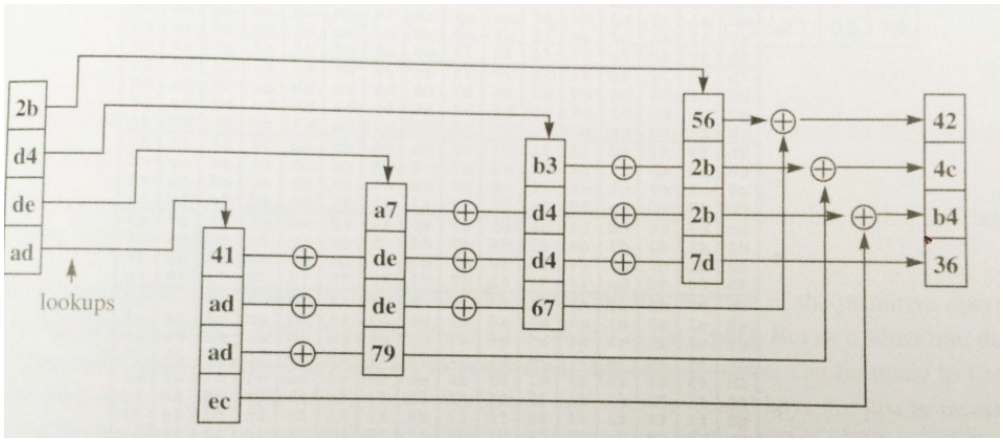
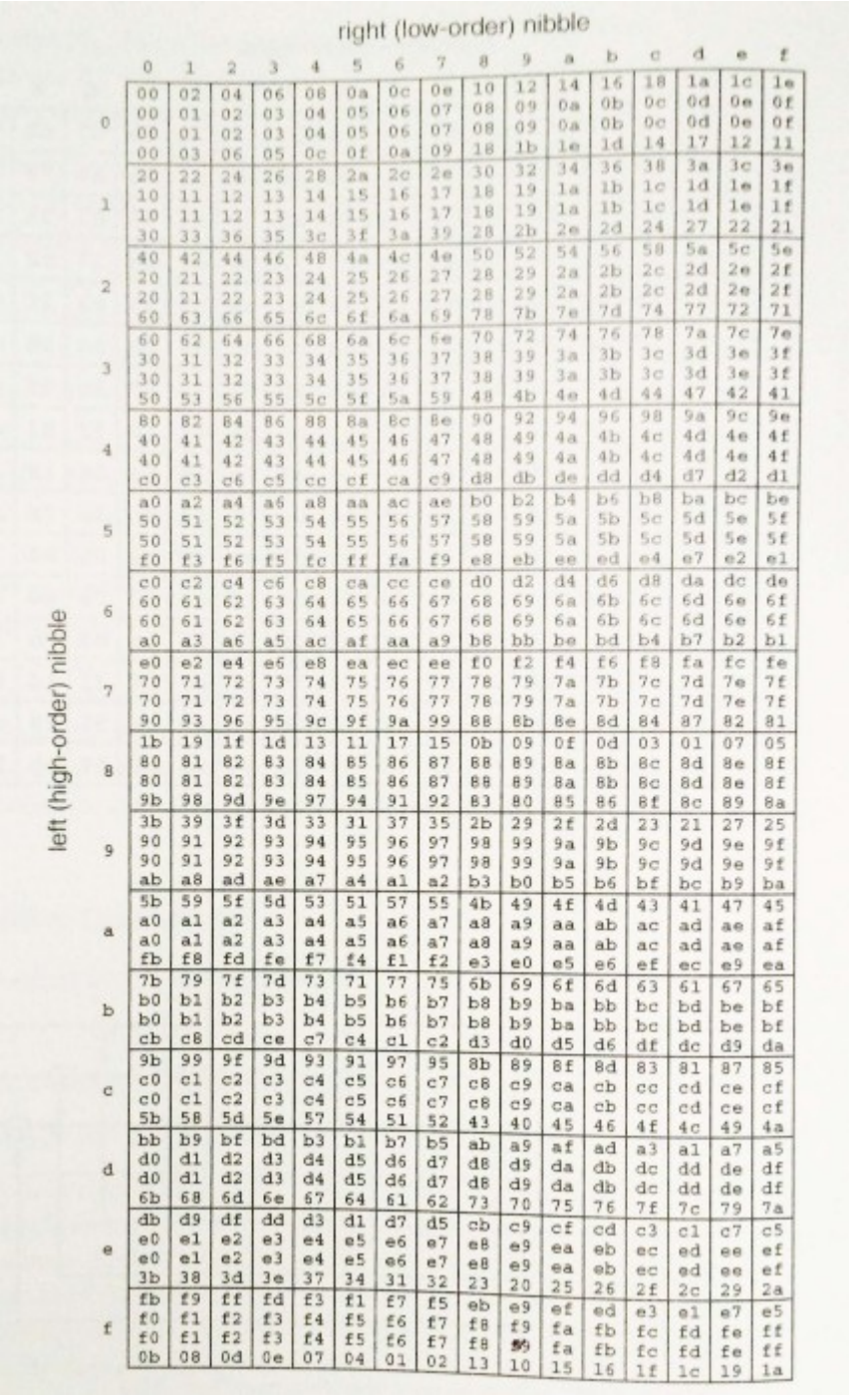
left (high-order) nibble \ right (low-order) nibble	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 3-24. Rijndael S-box

AES – S-BOX



***MixColumn* using table-lookup**



right (low-order) nibble

left (high-order) nibble	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00	02	04	06	08	0a	0c	0e	10	12	14	16	18	1a	1c	1e
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
	00	03	06	05	0c	0f	0a	09	18	1b	1e	1d	14	17	12	11
1	20	22	24	26	28	2a	2c	2e	30	32	34	36	38	3a	3c	3e
	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
	30	33	36	35	3c	3f	3a	39	28	2b	2e	2d	24	27	22	21
2	40	42	44	46	48	4a	4c	4e	50	52	54	56	58	5a	5c	5e
	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
	60	63	66	65	6c	6f	6a	69	78	7b	7e	7d	74	77	72	71
3	60	62	64	66	68	6a	6c	6e	70	72	74	76	78	7a	7c	7e
	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
	50	53	56	55	5c	5f	5a	59	48	4b	4e	4d	44	47	42	41
4	80	82	84	86	88	8a	8c	8e	90	92	94	96	98	9a	9c	9e
	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
	c0	c3	c6	c5	cc	cf	ca	c9	d8	db	de	dd	d4	d7	d2	d1
5	a0	a2	a4	a6	a8	aa	ac	ae	b0	b2	b4	b6	b8	ba	bc	be
	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
	f0	f3	f6	f5	fc	ff	fa	f9	e8	eb	ee	ed	e4	e7	e2	e1
6	c0	c2	c4	c6	c8	ca	cc	ce	d0	d2	d4	d6	d8	da	dc	de
	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
	a0	a3	a6	a5	ac	af	aa	a9	b8	bb	be	bd	b4	b7	b2	b1
7	e0	e2	e4	e6	e8	ea	ec	ee	f0	f2	f4	f6	f8	fa	fc	fe
	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f
	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f
	90	93	96	95	9c	9f	9a	99	88	8b	8e	8d	84	87	82	81
8	1b	19	1f	1d	13	11	17	15	0b	09	0f	0d	03	01	07	05
	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f
	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f
	9b	98	9d	9e	97	94	91	92	83	80	85	86	8f	8c	89	8a
9	3b	39	3f	3d	33	31	37	35	2b	29	2f	2d	23	21	27	25
	90	91	92	93	94	95	96	97	98	99	9a	9b	9c	9d	9e	9f
	90	91	92	93	94	95	96	97	98	99	9a	9b	9c	9d	9e	9f
	ab	a8	ad	ae	a7	a4	a1	a2	b3	b0	b5	b6	bf	bc	b9	ba
a	5b	59	5f	5d	53	51	57	55	4b	49	4f	4d	43	41	47	45
	a0	a1	a2	a3	a4	a5	a6	a7	a8	a9	aa	ab	ac	ad	ae	af
	a0	a1	a2	a3	a4	a5	a6	a7	a8	a9	aa	ab	ac	ad	ae	af
	fb	f8	fd	fe	f7	f4	f1	f2	e3	e0	e5	e6	ef	ec	e9	ea
b	7b	79	7f	7d	73	71	77	75	6b	69	6f	6d	63	61	67	65
	b0	b1	b2	b3	b4	b5	b6	b7	b8	b9	ba	bb	bc	bd	be	bf
	b0	b1	b2	b3	b4	b5	b6	b7	b8	b9	ba	bb	bc	bd	be	bf
	cb	c8	cd	ce	c7	c4	c1	c2	d3	d0	d5	d6	df	dc	d9	da
c	9b	99	9f	9d	93	91	97	95	8b	89	8f	8d	83	81	87	85
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	ca	cb	cc	cd	ce	cf
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	ca	cb	cc	cd	ce	cf
	5b	58	5d	5e	57	54	51	52	43	40	45	46	4f	4c	49	4a
d	bb	b9	bf	bd	b3	b1	b7	b5	ab	a9	af	ad	a3	a1	a7	a5
	d0	d1	d2	d3	d4	d5	d6	d7	d8	d9	da	db	dc	dd	de	df
	d0	d1	d2	d3	d4	d5	d6	d7	d8	d9	da	db	dc	dd	de	df
	6b	68	6d	6e	67	64	61	62	73	70	75	76	7f	7c	79	7a
e	db	d9	df	dd	d3	d1	d7	d5	cb	c9	cf	cd	c3	c1	c7	c5
	e0	e1	e2	e3	e4	e5	e6	e7	e8	e9	ea	eb	ec	ed	ee	ef
	e0	e1	e2	e3	e4	e5	e6	e7	e8	e9	ea	eb	ec	ed	ee	ef
	3b	38	3d	3e	37	34	31	32	23	20	25	26	2f	2c	29	2a
f	fb	f9	ff	fd	f3	f1	f7	f5	eb	e9	ef	ed	e3	e1	e7	e5
	f0	f1	f2	f3	f4	f5	f6	f7	f8	f9	fa	fb	fc	fd	fe	ff
	f0	f1	f2	f3	f4	f5	f6	f7	f8	f9	fa	fb	fc	fd	fe	ff
	0b	08	0d	0e	07	04	01	02	13	10	15	16	1f	1c	19	1a

***MixColumn* table**