

Appendix A - Key Expansion Examples

This appendix shows the development of the key schedule for various key sizes. Note that multi-byte values are presented using the notation described in Sec. 3. The intermediate values produced during the development of the key schedule (see Sec. 5.2) are given in the following table (all values are in hexadecimal format, with the exception of the index column (i)).

A.1 Expansion of a 128-bit Cipher Key

This section contains the key expansion of the following cipher key:

Cipher Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

for $Nk = 4$, which results in

$w_0 = 2b7e1516$ $w_1 = 28aed2a6$ $w_2 = abf71588$ $w_3 = 09cf4f3c$

i (dec)	temp	After RotWord()	After SubWord()	Rcon[i/Nk]	After XOR with Rcon	w[i-Nk]	w[i]= temp XOR w[i-Nk]
4	09cf4f3c	cf4f3c09	8a84eb01	01000000	8b84eb01	2b7e1516	a0fafa17
5	a0fafa17					28aed2a6	88542cb1
6	88542cb1					abf71588	23a33939
7	23a33939					09cf4f3c	2a6c7605
8	2a6c7605	6c76052a	50386be5	02000000	52386be5	a0fafa17	f2c295f2
9	f2c295f2					88542cb1	7a96b943
10	7a96b943					23a33939	5935807a
11	5935807a					2a6c7605	7359f67f
12	7359f67f	59f67f73	cb42d28f	04000000	cf42d28f	f2c295f2	3d80477d
13	3d80477d					7a96b943	4716fe3e
14	4716fe3e					5935807a	1e237e44
15	1e237e44					7359f67f	6d7a883b
16	6d7a883b	7a883b6d	dac4e23c	08000000	d2c4e23c	3d80477d	ef44a541
17	ef44a541					4716fe3e	a8525b7f
18	a8525b7f					1e237e44	b671253b
19	b671253b					6d7a883b	db0bad00
20	db0bad00	0bad00db	2b9563b9	10000000	3b9563b9	ef44a541	d4d1c6f8
21	d4d1c6f8					a8525b7f	7c839d87
22	7c839d87					b671253b	caf2b8bc
23	caf2b8bc					db0bad00	11f915bc

24	11f915bc	f915bc11	99596582	20000000	b9596582	d4d1c6f8	6d88a37a
25	6d88a37a					7c839d87	110b3efd
26	110b3efd					caf2b8bc	dbf98641
27	dbf98641					11f915bc	ca0093fd
28	ca0093fd	0093fdca	63dc5474	40000000	23dc5474	6d88a37a	4e54f70e
29	4e54f70e					110b3efd	5f5fc9f3
30	5f5fc9f3					dbf98641	84a64fb2
31	84a64fb2					ca0093fd	4ea6dc4f
32	4ea6dc4f	a6dc4f4e	2486842f	80000000	a486842f	4e54f70e	ead27321
33	ead27321					5f5fc9f3	b58dbad2
34	b58dbad2					84a64fb2	312bf560
35	312bf560					4ea6dc4f	7f8d292f
36	7f8d292f	8d292f7f	5da515d2	1b000000	46a515d2	ead27321	ac7766f3
37	ac7766f3					b58dbad2	19fadc21
38	19fadc21					312bf560	28d12941
39	28d12941					7f8d292f	575c006e
40	575c006e	5c006e57	4a639f5b	36000000	7c639f5b	ac7766f3	d014f9a8
41	d014f9a8					19fadc21	c9ee2589
42	c9ee2589					28d12941	e13f0cc8
43	e13f0cc8					575c006e	b6630ca6

A.2 Expansion of a 192-bit Cipher Key

This section contains the key expansion of the following cipher key:

Cipher Key = 8e 73 b0 f7 da 0e 64 52 c8 10 f3 2b
 80 90 79 e5 62 f8 ea d2 52 2c 6b 7b

for $Nk = 6$, which results in

$w_0 = 8e73b0f7$ $w_1 = da0e6452$ $w_2 = c810f32b$ $w_3 = 809079e5$
 $w_4 = 62f8ead2$ $w_5 = 522c6b7b$

i (dec)	temp	After RotWord()	After SubWord()	Rcon[i/Nk]	After XOR with Rcon	w[i-Nk]	w[i]= temp XOR w[i-Nk]
6	522c6b7b	2c6b7b52	717f2100	01000000	707f2100	8e73b0f7	fe0c91f7
7	fe0c91f7					da0e6452	2402f5a5
8	2402f5a5					c810f32b	ec12068e

Appendix B – Cipher Example

The following diagram shows the values in the State array as the Cipher progresses for a block length and a Cipher Key length of 16 bytes each (i.e., $Nb = 4$ and $Nk = 4$).

Input = 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34

Cipher Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

The Round Key values are taken from the Key Expansion example in Appendix A.

Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns	Round Key Value																																																																																	
input	<table><tr><td>32</td><td>88</td><td>31</td><td>e0</td></tr><tr><td>43</td><td>5a</td><td>31</td><td>37</td></tr><tr><td>f6</td><td>30</td><td>98</td><td>07</td></tr><tr><td>a8</td><td>8d</td><td>a2</td><td>34</td></tr></table>	32	88	31	e0	43	5a	31	37	f6	30	98	07	a8	8d	a2	34	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table><tr><td>2b</td><td>28</td><td>ab</td><td>09</td></tr><tr><td>7e</td><td>ae</td><td>f7</td><td>cf</td></tr><tr><td>15</td><td>d2</td><td>15</td><td>4f</td></tr><tr><td>16</td><td>a6</td><td>88</td><td>3c</td></tr></table> \oplus	2b	28	ab	09	7e	ae	f7	cf	15	d2	15	4f	16	a6	88	3c	=
	32	88	31	e0																																																																																		
	43	5a	31	37																																																																																		
	f6	30	98	07																																																																																		
a8	8d	a2	34																																																																																			
2b	28	ab	09																																																																																			
7e	ae	f7	cf																																																																																			
15	d2	15	4f																																																																																			
16	a6	88	3c																																																																																			
1	<table><tr><td>19</td><td>a0</td><td>9a</td><td>e9</td></tr><tr><td>3d</td><td>f4</td><td>c6</td><td>f8</td></tr><tr><td>e3</td><td>e2</td><td>8d</td><td>48</td></tr><tr><td>be</td><td>2b</td><td>2a</td><td>08</td></tr></table>	19	a0	9a	e9	3d	f4	c6	f8	e3	e2	8d	48	be	2b	2a	08	<table><tr><td>d4</td><td>e0</td><td>b8</td><td>1e</td></tr><tr><td>27</td><td>bf</td><td>b4</td><td>41</td></tr><tr><td>11</td><td>98</td><td>5d</td><td>52</td></tr><tr><td>ae</td><td>f1</td><td>e5</td><td>30</td></tr></table>	d4	e0	b8	1e	27	bf	b4	41	11	98	5d	52	ae	f1	e5	30	<table><tr><td>d4</td><td>e0</td><td>b8</td><td>1e</td></tr><tr><td>bf</td><td>b4</td><td>41</td><td>27</td></tr><tr><td>5d</td><td>52</td><td>11</td><td>98</td></tr><tr><td>30</td><td>ae</td><td>f1</td><td>e5</td></tr></table>	d4	e0	b8	1e	bf	b4	41	27	5d	52	11	98	30	ae	f1	e5	<table><tr><td>04</td><td>e0</td><td>48</td><td>28</td></tr><tr><td>66</td><td>cb</td><td>f8</td><td>06</td></tr><tr><td>81</td><td>19</td><td>d3</td><td>26</td></tr><tr><td>e5</td><td>9a</td><td>7a</td><td>4c</td></tr></table> \oplus	04	e0	48	28	66	cb	f8	06	81	19	d3	26	e5	9a	7a	4c	<table><tr><td>a0</td><td>88</td><td>23</td><td>2a</td></tr><tr><td>fa</td><td>54</td><td>a3</td><td>6c</td></tr><tr><td>fe</td><td>2c</td><td>39</td><td>76</td></tr><tr><td>17</td><td>b1</td><td>39</td><td>05</td></tr></table> \oplus	a0	88	23	2a	fa	54	a3	6c	fe	2c	39	76	17	b1	39	05	=
	19	a0	9a	e9																																																																																		
	3d	f4	c6	f8																																																																																		
	e3	e2	8d	48																																																																																		
be	2b	2a	08																																																																																			
d4	e0	b8	1e																																																																																			
27	bf	b4	41																																																																																			
11	98	5d	52																																																																																			
ae	f1	e5	30																																																																																			
d4	e0	b8	1e																																																																																			
bf	b4	41	27																																																																																			
5d	52	11	98																																																																																			
30	ae	f1	e5																																																																																			
04	e0	48	28																																																																																			
66	cb	f8	06																																																																																			
81	19	d3	26																																																																																			
e5	9a	7a	4c																																																																																			
a0	88	23	2a																																																																																			
fa	54	a3	6c																																																																																			
fe	2c	39	76																																																																																			
17	b1	39	05																																																																																			
2	<table><tr><td>a4</td><td>68</td><td>6b</td><td>02</td></tr><tr><td>9c</td><td>9f</td><td>5b</td><td>6a</td></tr><tr><td>7f</td><td>35</td><td>ea</td><td>50</td></tr><tr><td>f2</td><td>2b</td><td>43</td><td>49</td></tr></table>	a4	68	6b	02	9c	9f	5b	6a	7f	35	ea	50	f2	2b	43	49	<table><tr><td>49</td><td>45</td><td>7f</td><td>77</td></tr><tr><td>de</td><td>db</td><td>39</td><td>02</td></tr><tr><td>d2</td><td>96</td><td>87</td><td>53</td></tr><tr><td>89</td><td>f1</td><td>1a</td><td>3b</td></tr></table>	49	45	7f	77	de	db	39	02	d2	96	87	53	89	f1	1a	3b	<table><tr><td>49</td><td>45</td><td>7f</td><td>77</td></tr><tr><td>db</td><td>39</td><td>02</td><td>de</td></tr><tr><td>87</td><td>53</td><td>d2</td><td>96</td></tr><tr><td>3b</td><td>89</td><td>f1</td><td>1a</td></tr></table>	49	45	7f	77	db	39	02	de	87	53	d2	96	3b	89	f1	1a	<table><tr><td>58</td><td>1b</td><td>db</td><td>1b</td></tr><tr><td>4d</td><td>4b</td><td>e7</td><td>6b</td></tr><tr><td>ca</td><td>5a</td><td>ca</td><td>b0</td></tr><tr><td>f1</td><td>ac</td><td>a8</td><td>e5</td></tr></table> \oplus	58	1b	db	1b	4d	4b	e7	6b	ca	5a	ca	b0	f1	ac	a8	e5	<table><tr><td>f2</td><td>7a</td><td>59</td><td>73</td></tr><tr><td>c2</td><td>96</td><td>35</td><td>59</td></tr><tr><td>95</td><td>b9</td><td>80</td><td>f6</td></tr><tr><td>f2</td><td>43</td><td>7a</td><td>7f</td></tr></table> \oplus	f2	7a	59	73	c2	96	35	59	95	b9	80	f6	f2	43	7a	7f	=
	a4	68	6b	02																																																																																		
	9c	9f	5b	6a																																																																																		
	7f	35	ea	50																																																																																		
f2	2b	43	49																																																																																			
49	45	7f	77																																																																																			
de	db	39	02																																																																																			
d2	96	87	53																																																																																			
89	f1	1a	3b																																																																																			
49	45	7f	77																																																																																			
db	39	02	de																																																																																			
87	53	d2	96																																																																																			
3b	89	f1	1a																																																																																			
58	1b	db	1b																																																																																			
4d	4b	e7	6b																																																																																			
ca	5a	ca	b0																																																																																			
f1	ac	a8	e5																																																																																			
f2	7a	59	73																																																																																			
c2	96	35	59																																																																																			
95	b9	80	f6																																																																																			
f2	43	7a	7f																																																																																			
3	<table><tr><td>aa</td><td>61</td><td>82</td><td>68</td></tr><tr><td>8f</td><td>dd</td><td>d2</td><td>32</td></tr><tr><td>5f</td><td>e3</td><td>4a</td><td>46</td></tr><tr><td>03</td><td>ef</td><td>d2</td><td>9a</td></tr></table>	aa	61	82	68	8f	dd	d2	32	5f	e3	4a	46	03	ef	d2	9a	<table><tr><td>ac</td><td>ef</td><td>13</td><td>45</td></tr><tr><td>73</td><td>c1</td><td>b5</td><td>23</td></tr><tr><td>cf</td><td>11</td><td>d6</td><td>5a</td></tr><tr><td>7b</td><td>df</td><td>b5</td><td>b8</td></tr></table>	ac	ef	13	45	73	c1	b5	23	cf	11	d6	5a	7b	df	b5	b8	<table><tr><td>ac</td><td>ef</td><td>13</td><td>45</td></tr><tr><td>c1</td><td>b5</td><td>23</td><td>73</td></tr><tr><td>d6</td><td>5a</td><td>cf</td><td>11</td></tr><tr><td>b8</td><td>7b</td><td>df</td><td>b5</td></tr></table>	ac	ef	13	45	c1	b5	23	73	d6	5a	cf	11	b8	7b	df	b5	<table><tr><td>75</td><td>20</td><td>53</td><td>bb</td></tr><tr><td>ec</td><td>0b</td><td>c0</td><td>25</td></tr><tr><td>09</td><td>63</td><td>cf</td><td>d0</td></tr><tr><td>93</td><td>33</td><td>7c</td><td>dc</td></tr></table> \oplus	75	20	53	bb	ec	0b	c0	25	09	63	cf	d0	93	33	7c	dc	<table><tr><td>3d</td><td>47</td><td>1e</td><td>6d</td></tr><tr><td>80</td><td>16</td><td>23</td><td>7a</td></tr><tr><td>47</td><td>fe</td><td>7e</td><td>88</td></tr><tr><td>7d</td><td>3e</td><td>44</td><td>3b</td></tr></table> \oplus	3d	47	1e	6d	80	16	23	7a	47	fe	7e	88	7d	3e	44	3b	=
	aa	61	82	68																																																																																		
	8f	dd	d2	32																																																																																		
	5f	e3	4a	46																																																																																		
03	ef	d2	9a																																																																																			
ac	ef	13	45																																																																																			
73	c1	b5	23																																																																																			
cf	11	d6	5a																																																																																			
7b	df	b5	b8																																																																																			
ac	ef	13	45																																																																																			
c1	b5	23	73																																																																																			
d6	5a	cf	11																																																																																			
b8	7b	df	b5																																																																																			
75	20	53	bb																																																																																			
ec	0b	c0	25																																																																																			
09	63	cf	d0																																																																																			
93	33	7c	dc																																																																																			
3d	47	1e	6d																																																																																			
80	16	23	7a																																																																																			
47	fe	7e	88																																																																																			
7d	3e	44	3b																																																																																			
4	<table><tr><td>48</td><td>67</td><td>4d</td><td>d6</td></tr><tr><td>6c</td><td>1d</td><td>e3</td><td>5f</td></tr><tr><td>4e</td><td>9d</td><td>b1</td><td>58</td></tr><tr><td>ee</td><td>0d</td><td>38</td><td>e7</td></tr></table>	48	67	4d	d6	6c	1d	e3	5f	4e	9d	b1	58	ee	0d	38	e7	<table><tr><td>52</td><td>85</td><td>e3</td><td>f6</td></tr><tr><td>50</td><td>a4</td><td>11</td><td>cf</td></tr><tr><td>2f</td><td>5e</td><td>c8</td><td>6a</td></tr><tr><td>28</td><td>d7</td><td>07</td><td>94</td></tr></table>	52	85	e3	f6	50	a4	11	cf	2f	5e	c8	6a	28	d7	07	94	<table><tr><td>52</td><td>85</td><td>e3</td><td>f6</td></tr><tr><td>a4</td><td>11</td><td>cf</td><td>50</td></tr><tr><td>c8</td><td>6a</td><td>2f</td><td>5e</td></tr><tr><td>94</td><td>28</td><td>d7</td><td>07</td></tr></table>	52	85	e3	f6	a4	11	cf	50	c8	6a	2f	5e	94	28	d7	07	<table><tr><td>0f</td><td>60</td><td>6f</td><td>5e</td></tr><tr><td>d6</td><td>31</td><td>c0</td><td>b3</td></tr><tr><td>da</td><td>38</td><td>10</td><td>13</td></tr><tr><td>a9</td><td>bf</td><td>6b</td><td>01</td></tr></table> \oplus	0f	60	6f	5e	d6	31	c0	b3	da	38	10	13	a9	bf	6b	01	<table><tr><td>ef</td><td>a8</td><td>b6</td><td>db</td></tr><tr><td>44</td><td>52</td><td>71</td><td>0b</td></tr><tr><td>a5</td><td>5b</td><td>25</td><td>ad</td></tr><tr><td>41</td><td>7f</td><td>3b</td><td>00</td></tr></table> \oplus	ef	a8	b6	db	44	52	71	0b	a5	5b	25	ad	41	7f	3b	00	=
	48	67	4d	d6																																																																																		
	6c	1d	e3	5f																																																																																		
	4e	9d	b1	58																																																																																		
ee	0d	38	e7																																																																																			
52	85	e3	f6																																																																																			
50	a4	11	cf																																																																																			
2f	5e	c8	6a																																																																																			
28	d7	07	94																																																																																			
52	85	e3	f6																																																																																			
a4	11	cf	50																																																																																			
c8	6a	2f	5e																																																																																			
94	28	d7	07																																																																																			
0f	60	6f	5e																																																																																			
d6	31	c0	b3																																																																																			
da	38	10	13																																																																																			
a9	bf	6b	01																																																																																			
ef	a8	b6	db																																																																																			
44	52	71	0b																																																																																			
a5	5b	25	ad																																																																																			
41	7f	3b	00																																																																																			
5	<table><tr><td>e0</td><td>c8</td><td>d9</td><td>85</td></tr><tr><td>92</td><td>63</td><td>b1</td><td>b8</td></tr><tr><td>7f</td><td>63</td><td>35</td><td>be</td></tr><tr><td>e8</td><td>c0</td><td>50</td><td>01</td></tr></table>	e0	c8	d9	85	92	63	b1	b8	7f	63	35	be	e8	c0	50	01	<table><tr><td>e1</td><td>e8</td><td>35</td><td>97</td></tr><tr><td>4f</td><td>fb</td><td>c8</td><td>6c</td></tr><tr><td>d2</td><td>fb</td><td>96</td><td>ae</td></tr><tr><td>9b</td><td>ba</td><td>53</td><td>7c</td></tr></table>	e1	e8	35	97	4f	fb	c8	6c	d2	fb	96	ae	9b	ba	53	7c	<table><tr><td>e1</td><td>e8</td><td>35</td><td>97</td></tr><tr><td>fb</td><td>c8</td><td>6c</td><td>4f</td></tr><tr><td>96</td><td>ae</td><td>d2</td><td>fb</td></tr><tr><td>7c</td><td>9b</td><td>ba</td><td>53</td></tr></table>	e1	e8	35	97	fb	c8	6c	4f	96	ae	d2	fb	7c	9b	ba	53	<table><tr><td>25</td><td>bd</td><td>b6</td><td>4c</td></tr><tr><td>d1</td><td>11</td><td>3a</td><td>4c</td></tr><tr><td>a9</td><td>d1</td><td>33</td><td>c0</td></tr><tr><td>ad</td><td>68</td><td>8e</td><td>b0</td></tr></table> \oplus	25	bd	b6	4c	d1	11	3a	4c	a9	d1	33	c0	ad	68	8e	b0	<table><tr><td>d4</td><td>7c</td><td>ca</td><td>11</td></tr><tr><td>d1</td><td>83</td><td>f2</td><td>f9</td></tr><tr><td>c6</td><td>9d</td><td>b8</td><td>15</td></tr><tr><td>f8</td><td>87</td><td>bc</td><td>bc</td></tr></table> \oplus	d4	7c	ca	11	d1	83	f2	f9	c6	9d	b8	15	f8	87	bc	bc	=
	e0	c8	d9	85																																																																																		
	92	63	b1	b8																																																																																		
	7f	63	35	be																																																																																		
e8	c0	50	01																																																																																			
e1	e8	35	97																																																																																			
4f	fb	c8	6c																																																																																			
d2	fb	96	ae																																																																																			
9b	ba	53	7c																																																																																			
e1	e8	35	97																																																																																			
fb	c8	6c	4f																																																																																			
96	ae	d2	fb																																																																																			
7c	9b	ba	53																																																																																			
25	bd	b6	4c																																																																																			
d1	11	3a	4c																																																																																			
a9	d1	33	c0																																																																																			
ad	68	8e	b0																																																																																			
d4	7c	ca	11																																																																																			
d1	83	f2	f9																																																																																			
c6	9d	b8	15																																																																																			
f8	87	bc	bc																																																																																			

6

f1	c1	7c	5d
00	92	c8	b5
6f	4c	8b	d5
55	ef	32	0c

a1	78	10	4c
63	4f	e8	d5
a8	29	3d	03
fc	df	23	fe

a1	78	10	4c
4f	e8	d5	63
3d	03	a8	29
fe	fc	df	23

4b	2c	33	37
86	4a	9d	d2
8d	89	f4	18
6d	80	e8	d8

 \oplus

6d	11	db	ca
88	0b	f9	00
a3	3e	86	93
7a	fd	41	fd

=

7

26	3d	e8	fd
0e	41	64	d2
2e	b7	72	8b
17	7d	a9	25

f7	27	9b	54
ab	83	43	b5
31	a9	40	3d
f0	ff	d3	3f

f7	27	9b	54
83	43	b5	ab
40	3d	31	a9
3f	f0	ff	d3

14	46	27	34
15	16	46	2a
b5	15	56	d8
bf	ec	d7	43

 \oplus

4e	5f	84	4e
54	5f	a6	a6
f7	c9	4f	dc
0e	f3	b2	4f

=

8

5a	19	a3	7a
41	49	e0	8c
42	dc	19	04
b1	1f	65	0c

be	d4	0a	da
83	3b	e1	64
2c	86	d4	f2
c8	c0	4d	fe

be	d4	0a	da
3b	e1	64	83
d4	f2	2c	86
fe	c8	c0	4d

00	b1	54	fa
51	c8	76	1b
2f	89	6d	99
d1	ff	cd	ea

 \oplus

ea	b5	31	7f
d2	8d	2b	8d
73	ba	f5	29
21	d2	60	2f

=

9

ea	04	65	85
83	45	5d	96
5c	33	98	b0
f0	2d	ad	c5

87	f2	4d	97
ec	6e	4c	90
4a	c3	46	e7
8c	d8	95	a6

87	f2	4d	97
6e	4c	90	ec
46	e7	4a	c3
a6	8c	d8	95

47	40	a3	4c
37	d4	70	9f
94	e4	3a	42
ed	a5	a6	bc

 \oplus

ac	19	28	57
77	fa	d1	5c
66	dc	29	00
f3	21	41	6e

=

10

eb	59	8b	1b
40	2e	a1	c3
f2	38	13	42
1e	84	e7	d2

e9	cb	3d	af
09	31	32	2e
89	07	7d	2c
72	5f	94	b5

e9	cb	3d	af
31	32	2e	09
7d	2c	89	07
b5	72	5f	94

 \oplus

d0	c9	e1	b6
14	ee	3f	63
f9	25	0c	0c
a8	89	c8	a6

=

output

39	02	dc	19
25	dc	11	6a
84	09	85	0b
1d	fb	97	32

Appendix C – Example Vectors

This appendix contains example vectors, including intermediate values – for all three AES key lengths ($Nk = 4, 6$, and 8), for the Cipher, Inverse Cipher, and Equivalent Inverse Cipher that are described in Sec. 5.1, 5.3, and 5.3.5, respectively. Additional examples may be found at [1] and [5].

All vectors are in hexadecimal notation, with each pair of characters giving a byte value in which the left character of each pair provides the bit pattern for the 4 bit group containing the higher numbered bits using the notation explained in Sec. 3.2, while the right character provides the bit pattern for the lower-numbered bits. The array index for all bytes (groups of two hexadecimal digits) within these test vectors starts at zero and increases from left to right.

Legend for CIPHER (ENCRYPT) (round number $r = 0$ to $10, 12$ or 14):

```
input:    cipher input
start:    state at start of round[r]
s_box:    state after SubBytes()
s_row:    state after ShiftRows()
m_col:    state after MixColumns()
k_sch:    key schedule value for round[r]
output:   cipher output
```

Legend for INVERSE CIPHER (DECRYPT) (round number $r = 0$ to $10, 12$ or 14):

```
iinput:   inverse cipher input
istart:   state at start of round[r]
is_box:   state after InvSubBytes()
is_row:   state after InvShiftRows()
ik_sch:   key schedule value for round[r]
ik_add:   state after AddRoundKey()
ioutput:  inverse cipher output
```

Legend for EQUIVALENT INVERSE CIPHER (DECRYPT) (round number $r = 0$ to $10, 12$ or 14):

```
iinput:   inverse cipher input
istart:   state at start of round[r]
is_box:   state after InvSubBytes()
is_row:   state after InvShiftRows()
im_col:   state after InvMixColumns()
ik_sch:   key schedule value for round[r]
ioutput:  inverse cipher output
```

C.1 AES-128 ($Nk=4, Nr=10$)

```
PLAINTEXT:    00112233445566778899aabbccddeeff
KEY:          000102030405060708090a0b0c0d0e0f
```

CIPHER (ENCRYPT):

```

round[ 0].input      00112233445566778899aabbccddeeff
round[ 0].k_sch      000102030405060708090a0b0c0d0e0f
round[ 1].start      00102030405060708090a0b0c0d0e0f0
round[ 1].s_box      63cab7040953d051cd60e0e7ba70e18c
round[ 1].s_row      6353e08c0960e104cd70b751bacad0e7
round[ 1].m_col      5f72641557f5bc92f7be3b291db9f91a
round[ 1].k_sch      d6aa74fdd2af72fadaa678f1d6ab76fe
round[ 2].start      89d810e8855ace682d1843d8cb128fe4
round[ 2].s_box      a761ca9b97be8b45d8ad1a611fc97369
round[ 2].s_row      a7bela6997ad739bd8c9ca451f618b61
round[ 2].m_col      ff87968431d86a51645151fa773ad009
round[ 2].k_sch      b692cf0b643dbdf1be9bc5006830b3fe
round[ 3].start      4915598f55e5d7a0daca94fa1f0a63f7
round[ 3].s_box      3b59cb73fcd90ee05774222dc067fb68
round[ 3].s_row      3bd92268fc74fb735767cbe0c0590e2d
round[ 3].m_col      4c9c1e66f771f0762c3f868e534df256
round[ 3].k_sch      b6ff744ed2c2c9bf6c590cbf0469bf41
round[ 4].start      fa636a2825b339c940668a3157244d17
round[ 4].s_box      2dfb02343f6d12dd09337ec75b36e3f0
round[ 4].s_row      2d6d7ef03f33e334093602dd5bfb12c7
round[ 4].m_col      6385b79ffc538df997be478e7547d691
round[ 4].k_sch      47f7f7bc95353e03f96c32bcfd058dfd
round[ 5].start      247240236966b3fa6ed2753288425b6c
round[ 5].s_box      36400926f9336d2d9fb59d23c42c3950
round[ 5].s_row      36339d50f9b539269f2c092dc4406d23
round[ 5].m_col      f4bcd45432e554d075f1d6c51dd03b3c
round[ 5].k_sch      3caaa3e8a99f9deb50f3af57adf622aa
round[ 6].start      c81677bc9b7ac93b25027992b0261996
round[ 6].s_box      e847f56514dadde23f77b64fe7f7d490
round[ 6].s_row      e8dab6901477d4653ff7f5e2e747dd4f
round[ 6].m_col      9816ee7400f87f556b2c049c8e5ad036
round[ 6].k_sch      5e390f7df7a69296a7553dc10aa31f6b
round[ 7].start      c62fe109f75eedc3cc79395d84f9cf5d
round[ 7].s_box      b415f8016858552e4bb6124c5f998a4c
round[ 7].s_row      b458124c68b68a014b99f82e5f15554c
round[ 7].m_col      c57e1c159a9bd286f05f4be098c63439
round[ 7].k_sch      14f9701ae35fe28c440adf4d4ea9c026
round[ 8].start      d1876c0f79c4300ab45594add66ff41f
round[ 8].s_box      3e175076b61c04678dfc2295f6a8bfc0
round[ 8].s_row      3e1c22c0b6fcbf768da85067f6170495
round[ 8].m_col      baa03de7a1f9b56ed5512cba5f414d23
round[ 8].k_sch      47438735a41c65b9e016baf4aebf7ad2
round[ 9].start      fde3bad205e5d0d73547964ef1fe37f1
round[ 9].s_box      5411f4b56bd9700e96a0902fa1bb9aa1
round[ 9].s_row      54d990a16ba09ab596bbf40ea111702f
round[ 9].m_col      e9f74eec023020f61bf2ccf2353c21c7
round[ 9].k_sch      549932d1f08557681093ed9cbe2c974e
round[10].start      bd6e7c3df2b5779e0b61216e8b10b689
round[10].s_box      7a9f102789d5f50b2beffd9f3dca4ea7
round[10].s_row      7ad5fda789ef4e272bca100b3d9ff59f
round[10].k_sch      13111d7fe3944a17f307a78b4d2b30c5
round[10].output     69c4e0d86a7b0430d8cdb78070b4c55a

```

INVERSE CIPHER (DECRYPT):

```

round[ 0].iinput     69c4e0d86a7b0430d8cdb78070b4c55a
round[ 0].ik_sch     13111d7fe3944a17f307a78b4d2b30c5
round[ 1].istart     7ad5fda789ef4e272bca100b3d9ff59f

```

```

round[ 1].is_row 7a9f102789d5f50b2beffd9f3dca4ea7
round[ 1].is_box bd6e7c3df2b5779e0b61216e8b10b689
round[ 1].ik_sch 549932d1f08557681093ed9cbe2c974e
round[ 1].ik_add e9f74eec023020f61bf2ccf2353c21c7
round[ 2].istart 54d990a16ba09ab596bbf40ea111702f
round[ 2].is_row 5411f4b56bd9700e96a0902fa1bb9aa1
round[ 2].is_box fde3bad205e5d0d73547964ef1fe37f1
round[ 2].ik_sch 47438735a41c65b9e016baf4aebf7ad2
round[ 2].ik_add baa03de7a1f9b56ed5512cba5f414d23
round[ 3].istart 3e1c22c0b6fcfbf768da85067f6170495
round[ 3].is_row 3e175076b61c04678dfc2295f6a8bfc0
round[ 3].is_box d1876c0f79c4300ab45594add66ff41f
round[ 3].ik_sch 14f9701ae35fe28c440adf4d4ea9c026
round[ 3].ik_add c57e1c159a9bd286f05f4be098c63439
round[ 4].istart b458124c68b68a014b99f82e5f15554c
round[ 4].is_row b415f8016858552e4bb6124c5f998a4c
round[ 4].is_box c62fe109f75eedc3cc79395d84f9cf5d
round[ 4].ik_sch 5e390f7df7a69296a7553dc10aa31f6b
round[ 4].ik_add 9816ee7400f87f556b2c049c8e5ad036
round[ 5].istart e8dab6901477d4653ff7f5e2e747dd4f
round[ 5].is_row e847f56514dadde23f77b64fe7f7d490
round[ 5].is_box c81677bc9b7ac93b25027992b0261996
round[ 5].ik_sch 3caaa3e8a99f9deb50f3af57adf622aa
round[ 5].ik_add f4bcd45432e554d075f1d6c51dd03b3c
round[ 6].istart 36339d50f9b539269f2c092dc4406d23
round[ 6].is_row 36400926f9336d2d9fb59d23c42c3950
round[ 6].is_box 247240236966b3fa6ed2753288425b6c
round[ 6].ik_sch 47f7f7bc95353e03f96c32bcfd058dfd
round[ 6].ik_add 6385b79ffc538df997be478e7547d691
round[ 7].istart 2d6d7ef03f33e334093602dd5bfb12c7
round[ 7].is_row 2dfb02343f6d12dd09337ec75b36e3f0
round[ 7].is_box fa636a2825b339c940668a3157244d17
round[ 7].ik_sch b6ff744ed2c2c9bf6c590cbf0469bf41
round[ 7].ik_add 4c9c1e66f771f0762c3f868e534df256
round[ 8].istart 3bd92268fc74fb735767cbe0c0590e2d
round[ 8].is_row 3b59cb73fcd90ee05774222dc067fb68
round[ 8].is_box 4915598f55e5d7a0daca94fa1f0a63f7
round[ 8].ik_sch b692cf0b643dbdf1be9bc5006830b3fe
round[ 8].ik_add ff87968431d86a51645151fa773ad009
round[ 9].istart a7be1a6997ad739bd8c9ca451f618b61
round[ 9].is_row a761ca9b97be8b45d8ad1a611fc97369
round[ 9].is_box 89d810e8855ace682d1843d8cb128fe4
round[ 9].ik_sch d6aa74fdd2af72fadaa678f1d6ab76fe
round[ 9].ik_add 5f72641557f5bc92f7be3b291db9f91a
round[10].istart 6353e08c0960e104cd70b751bacad0e7
round[10].is_row 63cab7040953d051cd60e0e7ba70e18c
round[10].is_box 00102030405060708090a0b0c0d0e0f0
round[10].ik_sch 000102030405060708090a0b0c0d0e0f
round[10].ioutput 00112233445566778899aabbccddeeff

```

EQUIVALENT INVERSE CIPHER (DECRYPT):

```

round[ 0].iinput 69c4e0d86a7b0430d8cdb78070b4c55a
round[ 0].ik_sch 13111d7fe3944a17f307a78b4d2b30c5
round[ 1].istart 7ad5fda789ef4e272bca100b3d9ff59f
round[ 1].is_box bdb52189f261b63d0b107c9e8b6e776e
round[ 1].is_row bd6e7c3df2b5779e0b61216e8b10b689
round[ 1].im_col 4773b91ff72f354361cb018ea1e6cf2c

```

```

round[ 1].ik_sch 13aa29be9c8faff6f770f58000f7bf03
round[ 2].istart 54d990a16ba09ab596bbf40ea111702f
round[ 2].is_box fde596f1054737d235febad7f1e3d04e
round[ 2].is_row fde3bad205e5d0d73547964ef1fe37f1
round[ 2].im_col 2d7e86a339d9393ee6570a1101904e16
round[ 2].ik_sch 1362a4638f2586486bff5a76f7874a83
round[ 3].istart 3e1c22c0b6fcbf768da85067f6170495
round[ 3].is_box d1c4941f7955f40fb46f6c0ad68730ad
round[ 3].is_row d1876c0f79c4300ab45594add66ff41f
round[ 3].im_col 39daee38f4f1a82aaf432410c36d45b9
round[ 3].ik_sch 8d82fc749c47222be4dad3e9c7810f5
round[ 4].istart b458124c68b68a014b99f82e5f15554c
round[ 4].is_box c65e395df779cf09ccf9e1c3842fed5d
round[ 4].is_row c62fe109f75eedc3cc79395d84f9cf5d
round[ 4].im_col 9a39bf1d05b20a3a476a0bf79fe51184
round[ 4].ik_sch 72e3098d11c5de5f789dfe1578a2cccb
round[ 5].istart e8dab6901477d4653ff7f5e2e747dd4f
round[ 5].is_box c87a79969b0219bc2526773bb016c992
round[ 5].is_row c81677bc9b7ac93b25027992b0261996
round[ 5].im_col 18f78d779a93eef4f6742967c47f5ffd
round[ 5].ik_sch 2ec410276326d7d26958204a003f32de
round[ 6].istart 36339d50f9b539269f2c092dc4406d23
round[ 6].is_box 2466756c69d25b236e4240fa8872b332
round[ 6].is_row 247240236966b3fa6ed2753288425b6c
round[ 6].im_col 85cf8bf472d124c10348f545329c0053
round[ 6].ik_sch a8a2f5044de2c7f50a7ef79869671294
round[ 7].istart 2d6d7ef03f33e334093602dd5bfb12c7
round[ 7].is_box fab38a1725664d2840246ac957633931
round[ 7].is_row fa636a2825b339c940668a3157244d17
round[ 7].im_col fc1fc1f91934c98210fbfb8da340eb21
round[ 7].ik_sch c7c6e391e54032f1479c306d6319e50c
round[ 8].istart 3bd92268fc74fb735767cbe0c0590e2d
round[ 8].is_box 49e594f755ca638fda0a59a01f15d7fa
round[ 8].is_row 4915598f55e5d7a0daca94fa1f0a63f7
round[ 8].im_col 076518f0b52ba2fb7a15c8d93be45e00
round[ 8].ik_sch a0db02992286d160a2dc029c2485d561
round[ 9].istart a7bela6997ad739bd8c9ca451f618b61
round[ 9].is_box 895a43e485188fe82d121068cbd8ced8
round[ 9].is_row 89d810e8855ace682d1843d8cb128fe4
round[ 9].im_col ef053f7c8b3d32fd4d2a64ad3c93071a
round[ 9].ik_sch 8c56dff0825dd3f9805ad3fc8659d7fd
round[10].istart 6353e08c0960e104cd70b751bacad0e7
round[10].is_box 0050a0f04090e03080d02070c01060b0
round[10].is_row 00102030405060708090a0b0c0d0e0f0
round[10].ik_sch 000102030405060708090a0b0c0d0e0f
round[10].ioutput 00112233445566778899aabbccddeeff

```

C.2 AES-192 ($Nk=6$, $Nr=12$)

```

PLAINTEXT: 00112233445566778899aabbccddeeff
KEY:       000102030405060708090a0b0c0d0e0f1011121314151617

```

```

CIPHER (ENCRYPT):
round[ 0].input 00112233445566778899aabbccddeeff
round[ 0].k_sch 000102030405060708090a0b0c0d0e0f
round[ 1].start 00102030405060708090a0b0c0d0e0f0

```


round[1].s_box	63cab7040953d051cd60e0e7ba70e18c
round[1].s_row	6353e08c0960e104cd70b751bacad0e7
round[1].m_col	5f72641557f5bc92f7be3b291db9f91a
round[1].k_sch	10111213141516175846f2f95c43f4fe
round[2].start	4f63760643e0aa85aff8c9d041fa0de4
round[2].s_box	84fb386f1ae1ac977941dd70832dd769
round[2].s_row	84e1dd691a41d76f792d389783fbac70
round[2].m_col	9f487f794f955f662afc86abd7f1ab29
round[2].k_sch	544afef55847f0fa4856e2e95c43f4fe
round[3].start	cb02818c17d2af9c62aa64428bb25fd7
round[3].s_box	1f770c64f0b579deaaac432c3d37cf0e
round[3].s_row	1fb5430ef0accf64aa370cde3d77792c
round[3].m_col	b7a53ecbbf9d75a0c40efc79b674cc11
round[3].k_sch	40f949b31cbabd4d48f043b810b7b342
round[4].start	f75c7778a327c8ed8cfefbfc1a6c37f53
round[4].s_box	684af5bc0acce85564bb0878242ed2ed
round[4].s_row	68cc08ed0abbd2bc642ef555244ae878
round[4].m_col	7a1e98bdacb6d1141a6944dd06eb2d3e
round[4].k_sch	58e151ab04a2a5557effb5416245080c
round[5].start	22ffc916a81474416496f19c64ae2532
round[5].s_box	9316dd47c2fa92834390alde43e43f23
round[5].s_row	93faa123c2903f4743e4dd83431692de
round[5].m_col	aaa755b34cffe57cef6f98e1f01c13e6
round[5].k_sch	2ab54bb43a02f8f662e3a95d66410c08
round[6].start	80121e0776fd1d8a8d8c31bc965d1fee
round[6].s_box	cdc972c53854a47e5d64c765904cc028
round[6].s_row	cd54c7283864c0c55d4c727e90c9a465
round[6].m_col	921f748fd96e937d622d7725ba8ba50c
round[6].k_sch	f501857297448d7ebdf1c6ca87f33e3c
round[7].start	671ef1fd4e2a1e03dfdcblf3d789b30
round[7].s_box	8572a1542fe5727b9e86c8df27bc1404
round[7].s_row	85e5c8042f8614549ebca17b277272df
round[7].m_col	e913e7b18f507d4b227ef652758acbcc
round[7].k_sch	e510976183519b6934157c9ea351f1e0
round[8].start	0c0370d00c01e622166b8accd6db3a2c
round[8].s_box	fe7b5170fe7c8e93477f7e4bf6b98071
round[8].s_row	fe7c7e71fe7f807047b95193f67b8e4b
round[8].m_col	6cf5edf996eb0a069c4ef21cbfc25762
round[8].k_sch	1ea0372a995309167c439e77ff12051e
round[9].start	7255dad30fb80310e00d6c6b40d0527c
round[9].s_box	40fc5766766c7bcae1d7507f09700010
round[9].s_row	406c501076d70066e17057ca09fc7b7f
round[9].m_col	7478bcdce8a50b81d4327a9009188262
round[9].k_sch	dd7e0e887e2fff68608fc842f9dcc154
round[10].start	a906b254968af4e9b4bdb2d2f0c44336
round[10].s_box	d36f3720907ebf1e8d7a37b58c1c1a05
round[10].s_row	d37e3705907a1a208d1c371e8c6fbfb5
round[10].m_col	0d73cc2d8f6abe8b0cf2dd9bb83d422e
round[10].k_sch	859f5f237a8d5a3dc0c02952beefd63a
round[11].start	88ec930ef5e7e4b6cc32f4c906d29414
round[11].s_box	c4cedcabe694694e4b23bfdd6fb522fa
round[11].s_row	c494bffae62322ab4bb5dc4e6fce69dd
round[11].m_col	71d720933b6d677dc00b8f28238e0fb7
round[11].k_sch	de601e7827bcdff2ca223800fd8aeda32
round[12].start	afb73eeblcd1b85162280f27fb20d585
round[12].s_box	79a9b2e99c3e6cd1aa3476cc0fb70397
round[12].s_row	793e76979c3403e9aab7b2d10fa96ccc

```
round[12].k_sch      a4970a331a78dc09c418c271e3a41d5d
round[12].output     dda97ca4864cdfe06eaf70a0ec0d7191
```

INVERSE CIPHER (DECRYPT):

```
round[ 0].iinput      dda97ca4864cdfe06eaf70a0ec0d7191
round[ 0].ik_sch      a4970a331a78dc09c418c271e3a41d5d
round[ 1].istart       793e76979c3403e9aab7b2d10fa96ccc
round[ 1].is_row       79a9b2e99c3e6cd1aa3476cc0fb70397
round[ 1].is_box       afb73eeb1cd1b85162280f27fb20d585
round[ 1].ik_sch       de601e7827bcd2ca223800fd8aeda32
round[ 1].ik_add       71d720933b6d677dc00b8f28238e0fb7
round[ 2].istart       c494bffa6e2322ab4bb5dc4e6fce69dd
round[ 2].is_row       c4cedcabe694694e4b23bfdd6fb522fa
round[ 2].is_box       88ec930ef5e7e4b6cc32f4c906d29414
round[ 2].ik_sch       859f5f237a8d5a3dc0c02952beefd63a
round[ 2].ik_add       0d73cc2d8f6abe8b0cf2dd9bb83d422e
round[ 3].istart       d37e3705907a1a208d1c371e8c6fbfb5
round[ 3].is_row       d36f3720907ebf1e8d7a37b58c1c1a05
round[ 3].is_box       a906b254968af4e9b4bdb2d2f0c44336
round[ 3].ik_sch       dd7e0e887e2fff68608fc842f9dcc154
round[ 3].ik_add       7478bcdce8a50b81d4327a9009188262
round[ 4].istart       406c501076d70066e17057ca09fc7b7f
round[ 4].is_row       40fc5766766c7bcae1d7507f09700010
round[ 4].is_box       7255dad30fb80310e00d6c6b40d0527c
round[ 4].ik_sch       1ea0372a995309167c439e77ff12051e
round[ 4].ik_add       6cf5edf996eb0a069c4ef21cbfc25762
round[ 5].istart       fe7c7e71fe7f807047b95193f67b8e4b
round[ 5].is_row       fe7b5170fe7c8e93477f7e4bf6b98071
round[ 5].is_box       0c0370d00c01e622166b8accd6db3a2c
round[ 5].ik_sch       e510976183519b6934157c9ea351f1e0
round[ 5].ik_add       e913e7b18f507d4b227ef652758acbcc
round[ 6].istart       85e5c8042f8614549ebca17b277272df
round[ 6].is_row       8572a1542fe5727b9e86c8df27bc1404
round[ 6].is_box       671ef1fd4e2a1e03dfdcblef3d789b30
round[ 6].ik_sch       f501857297448d7ebdf1c6ca87f33e3c
round[ 6].ik_add       921f748fd96e937d622d7725ba8ba50c
round[ 7].istart       cd54c7283864c0c55d4c727e90c9a465
round[ 7].is_row       cdc972c53854a47e5d64c765904cc028
round[ 7].is_box       80121e0776fd1d8a8d8c31bc965d1fee
round[ 7].ik_sch       2ab54bb43a02f8f662e3a95d66410c08
round[ 7].ik_add       aaa755b34cffe57cef6f98e1f01c13e6
round[ 8].istart       93faa123c2903f4743e4dd83431692de
round[ 8].is_row       9316dd47c2fa92834390a1de43e43f23
round[ 8].is_box       22ffc916a81474416496f19c64ae2532
round[ 8].ik_sch       58e151ab04a2a5557effb5416245080c
round[ 8].ik_add       7a1e98bdacb6d1141a6944dd06eb2d3e
round[ 9].istart       68cc08ed0abbd2bc642ef555244ae878
round[ 9].is_row       684af5bc0acce85564bb0878242ed2ed
round[ 9].is_box       f75c7778a327c8ed8cfefbfc1a6c37f53
round[ 9].ik_sch       40f949b31cbabd4d48f043b810b7b342
round[ 9].ik_add       b7a53ecbbf9d75a0c40efc79b674cc11
round[10].istart       1fb5430ef0accf64aa370cde3d77792c
round[10].is_row       1f770c64f0b579deaaac432c3d37cf0e
round[10].is_box       cb02818c17d2af9c62aa64428bb25fd7
round[10].ik_sch       544afef55847f0fa4856e2e95c43f4fe
round[10].ik_add       9f487f794f955f662afc86abd7f1ab29
round[11].istart       84e1dd691a41d76f792d389783fbac70
```

```

round[11].is_row 84fb386f1aelac977941dd70832dd769
round[11].is_box 4f63760643e0aa85aff8c9d041fa0de4
round[11].ik_sch 10111213141516175846f2f95c43f4fe
round[11].ik_add 5f72641557f5bc92f7be3b291db9f91a
round[12].istart 6353e08c0960e104cd70b751bacad0e7
round[12].is_row 63cab7040953d051cd60e0e7ba70e18c
round[12].is_box 00102030405060708090a0b0c0d0e0f0
round[12].ik_sch 000102030405060708090a0b0c0d0e0f
round[12].ioutput 00112233445566778899aabbccddeeff

```

EQUIVALENT INVERSE CIPHER (DECRYPT):

```

round[ 0].iinput dda97ca4864cdfe06eaf70a0ec0d7191
round[ 0].ik_sch a4970a331a78dc09c418c271e3a41d5d
round[ 1].istart 793e76979c3403e9aab7b2d10fa96ccc
round[ 1].is_box afd10f851c28d5eb62203e51fbb7b827
round[ 1].is_row afb73eeb1cd1b85162280f27fb20d585
round[ 1].im_col 122a02f7242ac8e20605afce51cc7264
round[ 1].ik_sch d6bebd0dc209ea494db073803e021bb9
round[ 2].istart c494bffaef62322ab4bb5dc4e6fce69dd
round[ 2].is_box 88e7f414f532940eccd293b606ece4c9
round[ 2].is_row 88ec930ef5e7e4b6cc32f4c906d29414
round[ 2].im_col 5cc7aeece3c872194ae5ef8309a933c7
round[ 2].ik_sch 8fb999c973b26839c7f9d89d85c68c72
round[ 3].istart d37e3705907a1a208d1c371e8c6fbfb5
round[ 3].is_box a98ab23696bd4354b4c4b2e9f006f4d2
round[ 3].is_row a906b254968af4e9b4bdb2d2f0c44336
round[ 3].im_col b7113ed134e85489b20866b51d4b2c3b
round[ 3].ik_sch f77d6ec1423f54ef5378317f14b75744
round[ 4].istart 406c501076d70066e17057ca09fc7b7f
round[ 4].is_box 72b86c7c0f0d52d3e0d0da104055036b
round[ 4].is_row 7255dad30fb80310e00d6c6b40d0527c
round[ 4].im_col ef3b1be1b9b0e64bdcb79f1e0a707fbb
round[ 4].ik_sch 1147659047cf663b9b0ece8dfc0bf1f0
round[ 5].istart fe7c7e71fe7f807047b95193f67b8e4b
round[ 5].is_box 0c018a2c0c6b3ad016db7022d603e6cc
round[ 5].is_row 0c0370d00c01e622166b8accd6db3a2c
round[ 5].im_col 592460b248832b2952e0b831923048f1
round[ 5].ik_sch dcc1a8b667053f7dcc5c194ab5423a2e
round[ 6].istart 85e5c8042f8614549ebca17b277272df
round[ 6].is_box 672ab1304edc9bfddf78f1033d1e1eef
round[ 6].is_row 671ef1fd4e2a1e03dfdcbl1ef3d789b30
round[ 6].im_col 0b8a7783417ae3a1f9492dc0c641a7ce
round[ 6].ik_sch c6deb0ab791e2364a4055fbe568803ab
round[ 7].istart cd54c7283864c0c55d4c727e90c9a465
round[ 7].is_box 80fd31ee768c1f078d5d1e8a96121dbc
round[ 7].is_row 80121e0776fd1d8a8d8c31bc965d1fee
round[ 7].im_col 4ee1ddf9301d6352c9ad769ef8d20515
round[ 7].ik_sch dd1b7cdaf28d5c158a49ab1dbbc497cb
round[ 8].istart 93faa123c2903f4743e4dd83431692de
round[ 8].is_box 2214f132a896251664aec94164ff749c
round[ 8].is_row 22fffc916a81474416496f19c64ae2532
round[ 8].im_col 1008ffe53b36ee6af27b42549b8a7bb7
round[ 8].ik_sch 78c4f708318d3cd69655b701bfc093cf
round[ 9].istart 68cc08ed0abbd2bc642ef555244ae878
round[ 9].is_box f727bf53a3fe7f788cc377eda65cc8c1
round[ 9].is_row f75c7778a327c8ed8cfefbfc1a6c37f53
round[ 9].im_col 7f69ac1ed939ebaac8ece3cb12e159e3

```

round[9].ik_sch	60dcef10299524ce62dbef152f9620cf
round[10].istart	1fb5430ef0accf64aa370cde3d77792c
round[10].is_box	cbd264d717aa5f8c62b2819c8b02af42
round[10].is_row	cb02818c17d2af9c62aa64428bb25fd7
round[10].im_col	cfaf16b2570c18b52e7fef50cab267ae
round[10].ik_sch	4b4ecbdb4d4dcfda5752d7c74949cbde
round[11].istart	84e1dd691a41d76f792d389783fbac70
round[11].is_box	4fe0c9e443f80d06affa76854163aad0
round[11].is_row	4f63760643e0aa85aff8c9d041fa0de4
round[11].im_col	794cf891177bfd1d8a327086f3831b39
round[11].ik_sch	1a1f181d1e1b1c194742c7d74949cbde
round[12].istart	6353e08c0960e104cd70b751bacad0e7
round[12].is_box	0050a0f04090e03080d02070c01060b0
round[12].is_row	00102030405060708090a0b0c0d0e0f0
round[12].ik_sch	000102030405060708090a0b0c0d0e0f
round[12].ioutput	00112233445566778899aabbccddeeff

C.3 AES-256 ($Nk=8, Nr=14$)

PLAINTEXT: 00112233445566778899aabbccddeeff

KEY: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f

CIPHER (ENCRYPT):

round[0].input	00112233445566778899aabbccddeeff
round[0].k_sch	000102030405060708090a0b0c0d0e0f
round[1].start	00102030405060708090a0b0c0d0e0f0
round[1].s_box	63cab7040953d051cd60e0e7ba70e18c
round[1].s_row	6353e08c0960e104cd70b751bacad0e7
round[1].m_col	5f72641557f5bc92f7be3b291db9f91a
round[1].k_sch	101112131415161718191a1b1c1d1e1f
round[2].start	4f63760643e0aa85efa7213201a4e705
round[2].s_box	84fb386f1aelac97df5cfd237c49946b
round[2].s_row	84e1fd6b1a5c946fdf4938977cfbac23
round[2].m_col	bd2a395d2b6ac438d192443e615da195
round[2].k_sch	a573c29fa176c498a97fce93a572c09c
round[3].start	1859fbc28a1c00a078ed8aadca2f6109
round[3].s_box	adcb0f257e9c63e0bc557e951c15ef01
round[3].s_row	ad9c7e017e55ef25bc150fe01ccb6395
round[3].m_col	810dce0cc9db8172b3678c1e88a1b5bd
round[3].k_sch	1651a8cd0244beda1a5da4c10640bade
round[4].start	975c66c1cb9f3fa8a93a28df8ee10f63
round[4].s_box	884a33781fdb75c2d380349e19f876fb
round[4].s_row	88db34fb1f807678d3f833c2194a759e
round[4].m_col	b2822d81abe6fb275faf103a078c0033
round[4].k_sch	ae87dff00ff11b68a68ed5fb03fc1567
round[5].start	1c05f271a417e04ff921c5c104701554
round[5].s_box	9c6b89a349f0e18499fda678f2515920
round[5].s_row	9cf0a62049fd59a399518984f26be178
round[5].m_col	aeb65ba974e0f822d73f567bdb64c877
round[5].k_sch	6de1f1486fa54f9275f8eb5373b8518d
round[6].start	c357aae11b45b7b0a2c7bd28a8dc99fa
round[6].s_box	2e5bacf8af6ea9e73ac67a34c286ee2d
round[6].s_row	2e6e7a2dafc6eef83a86ace7c25ba934
round[6].m_col	b951c33c02e9bd29ae25cdb1efa08cc7
round[6].k_sch	c656827fc9a799176f294cec6cd5598b
round[7].start	7f074143cb4e243ec10c815d8375d54c
round[7].s_box	d2c5831a1f2f36b278fe0c4cec9d0329