Blog Entry © Monday, March 9, 2026, by James Pate Williams, Jr. Testing a Translation of My C# Advanced Encryption Standard (AES) to the Programming Language C

Back in 2009 and 2010, I implemented NIST's FIPS 197 encryption algorithm (AES). I was late coming to the AES parade which began in earnest in 2001. In this blog entry I implement two of the test suites found in FIPS 197. The first test is encryption using a 128-bit key. See FIPS 197 Appendix B and then I explore the inverse operation (decryption).

```
== Menu ==
1 Detailed 128-Bit Encryption
2 Detailed 128-Bit Decryption
3 Exit
Enter option = 1
Expanded key
2b7e1516 28aed2a6 abf71588 09cf4f3c

NIST Standard Test Data
Cipher Detailed Example
FIPS 197 Pages 33 to 34

Input into Cipher
32 88 31 e0
43 5a 31 37
f6 30 98 07
a8 8d a2 34
After AddRoundKey
19 a0 9a e9
3d f4 c6 f8
e3 e2 8d 48
be 2b 2a 08
After SubBytes
d4 e0 b8 1e
27 bf b4 41
11 98 5d 52
ae f1 e5 30
After ShiftRows
d4 e0 b8 1e
bf b4 41 27
5d 52 11 98
30 ae f1 e5
After MixColumns
04 e0 48 28
66 cb f8 06
81 19 d3 26
e5 9a 7a 4c
After AddRoundKey
a4 68 6b 02
```

```
9c 9f 5b 6a
7f 35 ea 50
f2 2b 43 49
After SubBytes
49 45 7f 77
de db 39 02
d2 96 87 53
89 f1 1a 3b
After ShiftRows
49 45 7f 77
db 39 02 de
87 53 d2 96
3b 89 f1 1a
After MixColumns
58 1b db 1b
4d 4b e7 6b
ca 5a ca b0
f1 ac a8 e5
After AddRoundKey
aa 61 82 68
8f dd d2 32
5f e3 4a 46
03 ef d2 9a
After SubBytes
ac ef 13 45
73 c1 b5 23
cf 11 d6 5a
7b df b5 b8
After ShiftRows
ac ef 13 45
c1 b5 23 73
d6 5a cf 11
b8 7b df b5
After MixColumns
75 20 53 bb
ec 0b c0 25
09 63 cf d0
93 33 7c dc
After AddRoundKey
48 67 4d d6
6c 1d e3 5f
4e 9d b1 58
ee 0d 38 e7
After SubBytes
52 85 e3 f6
50 a4 11 cf
2f 5e c8 6a
```

28 d7 07 94
After ShiftRows
52 85 e3 f6
a4 11 cf 50
c8 6a 2f 5e
94 28 d7 07
After MixColumns
0f 60 6f 5e
d6 31 c0 b3
da 38 10 13
a9 bf 6b 01
After AddRoundKey
e0 c8 d9 85
92 63 b1 b8
7f 63 35 be
e8 c0 50 01
After SubBytes
e1 e8 35 97
4f fb c8 6c
d2 fb 96 ae
9b ba 53 7c
After ShiftRows
e1 e8 35 97
fb c8 6c 4f
96 ae d2 fb
7c 9b ba 53
After MixColumns
25 bd b6 4c
d1 11 3a 4c
a9 d1 33 c0
ad 68 8e b0
After AddRoundKey
f1 c1 7c 5d
00 92 c8 b5
6f 4c 8b d5
55 ef 32 0c
After SubBytes
a1 78 10 4c
63 4f e8 d5
a8 29 3d 03
fc df 23 fe
After ShiftRows
a1 78 10 4c
4f e8 d5 63
3d 03 a8 29
fe fc df 23
After MixColumns

```
4b 2c 33 37
86 4a 9d d2
8d 89 f4 18
6d 80 e8 d8
After AddRoundKey
26 3d e8 fd
0e 41 64 d2
2e b7 72 8b
17 7d a9 25
After SubBytes
f7 27 9b 54
ab 83 43 b5
31 a9 40 3d
f0 ff d3 3f
After ShiftRows
f7 27 9b 54
83 43 b5 ab
40 3d 31 a9
3f f0 ff d3
After MixColumns
14 46 27 34
15 16 46 2a
b5 15 56 d8
bf ec d7 43
After AddRoundKey
5a 19 a3 7a
41 49 e0 8c
42 dc 19 04
b1 1f 65 0c
After SubBytes
be d4 0a da
83 3b e1 64
2c 86 d4 f2
c8 c0 4d fe
After ShiftRows
be d4 0a da
3b e1 64 83
d4 f2 2c 86
fe c8 c0 4d
After MixColumns
00 b1 54 fa
51 c8 76 1b
2f 89 6d 99
d1 ff cd ea
After AddRoundKey
ea 04 65 85
83 45 5d 96
```

```
5c 33 98 b0
f0 2d ad c5
After SubBytes
87 f2 4d 97
ec 6e 4c 90
4a c3 46 e7
8c d8 95 a6
After ShiftRows
87 f2 4d 97
6e 4c 90 ec
46 e7 4a c3
a6 8c d8 95
After MixColumns
47 40 a3 4c
37 d4 70 9f
94 e4 3a 42
ed a5 a6 bc
After AddRoundKey
eb 59 8b 1b
40 2e a1 c3
f2 38 13 42
1e 84 e7 d2
After SubBytes
e9 cb 3d af
09 31 32 2e
89 07 7d 2c
72 5f 94 b5
After ShiftRows
e9 cb 3d af
31 32 2e 09
7d 2c 89 07
b5 72 5f 94
After AddRoundKey
39 02 dc 19
25 dc 11 6a
84 09 85 0b
1d fb 97 32

== Menu ==
1 Detailed 128-Bit Encryption
2 Detailed 128-Bit Decryption
3 Exit
Enter option = 2
Expanded key
2b7e1516 28aed2a6 abf71588 09cf4f3c

NIST Standard Test Data
```

Inverse Cipher Detailed Example
FIPS 197 Pages 33 to 34

Input to Inverse Cipher
39 02 dc 19
25 dc 11 6a
84 09 85 0b
1d fb 97 32
After AddRoundKey
e9 cb 3d af
31 32 2e 09
7d 2c 89 07
b5 72 5f 94
After InvShiftRows
e9 cb 3d af
09 31 32 2e
89 07 7d 2c
72 5f 94 b5
After InvSubBytes
eb 59 8b 1b
40 2e a1 c3
f2 38 13 42
1e 84 e7 d2
After AddRoundKey
47 40 a3 4c
37 d4 70 9f
94 e4 3a 42
ed a5 a6 bc
After InvMixColumns
87 f2 4d 97
6e 4c 90 ec
46 e7 4a c3
a6 8c d8 95
After InvShiftRows
87 f2 4d 97
ec 6e 4c 90
4a c3 46 e7
8c d8 95 a6
After InvSubBytes
ea 04 65 85
83 45 5d 96
5c 33 98 b0
f0 2d ad c5
After AddRoundKey
00 b1 54 fa
51 c8 76 1b
2f 89 6d 99

```
d1 ff cd ea
After InvMixColumns
be d4 0a da
3b e1 64 83
d4 f2 2c 86
fe c8 c0 4d
After InvShiftRows
be d4 0a da
83 3b e1 64
2c 86 d4 f2
c8 c0 4d fe
After InvSubBytes
5a 19 a3 7a
41 49 e0 8c
42 dc 19 04
b1 1f 65 0c
After AddRoundKey
14 46 27 34
15 16 46 2a
b5 15 56 d8
bf ec d7 43
After InvMixColumns
f7 27 9b 54
83 43 b5 ab
40 3d 31 a9
3f f0 ff d3
After InvShiftRows
f7 27 9b 54
ab 83 43 b5
31 a9 40 3d
f0 ff d3 3f
After InvSubBytes
26 3d e8 fd
0e 41 64 d2
2e b7 72 8b
17 7d a9 25
After AddRoundKey
4b 2c 33 37
86 4a 9d d2
8d 89 f4 18
6d 80 e8 d8
After InvMixColumns
a1 78 10 4c
4f e8 d5 63
3d 03 a8 29
fe fc df 23
After InvShiftRows
```

```
a1 78 10 4c
63 4f e8 d5
a8 29 3d 03
fc df 23 fe
After InvSubBytes
f1 c1 7c 5d
00 92 c8 b5
6f 4c 8b d5
55 ef 32 0c
After AddRoundKey
25 bd b6 4c
d1 11 3a 4c
a9 d1 33 c0
ad 68 8e b0
After InvMixColumns
e1 e8 35 97
fb c8 6c 4f
96 ae d2 fb
7c 9b ba 53
After InvShiftRows
e1 e8 35 97
4f fb c8 6c
d2 fb 96 ae
9b ba 53 7c
After InvSubBytes
e0 c8 d9 85
92 63 b1 b8
7f 63 35 be
e8 c0 50 01
After AddRoundKey
0f 60 6f 5e
d6 31 c0 b3
da 38 10 13
a9 bf 6b 01
After InvMixColumns
52 85 e3 f6
a4 11 cf 50
c8 6a 2f 5e
94 28 d7 07
After InvShiftRows
52 85 e3 f6
50 a4 11 cf
2f 5e c8 6a
28 d7 07 94
After InvSubBytes
48 67 4d d6
6c 1d e3 5f
```

```
4e 9d b1 58
ee 0d 38 e7
After AddRoundKey
75 20 53 bb
ec 0b c0 25
09 63 cf d0
93 33 7c dc
After InvMixColumns
ac ef 13 45
c1 b5 23 73
d6 5a cf 11
b8 7b df b5
After InvShiftRows
ac ef 13 45
73 c1 b5 23
cf 11 d6 5a
7b df b5 b8
After InvSubBytes
aa 61 82 68
8f dd d2 32
5f e3 4a 46
03 ef d2 9a
After AddRoundKey
58 1b db 1b
4d 4b e7 6b
ca 5a ca b0
f1 ac a8 e5
After InvMixColumns
49 45 7f 77
db 39 02 de
87 53 d2 96
3b 89 f1 1a
After InvShiftRows
49 45 7f 77
de db 39 02
d2 96 87 53
89 f1 1a 3b
After InvSubBytes
a4 68 6b 02
9c 9f 5b 6a
7f 35 ea 50
f2 2b 43 49
After AddRoundKey
04 e0 48 28
66 cb f8 06
81 19 d3 26
e5 9a 7a 4c
```

After InvMixColumns
d4 e0 b8 1e
bf b4 41 27
5d 52 11 98
30 ae f1 e5
After InvShiftRows
d4 e0 b8 1e
27 bf b4 41
11 98 5d 52
ae f1 e5 30
After InvSubBytes
19 a0 9a e9
3d f4 c6 f8
e3 e2 8d 48
be 2b 2a 08
After AddRoundKey
32 88 31 e0
43 5a 31 37
f6 30 98 07
a8 8d a2 34