



Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: Ing. Magdalena Reyes Granados

Asignatura: Laboratorio de Redes de Datos

Grupo: 02

No de Práctica(s): 10

Integrante(s): Amado Fuentes Yerenia

Moreno Madrid Maria Guadalupe

*No. de Equipo de
cómputo empleado:*

Semestre:


2021-1

Fecha de entrega:

9/12/2020

Observaciones:


CALIFICACIÓN: _____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	148/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 10

Funciones de la capa de presentación

Capa 6 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	149/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1.- Objetivo de Aprendizaje

- El alumno al finalizar la práctica, conocerá algunos de los conceptos básicos de la Capa 6 del Modelo OSI (Capa de Presentación), utilizando algunos programas de uso común.
- El alumno conocerá las funciones principales de la Capa de Presentación, y utilizará adecuadamente estas características según las situaciones que se le presenten.

2.- Conceptos Teóricos

La capa de presentación se encarga del formato y representación de los datos. De ser necesario, esta capa puede servir de intermediario entre distintos formatos.

La capa 6, o capa de presentación, cumple tres funciones principales (ver Figura No. 1). Estas funciones son las siguientes:

- Formateo de datos (presentación)
- Cifrado de datos
- Compresión de datos

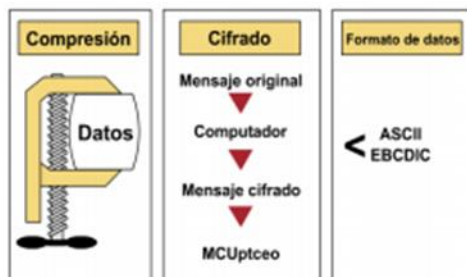



Figura No. 1. Funciones principales de la Capa 6.

Después de recibir los datos de la capa de aplicación, la capa de presentación ejecuta una de sus funciones, o todas ellas, con los datos antes de mandarlos a la capa de sesión. En la estación receptora, la capa de presentación toma los datos de la capa de sesión y ejecuta las funciones requeridas antes de pasarlos a la capa de aplicación.

Los estándares de la Capa 6 también determinan la presentación de las imágenes gráficas. A continuación, se presentan tres de estos estándares:

- **PICT:** Un formato de imagen utilizado para transferir gráficos QuickDraw entre programas del sistema operativo MAC
- **TIFF** (Formato de archivo de imagen etiquetado): Un formato para imágenes con asignación de bits de alta resolución
- **JPEG** (Grupo conjunto de expertos fotográficos): Formato gráfico utilizado con frecuencia para comprimir imágenes fijas de ilustraciones o fotografías complejas

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	150/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Otros estándares de la Capa 6 regulan la presentación de sonido y películas. Entre estos estándares se encuentran:

- *MIDI* (Interfaz digital para instrumentos musicales): para música digitalizada
- *MPEG* (Grupo de expertos en películas): Estándar para la compresión y codificación de vídeo con movimiento para el almacenamiento en CD y digital
- *QuickTime*: Estándar para el manejo de audio y vídeo para los sistemas operativos de los MAC y de los PC

También existen estándares para el formato del texto, éstos son:

- *EBCDIC* (Código de caracteres decimal codificados en binario): Es un código estándar de 8 bits usado por computadoras *mainframe* IBM.
- *ASCII* (Código americano normalizado para el intercambio de información): Es un código de caracteres basado en el alfabeto latino tal como se usa en inglés moderno y en otras lenguas occidentales.

Otro formato de archivo común es el formato binario. Los archivos binarios contienen datos codificados especiales que sólo se pueden leer con aplicaciones de software específicas. Programas como FTP utilizan el tipo de archivo binario para transferir archivos.

Otro tipo de formato de archivo es el lenguaje de etiquetas. Este formato actúa como un conjunto de instrucciones que le indican al navegador de Web cómo mostrar y administrar los documentos. El Lenguaje de etiquetas por hipertexto (HTML) es el lenguaje de Internet. Las direcciones HTML le indican al navegador dónde mostrar texto o un hipervínculo con otro URL. El formato HTML no es un lenguaje de programación sino un conjunto de direcciones para la visualización de una página.


La capa 6 también es responsable por el cifrado de datos. El cifrado de los datos protege la información durante la transmisión.

La capa de presentación también se ocupa de la compresión de los archivos. La compresión funciona mediante el uso de algoritmos (fórmulas matemáticas complejas) para reducir el tamaño de los archivos.

3.- Equipo y material necesario

Computadora con Sistema Operativo Windows, acceso a Internet, y las siguientes herramientas instaladas:

- Paint
- Mozilla Firefox

	Manual de prácticas del Laboratorio de Redes de Datos Seguras		Código:	MADO-31
			Versión:	03
			Página	151/298
			Sección ISO	8.3
			Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- AxCrypt

4.- Desarrollo

Modo de trabajar

Se trabajará por parejas

4.1. Realización de la práctica

4.1.1 Encienda la computadora y acceda a Windows

4.2. Formato de texto

4.2.1 Abra las aplicaciones de Mozilla Firefox e Internet explorer (puede abrir Internet explorer usando Edge en caso de contar con esta aplicación).

4.2.2 Ingrese a la página [http://es.wikipedia.org/wiki/Facultad_de_Ingenieria_\(UNAM\)](http://es.wikipedia.org/wiki/Facultad_de_Ingenieria_(UNAM)) (ver Figura No. 2.) en ambos navegadores

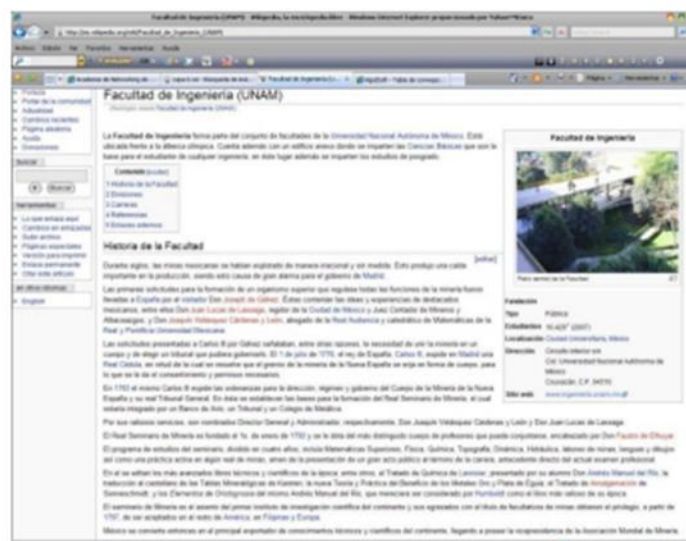



Figura No. 2. Página de Internet con codificación Unicode UTF-8.

4.2.3 En el menú Ver de Mozilla Firefox, elija la opción: Ver > Codificación de Texto> Centroeuropeo (ISO), y espere a que cargue nuevamente la página de Internet (ver Figura No. 3).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	152/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

NOTA: Si no observa la Barra de Menú, dé clic derecho en la parte superior del navegador para habilitar esa opción

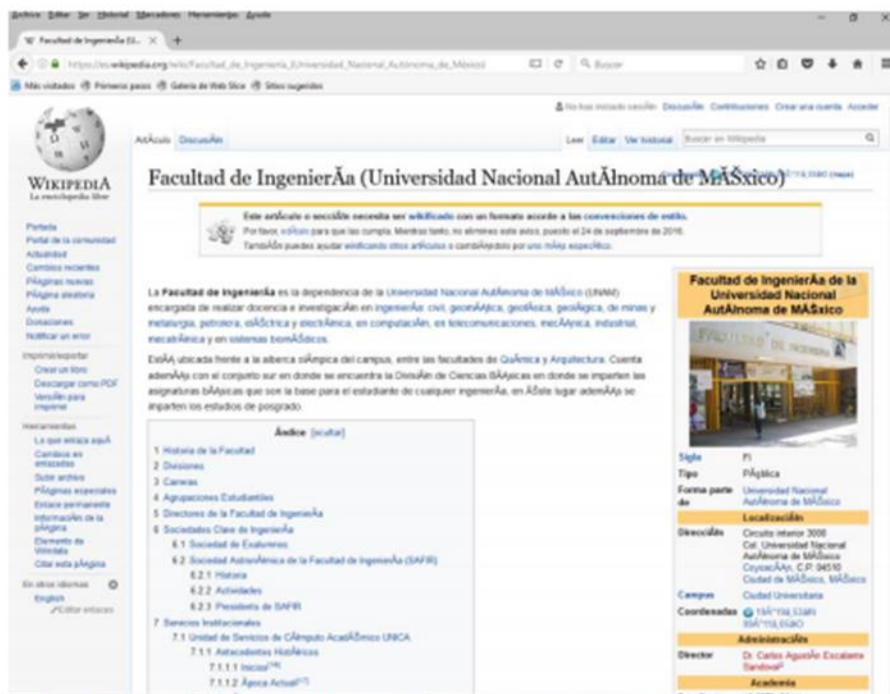



Figura No. 3. Página de Mozilla Firefox con codificación ISO (Centroeuropo).

NOTA: El procedimiento para cambiar la codificación puede variar entre versiones de Mozilla Firefox.

4.2.4 En caso de que haga uso de Edge, para abrir Internet explorer debe dar clic sobre los tres puntos ubicados en la parte superior derecha y posteriormente seleccione la opción Abrir con Internet Explorer, haciendo uso de Internet Explorer elija la opción Ver > Codificación> Más> Centroeuropo (ISO), y espere a que cargue nuevamente la página de Internet (ver Figura No. 3b)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	153/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

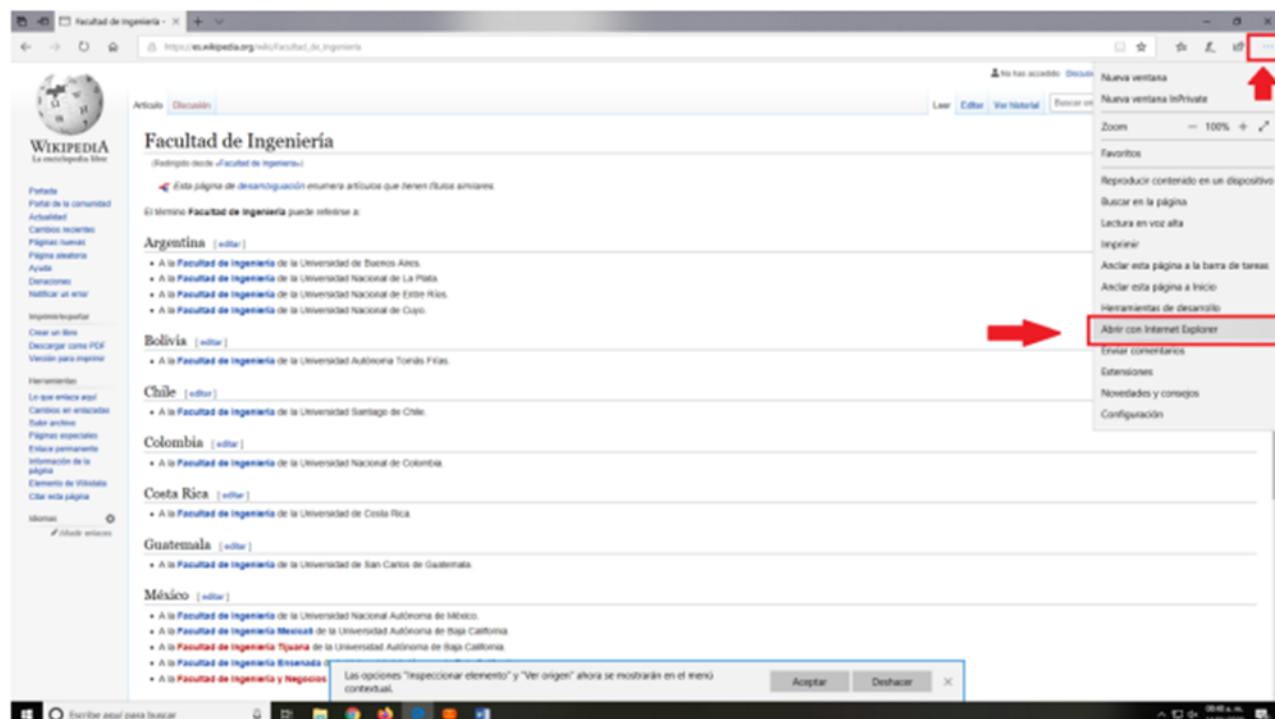


Figura No. 3b. Abrir Internet Explorer desde Edge

4.2.5 Observe la página detenidamente. ¿Fue posible realizar algún cambio en ambos navegadores?, de ser así describa los cambios que hubo entre la página con codificación Unicode e ISO. Si no fue posible cambiar la codificación explique por qué.

No marca los caracteres con acento, puede ser debido a que en ese lenguaje no se utilizan los acentos.


4.2.6 Busque en Internet una tabla de caracteres ISO

4.2.7 Escriba 5 caracteres ISO y su número correspondiente

A	#	2	{		Caracteres ISO8859-1.
Hx: %41	Hx: %23	Hx: %32	Hx: %7B	Hx: %49	Hx: Código hexadecimal
Dc: 65	Dc: 35	Dc: 50	Dc: 123	Dc: 73	Dc: Código decimal
Oc: 0101	Oc: 043	Oc: 062	Oc: 0173	Oc: 0111	Oc: Código Octal
&#: A	&#: #	&#: 2	&#: {	&#: I	&#: Número de entidad HTML

4.2.8 Repita la actividad con una codificación diferente

4.2.9 Del menú Ver de Mozilla Firefox, elija Código fuente de esta página

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	154/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.10 Observe el código fuente de la página de Internet. Y describa el funcionamiento de algunas etiquetas de HTML.

— meta: Información genérica
— title: Título de documento
— link: Vínculo independiente del medio

4.2.11 Mencione cuál es la relación entre el formato HTML y la capa de presentación.

— La capa de presentación interpreta la información contenida de HTML.

4.3 Compresión de datos

4.3.1 Busque y descargue de Internet una imagen de formato bmp, con un tamaño que exceda los 2000 píxeles por 2000 píxeles, y que de preferencia maneje varias tonalidades de colores.

4.3.2 Abra la imagen con el programa Paint y guárdela, pero esta vez con formato jpg (Figura No. 4)

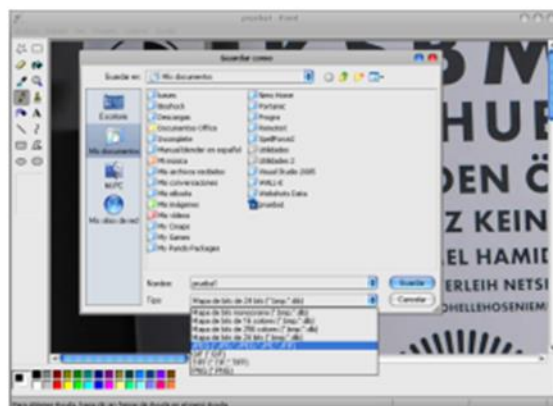



Figura No. 4. Guardando la imagen bmp a jpg.

4.3.3 Abra ambas imágenes en ventanas diferentes. Reajuste las ventanas para poder comparar las imágenes. (ver Figura No. 5)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	155/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

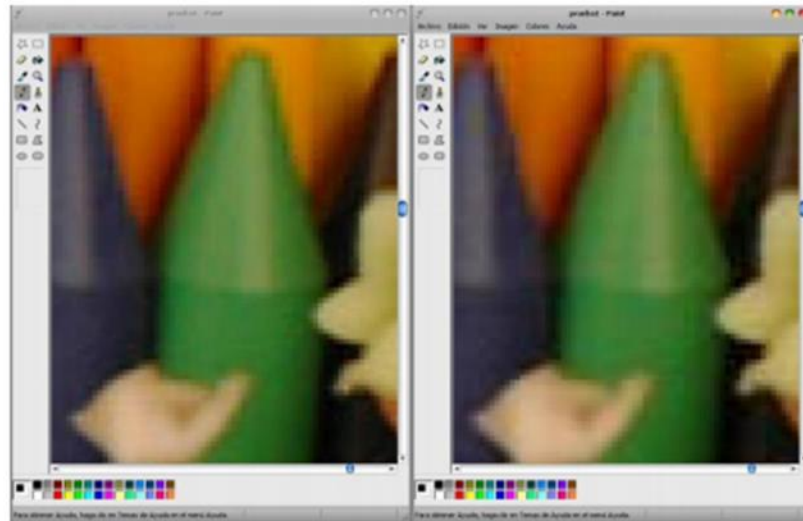


Figura No. 5. Imagen bmp e imagen jpg.

4.3.4 ¿Qué diferencias hay entre las imágenes?

—A simple vista no se nota la diferencia entre ellas, pero al acercarlas podemos observar que en el formato jpg la imagen tiene pérdidas en cuanto a su estructura, ya que pierde calidad y color.—

Nota: Se sugiere que para observar algunas diferencias se haga un acercamiento en ambas imágenes.


4.3.5 ¿Qué diferencias hay entre los formatos bmp y jpg? (Observe el tamaño de ambos archivos y la calidad de las imágenes).

—bmp guarda las imágenes sin pérdida mientras que jpg con pérdida por eso es más pequeño el archivo y se pierden datos.—

4.3.6 Tras haber hecho el análisis anterior, ¿Cómo se podría considerar al formato jpg respecto al bmp, un formato de compresión con pérdida o sin pérdida de datos? (Justifique su respuesta).

—Con pérdidas, ya que comprime más que bmp, por lo tanto, va a guardar menos datos.—

4.3.7 Repita la actividad guardando esta vez la imagen en formato tiff.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	156/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4 Cifrado de Datos

4.4.1 Cree un archivo de texto en el bloc de notas con un mensaje genérico, y guárdelo.

4.4.2 Dé click derecho sobre el archivo, y elija la opción *AxCrypt*-> *Cifrar*. (ver Figura No. 6)

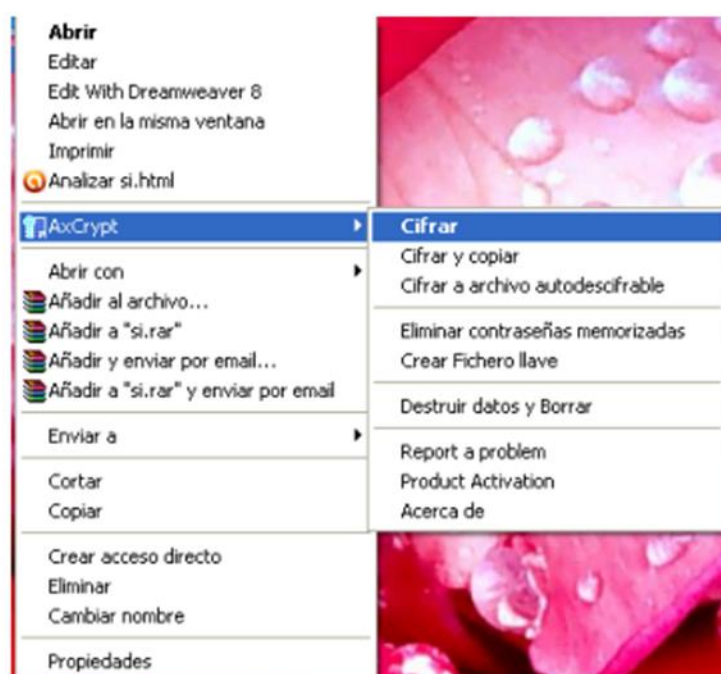


Figura No. 6. Opción de cifrar archivo tras haber instalado AxCrypt.

4.4.3 Introduzca la clave con la que será encriptado el archivo. Tendrá que recordar la clave para descifrar posteriormente el archivo. (ver Figura No. 7)


	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	157/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



Figura No. 7. Ingreso de clave.

4.4.4 Ahora el archivo ha sido reemplazado por un archivo protegido de AxCrypt. Intercambie vía memoria usb o e-mail con uno de sus compañeros, el archivo creado.

4.4.5 Abra con block de notas el archivo que le proporcionó su compañero. ¿Qué observa? ¿Es legible el mensaje que muestra el bloc de notas? (Justifique su respuesta).

No es legible, ya que el archivo está cifrado.


4.4.6 Ahora dé click derecho sobre el archivo, y elija la opción *AxCrypt->Descifrar*. Solicite a su compañero la clave de acceso y vuelva a abrir con block de notas el archivo. ¿Es ahora legible el texto? Describa la función que realiza AxCrypt.

Encripta el archivo con una clave que nos va a pedir al momento de encriptarlo.

4.4.7 Investigue qué tipo de cifrado emplea AxCrypt El cifrado usado es AES-128 y SHA-1.

Advanced Encryption Standard (AES): El estándar de cifrado avanzado, describe una fórmula matemática o algoritmo, para la conversión de datos electrónicos en una forma ininteligible, denominada texto cifrado. El texto cifrado no puede ser leído por cualquier persona que no sea el destinatario. El AES funciona alimentando una clave de cifrado, esencialmente una cadena de dígitos en el algoritmo de cifrado y realizando de una serie de operaciones matemáticas basadas en esa clave de cifrado.

Secure Hash Algorithm (SHA1): Es una función hash criptográfica ampliamente utilizado, que genera un 160 bits (20 bytes) hash a partir de cualquier valor de entrada. Esto se utiliza para calcular un valor de comprobación única para todos los datos digitales (mensajes) de no más de 264 -1 bit (≈ 2 exbibyte) de longitud y es la base para la creación de una firma digital.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	158/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4.8 ¿Esta actividad simula un tipo de cifrado con Clave Pública o Privada? (Justifique su respuesta).

Cifrado con clave privada, ya que solo abre si se introduce esa clave privada.

4.4.9 Realice la actividad extra que le deje el profesor

4.4.10 Cierre la sesión.

5.- Cuestionario

1. ¿Para qué sirve el programa AxCrypt?

AxCrypt es un programa open source gratuito para cifrar y descifrar datos que utiliza el algoritmo AES con un largo de clave de 128 bits y de esta manera proteger los datos con una clave.

2. Mencione algunas aplicaciones de la criptografía.


- Cifrado de datos: Garantizar la confidencialidad de los documentos aunque estos resulten accesibles a personas no autorizadas.
- Firma electrónica: Para conseguir dos de las características de seguridad: integridad y autenticación.
- Certificados digitales: los que utilizan una clave pública y una clave privada, fueron diseñados para poder intercambiar información de manera segura sin necesidad de haber acordado previamente una clave secreta de cifrado.
- Seguridad en medios electrónicos: Análogamente se aplican cifrados simétricos con claves autogeneradas y luego dichas claves se cifran con algoritmos asimétricos.

3. Mencione algunas aplicaciones de la compresión de datos y en qué situaciones se usaría compresión con pérdida de datos.

— La compresión de datos es común para cuando se requiere transferir archivos, en el caso de compresión de datos con pérdida un ejemplo sería para pasar archivos de imágenes como jpg, debido a que la información perdida no es tan importante porque se logra ver bien a simple vista.

4. Menciona en qué situaciones se usaría compresión sin pérdida de datos.

— Para transferir archivos de importancia como archivos de texto, en donde se requiere que la información llegue completa y no haya pérdida de paquetes, por ejemplo, en el caso de un zip, se comprime para que pese menos y el paquete llegue completo, es decir compresión sin pérdidas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	159/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5. Investigue la relación entre las formas de codificación de texto que maneja Mozilla Firefox y el código ASCII.

- Sería por la página de código, ya que ahí va a estar definido el lenguaje en el que se verá la página y la estructura. La relación podría ser el tipo de lenguaje que se usa a través de símbolos para representar los caracteres.

6.- Anote sus Conclusiones u Observaciones; revisando los objetivos planteados al inicio de la práctica:

Conclusiones:

Yerenia Amado: En esta práctica vimos la capa 6 de presentación del modelo OSI en donde comprendimos las funciones principales que tiene, como formato de datos, cifrado y compresión. Aprendimos a cifrar archivos con clave, utilizando el programa AxCrypt y vimos la diferencia entre la compresión de datos con pérdida que aplica para las imágenes, mp3 etc. y sin pérdida que se usa para archivos de texto principalmente.

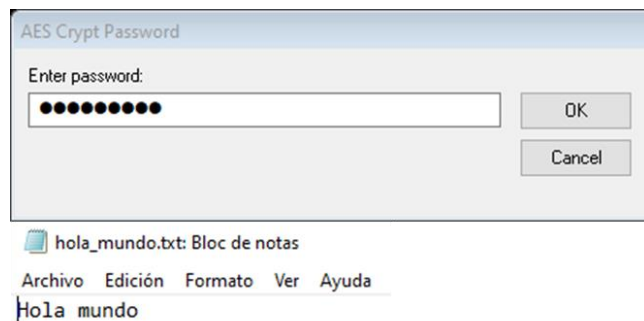
Guadalupe Moreno: La capa de presentación se encarga del formato y representación de los datos. Sus funciones principales son: Formateo de datos, Cifrado de datos y Compresión de datos. Después de recibir los datos de la capa de aplicación, la capa de presentación ejecuta una de sus funciones, o todas ellas, con los datos antes de mandarlos a la capa de sesión. También pudimos darnos cuenta que al modificar el formato de cualquier imagen de png a jpg hay una clara disminución en los valores de resolución de la misma, podemos observar que existe una pérdida de nitidez en la imagen.

Referencias:

- <https://www.cdmon.com/es/tabla-caracteres>
- https://techlandia.com/funciona-aes-info_215975/
- <https://www.sha1-generator.info/es/cual-es-sha1-hash>
- <https://www.strato.es/faq/disco-duro-online/que-es-axcrypt-y-como-se-utiliza/>
- https://www.icaei.es/contenidos/publicaciones/anales_get.php?id=1235

The screenshot shows a Windows desktop with a dark background. A file named 'hola_mundo.txt' is selected, and a context menu is open. The menu options are: 'Abrir', 'Imprimir', 'Editar', 'AES Encrypt', and 'Edit with Notepad++'. Below the menu is a dialog box titled 'AES Crypt Password'. The dialog has two input fields: 'Enter password:' and 'Confirm password:'. Each field contains a password mask of 12 dots. To the right of each field are buttons for 'OK' and 'Cancel'.

Si la contraseña es correcta se crea el archivo decodificado



AES Crypt Progress

Decrypting...
C:\Users\Guadalupe
Moreno\Desktop\hola_mundo.txt.aes

Cancel

AES Crypt Error

Error in file C:\Users\Guadalupe Moreno\Desktop\hola_mundo.txt.aes
Message has been altered or password is incorrect

Aceptar

hola_mundo.txt.aes

```

1 AES-256-GCM-CREATED_BY_NUAAescrypt (Windows GUI) 3.10-NUAA-NUAA-NUAA
2 USet?,ILO?eMVI°L«S 6û 988°IYÊSIZôI«ZSYNRâçcB+US-UNUøIS
3 ôEOTAB"wAOBSRvø°JPô,cEOPYzZùETEdcPXNù:øj~

```