Proyecto CLCript
Cuadernos de Laboratorio de Criptografía. Entrega nº 1. Ultima actualización 06/05/19
Autor: Dr. Jorge Ramió Aguirre (@criptored)
Prácticas con algoritmos DES y AES: cifra, rellenos y modos de cifra

- Software safeDES: http://www.criptored.upm.es/software/sw_m001j.htm
- Software AESPhere: http://www.criptored.upm.es/software/sw_m001p.htm
- HexEd.it: https://hexed.it/
- Lectura de interés: https://en.wikipedia.org/wiki/Padding_(cryptography)
- Tablas y códigos: http://www.criptored.upm.es/descarga/Codigos_y_tablas_de_uso_frecuente_en_criptografia.pdf

Objetivos:
1. Comprobar el cifrado en mod ECB y CBC.
2. Cifrado y descifrado de textos y archivos.
3. Observar la deficiencia del cifrado ECB que muestra en el criptograma las repeticiones de bloques del archivo en claro, editando los archivos con un editor hexadecimal.
4. Observar dos tipos de relleno, zero padding usado en el algoritmo DES y PKCS7 usado en el algoritmo AES.

I. DES modo ECB

Ejercicio 1)

1.1. Pinchando en el icono verde del Menú, cifra el texto M1 en ASCII con la clave K en hexadecimal que se indican.
Entrada del texto en claro desde pestaña Teclado, entrada de la clave desde pestaña Opciones, visionado del criptograma desde pestaña Resultado Teclado, opciones cifrar, descifrar desde el combo debajo del Menú. Pincha en flecha Comenzar para operar.
M1 = Aquí habrá relleno
K = 0x FF90B1C2D054D89A

1.2. ¿Cuántos bloques se han cifrado y por qué?

1.3. Introduce como entrada en hexadecimal el criptograma encontrado en el apartado1.

1.4. Descifra el criptograma

1.5. Observa el relleno que se muestra en el texto en claro en hexadecimal.

1.6. ¿Cuántos bits de relleno se han usado?

Comprueba tu trabajo:

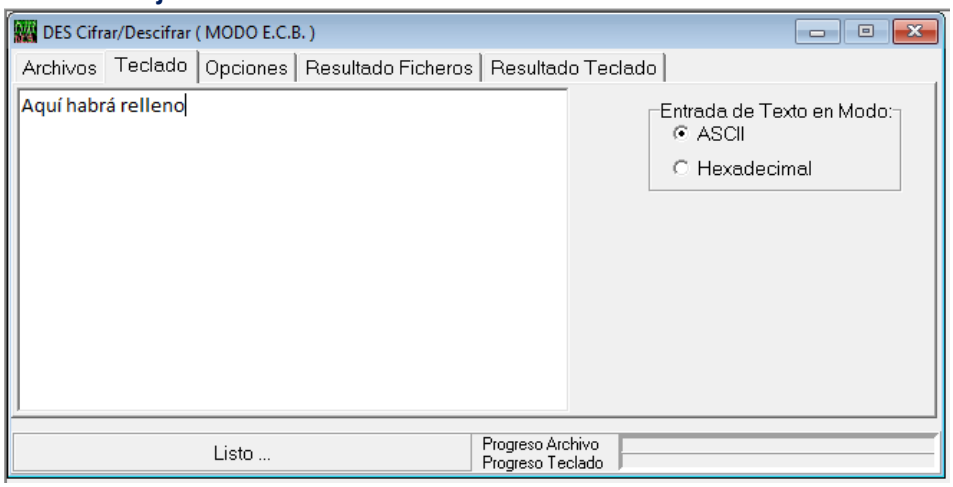

Figura 1. Entrada del texto en claro en ASCII.

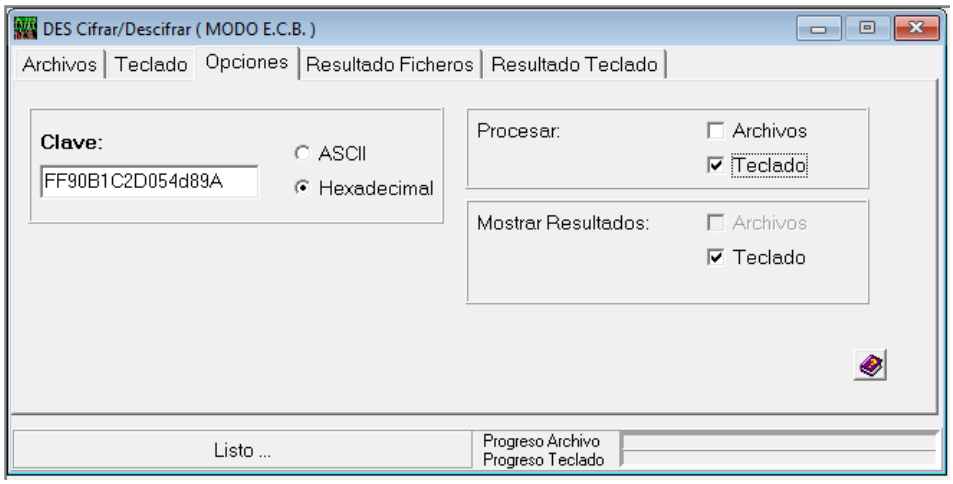

Figura 2. Entrada de la clave en Hexadecimal.

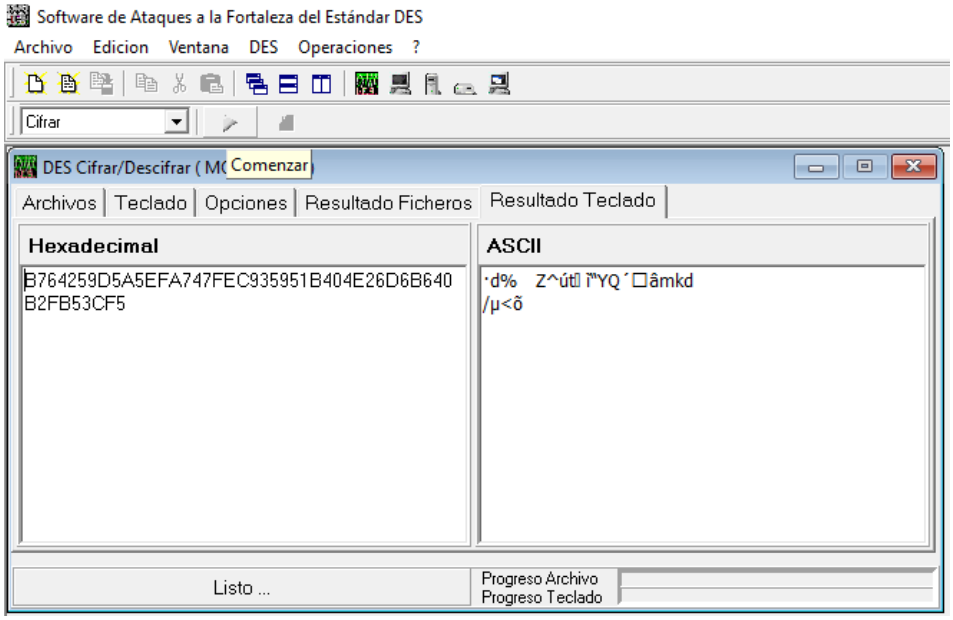

Figura 3. Cifrado del mensaje M1. Criptograma en Resultados Teclado, combo Cifrar.

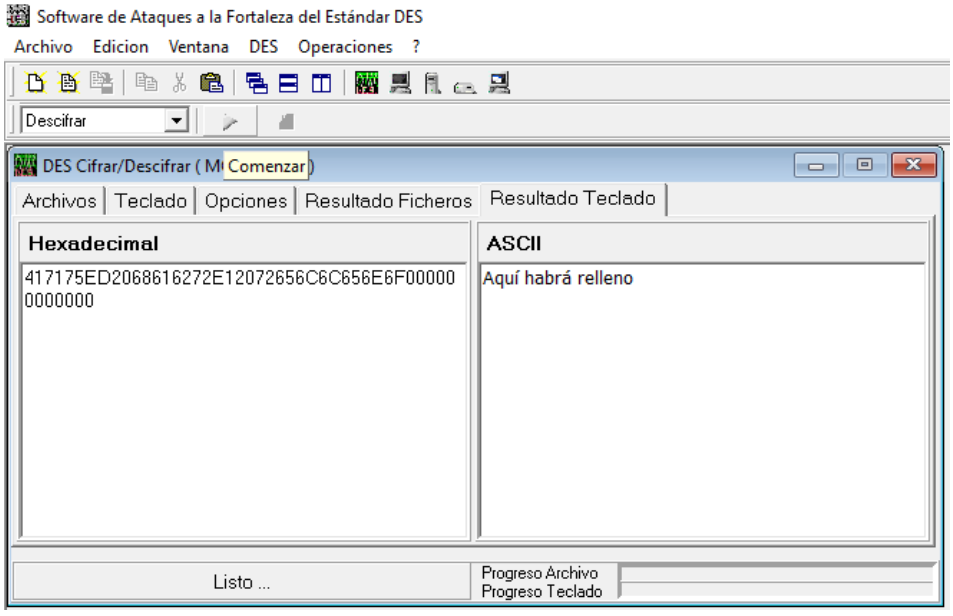

Figura 4. Descifrado del criptograma en Resultados Teclado, combo Descifrar, y relleno de 6 bytes en hexadecimal.

Ejercicio 2)

4.1. Cifra ahora el texto M2 con la clave K y repite los pasos del ejercicio 1
M2 = Aquí ya no habrá relleno
K = 0x FF90B1C2D054D89A

4.2. ¿Por qué en este caso ya no hay relleno?

4.3. Saca conclusiones de lo visto en estos dos ejercicios

Comprueba tu trabajo:

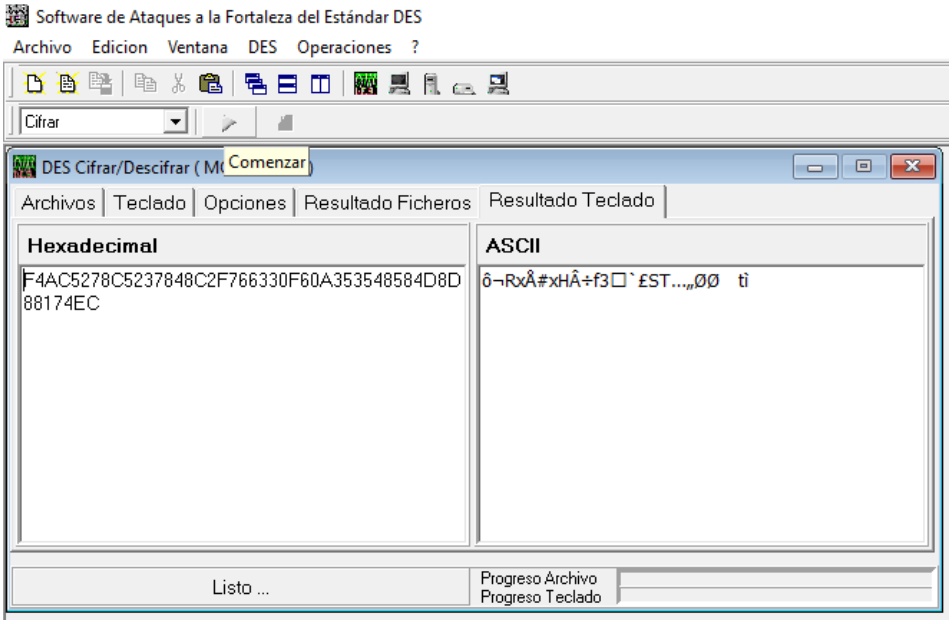

Figura 5. Cifrado del mensaje M2. Criptograma en Resultados Teclado, combo Cifrar.

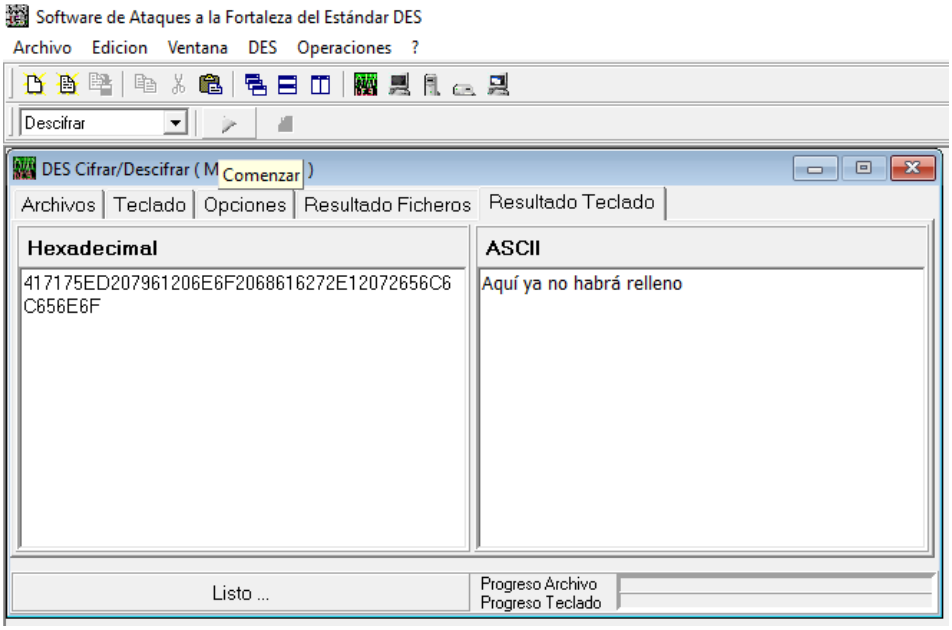

Figura 6. Descifrado del criptograma en Resultados Teclado, combo Descifrar, sin relleno.

Ejercicio 3)

3.1. Con safeDES es recomendable introducir el criptograma en hexadecimal, ya que el programa a propósito no guarda valores ASCII no imprimibles del criptograma, aunque lógicamente sí conserve esos bytes en el formato hexadecimal. Esto se hizo con la

intención de que los alumnos se acostumbrasen a trabajar en hexadecimal, muy común en criptografía.

3.2. Comprueba que si cifras el siguiente texto en claro M3 (punto incluido), con la clave K y luego descifras el criptograma introduciendo éste como ASCII, no vas a poder descifrar correctamente todo el criptograma.
M3 = Una función hash no es un algoritmo de cifrado.
K = 0x ABCDEF0123456789

3.3. Dependiendo de la clave utilizada, algunas veces sí podemos descifrar parte del criptograma porque en el criptograma aparecen valores ASCII imprimibles. Repite este ejercicio cifrando M3 con K = 0x ABCDEF987654ABCD.

3.4. Observa que puedes descifrar correctamente sólo algunos los bloques.

Comprueba tu trabajo:

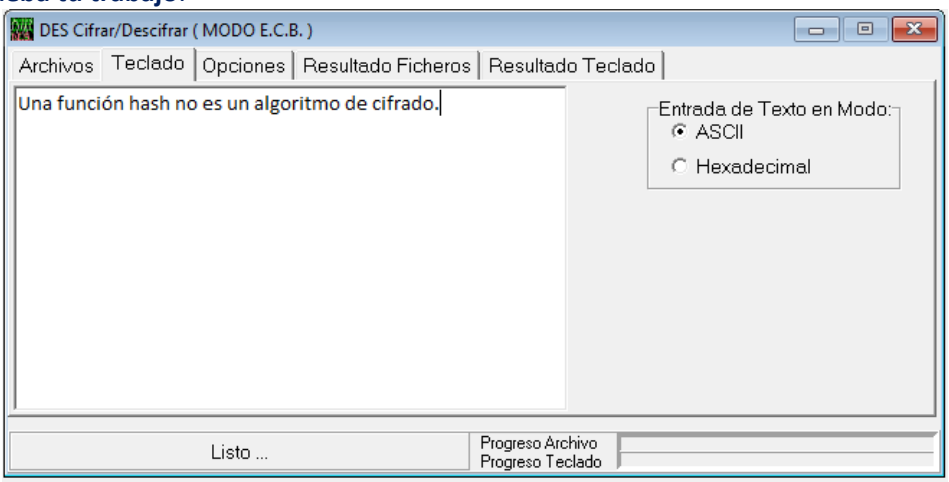

Figura 7. Entrada del texto M3.

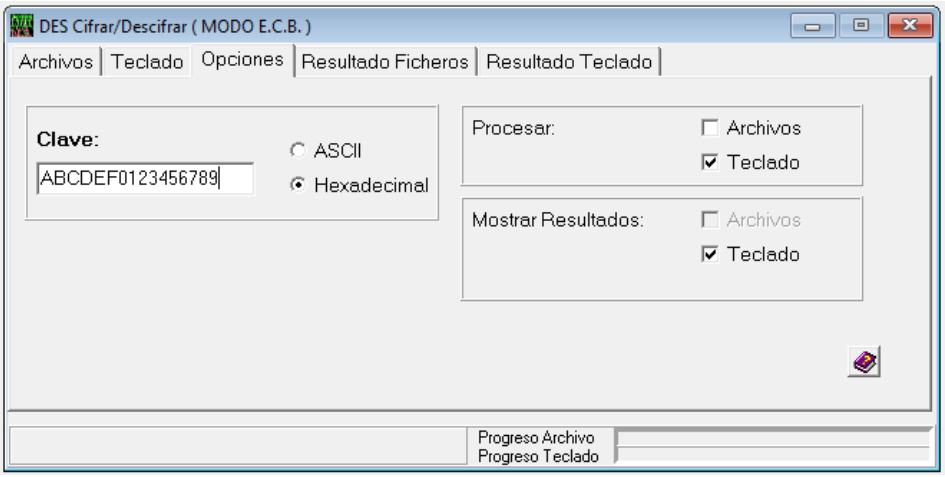

Figura 8. Entrada de la clave K.

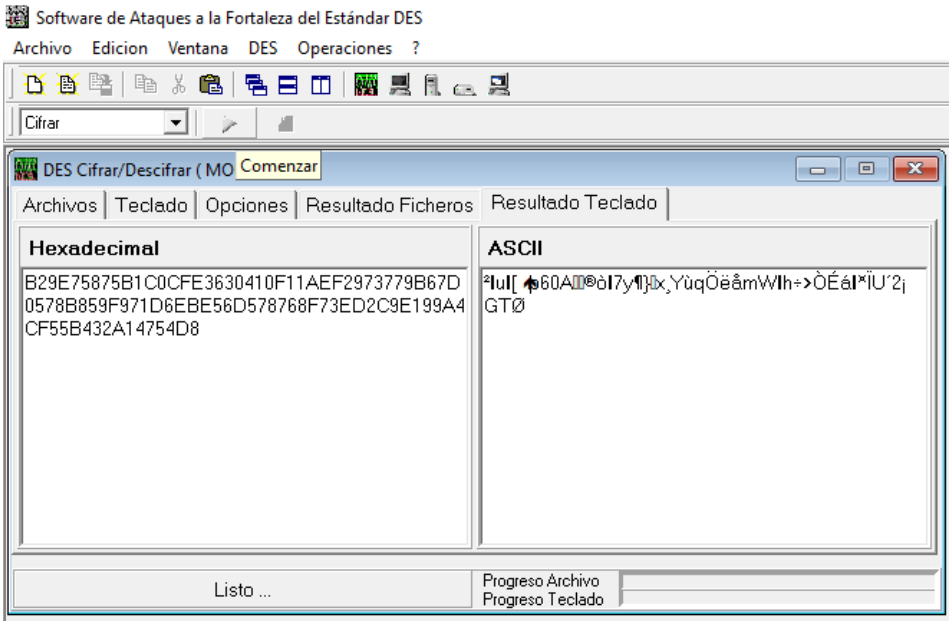

Figura 9. Cifrado del texto M3.

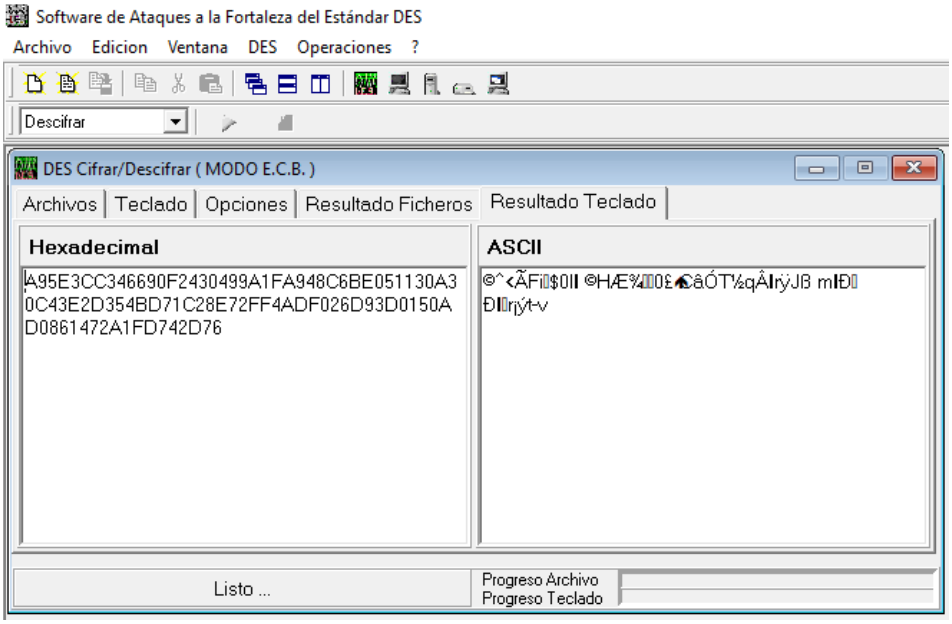

Figura 10. Descifrado incorrecto al haber introducido como entrada el criptograma en ASCII.

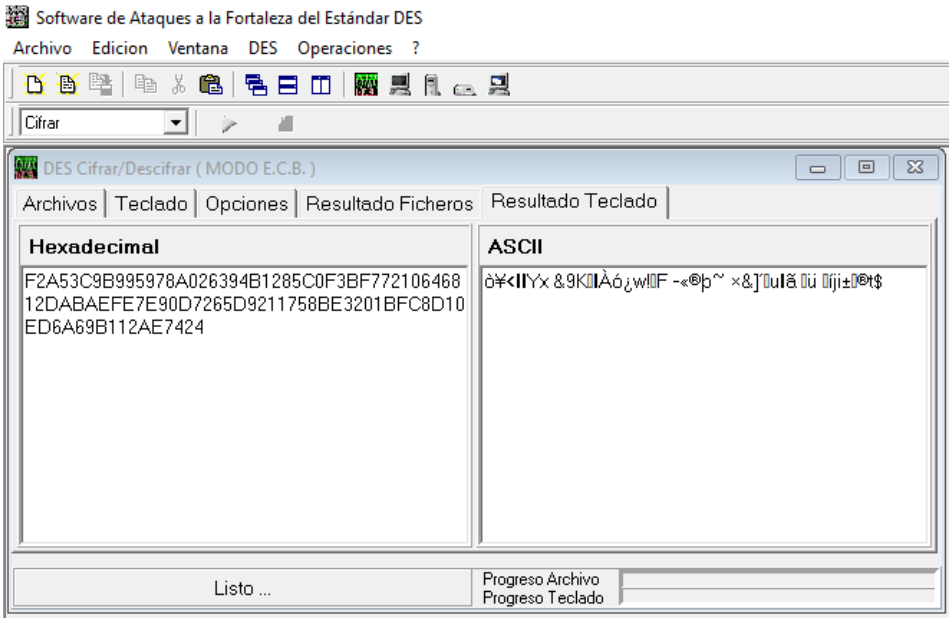

Figura 11. Cifrado de M3 con la clave K = 0x ABCDEF0123456789.

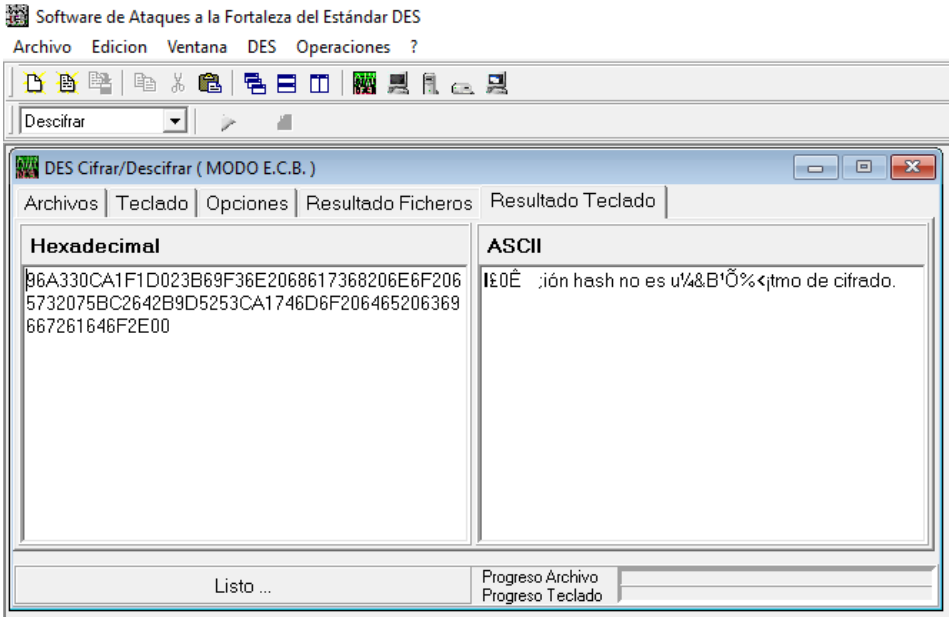

Figura 12. Descifrado parcialmente incorrecto al haber introducido el criptograma en ASCII. Sólo se descifran correctamente los bloques 2, 3, 5 y 6 (Bloques de texto en claro: “Una func”, “ión hash”, “ no es u”, “n algori”, “tmo de c”, “ifrado.”)

Observación:
En el descifrado de texto, safeDES lo hace por líneas, lo cual no es del todo correcto ya que el texto descifrado tendrá estos dos caracteres ASCII añadidos 0D 0A y que significan 0D = CR = Retorno de carro y 0A = LF = Salto de línea, en cada línea de texto de la caja de entrada.

- Comprueba estos códigos en el archivo pdf de Tablas y códigos, indicado al comienzo de esta práctica.
- Cifra con la clave K = 0x FF90B1C2D054D89A el texto M4.
- M4 = Una función hash es un algoritmo que transforma un conjunto arbitrario de elementos de datos, como puede ser un fichero de texto, en un único valor de longitud fija.

- Luego descifra el criptograma y observa esos dos caracteres 0D 0A que marcan el fin de línea, justo después de los espacios en blanco (20) de las palabras un de la primera línea y ser en la segunda línea.

Comprueba tu trabajo:

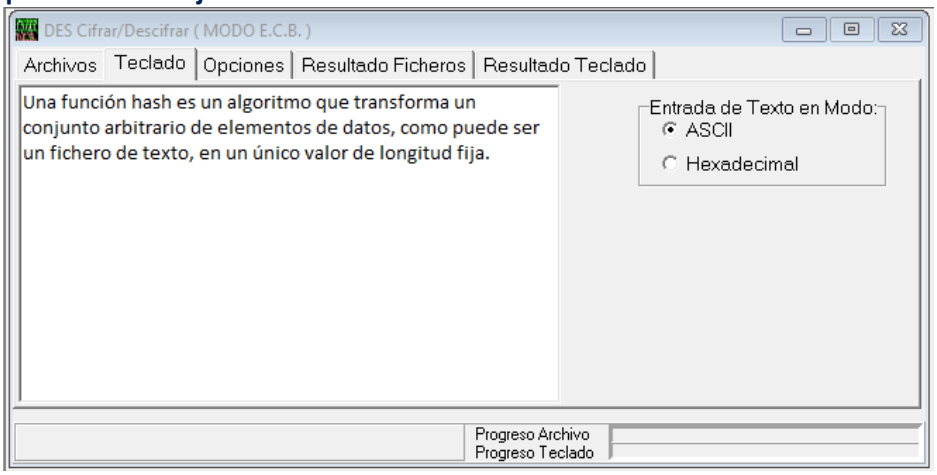

Figura 13. Texto M4 que al introducirse forma tres líneas de texto.

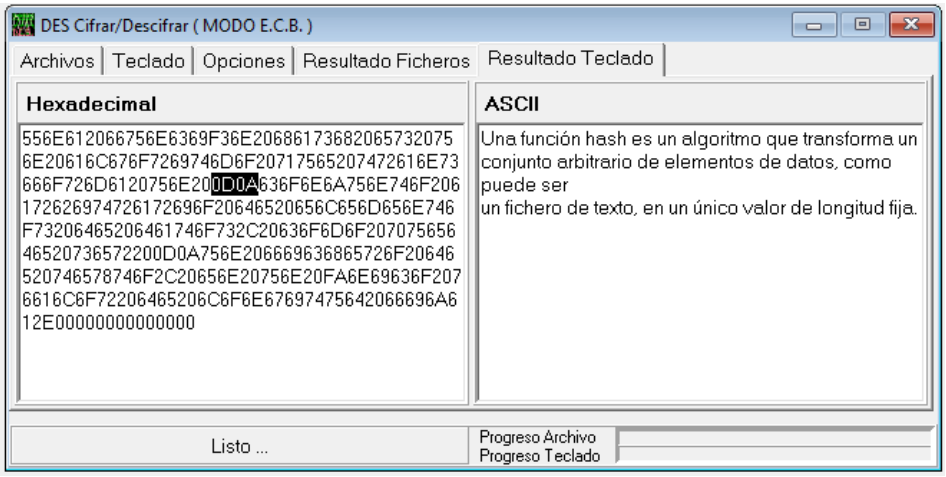

Figura 14. Descifrado de C4 donde se observa el cambio de la primera línea 0D0A.

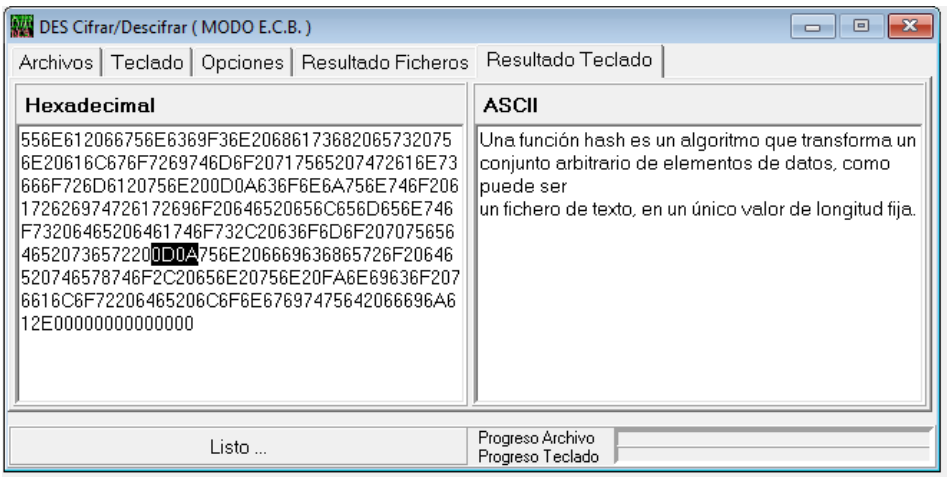

Figura 15. Descifrado de C4 donde se observa el cambio de la segunda línea 0D0A.

Ejercicio 4)

4.1. Con safeDES y la clave K = 0x 78AF902E8CA1F03D descifra el archivo cifrado.cif que podrás descargar aquí http://www.criptored.upm.es/descarga/cifrado.cif o también desde el proyecto CLCript http://www.criptored.upm.es/software/sw_m001s.htm.

4.2. Elige cifrado.dcf como nombre de archivo de destino.

4.3. Observa que en Resultado Ficheros se aprecian muchas cadenas de 0 repetidas, incluso una gran cantidad al final del archivo. ¿Por qué? Si no sabes la respuesta, busca en Internet algún editor en hexadecimal e.g. https://hexed.it/ y edita (Open file) el archivo cifrado.dcf. Abierto el archivo, recorre el código y observa que hay texto legible, incluso repetido, así como muchos bytes iguales, que es propio de un formato de archivo.

4.4. Cambia la extensión del archivo descifrado de cifrado.dcf a cifrado.exe y observa que se ha recuperado la calculadora de Windows 95.

4.5. Comprueba un bug de esta calculadora, resolviendo 10^{15} mod 61. Debe ser 50 y la calc.exe entregaba 100, un valor erróneo y, más aún, fuera del cuerpo n = 61.

4.6. Cifra el archivo calc.exe con K = 0x 78AF902E8CA1F03D. Observa que las cadenas de 8 bytes en 0 al final del archivo en claro en el criptograma son 6205A78E5078C972.

4.7. ¿Cómo explicas que esto es algo muy negativo del modo de cifra ECB?

Comprueba tu trabajo:

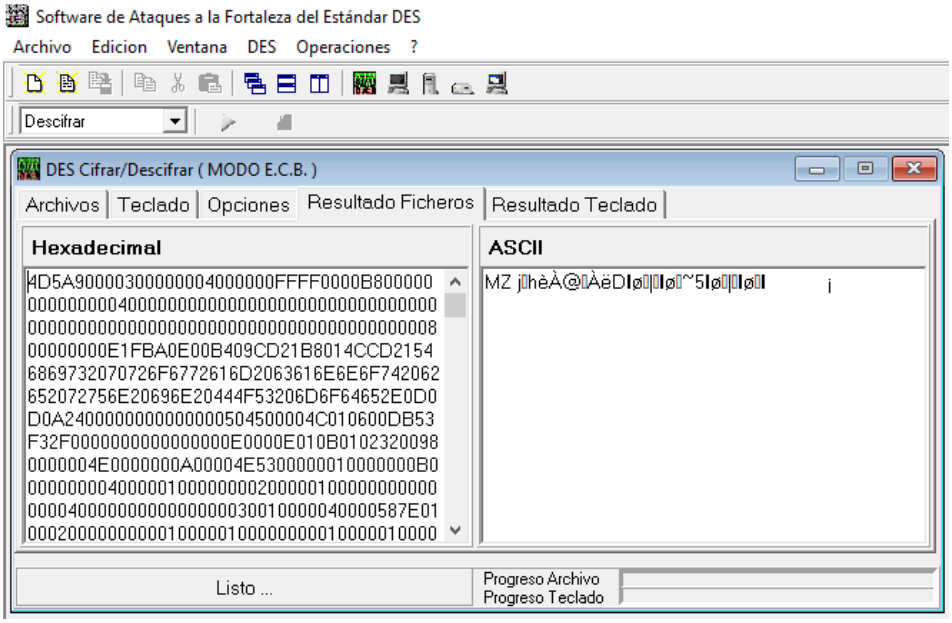

Figura 16. Primeros bloques del descifrado del archivo cifrado.cif desde Resultado Ficheros.

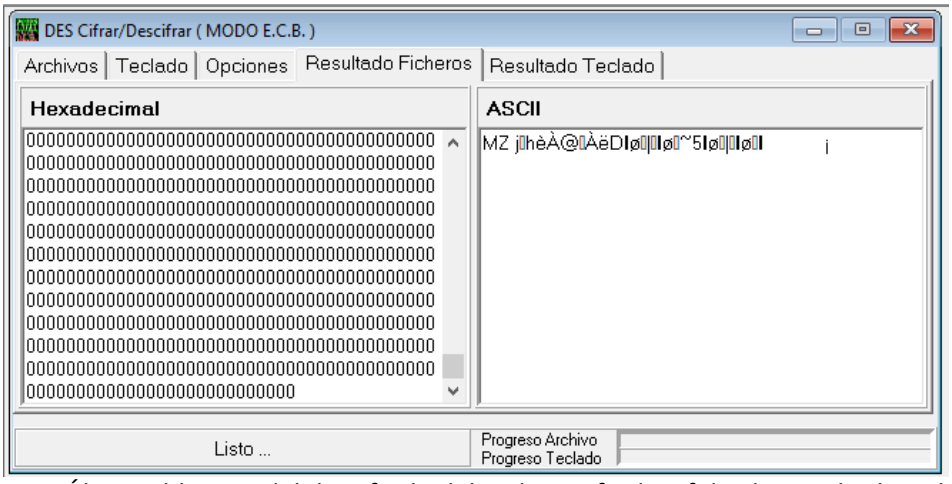

Figura 17. Últimos bloques del descifrado del archivo cifrado.cif desde Resultado Ficheros.

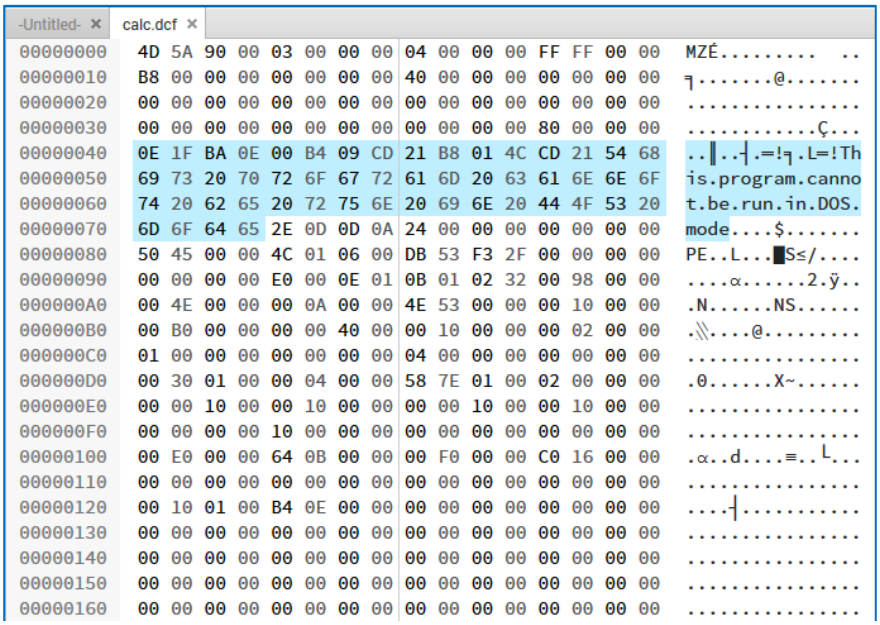

Figura 18. Archivo cifrado.dcf editado online con HexEd.it (comienzo del archivo).

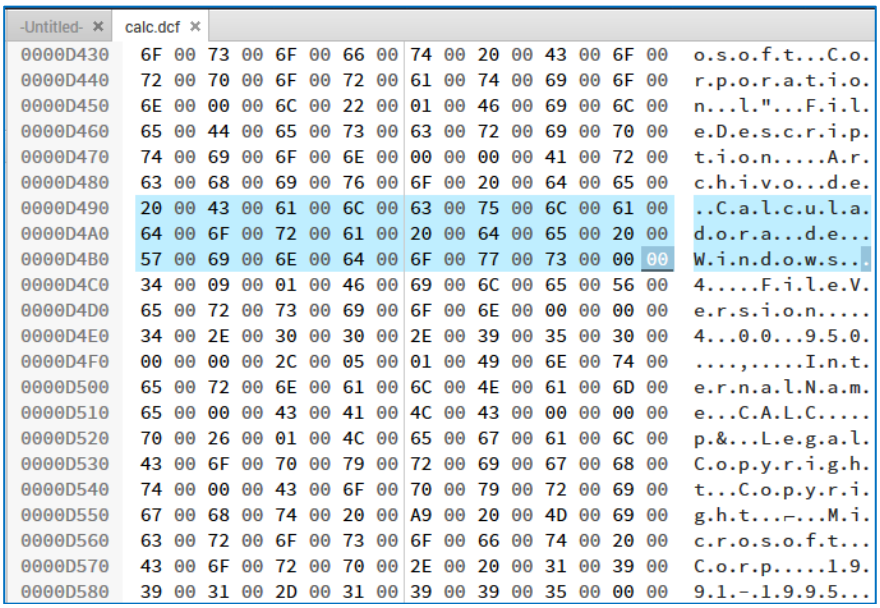

Figura 19. Archivo cifrado.dcf editado online con HexEd.it (casi al final del archivo).

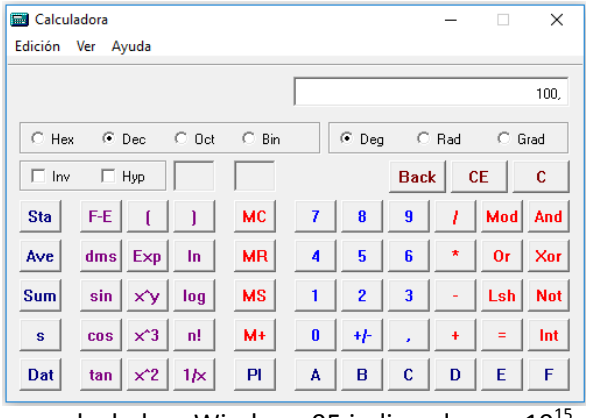

Figura 20. Bug en calculadora Windows 95 indicando que 10^{15} mod 61 = 100.

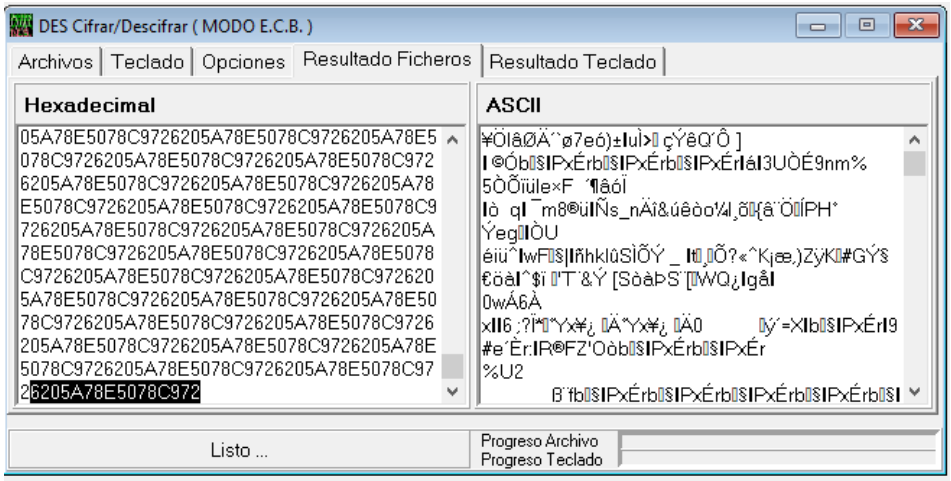

Figura 21. Cadenas de 8 bytes en 0 del archivo en claro se cifran como 0x 6205A78E5078C972.

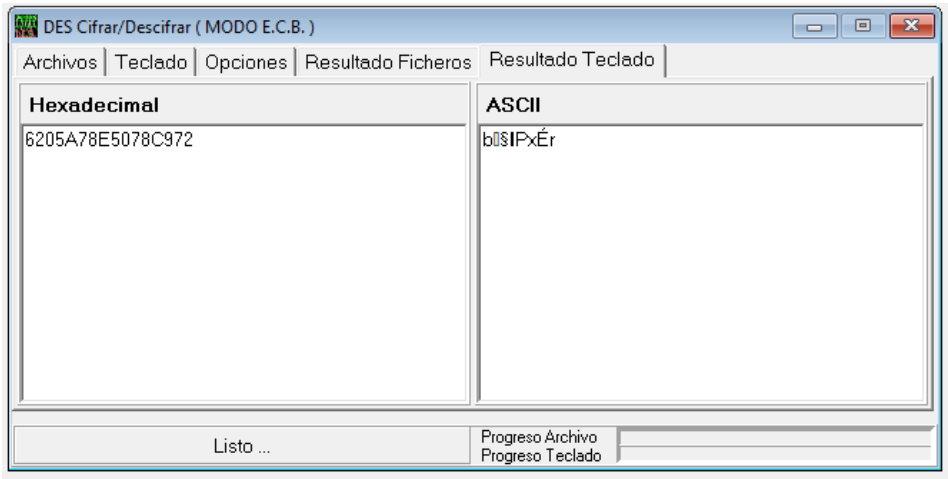

Figura 22. Comprobación con safeDES de que el texto en hexadecimal 0x 0000000000000000 al cifrarlo con K = 0x 78AF902E8CA1F03D, se obtiene el criptograma 0x 6205A78E5078C972.

II. AES 128 modo CBC

Ejercicio 5)

5.1. Cifra de forma Directa el texto M1 con salida en Base 64
M1 = La cifra con AES usa bloques de texto de 128 bits
K = 0x 11223344556677889900AABBCCDDEEFF
IV = 0x FFFF1111BBBB2222CCCC3333DDDD0000

5.2. Observa el relleno que se indica en el texto en claro.

5.3. ¿Qué relleno se ha utilizado y por qué?

Comprueba tu trabajo:

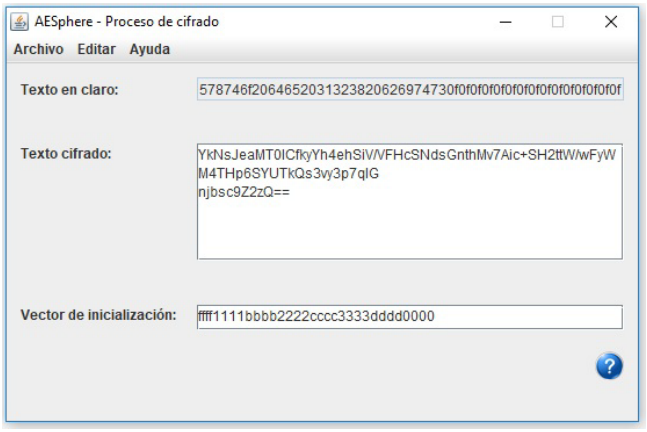

Figura 23. Relleno en AES de tamaño 0F.

Ejercicio 6)

6.1. Con las mismas claves K e IV, cifra de forma Directa M2 (se ha quitado la "s" en bits) de forma que el texto en claro tiene 48 caracteres = 384 bits, exactamente 3 bloques:
M2 = La cifra con AES usa bloques de texto de 128 bit
K = 0x 11223344556677889900AABBCCDDEEFF
IV = 0x FFFF1111BBBB2222CCCC3333DDDD0000

6.2. Observa el relleno que se indica ahora en el texto en claro.

6.3. ¿Por qué, a pesar de que la cifra es en modo CBC, excepto el último bloque del criptograma, los demás bloques son iguales en C1 y C2?

6.4. ¿Cuántos bloques se han cifrado en M1 y cuántos bloques han cifrado en M2?

6.5. ¿Por qué si M1 y M2 tienen diferentes tamaños, en C1 y C2 se observa en el código Base 64 dos signos =?

Comprueba tu trabajo:

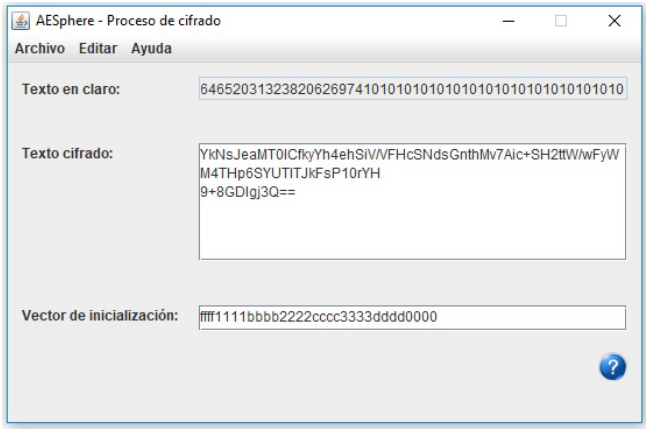

Figura 24. Relleno en AES de un bloque completo.

III. AES 128 modo ECB

Ejercicio 7)

7.1. Cifra el texto anterior M2 en modo ECB pero ahora Paso a Paso:
M2 = La cifra con AES usa bloques de texto de 128 bit
K = 0x 11223344556677889900AABBCCDDEEFF

7.2. Observa que el relleno que se indica en el texto es el mismo que en el ejercicio 4.

7.3. Como el último bloque es todo relleno, comprueba que la entrada a la primera vuelta de ese 4to y último bloque de cifra después de AddRoundKey es: "*Comienzo de ronda: 01322354457667988910baabdccdfeef*". Para ello usa la opción Operaciones de AESPhere y calcula el AddRoundKey de estas dos matrices:

Matriz de estado: 0x 10101010101010101010101010101010
Clave k_0: 0x 112233445566778899 00AABBCCDDEEFF

7.4. Según lo que has observado, ¿el relleno también se cifra?

Comprueba tu trabajo:

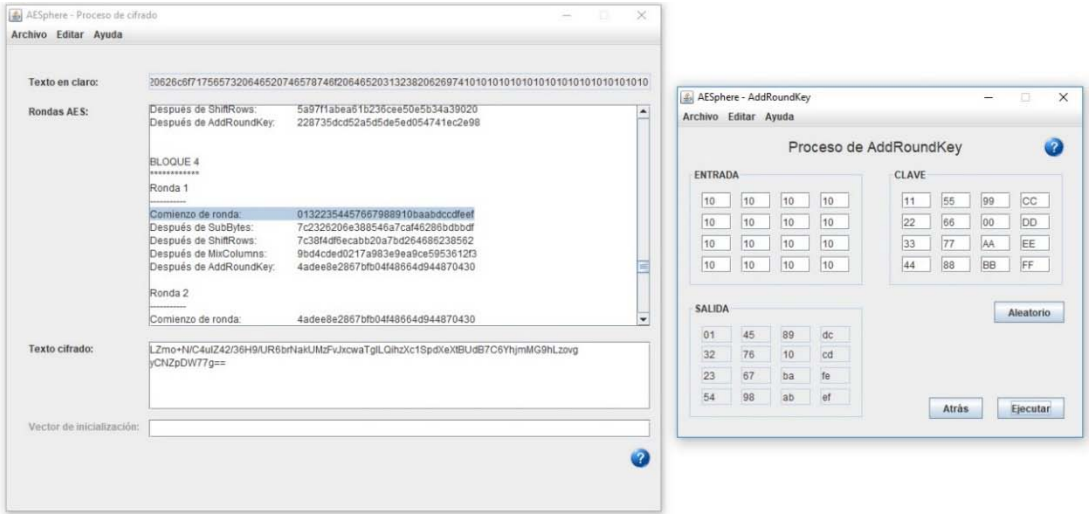

Figura 25. Cifra con AESPhere Paso a Paso y función AddRoundKey.

Puedes utilizar esta documentación, otros libros, material multimedia y software de prácticas generados en Criptored, todos de libre distribución en Internet, para poder demostrar que entiendes y sabes cómo trabaja la criptografía, logrando la nueva certificación técnica profesional CriptoCert Certified Crypto Analyst, reconocida por el Centro Criptológico Nacional CCN de España, disponible desde el mes de abril de 2019.

Encontrarás más información sobre esta certificación y correo de contacto en el sitio web: https://www.criptocert.com

Madrid, 6 de mayo de 2019
Dr. Jorge Ramió Aguirre