Casos prácticos

Cifrado en bloque DES

Telefónica EDUCACIÓN DIGITAL

Casos prácticos

Software: safeDES: http://www.criptored.upm.es/software/sw_m001j.htm

1 | Comprobación del funcionamiento de DES

Comprueba que se cumple la cifra en modo ECB de los siguientes mensajes con las claves indicadas. Observa que hay valores en formato hexadecimal y otros en ASCII.

a. Si ciframos **M_{HEX} = 8787878787878787, con la clave K_{HEX} = 0E329232EA6D0D73, se obtiene $_{CHEX}$ = 0000000000000000.**

b. Si ciframos **M_{HEX} = 0000000000000000**, con la clave **K_{HEX} = 0123456789ABCDEF**, se obtiene **C_{HEX} = D5D44FF720683D0D.**

c. Si ciframos **M_{ASCII} = Probándolo**, con la clave **K_{ASCII} = 66666666**, se obtiene **C_{ASCII} = ûÔWBH¼{ú=âw+ËC€ÿ.**

d. Repite la operación del apartado c) ahora con la clave **K_{ASCII} = 77777777**. y compáralo con lo que se obtenía en el apartado c).

2 | Operaciones de cifrado con teclado y ficheros de texto

a. Cifra el mensaje el mensaje M con la clave K. Recupera luego el texto original con la ayuda del portapapeles a partir del criptograma, tanto en formato ASCII como en formato hexadecimal.

    M = Esta es una prueba de teclado

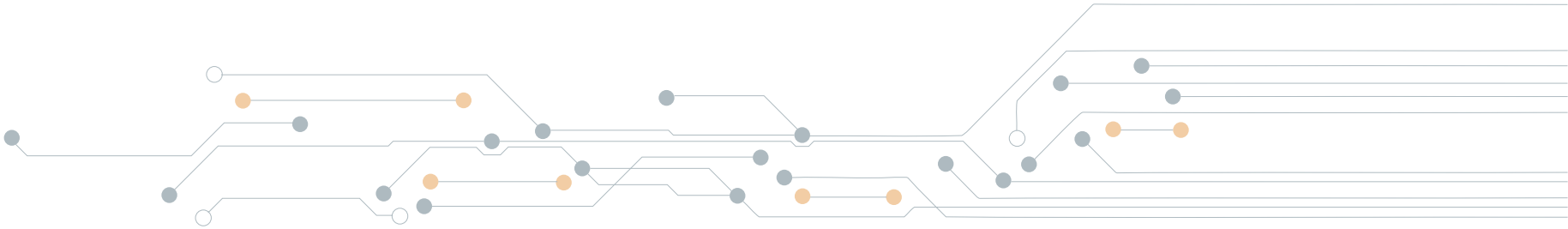
    K = UnaTecla

b. Repite el punto anterior ahora con este nuevo mensaje y observa lo que sucede al recuperar el texto desde un criptograma en ASCII con el portapapeles.

    M = A ver qué pasa con esta segunda prueba de teclado.

c. Usando la clave K = CLAVEDES, cifra el mensaje de 8 caracteres M = CIFRADOR. Repite la operación de cifra ahora con el mensaje de 12 caracteres M = CIFRADOR DES. Observa semejanzas y/o diferencias a través de la salida en hexadecimal de cada cifrado.

d. Intenta descifrar el fichero *prometeo.cif* adjunto, llamando al fichero de salida *prometeo.dcf.* Si nos han dicho que la clave puede ser cualquiera de las siguientes combinaciones de 8 caracteres: Frank123 MaryMary Frankens marymary 1234Mary.



3 | Operaciones de cifra con claves débiles y semidébiles

Definición 1: Una clave k se considera débil si se verifica que $E_k[E_k(M)] = M$, es decir, al cifrar dos veces con la clave se vuelve a obtener el mensaje M. Estas claves son fáciles de romper y en DES tienen la peculiaridad de que las 16 subclaves generadas son todas iguales.

Definición 2: Una pareja de claves k1, k2 se consideran semidébiles si se verifica que $E_{k1}[E_{k2}(M)] = M$. En este caso se generan dos valores de subclaves diferentes, obteniéndose ocho veces cada uno.

Durante una operación, la clave secreta de 56 bits se descompone en 16 sub-claves de acuerdo con el procedimiento de clave de DES, una de cada cual es usada en cada uno de las dieciséis rondas de DES. Las claves débiles de DES son aquellas que producen 16 subclaves idénticas. Esto ocurre cuando los bits de la clave son:

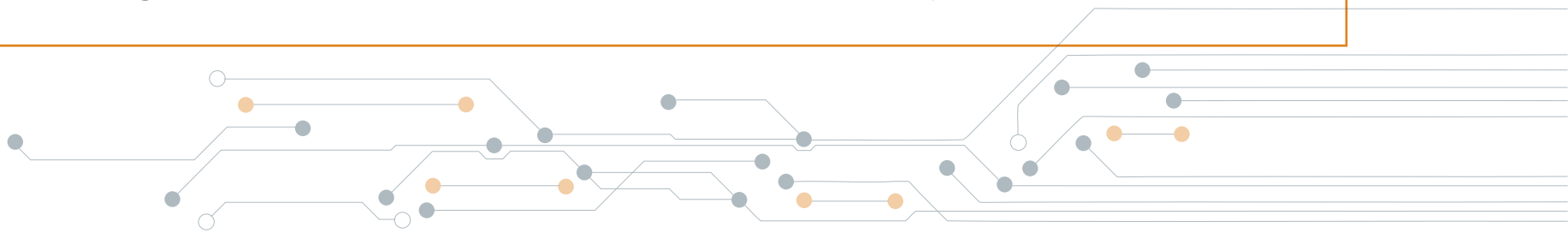
1) Todo ceros.
2) Todo unos.
3) La primera mitad ceros y la segunda unos.
4) La primera mitad unos y la segunda ceros.

Dado que todas las subclaves son idénticas y que DES es una red de Feistel, el cifrado es autoreversible, esto es, cifrar dos veces produce el texto plano original.

DES tiene también claves semi-débiles. Vienen en pares K1 and K2 y poseen la siguiente propiedad:

$$DES_{k1}(DES_{k2}(M)) = M$$

donde EK(M) es el algoritmo de cifrado cifrando el mensaje M con la clave K. Existen seis pares de claves semi-débiles.



4 | Ataque Monousuario

a. Primero cifra el mensaje M con la clave K que se indica:

M = Prueba de ataque monousuario.

K_{HEX}= 1111111122222222.

b. Ahora con la ayuda del portapapeles, realiza un Ataque Monousuario al texto anteriormente cifrado con una búsqueda delimitada de claves, siendo las claves inicial y final las que se indican:

Clave inicial: $K_{i\ HEX}$ = 1111111122000000.

Clave final: $K_{f\ HEX}$ = 1111111122333333.

c. Observa todas las claves posibles, el tiempo que tarda en encontrarlas y la tasa de búsqueda del programa.

4 | Solución

a. Primero cifra el mensaje M con la clave K que se indica:

M = Prueba de ataque monousuario.

C= = FF 37 7C C9 CE 6B 23 1A 51 67 BE 0A F4 3C 4E A0 27 11 8C 01 0F 0C D7 59 72 64 7F 27 B8 4F 30 37

FF377CC9CE6B231A5167BE0AF43C4EA027118C010F0CD75972647F27B84F3037

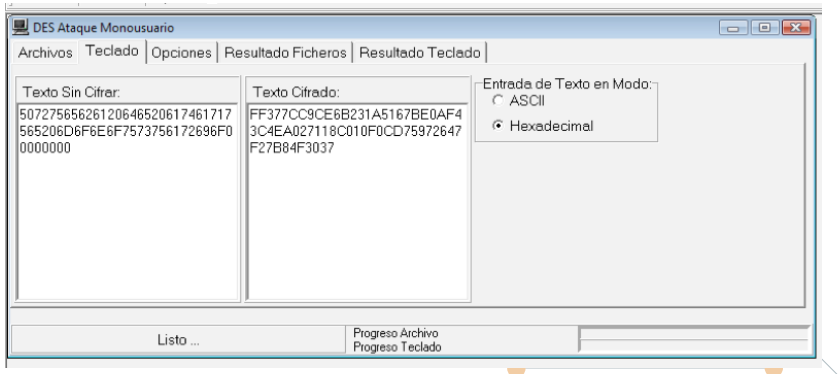
b. Ahora con la ayuda del portapapeles, realiza un Ataque Monousuario al texto anteriormente cifrado con una búsqueda delimitada de claves, siendo las claves inicial y final las que se indican:

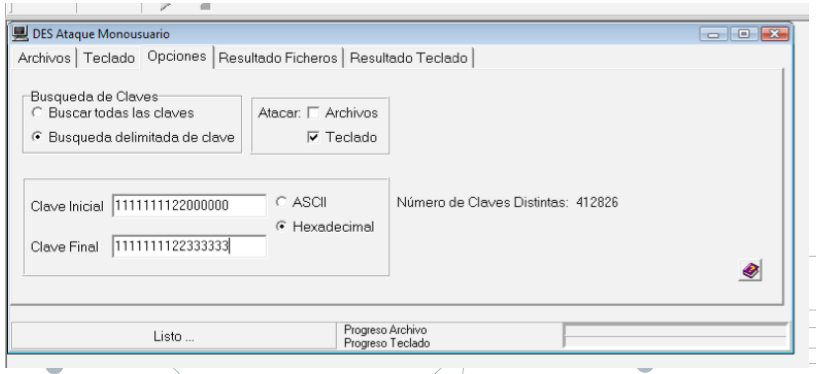
Clave inicial: $K_{i\,HEX}$ = 1111111122000000.

Clave final: $K_{f\,HEX}$ = 1111111122333333.

M_{HEX}= 50 72 75 65 62 61 20 64 65 20 61 74 61 71 75 65 20 6D 6F 6E 6F 75 73 75 61 72 69 6F 00 00 00 00

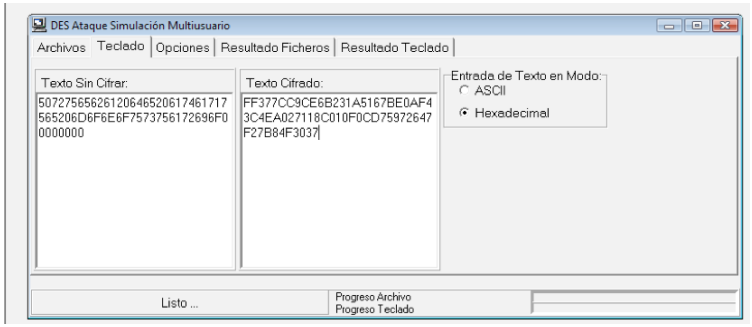
C_{HEX}= = FF 37 7C C9 CE 6B 23 1A 51 67 BE 0A F4 3C 4E A0 27 11 8C 01 0F 0C D7 59 72 64 7F 27 B8 4F 30 37

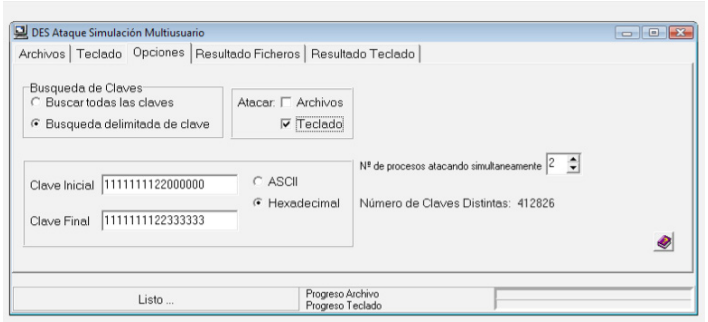


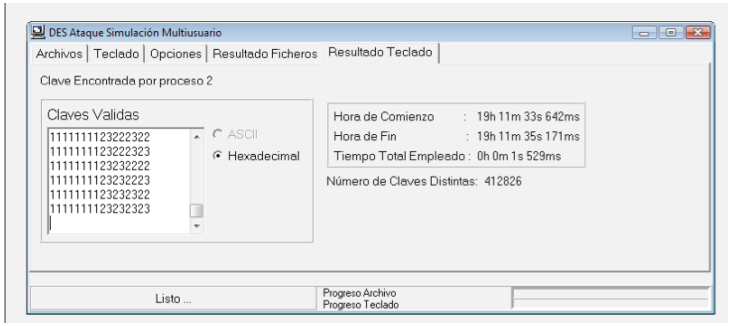


5 | Ataque Simulación Multiusuario

a. Vuelve a repetir el ataque a la cifra del mensaje anterior usando ahora el modo Ataque Simulación Multiusuario con dos procesos.







b. Repite el punto anterior usando ahora en el ataque desde 3 hasta 10 procesos. Observa qué proceso es el que logra romper la clave.

6 | Ataque Multiusuario

Si tienes posibilidad de trabajar en una red con direcciones IP, vas a realizar un ataque multiusuario real sobre una clave delimitada en términos similares al que has simulado con una sola máquina.

a. Con la participación simultánea de todos los asistentes en el aula, se elegirá una clave de cifra, así como la clave inicial y final del ataque. Definido el ámbito de ataque, una máquina actuará como servidor ejecutando la opción Ataque Servidor y las demás máquinas actuarán como clientes ejecutando cada una de ellas la opción Ataque Cliente.

7 | Simulación del Ataque DES Challenge III

En el tercer desafío RSA al DES, el texto cifrado era *DESIII.txt*, que se muestra además agrupado en bloques de 64 bits para una mejor visualización y un trabajo con bloques más cómodo. El modo de cifra en este caso era de tipo CBC, Encadenamiento de Bloques Cifrados, y el vector inicial IV usado, así como la clave K encontrada eran:

IV_{HEX} = DA4BBEF16B6E983D.

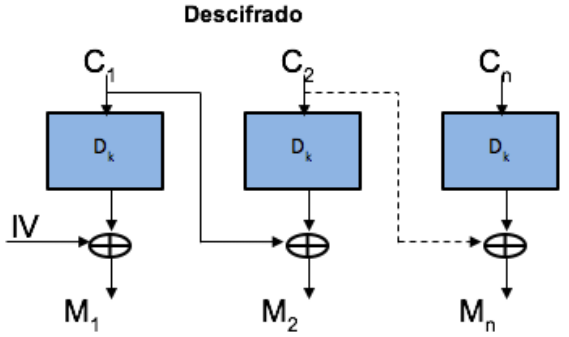
K_{HEX} = 922C68C47AEADFF2.

DESIII.txt

BD 0D DE 91 99 60 B8 8A	47 9C B1 5C 23 7B 81 18
99 05 45 BC DE 82 01 AB	53 4D 6F 1C B4 30 63 3C
EE CD 96 2E 07 C6 E6 95	99 9C 96 46 5A 95 70 02
02 70 98 BD 41 C2 88 A9	F0 2F 8B E5 48 20 D2 A8
A0 6B BF 93 DE 89 F6 E2	52 FD 8A 25 EB D0 7D 96
83 EE A4 2D C8 8D 1B 71	

a. Encuentra el primer bloque del mensaje original haciendo uso de la calculadora de Windows para la operación XOR necesaria, puesto que el programa safeDES trabaja en modo ECB, Electronic CodeBook.

b. De la misma forma que en el apartado anterior, encuentra ahora el mensaje completo de ese desafío.



Telefónica EDUCACIÓN DIGITAL