

# Práctica 1 - Cifrados simétricos

1. Partiremos de un archivo binario de 1024 bits, todos ellos con valor 0 . Para hacer referencia al mismo voy a suponer que se llama input.bin , pero podeis dar el nombre que os convenga.

Programa usado para crear el archivo binario de 1024 bits.

```
#include <stdio.h>

int main()
{
    FILE* pFile;
    pFile = fopen("input.bin", "wb");
    int buffer[1] = {0};
    for (int j = 0; j < 1024; ++j){
        fwrite(buffer,sizeof(int),sizeof(buffer),pFile);
    }
    fclose(pFile);
    return 0;
}
```

Mostrar el tamaño del fichero:

```
du -bsh input.bin
```

```
Xxd input.bin
```

```
MacBook-Pro-de-Rafael:p1 rafa$ xxd input.bin
00000000: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000010: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000020: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000030: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000040: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000050: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000060: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000070: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
```

Vemos todo el fichero lleno de 0

2. Creamos otro archivo binario del mismo tamaño, que contenga un unico bit con valor 1 dentro de los primeros 40 bits y todos los demás con valor 0 . Me

referire a este archivo como input1.bin

Pequeño programa usado para generar el archivo input1.bin. Se elige una posición al azar dentro de las cuarenta primeras posiciones.

Sustituye el primer carácter por 1

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
int main()
{
    srand(time(NULL));
    int r = rand()%40;           // 40 primeras posiciones

    FILE* pFile;
    pFile = fopen("input1.bin", "wb");
    int buffer[1] = {0};
    int buffer2[1] = {1};
    for (int j = 0; j < 1024; ++j){
        if (j==r){
            fwrite(buffer2,sizeof(int),sizeof(buffer),pFile);
        }
        else{
            fwrite(buffer,sizeof(int),sizeof(buffer),pFile);
        }
    }
    fclose(pFile);
    return 0;
}
```

```
MacBook-Pro-de-Rafael:p1 rafa$ 
MacBook-Pro-de-Rafael:p1 rafa$ xxd input1.bin
00000000: 0000 0000 0000 0000 b009 4000 0000 0000
00000010: 0000 0000 0000 0000 b009 4000 0000 0000
00000020: 0000 0000 0000 0000 b009 4000 0000 0000
00000030: 0000 0000 0000 0000 b009 4000 0000 0000
00000040: 0000 0000 0000 0000 b009 4000 0000 0000
00000050: 0000 0000 0000 0000 b009 4000 0000 0000
00000060: 0000 0000 0000 0000 b009 4000 0000 0000
00000070: 0000 0000 0000 0000 b009 4000 0000 0000
00000080: 0000 0000 0000 0000 b009 4000 0000 0000
00000090: 0000 0000 0000 0000 b009 4000 0000 0000
000000a0: 0100 0000 fe7f 0000 0040 78ca 1b56 4ac2
000000b0: 0000 0000 0000 0000 b009 4000 0000 0000
000000c0: 0000 0000 0000 0000 b009 4000 0000 0000
000000d0: 0000 0000 0000 0000 b009 4000 0000 0000
000000e0: 0000 0000 0000 0000 b009 4000 0000 0000
000000f0: 0000 0000 0000 0000 b009 4000 0000 0000
00000100: 0000 0000 0000 0000 b009 4000 0000 0000
```

**3. Cifrad input.bin con DES en modos ECB, CBC y OFB usando como claves una débil y otra semidebil, con vector de inicializacion a vuestra elección, y explicad los diferentes resultados.**

### #Claves débiles

#### #ECB

```
openssl enc -des-ecb -in input.bin -out cipherECB.txt -K 0101010101010101
```

Encripta ECB con una clave débil en hexadecimal. Resultado:

```
00000000: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000010: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000020: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000030: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000040: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000050: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000060: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000070: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000080: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000090: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
000000a0: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....
```

Mostramos las 10 primeros líneas, ya que al ser un cifrado en bloque y ser siempre el valor 0, se repiten los bloques.

#### #CBC

```
openssl enc -des-cbc -in input.bin -out cipherCBC.txt -K 0101010101010101 -iv 0
```

```
00000000: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000010: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000020: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000030: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000040: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000050: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000060: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000070: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000080: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
00000090: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....  
000000a0: c994 7278 8f34 8c4c 1580 5e49 b10a 87a6 ..rx.4.L..^I....
```

### #OFB

```
openssl enc -des-ofb -in input.bin -out cipherOFB.txt -K 0101010101010101 -iv 0
```

MacBook-Pro-de-Rafael:p1 rafa\$ xxd cipherOFB.txt

```
00000000: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000010: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000020: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000030: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000040: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000050: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000060: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000070: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000080: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
00000090: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I  
000000a0: 8ca6 4de9 3fce 23a7 00b0 ab7d 9b52 316c ..M.?.#....}.R1I
```

### #Claves semidébiles

```
openssl enc -des-ecb -in input.bin -out cipherECB2.txt -K 01FE01FE01FE01FE
```

```
00000000: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000010: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000020: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000030: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000040: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000050: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000060: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000070: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000080: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
00000090: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....  
000000a0: 685d 8c7c 7969 72a7 29bd 3389 e394 90f5 h].|yir.).3.....
```

```
openssl enc -des-cbc -in input.bin -out cipherCBC2.txt -K 01FE01FE01FE01FE -iv 0
```

```
00000000: 685d 8c7c 7969 72a7 2206 ff73 aa01 c020 h].|yir."..s...  
00000010: b51e 575e 0861 8ced f329 5c96 2524 950b ..W^.a...)\.%$..  
00000020: 5b00 e231 0ad2 4306 cb7e f144 24c3 d598 [..1..C..~.D$...
```

```
00000030: 21b1 8188 966d 7a82 1a69 e85a 3253 76af !....mz..i.Z2Sv.  
00000040: cc08 67f7 40d1 e3e1 6492 4769 0d82 c421 ..g.@...d.Gi...!  
00000050: e05e cf24 89fd d7f1 c554 9948 1004 079a ^$.....T.H....  
00000060: 84c3 2214 1b73 3a87 89b5 3136 1ab7 ad7b .."s:..16...{  
00000070: 2d43 985d 0e42 607c 8a62 850b df48 0db0 -C.].B`|.b...H..  
00000080: 003a a5e4 17e7 8de4 2dea 5b00 0f51 35cc :.....-[..Q5.  
00000090: 276b 94aa 6a1d 36ad e4e7 f106 3785 8c7a 'k..j.6.....7..z  
000000a0: 8b73 88eb 9e6a 586a 500f 1db8 9666 3fc8 .s...jXjP....f?.
```

```
openssl enc -des-ofb -in input.bin -out cipherOFB2.txt -K 01FE01FE01FE01FE -iv 0
```

```
00000000: 01db 63b4 d414 7260 c40e 9bcf 9178 4374 ..c...r`.....xCt  
00000010: dddc a695 1dea bc08 d85e 7131 d8cf b1c2 .....^q1....  
00000020: 279e b977 4905 d15c 692b b87c 32ec 475c '..wl..Vi+.|2.G\  
00000030: 9afa 313c 3146 7523 f538 5f37 4b69 75bc ..1<1Fu#.8_7Kiu.  
00000040: 76e5 29d0 d001 7519 bbda 522a dc52 85c8 v.)...u...R*.R..  
00000050: 81e0 96c9 4476 96f7 1e8d 7b97 3afe cc48 ....Dv....{.:H  
00000060: 8c5f 08f2 67e7 9fa2 6b53 96dc e0c5 8635 ..g...kS.....5  
00000070: 2a8a 56b3 7694 10e7 38a1 2928 a24a ed58 *.V.v...8.)(.J.X  
00000080: e050 d02c 6b2e e0f5 0798 6946 085a c974 .P.,k....iF.Z.t  
00000090: 313f 0d31 c73d 66bf 7e59 b43f 3470 c9ea 1?.1.=f.~Y.?4p..  
000000a0: a372 226b 3d02 173b bae2 5964 954f 2f3a .r"=..;..Yd.O:/
```

Podemos ver que solo cambia el cifrado en OFB, donde para cifrar se usa un cifrado aleatorio previo, mediante el vector de inicialización y la clave, y después se genera una operación XOR con el texto plano, para dar lugar al texto cifrado.

Esto no ocurre en los demás algoritmos de cifrado previos, ya que se aplica la operación directamente sobre el bloque de texto plano, aplicando XOR entre el texto plano y el vector de inicialización en el caso de OCB, o directamente aplicando la clave a cada bloque de texto plano como en ECB.

#### 4. Cifrad input.bin e input1.bin con DES en modo

**ECB y clave a elegir, pero no débil ni semidebil. Explicad la forma de los resultados obtenidos.**

Hemos usado estas dos órdenes para obtener los resultados:

#ECB

```
openssl enc -des-ecb -in input1.bin -out cipherECB_Ej4-Input.1.txt -K 1010
```

```
openssl enc -des-ecb -in input.bin -out cipherECB_Ej4-Input.txt -K 1010
```

Como podemos ver, hemos usado la clave 1010.

Resultados:

#### Input.bin (almacenados el resultado encriptado en cipherECB\_Ej4-Input.txt)

```
[MacBook-Pro-de-Katael:p1 rafas]$ xxd cipherECB_Ej4-Input.txt
00000000: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000010: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000020: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000030: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000040: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000050: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000060: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000070: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000080: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000090: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
000000a0: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
000000b0: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
000000c0: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
000000d0: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
000000e0: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
000000f0: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
00000100: 108f 4b50 85f5 cfed 253d 0090 ce3f 0d8c ..KP....%=?...
```

#### Input1.bin cipherECB\_Ej4-Input.1.txt

```
[MacBook-Pro-de-Katael:p1 rafas]$ xxd cipherECB_Ej4-Input.1.txt
00000000: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000010: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000020: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000030: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000040: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000050: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000060: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000070: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000080: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000090: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
000000a0: a3d6 0b61 71b3 3d64 7999 a937 e1c7 4cc0 ...aq.=dy..7..L.
000000b0: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
000000c0: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
000000d0: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
000000e0: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
000000f0: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
00000100: 49b7 1bdb 86de d930 2e22 8a62 25e8 48e1 I.....0.".b%.H.
```

Como podemos apreciar, el valor del fichero hace que cambie la forma de cifrado, obteniendo resultados distintos en ambos ficheros. Aún así, es un cifrado de bloques, y vemos que en Input1, se repiten todos los bloques, excepto el bloque 10, donde tenemos el número 1.

En input.bin, en el resultado obtenido vemos que se repiten todos los bloques cifrados, ya que no cambia en todo el texto el valor del texto plano cifrado.

**5. Cifrad input.bin e input1.bin con DES en modo**

**CBC , clave y vector de inicialización a elegir. Comparad con los resultados obtenidos en el apartado anterior.**

Órdenes usadas:

#CBC

```
openssl enc -des-cbc -in input.bin -out cipherCBC_Ej5-Input.txt -K 1010 -iv 0
```

```
openssl enc -des-cbc -in input1.bin -out cipherCBC_Ej5-Input1.txt -K 1010 -iv 0
```

**Clave 1010. Vector inicialización 0.**

**Resultados:**

**Input (cipherCBC\_Ej5-Input.txt)**

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd cipherCBC_Ej5-Input.txt
00000000: 108f 4b50 85f5 cfed 5e7b 1250 88ef b1e2 ..KP....^.{P....
00000010: 2753 312a ea2f 2cd9 9158 964d 7379 6f07 'S1*./,...X.Msyo.
00000020: 593b 17de e41f 8b2c 1fc0 0ef1 eebc 0878 Y;.....,.....x
00000030: cc96 a352 03a0 f977 b92f 4c26 3510 025a ...R...w./L&5..Z
00000040: 4b4b 5225 4a74 8b50 3e71 be63 6cb5 95d9 KKR%Jt.P>q.cl...
00000050: ce3f 6957 4408 5973 0d29 45f7 5de2 61b1 .?iWD.Ys.)E.].a.
00000060: 4d87 f416 fe4d b7cf 1746 8ca1 53c0 fc0c M....M....F..S...
00000070: 5931 aa74 b9b6 fb33 ba0f 7afc cbb8 26e3 Y1.t...3..z...&.
00000080: 20bf 557d 8b21 76db 9512 5a08 558e ea2d ..U}.!v...Z.U..-
00000090: a8dd 8285 46ae 94a7 0e84 868f 0535 9609 ....F.....5..
000000a0: ac9e ead1 582a 2b45 ada5 c48a 6381 bf51 ....X*+E....c..Q
000000b0: aa4b b6b3 6693 bb42 ca11 eb97 5b27 d758 .K..f..B....['.X
000000c0: 90cc fc02 c539 1b32 2d31 0f93 df3d 7045 ....9.2-1...=pE
000000d0: a778 b10f d26f 22f3 77eb 9673 0b7e 46c3 .x...o".w..s..~F.
000000e0: 1d7e f5fc 1f91 d5f0 1243 7d7d 6634 b33a ..~.....C}]f4.:.
000000f0: a14f 8ece 82d6 ee30 1267 4d0a aea3 b78b .0.....0.gM.....
00000100: 7c38 a5f1 f9bc a496 dfe5 c03e d536 9ff5 18.....>.6..
00000110: 1f80 c24d 154a bc27 f23f c8f3 8dfe dfe5 ...M.J.'.?.....
00000120: 627d d5da a284 64e2 eb24 1fdc 5319 7914 b}....d..$.S.y.
00000130: bff3 982f 41a1 c698 8a4f 58ec 22c4 9e34 .../A....0X.."4
00000140: 3660 7eee fc42 9d48 f17c 2222 2dd1 8bf2 6`~..B.H.I""-...
00000150: d06c f610 04f9 816e d5f4 7788 7a32 649a .l.....n..w.z2d.
00000160: 6943 1b42 ae61 34fd efb9 c463 1103 4b42 iC.B.a4....c..KB
00000170: 3e03 07af 2111 31d6 f657 d65f 281b bfec >...!.1..W._C...
00000180: bf09 3ea2 2c87 95cb 5ddc 9ea7 e586 87c7 ..>.,...]......
00000190: 6b0d abff 8def cbda 17ac a66a 3686 2e28 k.....,....j6..C
000001a0: cf22 18fa 11d8 2e41 7472 6bac 4100 c250 .".....Atrk.A..P
```

Input1 (cipherCBC\_Ej5-Input1.txt)

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd cipherCBC_Ej5-Input1.txt
00000000: 49b7 1bdb 86de d930 21a0 619d 6e0f b746 I.....0!.a.n..F
00000010: 23be 35d2 318f b913 d169 7da3 0475 2135 #.5.1....i}...u!5
00000020: cb0f 8e2c 34d4 aff1 9d01 e0c8 ff3c a443 ...,4.....<.C
00000030: b456 1420 6043 17be 3e22 8808 fc28 12a8 .V. `C..>"...C..
00000040: e2ee 7504 8346 0179 c0f1 12a8 2c45 e492 ..u..F.y....,E..
00000050: 5cb3 7bb9 5107 4a34 1049 ac36 b77f caf0 \.{.Q.J4.I.6....
00000060: 471d ff9f 8055 56f8 5c82 3894 e9b3 b7c7 G....UV.\.8.....
00000070: 714c 2b5c b446 24e7 94c3 6201 2bcb 9f81 qL+\.F$...b.+...
00000080: c578 8724 0f20 a188 55ab 5ff7 8c53 5cb3 .x.$. ...U._..S\.
00000090: f61f b27a 6f6c 0e25 2e24 562a 2cf8 1519 ...zol%.$V*,...
000000a0: b114 6484 ff89 8330 9aad 3d0e 4d9e df83 ..d....0..=.M...
000000b0: 859c b62b 5bbf 7f50 4417 3c4e 21f3 b91a ...+[..PD.<N!...
000000c0: 770d e2be 9f42 687d 2ea5 8871 5258 b4e8 w....Bh}...qRX..
000000d0: d2b9 a5ef b5d7 2b80 5da6 8e89 a961 66ea .....+.]....af.
000000e0: a526 dc8a 634d cc52 6982 2cc6 86eb a1fc .&..cM.Ri.,.....
000000f0: 07ac 461c 8ccd bfa7 4d75 2076 0c1b 38e1 ..F.....Mu v..8.
00000100: d682 c1a7 2a38 f4a5 a831 cf93 d2ed 976e ....*8...1.....n
00000110: 400d 18d6 c78b 8b0f 0e9c 5175 1f1e 10ea @.....Qu.....
00000120: 2d4f 8ad4 80b4 c714 e311 ebe9 b094 feac -0.....,.....
00000130: e1a1 38ae 01da cb88 9d32 e0e9 6b0f 6d97 ..8.....2..k.m.
00000140: 8195 c215 bb76 9573 ae57 3e45 0147 cee9 .....v.s.W>E.G..
00000150: 3adf 091d 83ac a51a d9ac ddef 1c14 1ae8 :.....,.....
00000160: 1aa8 b2a6 29a6 b413 5f28 a9da 794f 1aa2 ....)....(..y0..
00000170: 212a 9a2c 87b5 a78c 81d7 01f2 bcfb 9492 !*.,.....
00000180: 6ab1 ab71 3920 facb 3d84 7083 b7b4 b61c j..q9 ..=p.....
00000190: de98 5407 f055 ec79 a306 5cc2 d9d2 662e ..T..U.y..\...f.
000001a0: 6b9b 0b58 5a3d 8854 76c9 d3e5 3262 c078 k..XZ=.Tv...2b.x
```

Podemos ver, cómo al usar una clave más aleatoria, ni débil ni semidébil, obtenemos un texto encriptado más robusto, en el que no se repiten bloques encriptados y no es posible diferenciar si todo el texto plano era igual (todos los mismos caracteres), ya que existen diferencias entre el código encriptado entre Input y Input1.

El cifrado CBC se vuelve mucho más seguro usando una clave, que no sea tan vulnerable.

## 6. Repetid los puntos 4 a 5 con AES-128 y AES-256.

A continuación, podemos ver las instrucciones que hemos usado en nuestro script para ejecutar los encriptados.

**AES 128**

Usamos la clave 1010 y el vector de inicialización 0.

### ECB

#AES 128

#ECB

```
openssl enc -aes-128-ecb -in input.bin -out cipherAES128ECB-Input.txt -K 1010
```

```
openssl enc -aes-128-ecb -in input1.bin -out cipherAES128ECB-Input1.txt -K 1010
```

Input.bin - CipherAES128ECB-Input.txt

```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd cipherAES128ECB-Input.txt
AES-128
00000000: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000010: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000020: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000030: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000040: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000050: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000060: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000070: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000080: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000090: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
000000a0: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
000000b0: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
000000c0: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
000000d0: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
000000e0: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
000000f0: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
00000100: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR....^$.....1
```

Input1.bin - CipherAES128ECB-Input1.txt

```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd cipherAES128ECB-Input1.txt
AES-128
00000000: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000010: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000020: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000030: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000040: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000050: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000060: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000070: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000080: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000090: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
000000a0: d7f9 70a0 7f6a 4bf7 18bc ff83 24f2 83b5 ..p..jk.....$...
000000b0: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
000000c0: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
000000d0: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
000000e0: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
000000f0: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
00000100: 748f 1096 8003 732c 5a00 4c51 5cea be8e t.....s,Z.LQ\...
```

Al igual que en los ejercicios anteriores, se repiten los bloques, excepto en el bloque 10, en el caso de la segunda imagen, donde estaba el 1, que es el bloque que cambia.

### CBC

#CBC

```
openssl enc -aes-128-cbc -in input.bin -out cipherAES128CBC-Input.txt -K 1010 -iv 0
```

```
openssl enc -aes-128-cbc -in input1.bin -out cipherAES128CBC-Input1.txt -K 1010 -iv 0
```

#### Input.bin (cipherAES128CBC-Input)

```
rata@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd cipherAES128CBC-Input.txt
00000000: 0754 52c4 83b1 b75e 24ea f12c e6fa d431 .TR...^$....1
00000010: 6287 0a12 6943 3ef6 c7c7 b5ad 5fb0 d5d7 b...ic>.....
00000020: b614 9a4b 419d 196c f9ad 52b3 7f77 e428 ...KA..l..R..w.(
00000030: dc3e 4a40 4f7f 57f7 8dce 7b6b 9daf cb84 .>J@O.W...{k....
00000040: 06a9 6df0 dfef 7179 a811 4a1f fee5 1276 ..m...qy..J....v
00000050: eac5 4e35 8fd8 7c19 7953 6ec8 b96a 0de8 ..N5..|.ySn..j..
00000060: efe6 12cb 991f 0092 c4ed e7ef 314a f8a4 .....1J..
00000070: 8c92 d92c 1810 84fd 70eb 3648 6fcf ba8d ....,....p.6Ho...
00000080: eb86 af35 24cb f404 6dbc b991 b1fb 7f23 ...5$...m.....#
00000090: 7ad7 ad60 da72 c312 cb41 016b 17b1 435c z...`r...A.k..C\
000000a0: d0c0 70d3 beb9 c2cb dcad b5c8 8d8f 7868 ..p.....xh
000000b0: e459 d1f6 32a5 362d f244 3dac a8ee 5bdb .Y..2.6-.D=...[.
000000c0: ef97 a8e5 2890 fe05 f004 5b36 2dc3 68dd ....([....[6-.h.
000000d0: 9a0a 4f95 ccc2 7be9 8f50 00e1 3959 a26d ..0...{..P..9Y.m
000000e0: 87df 6a3c 9d30 947b 2e13 eaea 0687 49b0 ..j<.0.{....I.
000000f0: 0a3c 54d2 fcb1 6f63 7c68 5320 ed45 975a .<T...oc|hS .E.Z
00000100: 5c0e caf4 6fc7 8bd7 3bc0 d373 cc75 354c \...o...;..s.u5L
```

#### Input1.bin (cipherAES128CBC-Input1)

```
rata@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd cipherAES128CBC-Input1.txt
00000000: 748f 1096 8003 732c 5a00 4c51 5cea be8e t....s,Z.LQ\...
00000010: c2f1 5eb5 d3c5 d598 266a ea72 a930 79a5 ..^.....&j.r.0y.
00000020: 3f2c d462 2eac 14c4 7d38 c4af a3d2 3391 ?,b....}8....3.
00000030: d89c 1faa a155 67e5 3f79 9f00 7d5b 945c ....Ug.?y..}{..
00000040: 8ef2 9cb4 81a0 15cc f4b9 33a8 f5a4 8997 .....3.....
00000050: ada5 3ab6 9dae 7078 6e34 3b23 6c19 bbba .....pxn4;#1...
00000060: 4c17 e95d f4e8 6c95 fae8 9470 f79e bb3c L..].1....p...<
00000070: cbf4 7d6c 896b 21b2 f69f f93d 7849 2397 ..}1.k!....=xI#.
00000080: 4f52 11d7 0eda f405 2468 bdef 4744 0053 OR.....$h..GD.S
00000090: c7ad 7cf0 0598 d061 d719 7298 d64b 1f45 ..|....a.r..K.E
000000a0: ba36 9d26 a606 a2f0 4542 b9ac ab23 215a .6.&....EB...#!Z
```

Vemos como en este caso, con la encriptación CBC, y una llave aleatoria (ni débil ni semidébil) no podemos diferenciar bloques, ni repeticiones en el texto en claro.

## AES 256

#AES 256

#ECB

```
openssl enc -aes-256-ecb -in input.bin -out cipherAES256ECB-Input.txt -K 1010
```

```
openssl enc -aes-256-ecb -in input1.bin -out cipherAES256ECB-Input1.txt -K 1010
```

#CBC

```
openssl enc -aes-256-cbc -in input.bin -out cipherAES256CBC-Input.txt -K 1010 -iv 0
```

```
openssl enc -aes-256-cbc -in input1.bin -out cipherAES256CBC-Input1.txt -K 1010 -iv 0
```

## AES256ECB

```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd cipherAES256ECB-Input.txt
00000000: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000010: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000020: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000030: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000040: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000050: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000060: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000070: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000080: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
00000090: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
000000a0: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
000000b0: 4210 d06c a54d f054 c523 c393 61ec 83e0 B..1.M.T.#..a...
```

## AES256ECB Input1.bin

```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd cipherAES256ECB-Input1.txt
00000000: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000010: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000020: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000030: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000040: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000050: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000060: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000070: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000080: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000090: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
000000a0: 75ab e650 c2ec ca09 430e 5dff 8390 0075 u..P....C.]....u
```

Al igual que antes, vemos en el bloque 10, la diferencia respecto a los demás bloques, del número 1, y los demás 0 en el texto plano que se cifró.

### AESCBC256 Input.bin

```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd cipherAES256CBC-Input.txt
00000000: 4219 d06c a54d f054 c523 c393 61ec 83e0 B..l.M.T.#..a...
00000010: 69e1 7c9f ae5f 4df8 b6c6 db97 2022 f6ef i.|.._M....."..
00000020: 57c3 9114 4104 dc0f 404a 1a59 79b1 9d2a W...A...@J.Yy...*
00000030: f7a8 efc0 3f78 690a 6086 aed0 8480 dea7 ....?xi.`.....
00000040: 452f 1362 8464 c244 4dae c83d e670 fac4 E/.b.d.DM..=p..
00000050: f44e fab6 5e9f a184 be21 cfd7 e4f4 bb6d .N..^....!....m
00000060: d119 0e0b eeee 7180 af7e c1b6 17cb 9470 .....q..~....p
00000070: d182 4df8 f96e f148 e085 3519 88cb 1ef9 ..M..n.H..5.....
00000080: 760a 624f 5963 d279 4a2a eeb3 d401 1dbc v.b0Yc.yJ*.....
00000090: 6538 7abd 1745 8635 d1dd 2c3a 0fd5 12da e8z..E.5.,:....
000000a0: 7635 2d8c c2f1 0246 f41b 4aab d6c1 db12 v5-....F..J.....
000000b0: 0b8a 6efb ab53 69cc 8d5a 92ca 3428 bbef ..n..Si..Z..4(...
000000c0: 43e6 b15e ba27 bd3d 6a56 cdf7 fa30 1006 C..^.'.=jV...0..
000000d0: 4580 3e88 b89b a8a1 ee6f da78 8880 a9ad E.>.....o.x.....
000000e0: c80b d414 9760 1b39 09dd 1492 c2a4 d645 .....9.....E
000000f0: 30cf 3ced 0860 ce43 c1ee edb9 af6b f3d8 0.<...C.....k..
00000100: 1da3 a7e2 50da 1c37 6c8b f212 544f b37d ....P..71...T0.}
```

### AESCBC256 Input1.bin

```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd cipherAES256CBC-Input1.txt
00000000: 2993 1923 c16c 23a1 5abe f8bf 2f9b 5551 )..#.1#.Z.../.UQ
00000010: c7af 0c13 b2c8 dd9f 586f 2b8d b51a c8b0 .....Xo+.....
00000020: 2d6e 55d1 a9ef 98e3 da92 bf3c cdc6 4b2f -nU.....<..K/
00000030: f5ea c85d 27cd eba4 ea52 a434 ced2 6a20 ...]'....R.4..j
00000040: a840 c813 f75a 9074 85b0 fcd2 c406 7eb5 @...Z.t.....~.
00000050: 3a93 e840 2e84 fdd9 e165 bd5f a239 8ad4 :..@.....e._9..
00000060: a4fd 5702 1b9d 97ff d56b 493d 80ca c86a ..W.....kI=...j
00000070: 319c 4400 0765 2d1c fbcd 6e9d 68dd 288b 1.D..e-...n.h.(.
00000080: 23bd 32d8 d5b9 5664 fb4e 2b7f b004 efe0 #.2...Vd.N+.....
00000090: c483 069d d011 4105 5b29 0f28 cad8 f991 .....A.[).(....
000000a0: 3076 3e85 d8f3 ff7e 17e2 62af 291b 6925 0v>....~..b.).i%
000000b0: 3a66 d631 c0e0 f506 d5b1 8ad8 1461 6eeb :f.1.....an.
000000c0: 006b ea94 720b acbf a951 ebff 8e75 2438 .k..r....Q..u$8
000000d0: 5be0 ecde 1b1f 4358 8a9a 8b6a 3f92 5d10 [.....CX...j?..].
000000e0: 6fa5 d5e2 0c97 b491 a9f5 60b3 9deb d644 o.....`....D
000000f0: 986f 64e9 e105 8b91 b7e0 8015 40f9 b778 .od.....@..x
00000100: febe 15b7 c15c c4e8 bc15 cbd2 8756 cd8a .....\\.....V..
```

Igual que antes, no se pueden diferenciar los bloques, ni se aprecian similitudes.

### 7. Cifrad input.bin con AES-192 en modo OFB , clave

y vector de inicializacion a elegir. Supongamos que la salida es output.bin .

```
openssl enc -aes-192-ofb -in input.bin -out output.bin -K 1010 -iv 0
```

### Output.bin

```
00000000: 93a3 5f8f ddbf f078 1f3d 705b 1c97 17e1 .._.x.=p[....
```

```

00000010: 7eb2 44b8 2e88 7dfc fa8f 1114 8f24 c0ca ~.D...}.....$..
00000020: 525d 3d4a 513e a788 acc1 b6c2 26cb 2edb R]=JQ>.....&...
00000030: c2a8 d169 f0d4 d4f7 24af cb71 22bb 769b ...i....$..q".v.
00000040: 4f3c 1ab5 eb4b 1962 8e31 126c 6b9e 758f 0<...K.b.1.lk.u.
00000050: 5fc3 7b28 3cd0 7248 7131 cdd2 26d6 a1a3 _.{(<.rHq1..&...
00000060: 95cc 188a 0e86 d881 6b14 5874 b491 edfd .....k.Xt....
00000070: e6d8 922e f083 0299 0c4b 4f34 2a05 cb1c .....K04*...
00000080: ee1a 040b 3b56 c18f 2d18 49ac 9718 ee4e ....;V...-I...N
00000090: fd3b 5406 1125 b725 83e3 e5c8 238f cf28 .;T.%.%....#..(
000000a0: 5c02 ec62 196c 0f4b 89de ea33 9d03 ba23 \..b.1.K...3...#
000000b0: e294 e4a8 3ec4 859b 7b56 17c4 fa76 ae90 ....>...{V...v..
000000c0: 8060 2449 2fb9 acef a6f2 b015 9bf1 6c01 .`$I/.....1.
000000d0: 146a a0aa 1eba 8c76 e4d4 c77e df54 aae8 .j.....v...~.T..
000000e0: a0b1 c4c5 77c4 5f1d d3ff 91c5 3091 5dde ....w._.....0.].
000000f0: 52a2 d487 e971 43eb 68c1 7aa4 c1a8 cbb9 R....qC.h.z.....
00000100: d7d5 650b 5a50 e9a3 565e 6db1 714c 52d5 ..e.ZP..V^m.qLR.
00000110: af35 f5ef d5de 402b 48fd 0159 e4ca 74d3 .5....@+H..Y..t.
00000120: 46c8 b00f 1e8f 5ddf 7f64 a86f dad8 403b F.....]..d.o..@;
00000130: 4fc8 dff0 467a 30ae f06f ff97 93c8 afec 0...Fz0..o.....
00000140: 106b eff3 f832 d861 bdbc cbeb 8906 1f36 .k...2.a.....6
00000150: f320 9f0e 8856 3d89 6f6b 4a6a bb55 85f5 . . .V=.okJj.U..
..... (mostramos solo las primeras líneas)

```

**Input.bin**

```

00000000: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000010: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000020: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000030: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000040: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000050: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000060: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000070: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000080: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000090: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000a0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000b0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000c0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000d0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000e0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000f0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000100: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000110: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000120: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000130: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000140: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000150: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11

```

**8. Descifra output.bin utilizando la misma clave y vector de inicialización que en 7.**

```
openssl aes-192-ofb -d -in output.bin -out descifrado8.txt -K 1010 -iv 0
```

### Descifrado8.txt

```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd descifrado8.txt
00000000: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .inicializacion}.R11
00000010: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000020: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000030: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000040: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000050: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000060: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000070: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000080: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000090: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000a0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000b0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000c0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000d0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000e0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000f0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000100: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000110: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000120: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000130: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000140: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000150: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
```

Vemos que el descifrado es correcto, y coincide con input.bin

### 9. Vuelve a cifrar output.bin con AES-192 en modo OFB , clave y vector de inicialización del punto 7. Compara el resultado obtenido con el punto 8, explicando el resultado

```
openssl enc -aes-192-ofb -in output.bin -out output2.bin -K 1010 -iv 0
```

#### Output.bin

```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd output.bin
00000000: 93a3 5f8f ddbf f078 1f3d 705b 1c97 17e1 .._.x=p[....
00000010: 7eb2 44b8 2e88 7dfc fa8f 1114 8f24 c0ca ~.D...}.....$..
00000020: 525d 3d4a 513e a788 acc1 b6c2 26cb 2edb R]=JQ>.....&...
00000030: c2a8 d169 f0d4 d4f7 24af cb71 22b 769b ..i....$.q".v.
00000040: c4f3c 1ab5 eb4b 1962 8e31 126c 6b9e 758f 0<...K.b.1.lk.u.
00000050: 5fc3 7b28 3cd0 7248 7131 cdd2 26d6 a1a3 ..{(<.rHq1.&...
00000060: 95cc 188a 0e86 d881 6b14 5874 b491 edfd .....k.Xt....
00000070: e6d8 922e f083 0299 0c4b 4f34 2a05 cb1c .....K04*...
00000080: ee1a 040b 3b56 c18f 2d18 49ac 9718 e4e .....;V...I...N
00000090: fd3b 5406 1125 b725 83e3 e5c8 238f cf28 ..T..%.%....#...(.
000000a0: 5c02 ec62 196c 0f4b 89de ea33 9d03 ba23 \..b.l.K..3..#.
000000b0: e294 e4a8 3ec4 859b 7b56 17c4 fa76 ae90 .....>...{V...v...
000000c0: 8060 2449 2fdb acf a6f2 b015 9bf1 6c01 ..`SI/.....1.
000000d0: 146a a0aa 1eba 8c76 e4d4 c77e df54 aae8 j.....v....~.T..
000000e0: a0b1 c4c5 77c4 5f1d d3ff 91c5 3091 5dde .....w.....0].
000000f0: 52a2 d487 e971 43eb 68c1 7aa4 c1a8 cbb9 R....qC.h.z.....
00000100: d7d5 650b 5a50 e9a3 565e 6db1 714c 52d5 ..e.ZP..V^m.qLR.
00000110: af35 f5ef d5de 402b 48fd 0159 e4ca 74d3 5.....@+H..Y..t.
00000120: 46c8 b00f 1e8f 5ddf 7f64 a86f dad8 403b F.....]..d.o..@;
00000130: 4fc8 dff0 467a 30ae f06f ff97 93c8 afec 0...Fz0..o.....
00000140: 106b eff3 f832 d861 bd8c cbeb 8906 1f36 .k...2.a.....6
00000150: f320 9f0e 8856 3d89 6f6b 4a6a bb55 85f5 ..V=.okJj.U..
```

#### Output2.bin

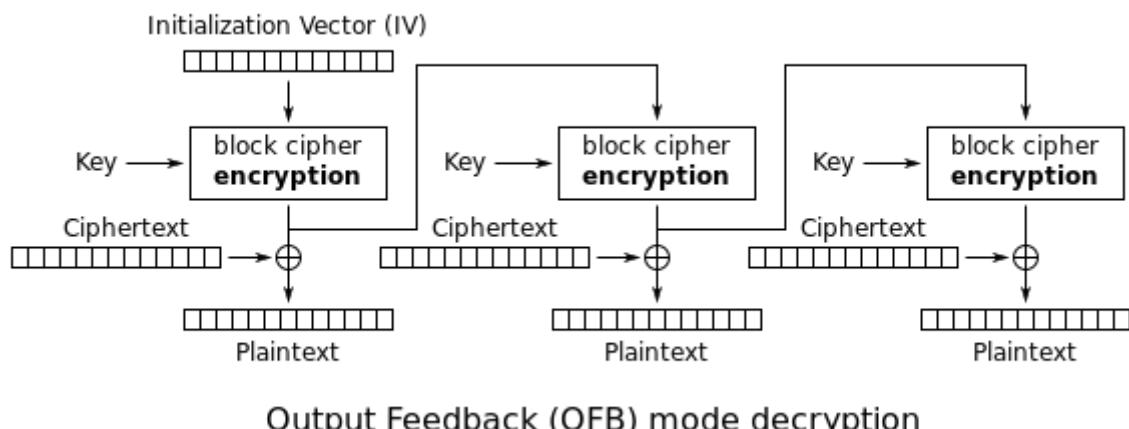
```
rafa@system32:~/Documentos/SPSI/SPSI/2017/p1$ xxd output2.bin
00000000: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000010: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000020: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000030: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000040: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000050: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000060: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000070: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000080: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000090: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000a0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000b0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000c0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000d0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000e0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
000000f0: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000100: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000110: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000120: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000130: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000140: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
00000150: 0000 0000 fe7f 0000 00b0 ab7d 9b52 316c .....}.R11
```

Vemos que volvemos al texto plano.

Esto se debe porque OFB utiliza una operación XOR con la llave y el bloque cifrado, si vemos en cualquier calculadora, al hacer una operación XOR de la siguiente forma:

texto XOR llave = cifrado

Cifrado XOR llave = texto



10. Presentad la descripción de otro cifrado simétrico que aparezca en vuestra implementación de OpenSSL.

## Cifrado RC2

Este algoritmo pertenece a la categoria de cifradores de bloque que emplean una funcion de feistel, el metodo siguiendo el mismo que en los demas algoritmos, la division en bloques, la aplicacion de s-cajas y la funcion XOR.

La diferencia de este algoritmo con los otros es que aunque usa una clave con bloque de 64 bits, realmente la longitud de la clave puede ser variable, es decir no obliga a que sean exactamente claves de 64 bits, lo cual dificulta su decodificacion, aunque cabe mencionar que este algoritmo ya no es empleado debido a que ya ha sido vulnerado y fue revelado en internet de forma anonima.

**11. Repetid los puntos 3 a 5 con el cifrado presentado en el punto 10 (el 3 si el cifrado elegido tuviese claves débiles o semidébiles).**

### #11.3

#Clave débiles

#ECB

```
openssl enc -rc2-ecb -in input.bin -out rc2-ECB.txt -K 0101010101010101
```

#CBC

```
Openssl enc -rc2-cbc -in input.bin -out rc2-CBC.txt -K 0101010101010101 -iv 0123
```

#OFB

```
openssl enc -rc2-ofb -in input.bin -out rc2-OFB.txt -K 0101010101010101 -iv 0123
```

-----

#Claves semidébiles

#ECB

```
openssl enc -rc2-ecb -in input.bin -out rc2-ECBv2.txt -K 01FE01FE01FE01FE
```

#CBC

```
Openssl enc -rc2-cbc -in input.bin -out rc2-CBCv2.txt -K 01FE01FE01FE01FE -iv 0123
```

#OFB

```
openssl enc -rc2-ofb -in input.bin -out rc2-OFBv2.txt -K 01FE01FE01FE01FE -iv 0123
```

-----

#11.4

```
openssl enc -rc2-ecb -in input.bin -out rc2-ECB-input.txt -K ABCD
```

```
openssl enc -rc2-ecb -in input1.bin -out rc2-ECB-input1.txt -K ABCD
```

-----  
#11.5

```
openssl enc -rc2-ecb -in input.bin -out rc2-CBC-input.txt -K ABCD -iv 0123
```

```
openssl enc -rc2-ecb -in input1.bin -out rc2-CBC-input1.txt -K ABCD -iv 0123
```

## 11.3

### Claves débiles

#### ECB

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-ECB.txt
00000000: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000010: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000020: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000030: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000040: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000050: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000060: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000070: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000080: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000090: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
000000a0: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
000000b0: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
000000c0: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
000000d0: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
000000e0: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
000000f0: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000100: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000110: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000120: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000130: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000140: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000150: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000160: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000170: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000180: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
00000190: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
000001a0: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
000001b0: d715 21a5 10bc 989b 13e4 3233 c44d 7b3a ..!.....23.M{:;
```

#### CBC

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-CBC.txt
00000000: 28ad 51e3 2ea7 b04d fa44 4085 057f c3f4 C.Q....M.D@.....
00000010: c84e 3461 6ad5 31bf b143 972a c36e f1ea .N4aj.1..C.*.n..
00000020: 8c00 3bca f81b 0c90 2e10 3804 039b 51ec ..;.....8...Q.
00000030: 0e26 bc5e baee d6ac 9e10 225b 162f 4b42 .&.^. ...."[/KB
00000040: 8817 ff76 aab7 d72d d3c8 4fe8 8b69 1214 ...v.....0..i..
00000050: 200d de9e 3599 8864 c77c f919 fc52 25fc ...5..d.l...R%.
00000060: 3bef f114 a14d c874 5548 22b3 3d0e fc21 ;....M.tUH"=..!
00000070: 38b9 2dfb 9845 7b15 18c3 b9f2 2a3e 8aba 8...E{.....*>..
00000080: c545 e716 39dd 5ccf a590 a5a9 07e2 b821 .E..9.\.....!
00000090: 8258 e3d5 0c98 148b e2b2 732b 6831 7cb7 .X.....s+h1I.
000000a0: cbd7 32cf 12d0 06f2 e919 72fa 8fdc 3080 ..2.....r...0.
000000b0: 9abc 8135 80ff 6392 37a5 caca cede 94ed ...5..c.7.....
000000c0: d729 e914 02a1 7690 67a0 2d97 99ab f99b .)....v.g.-....
000000d0: 1e29 b233 e369 95b8 5e53 79ec bb66 0d48 .).3.i..^Sy..f.H
000000e0: a947 1a4e 5677 789c 1afc eb86 f633 aa71 .G.NVwx.....3.q
000000f0: 8d3c 2cde c377 b31e 1108 a43a 4f44 8707 .<..w.....:OD..
00000100: f3b2 bce9 25f7 0961 26f3 d0ff f761 0f4b ...%.a&....a.K
00000110: 99bc aa20 d549 9e97 ad93 335d 4757 d85f ... .I....3]GW_.
00000120: 0786 438b 624e dc4d 1cad c004 d2f8 d317 ..C.bN.M.....
00000130: 1830 2ffc ac33 414a bf91 0a5a d2af 6bfa .0/..3AJ...Z..k.
00000140: 9ca6 eee1 4e49 b8cf 1c2a 7375 84bd 0a47 ...NI...*su...G
00000150: a765 49f7 f1a0 a534 c43d decd 2a61 8d46 .eI....4.=..*a.F
00000160: 7d57 f9ee e3d8 d0c5 0fa2 c5ba bb8a e969 }W.....i
00000170: 1ab0 222b 9642 516e f214 dc77 141f dfb4 .."+.BQn...w....
00000180: 1e99 68fe 54cf d7a8 e148 8297 7885 4ad3 ..h.T....H..x.J.
00000190: 81b6 d6b8 9fff db42 66f0 9c70 d27d ebae .....Bf..p.}..
000001a0: 48af 1d27 58d4 64b5 4f7c 1e30 5fa1 be55 H.. 'X.d.01.0..U
```

## OFB

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-OFB.txt
00000000: 7a58 8b0c 4ee6 ccaa 2d95 c4bf 9190 5d1a zX..N.....].
00000010: 0de7 46ac 3184 3428 4809 cae7 7d6a f500 ..F.1.4(H...}j..
00000020: db2f 165a 41f5 90b6 fe8f b177 3006 5dce ./ZA.....w0].
00000030: 87be e22e d3df 037a 6004 b602 3483 6507 .....z`...4.e.
00000040: aa7d 7347 02ef b27c 1f8c 3da4 e93e 4723 .}sG...l..=>G#
00000050: bbcd 088f 30df ae3c 49f4 ac01 522d 6cb1 ...0..<I...R-1.
00000060: aad0 0daf e3a8 d14b 29b4 36e2 a213 2df7 .....K).6.....
00000070: c2b5 fced 01dc 255c 7c5a 79d7 18a9 5e2b .....%\\|Zy...^+
00000080: ea6e e45f 5fac 959e 921b 7de5 366c e02b .n.....}.61.+
00000090: 3ba6 6422 d4a2 920c 5a88 9504 b0bf be67 ;.d"....Z.....g
000000a0: 3d11 f4af eea9 b85e 1242 46e2 1a4f 0e1f =.....^BF..O..
000000b0: bcfe eaf6 4809 3bb6 15cb 6451 6001 847f ...H.;...dQ`...
000000c0: b9b8 21bc 6d50 5841 c471 6b30 4dc4 ccbe ..!.mPXA.qk0M...
000000d0: 5989 b422 6bb0 7d18 6661 0f47 e3ac 1d87 Y.. "k.}.fa.G...
000000e0: f871 ae54 46c2 e474 7cd5 9ee7 0ece adeb .q.TF..t|.....
000000f0: db53 7093 8b02 b6a3 bea8 4d38 9595 3999 .Sp.....M8..9.
00000100: 10b3 0607 8f5e 3258 d340 f129 eb2d 2b70 .....^2X.@.)--+p
00000110: a9cc 2097 4f8a b440 b4e5 76be 3db5 2f13 .. .0..@..v.=./
00000120: a926 0c0e 0060 0fdf 390a 86e6 f2cd b849 .&...`..9.....I
00000130: 8577 2643 a9e0 5f97 e9cf 78c3 83e3 a340 .w&C.....x...@
00000140: 573a bf06 4d69 186e d8e8 0fe1 bf1a 81a3 W:..Mi.n.....
00000150: a147 98e1 c55f 3a0b f88c fa04 fe07 6afb .G....:.....j.
00000160: 1126 4a6b 9c0f 1d54 733e 1125 e705 f550 .&Jk...Ts>.%...P
00000170: 5589 fce4 cb72 3641 2468 53c8 3918 d02f U....r6A$hS.9.../
00000180: 2cac c72a ae9f f780 b994 26c2 2688 413e ,...*.....&.&A>
00000190: 3b66 58f2 31f1 0c8e 6383 ae28 5d59 090f ;fx.1...c..(]Y..
000001a0: 7c28 3d9e 4ceb 2e0d 3cff 38ef a482 f442 lC=L...<.8....B
000001b0: a9df 4593 f439 c7c0 e324 b71d 2336 45d8 ..E..9...$.#6E.
000001c0: be2e 1b13 adf5 7816 606b e3c7 467d d82f .....x.`k..F}./
000001d0: 45bb 74cc 6512 b989 a5af 86c1 7572 0086 E.t.e.....ur..
000001e0: 8f82 de33 0fb8 540e 1951 db68 78fa f72e ...3..T..Q.hx...
000001f0: 58c4 5170 0880 fa83 aa8a b0e6 5fb5 d66e X.Qp.....n
00000200: 1fe2 74a2 3bc3 c518 c503 1716 476a eb56 ..t.;.....Gj.V
```

## Claves semidébiles

**ECB**

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-ECBv2.txt
00000000: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000010: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000020: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000030: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000040: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000050: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000060: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000070: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000080: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000090: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000000a0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000000b0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000000c0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000000d0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000000e0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000000f0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000100: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000110: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000120: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000130: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000140: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000150: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000160: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000170: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000180: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000190: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000001a0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000001b0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000001c0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000001d0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000001e0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
000001f0: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
00000200: a849 9956 ceb5 78b7 a25d 83ab 17b1 499a .I.V..x..]....I.
```

**CBC**

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-CBCv2.txt
00000000: 5dd2 2ea2 e03e ee08 645a 745d 3001 2abd ]....>..dZt]0.*.
00000010: 2f7b 23a7 af7e fac2 baae f619 2c62 12e1 /{#..~.....,b..
00000020: c971 8c94 e6ae f628 4406 5512 1edd efb3 .q.....(D.U.....
00000030: 8c6b 5fe3 ef91 841d 6105 870d af78 9592 .k.....a....x..
00000040: e1bb 54be e08c 6425 a401 0e39 cacf 5f70 ..T...d%...9...p
00000050: b879 ca86 9fb6 74c3 bef8 f524 8d7f 9a81 .y....t....$....
00000060: 7a62 df6f b318 4eff ff7d ba80 b821 0ae0 zb.o..N..}....!
00000070: 2f4e 2f89 ff05 91e6 487b 2b0c 89f3 5e03 /N/....H{+....^.
00000080: ec43 6e3b 0fd4 45a8 f313 d59d ccca 9e95 .Cn;..E.....
00000090: d44c 0f6a 8721 afc4 440e 0685 96dd 5dae .L.j.!..D....].
000000a0: 4bae 4385 5d81 4e5c fb90 d4ae c6c0 9f66 K.C.]..N\.....f
000000b0: fd15 4555 aae0 728c 5f12 56c3 bcb7 d5e1 ..EU..r..._v...
000000c0: 8346 e652 f222 9e89 da50 e6a8 a4a9 f697 .F.R."...P.....
000000d0: f26d edec 64f0 a32d ad0b 5b29 7676 1693 .m..d....Dvv..
000000e0: abef 1c4d 0dc6 fd4e c852 37a0 a5b3 2181 ...M...N.R7...!.
000000f0: 7d5c 7d47 4a4e 4c9f c923 6d48 8002 8b1f }\\}GJNL..#mH...
00000100: c9b6 65e5 5790 4aca 2799 0985 72c1 4acf ..e.W.J.'...r.J.
00000110: 0b6d e8d7 c00a 92bf 0a26 e0b3 dd89 81d8 ..m.....&.....
00000120: 9c60 6fdf f973 8dfa bd4e cf69 824c 471c .`o..s...N.i.LG.
00000130: 8348 9a17 2647 abc5 7629 d855 ee44 1928 .H..&G..v).U.D.(
00000140: 94de 6d66 8e7b 0830 8a83 c452 7b87 21b5 ..mf.{.0...R{!.!
00000150: 465e b829 30ad ae20 2664 a1f4 690e 1c4e F^..)0.. &d..i..N
00000160: 21c1 ddd2 98de cfbff dd73 b36d a2f3 2e83 !.....s.m...
00000170: 6144 1ef0 317e 1d4a bb9b 6d65 a7ac 864e aD..1~.J..me..N
00000180: 3929 7600 f6b6 296d 85dc 20b2 307f 2246 9)v...).m... .0.."F
00000190: 4296 e69c 5af0 31cb 99be 73ea 0578 e3d7 B...Z.1...s..x..
000001a0: a849 d642 7a64 da1f affb 8050 acc4 1a92 .I.Bzd.....P...
000001b0: 0331 8e53 4962 92b2 d92f 0509 0158 5795 .1.SIb.../.XW.
000001c0: f438 f9ae ee7d 1a52 52ff 6441 c561 dbda .8...}.RR.dA.a..
000001d0: 0049 74bb a7df 4085 57ae a639 d2b5 23dc .It...@.W..9..#.
000001e0: acd0 13ba b189 a732 a9a2 6187 a84e 0721 .....2..a..N.!
000001f0: 9d0b a58f b96a d056 b7b6 f049 ac27 b901 .....j.V...I.'..
00000200: dc11 f765 6c9c 8e64 6c0afaf5 945d 62e7 ...el..dl...].b.
```

**OFB**

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-OFBv2.txt
00000000: 1732 b483 9da1 22fc bdaa 0b69 8da5 93e2 .2...."....i....
00000010: a763 3e8d 4295 f177 a2f3 0d75 57c9 90d9 .c>.B..w...uW...
00000020: 8c8e 4574 6949 82e5 fa6e c3b3 fdbe 9469 ..EtiI...n.....i
00000030: 5271 2593 8b4f cbce 3155 d38c 78da b06d Rq%..O..1U..x..m
00000040: b7fe be5c bc9d dff3 710f 1daf 41ab f195 ...\\....q...A...
00000050: 1144 a793 9d96 8a4e d026 70c9 e794 9837 .D.....N.&p....7
00000060: f818 d790 fff8 b767 ea99 168f e735 27dc .....g.....5'.
00000070: 25cc fa8c 238d 6053 ba74 0f8f f77a 1aa5 %...#.`S.t...z..
00000080: ef1c 9fb3 3a5e b290 420b ee87 d96b 356e ....:^..B....k5n
00000090: 10c0 3c3d fc3a acb4 91b9 4cc8 d57b ee01 ..<.=...L..{..
000000a0: 05f5 caa0 da0a bbf8 672f 35d0 cc4a b9c5 .....g/5..J..
000000b0: b4dc 0ce7 4e99 32c8 ad08 7188 2b5c d220 ....N.2...q.+\
000000c0: 3d4e 721c 264f dc40 2de3 bcf7 fcb4 1eab -Nr.&0.@-.....
000000d0: 1615 360a 5be4 c4d2 2c1c 4da4 b90d fc1f ..6.[...,M....
000000e0: 6bc5 a8f3 af17 017c 7477 97d2 06ab b990 k.....ltw.....
000000f0: 3ba3 d316 1ef2 258a b8cc 758d d564 b7f4 ;.....%...u..d..
00000100: 8070 ffc3 58fe 2768 b3ef 8d69 fe4f f916 .p..X.'h...i.O..
00000110: 7574 8746 2ff2 20d3 aee0 a273 4d89 949d ut.F/. ....sM...
00000120: f9f5 d3f3 b4ca f3a3dbe5 9fea b376 d6ed .....v...
00000130: 087f a24d 008d b153 84d3 7c69 2b1e 80d6 ...M...S..|i+...
00000140: 88d1 9785 a7e8 e4bc d14b e0fe 7e85 c6dc .....K..~...
00000150: 465c 6629 b033 b68e 266a 2897 2bc2 a17b F\f).3..&j(.+..{
00000160: 5719 64b9 a0db 1822 36dd d3bd bcae 8901 W.d...."6.....
00000170: f785 916e e80b 98dc 1dae 10d6 ef34 09cf ...n.....4..
00000180: a685 c13d 79a2 a11c b2df 6f0f 3059 a7ee ...=y.....o.0Y..
00000190: f0db 9ee7 8f02 bc6d e4d0 de30 c80a 2193 .....m...0..!.
000001a0: ea32 76b4 6be3 0958 6497 ad4c 2eba 5a20 .2v.k..Xd..L..Z
000001b0: 7b91 8d09 f267 f28c 63f5 9b96 3bb6 5af0 {....g..c...;..Z.
000001c0: a5d2 65b0 7181 1187 1d85 1a2f c4ef a568 ..e.q...../...h
000001d0: dfa9 4946 6fb1 dc0a 5a24 5258 a4ec 5f94 ..IFo...Z$RX..._
000001e0: da04 b6f8 ebe0 3e83 87f5 9e07 f844 7ebb .....>.....D~.
000001f0: 78e2 7a9e fd86 8f96 66e6 78cd 8cf2 44fd x.z.....f.x...D.
00000200: 00e7 5a9b c4e0 fd8c ac45 afa2 b336 7387 ..Z.....E...6s.
```

## ECB Input

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-ECB-input.txt
00000000: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000010: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000020: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000030: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000040: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000050: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000060: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000070: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000080: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000090: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000a0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000b0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000c0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000d0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000e0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000f0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000100: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000110: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000120: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000130: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000140: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000150: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000160: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000170: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000180: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000190: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001a0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001b0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001c0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001d0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001e0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001f0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000200: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
```

## ECB Input 1

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-ECB-input1.txt
00000000: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000010: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000020: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000030: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000040: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000050: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000060: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000070: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000080: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000090: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000a0: 73b5 109a 3596 b015 6e48 8034 7395 05d3 s...5..nH.4s...
000000b0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000c0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000d0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000e0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000f0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000100: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000110: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000120: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000130: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000140: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000150: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000160: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000170: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000180: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000190: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001a0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001b0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001c0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001d0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001e0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001f0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000200: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
```

Aquí vemos como cambia en el bloque 10 el cifrado, donde está el número 1.

## CBC Input

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-CBC-input.txt
00000000: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000010: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000020: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000030: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000040: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000050: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000060: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000070: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000080: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000090: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000a0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000b0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000c0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000d0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000e0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000000f0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000100: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000110: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000120: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000130: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000140: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000150: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000160: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000170: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000180: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000190: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001a0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001b0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001c0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001d0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001e0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
000001f0: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
00000200: f634 2c8c e004 1bef 6281 4461 0886 f14a .4,.....b.Da...J
```

## CBC Input 1

```
[MacBook-Pro-de-Rafael:p1 rafa$ xxd rc2-CBC-input1.txt
00000000: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000010: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000020: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000030: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000040: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000050: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000060: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000070: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000080: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000090: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000a0: 73b5 109a 3596 b015 6e48 8034 7395 05d3 s...5..nH.4s...
000000b0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000c0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000d0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000e0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000000f0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000100: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000110: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000120: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000130: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000140: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000150: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000160: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000170: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000180: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000190: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001a0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001b0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001c0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001d0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001e0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
000001f0: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
00000200: 7895 07d9 90ef edf6 f872 36ab 0a55 20c8 x.....r6..U .
```

Igual que antes, todos los bloques cifrados son iguales, excepto el 10 que es donde está el 1.