Cayptography and Network Security Digetal Assignment - I Course code: BCSE3091 Slat: E2 + TE2 Class no .: 0744 Given the plaintext 30FOEODOCOBOA0908 0706050403020100 ] and the key a) shows the oxiginal contents of state displayed as a 4 × 4 matrix. B show the value of state after initial Add Round Key. 25 Show the value of State after SubBytes. 3) Show the value of state after Shigtrows E) show the value of state after MixColumns.

Answer  The original countents of state, displayed as a 4 × 4 matrix.  Solve = 02 06 0A 0E  03 07 08 0F  Cosarangement of values of plaintest in 4 × 4 matrix.  The original countents of plaintest in  10 02 02 02 02 02  10		Date:
assangement of values of Ney 30  Key = 02 02 02 02  Casangement of values of Ney 30	· vole	Answer
5  OO OH OS OC  O1 OS O9 OD  State = 02 OG OA OE  O3 O7 OB OF  10  aggangement of values of plaintext in  H × H materix  C2 O2 O2 O2  O2 O2 O2 O2  O2 O2  O2 O2 O2  O2 O2  O2 O2 O2  O2 O2		
5  OO OH OS OC  O1 OS O9 OD  State = 02 OG OA OE  O3 O7 OB OF  10  aggangement of values of plaintext in  H × H materix  C2 O2 O2 O2  O2 O2 O2 O2  O2 O2  O2 O2 O2  O2 O2  O2 O2 O2  O2 O2	2	The original contents of State
5  OO OH OS OC  O1 OS O9 OD  State = 02 OG OA OE  O3 O7 OB OF  10  aggangement of values of plaintext in  H × H materix  C2 O2 O2 O2  O2 O2 O2 O2  O2 O2  O2 O2 O2  O2 O2  O2 O2 O2  O2 O2	9	1: all 4 x 4 mostain
5  OO OH OS OC  O1 OS O9 OB  State = 02 OG OA OE  O3 O7 OB OF  10  assangement of values of key in  4 × 4 materix  assangement of values of key in  4 × 4 materix		
25 agrangement of values of key an 4x 4 mateix		
State = 02 06 0A 0E  03 07 0B 0F  10  aggangement of values of Rey an  4 × 4 mataix  aggangement of values of Rey an  4 × 4 mataix	5	1091012 BN 608
State = 02 06 0A 0E  03 07 0B 0F  10  aggangement of values of plaintest in  14 × 4 matrix  22  02 02 02 02  02 02 02  02 02 02  02 02 02  02 02 02  02 02 02  02 02 02  02 02 02  03 02 02  04 × 4 matrix		00 04 08 00
03 07 08 0F  03 07 08 0F  04 02 02 02 02 02  02 02 02 02 02  02 02 02 02 02  02 02 02 02 02  02 02 02 02 02  02 02 02 02 02  02 02 02 02 02  02 02 02 02 02  03 04 values of key in		01 05 09 00
03 07 08 0F  03 07 08 0F  04 02 values of plaintext in  15  02 02 02 02 02  02 02 02 02  02 02 02 02  02 02 02 02  02 02 02 02  02 02 02 02  02 02 02 02  02 02 02 02  02 02 02 02  03 02 02 02  04 4 4 mataix		State = 02 06 0A OE
aggangement as values of plaintext in  15  O2 O2 O2 O2 O2  O2 O2 O2 O2  O2 O2 O2 O2  Rey = O2 O2 O2  O2 O2 O2 O2  A CO2 O2		
02 4 × 4 mataix	10	
02 4 × 4 mataix		2
02 4 × 4 mataix		0990
02 4 × 4 mataix	en PAR	returgement of values of plaintext in
02 02 02 02 02 02 02 02 4 × 4 matrix		
02 02 02 02 02 02 02 02 4× 4 mataix	000	
02 02 02 02 Key = 02 02 02 02 02 02 02 02 20  agrangement of values of Rey in	15	
Rey = 02 02 02 02 02 02 02 02 accargement of values of key in 4 × 4 matoix		02 02 02
agrangement of values of key in		02 02 02 02
agrangement of values of key in  4 × 4 matrix	1702	Rey = 102 02 02 02
agrangement of values of key in  4 × 4 matrix		02 02 02 02
25 Land Land Land Land Land Land Land Land	20	
25 Land Land Land Land Land Land Land Land	laitie	PAHAMAPADHAL
25 Land Land Land Land Land Land Land Land		agrangement of values of
25 soll state la willow with works to		4 × 4 mataix
summer things notice where		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
superiore motes to the cultivate of another the	- etype	Total Comments
S evelor out works ?	25	Total for sular out work?
	25	28 10/80 19/70

13	Date :
(6)	The value of state after initial AddRoundKey.
	Agter AddRoundKey.
5	We do xor for 00 P 02, 01 P 02  and so on.
	and so an.
	Ess example, 00 P 02, use red
10	to convert those in
0	do xor (if both bits are 1 then xored bit will be 0, if both
10	lista are O then will
15	be o , if one of worked bit
S	will be 1] operation.
01	Then we get the hexadecimal
111	equiambent
10	00 = 00000000 (xor)
00	102 = 00000010 ije ole
4	02 = 00000010
. 25	0110000 000 000 00 130 1
P	AJAMA PADHALO
	(110000 = 30   0001 = 00   00
30	00 04 08 00 (02 02 02 02 02 02 02
	02 06 0A 0E 02 02 02 02
	08 07 08 06 02 02 02 02

tandos						Da	te :
	=	02	0G 07	0A 08	OF OC	christ.	AA AAA
5		01	05	09	/OD	16.18 - L	THE STATE OF THE S
3.3	13 10	1	4 (9)		0 A	X of	
	2	XOR	ed.	Alien	plaint	text n	, xietar
-6ean	0,04	0	a 13	00	Section 1988	pur person	
S 10	100		0000		The Transition of the Parket	< 0800 ×	
7€		THE RESERVE	000		700	= 000	
	03 =	Company of the last	0000			= 000	
5	02 =		1 0000			=000	
28	02 =	1	00000	-	100	= 0000	
<u> </u>	03 =		0001	to Market Property		- 000	
3.	02 =		0000	ALC: U	02	= 000	00000
<i>L</i> ⊕			0000			= 000	The second secon
		1		OV.	OB	Control of the last of the las	11010
20	06 =	000	00110		@02	= 000	00000
	02 =	000	00010	5	09	2000	100100
<b>B</b>	04 =	000	0010	0	00	The same of the sa	001100
4/0	9	4	1000	107		= O <b>O</b> O	-460
0	07 =	0000		-	OE	V	01110
25	02 =		00010		OD :	000	
PA	03 =	0000	010	P	@ 02°		0010
	08 =	0000	1000			- 0000	
Com	02 =		000016	4	p 02 =	0000	
\$ 30	OA =		1001	-	OC:		1100
1-50	10 1	20-	20		A OE	0 00	-01
-02-0		0000	- 4		90 8	0 10	RO
Ø	02 =		0010				
	00 =	0000	101			***	

2	The value of state efter Subsytes
	ARRENT BELLE TO THE STATE OF TH
	In this step, we use a lookup
1100	table called 3-box to perform a
5	byte - by - byte substitution of
	the block.
	For example,
10	9E Room 9 Coolumn E
	Column
	50, the value of State after
	SubRytes:
15	
15	02 06 0A 0E 27 71 72 28 03 07 0B 0F => 20 23 AB 6F
	00 04 08 OC 7F GE FA D4
	01/05/09/00 45 83 70 68
1 AC 20	
13 20	90 22 9B CF = 7 1F 12 12
185	12 00 FC 190 OF 100 2.4

after ShiftRays a) Value of state In this step, a farmand shift saw transformation, called shift Roux 5 performed. -> The first now of state is not -> For the second som , a 12-byte altered. 10 ciacular left shift is performed For the third sour, a 2- byte ciacular left shift is pergonned.
For the fourth scow, a 3 byte circular left shift is performed so, the value of state after 28 30 GE 1D 28 72 GF 71 6F Dle AB GB PA

	Date :
e	Value of State after MixColumns.
5	In this step, each column of state materix is multiplied with a fixed palynamial modula (at + 1) over
	palynamial madula (24+1) over GF (2°) and their reduced modulo 24+1.
10	Mix Columns:  65 8E 4B A4
	BD 72 BI 86  OS 13 IF 27  B5 D6 77 5D
15	There are values of the State
	oncamption process with the given
	plaintext and kay.

	0	A	2	2	A	E	•	-7	0	0	Α.	D	0	D		Е
	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	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	В7	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	В3	29	E3	2F	84
5	<b>5</b> 3	D1	00	ED	20	FC	B1	5B	6A	СВ	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	АЗ	40	8F	92	9D	38	F5	ВС	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	В8	14	DE	5E	0B	DB
Α	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
В	E7	C8	37	6D	8D	D5	4E	<b>A</b> 9	6C	56	F4	EA	65	<b>7</b> A	AE	08
С	ВА	78	25	2E	1C	A6	В4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	<b>7</b> 0	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
Е	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	В0	54	BB	16

PAJAM Table 1: S-box DHA