
	<p align="center">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p align="center">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p align="center">Código: GUIA-PRLE-001</p>	<p align="right">Página: 1</p>

INFORME DE LABORATORIO

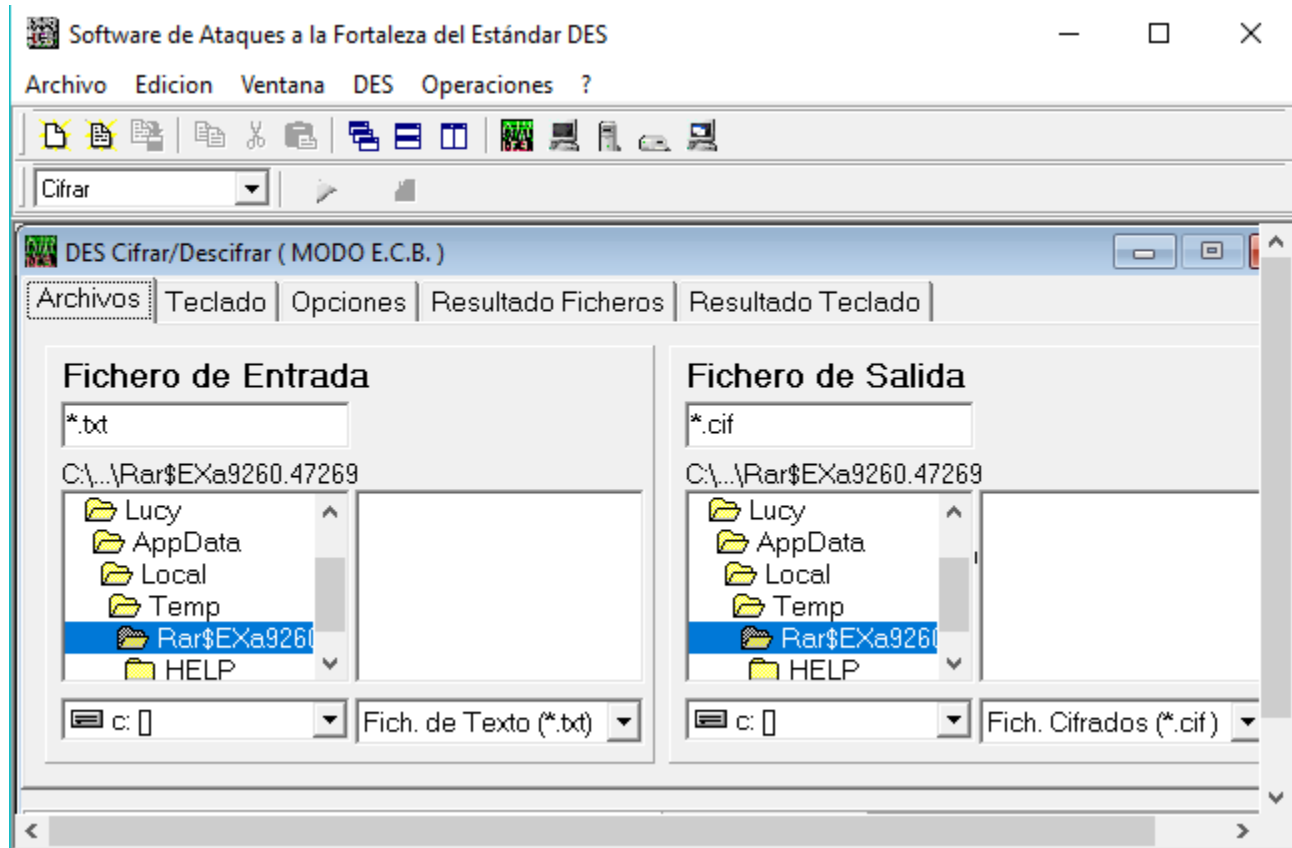
(formato estudiante)

INFORMACIÓN BÁSICA					
ASIGNATURA:	Seguridad Informatica				
TÍTULO DE LA PRÁCTICA:	<i>CRIPTOGRAFÍA MODERNA CIFRADO POR BLOQUES</i>				
NÚMERO DE PRÁCTICA:	<i>04</i>	AÑO LECTIVO:	<i>2023</i>	NRO. SEMESTRE:	<i>A</i>
FECHA DE PRESENTACIÓN	<i>16/07/2023</i>	HORA DE PRESENTACIÓN			
INTEGRANTE (s): Yoset Cozco Mauri				NOTA:	
DOCENTE(s): <i>Juan carlos Zuñiga</i>					

SOLUCIÓN Y RESULTADOS

SOLUCIÓN DE EJERCICIOS/PROBLEMAS

2. Seleccione DES/ Cifrar/Descifrar, por defecto en modo E.C.B



a) En el folder teclado, ingresa el texto claro en modo hexadecimal.

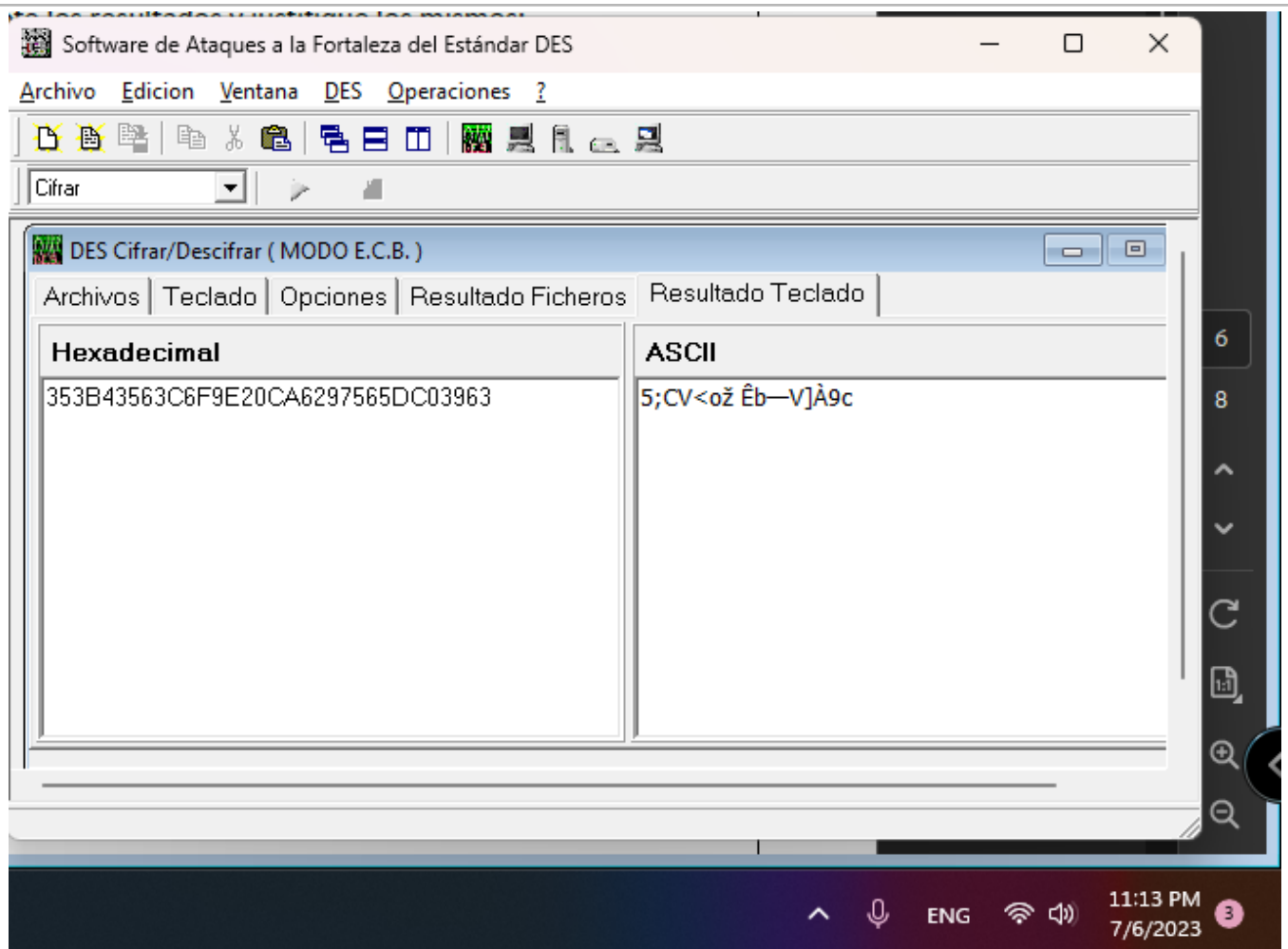
MHEX = 5656565656565656

En el folder opciones, ingresa la clave en modo hexadecimal.

KHEX = 0E439232EB6D1D62

y selecciona el Procesar hacia la opción Teclado

Seleccionar Operaciones/Comenzar o play.



b) Anote el resultado del folder Resultado Teclado en ASCII y hexadecimal

CHEX=6C2E1472D0CE5465

CASCII=I._rĐîTe

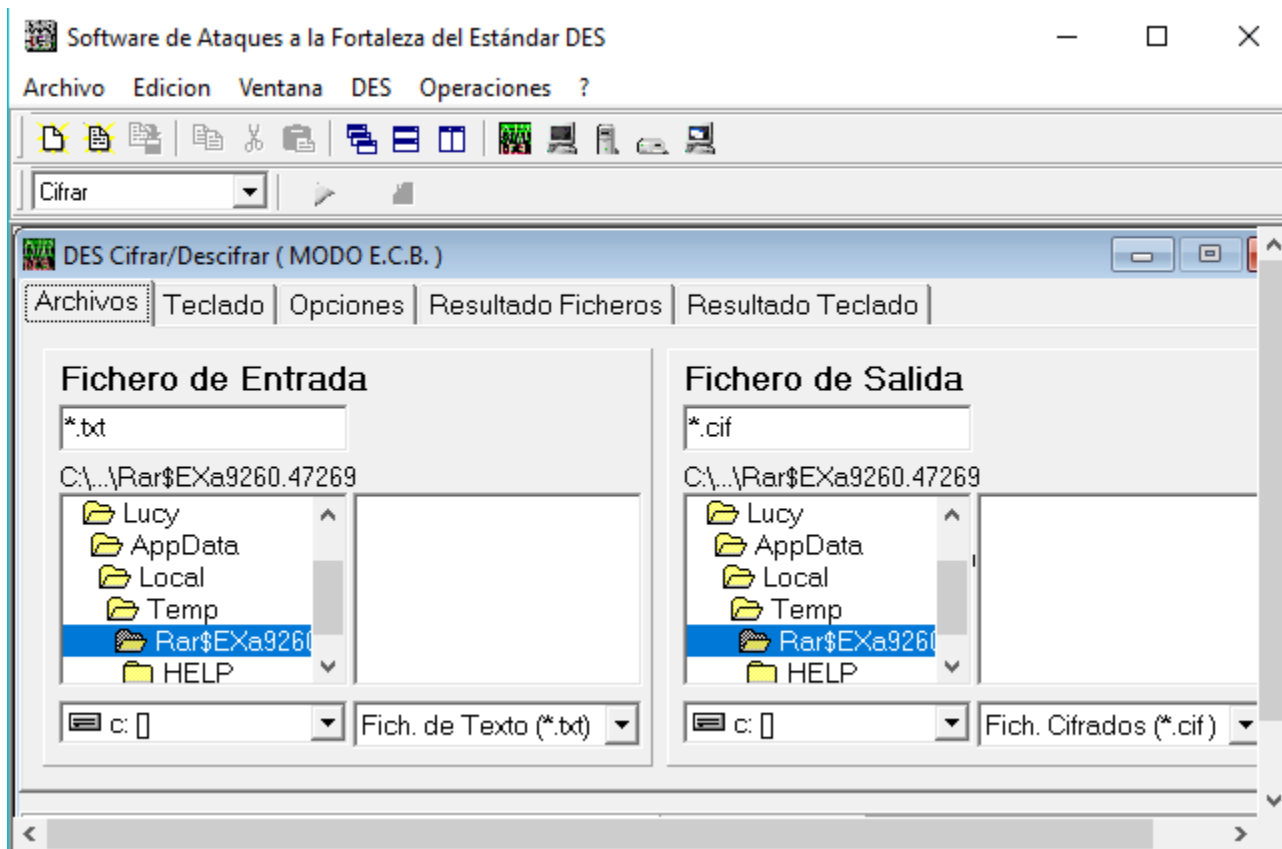
c) Descifre el resultado hexadecimal, anote la respuesta e interprete el resultado

M' HEX=5656565656565656

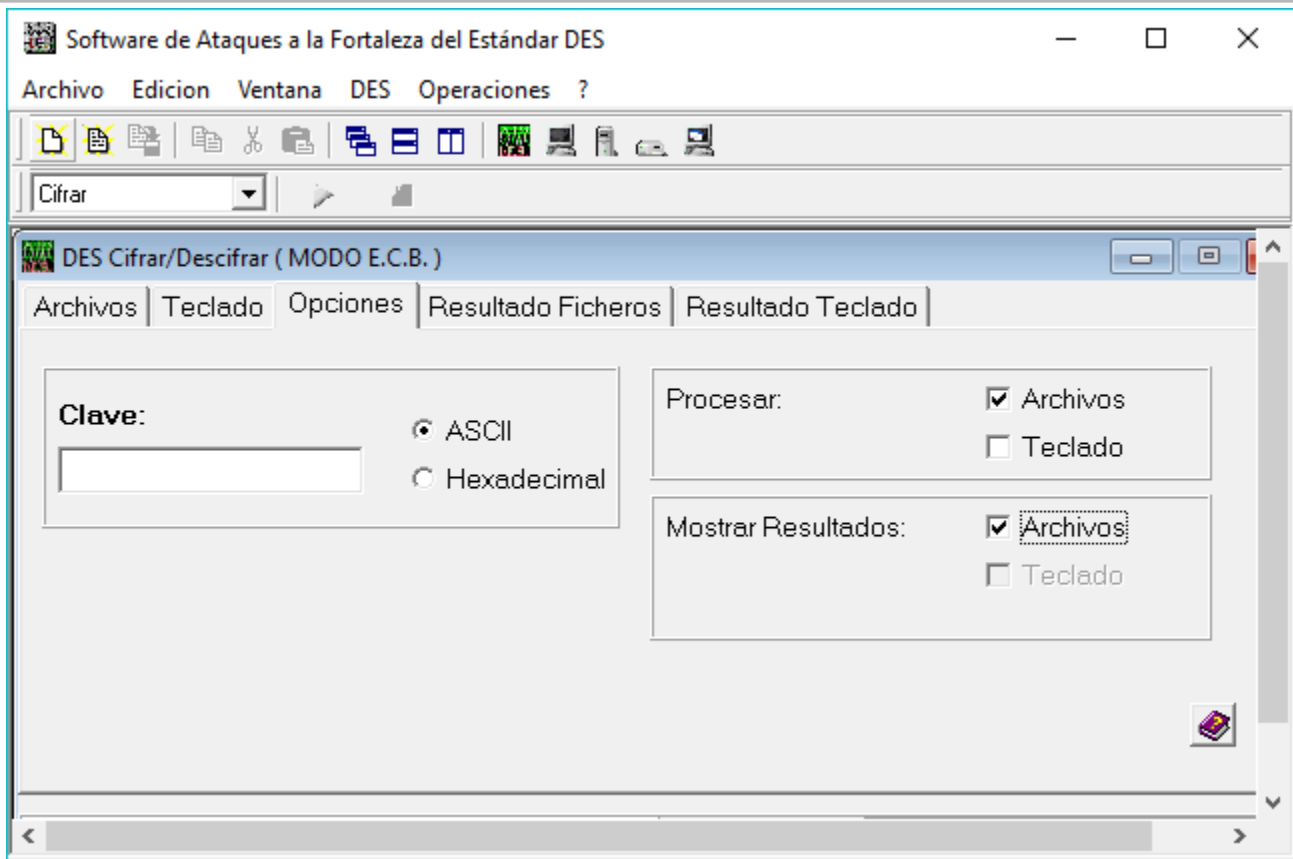
M'ASCII=VVVVVVVV

ARCHIVOS DE CIFRADO SIMÉTRICO DES

Cree el archivo “prueba.txt” llenando sus apellidos, nombres y código, elija la opción cifrar y en el folder Archivos en Fichero de Entrada seleccione el archivo creado, en el folder Fichero de Salida definir el archivo “PruebaClaro.cif”

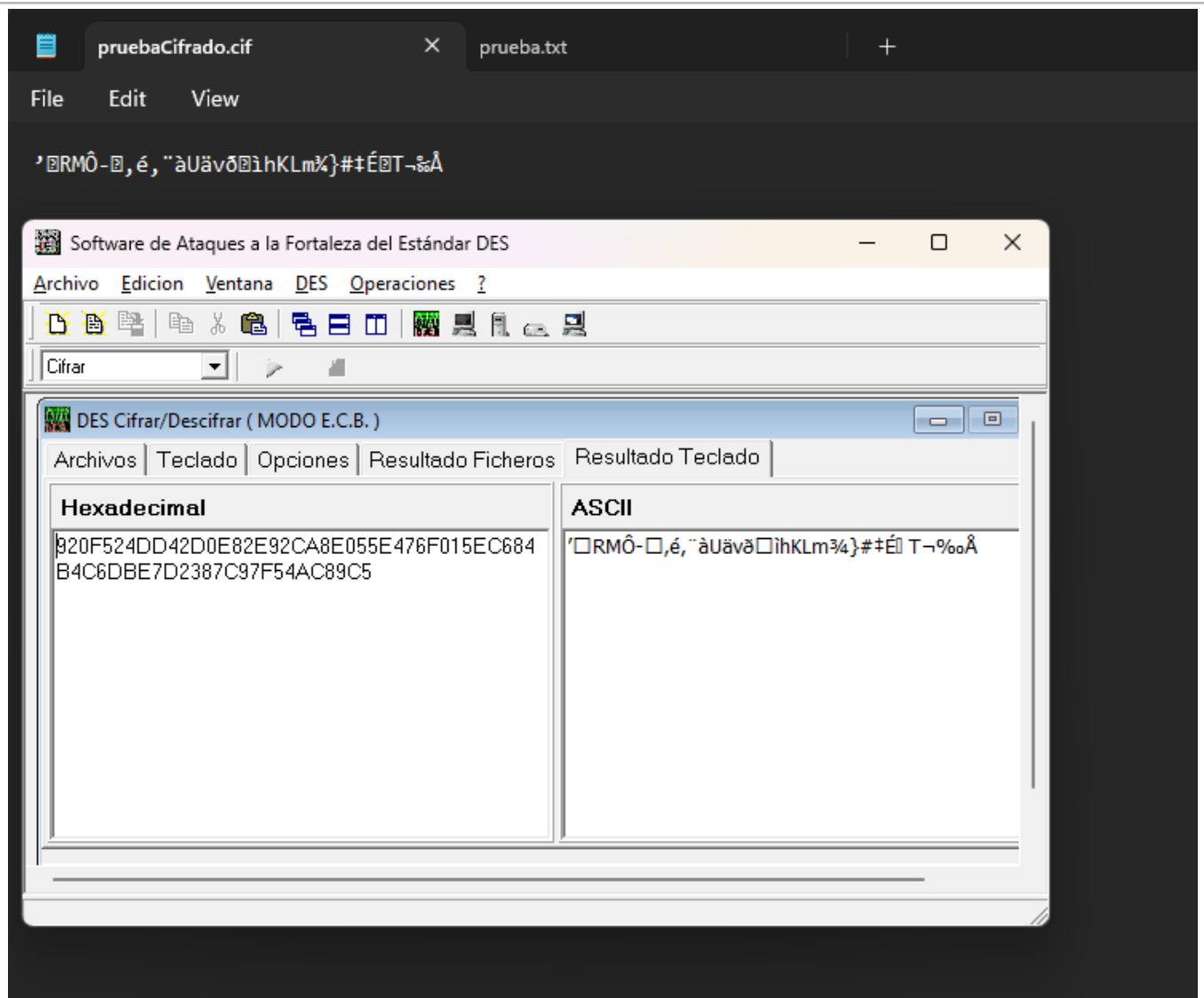


En el folder Opciones defina Procesar y Mostrar Resultados con la opción Archivos. Finalmente ingrese una clave ASCII de 8 caracteres e inicie el cifrado, guarde el resultado en el archivo “PruebaCifrado.cif”



Muestre el archivo generado a partir del block de notas

Genere el archivo "PruebaDescifrado.cif" a partir del proceso de descifrado, muestre los resultados y compare con el archivo de cifrado



Los resultados son totalmente iguales.

Ejercicios propuestos:

1. Cifre considerando los valores hexadecimales. Anote los resultados y justifique los mismos:

a) MHEX = 6503100E95ACBDEE

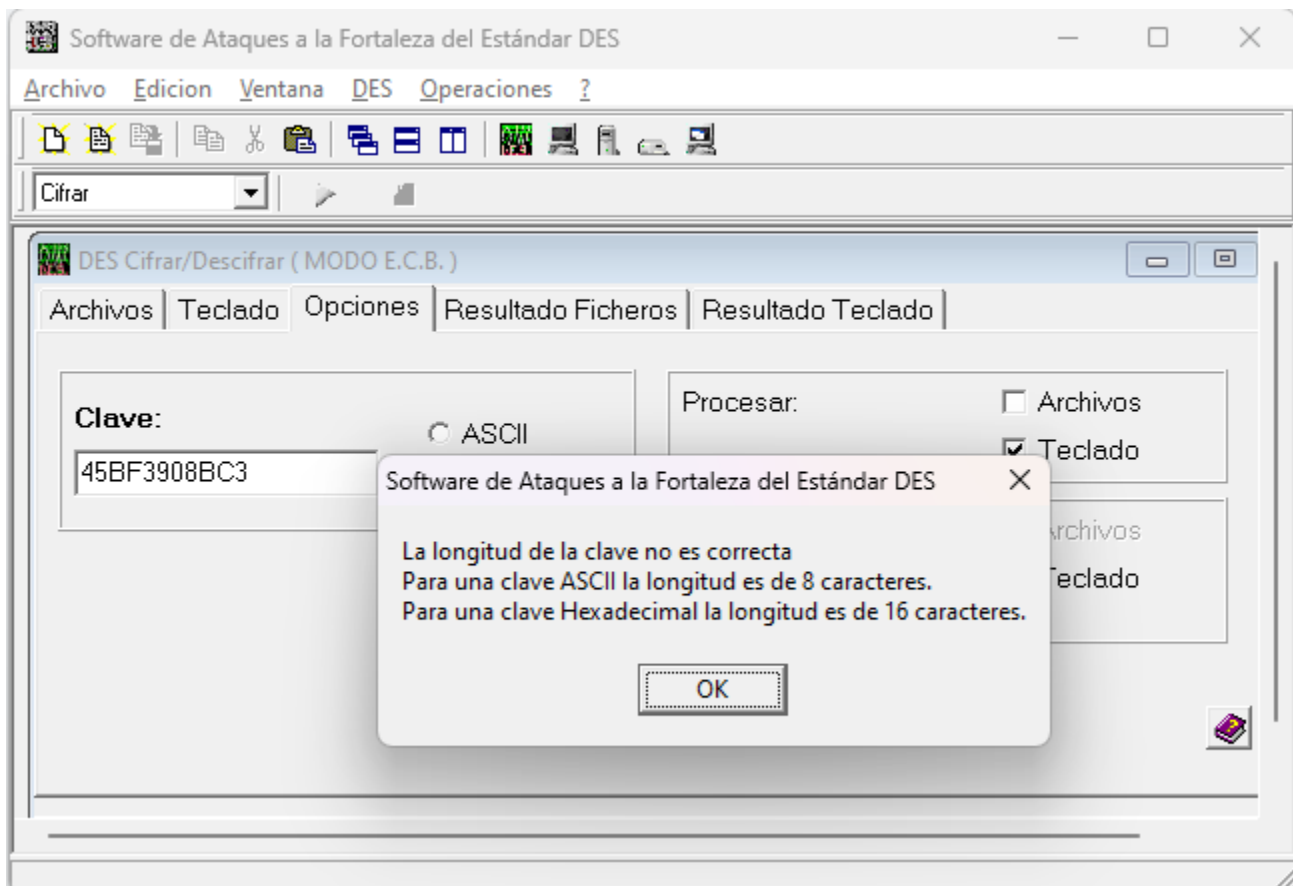
KHEX = 0123456789ABCDEF

CHEX =2B5FF3390EABDF15524532DE180E1007

b) MHEX = 56CC3000E012F08B

KHEX = 45BF3908BC3

CHEX =



2. Cifre considerando los valores ASCII. Anote los resultados y justifique los mismos:

a) MASCII = CIBERSEGURIDADWEB

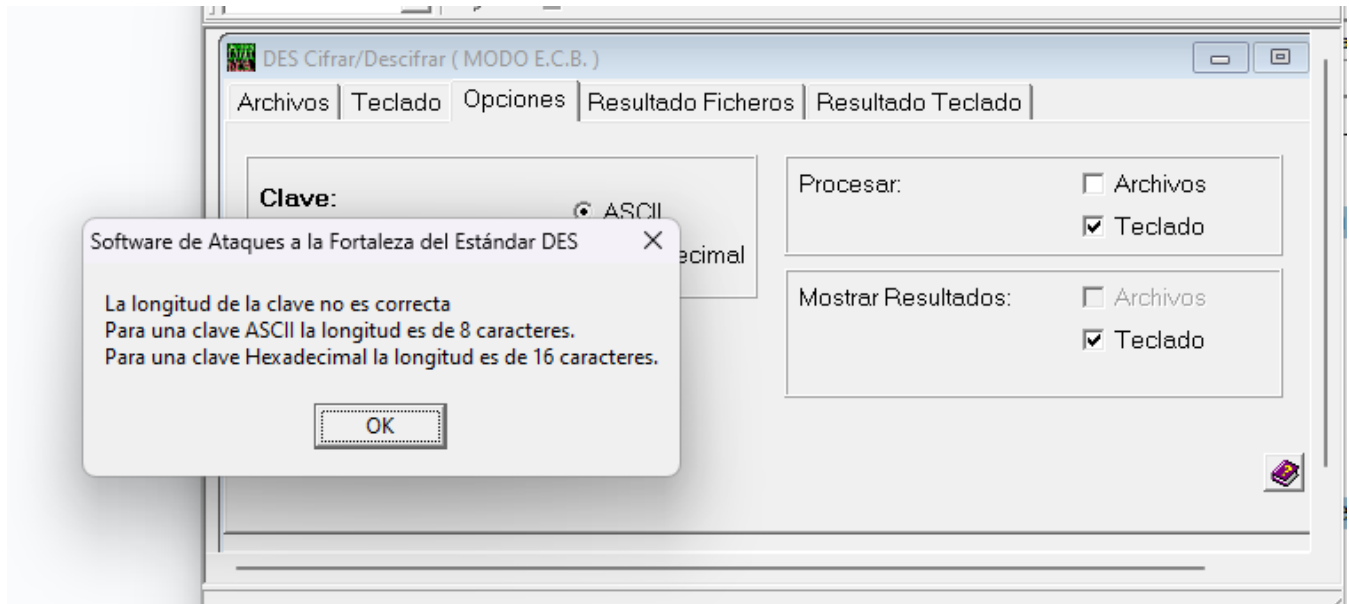
KASCII = ESPECIAL

CHEX =A266172476EA6DA0DF33901C4E6CEC6D73D1F7A9D60C4A44

b) MASCII = MISEGURIDAD

KASCI = LLAVE

CHEX =



3. Cifre considerando el texto y la clave ASCII

a) MASCI = "Seguridad en Redes con la clave en ASCII"

KASCI = FFFFFFFF

CHEX

=74D40DD80A5902E6936CE7A44D90AC33ACD225DF383240CF00597C124C171C3F9487DDEB9AA6165
1


b) MASCI = "Seguridad en Redes con la clave en ASCII"

KASCI = EEEEEEEE

CHEX

=1C883BF37869B653870D11B04733965146FCA39B018CBCDB6717403BCB54B3DC704E46ACECDC6CE
C

Compare los resultados, observando que las claves difieren en unos cuantos bits, explique los resultados.

	<p style="text-align: center;">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p style="text-align: center;">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLE-001</p>	<p>Página: 9</p>

En ambos casos, se utiliza el mismo mensaje y se observa que el texto cifrado (CHEX) es diferente. Esto se debe a que el cifrado DES es altamente dependiente de la clave utilizada. Incluso un cambio pequeño en la clave puede generar un resultado completamente diferente.

4. Compare los resultados de cifrar el mensaje de 8 bytes MASCII = ENCRIPTO con KASCII = CLAVEDES y el mensaje de 12 bytes MASCII = ENCRIPCIÓN usando la misma clave

Chex 01 = 2E4DC8380A2E6B96

Chex02 = 3991CF8D8439B44E1946D2CF976D60A0

La diferencia en los resultados se debe a que el cifrado DES en modo ECB cifra cada bloque de manera independiente, lo que resulta en diferentes resultados de cifrado para mensajes de diferentes longitudes, incluso cuando se utiliza la misma clave.

CLAVES DÉBILES Y SEMIDÉBILES EN DES

ASEGÚRESE DE HACER EL INGRESO DE TEXTO Y CLAVES EN FORMATO HEXADECIMAL, AYÚDESE DEL PORTAPAPELES

5. Cifrar el mensaje M = “En este punto vamos a usar el proceso de cifrado para demostrar lo que significa el concepto de claves débiles en el algoritmo DES” utilice las siguientes claves y demuestre que se cumpla que $M = E_k[E_k(M)]$, donde E_k representa el algoritmo de encriptación corrido con la clave K

MHEX

=456E20657374652070756E746F2076616D6F732061207573617220656C2070726F6365736F206465206369667261646F20707565646F2064656D6F7374726172206C6F20717565207369676E69666963612E

● K1 HEX = 0101010101010101

CHEX K1 = 920F524DD42D0E82E92CA8E055E476F015EC684B4C6DBE7D2387C97F54AC89C5



C'HEXK1 = M'HEXK1

● K2 HEX = E0E0E0E0F1F1F1F1

CHEX K2 = F3076AF87C060B62070D0C60D32B6D5C

C'HEXK2 =

● K3 HEX = 1F1F1F1F0E0E0E0E

	<p style="text-align: center;">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p style="text-align: center;">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLE-001</p>	<p>Página: 10</p>

CHEX K3 =2C26360361E94D57B4D98A8C3136027F

C'HEXK3 =

6. Cifrar el mensaje M = "En este punto vamos a usar el proceso de cifrado para demostrar lo que significa el concepto de claves semidébiles en el algoritmo DES". utilice las siguientes claves y demuestre que se cumpla que $M = E_{K1}[E_{K2}(M)]$, donde EK representa el algoritmo de encriptación corrido con la clave K

MHEX

=456E20657374652070756E746F2076616D6F732061207573617220656C2070726F6365736F206465206369667261646F20707565646F2064656D6F7374726172206C6F20617573617220656C2070726F6365736F20646520636C617665732073656D696465626C657320656E20656C20616C676F7269746D6F20444553

● K1 HEX = 01FE01FE01FE01FE K2 HEX = FE01FE01FE01FE01

CHEX K1 =4FDEA21FCD7FCA4AABF7C0B394B26CC5

C'HEX K2 = M'HEXK1

● K1 HEX = 1FE01FE00EF10EF1 K2 HEX = E01FE01FF10EF10E

CHEX K1 = 4FDEA21FCD7FCA4AABF7C0B394B26CC5

C'HEX K2 = 4ED5DB3E1FA2D5037E8E7841022A6FF5

DES EN MODO CBC

7. Asumiendo un modo de cifrado CBC encriptar usando KHEX=534C68D48AEADFF2, MASCI="vamos a cifrar el mensaje usando DES en modo CBC", si IVHEX=DA5BEEF16B26983D, si lo necesita recuerde que puede usar alguna calculadora disponibles en Internet

Calculadora on-line convertidor (1)

<https://www.rapidtables.com/convert/number/ascii-to-hex.html>

Calculadora on-line operaciones (2)

<https://toolslick.com/math/bitwise/xor-calculator>

a) Convertir el mensaje a hexadecimal usando (1) y definir los bloques a cifrar, llene la segunda columna de la TABLA 1

b) Operar la función XOR usando (2), entre cada bloque del mensaje claro Operando1 y el texto cifrado del bloque anterior Operando2 (salvo en el primer bloque donde deberá usar el IV, llene la cuarta columna de la TABLA 1

c) Cifrar el resultado de la operación XOR, llene la quinta columna de la TABLA 1

d) Repetir hasta completar la totalidad de bloques e indicar el resultado del cifrado

bloque	Operando 1	Operando 2	Salida XOR	Cifrado DES
1	76616D6F732061 20	DA5BEEF16B2698 3D	A33E83DF1956C1 7D	E0537D22C69ABF 5C
2	63696672617220 65	E0537D22C69ABF 5C	A30C1E5455FD9F 39	F5D132EA827E6A 2B
3	6C206D656E7361 6A	F5D132EA827E6A 2B	91130D84A15BB D01	129FC6C26EE836 9D
4	65207573616E64 6F	129FC6C26EE836 9D	74BDA0E44D0FF4 94	1EF876C26AA55D 94
5	2044455320656E 20	1EF876C26AA55D 94	3E3F32F46F4F394 4	6B4C59DD635B34 66
6	6D6F646F204342 43	6B4C59DD635B34 66	6B7D0C09C66E86 35	11F0F5A9D66A82 84

I. SOLUCIÓN DEL CUESTIONARIO

1. Visualize el video <https://www.youtube.com/watch?v=2ssaCyXRJIU>, luego responda

a) Describa funcionalmente los modos de cifrado por bloque, indicando en cada caso las fortalezas, debilidades y aplicaciones

Los modos de cifrado por bloque son técnicas utilizadas en criptografía para cifrar mensajes divididos en bloques de datos de tamaño fijo.

Algunos modos comunes son ECB, CBC, CFB, OFB y CTR:

- *ECB cifra cada bloque de forma independiente, lo que puede revelar patrones repetitivos.*

- CBC introduce aleatoriedad y oculta patrones repetitivos al cifrar cada bloque utilizando el resultado del cifrado anterior.
- CFB y OFB transforman el cifrador en un cifrado de flujo utilizando la salida del cifrado anterior como retroalimentación.
- CTR utiliza una función de contador para combinar una secuencia de bits con el mensaje original.

b) Defina claramente el concepto de fortaleza de clave

La fortaleza de clave se refiere a la resistencia de una clave criptográfica a los intentos de descifrado sin autorización.

Una clave fuerte tiene alta entropía y es resistente a ataques de fuerza bruta o criptoanálisis.

2. ¿Por qué AES reemplaza a DES?

- AES reemplaza a DES debido a su mayor seguridad, ya que admite claves más largas y tiene un tamaño de bloque fijo.
- AES es más eficiente y resistente a ciertos ataques criptoanalíticos, lo que lo hace más adecuado para aplicaciones de seguridad en la actualidad.

II. CONCLUSIONES

Este laboratorio me ha brindado información para entender que la criptografía es fundamental para la seguridad de la información y abarca conceptos como algoritmos de cifrado simétrico, modos de cifrado por bloque y la importancia de utilizar claves seguras. Los algoritmos como DES y AES ofrecen diferentes niveles de seguridad y eficiencia, y AES ha reemplazado a DES debido a su mayor seguridad. Comprender estos conceptos es crucial para proteger la información en entornos digitales y garantizar la confidencialidad, integridad y autenticidad de los datos.

RETROALIMENTACIÓN GENERAL**REFERENCIAS Y BIBLIOGRAFÍA**



UNIVERSIDAD NACIONAL DE SAN AGUSTIN
FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA



Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación

Aprobación: 2022/03/01

Código: GUIA-PRLE-001

Página: 13

Gómez, S., Arias, J. D., & Agudelo, D. (2012). Cripto-análisis sobre métodos clásicos de cifrado. Scientia et technica, 2(50), 97-102.