shaktawat, R. S., Lakshmi, N., Panwar, A., & Vaishnav, A. (2020). A Hybrid Technique of Combining AES Algorithm with Block Permutation for Image Encryption. Reliability: Theory & Applications, 15(1), 51–56.

Criterios de evaluación:

- Aplicación de técnicas y herramientas de cifrados criptográficos.
- Entendimiento de ciberseguridad en el ámbito de criptografía.