Tutorial Sheet-03

(02.) Sol^n:

plaintext: 123456ABCD132536

⇓ Binary form

1 2 3 4 : 0 0 0 1 → 1
5 6 7 8 : 0 0 1 0 → 2
9 10 11 12 : 0 0 1 1 → 3
13 14 15 16 : 0 1 0 0 → 4
17 18 19 20 : 0 1 0 1 → 5
21 22 23 24 : 0 1 1 0 → 6
25 26 27 28 : 1 0 1 0 → A
29 30 31 32 : 1 0 1 1 → B
33 34 35 36 : 1 1 0 0 → C
37 38 39 40 : 1 1 0 1 → D
41 42 43 44 : 0 0 0 1 → 1
45 46 47 48 : 0 0 1 1 → 3
49 50 51 52 : 0 0 1 0 → 2
53 54 55 56 : 0 1 0 1 → 5
57 58 59 60 : 0 0 1 1 → 3
61 62 63 64 : 0 1 1 0 → 6

initial permutation

0001 = 1
1010 = A
1101 = D

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

→ 0100 = 4
0111 = 7
0110 = 6
1001

14A7D67818BCA18AD
by initial permutation

Final permutation / inverse initial per
or initial per box
output

1010 = A
0111 = 7
1001 = 9

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

A9679E81761B8481
by inverse initial permutation

(04) Sol^{n} "COMPUTER"

ASCII:

C = 01000011 →

O = 01001111 →

M = 01001101

P = 01010000

U = 01010101

T = 01010100

E = 01000101

R = 01010010

Initial Permutation:

58 1	50 1	42 1	34 1	26 1	18 1	10 1	2 1
60 1	52 0	44 1	36 1	28 1	20 0	12 0	4 0
62 0	54 1	46 1	38 1	30 0	22 1	14 1	6 0
64 0	56 1	48 0	40 1	32 0	24 1	16 1	8 1
57 0	49 0	41 0	33 0	25 0	17 0	9 0	1 0
59 0	51 0	43 0	35 0	27 0	19 0	11 0	3 0
61 0	53 0	45 0	37 0	29 0	21 1	13 1	5 0
63 1	55 0	47 0	39 0	31 0	23 0	15 1	7 1

Inverse initial permutation:

40 1	8 1	48 0	16 1	56 1	24 1	64 0	32 0
39 0	7 1	47 0	15 1	55 0	23 0	63 1	31 0
38 1	6 0	46 1	14 1	54 1	22 1	62 0	30 0
37 0	5 0	45 0	13 1	53 0	21 1	61 0	29 0
36 1	4 0	44 1	12 0	52 0	20 0	60 1	28 1
35 0	3 0	43 0	11 0	51 0	19 0	59 0	27 0
34 1	2 1	42 1	10 1	50 1	18 1	58 1	26 1
33 0	1 0	41 0	9 0	49 0	17 0	57 0	25 0

U C T O E M R P

(05) Sol^{n}:

AAAA BBBB CCCC DDDD

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

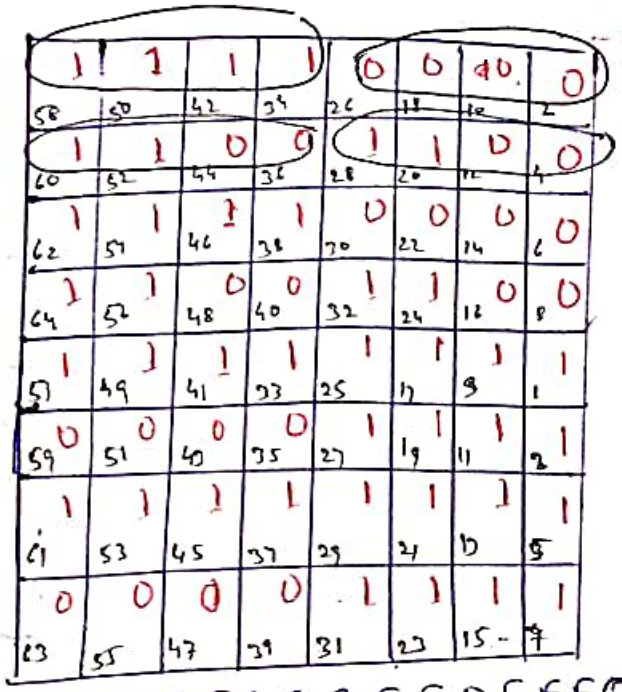
1 0 1 0 1 0 1 0 1 0 1 1 0 1 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 1

AA BB

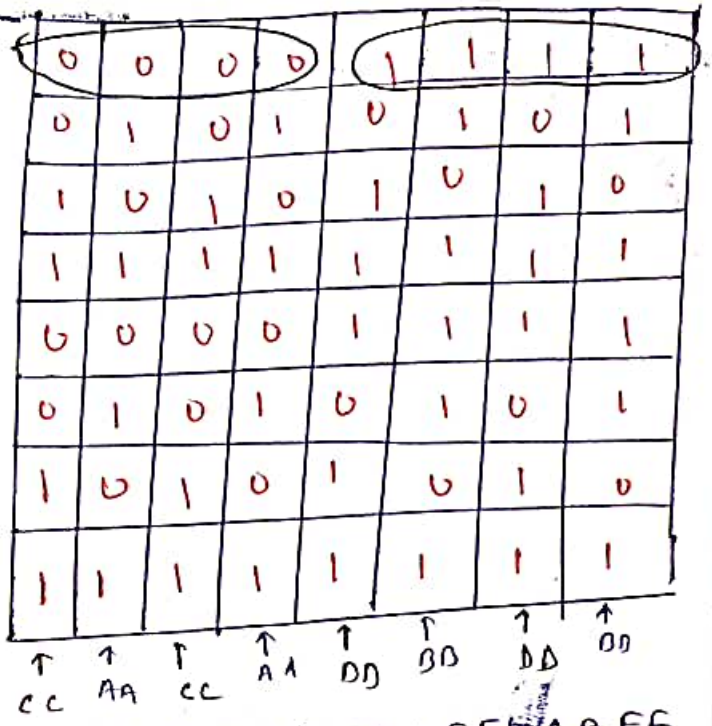
33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 1 1 0 1 1 0 1 1 1 0 1

CC DD



FOCC FOCC FF0f FF0F



0F55AA FF 0f 55AA FF

(7) Sol^n

LOMPUTERENGINEER ← plain text

A=0
B=1
⋮
hexadecimal.

C	O	M	P	U	T	E	R	E	N	G	I	N	E	E	R
2	E	C	F	14	13	4	11	4	D	6	8	D	4	4	11

~~plain text~~ → hexadecimal.

U = 21 - 7 = 20

14 | 20 | 4 | 1 | 0 (14)

State:

2 b_{00}	14 b_{10}	4 b_{20}	D b_{30}
E b_{01}	B b_{11}	D b_{21}	4 b_{31}
C b_{02}	4 b_{12}	6 b_{22}	4 b_{32}
F b_{03}	11 b_{13}	8 b_{23}	11 b_{33}

Ans.

(08) Soln Given

for AES-192, IP = $x^8+x^4+x^3+x+1$ = prime

RCon[11] = $RC_{11} = x^{11-1} \bmod \text{prime} = x^{10} \bmod \text{prime}$

$= x^2(x^8) \bmod \text{prime}$

$= x^2(x^4+x^3+x+1)$

$= x^6+x^5+x^3+x^2$

$= 01101100$

$= (6C\ 00\ 00\ 00)_{16}$

RCon[12] = $RC_{12} = x^{12-1} \bmod \text{prime} = x^{11} \bmod \text{prime}$

$= x^3(x^8) \bmod \text{prime}$

$= x^3(x^4+x^3+x+1)$

$= x^7+x^6+x^4+x^3$

$= 11011000$

$(D8\ 00\ 00\ 00)_{16}$

for AES-256, IP = $x^8+x^4+x^3+x+1$

RCon[13] = $RC_{13} = x^{13-1} \bmod \text{prime} = x^{12} \bmod \text{prime}$

$= x^4(x^8) \bmod \text{prime}$

$= x^4(x^4+x^3+x+1)$

$= x^8+x^7+x^5+x^4$

$= x^4+x^3+x+1 +$

$x^7+x^5+x^4$ cancels (even coefficient)

$= x^7+x^5+x^3+x+1$

$= 10101011$

A B

$= (AB\ 00\ 00\ 00)_{16}$

(05)

$Rcon[14] = RC14 = x^{14-1} \bmod prime = x^5 (x^8) \bmod prime$

$= x^5(x^4+x^3+x+1)$

$= x^9+x^8+x^6+x^5$

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

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

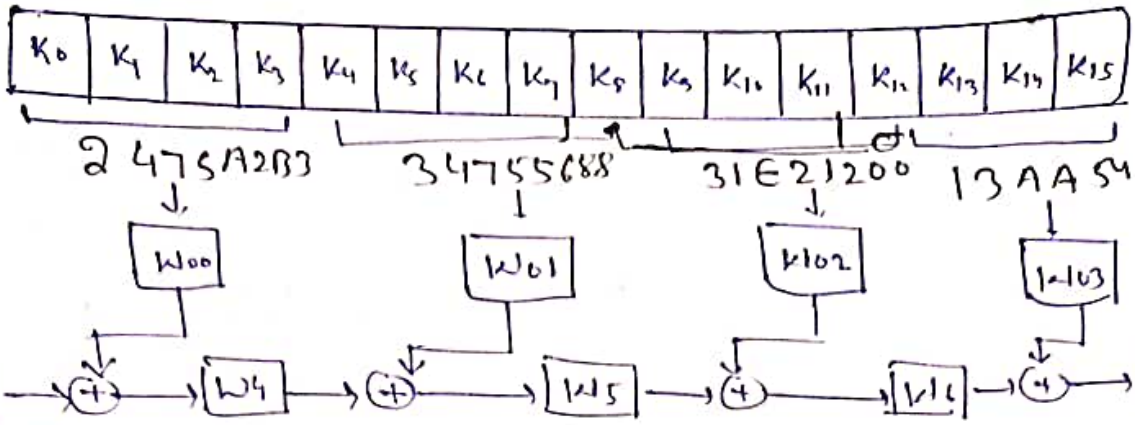
$= x^6+x^3+x^2+1$

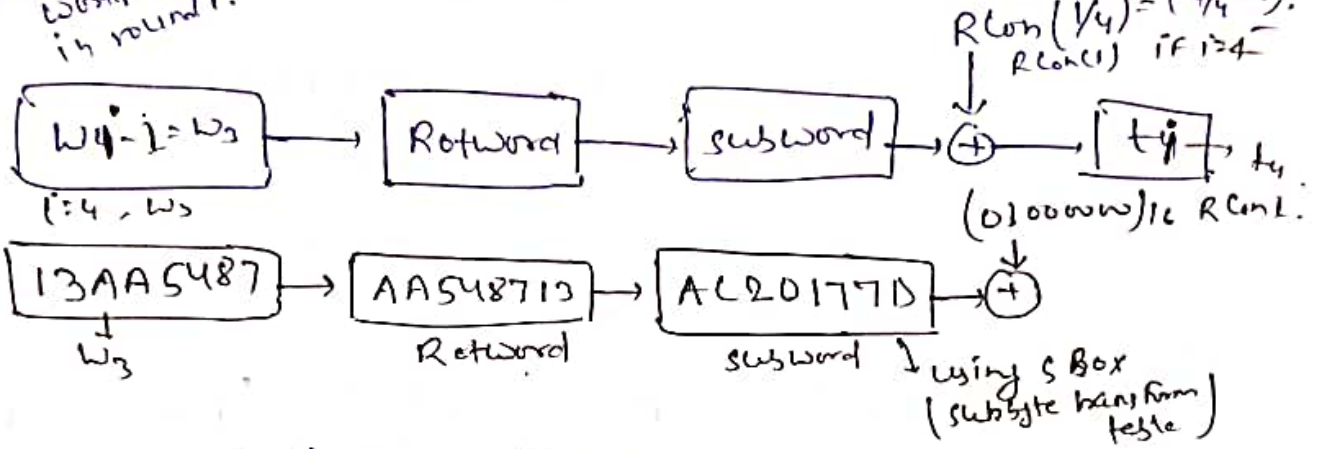
$= 01001101$

$= (4D\,00\,00\,00)_{16}$

Round	(Rcon)	Round	(Rcon)	Round	(Rcon)
1	$(01\,00\,00\,00)_{16}$	5		9	
		6		10	
2		7		11	$(6C\,00\,00\,00)_{16}$
3		8		12	$(D8\,00\,00\,00)_{16}$
4					

(09) Soln:





$$\begin{array}{r} AC201771D \\ \oplus\ 01000000 \\ \hline \end{array} \quad \text{or} \quad \begin{array}{r} A\,[1100]\,201771D \\ \oplus\ 0\,[0001]\,000000 \\ \hline A\,[1101]\,201771D \end{array}$$

$$= AD201771D = t4 \quad \text{Ans.}$$

(10) Soln:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 40 & 97 \\ CE & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix}$$

$(02 \times 87) \oplus (03 \times CE) \oplus (01 \times 46) \oplus (01 \times A6)$

$02 = 00000010 = x$

$87 = \underbrace{1000}_{7\,6\,5\,4}\ \underbrace{0111}_{3\,2\,1\,0} = x^7 + x^2 + x + 1$

$x \cdot (x^7 + x^2 + x + 1) = x^8 + x^3 + x^2 + x$

$= x^4 + x^3 + x + 1 + x^3 + x^2 + x = x^4 + x^2 + 1$