Teknik Informatika udinus 2015

Lakukan enkripsi dengan algoritma AES jika diketahui plainteks dan kunci sebagai berikut:

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

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

JAWAB

Langkah 0 Plainteks ⊕ Kunci

32	88	31	e0	0	0	1	1	0	0	1	0	1	0	0	0	1	0	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	0	0
43	5a	31	37	0	1	0	0	0	0	1	1	0	1	0	1	1	0	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	1	1	1
f6	30	98	07	1	1	1	1	0	1	1	0	0	0	1	1	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	1	1	1	
a8	8d	a2	34	1	0	1	0	1	0	0	0	1	0	0	0	1	1	0	1	1	0	1	0	0	0	1	0	0	0	1	1	0	1	0	0
																		⊕														
2b	28	ab	09	0	0	1	0	1	0	1	1	0	0	1	0	1	0	0	0	1	0	1	0	1	0	1	1	0	0	0	0	1	0	0	1
7e	ae	f7	cf	0	1	1	1	1	1	1	0	1	0	1	0	1	1	1	0	1	1	1	1	0	1	1	1	1	1	0	0	1	1	1	1
15	d2	15	4f	0	0	0	1	0	1	0	1	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	0	0	1	1	1	1		
16	a6	88	3c	0	0	0	1	0	1	1	0	1	0	1	0	0	1	1	0	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	0
19	a0	9a	e9	0	0	0	1	1	0	0	1	1	0	1	0	0	0	0	0	1	0	0	1	1	0	1	0	1	1	1	0	1	0	0	1
3d	f4	c6	f8	0	0	1	1	1	1	0	1	1	1	1	1	0	1	0	0	1	1	0	0	0	1	1	0	1	1	1	1	1	0	0	0
e3	e2	8e	48	1	1	1	0	0	0	1	1	1	1	1	0	0	0	1	0	1	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0
be	2b	2a	08	1	0	1	1	1	1	1	0	0	0	1	0	1	0	1	1	0	0	1	0	1	0	1	0	0	0	0	1	0	0	0	

PUTARAN 1

Langkah 1 **Transformasi SubBytes menggunakan S-Box**

19 a0 9a e9 →
3d f4 c6 f8
e3 e2 8e 48
be 2b 2a 08

S-BOX

x \ y	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

→
d4 e0 b8
27 bf b4
11 98 5d
ae f1 e5

Langkah 2 **Transformasi ShifRows**

d4	e0	b8	1e	→	0	d4	e0	b8	1e
27	bf	b4	41	→	1	bf	b4	41	27
11	98	5d	52	→	2	5d	52	11	98
ae	f1	e5	30	→	3	30	ae	f1	e5

Langkah 3 **Transformasi MixColumns**

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} d4 & e0 & b8 & 1e \\ bf & b4 & 41 & 27 \\ 5d & 52 & 11 & 98 \\ 30 & ae & f1 & e5 \end{bmatrix} = \begin{bmatrix} 04 & e0 & 48 & 28 \\ 66 & cb & f8 & 06 \\ 81 & 19 & d3 & 26 \\ e5 & 9a & 7a & 4c \end{bmatrix}$$

Jadi hasil MixCloumns diperoleh:

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

04 diperoleh dari perkalian elemen-elemen matriks:

= 2*d4 + 3*bf + 1*5d + 1*30 ;

Polinom pad

	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0	↓
d4	1	1	0	1	0	1	0	0	→ $x^7+x^6+x^4+x^2$
bf	1	0	1	1	1	1	1	1	→ $x^7+x^5+x^4+x^3+$
5d	0	1	0	1	1	1	0	1	→ $x^6+x^4+x^3+x^2+$
30	0	0	1	1	0	0	0	0	→ x^5+x^4
3	0	0	0	0	0	0	1	1	→ **x+1**
2	0	0	0	0	0	0	1	0	→ **x**
1	0	0	0	0	0	0	0	1	→ **1**

= x * ($x^7+x^6+x^4+x^2$) + (x+1) *($x^7+x^5+x^4+x^3+x^2+x+1$) + 1* (x^6+x^4+x

= $x^8+x^7+x^5+x^3$ + $x^8+x^6+x^5+x^4+x^3+x^2+x+x^7+x^5+x^4+x^3+x^2+x+1$ + $x^6+x^4+x^3+x^2+$

= x^2 = 00000100 = **04 (Hexa)**

Jika diperoleh polinom dng pangkat lebih dari 7, disederhanakan dengan modulo $x^8+x^4+x^3+x+$

Langkah 4 **Transformasi AddRoundKeys**

04	e0	48	28	⊕	**a0**	**88**	**23**	**2a**
66	cb	f8	06		**fa**	**54**	**a3**	**6c**

RoundKeys
CipherKey
2b 28 ab 09

81	19	d3	26
e5	9a	7a	4c

fe	**2c**	**39**	**76**
17	**b1**	**39**	**05**

=

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

7e	**ae**	**f7**	**cf**
15	**d2**	**15**	**4f**
16	**a6**	**88**	**3c**

↓

09	→ **cf**	→
cf		**4f**
4f		**3c**
3c		**09**

Rotword

S-BOX

hex	y 0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x 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

2b		**8a**		**01**		**a0**
7e	⊕	**84**	⊕	**00**	=	**fa**
15		**eb**		**00**		**fe**
16		**01**		**00**		**17**

2b	0	0	1	0	1	0	1	1
8a	1	0	0	0	1	0	1	0
⊕ 01	0	0	0	0	0	0	0	1
a0	1	0	1	0	0	0	0	0

(Baris 1)

Dengan cara yg sama, diperoleh fa, fe, 17 untuk baris 2,3, dan 4

01	**02**	**04**	**08**	**10**	**20**	**40**	**80**	**1b**	**36**
00	**00**	**00**	**00**	**00**	**00**	**00**	**00**	**00**	**00**
00	**00**	**00**	**00**	**00**	**00**	**00**	**00**	**00**	**00**
00	**00**	**00**	**00**	**00**	**00**	**00**	**00**	**00**	**00**

TABEL RCON

28		a0	**88**		ab		88	**23**		09		23	**2a**
ae	⊕	fa	**54**		f7	⊕	54	**a3**		cf	⊕	a3	**6c**
d2		fe	**2c**		15		2c	**39**		4f		39	**76**
a6		17	**b1**		88		b1	**39**		3c		39	**05**

RoundKey 1 untuk kolom 2,3, dan 4 dilakukan secara berantai me antara kolom di cipherkey dengan hasil roundkey kolom sebelum

key awal

2b	**28**	**ab**	**09**	**a0**	**88**	**23**	**2a**
7e	**ae**	**f7**	**cf**	**fa**	**54**	**a3**	**6c**
15	**d2**	**15**	**4f**	**fe**	**2c**	**39**	**76**
16	**a6**	**88**	**3c**	**17**	**b1**	**39**	**05**

CipherKey **RoundKey 1**

Resume Hasil Putaran 1

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

RoundKeys

a0	**88**	**23**	**2a**
fa	**54**	**a3**	**6c**
fe	**2c**	**39**	**76**
17	**b1**	**39**	**05**

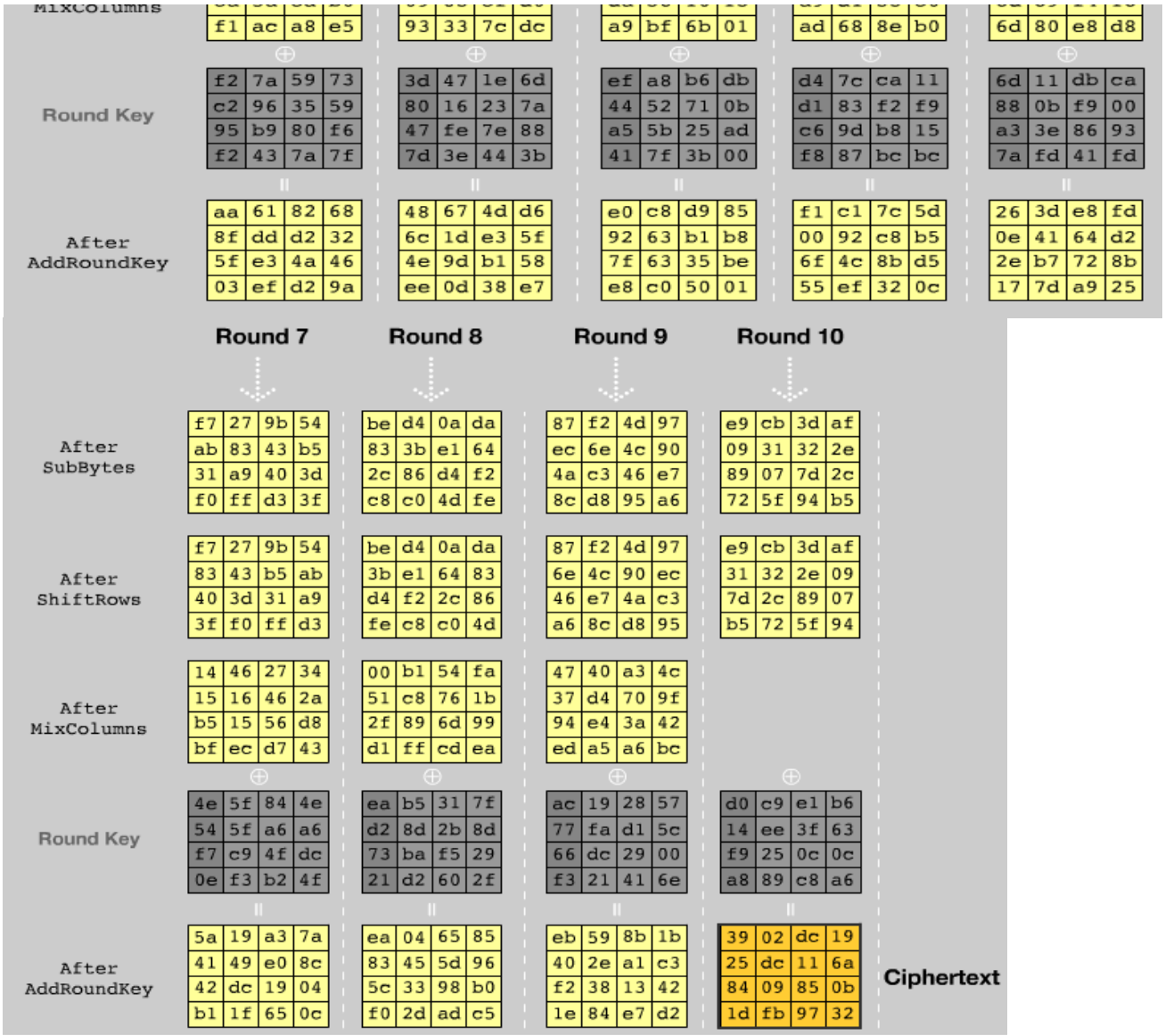
After AddRoundKeys

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

PUTARAN 2 s.d PUTARAN 10

Mengulangi langkah 2 sampai langkah 4 seperti pada Putaran 1.
Masukan awal untuk putaran 2 diambil dari hasil AfterRoundKeys putaran 1
Masukan awal untuk putaran 3 diambil dari hasil AfterRoundKeys putaran 2
Dan seterusnya, sehingga diperoleh hasil sebagai berikut:

	Round 2	Round 3	Round 4	Round 5	Round 6
After SubBytes	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	52 85 e3 f6 50 a4 11 cf 2f 5e c8 6a 28 d7 07 94	e1 e8 35 97 4f fb c8 6c d2 fb 96 ae 9b ba 53 7c	a1 78 10 4c 63 4f e8 d5 a8 29 3d 03 fc df 23 fe
After ShiftRows	49 45 7f 77 db 39 02 de 87 53 d2 96 3b 89 f1 1a	ac ef 13 45 c1 b5 23 73 d6 5a cf 11 b8 7b df b5	52 85 e3 f6 a4 11 cf 50 c8 6a 2f 5e 94 28 d7 07	e1 e8 35 97 fb c8 6c 4f 96 ae d2 fb 7c 9b ba 53	a1 78 10 4c 4f e8 d5 63 3d 03 a8 29 fe fc df 23
After MixColumns	58 1b db 1b 4d 4b e7 6b ca 5a ca b0	75 20 53 bb ec 0b c0 25 09 63 cf d0	0f 60 6f 5e d6 31 c0 b3 da 38 10 13	25 bd b6 4c d1 11 3a 4c a9 d1 33 c0	4b 2c 33 37 86 4a 9d d2 8d 89 f4 18



Jadi:

Plainteks	**a3**	**c5**	**08**	**08**	**43**	**51**	**31**	**37**	**f6**	**30**	**98**	**07**	**a8**	**8d**	**a2**	**34**
Kunci	**2b**	**28**	**ab**	**09**	**7e**	**ae**	**f7**	**cf**	**15**	**d2**	**15**	**4f**	**16**	**a6**	**88**	**3c**
Cipherteks	**39**	**02**	**dc**	**19**	**25**	**dc**	**11**	**6a**	**84**	**09**	**85**	**0b**	**1d**	**fb**	**97**	**32**

1e
41
52
30

a GF(2^n)

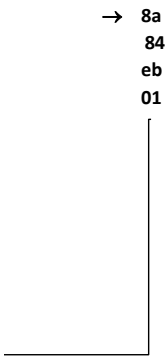
·x^2+x+1

·1

(x^3+x^2+1) + 1* (x^5+x^4)

·1 + x^5+x^4

l



lalui XOR
nya