SEGURIDAD Y PROTECCIÓN DE SISTEMAS INFORMÁTICOS

Grado en Ingeniería Informática

Universidad de Granada

Practica 1 Criptosistemas Simétricos

29 de octubre de 2018

Índice

En este documento se explica la primera practica de la asignatura, que trata de aprender a utilizar la herramienta OpenSSL, y para completarla es necesrio entregar los 11 puntos de la misma, hay que entregar este pdf con los comandos y las capturas de pantalla necesarias para demostrar que se ha realizado la practica.

This document explains the first practice of the subject, which tries to learn how to use the OpenSSL tool, and to complete it, it is necessary to deliver the 11 points of the same, this pdf must be delivered with the commands and screenshots necessary to demonstrate that the practice has been carried out.

Tareas a realizar

1. Partiremos de un archivo binario de 1024 bits, todos ellos con valor 0. dicho fichero se llama imput.bin

Para realizar esta tarea ejecutaremos en la consola el siguientes comando:

```
[usuario@portatil ~/] dd if=/dev/zero of=/tmp/imput.bin bs=1024 count=1
1+0 registros leídos
1+0 registros escritos
1024 bytes (1,0 kB, 1,0 KiB) copied, 0,000323338 s, 3,2 MB/s
```

2. Creamos otro archivo binario del mismo tamaño, que contenga un único bit con valor 1 dentro de los primeros 40 bits y todos los demás con valor 0. Se llamará input1.bin

Para nuestro ejemplo la posición del UNO esta en el byte 136 Para realizar esta tarea ejecutaremos en la consola el siguientes comando:

```
[usuario@portatil:~]$ dd if=/dev/zero count=1 bs=135 >> /tmp/imput1.bin
1+0 registros leídos
1+0 registros escritos
45 bytes copied, 2,0989e-05 s, 2,1 MB/s
[usuario@portatil:~]$
1+0 registros leídos
1+0 registros escritos
1 byte copied, 0,000106516 s, 9,4 kB/s
[usuario@portatil:~]$ dd if=/dev/zero count=1 bs=888 >> /tmp/imput1.bin
1+0 registros leídos
1+0 registros escritos
978 bytes copied, 2,371e-05 s, 41,2 MB/s
[usuario@portatil:~]$ ll /tmp
-rw-rw-r--   1 usuario usuario 1,0K sep 29 18:59 imput1.bin
-rw-rw-r--   1 usuario usuario 1,0K sep 29 18:25 imput.bin
[usuario@portatil:~]$ hexdump -C /tmp/imput.bin
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000400
[usuario@portatil:~]$ hexdump -C /tmp/imput1.bin
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000080  00 00 00 00 00 00 00 01  00 00 00 00 00 00 00 00  |................|
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000400
```

3. Cifrar input.bin con AES-256 en modos ECB, CBC y OFB usando una clave, , y con vector de inicialización 0123456789abcdef, cuando sea necesario. Explicar los diferentes resultados.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

3.1. Modo ECB

```
[usuario@portatil:~]$ openssl enc --aes-256-ecb -K e0e0e0e0f1f1f1f1 -in /tmp/imput.bin -
    out /tmp/imput_aes256_ecb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes256_ecb.enc
```

```
00000000  01 8f 3c a3 90 c9 bc f9  d7 17 7c bd 4c 3d 19 f9  |..<.......|.L=..|
*
00000400  0b 1f eb 61 6b 41 78 41  37 e6 5b 68 f5 0a 60 c7  |...akAxA7.[h..`.|
00000410
[usuario@portatil:~]$ openssl enc --aes-256-ecb -K e0e0e0e0f1f1f1f1 -in /tmp/imput1.bin -
    out /tmp/imput1_aes256_ecb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes256_ecb.enc
00000000  01 8f 3c a3 90 c9 bc f9  d7 17 7c bd 4c 3d 19 f9  |..<.......|.L=..|
*
00000080  79 51 4b 8f fc 21 b5 67  ee e6 09 4a 03 38 2b 59  |yQK..!.g...J.8+Y|
00000090  01 8f 3c a3 90 c9 bc f9  d7 17 7c bd 4c 3d 19 f9  |..<.......|.L=..|
*
00000400  0b 1f eb 61 6b 41 78 41  37 e6 5b 68 f5 0a 60 c7  |...akAxA7.[h..`.|
00000410
```

Como se puede apreciar, el cifrado de imput.bin con clave, es un cifrado simple el cual modifica el fichero de entrada en todas sus lineas, en el segundo fichero imput1.bin, se puede apreciar que en cuanto cambia un solo bit del fichero cambia solamente esa linea de cifrado manteniendo las demas lineas intactas igual que en el fichero anterior.

3.2. Modo CBC

```
[usuario@portatil:~]$ openssl enc -aes-256-cbc -K e0e0e0e0f1f1f1f1 -iv 0123456789abcdef -
    in /tmp/imput.bin -out /tmp/imput_aes256_cbc.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes256_cbc.enc
00000000  51 0d 5e 09 5e 07 83 64  e7 01 0c db 66 b2 b2 e7  |Q.^.^..d....f...|
00000010  31 83 f6 13 9d 9a 8d 37  3c 07 fb 37 7c f0 a0 75  |1......7<..7|..u|
00000020  9d db 94 15 4b 49 86 4c  8b 2f 47 ee 7b 83 03 72  |....KI.L./G.{..r|
00000030  d7 2a 28 48 e6 ed ed 92  f2 aa 81 71 c1 ae 60 fe  |.*(H.......q..`.|
00000040  43 35 4d 85 8b 40 5d 1c  9f 8f d1 86 4d 27 5a 8c  |C5M..@].....M'Z.|
00000050  67 0a 5d 63 4a 68 b7 d5  a0 17 2c 27 9a d1 4e 5d  |g.]cJh....,'..N]|
00000060  f1 4d 84 3d 15 69 15 61  f5 90 42 bd 84 6b 54 77  |.M.=.i.a..B..kTw|
00000070  46 3e f8 3e 5f 1d 68 42  ab c4 2d c7 54 9e a6 8b  |F>.>_.hB..-.T...|
00000080  a5 25 b6 ba f4 f4 35 e9  6b f0 95 13 b3 ad ad 07  |.%....5.k.......|
00000090  36 c9 68 3b ba 1b 7e a0  5c 59 34 1b 88 b2 22 8f  |6.h;..~.\Y4..'.|
000000a0  28 cb fa 95 59 92 8c 0f  06 41 32 f8 20 fb 46 32  |(...Y....A2. .F2|
000000b0  d3 09 b7 13 f7 69 c0 69  7d 41 45 91 b6 ac 4c 84  |.....i.i}AE...L.|
000000c0  35 8e bc a6 eb 6b 8a d1  67 33 4f 7b a7 61 ea f0  |5....k..g3O{.a..|
000000d0  9b 4f 54 85 c9 94 46 5d  32 00 6c 9d be 78 91 1b  |.OT...F]2.l..x..|
000000e0  8d 16 52 a9 c1 52 a9 90  bc 31 0f 01 10 4d 60 cc  |..R..R...1...M`.|
000000f0  70 91 c5 59 0d 72 28 23  81 b2 ea 7c 80 cd 8a ea  |p..Y.r(....|....|
00000100  53 00 c0 68 7b d6 fd 63  cf 5b 8d 2f 25 8c 00 bb  |S..h{..c.[./%...|
00000110  b1 01 62 60 2d b7 ab ed  dd b8 af 7b da 34 84 97  |..b`-......{.4..|
00000120  ed 20 64 ba 42 6b cc 7f  77 80 48 7e e8 ad 52 9d  |. d.Bk..w.H~..R.|
00000130  d6 e1 6e 5c 5f 18 c4 24  5f d5 6b 4d 78 cf d4 a7  |..n\_..$_.kMx...|
00000140  a0 07 6c ea 41 c4 04 85  58 f5 0a 9d f7 47 55 8f  |..l.A...X....GU.|
00000150  13 3c a4 12 f7 90 5a 04  8d 9d 6a 00 2c a5 79 3e  |.<....Z...j.,.y>|
00000160  48 63 9f 4d 33 bd cd 71  a9 7f b7 c0 c8 da 3d fe  |Hc.M3..q......=.|
00000170  e8 75 44 3d 99 b3 6f 06  c7 78 1e 74 a6 30 a7 27  |.uD=..o..x.t.0.'|
00000180  e2 f2 c6 40 0b 47 24 38  27 79 6a 31 42 c1 6d a7  |...@.G$8'yj1B.m.|
00000190  22 5e de 4e 5f 86 78 49  57 d3 e8 4a ff ce 5c 48  |'^.N_.xIW..J..\H|
000001a0  8e 8d 55 1b 03 85 be 94  31 b8 80 26 5b 7d ce 4c  |..U.....1..&[}.L|
000001b0  f6 af d1 1d ec 58 2d 44  af bf 7a 27 f2 32 d9 78  |.....X-D..z'.2.x|
000001c0  2d 72 2e 0e b1 8f 0b eb  5f 85 c4 4e a5 be 7b 0e  |-r......_..N..{.|
000001d0  c0 8f f4 7f de 11 4f ff  89 37 24 7a b5 80 97 64  |......O..7$z...d|
000001e0  26 a6 d1 ad 92 3f 2a 95  f6 64 06 23 3b 8b d6 e1  |&....?*..d.;....|
000001f0  11 07 ca a3 dd 78 4f e7  62 26 cc 89 aa 03 80 85  |.....xO.b&......|
00000200  8f 6d f6 0e 19 08 78 6e  2b 07 d9 25 38 b3 40 52  |.m....xn+..%8.@R|
00000210  a7 90 70 cf aa 4a 36 0a  b0 e6 1e 34 89 29 4f 99  |..p..J6....4.)O.|
00000220  62 43 c6 d2 eb 36 1a 46  67 11 a7 3f 73 a2 cb 98  |bC...6.Fg..?s...|
00000230  fc f1 6d 69 c1 a5 ed c1  50 34 e4 49 85 99 39 9d  |..mi....P4.I..9.|
00000240  74 8d 50 8c af 2e c0 05  3b f1 38 cf c7 b7 b3 b1  |t.P.....;.8.....|
00000250  81 3f 23 38 dc da b4 60  46 ec a1 92 d1 67 16 37  |.?#8...`F....g.7|
00000260  7a 05 37 77 d5 f3 2e 7f  5a 73 6c 14 37 2d 74 33  |z.7w....Zsl.7-t3|
00000270  45 27 38 49 53 92 e3 31  80 73 d4 55 05 44 63 f0  |E'8IS..1.s.U.Dc.|
00000280  90 e0 cf 1a 52 db 26 97  7c 91 c5 4d 82 94 13 1e  |....R.&.|..M....|
00000290  40 bf da b6 96 db e0 06  cc e8 ed 7a b9 ba b0 2f  |@..........z.../|
000002a0  1d 63 80 67 81 28 1b 06  ac aa 07 76 a5 90 74 96  |.c.g.(.....v..t.|
000002b0  4d 30 02 e0 b4 51 53 4f  45 c3 0c 20 02 99 f1 e8  |M0...QSOE.. ....|
000002c0  c4 2e 62 ac 5c ce 95 e5  c5 3e d2 6e c0 15 e0 1a  |..b.\....>.n....|
000002d0  43 74 3a a2 6f dc 05 36  b7 50 33 23 21 39 9e 32  |Ct:.o..6.P3'!9.2|
```

```
000002e0  7e a7 9a ce 6d 35 df 99  c6 ad a2 22 fe d5 69 a7  |~...m5.....'..i.|
000002f0  44 68 9d 6a 98 69 a0 4f  6d 0c df 29 6a 41 67 2e  |Dh.j.i.Om..)jAg.|
00000300  b1 4e bd 8d d3 cb 7a 2f  f8 c4 3b 0c 25 33 32 10  |.N....z/..;.%32.|
00000310  72 c5 cf cb 9a 24 d9 2e  51 11 c5 03 50 bb 9d c1  |r....$..Q...P...|
00000320  39 e4 13 2b fe 2b 07 55  1f 7f ad f5 46 a7 cd df  |9..+.+.U....F...|
00000330  39 ba 46 d6 95 ba 35 60  4c e2 77 7a cf 8b 7b 2f  |9.F...5`L.wz..{/|
00000340  75 4a 38 f8 6e 83 58 6d  53 e0 b7 c8 95 c1 5f 74  |uJ8.n.XmS.....t|
00000350  bf 9c e8 31 40 82 db 5c  f4 d0 39 d3 d8 11 5a ac  |...1@..\..9...Z.|
00000360  85 37 df 47 43 a0 a9 93  21 78 58 9d 5f 92 2e 87  |.7.GC...!xX._...|
00000370  46 05 72 32 c3 f4 f6 27  41 02 ec 75 6e 12 d2 db  |F.r2...'A..un...|
00000380  0d ea 87 ad 71 12 d9 78  aa 5e 95 43 e1 7c c5 01  |....q..x.^.C.|..|
00000390  af bd 0b 99 59 cb e9 a5  ef cc 42 90 35 79 f9 88  |....Y.....B.5y..|
000003a0  69 84 d6 53 58 68 e5 ad  89 c0 20 83 51 d8 d5 2a  |i..SXh.... .Q..*|
000003b0  77 6a 1c 1c 9c 1e 35 10  83 92 a9 34 ae a1 d1 28  |wj....5....4...(|
000003c0  ca a4 fc 7a 02 25 39 6f  1d 82 28 38 47 ac 76 13  |...z.%9o..(8G.v.|
000003d0  d2 a3 9f f8 44 12 cc b3  37 8b 39 46 29 fe 8b 8d  |....D...7.9F)...|
000003e0  db a1 13 2c 07 ea 41 76  92 15 a6 68 9d 80 39 52  |...,..Av...h..9R|
000003f0  1f 19 5c c7 63 09 65 02  19 f5 54 d4 c2 19 49 1f  |..\.c.e...T...I.|
00000400  6f 03 1d 2f 93 ea 18 93  88 bf 7e 39 47 80 d8 0a  |o../......~9G...|
00000410
[usuario@portatil:~]$ openssl enc -aes-256-cbc -K e0e0e0e0f1f1f1f1 -iv 0123456789abcdef -
    in /tmp/imput1.bin -out /tmp/imput1_aes256_cbc.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes256_cbc.enc
00000000  51 0d 5e 09 5e 07 83 64  e7 01 0c db 66 b2 b2 e7  |Q.^.^..d....f...|
00000010  31 83 f6 13 9d 9a 8d 37  3c 07 fb 37 7c f0 a0 75  |1......7<..7|..u|
00000020  9d db 94 15 4b 49 86 4c  8b 2f 47 ee 7b 83 03 72  |....KI.L./G.{..r|
00000030  d7 2a 28 48 e6 ed ed 92  f2 aa 81 71 c1 ae 60 fe  |.*(H.......q..`.|
00000040  43 35 4d 85 8b 40 5d 1c  9f 8f d1 86 4d 27 5a 8c  |C5M..@].....M'Z.|
00000050  67 0a 5d 63 4a 68 b7 d5  a0 17 2c 27 9a d1 4e 5d  |g.]cJh....,'..N]|
00000060  f1 4d 84 3d 15 69 15 61  f5 90 42 bd 84 6b 54 77  |.M.=.i.a..B..kTw|
00000070  46 3e f8 3e 5f 1d 68 42  ab c4 2d c7 54 9e a6 8b  |F>.>_.hB..-.T...|
00000080  60 03 f1 13 eb 9f 77 c1  bc 5d 75 3a bc e7 4d 4a  |`.....w..]u:..MJ|
00000090  cb f6 93 9d bc 22 9b f8  12 8c 64 17 76 12 ab 5f  |.....'....d.v.._|
000000a0  68 6f 10 08 31 5f 87 fd  f6 b0 c9 3c 00 92 06 f8  |ho..1_.....<....|
000000b0  f1 ac 3e e3 b3 18 79 91  8f d6 65 7a e4 4e 3c 9f  |..>...y...ez.N<.|
000000c0  41 51 e5 ea bf e7 b6 27  94 d3 c1 0e 37 e0 f3 e9  |AQ.....'....7...|
000000d0  bc d1 e3 3d c9 84 44 ed  07 39 19 4f 4a 16 82 4f  |...=..D..9.OJ..O|
000000e0  c2 fb 1f 32 dd 13 27 b5  bc d3 ab 60 e4 52 fe 5b  |...2..'....`.R.[|
000000f0  e8 06 85 ed 0c a4 90 11  1e 6f 9d 39 06 5c 13 f8  |.........o.9.\..|
00000100  04 ab 00 64 f2 db 1e 4c  8a 0f 39 b3 fc 5c 0b 25  |...d...L..9..\.%|
00000110  c0 e3 c5 92 b4 e8 3e b3  66 2b 78 32 07 77 ae 0a  |......>.f+x2.w..|
00000120  33 93 f3 13 4e c7 68 6b  e8 2f 9c 0c 14 69 da c3  |3...N.hk./...i..|
00000130  7e 42 56 64 4b e7 f6 06  97 03 52 29 3e d7 dc 58  |~BVdK.....R)>..X|
00000140  16 7c f0 79 96 5a c7 9d  9b b5 2a 95 21 fd b0 19  |.|.y.Z....*.!...|
00000150  65 5f bf 81 e9 70 18 91  64 36 9c ea 1e 80 ca eb  |e_...p..d6......|
00000160  cc c9 f6 50 55 e3 99 14  ca eb 07 ca 2e 30 6a bd  |...PU........0j.|
00000170  e0 89 da 54 5a 6b f0 45  70 69 9f 61 9a 34 96 dc  |...TZk.Epi.a.4..|
00000180  23 30 16 27 69 eb 8f c9  f5 8e e5 9a c8 ab 6a df  |#0.'i.........j.|
00000190  cf 8a 9a a3 be 17 b6 d6  9f 74 67 af 17 13 36 4f  |.........tg...6O|
000001a0  da ff 49 e6 cb c5 d3 cf  5c 33 e0 a6 d1 0b cc ea  |..I.....\3......|
000001b0  9b 17 f3 fc c2 43 b8 54  53 54 f5 b1 e5 43 f4 98  |.....C.TST...C..|
000001c0  ae ff 7d ff a5 5a 9d e9  94 ec 9c 41 ee 7a b8 a0  |..}..Z.....A.z..|
000001d0  44 18 a5 90 a1 d7 73 1c  29 4c 69 d4 1f 2f 0e a1  |D.....s.)Li../..|
000001e0  1c 27 48 27 5a b6 e4 4c  6b 48 e8 0a ab f7 d2 de  |.'H'Z..LkH......|
000001f0  83 54 19 95 93 2c db e3  79 02 4a f4 d5 84 cb ca  |.T...,..y.J.....|
00000200  d2 dc 9d c7 d8 14 0d 23  cf 31 4b 73 f9 57 78 89  |.......#.1Ks.Wx.|
00000210  ae 24 f8 cc aa ce 60 cc  ff 2b b7 80 5e f3 b7 c1  |.$....`..+..^...|
00000220  cb 83 31 35 31 53 b1 ab  fd 84 8f 63 7b 29 9f 62  |..151S.....c{).b|
00000230  0c 91 b6 8c 7a 2c eb 65  f6 92 6a 07 b6 48 f7 3a  |....z,.e..j..H.:|
00000240  bc be f5 2a 16 c9 df c4  8f cf 30 93 3d 47 c1 74  |...*......0.=G.t|
00000250  93 f4 f8 d9 d5 78 c4 be  12 15 54 55 b5 88 af d8  |.....x....TU....|
00000260  25 9b 06 c7 5f ce e4 bd  29 97 cd 46 57 e8 94 2e  |%..._...)..FW...|
00000270  2e a6 92 44 45 66 b5 f9  c5 1a 1e 63 a8 01 af 85  |...DEf.....c....|
00000280  02 50 48 bc d4 18 90 23  30 7b e0 52 a9 25 7a 11  |.PH....#0{.R.%z.|
00000290  91 53 1d 91 25 a5 f3 74  29 83 07 8e 42 59 62 39  |.S..%..t)...BYb9|
000002a0  5b 21 aa 54 f8 44 89 e2  87 9e 99 ef d0 fe 4c f9  |[!.T.D........L.|
000002b0  02 8c 8e 61 45 64 87 2a  46 ae 77 d8 99 80 8e 25  |...aEd.*F.w....%|
000002c0  5e 45 7d d7 79 04 0a 6f  3a 90 37 ee 33 32 c6 84  |^E}.y..o:.7.32..|
000002d0  a3 3a cf df db 51 15 1c  43 3d 0f 5c 8a a8 67 dd  |.:...Q..C=.\..g.|
000002e0  62 85 6c 3e b3 88 27 2d  e2 64 47 fd 8d 78 fe e0  |b.l>..'-.dG..x..|
000002f0  c5 eb a5 52 eb eb 0f 6b  ff 16 a2 8a d4 0b bc 65  |...R...k.......e|
00000300  0d ae 2d e8 f9 8b 4e c3  0b 61 40 e0 53 a2 c6 f6  |..-...N..a@.S...|
00000310  60 53 a7 5c 87 9a 65 49  a2 e9 8b 02 12 33 cc 80  |`S.\..eI.....3..|
00000320  68 9a ed 39 9d 20 d8 bb  1e a4 ed 1a 6c b3 7a 5f  |h..9. ......l.z_|
00000330  1a 5f db a8 bf ee e0 20  d4 c1 20 d8 ae 0c e9 bb  |._..... .. .....|
```

```
00000340  3e b1 1b c8 76 4d d0 4d  1b ab 3c 90 30 c1 66 7e  |>...vM.M..<.0.f~|
00000350  55 60 c8 ee 1e a8 be 04  8e 85 33 67 cc 98 f3 be  |U`........3g....|
00000360  97 05 33 6e 57 fd 12 8b  18 f7 31 66 60 7f d7 30  |..3nW.....1f`..0|
00000370  15 e7 5b 97 1c cc 22 06  7d 6d b4 d1 45 58 f6 40  |..[...".}m..EX.@|
00000380  f1 e9 5a 3f 8c f4 ee aa  8b 78 24 68 bc c8 26 79  |..Z?.....x$h..&y|
00000390  90 80 f4 df 73 df 4f 49  6e a2 88 8c cb 55 70 b7  |....s.OIn....Up.|
000003a0  1e d9 47 dc ff 9b 30 50  09 29 37 ab 5a 46 43 c0  |..G...0P.)7.ZFC.|
000003b0  d4 30 46 29 56 90 30 93  4c 7a 45 8f a6 2a 9a c0  |.0F)V.0.LzE..*..|
000003c0  a1 45 65 ee 07 4b f1 98  78 f0 fe e0 1a 0e d0 30  |.Ee..K..x......0|
000003d0  3d d1 10 4e 1a 36 f7 30  11 9f be e6 76 55 84 fb  |=..N.6.0....vU..|
000003e0  8b 89 45 82 79 08 57 75  9e 9b a2 14 42 1b d7 c8  |..E.y.Wu....B...|
000003f0  42 0d f3 5e 0f a7 1e 21  c1 32 23 f9 50 e8 89 ce  |B..^...!.2#.P...|
00000400  3d 68 8b 7d 54 53 60 dc  8c 20 75 d6 3b 57 c8 e2  |=h.}TS`.. u.;W..|
00000410
```

En este modo a la hora de cifrar los datos, se cifran todas los bits de los ficheros de forma diferente, osea que, incluso teniendo todos los bits del fichero iguales, este modo cifra todos los bits de forma diferente, si es verdad que los primeros 60 bits de ambos ficheros cifrados son iguales pero a partir de ahí, se pierde dicha igualdad.

3.3. Modo OFB

```
[usuario@portatil:~]$ openssl enc -aes-256-ofb -K e0e0e0e0f1f1f1f1 -iv 0123456789abcdef -
    in /tmp/imput.bin -out /tmp/imput_aes256_ofb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes256_ofb.enc
00000000  51 0d 5e 09 5e 07 83 64  e7 01 0c db 66 b2 b2 e7  |Q.^.^..d....f...|
00000010  31 83 f6 13 9d 9a 8d 37  3c 07 fb 37 7c f0 a0 75  |1......7<..7|..u|
00000020  9d db 94 15 4b 49 86 4c  8b 2f 47 ee 7b 83 03 72  |....KI.L./G.{..r|
00000030  d7 2a 28 48 e6 ed ed 92  f2 aa 81 71 c1 ae 60 fe  |.*(H.......q..`.|
00000040  43 35 4d 85 8b 40 5d 1c  9f 8f d1 86 4d 27 5a 8c  |C5M..@].....M'Z.|
00000050  67 0a 5d 63 4a 68 b7 d5  a0 17 2c 27 9a d1 4e 5d  |g.]cJh....,'..N]|
00000060  f1 4d 84 3d 15 69 15 61  f5 90 42 bd 84 6b 54 77  |.M.=.i.a..B..kTw|
00000070  46 3e f8 3e 5f 1d 68 42  ab c4 2d c7 54 9e a6 8b  |F>.>_.hB..-.T...|
00000080  a5 25 b6 ba f4 f4 35 e9  6b f0 95 13 b3 ad ad 07  |.%....5.k.......|
00000090  36 c9 68 3b ba 1b 7e a0  5c 59 34 1b 88 b2 22 8f  |6.h;..~.\Y4...".|
000000a0  28 cb fa 95 59 92 8c 0f  06 41 32 f8 20 fb 46 32  |(...Y....A2. .F2|
000000b0  d3 09 b7 13 f7 69 c0 69  7d 41 45 91 b6 ac 4c 84  |.....i.i}AE...L.|
000000c0  35 8e bc a6 eb 6b 8a d1  67 33 4f 7b a7 61 ea f0  |5....k..g3O{.a..|
000000d0  9b 4f 54 85 c9 94 46 5d  32 00 6c 9d be 78 91 1b  |.OT...F]2.l..x..|
000000e0  8d 16 52 a9 c1 52 a9 90  bc 31 0f 01 10 4d 60 cc  |..R..R...1...M`.|
000000f0  70 91 c5 59 0d 72 28 23  81 b2 ea 7c 80 cd 8a ea  |p..Y.r(#...|....|
00000100  53 00 c0 68 7b d6 fd 63  cf 5b 8d 2f 25 8c 00 bb  |S..h{..c.[./%...|
00000110  b1 01 62 60 2d b7 ab ed  dd b8 af 7b da 34 84 97  |..b`-......{.4..|
00000120  ed 20 64 ba 42 6b cc 7f  77 80 48 7e e8 ad 52 9d  |. d.Bk..w.H~..R.|
00000130  d6 e1 6e 5c 5f 18 c4 24  5f d5 6b 4d 78 cf d4 a7  |..n\_..$_.kMx...|
00000140  a0 07 6c ea 41 c4 04 85  58 f5 0a 9d f7 47 55 8f  |..l.A...X....GU.|
00000150  13 3c a4 12 f7 90 5a 04  8d 9d 6a 00 2c a5 79 3e  |.<....Z...j.,.y>|
00000160  48 63 9f 4d 33 bd cd 71  a9 7f b7 c0 c8 da 3d fe  |Hc.M3..q......=.|
00000170  e8 75 44 3d 99 b3 6f 06  c7 78 1e 74 a6 30 a7 27  |.uD=..o..x.t.0.'|
00000180  e2 f2 c6 40 0b 47 24 38  27 79 6a 31 42 c1 6d a7  |...@.G$8'yj1B.m.|
00000190  22 5e de 4e 5f 86 78 49  57 d3 e8 4a ff ce 5c 48  |"^.N_.xIW..J..\H|
000001a0  8e 8d 55 1b 03 85 be 94  31 b8 80 26 5b 7d ce 4c  |..U.....1..&[}.L|
000001b0  f6 af d1 1d ec 58 2d 44  af bf 7a 27 f2 32 d9 78  |.....X-D..z'.2.x|
000001c0  2d 72 2e 0e b1 8f 0b eb  5f 85 c4 4e a5 be 7b 0e  |-r......_..N..{.|
000001d0  c0 8f f4 7f de 11 4f ff  89 37 24 7a b5 80 97 64  |......O..7$z...d|
000001e0  26 a6 d1 ad 92 3f 2a 95  f6 64 06 23 3b 8b d6 e1  |&....?*..d.#;...|
000001f0  11 07 ca a3 dd 78 4f e7  62 26 cc 89 aa 03 80 85  |.....xO.b&......|
00000200  8f 6d f6 0e 19 08 78 6e  2b 07 d9 25 38 b3 40 52  |.m....xn+..%8.@R|
00000210  a7 90 70 cf aa 4a 36 0a  b0 e6 1e 34 89 29 4f 99  |..p..J6....4.)O.|
00000220  62 43 c6 d2 eb 36 1a 46  67 11 a7 3f 73 a2 cb 98  |bC...6.Fg..?s...|
00000230  fc f1 6d 69 c1 a5 ed c1  50 34 e4 49 85 99 39 9d  |..mi....P4.I..9.|
00000240  74 8d 50 8c af 2e c0 05  3b f1 38 cf c7 b7 b3 b1  |t.P.....;.8.....|
00000250  81 3f 23 38 dc da b4 60  46 ec a1 92 d1 67 16 37  |.?#8...`F....g.7|
00000260  7a 05 37 77 d5 f3 2e 7f  5a 73 6c 14 37 2d 74 33  |z.7w....Zsl.7-t3|
00000270  45 27 38 49 53 92 e3 31  80 73 d4 55 05 44 63 f0  |E'8IS..1.s.U.Dc.|
00000280  90 e0 cf 1a 52 db 26 97  7c 91 c5 4d 82 94 13 1e  |....R.&.|..M....|
00000290  40 bf da b6 96 db e0 06  cc e8 ed 7a b9 ba b0 2f  |@..........z.../|
000002a0  1d 63 80 67 81 28 1b 06  ac aa 07 76 a5 90 74 96  |.c.g.(.....v..t.|
000002b0  4d 30 02 e0 b4 51 53 4f  45 c3 0c 20 02 99 f1 e8  |M0...QSOE.. ....|
000002c0  c4 2e 62 ac 5c ce 95 e5  c5 3e d2 6e c0 15 e0 1a  |..b.\....>.n....|
000002d0  43 74 3a a2 6f dc 05 36  b7 50 33 23 21 39 9e 32  |Ct:.o..6.P3#!9.2|
```

```
000002e0  7e a7 9a ce 6d 35 df 99  c6 ad a2 22 fe d5 69 a7  |~...m5.....'..i.|
000002f0  44 68 9d 6a 98 69 a0 4f  6d 0c df 29 6a 41 67 2e  |Dh.j.i.Om..)jAg.|
00000300  b1 4e bd 8d d3 cb 7a 2f  f8 c4 3b 0c 25 33 32 10  |.N....z/..;.%32.|
00000310  72 c5 cf cb 9a 24 d9 2e  51 11 c5 03 50 bb 9d c1  |r....$..Q...P...|
00000320  39 e4 13 2b fe 2b 07 55  1f 7f ad f5 46 a7 cd df  |9..+.+.U....F...|
00000330  39 ba 46 d6 95 ba 35 60  4c e2 77 7a cf 8b 7b 2f  |9.F...5`L.wz..{/|
00000340  75 4a 38 f8 6e 83 58 6d  53 e0 b7 c8 95 c1 5f 74  |uJ8.n.XmS.....t|
00000350  bf 9c e8 31 40 82 db 5c  f4 d0 39 d3 d8 11 5a ac  |...1@..\..9...Z.|
00000360  85 37 df 47 43 a0 a9 93  21 78 58 9d 5f 92 2e 87  |.7.GC...!xX._...|
00000370  46 05 72 32 c3 f4 f6 27  41 02 ec 75 6e 12 d2 db  |F.r2...'A..un...|
00000380  0d ea 87 ad 71 12 d9 78  aa 5e 95 43 e1 7c c5 01  |....q..x.^.C.|..|
00000390  af bd 0b 99 59 cb e9 a5  ef cc 42 90 35 79 f9 88  |....Y.....B.5y..|
000003a0  69 84 d6 53 58 68 e5 ad  89 c0 20 83 51 d8 d5 2a  |i..SXh.... .Q..*|
000003b0  77 6a 1c 1c 9c 1e 35 10  83 92 a9 34 ae a1 d1 28  |wj....5....4...(|
000003c0  ca a4 fc 7a 02 25 39 6f  1d 82 28 38 47 ac 76 13  |...z.%9o..(8G.v.|
000003d0  d2 a3 9f f8 44 12 cc b3  37 8b 39 46 29 fe 8b 8d  |....D...7.9F)...|
000003e0  db a1 13 2c 07 ea 41 76  92 15 a6 68 9d 80 39 52  |...,..Av...h..9R|
000003f0  1f 19 5c c7 63 09 65 02  19 f5 54 d4 c2 19 49 1f  |..\.c.e...T...I.|
00000400
[usuario@portatil:~]$ openssl enc -aes-256-ofb -K e0e0e0e0f1f1f1f1 -iv 0123456789abcdef -
    in /tmp/imput1.bin -out /tmp/imput1_aes256_ofb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes256_ofb.enc
00000000  51 0d 5e 09 5e 07 83 64  e7 01 0c db 66 b2 b2 e7  |Q.^.^..d....f...|
00000010  31 83 f6 13 9d 9a 8d 37  3c 07 fb 37 7c f0 a0 75  |1......7<..7|..u|
00000020  9d db 94 15 4b 49 86 4c  8b 2f 47 ee 7b 83 03 72  |....KI.L./G.{..r|
00000030  d7 2a 28 48 e6 ed ed 92  f2 aa 81 71 c1 ae 60 fe  |.*(H.......q..`.|
00000040  43 35 4d 85 8b 40 5d 1c  9f 8f d1 86 4d 27 5a 8c  |C5M..@].....M'Z.|
00000050  67 0a 5d 63 4a 68 b7 d5  a0 17 2c 27 9a d1 4e 5d  |g.]cJh....,'..N]|
00000060  f1 4d 84 3d 15 69 15 61  f5 90 42 bd 84 6b 54 77  |.M.=.i.a..B..kTw|
00000070  46 3e f8 3e 5f 1d 68 42  ab c4 2d c7 54 9e a6 8b  |F>.>_.hB..-.T...|
00000080  a5 25 b6 ba f4 f4 35 e8  6b f0 95 13 b3 ad ad 07  |.%....5.k.......|
00000090  36 c9 68 3b ba 1b 7e a0  5c 59 34 1b 88 b2 22 8f  |6.h;..~.\Y4...'.|
000000a0  28 cb fa 95 59 92 8c 0f  06 41 32 f8 20 fb 46 32  |(...Y....A2. .F2|
000000b0  d3 09 b7 13 f7 69 c0 69  7d 41 45 91 b6 ac 4c 84  |.....i.i}AE...L.|
000000c0  35 8e bc a6 eb 6b 8a d1  67 33 4f 7b a7 61 ea f0  |5....k..g3O{.a..|
000000d0  9b 4f 54 85 c9 94 46 5d  32 00 6c 9d be 78 91 1b  |.OT...F]2.l..x..|
000000e0  8d 16 52 a9 c1 52 a9 90  bc 31 0f 01 10 4d 60 cc  |..R..R...1...M`.|
000000f0  70 91 c5 59 0d 72 28 23  81 b2 ea 7c 80 cd 8a ea  |p..Y.r('...|....|
00000100  53 00 c0 68 7b d6 fd 63  cf 5b 8d 2f 25 8c 00 bb  |S..h{..c.[./%...|
00000110  b1 01 62 60 2d b7 ab ed  dd b8 af 7b da 34 84 97  |..b`-......{.4..|
00000120  ed 20 64 ba 42 6b cc 7f  77 80 48 7e e8 ad 52 9d  |. d.Bk..w.H~..R.|
00000130  d6 e1 6e 5c 5f 18 c4 24  5f d5 6b 4d 78 cf d4 a7  |..n\_..$_.kMx...|
00000140  a0 07 6c ea 41 c4 04 85  58 f5 0a 9d f7 47 55 8f  |..l.A...X....GU.|
00000150  13 3c a4 12 f7 90 5a 04  8d 9d 6a 00 2c a5 79 3e  |.<....Z...j.,.y>|
00000160  48 63 9f 4d 33 bd cd 71  a9 7f b7 c0 c8 da 3d fe  |Hc.M3..q......=.|
00000170  e8 75 44 3d 99 b3 6f 06  c7 78 1e 74 a6 30 a7 27  |.uD=..o..x.t.0.'|
00000180  e2 f2 c6 40 0b 47 24 38  27 79 6a 31 42 c1 6d a7  |...@.G$8'yj1B.m.|
00000190  22 5e de 4e 5f 86 78 49  57 d3 e8 4a ff ce 5c 48  |'^.N_.xIW..J..\H|
000001a0  8e 8d 55 1b 03 85 be 94  31 b8 80 26 5b 7d ce 4c  |..U.....1..'[}.L|
000001b0  f6 af d1 1d ec 58 2d 44  af bf 7a 27 f2 32 d9 78  |.....X-D..z'.2.x|
000001c0  2d 72 2e 0e b1 8f 0b eb  5f 85 c4 4e a5 be 7b 0e  |-r......_..N..{.|
000001d0  c0 8f f4 7f de 11 4f ff  89 37 24 7a b5 80 97 64  |......O..7$z...d|
000001e0  26 a6 d1 ad 92 3f 2a 95  f6 64 06 23 3b 8b d6 e1  |'....?*..d.';...|
000001f0  11 07 ca a3 dd 78 4f e7  62 26 cc 89 aa 03 80 85  |.....xO.b'......|
00000200  8f 6d f6 0e 19 08 78 6e  2b 07 d9 25 38 b3 40 52  |.m....xn+..%8.@R|
00000210  a7 90 70 cf aa 4a 36 0a  b0 e6 1e 34 89 29 4f 99  |..p..J6....4.)O.|
00000220  62 43 c6 d2 eb 36 1a 46  67 11 a7 3f 73 a2 cb 98  |bC...6.Fg..?s...|
00000230  fc f1 6d 69 c1 a5 ed c1  50 34 e4 49 85 99 39 9d  |..mi....P4.I..9.|
00000240  74 8d 50 8c af 2e c0 05  3b f1 38 cf c7 b7 b3 b1  |t.P.....;.8.....|
00000250  81 3f 23 38 dc da b4 60  46 ec a1 92 d1 67 16 37  |.?'8...`F....g.7|
00000260  7a 05 37 77 d5 f3 2e 7f  5a 73 6c 14 37 2d 74 33  |z.7w....Zsl.7-t3|
00000270  45 27 38 49 53 92 e3 31  80 73 d4 55 05 44 63 f0  |E'8IS..1.s.U.Dc.|
00000280  90 e0 cf 1a 52 db 26 97  7c 91 c5 4d 82 94 13 1e  |....R.'.|..M....|
00000290  40 bf da b6 96 db e0 06  cc e8 ed 7a b9 ba b0 2f  |@..........z.../|
000002a0  1d 63 80 67 81 28 1b 06  ac aa 07 76 a5 90 74 96  |.c.g.(.....v..t.|
000002b0  4d 30 02 e0 b4 51 53 4f  45 c3 0c 20 02 99 f1 e8  |M0...QSOE.. ....|
000002c0  c4 2e 62 ac 5c ce 95 e5  c5 3e d2 6e c0 15 e0 1a  |..b.\....>.n....|
000002d0  43 74 3a a2 6f dc 05 36  b7 50 33 23 21 39 9e 32  |Ct:.o..6.P3'!9.2|
000002e0  7e a7 9a ce 6d 35 df 99  c6 ad a2 22 fe d5 69 a7  |~...m5.....'..i.|
000002f0  44 68 9d 6a 98 69 a0 4f  6d 0c df 29 6a 41 67 2e  |Dh.j.i.Om..)jAg.|
00000300  b1 4e bd 8d d3 cb 7a 2f  f8 c4 3b 0c 25 33 32 10  |.N....z/..;.%32.|
00000310  72 c5 cf cb 9a 24 d9 2e  51 11 c5 03 50 bb 9d c1  |r....$..Q...P...|
00000320  39 e4 13 2b fe 2b 07 55  1f 7f ad f5 46 a7 cd df  |9..+.+.U....F...|
00000330  39 ba 46 d6 95 ba 35 60  4c e2 77 7a cf 8b 7b 2f  |9.F...5`L.wz..{/|
00000340  75 4a 38 f8 6e 83 58 6d  53 e0 b7 c8 95 c1 5f 74  |uJ8.n.XmS.....t|
```

```
00000350  bf 9c e8 31 40 82 db 5c  f4 d0 39 d3 d8 11 5a ac  |...1@..\..9...Z.|
00000360  85 37 df 47 43 a0 a9 93  21 78 58 9d 5f 92 2e 87  |.7.GC...!xX._...|
00000370  46 05 72 32 c3 f4 f6 27  41 02 ec 75 6e 12 d2 db  |F.r2...'A..un...|
00000380  0d ea 87 ad 71 12 d9 78  aa 5e 95 43 e1 7c c5 01  |....q..x.^.C.|..|
00000390  af bd 0b 99 59 cb e9 a5  ef cc 42 90 35 79 f9 88  |....Y.....B.5y..|
000003a0  69 84 d6 53 58 68 e5 ad  89 c0 20 83 51 d8 d5 2a  |i..SXh.... .Q..*|
000003b0  77 6a 1c 1c 9c 1e 35 10  83 92 a9 34 ae a1 d1 28  |wj....5....4...(|
000003c0  ca a4 fc 7a 02 25 39 6f  1d 82 28 38 47 ac 76 13  |...z.%9o..(8G.v.|
000003d0  d2 a3 9f f8 44 12 cc b3  37 8b 39 46 29 fe 8b 8d  |....D...7.9F)...|
000003e0  db a1 13 2c 07 ea 41 76  92 15 a6 68 9d 80 39 52  |...,..Av...h..9R|
000003f0  1f 19 5c c7 63 09 65 02  19 f5 54 d4 c2 19 49 1f  |..\.c.e...T...I.|
00000400
```

En este último modo, hay una cosa que sorprende a primera vista y es que aunque el contenido de los ficheros de entrada son diferentes, el contenido de los ficheros de salida son iguales, por lo tanto significa que el contenido del fichero de entrada no tiene nada que ver en el cifrado de datos, y lo que realmente tiene en cuenta es la clave y el vector de inicialización.

Los diferentes modos, se puede apreciar cuales son las caracteristicas principales de los mismos, el primero de todos es el mas simple, el segundo es el que mantiene parte de los datos de igual manera incluso cambiando los datos de entrada, y por ultimo y bajo mi punto de vista el mejor, el que cifra los datos independientemente de los datos de entrada que tenga.

4. Cifrar input.bin e input1.bin con AES-128 en modos ECB, CBC y OFB usando una contraseña a elegir. Explicar los diferentes resultados.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

4.1. Modo ECB

```
[usuario@portatil:~]$ openssl enc -aes-128-ecb -pass pass:mipass -in /tmp/imput.bin -out
    /tmp/imput_aes128_ecb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes128_ecb.enc
00000000  53 61 6c 74 65 64 5f 5f  fe e1 9b a0 9a 2d b6 11  |Salted__.....-..|
00000010  1e 9b f3 c6 d6 ed d1 e4  3f 3e c9 7c 7c 4b 27 81  |........?>.||K'.|
*
00000410  c9 a8 a5 ae 8d 0f 51 36  1f 8a 7d 49 ec 16 43 76  |......Q6..}I..Cv|
00000420
[usuario@portatil:~]$ openssl enc -aes-128-ecb -pass pass:mipass -in /tmp/imput1.bin -out
     /tmp/imput1_aes128_ecb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes128_ecb.enc
00000000  53 61 6c 74 65 64 5f 5f  c2 46 c5 30 d9 d8 e4 44  |Salted__.F.0...D|
00000010  11 70 c7 ac 7f 5d 1f b3  d4 e3 b1 e7 66 b3 2a 07  |.p...]......f.*.|
*
00000090  a5 97 88 8b c7 f8 bf 89  03 e9 b9 e7 25 86 f4 16  |............%...|
000000a0  11 70 c7 ac 7f 5d 1f b3  d4 e3 b1 e7 66 b3 2a 07  |.p...]......f.*.|
*
00000410  8e aa 95 da 0a 33 31 72  18 f1 41 5d f2 dc 45 11  |.....31r..A]..E.|
00000420
```

4.2. Modo CBC

```
[usuario@portatil:~]$ openssl enc -aes-128-cbc -iv 0123456789abcdef -pass pass:mipass -in
     /tmp/imput.bin -out /tmp/imput_aes128_cbc.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes128_cbc.enc
00000000  53 61 6c 74 65 64 5f 5f  4c 01 b2 34 61 99 53 41  |Salted__L..4a.SA|
00000010  16 d1 cb ae e2 26 a1 4a  84 e7 df 32 29 2c ef 80  |.....'.J...2),..|
00000020  71 80 ae a6 e9 7e 21 ef  d3 71 31 de 1f 31 31 aa  |q....~!..q1..11.|
00000030  59 4c 92 d7 4f 8d d7 ca  4d 7b 98 e5 7b 97 09 0b  |YL..O...M{..{...|
00000040  16 a2 46 1b f3 77 06 c5  66 9a 4d a8 03 2a b8 ad  |..F..w..f.M..*..|
00000050  13 67 2b 73 ff 16 35 95  e2 65 1f 89 1a a8 a0 44  |.g+s..5..e.....D|
```

```
00000060  38 ce e0 ff 62 76 89 91  e7 50 87 75 1a 77 17 27  |8...bv...P.u.w.'|
00000070  cc 5c 2a 30 33 1e 94 4b  8d 79 37 a0 60 03 b5 5e  |.'*03..K.y7.`..^|
00000080  f7 a4 37 b6 ee c8 38 d4  d4 ba ea ed 59 1a 2f e0  |..7...8.....Y./.|
00000090  1b 1d e4 7a 4f 42 61 52  b6 a3 dd 06 60 90 23 0b  |...zOBaR....`...|
000000a0  82 55 df 01 d7 c7 9a 1e  60 aa cf a8 d1 96 cc c7  |.U......`.......|
000000b0  6d 13 c1 18 0f 3e 27 ab  39 6a b2 5b 66 54 de 92  |m....>'.9j.[fT..|
000000c0  f4 35 c6 b1 e9 e2 44 3b  d9 29 52 fb e7 2f a4 5e  |.5....D;.)R../.^|
000000d0  82 5d 8c 66 c1 7d 2a c3  4d fe b9 15 7f ce e5 a3  |.].f.}*.M.......|
000000e0  3a e0 27 0e ae 7b 96 66  ff 58 2e 08 25 3f 5e 45  |:.'..{.f.X..%?^E|
000000f0  ff ec e8 66 92 4e d9 96  80 0c 91 06 39 e8 9e f6  |...f.N......9...|
00000100  0c 06 a5 24 3c a2 2c ef  67 3d e7 19 60 6e e5 98  |...$<.,.g=..`n..|
00000110  b4 eb 2f 79 fa 6c 50 0b  88 71 2a 1b 3a 83 a3 db  |../y.lP..q*.:...|
00000120  e6 fe cd 6e 7d 04 23 2e  7a d4 31 43 b6 fc a9 0f  |...n}...z.1C....|
00000130  40 d8 51 25 2b 80 79 79  c3 ec fd 6d 51 6f 76 a4  |@.Q%+.yy...mQov.|
00000140  ff 6d 08 e3 a6 0e 7e eb  e7 80 c8 76 71 d1 b4 ba  |.m....~....vq...|
00000150  ca 32 ce 84 63 bf 3a f7  9a 61 c4 a8 75 04 c8 46  |.2..c.:..a..u..F|
00000160  e8 eb 13 d5 36 e3 a2 8c  17 4f 2f e0 8c f9 04 84  |....6....O/.....|
00000170  7c 42 07 10 ff 07 67 09  f1 d2 68 c1 50 c6 b5 0e  ||B....g...h.P...|
00000180  e6 89 49 75 3f 39 8c 85  bd 41 d0 f0 3b 4b b8 49  |..Iu?9...A..;K.I|
00000190  c9 9d 7a 9a cd 9c 6d 7f  cb 12 d7 e2 21 21 5a 96  |..z...m.....!!Z.|
000001a0  8c 03 02 f4 e7 d1 80 95  9c c4 90 14 a3 c0 97 9a  |................|
000001b0  1b 1b 26 e6 e5 07 1d ca  ad 12 27 2a c4 74 2f 24  |..&.......'*.t/$|
000001c0  52 8d 77 fb c1 a4 ce 3d  7a 3a 61 5b b2 94 c3 08  |R.w....=z:a[....|
000001d0  a0 44 6c 36 29 3f d4 fd  86 5b 41 d3 8e d0 66 a3  |.Dl6)?...[A...f.|
000001e0  23 ae 94 a9 61 dc 86 59  61 f4 b3 ea 24 b4 b6 2b  |#...a..Ya...$..+|
000001f0  a4 8d ae 6f 52 2d ca 7a  39 98 b8 20 d2 0b 07 31  |...oR-.z9.. ...1|
00000200  9b 58 2f e6 d3 89 f8 81  ed b5 f9 d5 a2 bb 5a b1  |.X/...........Z.|
00000210  8a c2 97 3d 6f 48 49 fb  04 a8 62 be 99 98 31 be  |...=oHI...b...1.|
00000220  79 73 b9 85 87 d8 d0 af  dc bb 9f 89 6e ed 7f 09  |ys..........n...|
00000230  15 41 06 c4 7e 70 bf 25  d3 d2 bd 4d 54 41 b6 d3  |.A..~p.%...MTA..|
00000240  7e 83 b4 2f 95 c7 75 64  d2 7f be ab 9d c1 cd 48  |~../..ud.......H|
00000250  ad 5d 35 61 0a 4f 6c 21  2f 50 3d 1e 10 49 d7 f4  |.]5a.Ol!/P=..I..|
00000260  e5 64 80 61 66 fc ae 20  ec dd a6 84 64 8b cb 34  |.d.af.. ....d..4|
00000270  61 c3 3e cb 71 24 c9 9a  82 90 5f a5 24 e5 b5 96  |a.>.q$...._.$...|
00000280  89 cf 4f 5e f0 08 23 f7  1c b8 00 bb 31 70 b3 17  |..O^..#.....1p..|
00000290  a8 96 96 16 35 69 7d 9a  ff c2 73 1c 00 55 5e b8  |....5i}...s..U^.|
000002a0  3b c1 e0 81 eb c6 01 0c  63 3d 04 40 a6 fc b4 26  |;.......c=.@...'|
000002b0  cb 8c 43 b4 d6 c7 55 b0  07 b5 11 2b 4c d7 0c 0a  |..C...U....+L...|
000002c0  ae a0 ca 88 fb 49 76 b4  81 29 1e 50 d3 93 3a db  |.....Iv..).P..:.|
000002d0  95 eb 25 2a 09 f8 ea 41  17 e1 3d 7a 9b 7b c8 82  |..'*...A..=z.{..|
000002e0  44 4f df 56 3f 50 dd fa  64 0f 77 40 14 8f 8f b4  |DO.V?P..d.w@....|
000002f0  4b 92 d9 c8 19 ea 32 86  03 b8 35 12 2e 28 ea 19  |K.....2...5..(..|
00000300  dd 5d a8 66 d6 73 a6 a2  ab ed f5 77 92 c9 00 6a  |.].f.s.....w...j|
00000310  27 80 f4 3e 1f 4a 87 a1  72 1d 7c a5 e7 a5 95 17  |'..>.J..r.|.....|
00000320  de 00 6e 66 0f 58 95 11  63 c5 a5 e6 76 40 03 52  |..nf.X..c...v@.R|
00000330  26 29 b7 a3 14 62 31 08  0d 67 10 fa 69 67 e9 0d  |&)...b1..g..ig..|
00000340  b3 fe 8a fb 7a f9 74 5b  0b f1 d4 74 0d 7f 45 c4  |....z.t[...t..E.|
00000350  68 26 b8 bd 9f 24 37 96  77 57 a4 b6 51 32 bd 67  |h&...$7.wW..Q2.g|
00000360  22 2d f6 3c 0e 27 9c 2f  f3 15 b6 8e 70 fe 7e a6  |"-.<.'./....p.~.|
00000370  a9 f7 76 90 dd a9 28 fc  ff 64 10 bc 7b 4e 9c 49  |..v...(..d..{N.I|
00000380  01 ff ee 6e 70 bc e8 69  27 fc cc 30 5b 02 fd 36  |...np..i'..0[..6|
00000390  94 0e 38 10 0a e4 98 36  a7 93 b8 e3 7f 31 16 be  |..8....6.....1..|
000003a0  7b 74 b4 d7 b8 e5 9e c7  2a e5 9c 46 b7 5f 4c bc  |{t......*..F._L.|
000003b0  19 ac 35 61 9b 4b a8 62  a9 35 d7 c9 de 70 8c 8b  |..5a.K.b.5...p..|
000003c0  77 4c 55 4d 38 19 f3 76  1a b1 a5 f2 3a 0e 66 1d  |wLUM8..v....:.f.|
000003d0  b2 00 87 83 d0 f7 5b 29  cd 5b e1 55 68 5c 93 4a  |......[).[.Uh\.J|
000003e0  e7 dd a2 2b cf 0c 08 53  21 77 ad 1d fa 66 ac 3f  |...+...S!w...f.?|
000003f0  1e 54 3a 47 a5 66 ec 23  d6 5b 18 c1 9b 61 d5 cd  |.T:G.f...#.[...a..|
00000400  79 d1 74 d4 9d 1c 95 98  ac 22 49 71 ca f6 4f f2  |y.t......"Iq..O.|
00000410  7d e3 60 ef 32 7a 51 d0  04 ab cb 64 69 ba 79 78  |}.`.2zQ....di.yx|
00000420
[usuario@portatil:~]$ openssl enc -aes-128-cbc -iv 0123456789abcdef -pass pass:mipass -in
    /tmp/imput1.bin -out /tmp/imput1_aes128_cbc.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes128_cbc.enc
00000000  53 61 6c 74 65 64 5f 5f  1c d9 3e 49 bd e1 6b f7  |Salted__..>I..k.|
00000010  e3 7f df 1a 62 20 fc 42  c4 53 be bb 35 3c c8 1b  |....b .B.S..5<..|
00000020  3d a1 a8 75 68 d2 8f cd  89 49 4a d2 15 03 f7 0f  |=..uh....IJ.....|
00000030  78 d1 19 a9 ad f5 c1 3f  47 7e 1a 1c 79 3b f1 65  |x......?G~..y;.e|
00000040  e8 1a b8 db 22 93 26 4b  08 9d 94 56 ba 15 8f 63  |....".&K...V...c|
00000050  bc eb 87 ad 0f 8c ea 38  ac 5f 58 9e 66 bb 50 96  |.......8._X.f.P.|
00000060  80 fd 9d d8 bd 31 2a 22  6b 32 3e ba e5 ed f8 ff  |.....1*"k2>.....|
00000070  b8 08 92 71 c8 8a 95 d0  22 00 db 0a de 7d 65 67  |...q....".....}eg|
00000080  a4 71 89 36 c6 77 4f 68  b2 71 7f 2d bc 75 94 f8  |.q.6.wOh.q.-.u..|
00000090  c7 10 25 a0 fa 2b 97 52  10 ec 8f 6a 07 ef ac 37  |..%..+.R...j...7|
000000a0  f9 e6 dd 35 a7 8f 94 93  4c 3e e8 37 f4 6e 3f 55  |...5....L>.7.n?U|
```

```
000000b0  a7 57 74 a6 18 04 e3 46  e1 35 d2 06 3c 22 b7 99  |.Wt....F.5..<'..|
000000c0  07 86 b5 4e c2 69 03 6d  5f 0c a4 ee d8 6a d6 ec  |...N.i.m_....j..|
000000d0  9c 58 2c 16 b7 75 86 d9  34 33 93 d8 d1 11 cc 1a  |.X,..u..43......|
000000e0  ad 38 64 13 9d aa c4 67  cd ca 9e 1a f3 fb 50 d4  |.8d....g......P.|
000000f0  fa 82 8f 6e f8 96 e6 99  dc 02 f3 62 38 be 5d ed  |...n.......b8.].|
00000100  0e 3e 65 dc b0 74 7b 8e  a7 b3 8a 49 23 f5 f9 5b  |.>e..t{....I'..[|
00000110  55 98 33 49 d4 d1 77 e7  44 9d 6e 96 74 28 bb 94  |U.3I..w.D.n.t(..|
00000120  34 34 1e 1f d3 74 ea 03  04 fe 06 46 da a1 47 c9  |44...t.....F..G.|
00000130  50 bf 3f ea 80 22 68 46  ee 00 62 39 d7 2d fa 03  |P.?..'hF..b9.-..|
00000140  e3 8e d4 48 97 a0 06 a8  e4 b4 25 f2 de 3f 5b a1  |...H......%..?[.|
00000150  54 d4 3e 3e a7 59 81 52  62 54 ad 42 d7 bf db fe  |T.>>.Y.RbT.B....|
00000160  ed 26 61 b6 bf 5e f9 a8  54 f8 c6 bd 76 72 71 bd  |.'a..^..T...vrq.|
00000170  ca d9 5e 3b ee de 63 21  68 0c 6d 28 67 b2 85 84  |..^;..c!h.m(g...|
00000180  8c fb 98 41 75 c7 b4 d0  a0 ad fc 60 6e 15 50 b4  |...Au......`n.P.|
00000190  d0 7b 58 90 a0 0b 40 2e  1b 68 d6 ed 29 16 a4 18  |.{X...@..h..)...|
000001a0  17 ce b9 73 04 20 7f d7  81 7f ba 68 09 34 69 19  |...s. .....h.4i.|
000001b0  f0 88 b3 46 b2 3b ed 91  46 ac 83 90 66 92 e6 03  |...F.;..F...f...|
000001c0  8f bf 90 d1 ec d5 1e 0b  f2 5b d4 d9 c5 45 ec 1f  |.........[...E..|
000001d0  3b 89 0e 1f 28 98 67 2e  6f b9 3e 45 12 b0 3d 0e  |;...(.g.o.>E..=.|
000001e0  02 31 8f fd 0f d6 4b c8  88 e5 9e f8 40 6c a8 28  |.1....K.....@l.(|
000001f0  1a be 8d 9f 77 60 17 45  8d 83 c4 56 d9 dd 37 28  |....w`.E...V..7(|
00000200  eb a3 4c c0 f1 f9 50 b2  08 72 47 03 67 22 78 e9  |..L...P..rG.g.x.|
00000210  f6 24 fc 66 38 ef a9 5e  aa 39 4b 62 34 0e fe 62  |.$.f8..^.9Kb4..b|
00000220  58 b0 e1 da 73 73 6a f0  e4 fd b8 b3 3c 77 9d ce  |X...ssj.....<w..|
00000230  d3 71 e0 24 16 c0 83 b1  f7 6f 27 70 f3 a2 11 9e  |.q.$.....o'p....|
00000240  30 d9 86 3b 76 77 9f 04  1c ce b9 bb 47 f8 a2 c4  |0..;vw......G...|
00000250  72 8d c7 01 c2 e8 8c 5e  99 f8 26 06 80 cc d9 fb  |r......^..'.....|
00000260  8f 72 2d d7 fc b5 ce 3f  e2 d6 91 a7 cc ff 49 3f  |.r-....?......I?|
00000270  b1 51 bd 5b 45 c2 40 cf  23 14 50 d9 71 77 49 98  |.Q.[E.@...P.qwI.|
00000280  6c 3e 8d 85 64 30 bf 22  a5 53 4d 2e 69 2a 5d 12  |l>..d0..."SM.i*].|
00000290  90 d7 99 36 e9 0d 29 2d  f7 8d 6b f0 a5 64 ad 3b  |...6..)-..k..d.;|
000002a0  c7 f8 ee 07 8a b3 fc 5d  7d 40 80 02 49 75 82 32  |.......]}@..Iu.2|
000002b0  b4 6b 3a 40 71 ea a9 64  b7 50 17 a0 02 b4 08 44  |.k:@q..d.P.....D|
000002c0  ae 63 3b 30 08 d7 c8 d4  37 04 b4 25 ff f4 03 d4  |.c;0....7..%....|
000002d0  92 dc d4 b4 cb 9c da 85  cd 62 0c 07 63 f6 90 c1  |.........b..c...|
000002e0  12 e6 af a4 1c 2d b8 ae  65 92 9b 78 98 90 db 0e  |.....-..e..x....|
000002f0  e0 d8 1c 30 6b c3 17 1b  74 4e 14 98 b8 71 56 2a  |...0k...tN...qV*|
00000300  35 2f ea c8 54 58 cd e2  10 5f a0 80 5f 54 30 9d  |5/..TX..._..T0.|
00000310  9e d0 34 0a 86 7f 75 f4  f2 bb aa 30 36 e8 d9 eb  |..4...u....06...|
00000320  88 f2 70 30 17 03 c3 4d  65 ea 30 df bd 65 22 e4  |..p0...Me.0..e..|
00000330  b8 f9 f6 c5 8a 77 b8 99  01 2d 9f 0f 85 8e 6c 97  |.....w...-....l.|
00000340  1d ac 69 a1 b7 00 2e 13  6d 84 1a 5e a4 f1 72 66  |..i.....m..^..rf|
00000350  5f 64 54 06 19 e1 fe 0e  41 b6 22 1a 96 65 c4 21  |_dT.....A....e.!|
00000360  8e f1 fa 1c d7 b5 67 81  6a fb d1 10 70 c2 7e b8  |......g.j...p.~.|
00000370  12 bd f5 64 cb 33 4e ac  1a 62 68 65 45 ac d3 ad  |...d.3N..bheE...|
00000380  c3 15 50 f9 fe 0d 0f 42  0e b6 0d 09 d9 b4 45 e6  |..P....B......E.|
00000390  bb 30 16 e6 4f 13 37 8b  6d 49 f1 39 a9 a2 91 ee  |.0..O.7.mI.9....|
000003a0  33 b4 8a 7c 0e 78 00 bd  d5 51 fc 71 b6 c9 d6 99  |3..|.x...Q.q....|
000003b0  b2 4b e8 77 e4 7d 51 6f  89 b9 e6 4c d4 d9 97 f4  |.K.w.}Qo...L....|
000003c0  2d 3a 72 78 7b db 7e 37  fb 9e 0d 9d 1c 0a 96 7f  |-:rx{.~7........|
000003d0  bd f9 1b 71 40 f6 38 30  69 4f c6 5e f7 0c 53 d4  |...q@.80iO.^..S.|
000003e0  70 68 4d cd a4 d3 ba c4  26 65 56 b7 40 1a af c6  |phM.....'eV.@...|
000003f0  3c 1c 6c 74 87 9e af 59  b7 a1 53 72 9f 8a 6c f8  |<.lt...Y..Sr..l.|
00000400  0b a8 f3 af 65 4c 3d f4  9d 78 57 da ef 04 ef e9  |....eL=..xW.....|
00000410  f2 9a 62 0f 2b 0e 23 51  bc 9d f2 4e c7 b8 e2 b1  |..b.+..Q...N....|
00000420
```

4.3. Modo OFB

```
[usuario@portatil:~]$ openssl enc -aes-128-ofb -iv 0123456789abcdef -pass pass:mipass -in
    /tmp/imput.bin -out /tmp/imput_aes128_ofb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes128_ofb.enc
00000000  53 61 6c 74 65 64 5f 5f  9f 21 4a 48 44 47 05 0a  |Salted__.!JHDG..|
00000010  f7 d9 cf 15 73 70 b8 b7  b4 f2 ad 08 ed 81 97 04  |....sp..........|
00000020  ba ee 57 c3 58 8a 46 3d  0f b8 f0 67 4c fa aa 8f  |..W.X.F=...gL...|
00000030  e3 85 92 9f d0 6f da 50  5d 83 42 e1 f3 b4 70 d1  |.....o.P].B...p.|
00000040  eb 70 7a 70 17 61 3d f2  ff 96 02 d7 65 a6 98 1d  |.pzp.a=.....e...|
00000050  d1 53 40 99 b5 f3 62 7f  c0 63 bf f2 3f 7d 70 f7  |.S@...b..c..?}p.|
00000060  6b a6 45 84 01 4a dd fc  af d2 02 33 10 15 08 6c  |k.E..J.....3...l|
00000070  48 f1 10 23 ba 5c da 3c  0d 75 a8 a5 59 22 dd a3  |H......<.u..Y'..|
00000080  8a 27 25 b7 09 89 4b 37  f4 23 49 55 bb 61 e0 23  |.'%...K7..IU.a.'|
```

```
00000090  20 39 15 54 bf 7e 14 20  7c 43 ff ee 59 d7 a2 e3  | 9.T.~. |C..Y...|
000000a0  72 0c 6c fa 4c db 43 f1  88 8c 82 f3 6f 2c 45 25  |r.l.L.C.....o,E'|
000000b0  71 75 a8 aa a0 4b bc 73  c1 dd 17 87 24 69 3d 77  |qu...K.s....$i=w|
000000c0  b6 26 aa 11 dd ac 92 78  29 60 ea f2 3f 72 2c 0d  |.'.....x)`..?r,.|
000000d0  cc 23 7e 1e 22 93 b5 c4  31 4f 6d 4b 59 46 84 e9  |..~.'...1OmKYF..|
000000e0  8c f5 37 1b e4 5f 6e 34  66 5d f8 e0 1c d7 a0 6a  |..7.._n4f].....j|
000000f0  00 e7 54 c8 d3 63 7d be  6d ae 14 84 f4 d7 aa bd  |..T..c}.m.......|
00000100  c1 70 b1 f6 19 ee 41 12  1a 3b 95 98 50 3a 85 d4  |.p....A..;..P:..|
00000110  f9 a9 65 b1 84 c4 cc 83  cf 10 35 08 a1 af 8a cd  |..e.......5.....|
00000120  50 d7 62 a9 23 29 3f 49  d3 57 8c 56 04 0f 9a 9f  |P.b..)?I.W.V....|
00000130  c8 31 1c 8d 2a be 2a 99  fe 10 6b 63 a9 8c 20 cd  |.1..*.*...kc.. .|
00000140  48 f1 af d2 18 b0 d7 4d  f8 7d 3e c0 78 78 65 32  |H.......M.}>.xxe2|
00000150  90 2e c9 f9 ab ed 7d 10  80 45 5c 52 a9 53 f8 42  |......}..E...S.B|
00000160  ca d4 88 4b e8 7e 85 a6  eb 47 33 e5 f0 40 aa d7  |...K.~...G3..@..|
00000170  5e c2 7b 23 e2 9e 75 ab  e2 9d 86 07 a3 7e de b8  |^.{'..u......~..|
00000180  f5 6a 5b a9 88 af 28 9a  63 98 5b 08 13 48 e2 64  |.j[...(.c.[..H.d|
00000190  4e 0e ac 62 79 1f 1a 90  5c 8b 80 f0 f4 2d 27 7b  |N..by...\....-'{|
000001a0  b1 a7 87 aa 45 f3 5d 13  a0 ef 18 a1 46 88 35 b6  |....E.].....F.5.|
000001b0  54 39 98 7c d4 99 7d 93  d8 e9 97 54 1e 38 67 b8  |T9.|..}....T.8g.|
000001c0  ff cb f1 4b 6f 25 c8 79  e6 40 fc 6a 6b 94 d3 10  |...Ko%.y.@.jk...|
000001d0  24 07 1f ab b9 ae c3 ff  cd 2e c9 21 68 e0 56 86  |$..........!h.V.|
000001e0  1e af 02 a3 c9 e3 9d af  59 b2 f9 a7 ce 33 ff 7e  |........Y....3.~|
000001f0  87 59 7a a5 94 51 ec 61  98 5d 11 7c c9 7e c7 92  |.Yz..Q.a.].|.~..|
00000200  25 fb 09 b5 92 ac d0 05  ea cc c1 11 a3 a9 6c 26  |%.............l'|
00000210  34 87 4b 41 12 45 17 11  2c 5e c2 44 94 2b 11 4f  |4.KA.E..,^.D.+.O|
00000220  fe 59 df 7b e7 f1 0b 70  5e d3 91 71 6f c1 bc 39  |.Y.{...p^..qo..9|
00000230  38 4f 30 95 5b 55 2e c6  38 2d cf 5d 8b 31 9e 38  |8O0.[U..8-.].1.8|
00000240  d2 ed 06 6d 69 07 c9 9d  93 c8 52 e2 e5 82 bf b9  |...mi.....R.....|
00000250  3f e8 1c 78 e5 0c af 10  0e 40 e4 b7 59 0a 3e 5a  |?..x.....@..Y.>Z|
00000260  8f 94 83 89 2d 2d 99 66  7e f9 fa 8a ed 69 48 15  |....--.f~....iH.|
00000270  fb 8e 24 9a 5e 64 ec 62  74 77 02 4c 79 5a 9b 8b  |..$.^d.btw.LyZ..|
00000280  a4 f3 3d 8d bd df 1f 7c  c5 c6 67 e3 67 1b d5 51  |..=....|..g.g..Q|
00000290  06 3e 6a ac bb 4f 1d 30  a1 61 92 cc 54 bd d3 d5  |.>j..O.0.a..T...|
000002a0  d0 76 b2 be 97 38 8b 34  00 40 4c 75 a7 a6 a3 80  |.v...8.4.@Lu....|
000002b0  26 ec 5e ca 2d 94 14 37  17 06 3c e6 c5 dd dc c7  |..^.-..7..<.....|
000002c0  90 9d af 34 e8 59 fb 7c  5e ab 10 b0 82 2c ac 2a  |...4.Y.|^....,.*|
000002d0  b7 95 b3 29 a3 c1 a2 8f  48 13 54 0d a1 2a cd 68  |...)....H.T..*.h|
000002e0  af 3b 0c a2 62 39 31 01  46 ad 5b 82 b0 94 5c 49  |.;..b91.F.[....I|
000002f0  bb a1 1f f2 c9 b6 0c 22  08 19 40 4d 52 dd cf fb  |.......'..@MR...|
00000300  c1 39 cd fb fd 73 50 5b  78 62 15 fb f4 cd 42 19  |.9...sP[xb....B.|
00000310  37 34 19 85 b2 77 b4 42  87 44 ce d6 84 b4 6c f0  |74...w.B.D....l.|
00000320  c2 0a 99 a7 3e dd 7c 7c  41 5b d9 41 1a af 70 f1  |....>.||A[.A..p.|
00000330  72 8e b7 ce b9 2f 08 b4  d0 86 f8 87 20 44 14 d8  |r..../...... D..|
00000340  71 c5 eb 33 ec 4b bf 8f  15 67 b4 58 cb 0e 7c f8  |q..3.K...g.X..|.|
00000350  cd 70 7c b8 3d 0c 4e 5f  15 a8 64 84 a2 5a 20 5e  |.p|.=.N_..d..Z ^|
00000360  ca e7 5d 57 06 0e 6f 6d  d2 ba 9e 6e 50 d7 cd 6e  |..]W..om...nP..n|
00000370  c4 12 43 fe c7 ed e4 b3  b1 96 9f 9e 51 5a 35 6c  |..C.........QZ5l|
00000380  d9 be 75 44 3e 02 a7 e1  4e ac 2f db 4e c1 5c 80  |..uD>...N./.N.\.|
00000390  1b 0a 3d ab 38 7f 8a de  bf 36 d6 d8 fe db 89 d3  |..=.8....6......|
000003a0  61 4e f6 2b 3e 5c 83 c4  2e 1a ad 1f 5c c6 68 64  |aN.+>\......\.hd|
000003b0  00 8b 10 3f fc fc ef c1  a5 4a c8 5b e2 a0 23 10  |...?.....J.[..'.|
000003c0  89 0e b8 95 88 cb 5f 6e  26 85 37 5f be 75 7c f1  |......_n..7_.u|.|
000003d0  bc 02 dd 68 60 53 5c ab  38 e2 94 80 40 66 a5 6e  |...h`S\.8...@f.n|
000003e0  ae 9a d8 6e fd d5 3e 16  f4 b4 15 bc 6d ab 5d be  |...n..>.....m.].|
000003f0  6f 6c 73 21 09 33 a4 db  ce a5 0e be 37 1d 81 e6  |ols!.3......7...|
00000400  b6 c6 5a f4 ee d2 63 68  a7 26 e7 2b c1 79 57 96  |..Z...ch...+.yW.|
00000410
[usuario@portatil:~]$ openssl enc -aes-128-ofb -iv 0123456789abcdef -pass pass:mipass -in
     /tmp/imput1.bin -out /tmp/imput1_aes128_ofb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes128_ofb.enc
00000000  53 61 6c 74 65 64 5f 5f  fa 99 44 f0 c2 ff ed 87  |Salted__..D.....|
00000010  20 b8 16 2d 11 c1 10 b6  67 6e 01 81 0d 1b 9b 6d  | ..-....gn.....m|
00000020  d3 45 64 6c 29 67 49 5d  a2 ea 42 58 dd 16 eb 21  |.Edl)gI]..BX...!|
00000030  05 a6 1e 97 59 0e 6a b5  4f ae 1a 42 be 87 ab 1d  |....Y.j.O..B....|
00000040  58 89 c0 d1 27 9b 4d 46  ad fe 3c 95 ea 1a 90 b2  |X...'.MF..<.....|
00000050  1f bb 72 62 0c 8b 8f 1a  6e 77 24 ee 8a a3 13 36  |..rb....nw$....6|
00000060  47 d8 2c 2e 5a 8a 55 4a  01 f1 f3 a6 08 71 69 22  |G.,.Z.UJ.....qi'|
00000070  9a fe 41 4a 2f 0f dd 94  62 27 59 02 1b d0 98 f1  |..AJ/...b'Y.....|
00000080  e1 cb 08 e1 05 fe b7 a9  62 e4 8c fc 9b 1e 4d 2b  |........b.....M+|
00000090  3a 35 f2 82 32 3d 37 12  c9 01 2e ff 1b 3c bb fb  |:5..2=7......<..|
000000a0  5e f5 df 10 b1 41 c7 29  c4 d7 f3 d1 ec 13 c7 86  |^....A.)........|
000000b0  ff 08 34 7c 02 f3 3f b6  bd e6 40 6f 5c 7b 2c 80  |..4|..?...@o\{,.|
000000c0  f5 93 5f 02 4f 82 fa b3  80 97 c5 d8 c1 86 48 ed  |.._.O.........H.|
000000d0  09 96 8a 8c 78 eb 14 c9  12 e9 fa 83 55 44 fc ac  |....x.......UD..|
000000e0  17 7e 04 e4 a8 db 8b 07  3e 99 0b 8c 78 69 69 ad  |.~......>...xii.|
```

```
000000f0  68 79 50 f7 ee ff da 5a  74 8f db 4c d3 91 8f 6a  |hyP....Zt..L...j|
00000100  ee 85 d1 7a f9 e4 94 6e  95 c4 00 1d 73 a1 a9 0d  |...z...n....s...|
00000110  4c 3a 38 83 33 f2 a7 71  7d 9f c0 e3 a6 da d6 15  |L:8.3..q}.......|
00000120  0b cc fd 7c fe 8e f4 28  5b 91 df 7e 34 56 1f 56  |...|...([..~4V.V|
00000130  93 ba 9d 0f 53 13 3c 9c  57 d6 06 79 8c 11 e7 36  |....S.<.W..y...6|
00000140  69 48 5c e1 10 00 33 d3  07 d4 db 72 84 d4 94 d5  |iH\...3....r....|
00000150  4d 8c 2f 3b f8 22 b5 80  10 9b 5b e9 26 55 95 73  |M./;."....[..U.s|
00000160  27 bb 25 db e1 22 d7 fd  b0 6e 07 8d d3 48 e2 8c  |'.%.."...n...H..|
00000170  da 87 3e 48 21 ad d2 54  3c 5d 08 4f 4a 53 c1 32  |..>H!..T<].OJS.2|
00000180  85 44 30 84 d5 c1 96 a9  42 15 9e c5 4e 3d 45 5c  |.D0.....B...N=E\|
00000190  5f a5 7b 85 9f fd 1a 0b  79 3a fb 1a 97 8e 85 30  |_.{.....y:.....0|
000001a0  d9 11 27 6b 84 a4 44 87  ff d8 97 bc 8d 11 d4 bb  |..'k..D.........|
000001b0  db 3a a0 65 41 a7 76 f0  05 dd 76 2e d8 b0 10 50  |.:.eA.v...v....P|
000001c0  f5 5e 2f b1 63 ae 8b b9  9c 6e 58 5f c4 9d 4a 88  |.^/.c....nX_..J.|
000001d0  7d 30 fe 87 80 d7 08 6c  39 af 2e a5 05 a2 6a c3  |}0.....l9.....j.|
000001e0  d7 52 0c c9 00 2e 34 73  2d df 5b 70 c6 8a 75 0d  |.R....4s-.[p..u.|
000001f0  fa 8c da e4 03 0d 59 fd  6e f2 60 52 1f 4b cb fe  |......Y.n.`R.K..|
00000200  25 2f 79 b9 91 48 7a b0  4f 89 ba 62 af 0f 7a 6e  |%/y..Hz.O..b..zn|
00000210  81 44 37 99 dd 94 f0 39  22 34 0f 06 e1 f6 2a 7b  |.D7....9"4....*{|
00000220  b2 b4 14 60 8d 78 c4 c1  e4 e2 3a 70 dd 02 27 c0  |...`.x....:p..'.|
00000230  5b 85 f0 f1 7e 7d 0a f4  11 d2 64 ab 82 1a 3e 5d  |[...~}....d...>]|
00000240  b3 09 d9 e1 2f 5b 6c e3  df 42 9f 6d 7a 8c b7 e9  |..../[l..B.mz...|
00000250  ea 58 e8 c7 19 96 60 63  c5 82 20 86 65 96 95 a6  |.X....`c.. .e...|
00000260  2f bb 4a c1 91 1e 9b 5f  e3 87 6e 13 06 5f de 70  |/.J...._..n.._.p|
00000270  6b e3 8f 6c 2e 48 36 ee  94 24 a1 7e 8a 29 03 13  |k..l.H6..$.~.)..|
00000280  53 b1 e0 11 e2 5a 69 ec  ea e4 af ae e3 bf e8 0a  |S....Zi.........|
00000290  36 a3 34 3c 76 43 f2 ff  5c 65 69 71 b8 91 14 35  |6.4<vC...eiq...5|
000002a0  d2 63 3a b5 fc c1 b2 41  cc f4 8d 2b 4d 3f cd 85  |.c:....A...+M?..|
000002b0  5a 53 6a e9 a5 66 b3 cc  a1 aa f3 a0 8e b6 c0 57  |ZSj..f.........W|
000002c0  cc 3a f0 8d 4b 9a 8f 52  ff a1 50 aa ec 7b 24 cf  |.:..K..R..P..{$.|
000002d0  71 d0 8d be 4f 89 6d 67  fa 94 75 41 8f e7 77 9f  |q...O.mg..uA..w.|
000002e0  d7 1d 07 d5 95 29 92 b5  22 8d 9b c4 66 8d fb 92  |.....)..".../...|
000002f0  f9 84 14 dd 6c 44 37 a0  3c 8b c0 9a 02 5d 3c 70  |....lD7.<....]<p|
00000300  c7 78 12 dc 84 47 d6 95  6a 66 24 09 7d a7 26 eb  |.x...G..jf$.}.'.|
00000310  52 a7 d8 1a 42 12 be b0  e6 fd 67 26 ae 00 7f ed  |R...B.....g'....|
00000320  6a 55 23 37 cb aa 6c fe  08 82 29 f9 ba ff 2b 0b  |jU.7..l...)...+.|
00000330  0b 94 1a a8 fd 5a cb a3  4b 7e e5 73 ff 5f 69 d8  |.....Z..K~.s._i.|
00000340  2e 63 76 57 af d6 b2 60  61 b7 76 70 5d f5 79 24  |.cvW...`a.vp].y$|
00000350  a8 e9 93 a0 b0 fe 27 d2  5a c2 ff 8e 65 d0 af 3a  |......'.Z...e..:|
00000360  cf 2b ee db ef 96 83 e9  65 6c 55 06 6b 9b 4c 53  |.+......elU.k.LS|
00000370  d0 bd 3f b5 a3 4f f5 c3  02 f2 aa a1 8f 8e 3a 7b  |..?..O........:{|
00000380  0d 4f 03 b1 e5 06 06 65  b4 b3 0f a0 7d e8 50 80  |.O.....e....}.P.|
00000390  64 4b f5 34 36 60 35 96  dd 33 17 0e 60 9a fa c5  |dK.46`5..3..`...|
000003a0  8c 3c b6 e9 3e 87 29 21  7c 0a 18 01 82 f0 ec 44  |.<..>.)!|......D|
000003b0  a1 d5 6b d8 62 f1 b5 c2  95 1d 11 23 80 4e 5f 38  |..k.b......'.N_8|
000003c0  4d 5c dc b6 74 1b d0 96  ea 9f 92 ae b4 2f 9a 8a  |M\..t......../..|
000003d0  b9 a2 07 3c 38 2e 43 78  af 0b aa af 41 87 22 6f  |...<8.Cx....A."o|
000003e0  d1 f2 c6 bb 26 34 e5 0b  05 e6 25 61 ff 77 f2 05  |.....4....%a.w..|
000003f0  73 c1 4f 6a 0f fd 51 c9  93 d2 56 11 d0 3b 5b e1  |s.Oj..Q...V..;[.|
00000400  bd bb ae c5 cc 9e 1b 37  14 87 e4 63 3f 5b a7 d3  |.......7...c?[..|
00000410
```

En esta ocasión, con este algoritmo de cifrado se puede apreciar que openssl añade por defecto una cadena aleatoria, esto se puede apreciar en los primeros bits del fichero cifrado, aparte de esto la manera de cifrar es diferente en cuanto cambia un solo bit del fichero de entrada, a diferencia de los algoritmos anteriores.

Tambien hay que tener en cuenta que el algoritmo es independiente de los modos de cifrado que utilicemos, ya que el resultado de los ficheros cifrados varia siempre en cada modo y con cada fichero de entrada.

5. Repetir el punto anterior con la opción -nosalt.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

5.1. Modo ECB

```
[usuario@portatil:~]$ openssl enc -aes-128-ecb -pass pass:mipass -nosalt -in /tmp/imput.
    bin -out /tmp/imput_aes128_ecb.enc
```

```
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes128_ecb.enc
00000000  97 5e da c1 cd 03 e1 95  fb a5 84 88 8f 76 9b 42  |.^...........v.B|
*
00000400  a3 ed ff 8d aa 37 0e 32  9f 6a be 82 c9 8e 59 46  |.....7.2.j....YF|
00000410
[usuario@portatil:~]$ openssl enc -aes-128-ecb -pass pass:mipass -nosalt -in /tmp/imput1.
    bin -out /tmp/imput1_aes128_ecb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes128_ecb.enc
00000000  97 5e da c1 cd 03 e1 95  fb a5 84 88 8f 76 9b 42  |.^...........v.B|
*
00000080  41 6a 01 44 74 68 3b 2d  e4 ce dd 2a 2c 7f 81 39  |Aj.Dth;-...*,..9|
00000090  97 5e da c1 cd 03 e1 95  fb a5 84 88 8f 76 9b 42  |.^...........v.B|
*
00000400  a3 ed ff 8d aa 37 0e 32  9f 6a be 82 c9 8e 59 46  |.....7.2.j....YF|
00000410
```

5.2. Modo CBC

```
[usuario@portatil:~]$ openssl enc -aes-128-cbc -iv 0123456789abcdef -pass pass:mipass -
    nosalt -in /tmp/imput.bin -out /tmp/imput_aes128_cbc.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes128_cbc.enc
00000000  d7 92 75 83 6c 42 13 8c  1c 51 3e 38 66 02 75 bd  |..u.lB...Q>8f.u.|
00000010  86 39 49 11 50 5e e3 69  9c 4a 3e cc d4 8a 09 d6  |.9I.P^.i.J>.....|
00000020  de ca d3 3d 0a b6 6e 7e  d5 b7 d8 d1 a1 50 8b 24  |...=..n~.....P.$|
00000030  5f 18 27 ac 1b 86 27 7b  55 0e 5b 6e a8 66 ad dc  |_.'...'{U.[n.f..|
00000040  5b ba 6a 6d 34 ef c4 52  f8 31 1f 9c e5 53 27 90  |[.jm4..R.1...S'.|
00000050  30 a8 1e 6e c6 65 cc d1  af 39 c9 63 99 7b e8 dc  |0..n.e...9.c.{..|
00000060  28 9c 2e 2f 04 8e ed 66  52 36 24 95 ad 12 16 42  |(../...fR6$....B|
00000070  ad 56 d0 36 bc fc ac a5  bb 82 f5 f7 0b e5 b3 f0  |.V.6............|
00000080  8a 87 c2 de a0 a9 c7 4c  6d 09 ea 74 d6 1f 17 21  |.......Lm..t...!|
00000090  3b e3 53 f0 89 ac fd 24  f4 c7 57 e2 f8 6b bf a5  |;.S....$..W..k..|
000000a0  88 d7 33 75 6d 47 67 d1  b2 99 6d 61 20 d8 6d 25  |..3umGg...ma .m%|
000000b0  a4 a3 0a 29 3a 56 ba fe  2b 4a 4e c2 d6 b6 5c bf  |...):V..+JN...\.|
000000c0  12 db 1e b9 bd 4d c0 1a  10 3e 33 83 ac 6e 6c 53  |.....M...>3..nlS|
000000d0  ea 30 fe 9b 3b 49 78 51  aa 35 e2 c1 93 c3 1d 14  |.0..;IxQ.5......|
000000e0  c4 87 12 c9 3b c8 38 93  4e 37 d1 a1 d3 41 0d 22  |....;.8.N7...A..|
000000f0  8b 0f 17 90 a7 9e d0 ab  f3 e2 1c 2e 21 61 b7 44  |............!a.D|
00000100  2c 10 62 d7 47 15 5f a7  ec 02 41 13 37 1b 0d 45  |,.b.G._...A.7..E|
00000110  70 c8 3d 5e 02 68 02 68  30 13 1d 97 f4 67 a4 df  |p.=^.h.h0....g..|
00000120  70 46 8d 0b a1 57 6f 0e  87 a3 39 61 91 72 df 50  |pF...Wo...9a.r.P|
00000130  6f 71 14 ee e8 a1 d2 0d  cb c9 8e f2 37 c5 2e b7  |oq..........7...|
00000140  2f 76 6a 39 02 68 36 27  9c c0 49 e9 49 7f d1 6d  |/vj9.h6'..I.I..m|
00000150  52 e1 7c 64 d8 ec be a7  2a 9d 34 2d 72 f6 55 17  |R.|d....*.4-r.U.|
00000160  3a 58 dd d7 c3 a1 cf 1d  fc c5 97 e9 fc 78 49 18  |:X...........xI.|
00000170  61 52 95 eb b9 d3 df 89  6b f3 ac 74 5f 8d 61 00  |aR......k..t_.a.|
00000180  ab c6 23 f5 12 32 2b 88  fd 83 52 e7 15 65 ad 2b  |.....2+...R..e.+|
00000190  77 95 c3 4a 29 d2 b5 84  dd cb 58 b4 a4 1f 2c 5a  |w..J).....X...,Z|
000001a0  66 40 a2 46 04 72 b6 d5  2d be 1e b0 a7 55 e0 a8  |f@.F.r..-....U..|
000001b0  89 b2 d5 9a e4 00 ca a0  39 38 5e 85 f6 c1 a5 77  |........98^....w|
000001c0  a9 a0 17 98 a9 12 15 d7  c5 af 0f 18 5d 6e a6 cc  |............]n..|
000001d0  66 c4 45 3f 93 08 f6 2a  e6 89 ea ef e4 d2 8d a0  |f.E?...*........|
000001e0  e1 bd fa 87 27 e6 d0 32  09 ea 09 74 70 b9 89 76  |....'..2...tp..v|
000001f0  f9 83 d1 a4 e9 00 44 a4  a5 9b 24 cf db 29 c5 3c  |......D...$..).<|
00000200  86 1e 8b d4 f9 5d 66 b8  1b 0d 20 ff 58 14 65 ba  |.....]f... .X.e.|
00000210  01 dd d2 f6 cb 4f 7e a0  53 0c 74 a2 fd 05 84 4a  |.....O~.S.t....J|
00000220  46 86 90 2a 0a 69 51 aa  91 c5 bd 26 e9 1a 63 80  |F..*.iQ....&..c.|
00000230  c9 31 08 cd 32 ab 68 f0  8a 52 df a9 7d ac 1f de  |.1..2.h..R..}...|
00000240  bb da a7 c8 7a 88 45 56  f8 07 e0 6b db 38 8d 8e  |....z.EV...k.8..|
00000250  81 1d 33 04 9c 0a 31 3a  9f 24 e1 8f 04 d6 3c 2d  |..3...1:.$....<-|
00000260  96 c6 b1 3a 97 54 f3 cc  5e a4 16 e3 88 c8 84 0f  |...:.T..^.......|
00000270  82 ec ad 8c 95 a8 e5 16  17 75 4c 8e 7b 8d c1 d3  |.........uL.{...|
00000280  66 c4 ca af 01 14 f2 ff  39 f6 b8 07 e5 40 df c0  |f.......9....@..|
00000290  1e d1 21 ae b3 4c 30 52  2d 31 af 3a 07 a3 5f c8  |..!..L0R-1.:.._.|
000002a0  66 3c 54 a3 77 d6 23 ac  0f 81 8d 15 84 54 1d de  |f<T.w.#......T..|
000002b0  35 d1 97 f2 c6 47 ef be  81 d3 cd 1d 57 00 7a 87  |5....G......W.z.|
000002c0  23 b8 98 3f 19 42 66 63  f5 71 54 4d 46 98 80 7e  |...?.Bfc.qTMF..~|
000002d0  4c 91 59 c7 a3 70 c4 51  74 bb c6 33 01 23 2d ad  |L.Y..p.Qt..3..-.|
000002e0  6d 5c 6f 9f 46 95 d8 7c  b0 0d 54 10 3e f7 39 f8  |m\o.F..|..T.>.9.|
000002f0  a4 cc 3e 6f b5 48 72 b7  18 32 97 9c c8 87 92 bf  |..>o.Hr..2......|
00000300  43 bc 1c 03 77 3f 3c bd  79 ed c4 1d e4 24 a9 fb  |C...w?<.y....$..|
00000310  63 a5 d6 f1 d9 f2 8a df  c9 0a 47 c3 2e bc 69 da  |c.........G...i.|
```

```
00000320  6f 47 eb d7 3a 62 19 ba  87 1e ce 77 a3 15 44 ea  |oG..:b.....w..D.|
00000330  ef 7f 77 c6 14 c5 bb a6  8d e5 f1 32 af b3 93 80  |..w........2....|
00000340  09 1d 48 82 86 b3 89 1b  74 40 bd 6e 39 c6 a2 94  |..H.....t@.n9...|
00000350  b2 7d 8a d2 7e e9 ec d8  66 9f a5 e4 e7 b8 6b 95  |.}..~...f.....k.|
00000360  91 93 d9 67 47 94 8d 5d  b3 cd c4 ee 01 b5 67 39  |...gG..]......g9|
00000370  55 7f bc 47 0c 0d be 0e  9e c6 df c6 75 45 7e e1  |U..G........uE~.|
00000380  94 d3 e3 2e 14 ad ae 1e  2d 26 ff 8c ca bc c3 cc  |........-&......|
00000390  ef 3e f4 3a d7 25 a0 87  d5 f8 9b fa 45 1e bd 38  |.>.:.%......E..8|
000003a0  62 b6 1f cb 68 2a 8c 67  fd ff 44 6a 78 44 b2 35  |b...h*.g..DjxD.5|
000003b0  54 47 3d f4 d7 45 04 52  9e b8 49 e1 2c 48 4d d9  |TG=..E.R..I.,HM.|
000003c0  78 c7 c8 36 93 f5 e3 e4  91 8f 11 19 06 7d f0 6c  |x..6.........}.l|
000003d0  b7 a4 17 ae 60 72 df fd  19 b4 9b 81 d0 9b 1e f8  |....`r..........|
000003e0  cb 1d 8a fa 96 28 23 db  82 14 ff 85 69 1b da b9  |.....(......i...|
000003f0  d9 f0 8a 88 ca ae cb 42  dd b9 5f e6 3c 88 67 a8  |.......B.._.<.g.|
00000400  d1 bf 79 48 9a ca 42 2b  93 5d 5c ba f3 89 87 78  |..yH..B+.]\....x|
00000410
[usuario@portatil:~]$ openssl enc -aes-128-cbc -iv 0123456789abcdef -pass pass:mipass -
    nosalt -in /tmp/imput1.bin -out /tmp/imput1_aes128_cbc.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes128_cbc.enc
00000000  d7 92 75 83 6c 42 13 8c  1c 51 3e 38 66 02 75 bd  |..u.lB...Q>8f.u.|
00000010  86 39 49 11 50 5e e3 69  9c 4a 3e cc d4 8a 09 d6  |.9I.P^.i.J>.....|
00000020  de ca d3 3d 0a b6 6e 7e  d5 b7 d8 d1 a1 50 8b 24  |...=..n~.....P.$|
00000030  5f 18 27 ac 1b 86 27 7b  55 0e 5b 6e a8 66 ad dc  |_.'...'{U.[n.f..|
00000040  5b ba 6a 6d 34 ef c4 52  f8 31 1f 9c e5 53 27 90  |[.jm4..R.1...S'.|
00000050  30 a8 1e 6e c6 65 cc d1  af 39 c9 63 99 7b e8 dc  |0..n.e...9.c.{..|
00000060  28 9c 2e 2f 04 8e ed 66  52 36 24 95 ad 12 16 42  |(../...fR6$....B|
00000070  ad 56 d0 36 bc fc ac a5  bb 82 f5 f7 0b e5 b3 f0  |.V.6............|
00000080  5c de b0 db e5 d9 81 dd  42 39 14 cf a1 67 57 bc  |\.......B9...gW.|
00000090  35 42 96 cb 95 f1 33 6f  93 c7 42 dd 4f b4 69 16  |5B....3o..B.O.i.|
000000a0  4d ec 90 cb 91 f0 b6 a7  1e 13 7c 77 cc 9c 09 60  |M.........|w...`|
000000b0  b0 85 68 fb 40 4f c1 e6  94 13 e8 39 a8 fd 9c 12  |..h.@O.....9....|
000000c0  a9 e7 93 d3 14 c4 6f 62  c1 ec 9b f6 c7 8a f8 e6  |......ob........|
000000d0  fd 10 af f9 1c 85 90 fa  7d 33 0b 54 20 7d f2 12  |........}3.T }..|
000000e0  a3 e1 21 67 03 16 2a e6  9f 44 c4 de 7b 60 e1 b4  |..!g..*..D..{`..|
000000f0  dc d2 00 e0 fb 79 97 c2  c8 56 78 3f ea ea cb b4  |.....y...Vx?....|
00000100  79 3c c3 ba 6f 62 13 10  64 9a 01 80 c4 64 fa 00  |y<..ob..d....d..|
00000110  03 de e9 3d 7a 4a 3f 60  b9 08 2d cf 7c 7e 8b 0e  |...=zJ?`..-.|~..|
00000120  ae e1 79 e8 82 8d 2d 33  00 ab 84 f8 d4 82 73 70  |..y...-3......sp|
00000130  96 fe a3 1e 1a 33 ce eb  98 44 db 4a d9 16 81 75  |.....3...D.J...u|
00000140  27 7e 06 7a 67 07 d8 a0  68 9d 3c c1 15 5b 8a 5f  |'~.zg...h.<..[._|
00000150  38 6d 4e 83 e2 90 3a 92  1c a2 e8 ca 1a cd 17 d0  |8mN...:.........|
00000160  16 17 9b 08 90 b6 5c d0  a5 f0 fc 0f 4e d5 81 b5  |......\.....N...|
00000170  12 30 3c 14 ba 22 1d ac  e6 b3 52 aa 03 c3 de 6e  |.0<.....R....n|
00000180  79 e0 a4 72 f5 89 ec 5d  37 b6 83 fd ac e7 f7 ab  |y..r...]7.......|
00000190  a6 23 b1 3f 30 40 b9 f6  f7 24 d9 50 9a 51 14 c2  |...?0@...$.P.Q..|
000001a0  27 68 26 5c eb d0 47 53  08 d5 38 ed 45 29 6a fc  |'h&\..GS..8.E)j.|
000001b0  99 56 73 3f d6 0c bf 59  b4 fb 21 31 e2 68 97 0d  |.Vs?...Y..!1.h..|
000001c0  3e 30 29 44 cb dd bc fd  34 17 39 12 e9 00 73 ea  |>0)D....4.9...s.|
000001d0  49 46 2c 0b 4c 6b 32 f3  05 d4 b1 bc 1b d3 01 e9  |IF,.Lk2.........|
000001e0  c7 20 b4 61 d9 3d 13 bb  d9 49 50 ab 0c 14 31 cf  |. .a.=...IP...1.|
000001f0  fb cf 96 ec a1 0f e4 db  f8 df 54 2d b6 e9 05 74  |..........T-...t|
00000200  ac 09 91 ce 0c 79 24 13  9a 61 d0 bb 71 da 22 3f  |.....y$..a..q..?|
00000210  2b 86 fc 7d 6f ee cf 6d  96 fd b8 27 1f 6f bf 93  |+..}o..m...'.o..|
00000220  78 a3 5a 36 8b 9e f5 6f  01 84 9e b3 cd fb 68 05  |x.Z6...o......h.|
00000230  e7 78 cb 79 29 8e b2 12  67 61 25 6e 41 a0 4f 19  |.x.y)...ga%nA.O.|
00000240  b3 34 32 e3 6a 99 95 99  d8 45 5c ae 08 6d 0f 9a  |.42.j....E\..m..|
00000250  63 86 02 92 ee 80 0a ef  94 ce bd a9 4e 4e 71 e0  |c...........NNq.|
00000260  f5 ce 50 0a f7 7b 17 8e  40 5e 05 02 48 f5 27 44  |..P..{..@^..H.'D|
00000270  1a 75 c8 77 41 d0 d9 cc  58 4d 56 fd fe c0 34 8c  |.u.wA...XMV...4.|
00000280  d9 e5 13 ba e0 0c 77 25  c7 ef 0b 83 4d 5b cb 6a  |......w%....M[.j|
00000290  5a 0f f8 59 11 2c 1c f6  01 df 7c 16 df 11 32 bf  |Z..Y.,....|...2.|
000002a0  25 07 67 c0 b9 96 0b 11  00 22 3c 88 ed 21 d2 f4  |%.g.......<..!..|
000002b0  e4 5a 6c 91 31 f2 90 41  cf 24 56 ab d0 26 0e e5  |.Zl.1..A.$V..&..|
000002c0  3c b5 8c cc 9e 9e 97 78  94 14 68 d1 97 64 9b 56  |<......x..h..d.V|
000002d0  a2 90 f7 41 5e 7a 6b 1a  17 84 fd d9 00 6d 0d 8c  |...A^zk......m..|
000002e0  7c 9d 75 3f e8 88 7d 83  bd d7 49 3e 62 63 94 a2  ||.u?..}...I>bc..|
000002f0  c8 bb ed d1 4d 04 45 5d  23 a8 f4 5e f4 33 85 c4  |....M.E]...^.3..|
00000300  d2 c2 61 16 e3 d3 f3 57  3d bd 9e b1 84 58 55 23  |..a....W=....XU.|
00000310  30 30 b2 ee 9e 62 ed f6  93 f3 0a 2d ef bc 1c 4d  |00...b.....-...M|
00000320  d7 1b 4c 56 da ea 86 b3  ff d6 f1 ca 7c a2 d7 80  |..LV........|...|
00000330  94 a9 2b 33 a2 a7 72 15  fa 40 fa cb d7 74 17 f6  |..+3..r..@...t..|
00000340  8b 7f b2 f5 ba 2a f2 57  bc 9f ff 2f 63 e1 cf 33  |.....*.W.../c..3|
00000350  25 d5 e9 ba 58 82 e2 87  f4 8a df 87 16 a3 ba 78  |%...X..........x|
00000360  5f 59 c0 7d 69 f8 53 0c  64 14 fc 7e 2f 34 88 69  |_Y.}i.S.d..~/4.i|
00000370  43 32 4d f4 40 b7 66 b8  aa ff 58 f5 ff f5 35 07  |C2M.@.f...X...5.|
```

```
00000380  da 77 a8 72 6e 0a 2c 8c  cb 33 c7 ff cc 90 f5 40  |.w.rn.,..3.....@|
00000390  3f c9 ae 59 36 94 60 46  b8 36 3f 46 da d7 39 b5  |?..Y6.‘F.6?F..9.|
000003a0  ef 78 78 41 1c f2 4f cb  ab 3a 2c b5 dd 19 b1 6e  |.xxA..O..:,....n|
000003b0  34 de 23 66 6e 3a ca 9f  11 e1 b6 20 af dd cf dc  |4..fn:..... ....|
000003c0  7e db 87 e4 c5 55 24 a9  72 70 3d 8d 6e 7a e1 fc  |~....U$.rp=.nz..|
000003d0  66 55 f5 cb 5e 4d 33 ce  ae 10 69 aa 07 c3 ee a8  |fU..^M3...i.....|
000003e0  19 fb ee f5 d7 8e fe cc  f6 4a 7a eb 6b 00 40 4e  |.........Jz.k.@N|
000003f0  13 93 29 36 52 2d e8 a8  35 fd 32 5f 86 f1 0d db  |..)6R-..5.2_....|
00000400  34 a5 9d b8 68 81 d7 c8  7d 50 b5 3c 2d 3f c4 ec  |4...h...}P.<-?..|
00000410
```

5.3. Modo OFB

```
[usuario@portatil:~]$ openssl enc -aes-128-ofb -iv 0123456789abcdef -pass pass:mipass -
    nosalt -in /tmp/imput.bin -out /tmp/imput_aes128_ofb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes128_ofb.enc
00000000  d7 92 75 83 6c 42 13 8c  1c 51 3e 38 66 02 75 bd  |..u.lB...Q>8f.u.|
00000010  86 39 49 11 50 5e e3 69  9c 4a 3e cc d4 8a 09 d6  |.9I.P^.i.J>.....|
00000020  de ca d3 3d 0a b6 6e 7e  d5 b7 d8 d1 a1 50 8b 24  |...=..n~.....P.$|
00000030  5f 18 27 ac 1b 86 27 7b  55 0e 5b 6e a8 66 ad dc  |_.’...’{U.[n.f..|
00000040  5b ba 6a 6d 34 ef c4 52  f8 31 1f 9c e5 53 27 90  |[.jm4..R.1...S’.|
00000050  30 a8 1e 6e c6 65 cc d1  af 39 c9 63 99 7b e8 dc  |0..n.e...9.c.{..|
00000060  28 9c 2e 2f 04 8e ed 66  52 36 24 95 ad 12 16 42  |(../...fR6$....B|
00000070  ad 56 d0 36 bc fc ac a5  bb 82 f5 f7 0b e5 b3 f0  |.V.6............|
00000080  8a 87 c2 de a0 a9 c7 4c  6d 09 ea 74 d6 1f 17 21  |.......Lm..t...!|
00000090  3b e3 53 f0 89 ac fd 24  f4 c7 57 e2 f8 6b bf a5  |;.S....$..W..k..|
000000a0  88 d7 33 75 6d 47 67 d1  b2 99 6d 61 20 d8 6d 25  |..3umGg...ma .m%|
000000b0  a4 a3 0a 29 3a 56 ba fe  2b 4a 4e c2 d6 b6 5c bf  |...):V..+JN...\.|
000000c0  12 db 1e b9 bd 4d c0 1a  10 3e 33 83 ac 6e 6c 53  |.....M...>3..nlS|
000000d0  ea 30 fe 9b 3b 49 78 51  aa 35 e2 c1 93 c3 1d 14  |.0..;IxQ.5......|
000000e0  c4 87 12 c9 3b c8 38 93  4e 37 d1 a1 d3 41 0d 22  |....;.8.N7...A..|
000000f0  8b 0f 17 90 a7 9e d0 ab  f3 e2 1c 2e 21 61 b7 44  |............!a.D|
00000100  2c 10 62 d7 47 15 5f a7  ec 02 41 13 37 1b 0d 45  |,.b.G._...A.7..E|
00000110  70 c8 3d 5e 02 68 02 68  30 13 1d 97 f4 67 a4 df  |p.=^.h.h0....g..|
00000120  70 46 8d 0b a1 57 6f 0e  87 a3 39 61 91 72 df 50  |pF...Wo...9a.r.P|
00000130  6f 71 14 ee e8 a1 d2 0d  cb c9 8e f2 37 c5 2e b7  |oq..........7...|
00000140  2f 76 6a 39 02 68 36 27  9c c0 49 e9 49 7f d1 6d  |/vj9.h6’..I.I..m|
00000150  52 e1 7c 64 d8 ec be a7  2a 9d 34 2d 72 f6 55 17  |R.|d....*.4-r.U.|
00000160  3a 58 dd d7 c3 a1 cf 1d  fc c5 97 e9 fc 78 49 18  |:X...........xI.|
00000170  61 52 95 eb b9 d3 df 89  6b f3 ac 74 5f 8d 61 00  |aR......k..t_.a.|
00000180  ab c6 23 f5 12 32 2b 88  fd 83 52 e7 15 65 ad 2b  |.....2+...R..e.+|
00000190  77 95 c3 4a 29 d2 b5 84  dd cb 58 b4 a4 1f 2c 5a  |w..J).....X...,Z|
000001a0  66 40 a2 46 04 72 b6 d5  2d be 1e b0 a7 55 e0 a8  |f@.F.r..-....U..|
000001b0  89 b2 d5 9a e4 00 ca a0  39 38 5e 85 f6 c1 a5 77  |........98^....w|
000001c0  a9 a0 17 98 a9 12 15 d7  c5 af 0f 18 5d 6e a6 cc  |............]n..|
000001d0  66 c4 45 3f 93 08 f6 2a  e6 89 ea ef e4 d2 8d a0  |f.E?...*........|
000001e0  e1 bd fa 87 27 e6 d0 32  09 ea 09 74 70 b9 89 76  |....’..2...tp..v|
000001f0  f9 83 d1 a4 e9 00 44 a4  a5 9b 24 cf db 29 c5 3c  |......D...$..).<|
00000200  86 1e 8b d4 f9 5d 66 b8  1b 0d 20 ff 58 14 65 ba  |.....]f... .X.e.|
00000210  01 dd d2 f6 cb 4f 7e a0  53 0c 74 a2 fd 05 84 4a  |.....O~.S.t....J|
00000220  46 86 90 2a 0a 69 51 aa  91 c5 bd 26 e9 1a 63 80  |F..*.iQ....’..c.|
00000230  c9 31 08 cd 32 ab 68 f0  8a 52 df a9 7d ac 1f de  |.1..2.h..R..}...|
00000240  bb da a7 c8 7a 88 45 56  f8 07 e0 6b db 38 8d 8e  |....z.EV...k.8..|
00000250  81 1d 33 04 9c 0a 31 3a  9f 24 e1 8f 04 d6 3c 2d  |..3...1:.$....<-|
00000260  96 c6 b1 3a 97 54 f3 cc  5e a4 16 e3 88 c8 84 0f  |...:.T..^.......|
00000270  82 ec ad 8c 95 a8 e5 16  17 75 4c 8e 7b 8d c1 d3  |.........uL.{...|
00000280  66 c4 ca af 01 14 f2 ff  39 f6 b8 07 e5 40 df c0  |f.......9....@..|
00000290  1e d1 21 ae b3 4c 30 52  2d 31 af 3a 07 a3 5f c8  |..!..L0R-1.:.._.|
000002a0  66 3c 54 a3 77 d6 23 ac  0f 81 8d 15 84 54 1d de  |f<T.w.#......T..|
000002b0  35 d1 97 f2 c6 47 ef be  81 d3 cd 1d 57 00 7a 87  |5....G......W.z.|
000002c0  23 b8 98 3f 19 42 66 63  f5 71 54 4d 46 98 80 7e  |...?.Bfc.qTMF..~|
000002d0  4c 91 59 c7 a3 70 c4 51  74 bb c6 33 01 23 2d ad  |L.Y..p.Qt..3..-.|
000002e0  6d 5c 6f 9f 46 95 d8 7c  b0 0d 54 10 3e f7 39 f8  |m\o.F..|..T.>.9.|
000002f0  a4 cc 3e 6f b5 48 72 b7  18 32 97 9c c8 87 92 bf  |..>o.Hr..2......|
00000300  43 bc 1c 03 77 3f 3c bd  79 ed c4 1d e4 24 a9 fb  |C...w?<.y....$..|
00000310  63 a5 d6 f1 d9 f2 8a df  c9 0a 47 c3 2e bc 69 da  |c.........G...i.|
00000320  6f 47 eb d7 3a 62 19 ba  87 1e ce 77 a3 15 44 ea  |oG..:b.....w..D.|
00000330  ef 7f 77 c6 14 c5 bb a6  8d e5 f1 32 af b3 93 80  |..w........2....|
00000340  09 1d 48 82 86 b3 89 1b  74 40 bd 6e 39 c6 a2 94  |..H.....t@.n9...|
00000350  b2 7d 8a d2 7e e9 ec d8  66 9f a5 e4 e7 b8 6b 95  |.}..~...f.....k.|
00000360  91 93 d9 67 47 94 8d 5d  b3 cd c4 ee 01 b5 67 39  |...gG..]......g9|
```

```
00000370  55 7f bc 47 0c 0d be 0e  9e c6 df c6 75 45 7e e1  |U..G........uE~.|
00000380  94 d3 e3 2e 14 ad ae 1e  2d 26 ff 8c ca bc c3 cc  |........-'......|
00000390  ef 3e f4 3a d7 25 a0 87  d5 f8 9b fa 45 1e bd 38  |.>.:.%......E..8|
000003a0  62 b6 1f cb 68 2a 8c 67  fd ff 44 6a 78 44 b2 35  |b...h*.g..DjxD.5|
000003b0  54 47 3d f4 d7 45 04 52  9e b8 49 e1 2c 48 4d d9  |TG=..E.R..I.,HM.|
000003c0  78 c7 c8 36 93 f5 e3 e4  91 8f 11 19 06 7d f0 6c  |x..6.........}.l|
000003d0  b7 a4 17 ae 60 72 df fd  19 b4 9b 81 d0 9b 1e f8  |....`r..........|
000003e0  cb 1d 8a fa 96 28 23 db  82 14 ff 85 69 1b da b9  |.....(......i...|
000003f0  d9 f0 8a 88 ca ae cb 42  dd b9 5f e6 3c 88 67 a8  |.......B.._.<.g.|
00000400
[usuario@portatil:~]$ openssl enc -aes-128-ofb -iv 0123456789abcdef -pass pass:mipass -
    nosalt -in /tmp/imput1.bin -out /tmp/imput1_aes128_ofb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput1_aes128_ofb.enc
00000000  d7 92 75 83 6c 42 13 8c  1c 51 3e 38 66 02 75 bd  |..u.lB...Q>8f.u.|
00000010  86 39 49 11 50 5e e3 69  9c 4a 3e cc d4 8a 09 d6  |.9I.P^.i.J>.....|
00000020  de ca d3 3d 0a b6 6e 7e  d5 b7 d8 d1 a1 50 8b 24  |...=..n~.....P.$|
00000030  5f 18 27 ac 1b 86 27 7b  55 0e 5b 6e a8 66 ad dc  |_.'...'{U.[n.f..|
00000040  5b ba 6a 6d 34 ef c4 52  f8 31 1f 9c e5 53 27 90  |[.jm4..R.1...S'.|
00000050  30 a8 1e 6e c6 65 cc d1  af 39 c9 63 99 7b e8 dc  |0..n.e...9.c.{..|
00000060  28 9c 2e 2f 04 8e ed 66  52 36 24 95 ad 12 16 42  |(../...fR6$....B|
00000070  ad 56 d0 36 bc fc ac a5  bb 82 f5 f7 0b e5 b3 f0  |.V.6............|
00000080  8a 87 c2 de a0 a9 c7 4d  6d 09 ea 74 d6 1f 17 21  |.......Mm..t...!|
00000090  3b e3 53 f0 89 ac fd 24  f4 c7 57 e2 f8 6b bf a5  |;.S....$..W..k..|
000000a0  88 d7 33 75 6d 47 67 d1  b2 99 6d 61 20 d8 6d 25  |..3umGg...ma .m%|
000000b0  a4 a3 0a 29 3a 56 ba fe  2b 4a 4e c2 d6 b6 5c bf  |...):V..+JN...\.|
000000c0  12 db 1e b9 bd 4d c0 1a  10 3e 33 83 ac 6e 6c 53  |.....M...>3..nlS|
000000d0  ea 30 fe 9b 3b 49 78 51  aa 35 e2 c1 93 c3 1d 14  |.0..;IxQ.5......|
000000e0  c4 87 12 c9 3b c8 38 93  4e 37 d1 a1 d3 41 0d 22  |....;.8.N7...A..|
000000f0  8b 0f 17 90 a7 9e d0 ab  f3 e2 1c 2e 21 61 b7 44  |............!a.D|
00000100  2c 10 62 d7 47 15 5f a7  ec 02 41 13 37 1b 0d 45  |,.b.G._...A.7..E|
00000110  70 c8 3d 5e 02 68 02 68  30 13 1d 97 f4 67 a4 df  |p.=^.h.h0....g..|
00000120  70 46 8d 0b a1 57 6f 0e  87 a3 39 61 91 72 df 50  |pF...Wo...9a.r.P|
00000130  6f 71 14 ee e8 a1 d2 0d  cb c9 8e f2 37 c5 2e b7  |oq..........7...|
00000140  2f 76 6a 39 02 68 36 27  9c c0 49 e9 49 7f d1 6d  |/vj9.h6'..I.I..m|
00000150  52 e1 7c 64 d8 ec be a7  2a 9d 34 2d 72 f6 55 17  |R.|d....*.4-r.U.|
00000160  3a 58 dd d7 c3 a1 cf 1d  fc c5 97 e9 fc 78 49 18  |:X...........xI.|
00000170  61 52 95 eb b9 d3 df 89  6b f3 ac 74 5f 8d 61 00  |aR......k..t_.a.|
00000180  ab c6 23 f5 12 32 2b 88  fd 83 52 e7 15 65 ad 2b  |.....2+...R..e.+|
00000190  77 95 c3 4a 29 d2 b5 84  dd cb 58 b4 a4 1f 2c 5a  |w..J).....X...,Z|
000001a0  66 40 a2 46 04 72 b6 d5  2d be 1e b0 a7 55 e0 a8  |f@.F.r..-....U..|
000001b0  89 b2 d5 9a e4 00 ca a0  39 38 5e 85 f6 c1 a5 77  |........98^....w|
000001c0  a9 a0 17 98 a9 12 15 d7  c5 af 0f 18 5d 6e a6 cc  |............]n..|
000001d0  66 c4 45 3f 93 08 f6 2a  e6 89 ea ef e4 d2 8d a0  |f.E?...*........|
000001e0  e1 bd fa 87 27 e6 d0 32  09 ea 09 74 70 b9 89 76  |....'..2...tp..v|
000001f0  f9 83 d1 a4 e9 00 44 a4  a5 9b 24 cf db 29 c5 3c  |......D...$..).<|
00000200  86 1e 8b d4 f9 5d 66 b8  1b 0d 20 ff 58 14 65 ba  |.....]f... .X.e.|
00000210  01 dd d2 f6 cb 4f 7e a0  53 0c 74 a2 fd 05 84 4a  |.....O~.S.t....J|
00000220  46 86 90 2a 0a 69 51 aa  91 c5 bd 26 e9 1a 63 80  |F..*.iQ....'..c.|
00000230  c9 31 08 cd 32 ab 68 f0  8a 52 df a9 7d ac 1f de  |.1..2.h..R..}...|
00000240  bb da a7 c8 7a 88 45 56  f8 07 e0 6b db 38 8d 8e  |....z.EV...k.8..|
00000250  81 1d 33 04 9c 0a 31 3a  9f 24 e1 8f 04 d6 3c 2d  |..3...1:.$....<-|
00000260  96 c6 b1 3a 97 54 f3 cc  5e a4 16 e3 88 c8 84 0f  |...:.T..^.......|
00000270  82 ec ad 8c 95 a8 e5 16  17 75 4c 8e 7b 8d c1 d3  |.........uL.{...|
00000280  66 c4 ca af 01 14 f2 ff  39 f6 b8 07 e5 40 df c0  |f.......9....@..|
00000290  1e d1 21 ae b3 4c 30 52  2d 31 af 3a 07 a3 5f c8  |..!..L0R-1.:.._.|
000002a0  66 3c 54 a3 77 d6 23 ac  0f 81 8d 15 84 54 1d de  |f<T.w.#......T..|
000002b0  35 d1 97 f2 c6 47 ef be  81 d3 cd 1d 57 00 7a 87  |5....G......W.z.|
000002c0  23 b8 98 3f 19 42 66 63  f5 71 54 4d 46 98 80 7e  |...?.Bfc.qTMF..~|
000002d0  4c 91 59 c7 a3 70 c4 51  74 bb c6 33 01 23 2d ad  |L.Y..p.Qt..3..-.|
000002e0  6d 5c 6f 9f 46 95 d8 7c  b0 0d 54 10 3e f7 39 f8  |m\o.F..|..T.>.9.|
000002f0  a4 cc 3e 6f b5 48 72 b7  18 32 97 9c c8 87 92 bf  |..>o.Hr..2......|
00000300  43 bc 1c 03 77 3f 3c bd  79 ed c4 1d e4 24 a9 fb  |C...w?<.y....$..|
00000310  63 a5 d6 f1 d9 f2 8a df  c9 0a 47 c3 2e bc 69 da  |c.........G...i.|
00000320  6f 47 eb d7 3a 62 19 ba  87 1e ce 77 a3 15 44 ea  |oG..:b.....w..D.|
00000330  ef 7f 77 c6 14 c5 bb a6  8d e5 f1 32 af b3 93 80  |..w........2....|
00000340  09 1d 48 82 86 b3 89 1b  74 40 bd 6e 39 c6 a2 94  |..H.....t@.n9...|
00000350  b2 7d 8a d2 7e e9 ec d8  66 9f a5 e4 e7 b8 6b 95  |.}..~...f.....k.|
00000360  91 93 d9 67 47 94 8d 5d  b3 cd c4 ee 01 b5 67 39  |...gG..]......g9|
00000370  55 7f bc 47 0c 0d be 0e  9e c6 df c6 75 45 7e e1  |U..G........uE~.|
00000380  94 d3 e3 2e 14 ad ae 1e  2d 26 ff 8c ca bc c3 cc  |........-'......|
00000390  ef 3e f4 3a d7 25 a0 87  d5 f8 9b fa 45 1e bd 38  |.>.:.%......E..8|
000003a0  62 b6 1f cb 68 2a 8c 67  fd ff 44 6a 78 44 b2 35  |b...h*.g..DjxD.5|
000003b0  54 47 3d f4 d7 45 04 52  9e b8 49 e1 2c 48 4d d9  |TG=..E.R..I.,HM.|
000003c0  78 c7 c8 36 93 f5 e3 e4  91 8f 11 19 06 7d f0 6c  |x..6.........}.l|
000003d0  b7 a4 17 ae 60 72 df fd  19 b4 9b 81 d0 9b 1e f8  |....`r..........|
```

```
000003e0  cb 1d 8a fa 96 28 23 db  82 14 ff 85 69 1b da b9  |.....(......i...|
000003f0  d9 f0 8a 88 ca ae cb 42  dd b9 5f e6 3c 88 67 a8  |.......B.._.<.g.|
00000400
```

En esta ocasión, al eliminar la aleatoriedad que introduce openssl, es facilmente reconocible que el algoritmo cifra todos los bits del fichero de igual forma, y solo cambia cuando cambia los datos del fichero de entrada

6. Cifrar input.bin con AES-192 en modo OFB, clave y vector de inicialización a elegir (no contraseña). Supongamos que la salida es output.bin.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

```
[usuario@portatil:~]$ openssl enc -e -aes-192-ofb -K e0e0e0e0f1f1f1f1 -iv 0123456789
    abcdef -in /tmp/imput.bin -out /tmp/imput_aes192_ofb_output.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes192_ofb_output.enc
00000000  ea a8 b0 68 ed 5f 3b 30  f1 1c f6 4e 61 c2 35 9d  |...h._;0...Na.5.|
00000010  34 41 91 03 70 16 66 cc  7f 68 f5 29 36 e3 63 29  |4A..p.f..h.)6.c)|
00000020  83 6a cf 05 34 7c 4a c7  79 8a 0d 70 69 06 1d 67  |.j..4|J.y..pi..g|
00000030  fd bb ae 66 1e af 7b 81  80 aa 00 3c 30 5b 2f 35  |...f..{....<0[/5|
00000040  e0 8b 67 a4 9b d2 71 51  69 7f 85 4e cb fc 36 de  |..g...qQi..N..6.|
00000050  d0 fc 63 5b b8 81 01 25  60 58 02 ab e1 93 97 e6  |..c[...%`X......|
00000060  73 e4 66 e4 d7 33 96 b3  3a 55 69 ee a9 28 73 f2  |s.f..3..:Ui..(s.|
00000070  ef 85 98 d1 59 ad 17 c5  75 0a a6 4b ce f8 f3 e3  |....Y...u..K....|
00000080  fc b6 c6 fa 5e 89 70 e1  c2 c5 14 8d 73 c0 f9 ee  |....^.p.....s...|
00000090  29 c0 ef ed a4 8a 7c 57  b2 59 42 9b ac a4 fc c2  |).....|W.YB.....|
000000a0  64 05 02 c3 b4 42 9c 86  35 16 c1 f8 51 1c a5 17  |d....B..5...Q...|
000000b0  cf 1a b5 ea 59 69 8d 87  07 96 fc b1 af 7d c7 3f  |....Yi.......}.?|
000000c0  bf ad e3 f0 8b ee fb 2b  ed 4b d1 fd 3f f3 08 ac  |.......+.K..?...|
000000d0  b2 1c 5e e3 ce ac e7 df  91 2a c6 8c 88 14 1b eb  |..^......*......|
000000e0  61 32 f5 0e 44 98 9a c1  55 d3 c1 da 5b 2f b5 3a  |a2..D...U...[/.:|
000000f0  7d fe 64 9f a5 4a 0f 23  0a 33 e7 76 2c c3 4c b4  |}.d..J...3.v,.L.|
00000100  a6 cf 07 59 be fb 64 e3  27 47 1f 42 49 a8 27 c9  |...Y..d.'G.BI.'.|
00000110  cc 55 b9 99 4e 1d 6e 21  84 1f 7d e0 15 4b 7e ac  |.U..N.n!..}..K~.|
00000120  51 18 ac 11 59 ec 65 5d  1a 2d 09 cf 39 a7 93 62  |Q...Y.e].-..9..b|
00000130  2c 6f 63 87 87 60 51 2c  d3 96 2b 4e 0f d9 25 9d  |,oc..`Q,..+N..%.|
00000140  50 d0 49 fc 03 2e 0e f3  5b 93 45 f5 3a e2 03 ca  |P.I.....[.E.:...|
00000150  1c 4d 00 60 0b c0 d2 4e  16 87 f4 29 c6 fa df 7a  |.M.`...N...)...z|
00000160  11 72 c7 64 f4 c4 00 3d  f5 e7 df 11 0d 65 db e8  |.r.d...=.....e..|
00000170  09 75 ed 6a d2 30 9c 68  a7 62 4a 36 75 af 44 f4  |.u.j.0.h.bJ6u.D.|
00000180  ce 03 7c fe 01 63 57 e6  a7 5c d8 d7 5b 93 8c 2e  |..|..cW..\..[...|
00000190  a3 a3 c3 0e 2c 89 2f 43  d8 8b c8 31 73 9d 88 3a  |....,./C...1s..:|
000001a0  dd 5b 63 24 f0 9e 6f ce  b3 50 4f 9c 7a d1 d8 d0  |.[c$..o..PO.z...|
000001b0  6e e5 8a 72 09 c6 8a c6  72 ea a7 4b 00 4d 77 c1  |n..r....r..K.Mw.|
000001c0  9f b8 ee da ec 7b fa 07  82 7a cc 6b 5b 07 56 09  |.....{...z.k[.V.|
000001d0  55 3a 29 25 e2 4d 9c 79  a3 e9 4c 23 fd b8 dd fa  |U:)%.M.y..L#....|
000001e0  e6 1b 46 55 aa 16 bd 37  05 b9 5e 61 96 a0 2c 03  |..FU...7..^a..,.|
000001f0  69 b1 de 09 37 e5 86 d4  f4 cb 1a 31 2b 1b 57 04  |i...7......1+.W.|
00000200  32 b1 52 51 0a 65 f2 f6  80 de 93 c5 96 06 e1 30  |2.RQ.e.........0|
00000210  c0 db 3d 5b 2b ca 0c b5  ad 44 d3 24 12 61 c0 01  |..=[+....D.$.a..|
00000220  be 21 3e bd d2 81 00 8a  f5 b4 50 ae 48 4e 39 77  |.!>.......P.HN9w|
00000230  7b 69 f2 5d 36 03 a0 fc  85 3d 8d 27 4d ec f5 fb  |{i.]6....=.'M...|
00000240  69 f2 df a3 dd 77 a9 78  ad f8 77 51 89 65 f9 b9  |i....w.x..wQ.e..|
00000250  68 8a e8 9a 0a 43 39 2b  51 ed 75 59 c2 96 53 45  |h....C9+Q.uY..SE|
00000260  2d 6c b9 cc 74 62 5f cd  6c 8c 6d bf ad 47 b0 83  |-l..tb_.l.m..G..|
00000270  19 f2 b5 5c a8 f4 d7 b8  d3 7b e0 25 09 d5 06 d0  |...\.....{.%....|
00000280  ed 72 a6 65 91 32 1e 96  ca 73 8d 70 c8 3b ce 05  |.r.e.2...s.p.;..|
00000290  ca e0 5e 26 83 70 4a 45  ea d9 67 25 ae e2 b9 f6  |..^&.pJE..g%....|
000002a0  cc 8e e6 98 c3 52 ca cf  04 e7 e6 0c 00 fa d4 13  |.....R..........|
000002b0  c6 ce b8 2d d5 94 6f 88  97 5c 80 d4 ec 09 90 c5  |...-..o..\......|
000002c0  44 e9 d6 b7 f3 5d 22 52  7c 29 73 12 b7 9f 5c 6e  |D....]"R|)s...\n|
000002d0  c8 6a 5e 98 96 91 5d d3  7e e3 b5 2f fb a9 13 b5  |.j^...].~../....|
000002e0  3b 1b 62 a1 fd a1 b0 f0  09 b4 9b 82 97 46 b0 15  |;.b..........F..|
000002f0  16 43 da 3d 74 8a fd 29  9a 10 aa b5 30 82 4c b0  |.C.=t..)....0.L.|
00000300  36 0c 8c fc 3b 5b 7c 88  24 59 6e 85 09 41 08 61  |6...;[|.$Yn..A.a|
00000310  34 b2 49 e5 9f 9d 65 35  25 6f 36 d0 7f 08 82 0c  |4.I...e5%o6.....|
00000320  6e 33 54 ba bc 08 06 e6  25 7f 24 bc 24 86 b6 ab  |n3T.....%.$.$...|
00000330  86 00 52 9a 8a de 4a 6f  a1 ce 7a d2 a7 7b 55 41  |..R...Jo..z..{UA|
```

```
00000340  c4 43 7e c7 b1 b1 12 de  27 09 72 83 bf 64 e9 f2  |.C~.....'.r..d..|
00000350  40 c9 c1 0c 1e ef d0 33  ae dc 32 a2 b6 17 c5 a1  |@......3..2.....|
00000360  bf fd 39 8c 5a 7e 20 e4  7a 33 c8 61 5b ed 2d 32  |..9.Z~ .z3.a[.-2|
00000370  f6 72 b0 e8 89 70 d0 a3  d0 f2 26 b8 34 d0 a6 31  |.r...p....&.4..1|
00000380  17 00 2c 88 6c 55 ad 85  9e b6 f2 a6 42 ce d8 26  |..,.lU......B..&|
00000390  55 ee 60 a6 2d 28 7e 21  42 2b f9 0f 59 1a 3b e8  |U.`.-(~!B+..Y.;.|
000003a0  29 27 80 18 fd 9a bb 8d  50 b9 88 b9 63 3d a6 a9  |)'......P...c=..|
000003b0  57 60 51 68 0a 75 1b 6e  8e b2 27 d4 b7 12 2f 90  |W`Qh.u.n..'.../.|
000003c0  cd 29 19 8c 80 2a 9b a8  ca 6e 07 00 f3 0b f3 c4  |.)...*...n......|
000003d0  bc 9c 6f 1f 34 4b 3a ab  06 f4 23 12 21 9c d5 75  |..o.4K:.....!..u|
000003e0  63 d0 b3 1a ee 95 06 77  79 19 25 77 5f 47 8e c5  |c......wy.%w_G..|
000003f0  2a a5 6d 97 f7 01 1c ff  8c 65 75 d0 41 fc f1 54  |*.m......eu.A..T|
00000400
```

7. Descifrar output.bin utilizando la misma clave y vector de inicialización que en 6.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

```
[usuario@portatil:~]$ openssl enc -d -aes-192-ofb -K e0e0e0e0f1f1f1f1 -iv 0123456789
    abcdef -in /tmp/imput_aes192_ofb_output.enc -out /tmp/output.bin
[usuario@portatil:~]$ hexdump -C /tmp/output.bin
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000400
```

8. Vuelve a cifrar output.bin con AES-192 en modo OFB, clave y vector de inicialización del punto 6. Compara el resultado obtenido con el punto 7, explicando el resultado.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

```
[usuario@portatil:~]$ openssl enc -aes-192-ofb -K e0e0e0e0f1f1f1f1 -iv 0123456789abcdef -
    in /tmp/output.bin -out /tmp/imput_aes192_ofb_output2.enc  [usuario@portatil:~]$
    hexdump -C /tmp/imput_aes192_ofb_output2.enc
00000000  ea a8 b0 68 ed 5f 3b 30  f1 1c f6 4e 61 c2 35 9d  |...h._;0...Na.5.|
00000010  34 41 91 03 70 16 66 cc  7f 68 f5 29 36 e3 63 29  |4A..p.f..h.)6.c)|
00000020  83 6a cf 05 34 7c 4a c7  79 8a 0d 70 69 06 1d 67  |.j..4|J.y..pi..g|
00000030  fd bb ae 66 1e af 7b 81  80 aa 00 3c 30 5b 2f 35  |...f..{....<0[/5|
00000040  e0 8b 67 a4 9b d2 71 51  69 7f 85 4e cb fc 36 de  |..g...qQi..N..6.|
00000050  d0 fc 63 5b b8 81 01 25  60 58 02 ab e1 93 97 e6  |..c[...%`X......|
00000060  73 e4 66 e4 d7 33 96 b3  3a 55 69 ee a9 28 73 f2  |s.f..3..:Ui..(s.|
00000070  ef 85 98 d1 59 ad 17 c5  75 0a a6 4b ce f8 f3 e3  |....Y...u..K....|
00000080  fc b6 c6 fa 5e 89 70 e1  c2 c5 14 8d 73 c0 f9 ee  |....^.p.....s...|
00000090  29 c0 ef ed a4 8a 7c 57  b2 59 42 9b ac a4 fc c2  |).....|W.YB.....|
000000a0  64 05 02 c3 b4 42 9c 86  35 16 c1 f8 51 1c a5 17  |d....B..5...Q...|
000000b0  cf 1a b5 ea 59 69 8d 87  07 96 fc b1 af 7d c7 3f  |....Yi.......}.?|
000000c0  bf ad e3 f0 8b ee fb 2b  ed 4b d1 fd 3f f3 08 ac  |.......+.K..?...|
000000d0  b2 1c 5e e3 ce ac e7 df  91 2a c6 8c 88 14 1b eb  |..^......*......|
000000e0  61 32 f5 0e 44 98 9a c1  55 d3 c1 da 5b 2f b5 3a  |a2..D...U...[/.:|
000000f0  7d fe 64 9f a5 4a 0f 23  0a 33 e7 76 2c c3 4c b4  |}.d..J...3.v,.L.|
00000100  a6 cf 07 59 be fb 64 e3  27 47 1f 42 49 a8 27 c9  |...Y..d.'G.BI.'.|
00000110  cc 55 b9 99 4e 1d 6e 21  84 1f 7d e0 15 4b 7e ac  |.U..N.n!..}..K~.|
00000120  51 18 ac 11 59 ec 65 5d  1a 2d 09 cf 39 a7 93 62  |Q...Y.e].-..9..b|
00000130  2c 6f 63 87 87 60 51 2c  d3 96 2b 4e 0f d9 25 9d  |,oc..`Q,..+N..%.|
00000140  50 d0 49 fc 03 2e 0e f3  5b 93 45 f5 3a e2 03 ca  |P.I.....[.E.:...|
00000150  1c 4d 00 60 0b c0 d2 4e  16 87 f4 29 c6 fa df 7a  |.M.`...N...)...z|
00000160  11 72 c7 64 f4 c4 00 3d  f5 e7 df 11 0d 65 db e8  |.r.d...=.....e..|
00000170  09 75 ed 6a d2 30 9c 68  a7 62 4a 36 75 af 44 f4  |.u.j.0.h.bJ6u.D.|
00000180  ce 03 7c fe 01 63 57 e6  a7 5c d8 d7 5b 93 8c 2e  |..|..cW..\..[...|
00000190  a3 a3 c3 0e 2c 89 2f 43  d8 8b c8 31 73 9d 88 3a  |....,./C...1s..:|
000001a0  dd 5b 63 24 f0 9e 6f ce  b3 50 4f 9c 7a d1 d8 d0  |.[c$..o..PO.z...|
000001b0  6e e5 8a 72 09 c6 8a c6  72 ea a7 4b 00 4d 77 c1  |n..r....r..K.Mw.|
000001c0  9f b8 ee da ec 7b fa 07  82 7a cc 6b 5b 07 56 09  |.....{...z.k[.V.|
```

```
000001d0  55 3a 29 25 e2 4d 9c 79  a3 e9 4c 23 fd b8 dd fa  |U:)%.M.y..L#....|
000001e0  e6 1b 46 55 aa 16 bd 37  05 b9 5e 61 96 a0 2c 03  |..FU...7..^a..,.|
000001f0  69 b1 de 09 37 e5 86 d4  f4 cb 1a 31 2b 1b 57 04  |i...7......1+.W.|
00000200  32 b1 52 51 0a 65 f2 f6  80 de 93 c5 96 06 e1 30  |2.RQ.e.........0|
00000210  c0 db 3d 5b 2b ca 0c b5  ad 44 d3 24 12 61 c0 01  |..=[+....D.$.a..|
00000220  be 21 3e bd d2 81 00 8a  f5 b4 50 ae 48 4e 39 77  |.!>.......P.HN9w|
00000230  7b 69 f2 5d 36 03 a0 fc  85 3d 8d 27 4d ec f5 fb  |{i.]6....=.'M...|
00000240  69 f2 df a3 dd 77 a9 78  ad f8 77 51 89 65 f9 b9  |i....w.x..wQ.e..|
00000250  68 8a e8 9a 0a 43 39 2b  51 ed 75 59 c2 96 53 45  |h....C9+Q.uY..SE|
00000260  2d 6c b9 cc 74 62 5f cd  6c 8c 6d bf ad 47 b0 83  |-l..tb_.l.m..G..|
00000270  19 f2 b5 5c a8 f4 d7 b8  d3 7b e0 25 09 d5 06 d0  |...\.....{.%....|
00000280  ed 72 a6 65 91 32 1e 96  ca 73 8d 70 c8 3b ce 05  |.r.e.2...s.p.;..|
00000290  ca e0 5e 26 83 70 4a 45  ea d9 67 25 ae e2 b9 f6  |..^&.pJE..g%....|
000002a0  cc 8e e6 98 c3 52 ca cf  04 e7 e6 0c 00 fa d4 13  |.....R..........|
000002b0  c6 ce b8 2d d5 94 6f 88  97 5c 80 d4 ec 09 90 c5  |...-..o..\......|
000002c0  44 e9 d6 b7 f3 5d 22 52  7c 29 73 12 b7 9f 5c 6e  |D....]'R|)s...\n|
000002d0  c8 6a 5e 98 96 91 5d d3  7e e3 b5 2f fb a9 13 b5  |.j^...].~../....|
000002e0  3b 1b 62 a1 fd a1 b0 f0  09 b4 9b 82 97 46 b0 15  |;.b..........F..|
000002f0  16 43 da 3d 74 8a fd 29  9a 10 aa b5 30 82 4c b0  |.C.=t..)....0.L.|
00000300  36 0c 8c fc 3b 5b 7c 88  24 59 6e 85 09 41 08 61  |6...;[|.$Yn..A.a|
00000310  34 b2 49 e5 9f 9d 65 35  25 6f 36 d0 7f 08 82 0c  |4.I...e5%o6.....|
00000320  6e 33 54 ba bc 08 06 e6  25 7f 24 bc 24 86 b6 ab  |n3T.....%.$.$...|
00000330  86 00 52 9a 8a de 4a 6f  a1 ce 7a d2 a7 7b 55 41  |..R...Jo..z..{UA|
00000340  c4 43 7e c7 b1 b1 12 de  27 09 72 83 bf 64 e9 f2  |.C~.....'.r..d..|
00000350  40 c9 c1 0c 1e ef d0 33  ae dc 32 a2 b6 17 c5 a1  |@......3..2.....|
00000360  bf fd 39 8c 5a 7e 20 e4  7a 33 c8 61 5b ed 2d 32  |..9.Z~ .z3.a[.-2|
00000370  f6 72 b0 e8 89 70 d0 a3  d0 f2 26 b8 34 d0 a6 31  |.r...p....&.4..1|
00000380  17 00 2c 88 6c 55 ad 85  9e b6 f2 a6 42 ce d8 26  |..,.lU......B..&|
00000390  55 ee 60 a6 2d 28 7e 21  42 2b f9 0f 59 1a 3b e8  |U.`.-(~!B+..Y.;.|
000003a0  29 27 80 18 fd 9a bb 8d  50 b9 88 b9 63 3d a6 a9  |)'......P...c=..|
000003b0  57 60 51 68 0a 75 1b 6e  8e b2 27 d4 b7 12 2f 90  |W`Qh.u.n..'.../.|
000003c0  cd 29 19 8c 80 2a 9b a8  ca 6e 07 00 f3 0b f3 c4  |.)...*...n......|
000003d0  bc 9c 6f 1f 34 4b 3a ab  06 f4 23 12 21 9c d5 75  |..o.4K:.....!..u|
000003e0  63 d0 b3 1a ee 95 06 77  79 19 25 77 5f 47 8e c5  |c......wy.%w_G..|
000003f0  2a a5 6d 97 f7 01 1c ff  8c 65 75 d0 41 fc f1 54  |*.m......eu.A..T|
00000400
```

9. Repite los puntos 6 al 8 pero empleando contraseña en lugar de clave y vector de inicialización.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

```
[usuario@portatil:~]$ openssl enc -e -aes-192-ofb -pass pass:mypass -in /tmp/imput.bin -
    out /tmp/imput_aes192_ofb_output_pass.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes192_ofb_output_pass.enc
00000000  53 61 6c 74 65 64 5f 5f  ac f5 40 44 1a 56 57 1a  |Salted__..@D.VW.|
00000010  b2 6f 29 20 6a 1c b9 6b  ac 07 3c cb 94 66 cf c3  |.o) j..k..<..f..|
00000020  f2 9d 6c 5d 45 37 b0 48  b0 57 d0 db b7 8c 55 7a  |..l]E7.H.W....Uz|
00000030  8b be 61 86 8b c4 d5 c2  af 92 99 73 ea d3 41 9b  |..a........s..A.|
00000040  c8 8f 94 78 1d 1c d7 a8  18 c7 0e 1c 3b c2 03 bc  |...x........;...|
00000050  31 74 21 7f d4 33 da 9d  6d c9 5c ed cf 91 a9 2a  |1t!..3..m.\....*|
00000060  f5 b0 95 3a 94 44 9f 4a  5e 46 69 0e cd de 4c 63  |...:.D.J^Fi...Lc|
00000070  20 2c b6 a3 86 19 b2 4f  2a 83 b2 fd b9 6b 14 ec  | ,.....O*....k..|
00000080  da 7d 2c a1 7e 78 f1 ec  53 b5 c6 95 fc cf a2 b5  |.},.~x..S.......|
00000090  6b 04 31 87 dd 07 3f b1  f4 9d fd 93 ee 6c d4 c8  |k.1...?......l..|
000000a0  01 1a c0 55 2e ab 99 38  53 a4 11 0b 4a d1 4e a9  |...U...8S...J.N.|
000000b0  9e 32 63 c4 48 f6 6d c1  a8 2f ac 50 19 e6 4c 86  |.2c.H.m../.P..L.|
000000c0  b7 e5 35 4e c9 6b 02 1f  70 61 a6 b0 29 10 e2 87  |..5N.k..pa..)...|
000000d0  8f 0f 36 3c 63 cc e9 f2  55 7f 22 25 8d a2 66 c4  |..6<c...U."%..f.|
000000e0  97 86 68 b9 79 7b 2d 8e  8d 24 09 66 c5 57 db fe  |..h.y{-..$.f.W..|
000000f0  d4 77 8e b9 12 df 48 bc  9a 4b 0b 48 cf 7b e9 93  |.w....H..K.H.{..|
00000100  8d 5b db a6 12 ec b6 2e  11 5b a8 a1 c1 27 2e 4b  |.[.......[...'.K|
00000110  40 7d 82 bc 97 54 a6 cc  3c 5b db 28 33 a2 dd 59  |@}...T..<[.(3..Y|
00000120  59 3a ec ce 84 6e c5 08  99 80 7c 79 3c c5 03 9b  |Y:...n....|y<...|
00000130  45 1c 2b bd e1 f1 f0 54  d3 08 ce 28 57 39 dc cb  |E.+....T...(W9..|
00000140  c9 fa 40 82 e7 76 79 51  94 01 84 03 35 e1 97 2d  |..@..vyQ....5..-|
00000150  cc 67 36 fd 95 dd 13 f7  58 08 5c f7 0a 8c b6 ce  |.g6.....X.\.....|
00000160  f4 42 81 2a dc 75 ee 8d  62 f8 d4 11 00 2a 3b bc  |.B.*.u..b....*;.|
00000170  80 e1 a9 b1 56 af 7c 5e  1b b0 c0 31 f8 0e f1 f7  |....V.|^...1....|
00000180  14 af c6 83 5c e7 5c 6d  d2 49 99 c9 53 ad c9 92  |....\.\m.I..S...|
```

```
00000190  49 04 39 07 5b 51 4e c2  2d c1 8d 1b 0e 00 5d 09  |I.9.[QN.-.....].|
000001a0  5d 39 2d 66 15 0d 3f 65  bb b9 c9 e5 66 db 53 d4  |]9-f..?e....f.S.|
000001b0  a9 70 b6 17 46 13 51 d3  22 9c af df 4b 6b 6f 66  |.p..F.Q."...Kkof|
000001c0  00 64 fa 67 e1 2a fd 12  e8 23 0b fd 7b 10 f8 9e  |.d.g.*.....{...|
000001d0  a6 ab 2f 50 12 de dc 4e  01 6d a6 fd aa 79 e2 8b  |../P...N.m...y..|
000001e0  b5 61 f4 5d 60 c2 b9 87  44 c6 b3 3e c8 46 cb 02  |.a.]`...D..>.F..|
000001f0  35 f6 fa 22 55 29 73 0d  f6 04 b8 40 02 74 03 26  |5.."U)s....@.t.&|
00000200  6b 44 59 2a de f9 64 cd  1c a3 91 5b 47 01 4f f3  |kDY*..d....[G.O.|
00000210  e0 36 23 3d c7 19 76 1a  f8 a7 e1 95 8b e7 83 7c  |.6.=..v........||
00000220  45 59 58 97 0c 3d f5 a8  54 f8 84 52 74 dd 14 1b  |EYX..=..T..Rt...|
00000230  3d 2f 17 be f4 65 e9 60  ed d0 e2 60 77 45 4b 0d  |=/...e.`...`wEK.|
00000240  1d 0a 93 d2 83 cc d3 13  af 3a ab ec 6c 8b aa 37  |.........:..l..7|
00000250  9c 4c 4e 9a 9e 66 e3 ca  47 ad 6d f7 f5 12 56 b3  |.LN..f..G.m...V.|
00000260  8d 9d 8f 21 0b 8c ac 84  e0 69 ce 72 5e 5d 49 84  |...!.....i.r^]I.|
00000270  95 eb 59 cf e9 fa 9b 04  15 ae d1 89 cd d6 89 df  |..Y.............|
00000280  e5 d3 d0 e3 86 fb e9 06  c0 23 75 2f ff 15 0d 7f  |.........u/....|
00000290  bb 34 83 12 8d 66 4e 9f  54 c6 f1 65 e1 8f ac 9a  |.4...fN.T..e....|
000002a0  d3 6c d9 b4 f1 01 4a e7  64 bc 85 3d 23 41 7c 62  |.l....J.d..=.A|b|
000002b0  34 d7 64 e4 3c 7d 14 08  65 a0 7e 6d 83 07 c3 ad  |4.d.<}..e.~m....|
000002c0  be b2 0b b6 ad b2 77 55  76 45 0e a3 bf 36 72 87  |......wUvE...6r.|
000002d0  86 0b ec 62 3b fc 64 f2  5a 2f b8 d1 e8 03 ed 5f  |...b;.d.Z/....._|
000002e0  ff 0d e7 ac 0c db 11 45  1d a8 5b bf ee 9a cc f7  |.......E..[.....|
000002f0  86 e1 f1 3b 43 21 a5 87  ea cf 3d e1 d1 9e d5 17  |...;C!....=.....|
00000300  04 34 ce 7d d7 44 07 57  36 af f2 ca 38 fa 69 dc  |.4.}.D.W6...8.i.|
00000310  05 c0 d4 ab 37 51 95 2a  e4 2c 69 65 02 c8 6a d4  |....7Q.*.,ie..j.|
00000320  54 2e ac e3 cc 4d 5b ae  28 5d e6 e7 50 49 3c ff  |T....M[.(]..PI<.|
00000330  e1 22 0a 58 96 b9 e7 73  b9 04 dc 97 f1 d0 5a b8  |."X...s......Z.|
00000340  64 85 bd 7f 49 0b d7 c5  b4 e0 83 69 c1 a3 55 16  |d...I......i..U.|
00000350  1b c6 4d cb 28 df 30 88  37 0b 3f 99 26 35 4e 16  |..M.(.0.7.?.&5N.|
00000360  25 83 c1 bd d5 a7 e9 84  21 c0 d9 60 4c d0 e1 52  |%.......!..`L..R|
00000370  ce b3 7b 84 b5 f8 70 26  60 5f 58 5d 05 cd 1a c3  |..{...p&`_X]....|
00000380  66 d0 a3 5b a7 3d 4e bb  7f 52 0c 39 50 b0 23 8d  |f..[.=N..R.9P...|
00000390  59 46 0f c8 c2 d2 ea 18  ec 66 eb bd 9f 21 2f f8  |YF.......f...!/.|
000003a0  ad 78 c8 b1 f7 0d bc bc  35 48 8e 49 6b 40 7a 09  |.x......5H.Ik@z.|
000003b0  95 0d c5 36 a6 11 e5 ca  57 01 9d f1 fd c7 a7 63  |...6....W......c|
000003c0  42 bc 1a 5a 7b 4c 6c d1  7d 42 55 66 fc 8e 8c d8  |B..Z{Ll.}BUf....|
000003d0  e7 a7 93 e4 7c e6 b9 30  11 42 22 1c 0b 3e 0a 30  |....|..0.B"..>.0|
000003e0  c0 78 cd b5 c4 78 45 b1  58 4f 9b 64 b8 cb ca a7  |.x...xE.XO.d....|
000003f0  17 bd fb ee 75 62 60 9b  70 11 b2 0a d3 58 29 68  |....ub`.p....X)h|
00000400  a7 83 28 b8 01 11 92 7c  bd 71 f6 51 ff 5b 6c 6c  |..(....|.q.Q.[ll|
00000410
[usuario@portatil:~]$ openssl enc -d -aes-192-ofb -pass pass:mypass -in /tmp/
    imput_aes192_ofb_output_pass.enc -out /tmp/output_pass.bin
[usuario@portatil:~]$ hexdump -C /tmp/output_pass.bin
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000400
[usuario@portatil:~]$ openssl enc -e -aes-192-ofb -pass pass:mypass -in /tmp/output_pass.
    bin -out /tmp/imput_aes192_ofb_output2_pass.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_aes192_ofb_output2_pass.enc
00000000  53 61 6c 74 65 64 5f 5f  c4 c8 0d 8a d1 1a d0 9a  |Salted__........|
00000010  3a 04 20 83 6e 3c ce 84  89 62 e8 c6 3d 59 ed 08  |:. .n<...b..=Y..|
00000020  4a 9f 68 a7 02 aa 4f 03  1b 4e 37 01 52 78 23 d0  |J.h...O..N7.Rx..|
00000030  e0 82 44 2e f1 1b 76 c1  49 0b 4e 6d 0b 95 79 14  |..D...v.I.Nm..y.|
00000040  25 8f 29 12 51 a3 94 40  0a cb 61 66 50 a0 74 e3  |%.).Q..@..afP.t.|
00000050  db f2 41 60 bd 13 f5 8e  71 34 13 35 76 8f 20 2a  |..A`....q4.5v. *|
00000060  ea 8d 15 2c a5 ae ae a3  e3 26 55 1c 31 97 2b 26  |...,.....&U.1.+&|
00000070  b8 e8 bf 7b 49 03 df d1  64 0f 8d 0c 56 75 d5 b2  |...{I...d...Vu..|
00000080  31 6f 85 29 af 03 e2 f3  01 39 91 88 77 e0 30 ee  |1o.).....9..w.0.|
00000090  41 14 18 af 26 72 c9 e6  93 00 52 20 97 e6 5e 43  |A...&r....R ..^C|
000000a0  6c 1c 29 48 8d 48 5c 26  25 7c 11 d6 57 b0 5c 3b  |l.)H.H\&%|..W.\;|
000000b0  db e4 d3 03 56 2e 24 1f  e4 74 40 e3 41 f3 ad ca  |....V.$..t@.A...|
000000c0  6e 27 6e 7e 45 6e 2d 37  bf 3f e2 4e 5a fb 8b 71  |n'n~En-7.?.NZ..q|
000000d0  24 e8 69 9e 24 b6 2b 17  a5 de 02 10 9b db 93 58  |$.i.$.+........X|
000000e0  a3 9d dd e3 22 e1 1a 8f  a0 fd 7a 1a e6 65 c1 10  |....".....z..e..|
000000f0  78 34 ba 82 38 a1 ed 17  02 43 e7 ed 27 af 4d b6  |x4..8....C..'.M.|
00000100  88 97 aa f8 97 07 32 5c  60 c4 a9 40 e6 5f 59 6a  |......2\`..@._Yj|
00000110  d0 a3 21 d7 cc d3 02 2c  71 3c 27 24 5e dc bf 90  |..!....,q<'$^...|
00000120  d1 f7 2b c2 07 7b 0d 59  a3 6f fc f8 80 5b 62 73  |..+..{.Y.o...[bs|
00000130  f7 38 73 a0 6a 1e bb 52  de 7f fa 35 a8 66 79 c9  |.8s.j..R...5.fy.|
00000140  16 f6 5c e9 79 70 1f af  4c a2 5f f7 7d 58 f0 35  |..\.yp..L._.}X.5|
00000150  b5 a2 59 3f 7c 9a 51 34  40 c6 cf 99 fa 2d 88 9b  |..Y?|.Q4@....-..|
00000160  f2 c9 93 bb 19 aa 6e 3b  78 39 df d5 79 5f 69 ae  |......n;x9..y_i.|
00000170  e0 2d ea 4e 5a 9e 44 c1  1f d5 8f 25 df c9 f2 08  |.-.NZ.D....%....|
00000180  82 6d 46 c6 b2 30 e6 ef  36 32 9e df fa ff 88 3d  |.mF..0..62.....=|
```

```
00000190  7d 1b 48 86 5a 89 3e 8a  7e 70 f4 44 f8 86 8d 73  |}.H.Z.>.~p.D...s|
000001a0  76 b0 e7 f9 12 a1 f6 ed  75 cc 7a 93 5c 05 1e a2  |v.......u.z.\...|
000001b0  e7 bf 8a 2d 49 56 f1 4b  c5 ff 91 ba cb 3d 5e 8a  |...-IV.K.....=^.|
000001c0  fc 0d b4 49 6c e3 bd a2  f2 6b 95 10 59 af b7 ff  |...Il....k..Y...|
000001d0  9d 13 63 de 75 86 03 de  62 5a 32 1d a9 f8 58 c5  |..c.u...bZ2...X.|
000001e0  6e 61 fb 97 43 19 6c ab  ac a8 d5 70 c7 58 9c 68  |na..C.l....p.X.h|
000001f0  a9 fd 67 b8 8e a7 62 9b  f8 7e ba 9f c7 dc 70 17  |..g...b..~....p.|
00000200  22 b7 6a b5 e7 e1 3a 35  08 59 3f ae 54 cc 12 63  |'.j...:5.Y?.T..c|
00000210  b6 e1 55 d5 8f a8 92 13  f5 25 00 ab 72 25 43 ef  |..U......%..r%C.|
00000220  f5 aa 9e 6a 3c d4 2c 24  d4 a0 be ae d9 f9 79 40  |...j<.,$......y@|
00000230  1c 25 7d a5 f6 97 d1 dc  d5 5c 6d a5 ec e7 06 39  |.%}......\m....9|
00000240  39 10 7f d6 31 7a c8 91  bd 96 56 5b 88 6c 70 48  |9...1z....V[.lpH|
00000250  1a 13 c4 45 ac 9e 57 f0  0e 6e d7 0d c0 e4 52 b8  |...E..W..n....R.|
00000260  46 e3 ba aa b1 14 3c e6  8e fe b8 d4 ac 9a b6 62  |F.....<........b|
00000270  0a b2 12 73 67 47 6b 38  e1 36 ce 80 bc fa 04 74  |...sgGk8.6.....t|
00000280  25 5a 71 eb 1f 79 12 92  f5 35 2b aa db 82 92 d1  |%Zq..y...5+.....|
00000290  35 22 ca ee c1 83 61 8f  98 76 66 2b 7f c0 56 52  |5'....a..vf+..VR|
000002a0  72 9b 64 37 56 4e 46 2c  0a e0 fc 69 ad 4c 73 85  |r.d7VNF,...i.Ls.|
000002b0  b3 1e 89 5e c9 3c 01 1b  56 90 09 56 f7 e6 b5 72  |...^.<..V..V...r|
000002c0  1b 40 15 6d 14 68 eb 57  db f4 6c 58 83 c7 e2 5f  |.@.m.h.W..lX..._|
000002d0  c1 1e 6b 2c ba ce 95 e0  da 4b 12 df 88 be 35 5c  |..k,.....K....5\|
000002e0  e7 e1 ee e7 08 fe de e4  3e 38 0c 0d ed 8c 6a 09  |........>8....j.|
000002f0  c9 62 74 26 45 28 37 1e  d1 3f a2 4b 55 61 03 b9  |.bt&E(7..?.KUa..|
00000300  40 60 9b 7c 5f 53 f4 07  4b 0a 97 c7 b0 f7 e3 3e  |@`.|_S..K......>|
00000310  c6 83 d1 18 4a ef f1 2b  69 87 89 8e 85 38 a5 da  |....J..+i....8..|
00000320  37 fd b4 1a d0 53 6b d1  2e c1 ab 40 c0 cf 6e 89  |7....Sk....@..n.|
00000330  3d 47 f6 1a a4 b9 d6 0a  b2 d0 bf 9d 73 32 5e b6  |=G..........s2^.|
00000340  36 0a 38 7f 73 f6 d7 0a  81 66 3c 6a bc 0b 38 2b  |6.8.s....f<j..8+|
00000350  1e b3 c5 9c 0d ba 46 91  47 69 54 e7 de 7f fd 80  |......F.GiT.....|
00000360  aa cf ff c3 af 02 b6 f1  ba 0f 8b 24 8c 14 09 43  |...........$...C|
00000370  74 66 d3 31 68 5c 4a 4a  41 bd 2a 0e ed 04 f6 d8  |tf.1h\JJA.*.....|
00000380  4b 23 ea 5c 40 12 55 ed  55 38 f5 08 af 1e a9 66  |K..\@.U.U8.....f|
00000390  14 76 10 ae 0a 04 ab 9b  ef 08 45 d9 02 a0 33 b8  |.v........E...3.|
000003a0  87 1a c8 21 d8 71 34 71  8e 51 7f e6 4e d6 b0 6a  |...!.q4q.Q..N..j|
000003b0  f6 f3 f9 66 4d 7b f3 66  4c 26 80 bf 6f 8b 1a 7a  |...fM{.fL&..o..z|
000003c0  ed 33 55 31 4f 45 f1 c2  fd ef 55 e6 88 33 29 3a  |.3U1OE....U..3):|
000003d0  89 0a 6a 26 64 a5 8b 2e  b7 a8 b5 69 f4 b6 f8 67  |..j&d......i...g|
000003e0  e9 77 c1 f0 84 e2 f7 0b  6a 56 77 26 19 9d a4 b3  |.w......jVw&....|
000003f0  dc f4 8c e0 e5 8f c6 69  9a 51 12 44 20 55 a8 c2  |.......i.Q.D U..|
00000400  a8 47 23 70 db b8 ef db  1e a6 72 d3 16 c8 72 6e  |.G.p......r...rn|
00000410
```

Como ya hemos explicado en ejercicios anteriores el cifrado en modo OFB no depende del contenido del fichero, ya que como se puede apreciar nuevamente, aunque el contenido de los ficheros cifrados crece levemente, esto es debido a que se añade una cadena aleatoria o bien al padding, y sin embargo el contenido de los ficheros cifrados no se parecen en nada, aun teniendo el mismo fichero de entrada.

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

El algoritmo escogido es CAMELLIA[1], este algoritmo de cifrado fue desarrollado por las compañias japonesa Nippon Telegraph y Mitsubishi Electric para la competición NESSIE europea.

Este algoritmo consiste en un cifrado de bloque de tamaño fijo 128 bits, y el tamaño de clave variable entre 128, 192, 256 bits, tal y como se puede apreciar en las diferentes imagenes de esta presentación[2] consiste en un cifrar los bloques de datos 6 veces con unas claves ya generadas previamente y este paso lo hace 3 veces para tamaños de claves de 128, en la misma presentación se puede apreciar que ademas esos bloques de cifrado de 6 rondas se usan de diferentes formas para las claves de mayor tamaño.

11. Repetir los puntos 3 a 5 con el cifrado presentado en el punto 10.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

11.1. Modo ECB

```
[usuario@portatil:~]$ openssl enc -camellia-192-ecb -K e0e0e0e0f1f1f1f1 -in /tmp/imput.
    bin -out /tmp/imput_camellia192_ecb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_camellia192_ecb.enc
00000000  98 2e 91 b4 2c 59 ef c3  7c c1 76 15 9b 2a 05 a9  |....,Y..|.v..*..|
*
00000400  43 e1 9d 75 05 65 17 1c  8b 51 ad e5 0c ea be aa  |C..u.e...Q......|
00000410
```

11.2. Modo CBC

```
[usuario@portatil:~]$ openssl enc -camellia-192-cbc -K e0e0e0e0f1f1f1f1 -iv 0123456789
    abcdef -in /tmp/imput.bin -out /tmp/imput_camellia192_cbc.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_camellia192_cbc.enc
00000000  6e 63 00 5b 79 22 34 eb  96 48 04 db 61 8e 5d 0d  |nc.[y.4..H..a.].|
00000010  be 2b a4 34 3e 75 d1 c9  16 52 af 24 85 be 1e 0a  |.+.4>u...R.$....|
00000020  79 07 e9 5e cb f4 4b e7  a6 ad 94 1f 05 bd 35 2d  |y..^..K.......5-|
00000030  52 64 52 e0 58 19 0c b4  0e f4 36 25 99 a0 56 ab  |RdR.X.....6%..V.|
00000040  64 60 ad 5b c1 d0 56 7a  81 4c 3f 9d e5 7e 1e cd  |d`.[..Vz.L?..~..|
00000050  da 1f e1 c0 47 2f 32 64  92 be f8 dd 0b 69 e0 1f  |....G/2d.....i..|
00000060  5b 1a f6 94 21 97 17 4c  4a a1 7d ef 19 b0 7c c0  |[...!..LJ.}...|.|
00000070  2c 91 e6 4c 4b f8 0d b7  b2 a1 2c 86 c6 96 38 88  |,..LK.....,...8.|
00000080  8c 86 8b d2 5f a7 22 92  8c 2a 63 01 01 05 c6 ba  |...._....*c.....|
00000090  1d 36 ac 6d 91 cd da c1  57 a4 e3 bc ba 2b 11 49  |.6.m....W....+.I|
000000a0  2f 07 14 55 65 e9 d0 91  2b 8c c3 df 20 4e 28 f3  |/..Ue...+... N(.|
000000b0  ed 86 95 fe e9 e4 bd 5d  48 b3 22 62 1e d8 d4 3b  |.......]H.."b...;|
000000c0  fc 28 30 72 1d fd 6b aa  7f 9f 5a b0 b1 a6 91 8c  |.(0r..k...Z.....|
000000d0  e4 af 65 f1 12 54 ad cb  9c 3a a2 70 70 a0 6c 2e  |..e..T...:.pp.l.|
000000e0  39 5e 26 9e 18 5b 2e 72  5c f3 dc a3 67 5a 26 ec  |9^&..[.r\...gZ&.|
000000f0  dc 55 e7 11 3c 73 f1 8c  27 82 b1 7a 62 5d 4d 0e  |.U..<s..'..zb]M.|
00000100  c1 3f 95 fe 68 25 84 1f  96 c2 15 fe 17 64 56 c7  |.?..h%.......dV.|
00000110  f4 46 33 ca c9 c0 68 d5  8c 1c 46 98 e1 80 d0 d1  |.F3...h...F.....|
00000120  45 9f 8c 2d be 60 41 d6  7c 7b 8e d8 36 f6 c1 c9  |E..-.`A.|{..6...|
00000130  d5 ef 9f 34 60 8a 91 a1  0d b2 6c c9 ac 96 cf c6  |...4`.....l.....|
00000140  40 7b f9 5a 5b fd 4f 20  f6 59 3f 78 54 f9 30 ec  |@{.Z[.O .Y?xT.0.|
00000150  7a 49 ee d5 5c 15 54 ec  b7 51 f4 35 67 0c 9e d1  |zI..\.T..Q.5g...|
00000160  1f 89 65 a9 26 4b 1e aa  29 ac 15 04 23 09 0d 8b  |..e.&K..).......|
00000170  f9 14 66 87 bb 1b 81 3c  aa c6 29 3f 19 0b 18 92  |..f....<..)?....|
00000180  76 bf 02 37 a8 d1 42 ee  c2 3a 41 d9 1a 9f a2 80  |v..7..B..:A.....|
00000190  1c 30 21 32 8f e1 94 c9  a0 3b c4 cb 38 ae 31 52  |.0!2.....;..8.1R|
000001a0  74 6f bb c8 6c 7c 67 0e  53 62 68 54 0c 79 80 ba  |to..l|g.SbhT.y..|
000001b0  58 88 75 b4 da d8 fd 4d  94 eb 81 b9 31 8d 90 10  |X.u....M....1...|
000001c0  38 3e 62 2d bf bc dd 3e  27 19 a5 69 ed ad e4 12  |8>b-...>'..i....|
000001d0  12 18 6e 6e ec 21 9d 22  ec 3c f1 76 6c 6c 85 95  |..nn.!...<.vll..|
000001e0  27 a6 e2 35 90 94 73 ce  f2 2b a0 0b 7f 64 76 a1  |'..5..s..+...dv.|
000001f0  93 9e 0d 63 82 44 cd 5e  94 db 17 ef 1c 03 e4 e4  |...c.D.^........|
00000200  24 22 29 7b 71 c2 f7 df  0e bd cc 6e bf 0d 0a 8e  |$.){q......n....|
00000210  09 0b d8 27 65 6f ca 85  b0 95 40 21 0c ec ab 68  |...'eo....@!...h|
00000220  35 a3 47 6a bb 9b dd 63  00 d3 14 b4 0b c3 9a 3b  |5.Gj...c.......;|
00000230  16 2b 88 5b e7 89 9c ca  82 56 d6 f0 52 d3 61 1d  |.+.[.....V..R.a.|
00000240  4b f0 78 8e 8e 82 c8 5f  51 e6 5d 81 d7 7c 90 33  |K.x...._Q.]..|.3|
00000250  29 ec 75 fe 83 d8 3e d6  59 7c 60 c2 c0 4e 21 96  |).u...>.Y|`..N!.|
00000260  9e 63 b1 ea 39 e4 24 a3  ab 1e d1 58 4b c4 f4 35  |.c..9.$....XK..5|
00000270  2f ee 8c ba 0a c6 be 0b  01 af 08 03 13 92 96 18  |/...............|
00000280  9e e2 6d b8 8e fd 08 fd  24 74 5c 77 c5 9e 49 38  |..m.....$t\w..I8|
00000290  9d f8 e9 dd 57 5b bb c4  e2 23 c5 cd a8 ee 3c 7d  |....W[.....#....<}|
000002a0  29 72 23 02 14 d5 d6 e6  ac 62 0a 44 14 0f 1c cf  |)r#.....b.D....|
000002b0  dc f5 a6 6f 3e 2b 8e f1  db 42 11 e3 67 78 24 fc  |...o>+...B..gx$.|
000002c0  a2 c8 b7 82 01 a1 37 01  44 a1 b9 4f 9d 64 73 57  |......7.D..O.dsW|
000002d0  f8 f0 7e a5 42 a0 ab f1  bc 7a 64 e0 d4 aa 05 7b  |..~.B....zd....{|
000002e0  82 9a 68 41 14 48 0d c8  2b 5f 70 63 6b e2 dd 08  |..hA.H..+_pck...|
000002f0  4a 8b 44 df f7 20 71 fc  e9 5d 9b 4a f9 f9 d3 80  |J.D.. q..].J....|
00000300  cb bb 48 a6 58 62 31 24  75 e2 8f 6a e9 da 2f 9f  |..H.Xb1$u..j../.|
00000310  2d ac 6d 17 8d 38 3b 6e  d6 4a 47 89 1a 62 e9 16  |-.m..8;n.JG..b..|
00000320  4e 76 e7 57 54 96 b7 53  07 a5 f1 27 88 e8 63 25  |Nv.WT..S...'..c%|
00000330  4d 31 f9 ca 24 f3 71 42  d7 68 bb f7 eb 84 42 28  |M1..$.qB.h....B(|
00000340  52 2b e2 5e 17 db 6e 15  ca fe fa fd 65 f8 cb 4f  |R+.^..n.....e..O|
00000350  06 bd be 73 d9 fa 1e c8  e7 e9 41 b0 48 bd 29 68  |...s......A.H.)h|
00000360  1d de b8 44 34 5a 9b 53  3b df 48 b3 8f 67 2f 64  |...D4Z.S;.H..g/d|
00000370  89 67 87 99 be e4 ea b6  58 69 31 d0 cd 7d 83 38  |.g......Xi1..}.8|
```

```
00000380  af 5c bf ac af ce 6d 52  5a e2 67 09 d1 c4 e3 b2  |.\....mRZ.g.....|
00000390  e7 0c cb 4f 9a 4f 4a 99  da 77 77 13 c8 57 83 e1  |...O.OJ..ww..W..|
000003a0  29 e1 bf d4 9b 51 7a 3b  9b 16 ff be 8d fa af e2  |)....Qz;........|
000003b0  51 1a 70 8d c0 0c a3 08  65 76 63 8f 30 cb 0f 92  |Q.p.....evc.0...|
000003c0  ae 84 bf 3c 60 04 79 bf  51 f4 f1 bc b5 79 77 4b  |...<‘.y.Q....ywK|
000003d0  53 38 cb 65 7f 27 b4 55  80 6d 8d 6a 7f a4 14 a3  |S8.e.’.U.m.j....|
000003e0  c4 9b a2 0d ce 9c 90 e5  95 11 9d 88 d7 15 4a 75  |..............Ju|
000003f0  b2 c0 ce 2b 77 57 b2 09  81 8d 3c a8 7f 9b 35 65  |...+wW....<...5e|
00000400  05 71 49 58 f6 e1 16 6d  03 ce de fc b2 62 66 05  |.qIX...m.....bf.|
00000410
```

11.3. Modo OFB

```
[usuario@portatil:~]$ openssl enc -camellia-192-ofb -K e0e0e0e0f1f1f1f1 -iv 0123456789
    abcdef -in /tmp/imput.bin -out /tmp/imput_camellia192_ofb.enc
[usuario@portatil:~]$ hexdump -C /tmp/imput_camellia192_ofb.enc
00000000  6e 63 00 5b 79 22 34 eb  96 48 04 db 61 8e 5d 0d  |nc.[y.4..H..a.].|
00000010  be 2b a4 34 3e 75 d1 c9  16 52 af 24 85 be 1e 0a  |.+.4>u...R.$....|
00000020  79 07 e9 5e cb f4 4b e7  a6 ad 94 1f 05 bd 35 2d  |y..^..K.......5-|
00000030  52 64 52 e0 58 19 0c b4  0e f4 36 25 99 a0 56 ab  |RdR.X.....6%..V.|
00000040  64 60 ad 5b c1 d0 56 7a  81 4c 3f 9d e5 7e 1e cd  |d‘.[..Vz.L?..~..|
00000050  da 1f e1 c0 47 2f 32 64  92 be f8 dd 0b 69 e0 1f  |....G/2d.....i..|
00000060  5b 1a f6 94 21 97 17 4c  4a a1 7d ef 19 b0 7c c0  |[...!..LJ.}...|.|
00000070  2c 91 e6 4c 4b f8 0d b7  b2 a1 2c 86 c6 96 38 88  |,..LK.....,...8.|
00000080  8c 86 8b d2 5f a7 22 92  8c 2a 63 01 01 05 c6 ba  |...._....*c.....|
00000090  1d 36 ac 6d 91 cd da c1  57 a4 e3 bc ba 2b 11 49  |.6.m....W....+.I|
000000a0  2f 07 14 55 65 e9 d0 91  2b 8c c3 df 20 4e 28 f3  |/..Ue...+... N(.|
000000b0  ed 86 95 fe e9 e4 bd 5d  48 b3 22 62 1e d8 d4 3b  |.......]H..b...;|
000000c0  fc 28 30 72 1d fd 6b aa  7f 9f 5a b0 b1 a6 91 8c  |.(0r..k...Z.....|
000000d0  e4 af 65 f1 12 54 ad cb  9c 3a a2 70 70 a0 6c 2e  |..e..T...:.pp.l.|
000000e0  39 5e 26 9e 18 5b 2e 72  5c f3 dc a3 67 5a 26 ec  |9^&..[.r\...gZ&.|
000000f0  dc 55 e7 11 3c 73 f1 8c  27 82 b1 7a 62 5d 4d 0e  |.U..<s..’..zb]M.|
00000100  c1 3f 95 fe 68 25 84 1f  96 c2 15 fe 17 64 56 c7  |.?..h%.......dV.|
00000110  f4 46 33 ca c9 c0 68 d5  8c 1c 46 98 e1 80 d0 d1  |.F3...h...F.....|
00000120  45 9f 8c 2d be 60 41 d6  7c 7b 8e d8 36 f6 c1 c9  |E..-.‘A.|{..6...|
00000130  d5 ef 9f 34 60 8a 91 a1  0d b2 6c c9 ac 96 cf c6  |...4‘.....l.....|
00000140  40 7b f9 5a 5b fd 4f 20  f6 59 3f 78 54 f9 30 ec  |@{.Z[.O .Y?xT.0.|
00000150  7a 49 ee d5 5c 15 54 ec  b7 51 f4 35 67 0c 9e d1  |zI..\.T..Q.5g...|
00000160  1f 89 65 a9 26 4b 1e aa  29 ac 15 04 23 09 0d 8b  |..e.&K..).....|
00000170  f9 14 66 87 bb 1b 81 3c  aa c6 29 3f 19 0b 18 92  |..f....<..)?....|
00000180  76 bf 02 37 a8 d1 42 ee  c2 3a 41 d9 1a 9f a2 80  |v..7..B..:A.....|
00000190  1c 30 21 32 8f e1 94 c9  a0 3b c4 cb 38 ae 31 52  |.0!2.....;..8.1R|
000001a0  74 6f bb c8 6c 7c 67 0e  53 62 68 54 0c 79 80 ba  |to..l|g.SbhT.y..|
000001b0  58 88 75 b4 da d8 fd 4d  94 eb 81 b9 31 8d 90 10  |X.u....M....1...|
000001c0  38 3e 62 2d bf bc dd 3e  27 19 a5 69 ed ad e4 12  |8>b-...>’..i....|
000001d0  12 18 6e 6e ec 21 9d 22  ec 3c f1 76 6c 6c 85 95  |..nn.!...<.vll..|
000001e0  27 a6 e2 35 90 94 73 ce  f2 2b a0 0b 7f 64 76 a1  |’..5..s..+...dv.|
000001f0  93 9e 0d 63 82 44 cd 5e  94 db 17 ef 1c 03 e4 e4  |...c.D.^........|
00000200  24 22 29 7b 71 c2 f7 df  0e bd cc 6e bf 0d 0a 8e  |$.){q......n....|
00000210  09 0b d8 27 65 6f ca 85  b0 95 40 21 0c ec ab 68  |...’eo....@!...h|
00000220  35 a3 47 6a bb 9b dd 63  00 d3 14 b4 0b c3 9a 3b  |5.Gj...c.......;|
00000230  16 2b 88 5b e7 89 9c ca  82 56 d6 f0 52 d3 61 1d  |.+.[.....V..R.a.|
00000240  4b f0 78 8e 8e 82 c8 5f  51 e6 5d 81 d7 7c 90 33  |K.x...._Q.]..|.3|
00000250  29 ec 75 fe 83 d8 3e d6  59 7c 60 c2 c0 4e 21 96  |).u...>.Y|‘..N!.|
00000260  9e 63 b1 ea 39 e4 24 a3  ab 1e d1 58 4b c4 f4 35  |.c..9.$....XK..5|
00000270  2f ee 8c ba 0a c6 be 0b  01 af 08 03 13 92 96 18  |/...............|
00000280  9e e2 6d b8 8e fd 08 fd  24 74 5c 77 c5 9e 49 38  |..m.....$t\w..I8|
00000290  9d f8 e9 dd 57 5b bb c4  e2 23 c5 cd a8 ee 3c 7d  |....W[.....<}|
000002a0  29 72 23 02 14 d5 d6 e6  ac 62 0a 44 14 0f 1c cf  |)r#.....b.D....|
000002b0  dc f5 a6 6f 3e 2b 8e f1  db 42 11 e3 67 78 24 fc  |...o>+...B..gx$.|
000002c0  a2 c8 b7 82 01 a1 37 01  44 a1 b9 4f 9d 64 73 57  |......7.D..O.dsW|
000002d0  f8 f0 7e a5 42 a0 ab f1  bc 7a 64 e0 d4 aa 05 7b  |..~.B....zd....{|
000002e0  82 9a 68 41 14 48 0d c8  2b 5f 70 63 6b e2 dd 08  |..hA.H..+_pck...|
000002f0  4a 8b 44 df f7 20 71 fc  e9 5d 9b 4a f9 f9 d3 80  |J.D.. q..].J....|
00000300  cb bb 48 a6 58 62 31 24  75 e2 8f 6a e9 da 2f 9f  |..H.Xb1$u..j../.|
00000310  2d ac 6d 17 8d 38 3b 6e  d6 4a 47 89 1a 62 e9 16  |-.m..8;n.JG..b..|
00000320  4e 76 e7 57 54 96 b7 53  07 a5 f1 27 88 e8 63 25  |Nv.WT..S...’..c%|
00000330  4d 31 f9 ca 24 f3 71 42  d7 68 bb f7 eb 84 42 28  |M1..$.qB.h....B(|
00000340  52 2b e2 5e 17 db 6e 15  ca fe fa fd 65 f8 cb 4f  |R+.^..n.....e..O|
00000350  06 bd be 73 d9 fa 1e c8  e7 e9 41 b0 48 bd 29 68  |...s......A.H.)h|
00000360  1d de b8 44 34 5a 9b 53  3b df 48 b3 8f 67 2f 64  |...D4Z.S;.H..g/d|
```

```
00000370  89 67 87 99 be e4 ea b6  58 69 31 d0 cd 7d 83 38  |.g......Xi1..}.8|
00000380  af 5c bf ac af ce 6d 52  5a e2 67 09 d1 c4 e3 b2  |.\....mRZ.g.....|
00000390  e7 0c cb 4f 9a 4f 4a 99  da 77 77 13 c8 57 83 e1  |...O.OJ..ww..W..|
000003a0  29 e1 bf d4 9b 51 7a 3b  9b 16 ff be 8d fa af e2  |).....Qz;........|
000003b0  51 1a 70 8d c0 0c a3 08  65 76 63 8f 30 cb 0f 92  |Q.p.....evc.0...|
000003c0  ae 84 bf 3c 60 04 79 bf  51 f4 f1 bc b5 79 77 4b  |...<`.y.Q....ywK|
000003d0  53 38 cb 65 7f 27 b4 55  80 6d 8d 6a 7f a4 14 a3  |S8.e.'.U.m.j....|
000003e0  c4 9b a2 0d ce 9c 90 e5  95 11 9d 88 d7 15 4a 75  |..............Ju|
000003f0  b2 c0 ce 2b 77 57 b2 09  81 8d 3c a8 7f 9b 35 65  |...+wW....<...5e|
00000400
```

Referencias

[1] A description of the camellia encryption algorithm, Consultado el 29 de octubre de 2018. https://tools.ietf.org/html/rfc3713.

[2] Prezi, algoritmo camellia, Consultado el 29 de octubre de 2018. https://prezi.com/l7sn5efz9iyq/algoritmo-camellia/?webgl=0.