

alan luthfi

0721 184000 0063

Tugas kriptografi AES

Plain teks = NIP => 00721 184000 0063

Key => kebalikan plain teks => 3600 000481127000

Mulai

round mulai

sub bytes

shift row

mix column

round key

input ->

00	20	40	00
00	10	00	00
00	10	00	60
70	80	00	30

30	00	80	70
60	00	10	00
00	00	10	00
00	40	20	00

round 1 ->

30	20	00	70
60	10	10	00
00	10	10	60
70	00	20	30

04	b7	ba	51
d0	ca	ca	63
63	ca	ca	d0
51	ba	b7	04

04	b7	ba	51
ca	ca	63	d0
ca	d0	63	ca
04	51	ba	b7

83	b1	13	b4
ca	02	b3	10
4d	35	ca	cc
04	7a	ba	9c

52	52	d2	a2
03	03	13	13
b3	b3	73	73
51	11	31	31

round 2 ->

d1	e3	c1	16
c9	01	70	0b
2e	5b	b9	b5
55	6b	8b	a2

3e	11	78	47
d0	7c	51	2b
31	b1	5b	08
fc	75	3d	95

3e	11	78	47
7c	51	2b	d0
5b	08	31	b1
95	fc	75	3d

3b	25	c3	7e
a9	57	02	13
4a	48	b0	a4
69	89	6c	d5

2d	78	ad	af
8c	8f	9c	85
a4	c7	b4	c7
6b	7a	4b	7a

round 3 ->

1b	5a	6e	71
25	d8	9e	9c
ee	88	04	b3
32	f3	77	a5

47	be	9f	a3
3f	61	0b	de
28	c4	f2	fb
23	ad	cc	0b

47	be	9f	a3
61	0b	de	3f
f2	fb	28	c4
0b	23	ad	cc

d9	a2	73	14
8e	9d	4d	46
d3	3d	06	40
56	6f	56	86

5a	25	88	87
4a	c5	c9	d6
7e	b9	ad	ca
1d	67	2c	06

round 4 ->

83	87	f1	93
c4	58	14	90
ad	84	0b	8a
4b	08	7a	d0

ec	17	a1	dc
1c	6a	fa	60
95	5f	2b	7e
b3	30	da	70

ec	17	a1	dc
6a	fa	b0	1c
2b	9e	95	5f
70	b3	30	da

2b	56	5c	02
35	c9	5f	df
40	df	a0	0b
8e	c0	6d	93

a4	81	09	8e
3e	fb	a2	74
c5	76	7b	b1
0a	6d	4	17

round 5 ->

82	77	55	8c
0b	32	57	a2
8f	a9	db	ba
84	ad	2c	84

13	55	fc	64
2b	23	5b	62
73	d3	b9	f4
5f	95	71	5f

13	55	fc	64
23	5b	62	2b
b9	f4	73	d3
5f	5f	95	71

a5	b7	a3	17
da	1b	38	2d
b0	bc	dc	b1
11	15	3f	b6

26	a7	ae	20
5b	0d	a5	db
3f	49	32	83
13	7c	3f	28

round 6 ->

83	10	0d	37
2c	1b	97	fb
87	fs	ee	e2
02	6b	00	9e

ec	ca	d7	9a
71	47	88	42
17	e6	28	98
77	75	63	0b

ec	ca	d7	9a
47	88	42	71
28	98	17	e6
0b	77	75	63

29	e3	1b	39
11	05	15	2a
e6	50	3a	99
56	bb	c9	e4

b5	18	b6	96
1a	17	b0	63
0b	42	70	53
a4	da	e5	c2

Round 7 →

Round Mulai	Sub byte	Shift row	Mix Column	Round Kunci
96 fb ad af	90 of 8 79	96 of 95 79	ad 31 c6 c9	04 1c aa 3c
0b 12 af 49	2b c9 8 3b	c9 8 3b 2b	dd b1 f3 07	17 00 b8 db
ed b2 4a 6a	55 37 26 02	db 02 55 37	1a 1e 2e af	b6 f4 84 77
f2 b1 2c 09	89 ef 71 af	af 89 ef 71	es 8f 0f 78	34 ee 0b c6

Round 8 →

Round Mulai	Sub byte	Shift row	Mix Column	Round Kunci
0c 2d 6c f5	f2 d8 50 e6	f2 d8 50 e6	65 3a 4f 3e	3d 21 8b b7
ca b1 4b 2c	74 c8 b3 86	c8 b3 86 74	f7 38 00 6e	e2 e2 5a 81
ac ea aa d8	91 87 ac b1	ac b1 91 87	c2 eb c5 8a	02 46 72 05
d1 61 04 b3	3e ef f2 6d	6d 3e ef f2	af dd 22 3d	df 31 3a 5c

Round 9 →

Round Mulai	Sub byte	Shift row	Mix Column	Round Kunci
58 1b c4 89	6a af 1c a7	6a af 1c a7	fc 53 36 b7	2a 0b 80 37
15 da 5a ef	59 57 be df	57 be df 59	5c e1 a2 4f	89 6b 31 b0
c0 1d b7 8f	ba a4 a9 73	a9 73 ba a4	fc 28 e5 41	b2 44 36 33
78 ec 18 c1	bc ce ad 78	78 bc ce ad	b0 44 c6 4e	76 47 7d 81

Round 10 →

Round Mulai	Sub byte	Shift row	Round Kunci
d6 58 b6 80	f6 6a 4e cd	f6 6a 4e cd	f6 f0 70 47
d5 8a 93 ff	03 7e 2c 16	7e 2c 16 03	4a 21 10 a0
4e 6c d3 72	2f 58 b6 4b	66 40 2f 50	be 1a cc ff
c6 03 b6 cf	b4 7b ea 8a	8a b4 7b ea	ec ab d6 57

Output →

0d	9a	3e	8a
34	fd	06	a3
d8	ba	c3	af
66	1f	af	bd

Chipper telah enkripsi AES