aes-Valores_TEST

July 28, 2023

1 Polinomio: 0x11b

1.1 Appendix A - Key Expansion Examples

```
-------------------------------------------------------------------------------
Clave 128 bits: 2b7e151628aed2a6abf7158809cf4f3c
-------------------------------------------------------------------------------
w0 2b7e1516
w1 28aed2a6
w2 abf71588
w3 09cf4f3c
w4 a0fafe17
w5 88542cb1
w6 23a33939
w7 2a6c7605
w8 f2c295f2
w9 7a96b943
w10 5935807a
w11 7359f67f
w12 3d80477d
w13 4716fe3e
w14 1e237e44
w15 6d7a883b
w16 ef44a541
w17 a8525b7f
w18 b671253b
w19 db0bad00
w20 d4d1c6f8
w21 7c839d87
w22 caf2b8bc
w23 11f915bc
w24 6d88a37a
w25 110b3efd
w26 dbf98641
w27 ca0093fd
w28 4e54f70e
w29 5f5fc9f3
w30 84a64fb2
```

```
w31 4ea6dc4f
w32 ead27321
w33 b58dbad2
w34 312bf560
w35 7f8d292f
w36 ac7766f3
w37 19fadc21
w38 28d12941
w39 575c006e
w40 d014f9a8
w41 c9ee2589
w42 e13f0cc8
w43 b6630ca6
--------------------------------------------------------------------------------
Clave 192 bits: 8e73b0f7da0e6452c810f32b809079e562f8ead2522c6b7b
--------------------------------------------------------------------------------
w0 8e73b0f7
w1 da0e6452
w2 c810f32b
w3 809079e5
w4 62f8ead2
w5 522c6b7b
w6 fe0c91f7
w7 2402f5a5
w8 ec12068e
w9 6c827f6b
w10 0e7a95b9
w11 5c56fec2
w12 4db7b4bd
w13 69b54118
w14 85a74796
w15 e92538fd
w16 e75fad44
w17 bb095386
w18 485af057
w19 21efb14f
w20 a448f6d9
w21 4d6dce24
w22 aa326360
w23 113b30e6
w24 a25e7ed5
w25 83b1cf9a
w26 27f93943
w27 6a94f767
w28 c0a69407
w29 d19da4e1
w30 ec1786eb
w31 6fa64971
```

```
w32 485f7032
w33 22cb8755
w34 e26d1352
w35 33f0b7b3
w36 40beeb28
w37 2f18a259
w38 6747d26b
w39 458c553e
w40 a7e1466c
w41 9411f1df
w42 821f750a
w43 ad07d753
w44 ca400538
w45 8fcc5006
w46 282d166a
w47 bc3ce7b5
w48 e98ba06f
w49 448c773c
w50 8ecc7204
w51 01002202
--------------------------------------------------------------------------------
Clave 256 bits: 603deb1015ca71be2b73aef0857d77811f352c073b6108d72d9810a30914dff4
--------------------------------------------------------------------------------
w0 603deb10
w1 15ca71be
w2 2b73aef0
w3 857d7781
w4 1f352c07
w5 3b6108d7
w6 2d9810a3
w7 0914dff4
w8 9ba35411
w9 8e6925af
w10 a51a8b5f
w11 2067fcde
w12 a8b09c1a
w13 93d194cd
w14 be49846e
w15 b75d5b9a
w16 d59aecb8
w17 5bf3c917
w18 fee94248
w19 de8ebe96
w20 b5a9328a
w21 2678a647
w22 98312229
w23 2f6c79b3
w24 812c81ad
```

```
w25 dadf48ba
w26 24360af2
w27 fab8b464
w28 98c5bfc9
w29 bebd198e
w30 268c3ba7
w31 09e04214
w32 68007bac
w33 b2df3316
w34 96e939e4
w35 6c518d80
w36 c814e204
w37 76a9fb8a
w38 5025c02d
w39 59c58239
w40 de136967
w41 6ccc5a71
w42 fa256395
w43 9674ee15
w44 5886ca5d
w45 2e2f31d7
w46 7e0af1fa
w47 27cf73c3
w48 749c47ab
w49 18501dda
w50 e2757e4f
w51 7401905a
w52 cafaaae3
w53 e4d59b34
w54 9adf6ace
w55 bd10190d
w56 fe4890d1
w57 e6188d0b
w58 046df344
w59 706c631e
```

1.2 Appendix B – Cipher Example

```
Clave 128 bits: 2b7e151628aed2a6abf7158809cf4f3c

input
0x32 0x88 0x31 0xe0
0x43 0x5a 0x31 0x37
0xf6 0x30 0x98 0x7
0xa8 0x8d 0xa2 0x34

AddRoundKey
0x19 0xa0 0x9a 0xe9
```

```
0x3d 0xf4 0xc6 0xf8
0xe3 0xe2 0x8d 0x48
0xbe 0x2b 0x2a 0x8

ByteSub
0xd4 0xe0 0xb8 0x1e
0x27 0xbf 0xb4 0x41
0x11 0x98 0x5d 0x52
0xae 0xf1 0xe5 0x30

ShiftRow
0xd4 0xe0 0xb8 0x1e
0xbf 0xb4 0x41 0x27
0x5d 0x52 0x11 0x98
0x30 0xae 0xf1 0xe5

MixColumn
0x4 0xe0 0x48 0x28
0x66 0xcb 0xf8 0x6
0x81 0x19 0xd3 0x26
0xe5 0x9a 0x7a 0x4c

AddRoundKey
0xa4 0x68 0x6b 0x2
0x9c 0x9f 0x5b 0x6a
0x7f 0x35 0xea 0x50
0xf2 0x2b 0x43 0x49

ByteSub
0x49 0x45 0x7f 0x77
0xde 0xdb 0x39 0x2
0xd2 0x96 0x87 0x53
0x89 0xf1 0x1a 0x3b

ShiftRow
0x49 0x45 0x7f 0x77
0xdb 0x39 0x2 0xde
0x87 0x53 0xd2 0x96
0x3b 0x89 0xf1 0x1a

MixColumn
0x58 0x1b 0xdb 0x1b
0x4d 0x4b 0xe7 0x6b
0xca 0x5a 0xca 0xb0
0xf1 0xac 0xa8 0xe5

AddRoundKey
0xaa 0x61 0x82 0x68
```

```
0x8f 0xdd 0xd2 0x32
0x5f 0xe3 0x4a 0x46
0x3 0xef 0xd2 0x9a

ByteSub
0xac 0xef 0x13 0x45
0x73 0xc1 0xb5 0x23
0xcf 0x11 0xd6 0x5a
0x7b 0xdf 0xb5 0xb8

ShiftRow
0xac 0xef 0x13 0x45
0xc1 0xb5 0x23 0x73
0xd6 0x5a 0xcf 0x11
0xb8 0x7b 0xdf 0xb5

MixColumn
0x75 0x20 0x53 0xbb
0xec 0xb 0xc0 0x25
0x9 0x63 0xcf 0xd0
0x93 0x33 0x7c 0xdc

AddRoundKey
0x48 0x67 0x4d 0xd6
0x6c 0x1d 0xe3 0x5f
0x4e 0x9d 0xb1 0x58
0xee 0xd 0x38 0xe7

ByteSub
0x52 0x85 0xe3 0xf6
0x50 0xa4 0x11 0xcf
0x2f 0x5e 0xc8 0x6a
0x28 0xd7 0x7 0x94

ShiftRow
0x52 0x85 0xe3 0xf6
0xa4 0x11 0xcf 0x50
0xc8 0x6a 0x2f 0x5e
0x94 0x28 0xd7 0x7

MixColumn
0xf 0x60 0x6f 0x5e
0xd6 0x31 0xc0 0xb3
0xda 0x38 0x10 0x13
0xa9 0xbf 0x6b 0x1

AddRoundKey
0xe0 0xc8 0xd9 0x85
```

```
0x92 0x63 0xb1 0xb8
0x7f 0x63 0x35 0xbe
0xe8 0xc0 0x50 0x1

ByteSub
0xe1 0xe8 0x35 0x97
0x4f 0xfb 0xc8 0x6c
0xd2 0xfb 0x96 0xae
0x9b 0xba 0x53 0x7c

ShiftRow
0xe1 0xe8 0x35 0x97
0xfb 0xc8 0x6c 0x4f
0x96 0xae 0xd2 0xfb
0x7c 0x9b 0xba 0x53

MixColumn
0x25 0xbd 0xb6 0x4c
0xd1 0x11 0x3a 0x4c
0xa9 0xd1 0x33 0xc0
0xad 0x68 0x8e 0xb0

AddRoundKey
0xf1 0xc1 0x7c 0x5d
0x0 0x92 0xc8 0xb5
0x6f 0x4c 0x8b 0xd5
0x55 0xef 0x32 0xc

ByteSub
0xa1 0x78 0x10 0x4c
0x63 0x4f 0xe8 0xd5
0xa8 0x29 0x3d 0x3
0xfc 0xdf 0x23 0xfe

ShiftRow
0xa1 0x78 0x10 0x4c
0x4f 0xe8 0xd5 0x63
0x3d 0x3 0xa8 0x29
0xfe 0xfc 0xdf 0x23

MixColumn
0x4b 0x2c 0x33 0x37
0x86 0x4a 0x9d 0xd2
0x8d 0x89 0xf4 0x18
0x6d 0x80 0xe8 0xd8

AddRoundKey
0x26 0x3d 0xe8 0xfd
```

```
0xe 0x41 0x64 0xd2
0x2e 0xb7 0x72 0x8b
0x17 0x7d 0xa9 0x25

ByteSub
0xf7 0x27 0x9b 0x54
0xab 0x83 0x43 0xb5
0x31 0xa9 0x40 0x3d
0xf0 0xff 0xd3 0x3f

ShiftRow
0xf7 0x27 0x9b 0x54
0x83 0x43 0xb5 0xab
0x40 0x3d 0x31 0xa9
0x3f 0xf0 0xff 0xd3

MixColumn
0x14 0x46 0x27 0x34
0x15 0x16 0x46 0x2a
0xb5 0x15 0x56 0xd8
0xbf 0xec 0xd7 0x43

AddRoundKey
0x5a 0x19 0xa3 0x7a
0x41 0x49 0xe0 0x8c
0x42 0xdc 0x19 0x4
0xb1 0x1f 0x65 0xc

ByteSub
0xbe 0xd4 0xa 0xda
0x83 0x3b 0xe1 0x64
0x2c 0x86 0xd4 0xf2
0xc8 0xc0 0x4d 0xfe

ShiftRow
0xbe 0xd4 0xa 0xda
0x3b 0xe1 0x64 0x83
0xd4 0xf2 0x2c 0x86
0xfe 0xc8 0xc0 0x4d

MixColumn
0x0 0xb1 0x54 0xfa
0x51 0xc8 0x76 0x1b
0x2f 0x89 0x6d 0x99
0xd1 0xff 0xcd 0xea

AddRoundKey
0xea 0x4 0x65 0x85
```

```
0x83 0x45 0x5d 0x96
0x5c 0x33 0x98 0xb0
0xf0 0x2d 0xad 0xc5

ByteSub
0x87 0xf2 0x4d 0x97
0xec 0x6e 0x4c 0x90
0x4a 0xc3 0x46 0xe7
0x8c 0xd8 0x95 0xa6

ShiftRow
0x87 0xf2 0x4d 0x97
0x6e 0x4c 0x90 0xec
0x46 0xe7 0x4a 0xc3
0xa6 0x8c 0xd8 0x95

MixColumn
0x47 0x40 0xa3 0x4c
0x37 0xd4 0x70 0x9f
0x94 0xe4 0x3a 0x42
0xed 0xa5 0xa6 0xbc

AddRoundKey
0xeb 0x59 0x8b 0x1b
0x40 0x2e 0xa1 0xc3
0xf2 0x38 0x13 0x42
0x1e 0x84 0xe7 0xd2

ByteSub
0xe9 0xcb 0x3d 0xaf
0x9 0x31 0x32 0x2e
0x89 0x7 0x7d 0x2c
0x72 0x5f 0x94 0xb5

ShiftRow
0xe9 0xcb 0x3d 0xaf
0x31 0x32 0x2e 0x9
0x7d 0x2c 0x89 0x7
0xb5 0x72 0x5f 0x94

AddRoundKey
0x39 0x2 0xdc 0x19
0x25 0xdc 0x11 0x6a
0x84 0x9 0x85 0xb
0x1d 0xfb 0x97 0x32

output
0x39 0x2 0xdc 0x19
```

```
0x25 0xdc 0x11 0x6a
0x84 0x9 0x85 0xb
0x1d 0xfb 0x97 0x32
```