AES S 盒表

高位 \ 低位	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	1	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	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	c	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	b	db
a	e0	32	3a	a	49	6	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	8
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	3	f6	e	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	d	bf	e6	42	68	41	99	2d	f	b0	54	bb	16

AES 逆 S 盒表

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

Xtime 乘法表

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

生成元 03 的指数表

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

f	39	4b	dd	7c	84	97	a2	fd	1c	24	6c	b4	c7	52	f6	1

生成元 03 的对数表

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

AES 密钥状态

w 0	**w 1**	**w 2**	**w 3**	**w 4**	**w 5**	**w 6**	**w 7**	**w 8**	**w 9**	**w 10**	**w 11**	**w 12**	**w 13**	**w 14**	**w 15**	**w 16**	**w 17**	**w 18**	**w 19**	**w 20**	**w 21**	**w 22**	**w 23**	**w 24**	**w 25**	**w 26**	**w 27**	**w 28**	**w 29**	**w 30**	**w 31**	**w 32**	**w 33**	**w 34**	**w 35**	**w 36**	**w 37**	**w 38**	**w 39**	**w 40**	**w 41**	**w 42**	**w_4 3**
0	71	da	60	58	29	f3	93	77	5e	ad	3e	cf	91	3c	2	83	12	2e	2c	cc	de	f0	dc	96	48	b8	64	b4	fc	44	20	51	ad	e9	c9	68	c5	2c	e5	1b	de	f2	17
1	1	79	15	97	96	ef	fa	fb	6d	82	78	11	7c	fe	86	80	fc	2	84	c7	3b	39	bd	14	2f	16	ab	2e	1	17	bc	3e	3f	28	94	eb	d4	fc	68	4c	98	64	c
20	98	17	35	2	9a	8d	b8	14	8e	3	bb	9a	14	17	ac	b9	ad	ba	16	a8	5	bf	a9	b1	b4	b	a2	61	d5	de	7c	c2	17	c9	b5	e2	f5	3c	89	f	fa	c6	4f
1	ae	14	94	d1	7f	6b	ff	d	72	19	e6	bf	cd	d4	32	c8	5	d1	e3	b9	bc	6d	8e	3f	83	ee	60	7c	ff	11	71	cb	34	25	54	16	22	7	53	cf	ed	ea	b9