aes-Valores_TEST

July 28, 2023

1 Polinomio: 0x11d

1.1 Appendix A - Key Expansion Examples

```
--------------------------------------------------------------------------------
Clave 128 bits: 2b7e151628aed2a6abf7158809cf4f3c
--------------------------------------------------------------------------------
w0 2b7e1516
w1 28aed2a6
w2 abf71588
w3 09cf4f3c
w4 9d42c390
w5 b5ec1136
w6 1e1b04be
w7 17d44b82
w8 416ad395
w9 f486c2a3
w10 ea9dc61d
w11 fd498d9f
w12 51cae209
w13 a54c20aa
w14 4fd1e6b7
w15 b2986b28
w16 e315547b
w17 465974d1
w18 09889266
w19 bb10f94e
w20 d1b39314
w21 97eae7c5
w22 9e6275a3
w23 25728ced
w24 7cc70c03
w25 eb2debc6
w26 754f9e65
w27 503d1288
w28 dbec4f8a
w29 30c1a44c
w30 458e3a29
```

```
w31 15b328a1
w32 c55a9d41
w33 f59b390d
w34 b0150324
w35 a5a62b85
w36 3e383254
w37 cba30b59
w38 7bb6087d
w39 de1023f8
w40 2672a821
w41 edd1a378
w42 9667ab05
w43 487788fd
--------------------------------------------------------------------------------
Clave 192 bits: 8e73b0f7da0e6452c810f32b809079e562f8ead2522c6b7b
--------------------------------------------------------------------------------
w0 8e73b0f7
w1 da0e6452
w2 c810f32b
w3 809079e5
w4 62f8ead2
w5 522c6b7b
w6 4dac9748
w7 97a2f31a
w8 5fb20031
w9 df2279d4
w10 bdda9306
w11 eff6f87d
w12 b43627c9
w13 2394d4d3
w14 7c26d4e2
w15 a304ad36
w16 1ede3e30
w17 f128c64d
w18 06183d5c
w19 258ce98f
w20 59aa3d6d
w21 faae905b
w22 e470ae6b
w23 15586826
w24 bd733997
w25 98ffd018
w26 c155ed75
w27 3bfb7d2e
w28 df8bd345
w29 cad3bb63
w30 d61cb5ee
w31 4ee365f6
```

```
w32 8fb68883
w33 b44df5ad
w34 6bc626e8
w35 a1159d8b
w36 3d98ae3c
w37 737bcbca
w38 fccd4349
w39 4880b6e4
w40 2346900c
w41 82530d87
w42 1551502c
w43 662a9be6
w44 9ae7d8af
w45 d2676e4b
w46 f121fe47
w47 7372f3c0
w48 185ffc11
w49 7e7567f7
w50 e492bf58
w51 36f5d113
--------------------------------------------------------------------------------
Clave 256 bits: 603deb1015ca71be2b73aef0857d77811f352c073b6108d72d9810a30914dff4
--------------------------------------------------------------------------------
w0 603deb10
w1 15ca71be
w2 2b73aef0
w3 857d7781
w4 1f352c07
w5 3b6108d7
w6 2d9810a3
w7 0914dff4
w8 a93fa996
w9 bcf5d828
w10 978676d8
w11 12fb0159
w12 34e05033
w13 0f8158e4
w14 22194847
w15 2b0d97b3
w16 62ee37f4
w17 de1befdc
w18 499d9904
w19 5b66985d
w20 522feaea
w21 5daeb20e
w22 7fb7fa49
w23 54ba6dfa
w24 58a20707
```

```
w25 86b9e8db
w26 cf2471df
w27 9442e982
w28 96ee20fa
w29 cb4092f4
w30 b4f768bd
w31 e04d0547
w32 4af018e9
w33 cc49f032
w34 036d81ed
w35 972f686f
w36 47134bb5
w37 8c53d941
w38 38a4b1fc
w39 d8e9b4bb
w40 90e1777b
w41 5ca88749
w42 5fc506a4
w43 c8ea6ecb
w44 a30b6e26
w45 2f58b767
w46 17fc069b
w47 cf15b220
w48 7b93b4cc
w49 273b3385
w50 78fe3521
w51 b0145bea
w52 12c3083e
w53 3d9bbf59
w54 2a67b9c2
w55 e5720be2
w56 b6763e2d
w57 914d0da8
w58 e9b33889
w59 59a76363
```

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
0x60 0x16 0x65 0xca
0xe7 0x42 0x2e 0x9a
0x39 0x8a 0xa0 0x71
0xb5 0x62 0x37 0x94

ShiftRow
0x60 0x16 0x65 0xca
0x42 0x2e 0x9a 0xe7
0xa0 0x71 0x39 0x8a
0x94 0xb5 0x62 0x37

MixColumn
0x32 0x9a 0x22 0x0
0x8d 0x6c 0x65 0xad
0xde 0x18 0x2b 0x7d
0x77 0x12 0xc8 0x40

AddRoundKey
0xaf 0x2f 0x3c 0x17
0xcf 0x80 0x7e 0x79
0x1d 0x9 0x2f 0x36
0xe7 0x24 0x76 0xc2

ByteSub
0xa3 0xfd 0xd6 0x5
0xb7 0x4b 0x83 0xeb
0xcd 0x86 0xfd 0xa4
0x26 0x47 0x1c 0x6c

ShiftRow
0xa3 0xfd 0xd6 0x5
0x4b 0x83 0xeb 0xb7
0xfd 0xa4 0xcd 0x86
0x6c 0x26 0x47 0x1c

MixColumn
0x17 0xfd 0x1b 0x54
0x43 0x31 0x10 0xfd
0xbb 0x41 0x73 0x87
0x96 0x71 0xcf 0x6

AddRoundKey
0x56 0x9 0xf1 0xa9
```

```
0x29 0xb7 0x8d 0xb4
0x68 0x83 0xb5 0xa
0x3 0xd2 0xd2 0x99

ByteSub
0xe3 0x86 0x95 0xa8
0xda 0xaa 0xa0 0x11
0x6b 0x9 0x7 0x41
0x45 0xd3 0xd3 0x5e

ShiftRow
0xe3 0x86 0x95 0xa8
0xaa 0xa0 0x11 0xda
0x7 0x41 0x6b 0x9
0x5e 0x45 0xd3 0xd3

MixColumn
0x61 0xe8 0xbc 0xe4
0xfd 0x5d 0xd9 0xc9
0xa5 0x6b 0x3a 0x8
0x29 0xfc 0x63 0x8d

AddRoundKey
0x30 0x4d 0xf3 0x56
0x37 0x11 0x8 0x51
0x47 0x4b 0xdc 0x63
0x20 0x56 0xd4 0xa5

ByteSub
0x5c 0x1a 0xe 0xe3
0xef 0x88 0x94 0xa1
0x1f 0x28 0xfa 0x8c
0xc3 0xe3 0xde 0x15

ShiftRow
0x5c 0x1a 0xe 0xe3
0x88 0x94 0xa1 0xef
0xfa 0x8c 0x1f 0x28
0x15 0xc3 0xe3 0xde

MixColumn
0xd2 0xda 0x1e 0x1
0x57 0x65 0x93 0x86
0x2 0xd3 0xa9 0x23
0xbc 0xad 0x77 0x5e

AddRoundKey
0x31 0x9c 0x17 0xba
```

```
0x42 0x3c 0x1b 0x96
0x56 0xa7 0x3b 0xda
0xc7 0x7c 0x11 0x10

ByteSub
0xb 0x8b 0x5 0x3e
0xc1 0xd6 0xec 0xc6
0xe3 0x0 0xe8 0xf4
0xa7 0x90 0x88 0x22

ShiftRow
0xb 0x8b 0x5 0x3e
0xd6 0xec 0xc6 0xc1
0xe8 0xf4 0xe3 0x0
0x22 0xa7 0x90 0x88

MixColumn
0xbb 0x71 0x2e 0xaa
0xbd 0xe8 0x3c 0x29
0x76 0x66 0xb5 0x7a
0x67 0xcb 0x17 0x8e

AddRoundKey
0x6a 0xe6 0xb0 0x8f
0xe 0x2 0x5e 0x5b
0xe5 0x81 0xc0 0xf6
0x73 0xe 0xb4 0x63

ByteSub
0x6d 0xf6 0xb1 0x5a
0xce 0x56 0x2c 0x66
0xe1 0x29 0xac 0xfb
0x3d 0xce 0x11 0x8c

ShiftRow
0x6d 0xf6 0xb1 0x5a
0x56 0x2c 0x66 0xce
0xac 0xfb 0xe1 0x29
0x8c 0x3d 0xce 0x11

MixColumn
0x0 0x43 0xfa 0xc3
0xa4 0x83 0x8d 0xb1
0xf7 0x76 0x47 0xf5
0x48 0xaa 0xc8 0x2b

AddRoundKey
0x7c 0xa8 0x8f 0x93
```

```
0x63 0xae 0xc2 0x8c
0xfb 0x9d 0xd9 0xe7
0x4b 0x6c 0xad 0xa3

ByteSub
0x90 0x91 0x5a 0x1
0x8c 0x44 0x6c 0x74
0xd5 0x84 0x97 0x26
0x28 0x80 0x9b 0x69

ShiftRow
0x90 0x91 0x5a 0x1
0x44 0x6c 0x74 0x8c
0x97 0x26 0xd5 0x84
0x69 0x28 0x80 0x9b

MixColumn
0xf 0x85 0x7d 0x94
0xd5 0xb 0x50 0xe
0x5c 0xc9 0x4 0x28
0xac 0xb4 0x52 0x20

AddRoundKey
0xd4 0xb5 0x38 0x81
0x39 0xca 0xde 0xbd
0x13 0x6d 0x3e 0x0
0x26 0xf8 0x7b 0x81

ByteSub
0xde 0x7 0x55 0x29
0xbe 0x79 0x75 0xdb
0xad 0x4c 0xf1 0x63
0x4 0x9a 0x27 0x29

ShiftRow
0xde 0x7 0x55 0x29
0x79 0x75 0xdb 0xbe
0xf1 0x63 0xad 0x4c
0x29 0x4 0x9a 0x27

MixColumn
0xf2 0xf6 0xed 0xe6
0xb 0x4c 0x8e 0xbb
0x23 0xb8 0x7a 0x66
0xa5 0x17 0xa0 0xc7

AddRoundKey
0x37 0x3 0x5d 0x43
```

```
0x51 0xd7 0x9b 0x1d
0xbe 0x81 0x79 0x4d
0xe4 0x1a 0x84 0x42

ByteSub
0xef 0x45 0xd9 0xb9
0xa1 0x98 0x61 0xcd
0xb5 0x29 0xeb 0x1a
0xae 0x36 0x32 0xc1

ShiftRow
0xef 0x45 0xd9 0xb9
0x98 0x61 0xcd 0xa1
0xeb 0x1a 0xb5 0x29
0xc1 0xae 0x36 0x32

MixColumn
0x5c 0x9d 0x66 0x8a
0x23 0x7 0xaa 0xaf
0xe2 0xff 0x39 0x1c
0xc0 0xf5 0x62 0x3a

AddRoundKey
0x62 0x56 0x1d 0x54
0x1b 0xa4 0x1c 0xbf
0xd0 0xf4 0x31 0x3f
0x94 0xac 0x1f 0xc2

ByteSub
0xed 0xe3 0xcd 0xf3
0xec 0xd 0xf 0xbc
0x67 0x42 0xb 0xd7
0xc4 0x99 0x46 0x6c

ShiftRow
0xed 0xe3 0xcd 0xf3
0xd 0xf 0xbc 0xec
0xb 0xd7 0x67 0x42
0x6c 0xc4 0x99 0x46

AddRoundKey
0xcb 0xe 0x5b 0xbb
0x7f 0xde 0xdb 0x9b
0xa3 0x74 0xcc 0xca
0x4d 0xbc 0x9c 0xbb

output
0xcb 0xe 0x5b 0xbb
```

```
0x7f 0xde 0xdb 0x9b
0xa3 0x74 0xcc 0xca
0x4d 0xbc 0x9c 0xbb
```