aes-Valores_TEST

July 28, 2023

1 Polinomio: 0x177

1.1 Appendix A - Key Expansion Examples

```
-------------------------------------------------------------------------------
Clave 128 bits: 2b7e151628aed2a6abf7158809cf4f3c
-------------------------------------------------------------------------------
w0 2b7e1516
w1 28aed2a6
w2 abf71588
w3 09cf4f3c
w4 0eeb881e
w5 26455ab8
w6 8db24f30
w7 847d000c
w8 dd88c198
w9 fbcd9b20
w10 767fd410
w11 f202d41c
w12 fe8de360
w13 05407840
w14 733fac50
w15 813d784c
w16 a15a2a14
w17 a41a5254
w18 d725fe04
w19 56188648
w20 0c28d69c
w21 a83284c8
w22 7f177acc
w23 290ffc84
w24 9b425066
w25 3370d4ae
w26 4c67ae62
w27 656852e6
w28 1a264fe8
w29 29569b46
w30 65313524
```

```
w31 005967c2
w32 7847d18b
w33 51114acd
w34 34207fe9
w35 3479182b
w36 5bfa653a
w37 0aeb2ff7
w38 3ecb501e
w39 0ab24835
w40 dd0608e7
w41 d7ed2710
w42 e926770e
w43 e3943f3b
--------------------------------------------------------------------------------
Clave 192 bits: 8e73b0f7da0e6452c810f32b809079e562f8ead2522c6b7b
--------------------------------------------------------------------------------
w0 8e73b0f7
w1 da0e6452
w2 c810f32b
w3 809079e5
w4 62f8ead2
w5 522c6b7b
w6 50665b93
w7 8a683fc1
w8 4278ccea
w9 c2e8b50f
w10 a0105fdd
w11 f23c34a6
w12 cfd7bb6b
w13 45bf84aa
w14 07c74840
w15 c52ffd4f
w16 653fa292
w17 97039634
w18 2f980a0b
w19 6a278ea1
w20 6de0c6e1
w21 a8cf3bae
w22 cdf0993c
w23 5af30f08
w24 712f9da9
w25 1b081308
w26 76e8d5e9
w27 de27ee47
w28 13d7777b
w29 49247873
w30 3df806a7
w31 26f015af
```

```
w32 5018c046
w33 8e3f2e01
w34 9de8597a
w35 d4cc2109
w36 9c230ea2
w37 bad31b0d
w38 eacbdb4b
w39 64f4f54a
w40 f91cac30
w41 2dd08d39
w42 ee3885d5
w43 54eb9ed8
w44 be204593
w45 dad4b0d9
w46 23c81ce9
w47 0e1891d0
w48 d3c1b7a3
w49 872a297b
w50 390a6ce8
w51 e3dedc31
--------------------------------------------------------------------------------
Clave 256 bits: 603deb1015ca71be2b73aef0857d77811f352c073b6108d72d9810a30914dff4
--------------------------------------------------------------------------------
w0 603deb10
w1 15ca71be
w2 2b73aef0
w3 857d7781
w4 1f352c07
w5 3b6108d7
w6 2d9810a3
w7 0914dff4
w8 966d8518
w9 83a7f4a6
w10 a8d45a56
w11 2da92dd7
w12 68255bcc
w13 5344531b
w14 7edc43b8
w15 77c89c4c
w16 33744c77
w17 b0d3b8d1
w18 1807e287
w19 35aecf50
w20 057e7f8a
w21 563a2c91
w22 28e66f29
w23 5f2ef365
w24 c822c263
```

```
w25 78f17ab2
w26 60f69835
w27 55585765
w28 e088fb04
w29 b6b2d795
w30 9e54b8bc
w31 c17a4bd9
w32 b919f5e0
w33 c1e88f52
w34 a11e1767
w35 f4464002
w36 8e3b3f23
w37 3889e8b6
w38 a6dd500a
w39 67a71bd3
w40 8cd1cd81
w41 4d3942d3
w42 ec2755b4
w43 186115b6
w44 33a33080
w45 0b2ad836
w46 adf7883c
w47 ca5093ef
w48 eab4dfdf
w49 a78d9d0c
w50 4baac8b8
w51 53cbdd0e
w52 c09a16f6
w53 cbb0cec0
w54 664746fc
w55 ac17d513
w56 67ca3949
w57 c047a445
w58 8bed6cfd
w59 d826b1f3
```

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
0x8c 0xf1 0x9f 0xb
0x57 0x6e 0xa8 0xbf
0xfd 0xad 0x1b 0xfc
0xd8 0xb4 0x55 0x97

ShiftRow
0x8c 0xf1 0x9f 0xb
0x6e 0xa8 0xbf 0x57
0x1b 0xfc 0xfd 0xad
0x97 0xd8 0xb4 0x55

MixColumn
0x51 0x3e 0xb6 0x17
0xea 0x7d 0x52 0x70
0x1a 0xc9 0x6 0x8e
0xcf 0xf7 0x8b 0x4d

AddRoundKey
0x5f 0x18 0x3b 0x93
0x1 0x38 0xe0 0xd
0x92 0x93 0x49 0x8e
0xd1 0x4f 0xbb 0x41

ByteSub
0x14 0xbd 0x69 0x65
0x7c 0xc3 0x4b 0x7
0xd5 0x65 0xe 0x18
0xce 0x95 0x5d 0x80

ShiftRow
0x14 0xbd 0x69 0x65
0xc3 0x4b 0x7 0x7c
0xe 0x18 0xd5 0x65
0x80 0xce 0x95 0x5d

MixColumn
0x94 0x6 0x9b 0x76
0x77 0xcd 0xfa 0x6f
0x3c 0xe3 0x7b 0x34
0x86 0x8 0x34 0xc

AddRoundKey
0x49 0xfd 0xed 0x84
```

```
0xff 0x0 0x85 0x6d
0xfd 0x78 0xaf 0xe0
0x1e 0x28 0x24 0x10

ByteSub
0xe 0x93 0x1c 0x86
0x6c 0x63 0x6 0x94
0x93 0xd7 0xc7 0x4b
0x9 0x29 0x5c 0xd2

ShiftRow
0xe 0x93 0x1c 0x86
0x63 0x6 0x94 0x6c
0xc7 0x4b 0x93 0xd7
0xd2 0x9 0x29 0x5c

MixColumn
0xac 0x19 0x49 0x44
0x24 0x4b 0xa8 0xc
0x95 0x18 0xa2 0xd7
0x65 0x9d 0x71 0xfe

AddRoundKey
0x52 0x1c 0x3a 0xc5
0xa9 0xb 0x97 0x31
0x76 0x60 0xe 0xaf
0x5 0xdd 0x21 0xb2

ByteSub
0x64 0x22 0xc6 0x82
0x10 0xbe 0x60 0x45
0x66 0xd4 0x76 0xc7
0x1e 0x26 0xdb 0x68

ShiftRow
0x64 0x22 0xc6 0x82
0xbe 0x60 0x45 0x10
0x76 0xc7 0x66 0xd4
0x68 0x1e 0x26 0xdb

MixColumn
0x63 0x3d 0x74 0x4c
0x9d 0xc2 0xc0 0x72
0x8e 0x99 0x25 0x57
0xb4 0xfd 0x52 0xf4

AddRoundKey
0xc2 0x99 0xa3 0x1a
```

```
0xc7 0xd8 0xe5 0x6a
0xa4 0xcb 0xdb 0xd1
0xa0 0xa9 0x56 0xbc

ByteSub
0x9e 0x67 0xb8 0x51
0xd9 0x16 0x4a 0xaf
0x2b 0x39 0x35 0xce
0xf1 0x10 0x88 0xca

ShiftRow
0x9e 0x67 0xb8 0x51
0x16 0x4a 0xaf 0xd9
0x35 0xce 0x2b 0x39
0xca 0xf1 0x10 0x88

MixColumn
0x8e 0x2f 0xba 0xf
0x27 0x27 0xfc 0x57
0xcb 0xa2 0x71 0x15
0x15 0xb8 0x1b 0x74

AddRoundKey
0x82 0x87 0xc5 0x26
0xf 0x15 0xeb 0x58
0x1d 0x26 0xb 0xe9
0x89 0x70 0xd7 0xf0

ByteSub
0x92 0xd 0x82 0xa1
0xb7 0xf 0xe3 0xf6
0x28 0xa1 0xbe 0xb
0x2f 0x33 0xcb 0xf2

ShiftRow
0x92 0xd 0x82 0xa1
0xf 0xe3 0xf6 0xb7
0xbe 0xb 0x28 0xa1
0xf2 0x2f 0x33 0xcb

MixColumn
0xe 0x6c 0x5 0xf1
0xcb 0x8e 0x52 0xe7
0xf7 0x89 0x71 0x9
0xe3 0xa1 0x49 0x63

AddRoundKey
0x95 0x5f 0x49 0x94
```

```
0x89 0xfe 0x35 0x8f
0xa7 0x5d 0xdf 0x5b
0x85 0xf 0x2b 0x85

ByteSub
0xb9 0x14 0xe 0x1a
0x2f 0x34 0x6d 0xe7
0x25 0xc5 0x50 0x75
0x6 0xb7 0xb4 0x6

ShiftRow
0xb9 0x14 0xe 0x1a
0x34 0x6d 0xe7 0x2f
0x50 0x75 0x25 0xc5
0x6 0x6 0xb7 0xb4

MixColumn
0xf 0xec 0xd0 0x34
0x27 0x57 0x6f 0xc8
0x27 0x99 0xd 0x63
0xd4 0x28 0xc9 0xdb

AddRoundKey
0x15 0xc5 0xb5 0x34
0x1 0x1 0x5e 0x91
0x68 0x2 0x38 0x4
0x3c 0x6e 0xed 0x19

ByteSub
0xf 0x82 0xf5 0xb1
0x7c 0x7c 0x30 0xf9
0xc1 0x27 0xc3 0x8a
0x9d 0xe9 0x1c 0x8c

ShiftRow
0xf 0x82 0xf5 0xb1
0x7c 0x30 0xf9 0x7c
0xc3 0x8a 0xc1 0x27
0x8c 0x9d 0xe9 0x1c

MixColumn
0xd5 0x34 0xc9 0xaa
0x49 0x96 0xad 0x3c
0x61 0x1 0xb5 0xa7
0xc1 0x6 0xf5 0xc7

AddRoundKey
0xad 0x65 0xfd 0x9e
```

```
0xe 0x87 0x8d 0x45
0xb0 0x4b 0xca 0xbf
0x4a 0xcb 0x1c 0xec

ByteSub
0xdc 0x8e 0x93 0xd3
0x76 0xd 0x1b 0xaa
0xa9 0x3b 0x5e 0xb5
0x91 0x39 0x22 0x2a

ShiftRow
0xdc 0x8e 0x93 0xd3
0xd 0x1b 0xaa 0x76
0x5e 0xb5 0xa9 0x3b
0x2a 0x91 0x39 0x22

MixColumn
0xac 0x62 0x48 0x52
0xe 0x81 0x5 0x50
0x13 0x4c 0x57 0xb5
0x14 0x1e 0xb3 0xb

AddRoundKey
0xf7 0x68 0x76 0x58
0xf4 0x6a 0xce 0xe2
0x76 0x63 0x7 0xfd
0x2e 0xe9 0xad 0x3e

ByteSub
0x6b 0xc1 0x66 0xf6
0x6e 0xaf 0x62 0xad
0x66 0xf4 0xde 0x93
0xff 0xb 0xdc 0x87

ShiftRow
0x6b 0xc1 0x66 0xf6
0xaf 0x62 0xad 0x6e
0xde 0x93 0x66 0xf4
0x87 0xff 0xb 0xdc

AddRoundKey
0xb6 0x16 0x8f 0x15
0xa9 0x8f 0x8b 0xfa
0xd6 0xb4 0x11 0xcb
0x60 0xef 0x5 0xe7

output
0xb6 0x16 0x8f 0x15
```

```
0xa9 0x8f 0x8b 0xfa
0xd6 0xb4 0x11 0xcb
0x60 0xef 0x5 0xe7
```