

Laboratorio #4

Cifrado por Bloques: El Algoritmo DES/AES

Alumna: Sharon Rossely Chullunquia Rosas
Docente: Franklin Luis Antonio Cruz Gamero
Fecha: 19 de octubre de 2021

Arequipa, Perú

1. Cuestionario Previo

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

1. Describa funcionalmente el cifrado por flujo, ejemplifique

Se habla de cifrado por flujo cuando se realiza el cifrado bit a bit o byte a byte, es decir, una operación entre cada bit o byte del texto en claro con el correspondiente bit o byte de una clave binaria.

Ejemplos del cifrado por flujo son:

- El algoritmo A5 (Ejemplo de cifrado en flujo por bits)
- El algoritmo RC4 (Ejemplo de cifrado en flujo por bytes)

2. Describa funcionalmente el cifrado por bloque, ejemplifique

En el cifrado por bloque, la información para cifrar es separada por bloques de 8 bytes o 64 bits, como en DES, 3DES e IDEA, o bien 128 bits (16 bytes), como es el caso en AES, Serpent y Twofish.

Un ejemplo es Serpent, que toma bloques de tamaño fijo del texto plano y se produce un bloque de tamaño fijo de texto cifrado, generalmente del mismo tamaño que la entrada.

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

Según (Dworkin, 2001), los modos de cifrado por bloque son:

a) Modo CBC (Cipher-block Chaining):

En el modo CBC, la entrada del algoritmo de cifrado es el resultado de la operación XOR entre el actual bloque de texto plano a cifrar y el bloque de texto cifrado precedente. Se utiliza la misma clave en cada bloque.

En fortalezas, evita el ataque por repetición de bloque, enmascara el mensaje. En debilidades, existe la necesidad de realizar el cifrado de forma secuencial y existen ataques que se basan en el conocimiento del vector IV. Es aplicado en las estructuras como, DES, IDEA, RC2 y RC5.

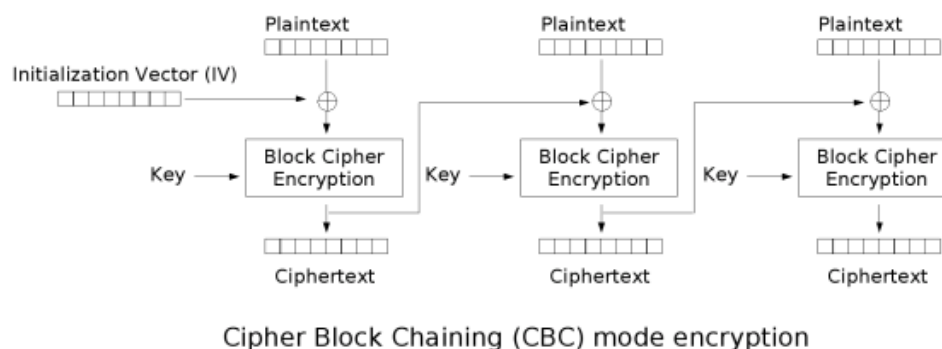


Figura 1: Cifrado con el modo CBC

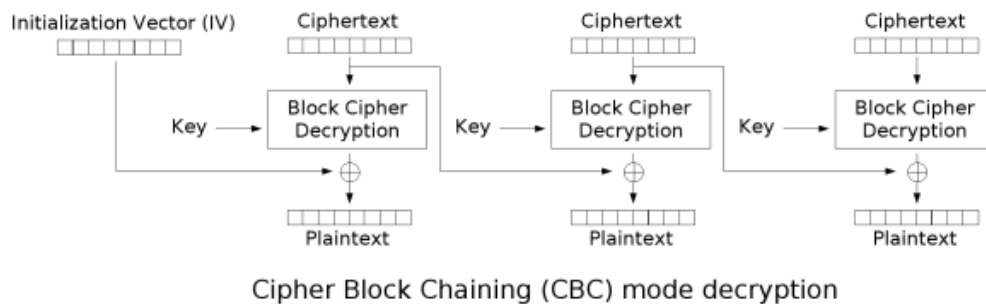


Figura 2: Descifrado con el modo CBC

b) Modo CTR (Counter Mode):

Este modo imita un cifrado de flujo, se utiliza un cifrado de bloque para generar un flujo pseudo aleatorio (keystream), que se mezcla con el texto plano a través de XOR dando lugar al cifrado. Para producir el keystream se cifra un contador combinado con un número aleatorio (nonce) mediante ECB y se va incrementando.

Como debilidad, reutiliza un contador en la misma clave que puede acabar con la seguridad del sistema, ya que generará de nuevo el mismo keystream. En fortalezas, CTR acentúa la posibilidad de precalcular el keystream y que revela poca información sobre la clave.

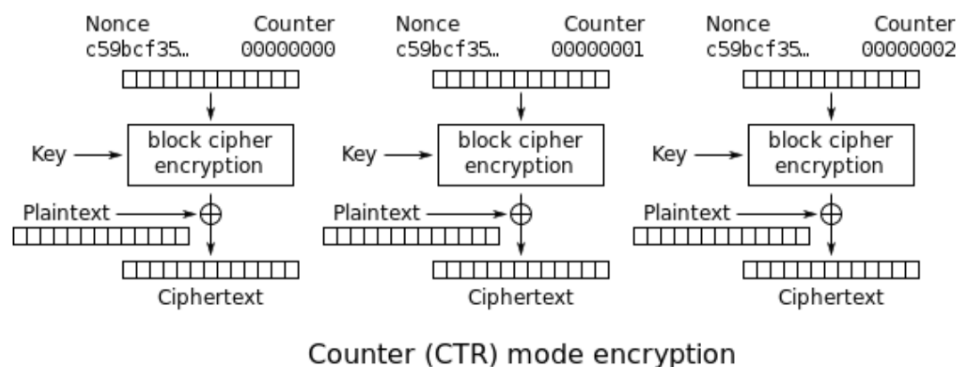


Figura 3: Cifrado en modo contador

c) Modo ECB (Electronic Codebook Mode):

En el modo ECB, cada bloque de longitud es cifrado de forma independiente. El texto cifrado es una sucesión de los bloques cifrados. Y el descifrado se realiza aplicando el algoritmo inverso a cada bloque del criptograma, también de manera independiente a los demás criptogramas. Este modo se emplea para el envío de valores sencillos. Estructuras que utilizan este modo; Des, 3Des, IDEA, RC5, RC4.

En debilidades, es posible reconocer patrones en el texto cifrado y es difícil de detectar si un atacante sustituye algunos bloques del texto cifrado con otros blo-

ques cifrados que hayan sido cifrados con la misma clave. En fortalezas, permite codificar bloques independientemente del orden en que estén y es resistente a errores

Una aplicación del modo ECB es el videojuego en línea Phantasy Star Online: Blue Burst que usa Blowfish en modo ECB.

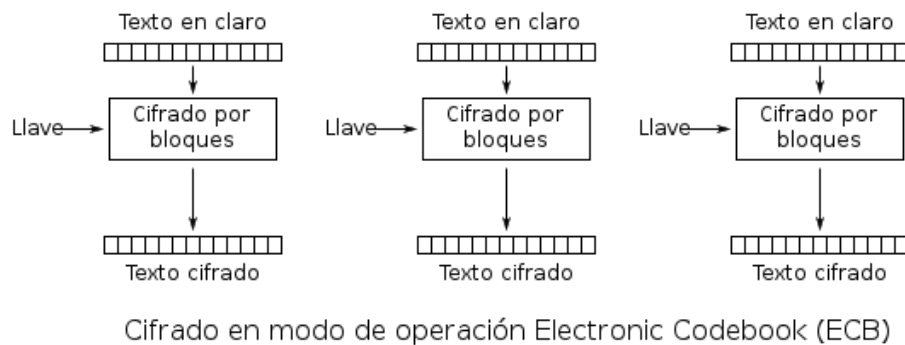


Figura 4: Modo ECB

d) Modo OFB (Output FeedBack):

Utiliza un bloque para cifrar de longitud n y lo divide en $enu = \frac{n}{r}$ sub-bloques con $1 \leq r \leq n$, y un vector de inicialización. El keystream se genera realizando el cifrado al anterior keystream, logrando dar lugar al siguiente bloque. Una fortaleza de este modo es que los errores de bit en la transmisión no se extienden. En debilidades, este modo es vulnerable a ataques por modificación de la cadena del mensaje. Este modo se aplica en estructuras como, DES, IDEA, RC2, RC5.

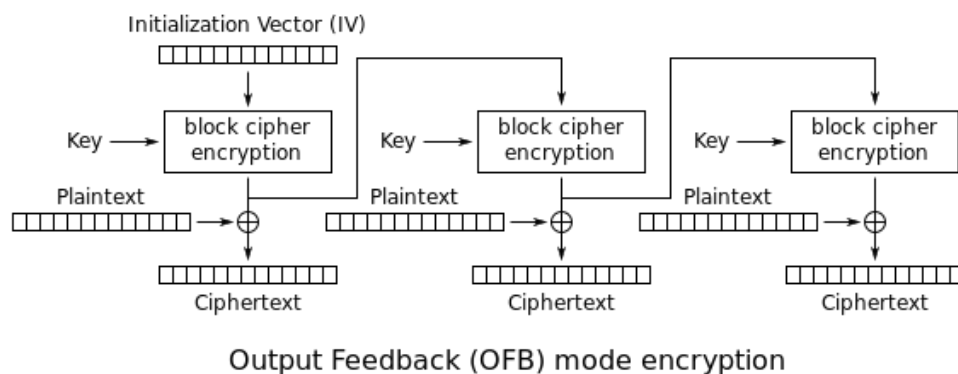


Figura 5: Encriptación en Modo OFB

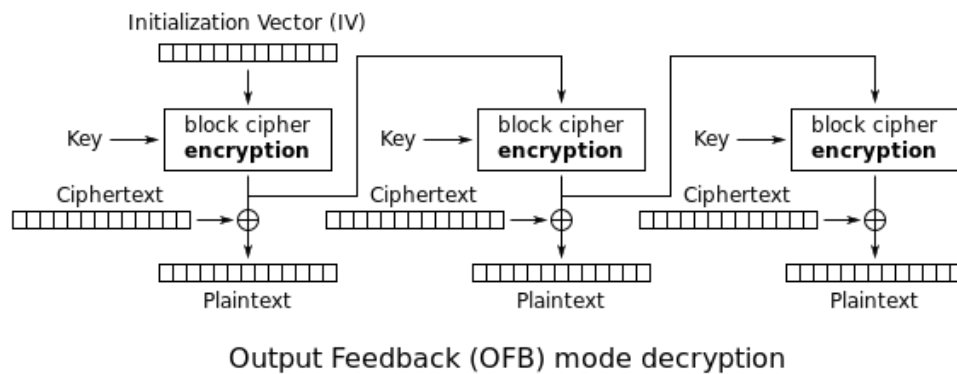


Figura 6: Descriptación en Modo OFB

- e) **Modo PCBC (Propagating Cipher-Block Chaining):** El modo Propagating Cipher-Block Chaining (PCBC) fue diseñado con el fin de que pequeños cambios en el texto ya cifrado se propaguen más que en el modo CBC. (Wikipedia contributors, 2020)

Tiene la debilidad de no poder ser paralelizable en la encriptación y descriptación.

Sus fortalezas son, cada encriptación solicita que intervengan el bloque de texto cifrado anterior y el bloque de texto sin formato. Y las pequeñas modificaciones en el texto sin formato cambiarán todos los textos cifrados posteriores.

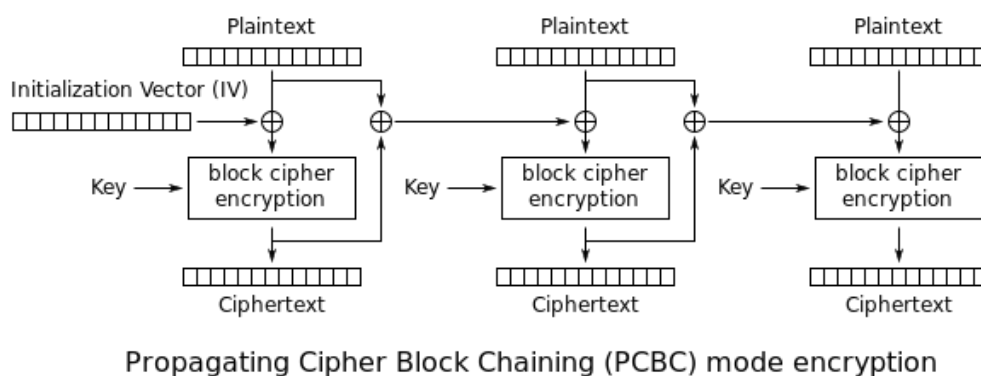


Figura 7: Encriptación en el Modo PCBC

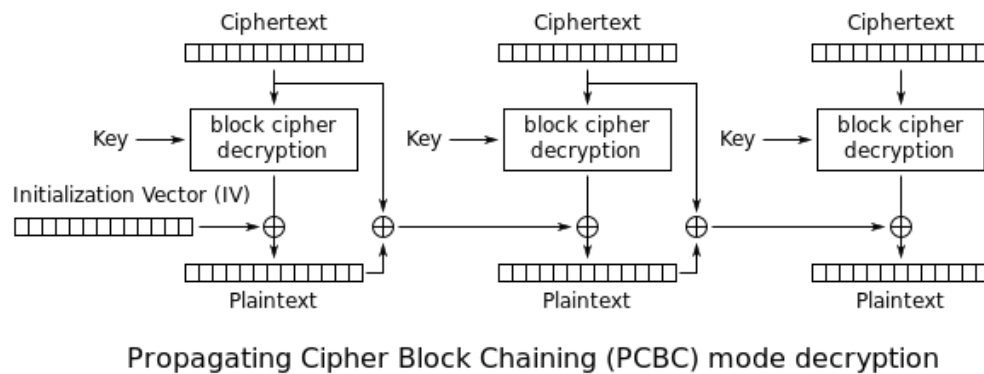


Figura 8: Descriptación en el Modo PCBC

4. Defina claramente el concepto de fortaleza de clave

La fuerza del cifrado se describe generalmente en términos del tamaño de las claves usadas para cifrar. Regularmente, las claves más largas brindan un cifrado más fuerte. La fuerza del cifrado está vinculada con la dificultad de descubrir la clave, que a su vez depende del cifrado utilizado y de la longitud de la clave. Por ejemplo, la dificultad de descubrir la clave para el cifrado RSA más comúnmente usado para el cifrado de clave pública depende de la dificultad de factorizar números grandes.

2. Actividades

CIFRADO SIMÉTRICO: DES

1. Ejecute safeDES

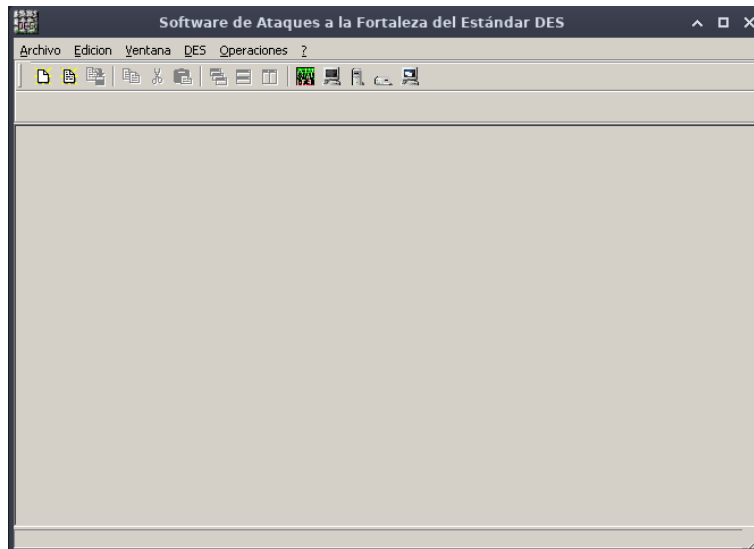


Figura 9: Ejecución

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

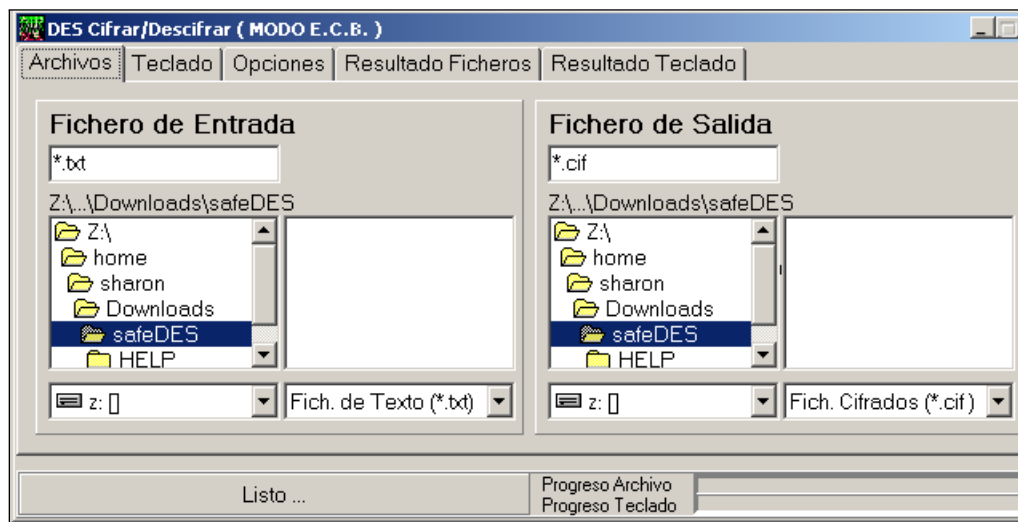


Figura 10: DES/ Cifrar/Descifrar, por defecto en modo E.C.B

3. En el folder teclado, ingresa el texto claro en modo hexadecimal. MHEX = 4545454545454545

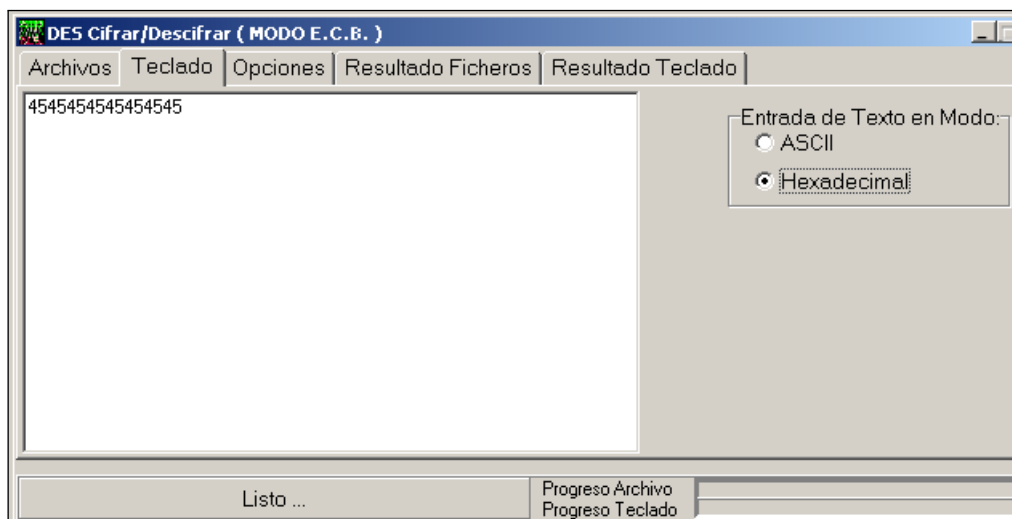


Figura 11: Ingresando el texto claro en modo hexadecimal

4. En el folder opciones, ingresa la clave en modo hexadecimal. KHEX = 0E419232EA6D0D62, y selecciona el Procesar hacia la opción Teclado

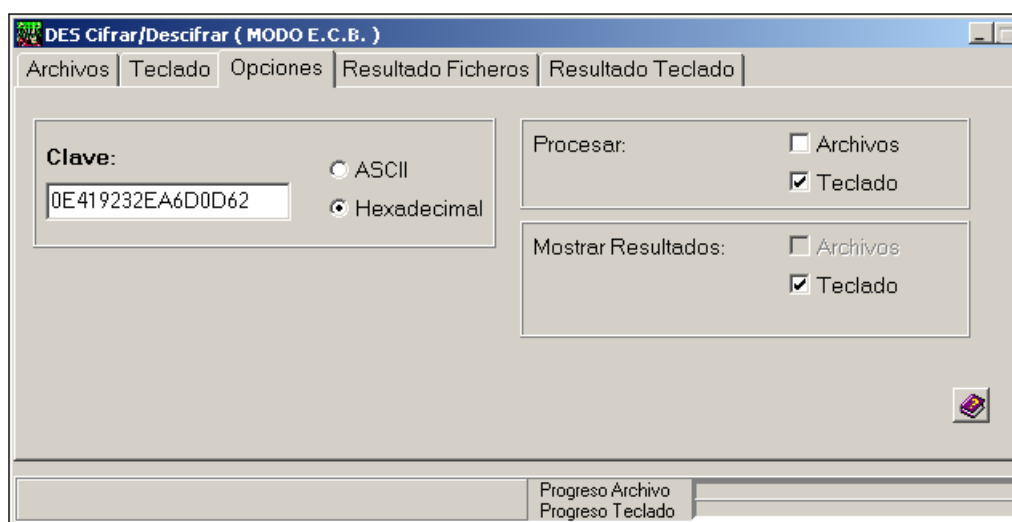


Figura 12: Ingresando la clave en modo hexadecimal

5. Seleccionar Operaciones/Comenzar o simplemente play.

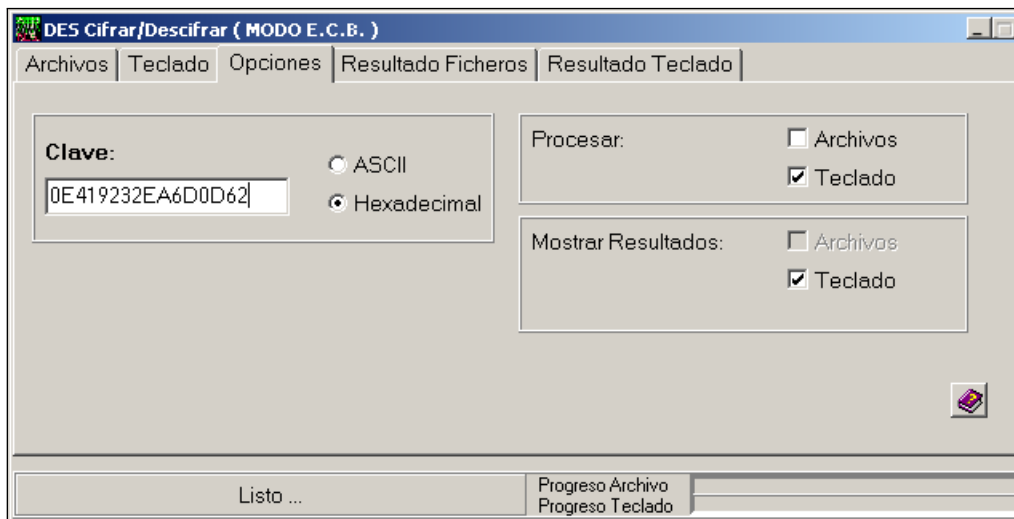


Figura 13: Operaciones/Comenzar

6. Anote el resultado del folder Resultado Teclado en ASCII y hexadecimal

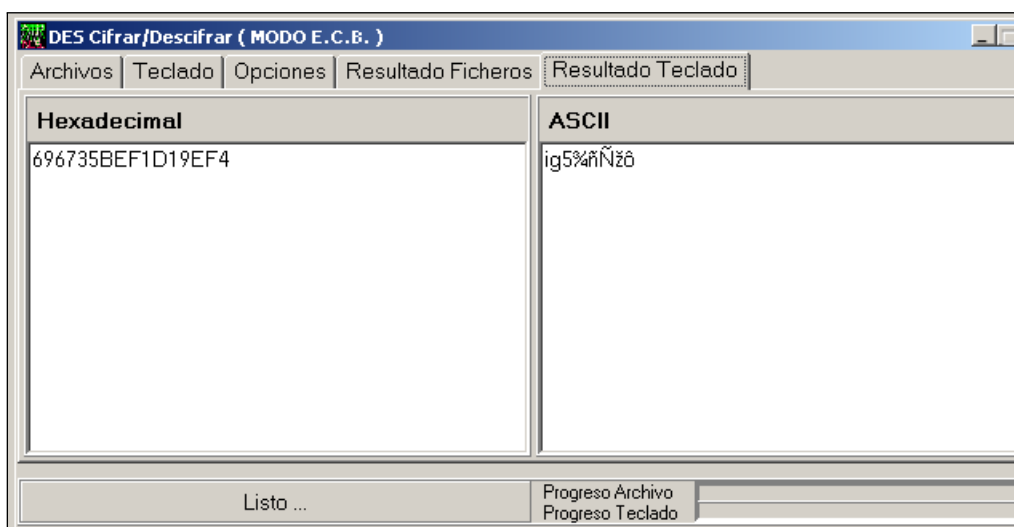


Figura 14: Resultado Teclado en ASCII y hexadecimal

Hexadecimal = 696735BEF1D19EF4

ASCII = ig5%4ñÑžô

7. Descifre el resultado hexadecimal, anote la respuesta

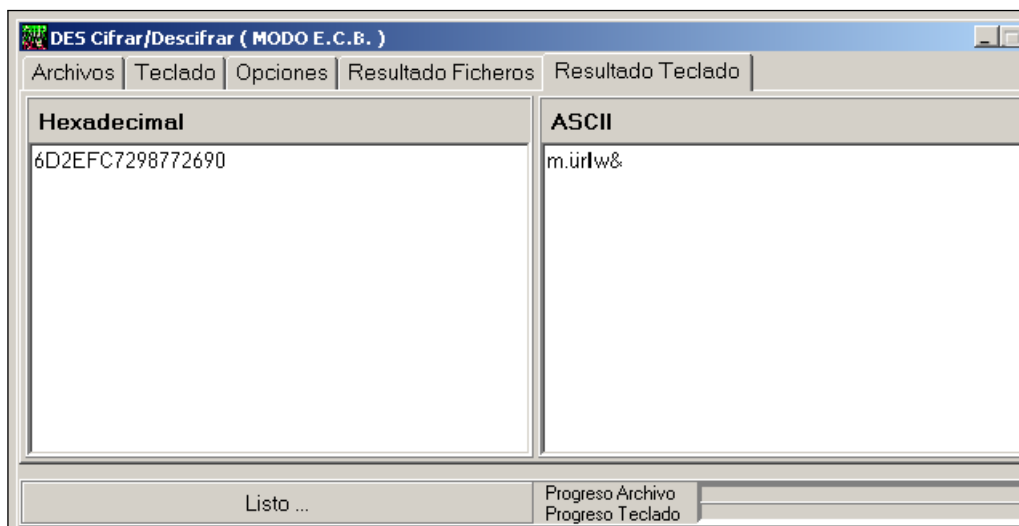


Figura 15: Descifrado del resultado hexadecimal

Hexadecimal = 6D2EFC7298772690

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

a) MHEX = 7003000E95ACBDEE

KHEX = 0123456789ABCDEF

CHEX = 30CC46A3A5B3F250

En la siguiente imagen se puede ver que el resultado de CHEX es 30CC46A3A5B3F250

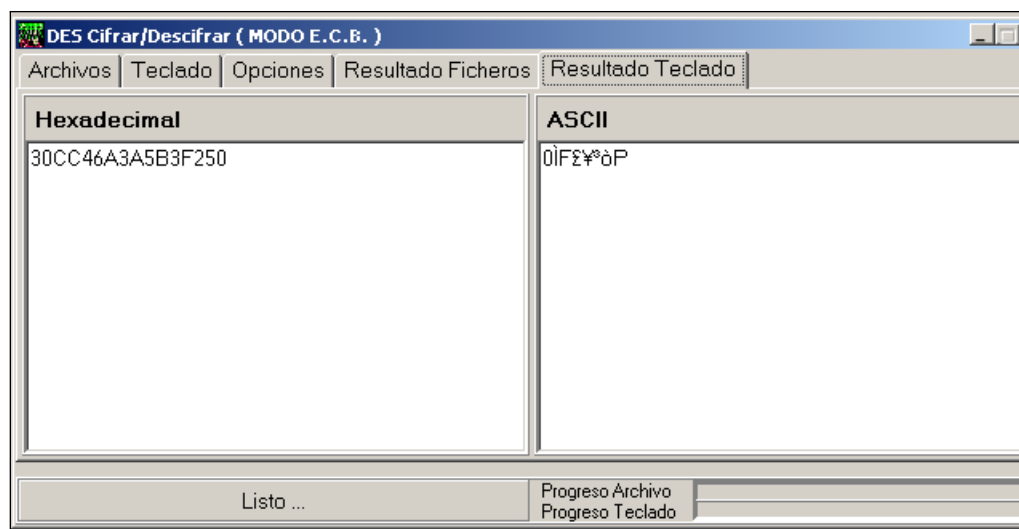


Figura 16: Resultado de cifrado DES

b) MHEX = 56003000E000F08B

KHEX = 45BF3708AC3

CHEX = -

Podemos ver en la siguiente imagen que no se puede cifrar porque la longitud de la clave no es correcta, y esto es porque para una clave hexadecimal se requiere de una longitud de 16 caracteres.

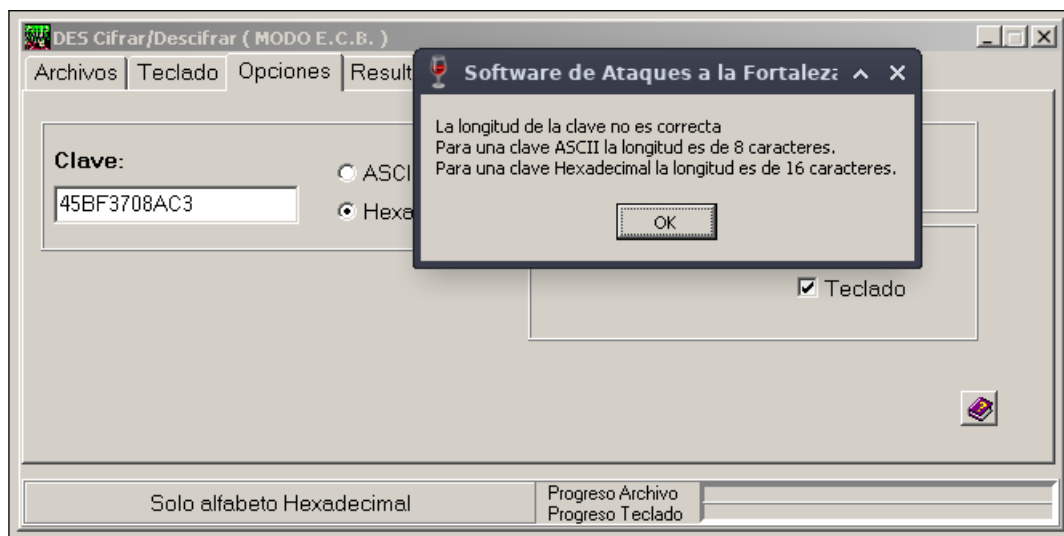


Figura 17: Sin resultado de cifrado DES

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

a) MASCII = MISTERIOSOSECRET0

KASCII = CLAVEDES

CHEX = C97677B7E1BE1A2A5CE089A945540CB4D08FF3803F384884

En la siguiente imagen se puede ver que el resultado de MASCII = MISTERIOSOSECRET0 con KASCII = CLAVEDES

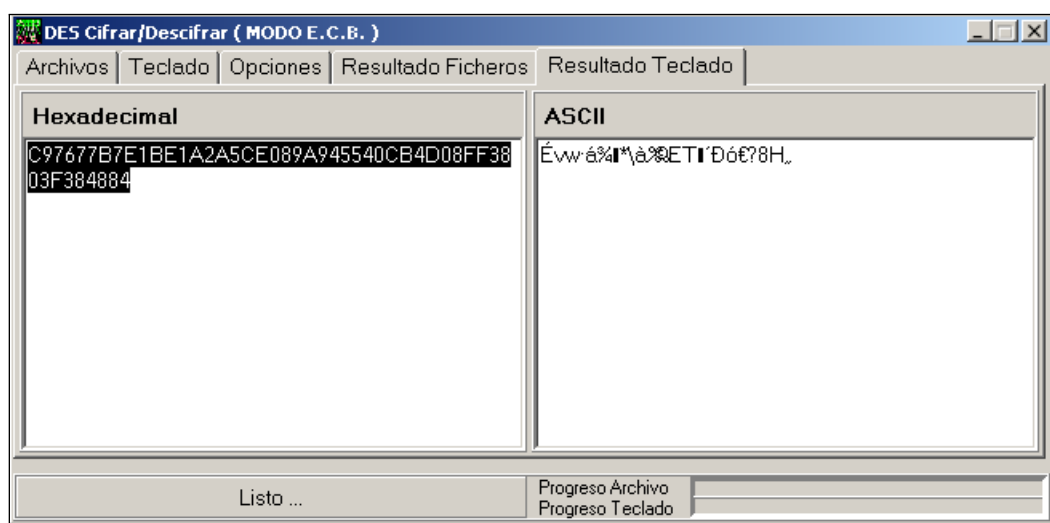


Figura 18: Resultado de cifrado DES para MASCII = MISTERIOSO-SECRET0

b) MASCII = MANDARINITA

KASCII = CLAVE

CHEX = -

En la siguiente imagen se puede ver que la longitud de la clave no es correcta porque para un clave en ASCII se requiere de una longitud de 8 caracteres, y también porque las propiedades del algoritmo DES es mayor a 64bits.

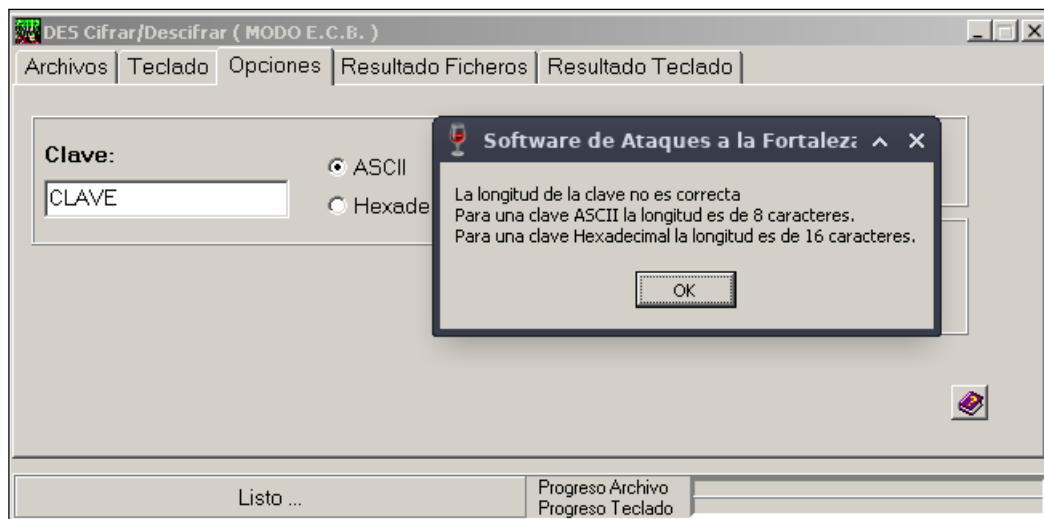


Figura 19: Longitud de la clave no correcta

10. **Cifre considerando el texto y la clave ASCII. Anote los resultados y justifique los mismos:**

MASCII = "Voy a encriptar ingresando la clave en ASCII"

KASCII = 77777777

CHEX = 22E09072065966BCFE04CC9D023C3F67D5671CC48516CE

E16F9739CEE3653840A59DC52EC22DB2539BCBF6263FF5F580

En la siguiente imagen se puede ver que el resultado de MASCII = "Voy a encriptar ingresando la clave en ASCII" con KASCII = 77777777

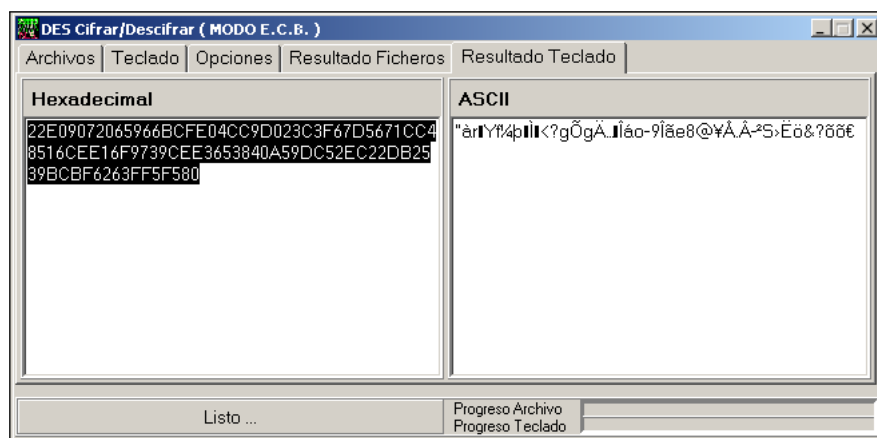


Figura 20: Cifrado con ASCII

11. Repetir 10 si KASCII = 66666666, explique los resultados

CHEX = 22E09072065966BCFE04CC9D023C3F67D5671CC48516CE

E16F9739CEE3653840A59DC52EC22DB2539BCBF6263FF5F580

Como vemos en la siguiente imagen, es el mismo resultado que el resultado anterior. Esto es debido a la periodicidad que existe en la clave.

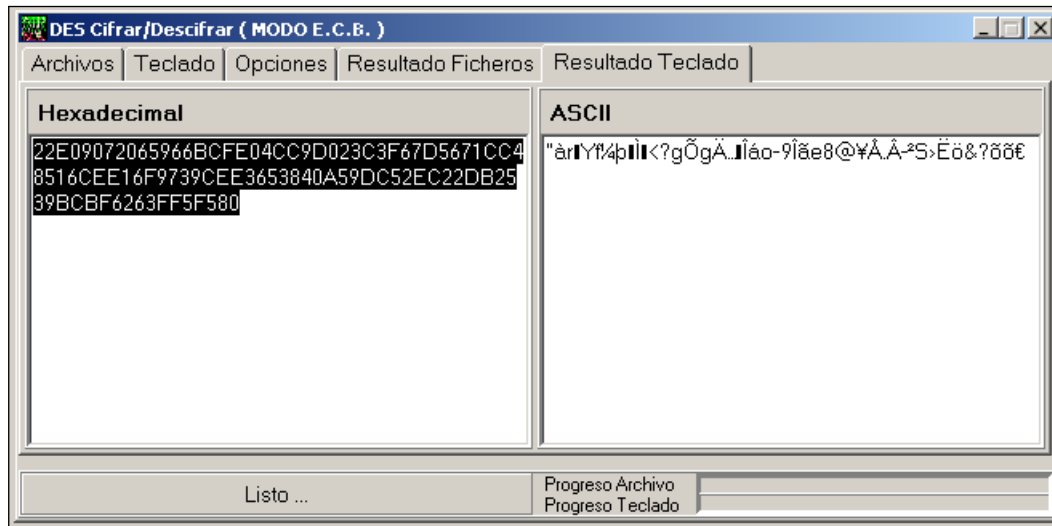


Figura 21: Resultado con KASCII = 66666666

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

Con MASCII = ENCRIPTO, el resultado en HEX fue AEDEEBFB3D9FF530

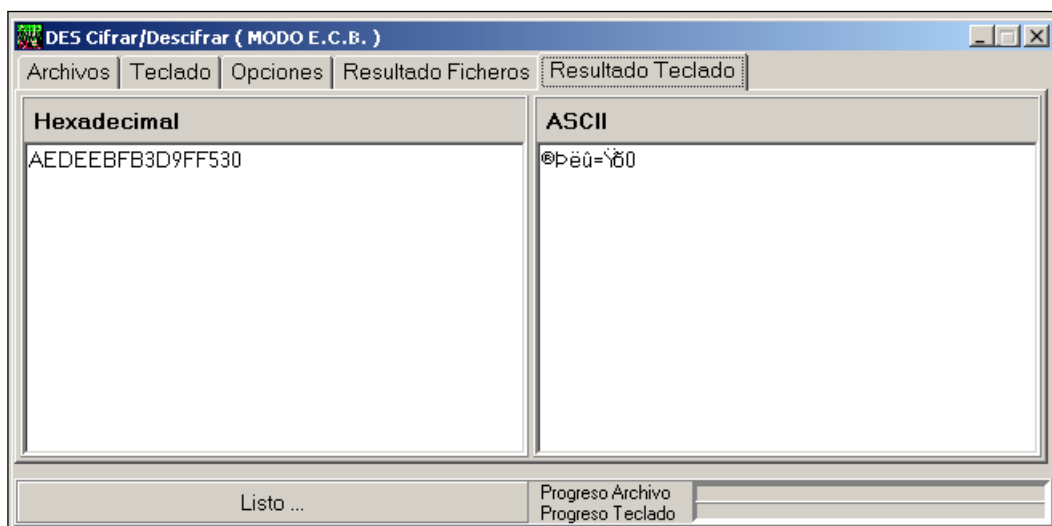


Figura 22: Resultado con el mensaje de 8 bytes MASCII = ENCRIPTO con KASCII = MARTILLO

Con MASCII = ENCRIPTACION, el resultado en HEX fue B0046E3787E15E7

ADD8FC12EA6502618

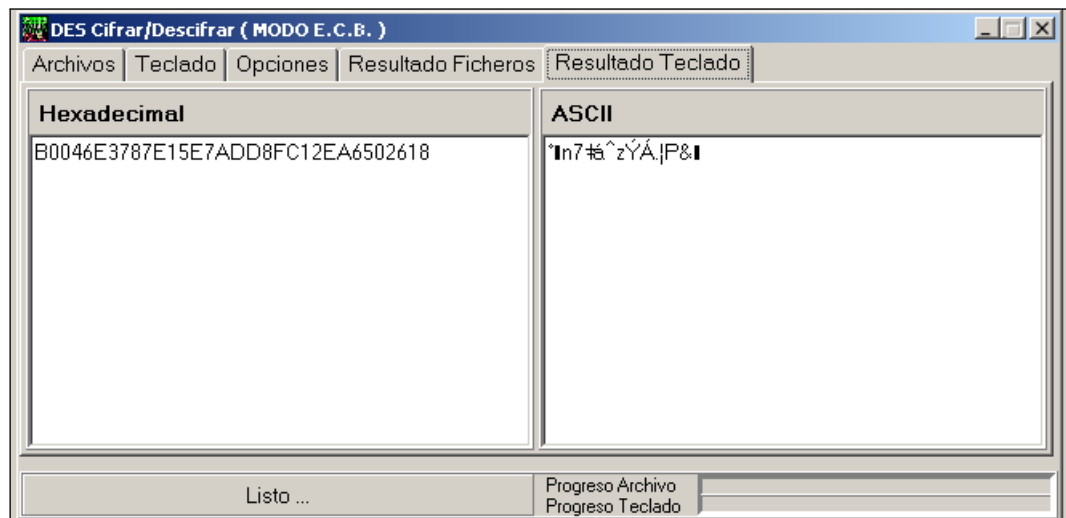


Figura 23: Resultado con el mensaje de 12 bytes MASCHII = ENCRIP-TACION usando la misma clave

ARCHIVOS CIFRADOS: DES

13. 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 “prueba.cif”

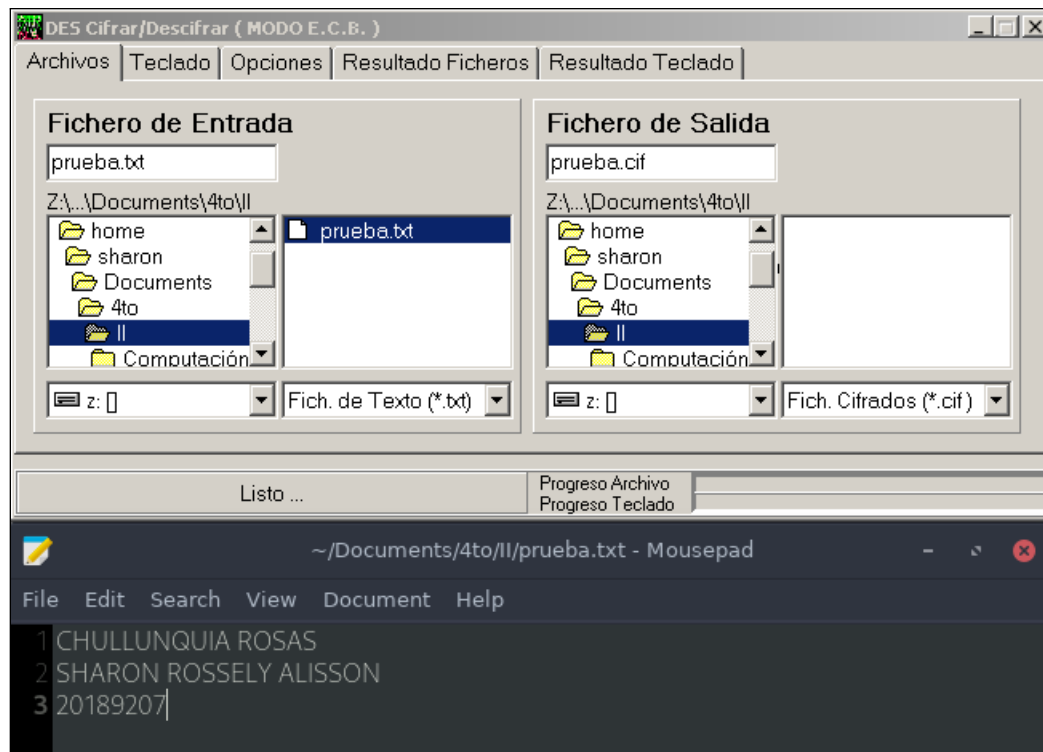


Figura 24: Cifrando datos

14. 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

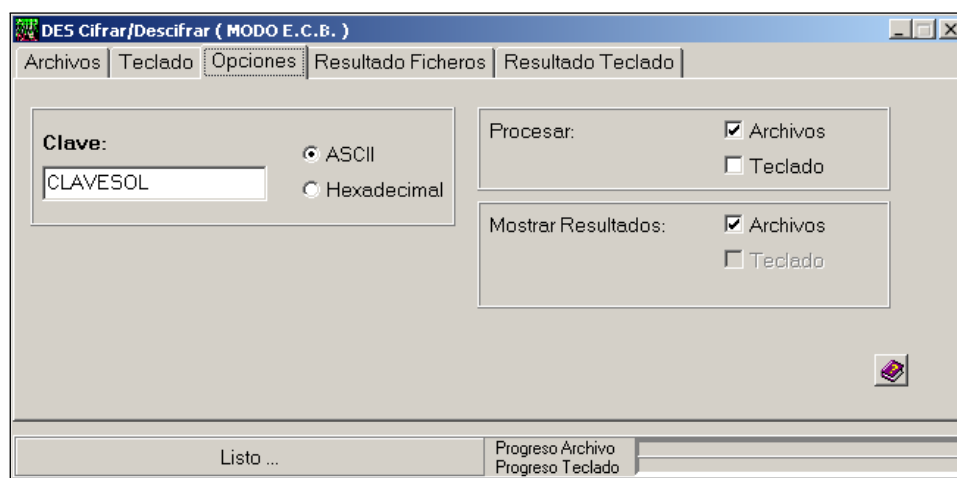


Figura 25: Definiendo clave

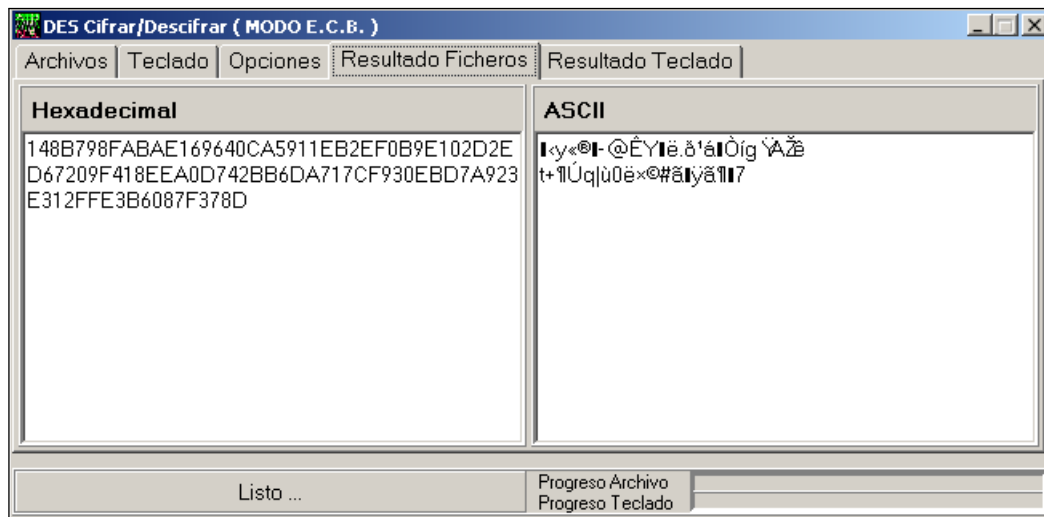


Figura 26: Resultado de cifrado

15. Muestre el archivo generado a partir del block de notas

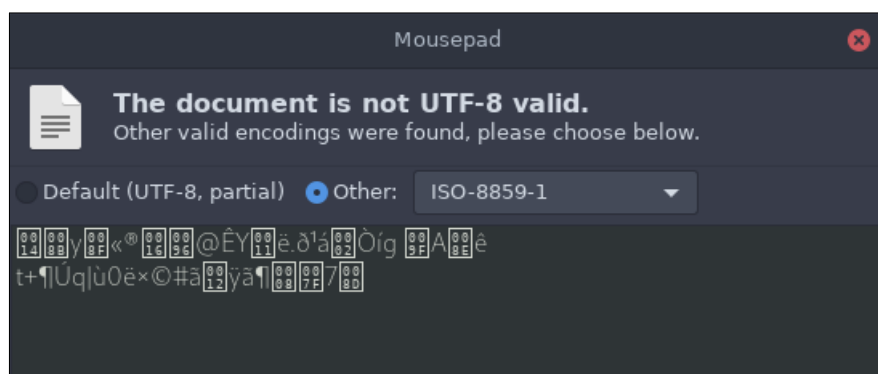


Figura 27: Resultado de cifrado en block de notas

16. Borre el archivo “prueba.txt” y genere un nuevo archivo a partir del proceso de descifrado, muestre los resultados y compare

Cambiamos de modo cifrado a modo descifrado, definiendo como archivo de entrada 'prueba.cif' y como archivo de salida 'prueba.dcf'. En el resultado podemos ver que el texto plano es igual al descifrado. A continuación se muestra el resultado en el block de notas.

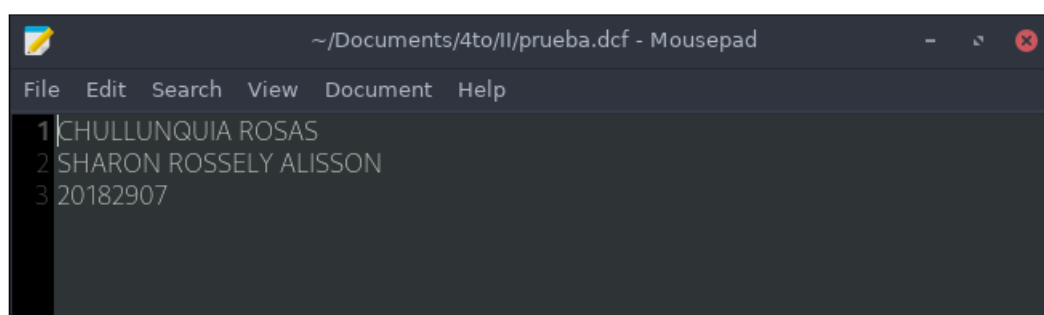


Figura 28: Resultado de descifrado en archivo 'prueba.dcf'

17. Repita los pasos del 13 al 16 implementando 3DES

CLAVES DÉBILES Y SEMIDÉBILES: DES

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

Realizando por segunda vez el cifrado, tomando en cuenta que el texto de ingreso y las claves se encuentran en formato hexadecimal.

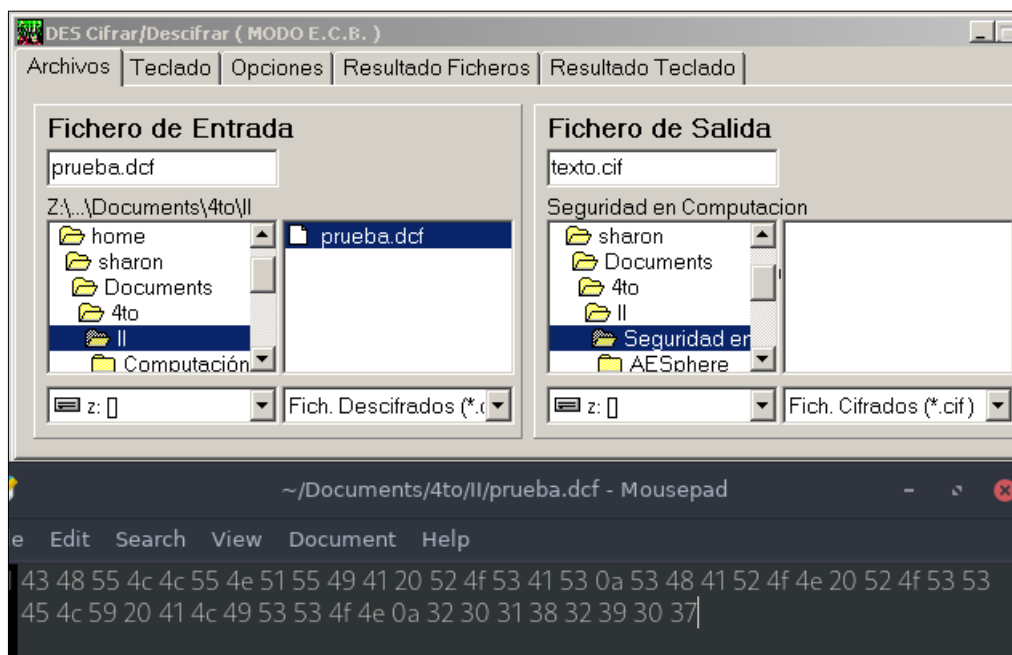


Figura 29: Definiendo archivo de entrada y archivo de salida

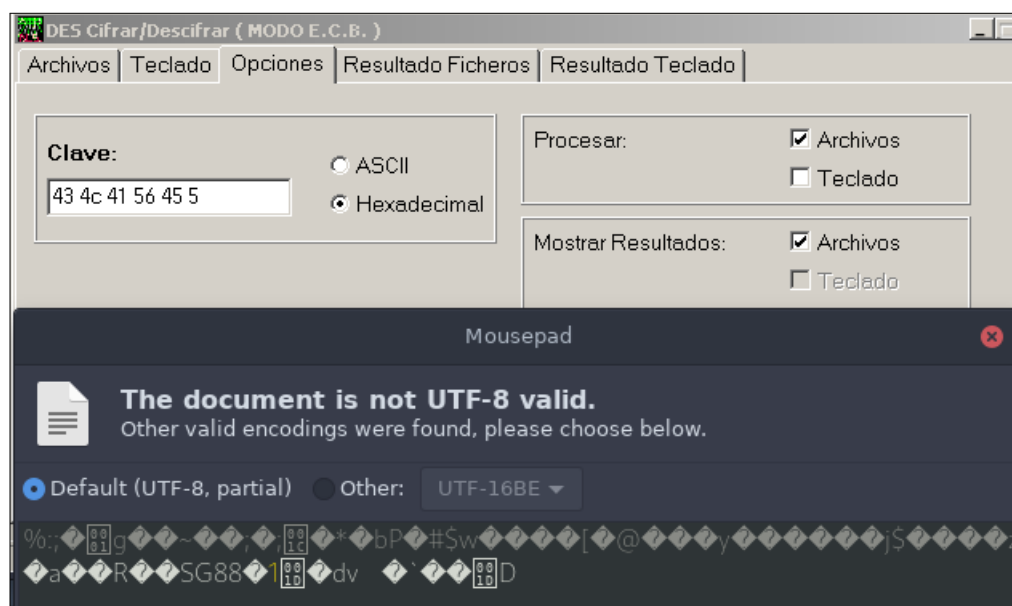


Figura 30: Resultado del cifrado obtenido en block de notas

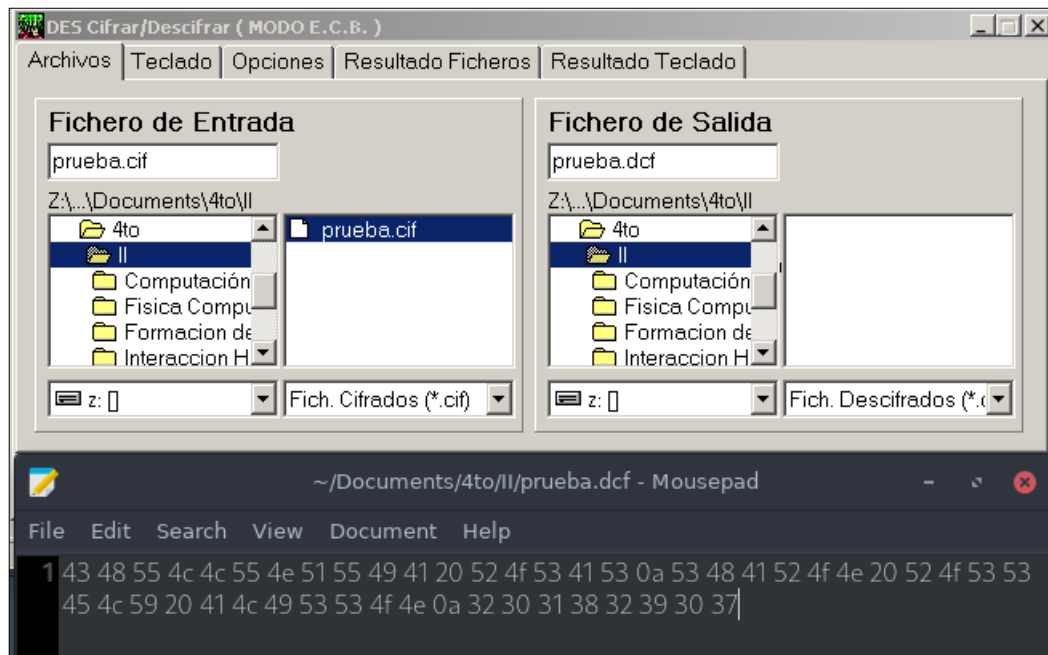


Figura 31: Resultado del descifrado

18. Cifrar el mensaje $M = \text{"En esta parte de la práctica vamos a comenzar a probar las llamadas claves débiles de DES mostradas en esta parte de la guía"}$ utilice las siguientes claves y demuestre que se cumpla que $M = E_k[E_k(M)]$

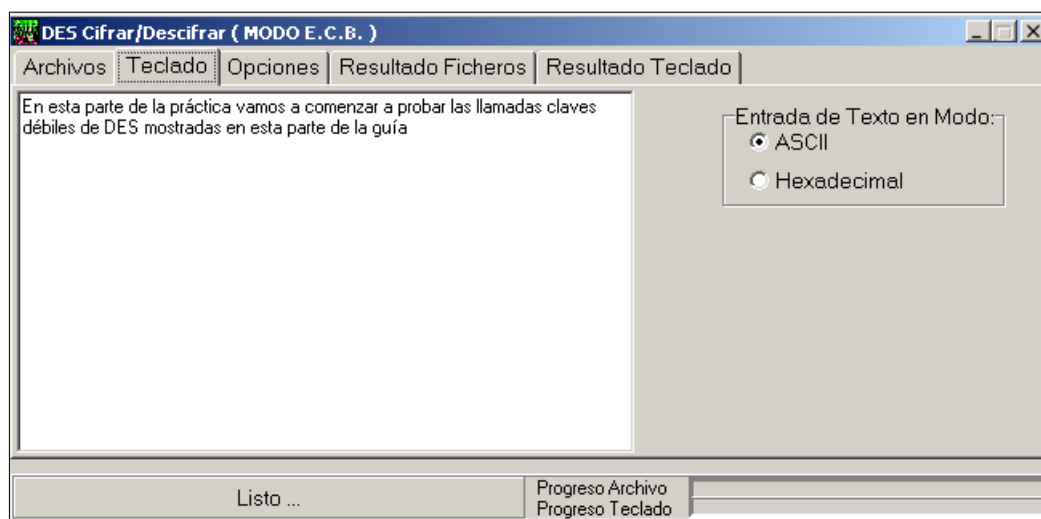


Figura 32: Ingresando el mensaje en ASCII

- $K_1 \text{ HEX} = 0101010101010101$

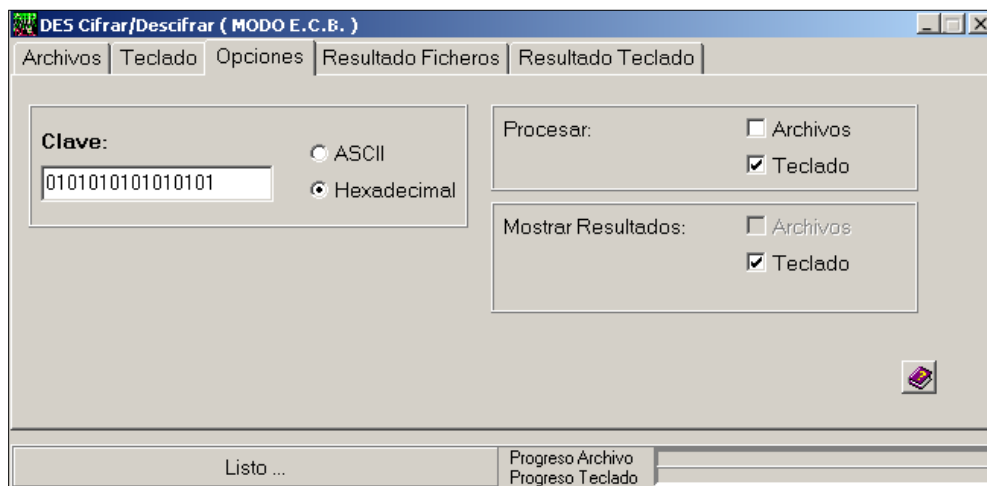


Figura 33: Ingresando clave en hexadecimal

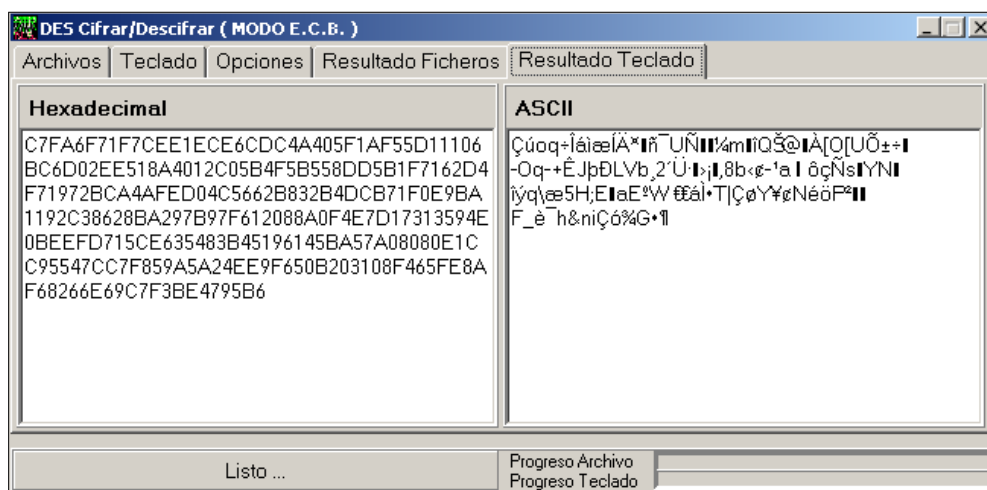


Figura 34: Resultado del cifrado con K1 HEX = 0101010101010101

- K2 HEX = E0E0E0E0F1F1F1F1

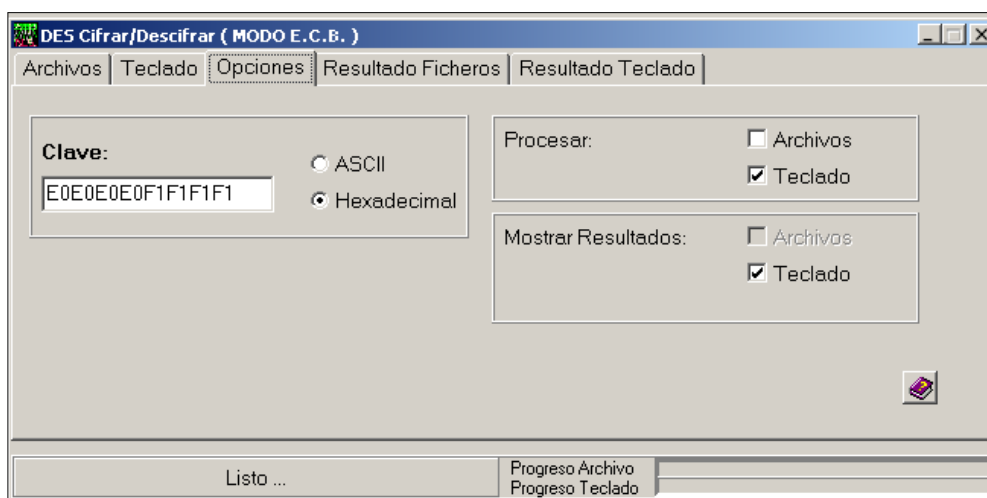


Figura 35: Ingresando clave en hexadecimal

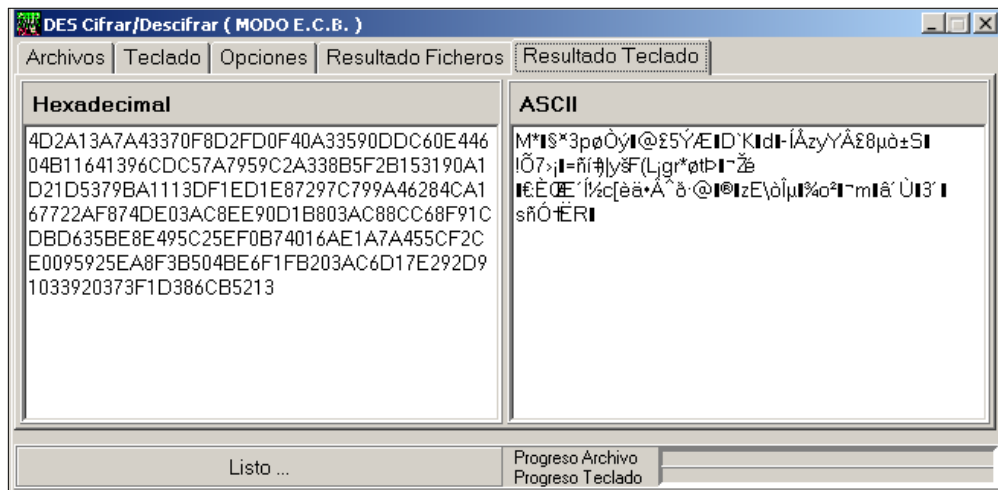


Figura 36: Resultado del cifrado con K1 HEX = E0E0E0E0F1F1F1F1

- K3 HEX = 1F1F1F1F0E0E0E0E

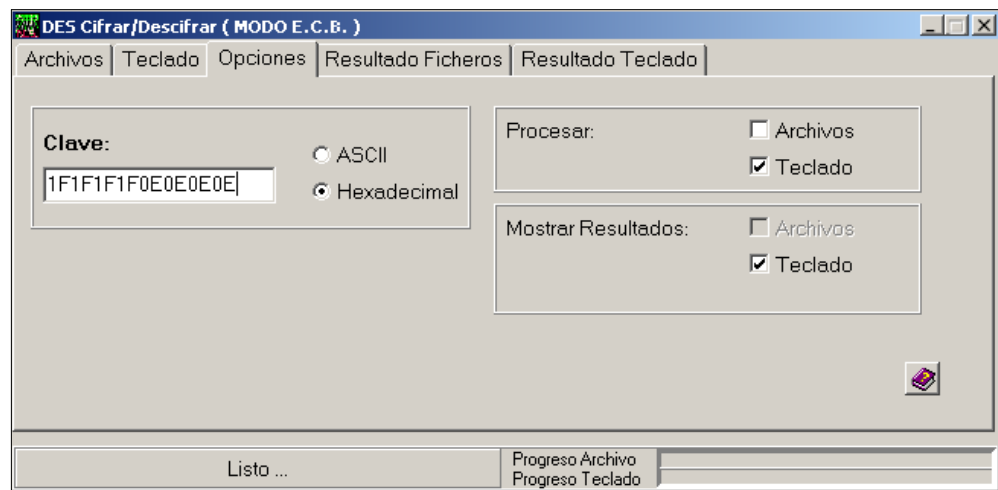


Figura 37: Ingresando clave en hexadecimal

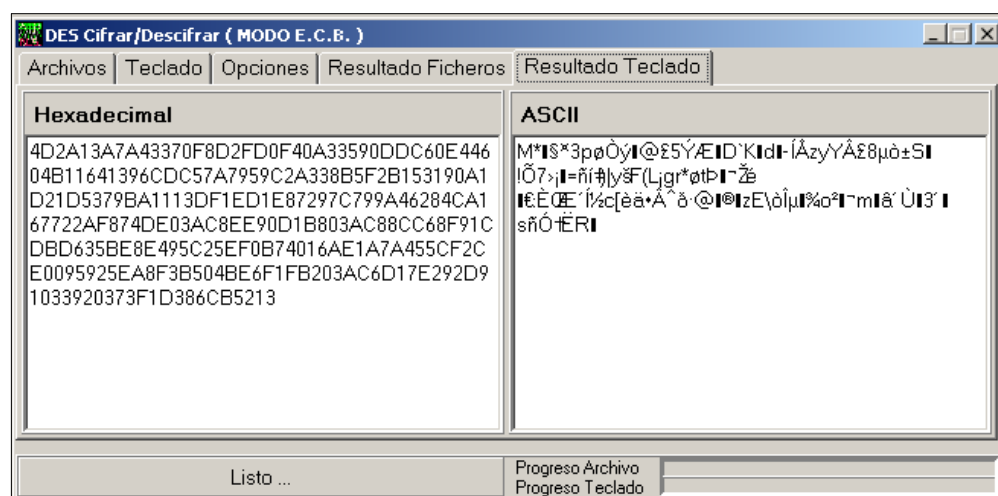


Figura 38: Resultado del cifrado con K1 HEX = 1F1F1F1F0E0E0E0E

19. Cifrar el mensaje $M = \text{“En esta parte de la práctica vamos a comenzar a probar las llamadas claves semidébiles de DES mostradas en esta parte de la guía”}$. utilice las siguientes claves y demuestre que se cumpla que $M = E_{k1}[E_{k2}(M)]$

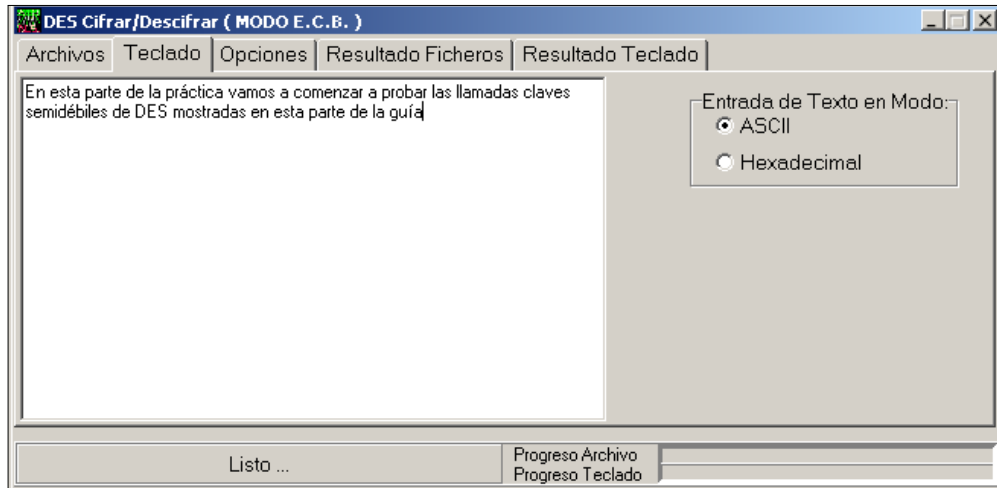


Figura 39: Ingresando el mensaje a cifrar

- $K1 \text{ HEX} = 01FE01FE01FE01FE$ $K2 \text{ HEX} = FE01FE01FE01FE01$

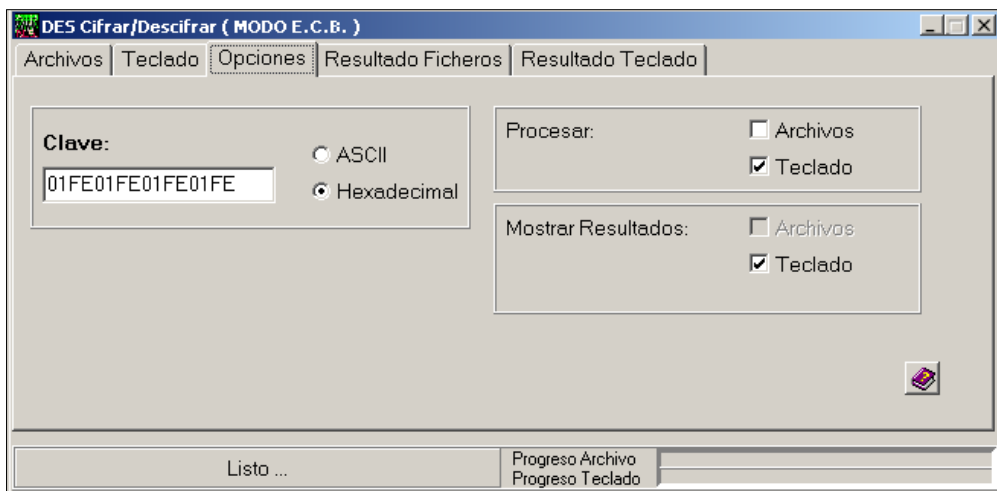


Figura 40: Ingresando la clave $K1 \text{ HEX} = 01FE01FE01FE01FE$

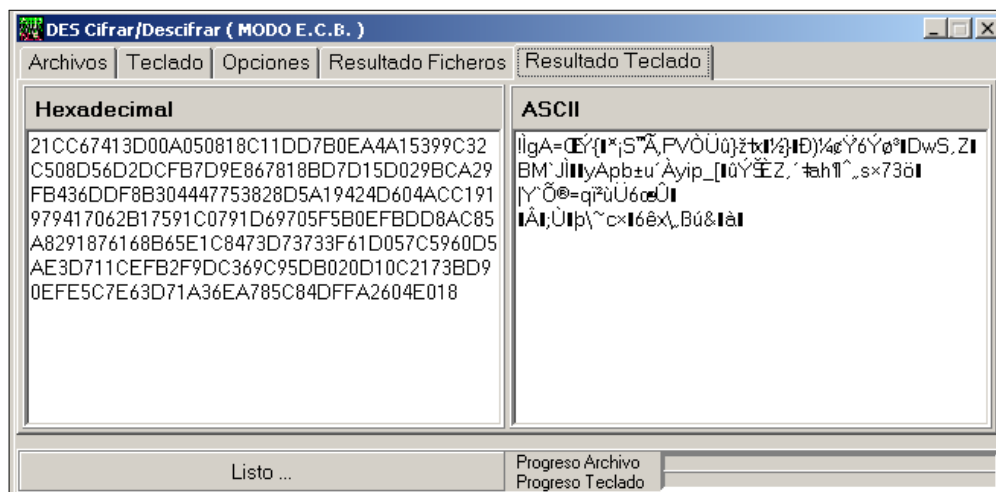


Figura 41: Resultado del cifrado con K1 HEX = 01FE01FE01FE01FE

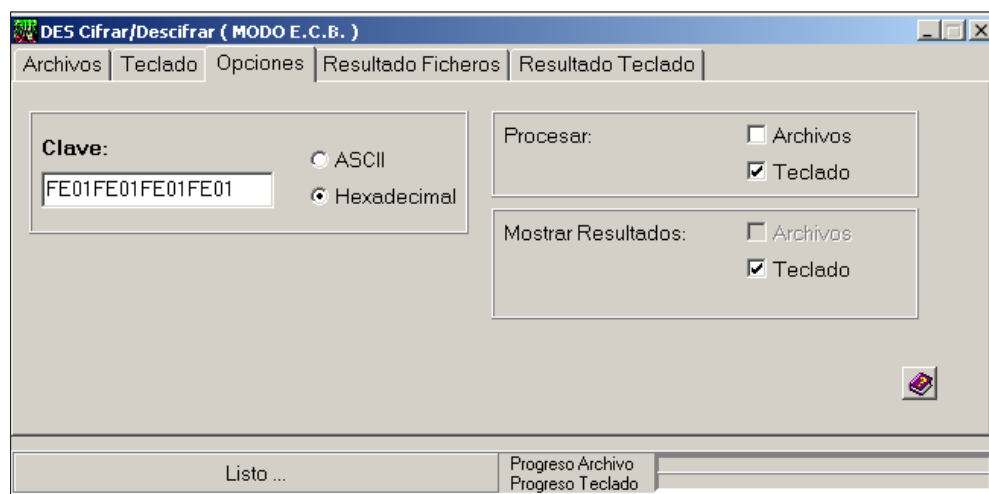


Figura 42: Ingresando la clave K1 HEX = FE01FE01FE01FE01

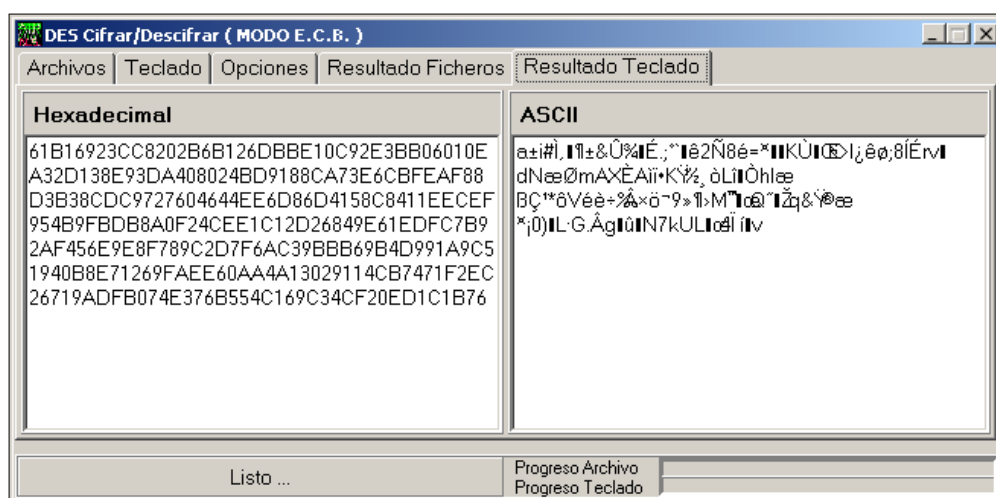


Figura 43: Resultado del cifrado con K2 HEX = FE01FE01FE01FE01

- K1 HEX = 1FE01FE00EF10EF1 K2 HEX = E01FE01FF10EF10E

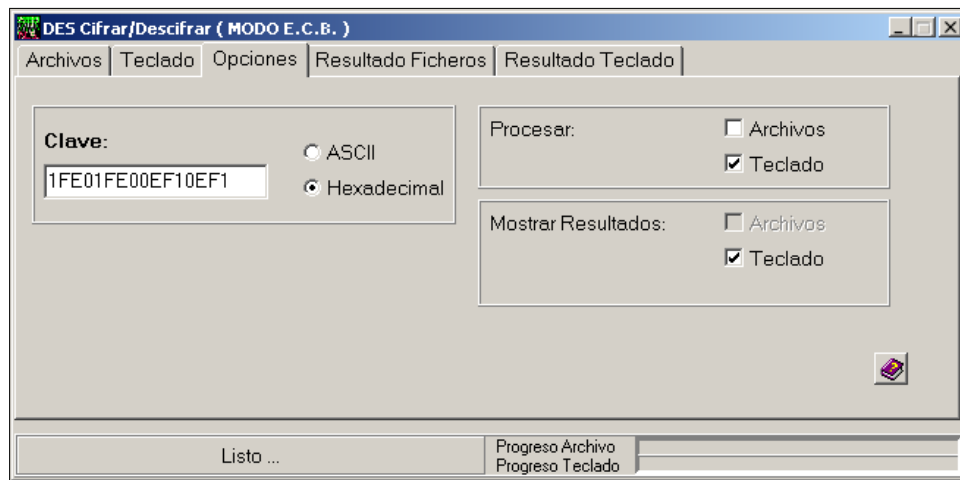


Figura 44: Ingresando la clave K1 HEX = 1FE01FE00EF10EF1

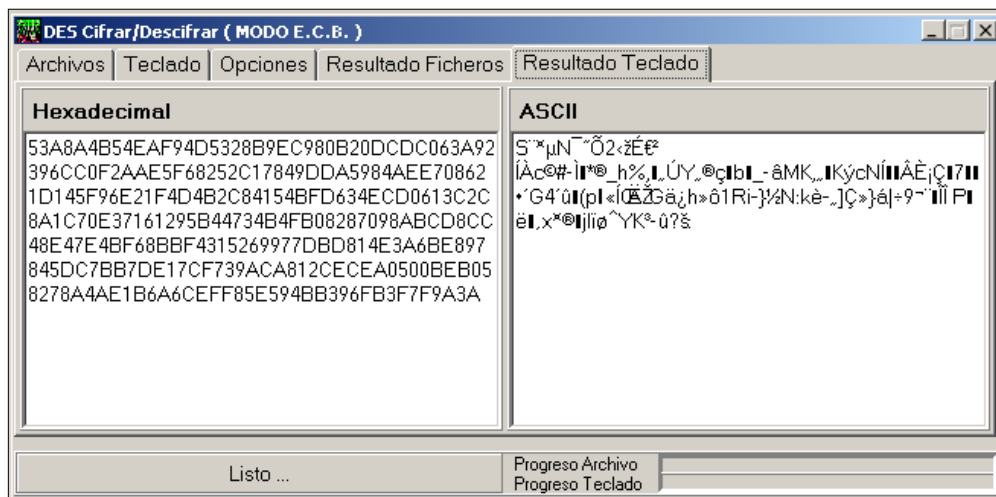


Figura 45: Resultado del cifrado con K1 HEX = 1FE01FE00EF10EF1

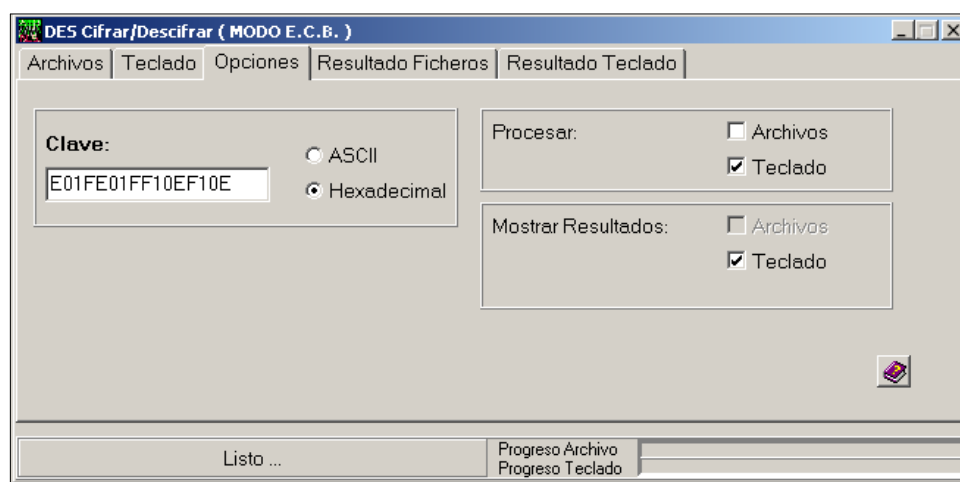


Figura 46: Ingresando la clave K2 HEX = E01FE01FF10EF10E

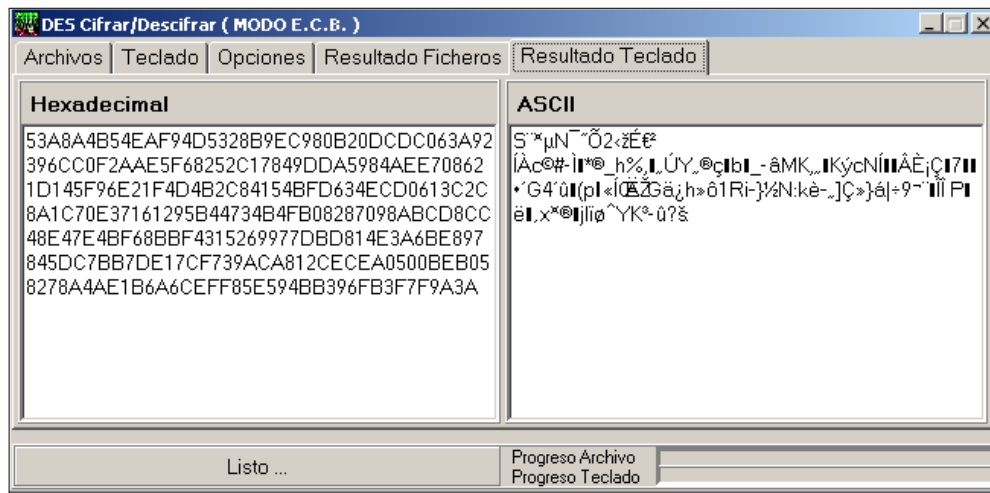


Figura 47: Resultado del cifrado con K2 HEX = E01FE01FF10EF10E

MODO CBC

20. Asumiendo un modo de cifrado CBC encriptar usando KHEX=922C68C47AEADFF2, MASII="vamos a implementar el modo CBC", si IVHEX=DA4BBEF16B6E983D, si lo necesita recuerde que puede usar calculadoras disponibles en Internet

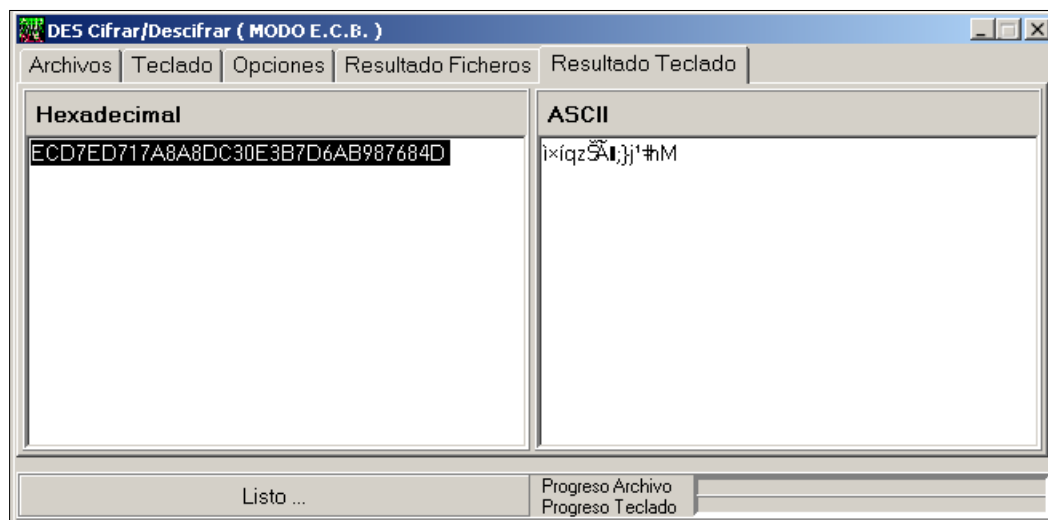
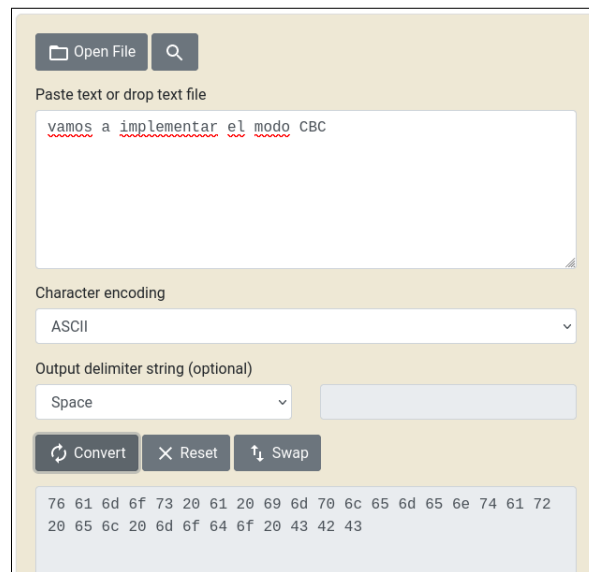


Figura 48: Modo de cifrado CBC

- a) Convertir el mensaje a hexadecimal y definir los bloques a cifrar (<https://www.rapidtables.com/convert/number/ascii-to-hex.html>)



Open File

Paste text or drop text file

vamos a implementar el modo CBC

Character encoding

ASCII

Output delimiter string (optional)

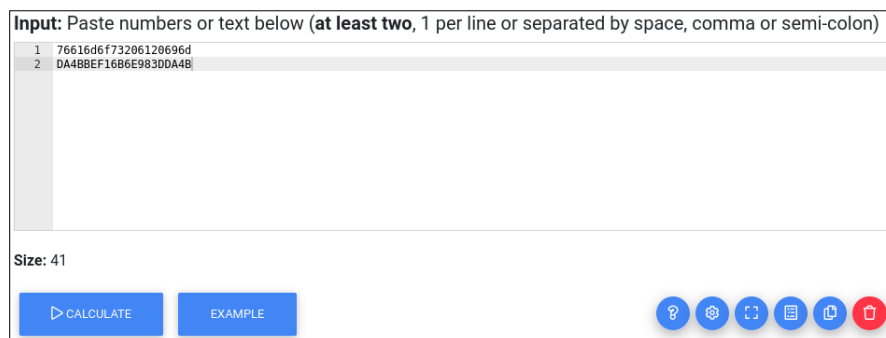
Space

Convert Reset Swap

76 61 6d 6f 73 20 61 20 69 6d 70 6c 65 6d 65 6e 74 61 72
20 65 6c 20 6d 6f 64 6f 20 43 42 43

Figura 49: Resultado de la conversión del mensaje a hexadecimal

- b) Operar la función XOR entre el cada bloque del mensaje y el texto cifrado anterior (salvo en el primer bloque donde deberá usar el IV (<https://toolslick.com/math/bitwise/xor-calculator>))



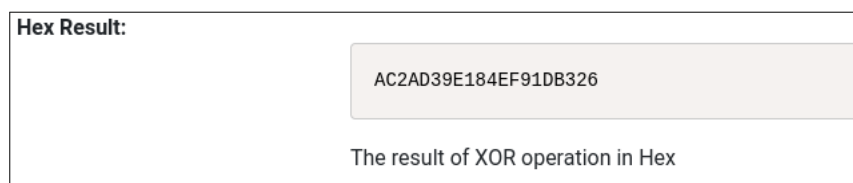
Input: Paste numbers or text below (at least two, 1 per line or separated by space, comma or semi-colon)

1 76616d6f73206120696d
2 DA48BEF1686E983DDA4B

Size: 41

CALCULATE EXAMPLE

Figura 50: Ingresando el texto en hexadecimal



Hex Result:

AC2AD39E184EF91DB326

The result of XOR operation in Hex

Figura 51: Resultados de XOR

- c) Cifrar el resultado de la operación XOR

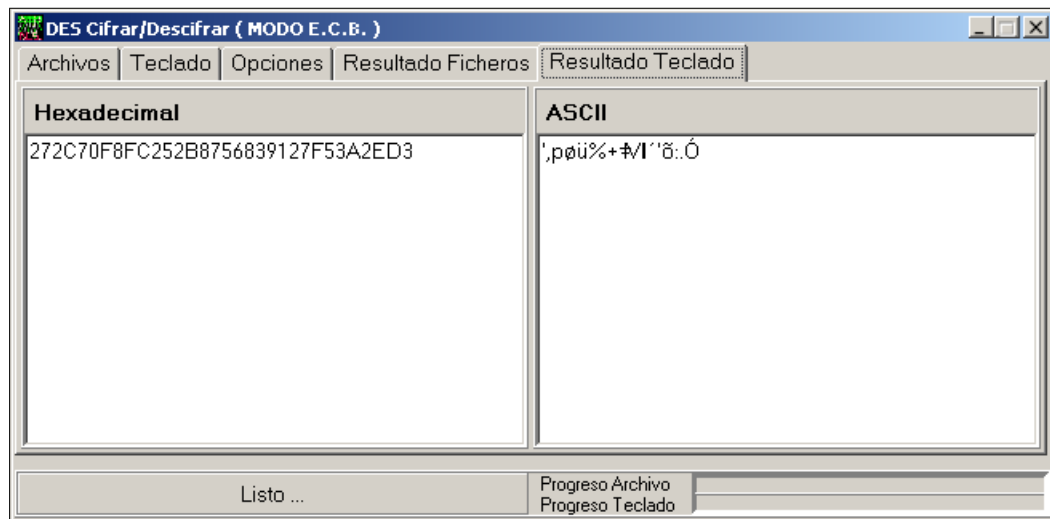


Figura 52: Resultados del cifrado

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

Bloque	Operando 1 _{xor}	Operando 2 _{xor}	Salida XOR	Cifrado DES
1	76616d6f73 206120696d	DA4BBEF16 B6E983DDA4B	AC2AD39E1 84EF91DB326	272C70F8FC252B87 56839127F53A2ED3
2	706c656d6 56e74617220	BEF16B6E9 8ECD7ED717A	CE9D0E03F D82A38C035A	184EF3DF141029B 604134EB55D28C5B3
3	656c206d6f6 46f20434243	8A8DC30E3B 7D6AB987684D	EFE1E3635 4190599C42A0E	7BC6B69C1EC0C30 63B2F9376D006E10F

ATAQUE A DES (MODO MONOUSUARIO)

21. Dado el texto claro M=“Vamos a atacar al algoritmo DES modo ECB en modo monousuario, es decir desde mi propia PC, para ello necesito un par texto claro/texto cifrado para atacar”

- a) Convierta a hexadecimal e identifique cuantos bloques van a ser cifrados, indique si los bloques están completos o necesitan relleno si es el caso ¿cuantos bytes de rellenos deberían agregarse?

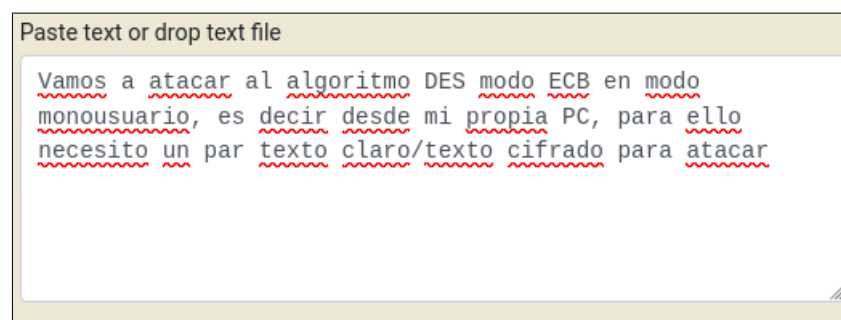


Figura 53: Conversión a hexadecimal

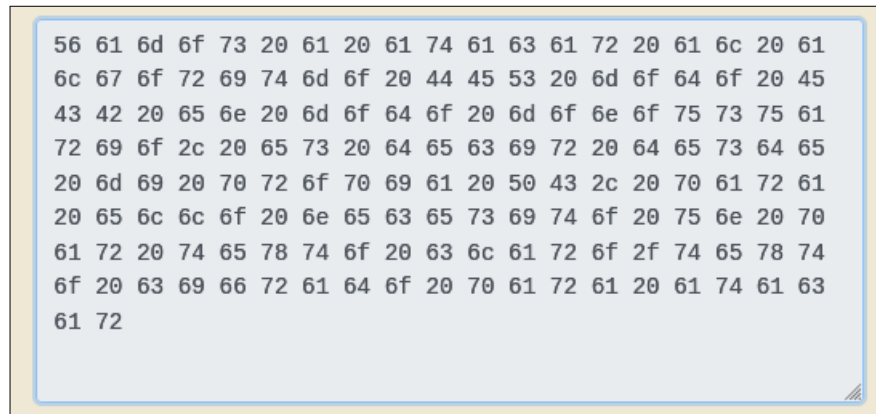


Figura 54: Conversión a hexadecimal

MHEX = 56 61 6d 6f 73 20 61 20 61 74 61 63 61 72 20 61 6c 20 61 6c 67 6f 72 69 74 6d 6f 20 44 45 53 20 6d 6f 64 6f 20 45 43 42 20 65 6e 20 6d 6f 64 6f 20 6d 6f 6e 6f 75 73 75 61 72 69 6f 2c 20 65 73 20 64 65 63 69 72 20 64 65 73 64 65 20 6d 69 20 70 72 6f 70 69 61 20 50 43 2c 20 70 61 72 61 20 65 6c 6c 6f 20 6e 65 63 65 73 69 74 6f 20 75 6e 20 70 61 72 20 74 65 78 74 6f 20 63 6c 61 72 6f 2f 74 65 78 74 6f 20 63 69 66 72 61 64 6f 20 70 61 72 61 20 61 74 61 63 61 72

El mensaje tiene 154 caracteres, dado que DES cifra bloques de 8 bytes (64 bits), cifrará 19 bloques. Necesitan relleno. Deberían agregarse 2 bytes.

- b) Cifrar usando KHEX=5285285285ABCDEF, guarde el resultado

CHEX = 485A8A4ACD150E29C448CDE93B9BE44A32B2E14A254C7DA1099
B4604FB997010C7BD0E71D4A6876EEDBE93B140FBBD900163D486C379301
A1E52A4B4AF7D73B627238C51D324FBE8217B0C426C5FC69E89861BE09B
45F44063CD4C18C62431950524BE7FB4ADE8CB2B81F3B3876BE34C687F2
A9C04793795FD0FEA4D17C13DCFBE479FBB00C3D704C15680129847E84D
D3EC898F29B078C9C238BEC9B1FDDBC3

22. Descifre CHEX, guarde el resultado

M'HEX = 56616D6F7320612061746163617220616C20616C676F7269746D6F204445
53206D6F646F2045434220656E206D6F646F206D6F6E6F7573756172696F2C206573
206465636972200D0A6465736465206D692070726F7069612050432C207061726120
656C6C6F206E6563657369746F20756E2070617220746578746F20636C61726F2F74
6578746F206369667261646F2070617261200D0A6174616361720000

M'ASCII = Vamos a atacar al algoritmo DES modo ECB en modo monousuario, es decir desde mi propia PC, para ello necesito un par texto claro/texto cifrado para atacar

23. Complete la siguiente tabla

Bloque	MHEX	CHEX	M'HEX
1	56 61 6d 6f 73 20 61 20	485A8A4ACD150E29	56616D6F73206120
2	61 74 61 63 61 72 20 61	C448CDE93B9BE44A	6174616361722061
3	6c 20 61 6c 67 6f 72 69	32B2E14A254C7DA10	6C20616C676F7269
4	74 6d 6f 20 44 45 53 20	99B4604FB997010C	746D6F2044455320
5	6d 6f 64 6f 20 45 43 42	7BD0E71D4A6876EE	6D6F646F20454342
6	20 65 6e 20 6d 6f 64 6f	DBE93B140FBBD900	20656E206D6F646F
7	20 6d 6f 6e 6f 75 73 75	163D486C379301A1	206D6F6E6F757375
8	61 72 69 6f 2c 20 65 73	E52A4B4AF7D73B62	6172696F2C206573
9	20 64 65 63 69 72 20 64	7238C51D324FBE82	206465636972200D
10	65 73 64 65 20 6d 69 20	17B0C426C5FC69E8	0A6465736465206D
11	70 72 6f 70 69 61 20 50	9861BE09B45F4406	692070726F706961
12	43 2c 20 70 61 72 61 20	3CD4C18C62431950	2050432C20706172
13	65 6c 6c 6f 20 6e 65 63	524BE7FB4ADE8CB2	6120656C6C6F206E
14	65 73 69 74 6f 20 75 6e	B81F3B3876BE34C6	6563657369746F20
15	20 70 61 72 20 74 65 78	87F2A9C04793795F	756E207061722074
16	74 6f 20 63 6c 61 72 6f	D0FEA4D17C13DCFB	6578746F20636C61
17	2f 74 65 78 74 6f 20 63	E479FBB00C3D704C	726F2F746578746F
18	69 66 72 61 64 6f 20 70	15680129847E84DD	206369667261646F
19	61 72 61 20 61 74 61 63	3EC898F29B078C9C	2070617261200D0A

24. Seleccione el ataque modo monousuario DES/Ataque Monousuario (ahora ya dispone de un para texto claro M'HEX/texto cifrado CHEX), ingrese ambos en Teclado

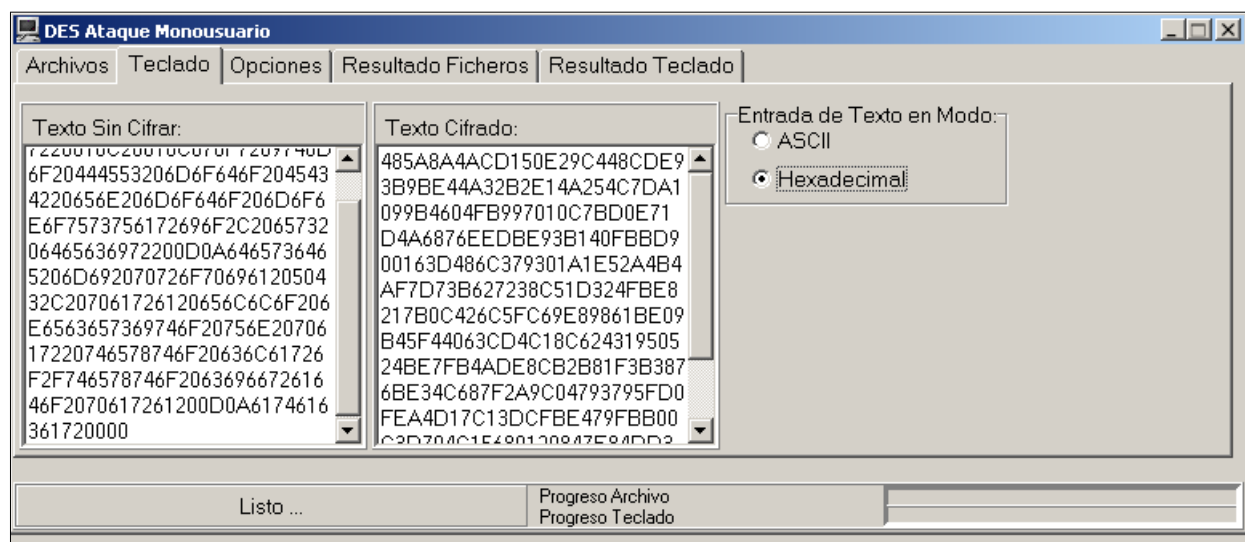


Figura 55: Modo monousuario DES/Ataque Monousuario

25. Seleccione Opciones e ingrese el rango de claves que deben ser probadas durante el ataque $KHEX_{inicial} = 5285285285000000$ y $KHEX_{final} =$

27. **¿Cuáles son las funciones en cada ronda? Explique**

En cada ronda normalmente está comprendida por la sustitución, permutación y mezcla con la clave. Realiza el cifrado en variedad de rondas, repitiendo en todas una serie de operaciones sobre los datos y utilizando una subclave distinta

28. **En el menú operaciones explique para la función Subbytes la salida si**

a) Todas las entradas son 00

Todas las salidas son 63

b) Todas las entradas son FF

Todas las salidas son 16

c) El mensaje

55 75 60 F3 15 27 10 F6 E5 18 F0 E3 D5 23 26 53

Para el mensaje anterior, el resultado es el siguiente:



Figura 57: Salida del mensaje

29. **Compare los resultados de los siguientes cifrados en modo ECB y CBC**

a) M=MANO

K= 0x 30313233343536373839414243444546

IV= 0x 313233566563746F72496E696369616C

CECB= cf5324b0fa3016c613c52faf49b661a6

CCBC= rrKnR9FvsbBFp70wpKk6kw==

b) M= 4142434445464748494A4B4C4D4E4F00

K= 0x 30313233343536373839414243444546

IV= 0x 313233566563746F72496E696369616C

CECB= 4rJO2FjnRSQTUOwp8bRiTjSvM2yfAxs1VnOMY+YeovY=

CCBC= HMysV9OHjEl/Hj+3+Nk73/np5Kv1X+ow4CgdtDFqegg=

c) M= COMPARANDO EL CIFRADO AES EN MODO ECB Y CBC

K= 0x 30313233343536373839414243444546

IV= 0x 313233566563746F72496E696369616C

CECB= YTyuaT336pr72lRV8T1ZmnGLCvx68XiWdnweKUCisGFR5uxnUg

T+XNjzRCq1oetD

CCBC= Eq+KxYvjo48Nz/Pi5r8yC9Z+P6ZhkkIBS2I/ddxF0rmLu5ExbYV49

dfz4ENZZN1U

3. Conclusiones

- El vector de inicialización IV se utiliza para la etapa siguiente, la cual luego se pasa a la función OR exclusiva (XOR).
- El cifrado por flujo genera en línea la salida mientras que el de Bloques trabaja por unidades funcionales, ya sean de 64 bits, 128 bits.
- La repetividad en el texto claro se traduce en el cipher.
- El algoritmo DES tiene un tamaño muy corto de clave, por ello es considerado como un algoritmo inseguro y además obsoleto.
- Hoy en la actualidad, AES es uno de los más algoritmos mas usados, tiene logitud variable de la clave, que puede llegar a ser hasta 256 bits lo que brinda mayor seguridad.
- AES tiene un buen rendimiento en los procesos de cifrado y descifrado.

4. Cuestionario Final

1. **Describa los modos de cifrado CFB y OFB. Defina las ventajas y desventajas computacionales de los cuatro modos de cifrado**

El modo CFB no cifra directamente del texto plano. Este modo cifra del texto cifrado anterior con XOR, la tecla clave, para obtener el texto cifrado. El primer texto se cifra con el vector inicial IV. El modo OFB, al momento de cifrar hace uso del cifrador para descifrar. Convierte el cifrado en bloque al modo de cifrado continuo. OFB resuelve este problema, ya que está libre de errores de bits en el bloque de texto sin formato. (GeeksforGeeks, 2018)

2. **¿A expensas de qué incrementa Triple DES la seguridad de DES?**

El algoritmo triple DES, está basado en DES. Este algoritmo aplica un conjunto de operaciones necesarias para cifrarlo, usando la clave criptográfica. 3DES hace triple cifrado del DES. Se basa en aplicarlo tres veces con tres claves distintas, resultando ser así mucho más seguro.

3. **¿Cuál es la principal debilidad de DES?**

Actualmente, DES es considerado inseguro, y la razón principal es porque el tamaño de su clave de 56 bits es demasiado corto, por lo que terminan rompiéndose en menos de 24 horas. (Wikipedia, 2021)

4. **¿Por qué AES supero a DES?**

Si comparamos DES y AES, se puede notar claramente que el algoritmo DES para el cifrado de datos no es útil, no debería de usarse porque es inseguro. Y esto es debido a que el tamaño de la clave es muy corta. Convirtiéndose en un algoritmo obsoleto hoy en día. En el caso de que se este usando DES o triple DES para cifrar datos, debería de cambiarse por el algoritmo AES. (*Difference Between DES and AES (with Comparison Chart)*)_{2016, 2016)}

Referencias

*Difference between des and aes (with comparison chart)*₂₀₁₆. (2016, Oct).

Dworkin, M. (2001). *Recommendation for block cipher modes of operation: Methods and techniques* (n.º NIST Special Publication (SP) 800-38A). doi: 10.6028/NIST.SP.800-38A

GeeksforGeeks. (2018, Jul). <https://www.geeksforgeeks.org/block-cipher-modes-of-operation>.

Wikipedia. (2021). *Data encryption standard* — *wikipedia, la enciclopedia libre*. ([Internet; descargado 29-octubre-2021])

Wikipedia contributors. (2020). *Block cipher mode of operation* — *Wikipedia, the free encyclopedia*. https://en.wikipedia.org/w/index.php?title=Block_cipher_mode_of_operation&oldid=986495646. ([Online; accessed 22-October-2021])