REG.NO.:

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

SLOT: E1 + TE1

CONTINUOUS ASSESSMENT TEST - I
WINTER SEMESTER 2024-2025

Programme Name & Branch : **B.Tech & Computer Science and Engineering**
Course Code and Course Name : **BCSE309L & Cryptography and Network Security**
Faculty Name(s) : **Applicable to all**
Class Number(s) : **Applicable to all**
Date of Examination : **31.01.25**
Exam Duration : **90 minutes** **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- CO1: To know the fundamental mathematical concepts related to security.
- CO2: To understand concept of various cryptographic techniques.

Q. No	Question	M	CO	BL
1.	a) Find 15^276 mod 97 using the method of fast modular exponentiation. Also, determine the result step-by-step and explain how the exponentiation and modular operations are applied iteratively.	7	CO1	BL3
	b) Compute ϕ (8820) using the property of Euler's Totient Function. Describe your steps clearly.	3	CO1	BL3
2.	a) Solve the following congruent equations and find the X value using Chinese Remainder Theorem. $X \equiv 5 \pmod{18}$ $X \equiv 3 \pmod{11}$ $X \equiv 0 \pmod{5}$	7	CO2	BL3
	b) Write the algorithm steps of Miller-Robin algorithm.	3	CO2	BL3
3.	Explain in detail the state and key initialization, initial state permutation, key stream generation and encryption process of RC4 algorithm with diagram and algorithm steps.	10	CO2	BL2
4.	Construct the shift row matrix from the given sub byte matrix (given in Hex) in AES algorithm. Also, find X and Y values in the given output of mix column matrix using the given fixed matrix and determined shift row matrix (Hint: when finding X & Y values, consider fixed matrix as first matrix and shift row matrix as second matrix) $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$ Fixed matrix $\begin{bmatrix} 63 & 09 & cd & ba \\ 53 & d0 & 30 & 20 \\ 72 & ca & 94 & 6d \\ 04 & 84 & 85 & 25 \end{bmatrix}$ Sub byte matrix $\begin{bmatrix} X & - & - & - \\ Y & - & - & - \\ - & - & - & - \\ - & - & - & - \end{bmatrix}$ Mix column matrix	10	CO2	BL3
5.	Describe the operation of S-Box group and S-Box rule. Also, Find the output of S box group from the output of the whitener (XOR) operation of DES function using given S-Box tables. The output of the whitener is 48-bit values, which serves as the input to the S-boxes. The 48-bit values are given as follows: 110011101010011001110110000011111000101011011110	10	CO2	BL4

Table 6.3 *S-box 1*

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Table 6.4 *S-box 2*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
1	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
2	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
3	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

Table 6.5 *S-box 3*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

Table 6.6 *S-box 4*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	6	09	10	1	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

Table 6.7 *S-box 5*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
1	14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
2	04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
3	11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

Table 6.8 *S-box 6*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
1	10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
2	09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
3	04	03	02	12	09	05	15	10	11	14	01	07	10	00	08	13

Table 6.9 *S-box 7*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	00	08	13	03	12	09	07	05	10	06	01
1	13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
2	01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
3	06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

Table 6.10 *S-box 8*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
1	01	15	13	08	10	03	07	04	12	05	06	11	10	14	09	02
2	07	11	04	01	09	12	14	02	00	06	10	10	15	03	05	08
3	02	01	14	07	04	10	8	13	15	12	09	09	03	05	06	11

7M

① (a) $276 = 256 + 16 + 4 = 2^8 + 2^4 + 2^2 \Rightarrow (100010100)$

$15^{276} = 15^{256} \cdot 15^{16} \cdot 15^4 \bmod 97 \Rightarrow$ ~~$75 \cdot 88 \cdot 89 \bmod 97$~~ $= (6600 \bmod 97)$

$15^1 \bmod 97 = 15$

$15^2 \bmod 97 = 225 \bmod 97 = 31$

$15^4 \bmod 97 = 15^2 \cdot 15^2 = 31 \cdot 31 \bmod 97 = 961 \bmod 97 = 89$ ~~88~~

$15^8 \bmod 97 = 15^4 \cdot 15^4 = 88 \cdot 88 \bmod 97 = 7744 \bmod 97 = 1$

$15^{16} \bmod 97 = 15^8 \cdot 15^8 = 89 \cdot 89 \bmod 97 = 7921 \bmod 97 = 34$

$15^{32} \bmod 97 = 15^{16} \cdot 15^{16} = 34 \cdot 34 \bmod 97 = 1156 \bmod 97 = 62$

$15^{64} \bmod 97 = (15^{32})^2 = 62 \cdot 62 \bmod 97 = 3844 \bmod 97 = 61$

$15^{128} \bmod 97 = 15^{64} \cdot 15^{64} = 61 \cdot 61 \bmod 97 = 3721 \bmod 97 = 35$

$15^{256} \bmod 97 = (15^{128})^2 = 35 \cdot 35 \bmod 97 = 1225 \bmod 97 = 61$

$35 \times 62 \times 88 \bmod 97$

$2170 \times 88 \bmod 97$

$36 \cdot 88 \bmod 97$

$3168 \bmod 97$

$= 864$

3M

(b) $\phi(8820)$

$8820 = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^2$

$\phi(n) = n * (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$

$= 8820 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{5})(1 - \frac{1}{7})$

$= 8820 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 2016$

2	8820
2	4410 – 0
2	2205 – 0
3	1102 = 1
5	735
7	245
7	49
7	7
	1

7M

② (a) $X \equiv 5 \pmod{18}$

$X \equiv 3 \pmod{11}$

$X \equiv 0 \pmod{5}$

$M = m_1 \times m_2 \times m_3$

$18 \cdot 11 \cdot 5 = 990$

$M_1 = \frac{M}{m_1} = \frac{990}{18} = 55$

$M_2 = \frac{M}{m_2} = \frac{990}{11} = 90$

$M_3 = \frac{M}{m_3} = \frac{990}{0}$ ✗ $a_3 = 0$

$a_1 = 5 \quad m_1 = 18$

$a_2 = 3 \quad m_2 = 11$

$a_3 = 0 \quad m_3 = 5$

Relatively prime: gcd(18,11) gcd(18,5) gcd(11,5)

$18 = 11 \cdot 1 + 7$

$11 = 7 \cdot 1 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 1 \cdot 3 + 0$

$18 = 5 \cdot 3 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 2 \cdot 2 + 0$

$11 = 5 \cdot 2 + 1$

$5 = 1 \cdot 5 + 0$

$M_1^{-1} = 55^{-1} \bmod 18$

$= 55 \cdot x \bmod 18$

$m_1^{-1} = 1$

$m_2^{-1} = m_2^{-1} \pmod{m_2}$

$= 90^{-1} \bmod 11$

$= 90 \cdot x \bmod 11$

$= 90 \cdot 6 \bmod 11$

$= 540 \bmod 11$

$m_3^{-1} \rightarrow$ no need

$m_2^{-1} = 6$

$X = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \bmod M$

$= 5 \cdot 55 \cdot 1 + 3 \cdot 90 \cdot 6$

$= (275 + 1620) \bmod 990$

$= 1895 \bmod 990$

$X = 905$

4Q

$X = 1C$

$Y = 5A$

5Q

$S_1 = 1011 \quad S_7 = 0100$

$S_2 = 0100$

$S_3 = 1100 \quad 58 = 0111$

$S_4 = 1110$

$S_5 = 1011$

$S_6 = 0001$

3M

2⑥ Miller Robin Alg

(3) RC4 Alg

State & key Initialization (Diagram + Algorithm steps + Explanation) = 2.5 M
Initial state permutation (") = 2.5 M
Key stream generation (") = 2.5 M
encryption (") = 2.5 M

(4) find shift row matrix [2 m]

$$\begin{bmatrix} 63 & 09 & cd & ba \\ 53 & d0 & 30 & 20 \\ 72 & ca & 94 & 6d \\ 04 & 84 & 85 & 25 \end{bmatrix} \Rightarrow \begin{bmatrix} 63 & 09 & cd & ba \\ d0 & 30 & 20 & 53 \\ 94 & 6d & 72 & ca \\ 25 & 04 & 84 & 85 \end{bmatrix}$$

No change
1 byte shift CL
2 "

Sub byte matrix

find X:- [4m]

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} 63 & 09 & cd & ba \\ d0 & 30 & 20 & 53 \\ 94 & 6d & 72 & ca \\ 25 & 04 & 84 & 85 \end{bmatrix} = \begin{bmatrix} X & - & - & - \\ Y & - & - & - \\ - & - & - & - \\ - & - & - & - \end{bmatrix}$$

$X = 02 \times 63 \oplus 03 \times d0 \oplus 01 \times 94 \oplus 01 \times 25 = 1C$

$Y = 5A$ $(01 \times 63 + 02 \times d0 + 03 \times 94 + 01 \times 25)$ read

$02 \times 63 = (0000\ 0010) \cdot (0110\ 0011)$
$= x \cdot (x^6 + x^5 + x + 1)$
$= x^7 + x^6 + x^2 + x$

$03 \times d0 = (0000\ 0011) \cdot (1101\ 0000)$
$= (x+1) \cdot (x^7 + x^6 + x^4)$
$= x^8 + x^7 + x^5 + x^7 + x^6 + x^4$
$= x^8 + x^6 + x^5 + x^4$

$01 \times 94 =$

01×25

(5) operation = 1M
S-box rule = 1M
o/p S box = 6M

(1) $11001| \Rightarrow (1)_2 \Rightarrow (3)_{10} \Rightarrow$ row
$(4001)_2 = (9)_{10} \Rightarrow$ cd
Result $\Rightarrow (11)_{10} \Rightarrow (1011)$

(2) $04 \Rightarrow 0100$
(3) $12 \Rightarrow 1100$
(4) $14 \Rightarrow 1110$
(5) $11 \Rightarrow 1011$
(6) $01 \Rightarrow 0001$
(7) $04 \Rightarrow 0100$
(8) $07 \Rightarrow 0111$

1011 0100 1100 1110 1011 0001 0100 0111

BCSE309L & Cryptography and Network Security – Winter 2024-25
Answer Key (E1 Slot)

Q. No	Question	M	CO	BL
1.	a) Find 15^276 mod 97 using the method of fast modular exponentiation. Also, determine the result step-by-step and explain how the exponentiation and modular operations are applied iteratively. **Answer:**	7		

$15^{276} \bmod 97$

$276 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8$

$276 = 2^2 + 2^4 + 2^8$

$276 = 4 + 16 + 256$

$15^{276} \bmod 97 = 15^{4+16+256} \bmod 97$

$= (15^4 \bmod 97 * 15^{16} \bmod 97 * 15^{256} \bmod 97) \bmod 97$

$15^2 \bmod 97 = 225 \bmod 97$

$= 31$

$15^4 \bmod 97 = 31^2 \bmod 97$

$= 961 \bmod 97$

$= 88$

$15^8 \bmod 97 = 88^2 \bmod 97$

$= 7744 \bmod 97$

$= 81$

$15^{16} \bmod 97 = 81^2 \bmod 97$

$= 62$

$15^{32} \bmod 97 = 62^2 \bmod 97$

$= 61$

$15^{64} \bmod 97 = 61^2 \bmod 97$

$= 35$

$15^{128} \bmod 97 = 35^2 \bmod 97$

$= 61$

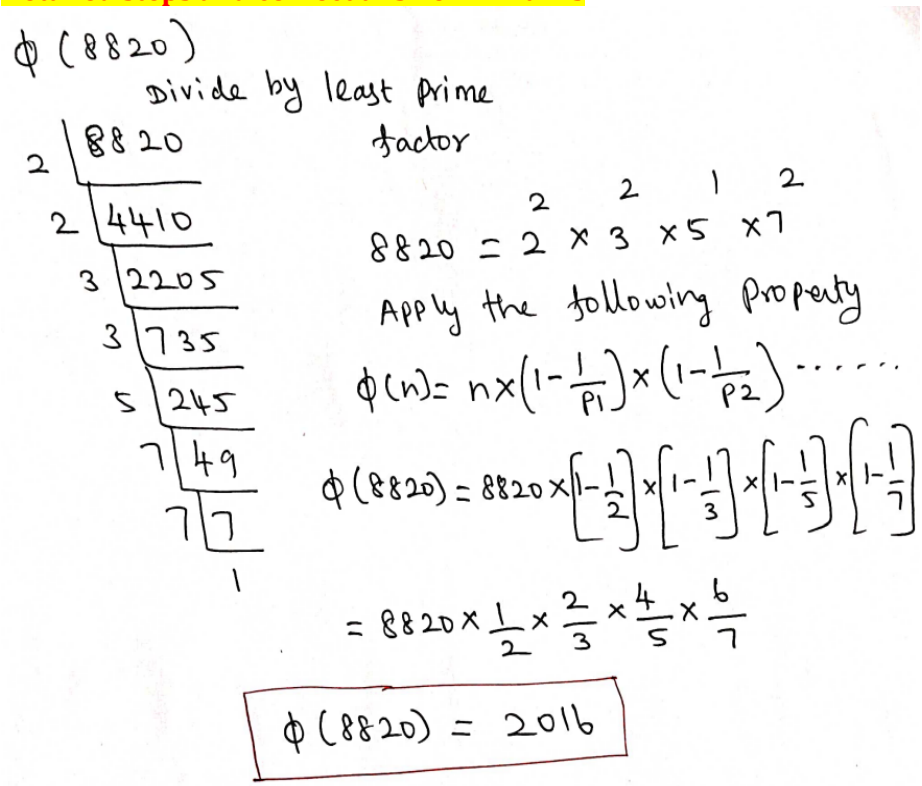
$15^{256} \bmod 97 = 61^2 \bmod 97$

$= 35$

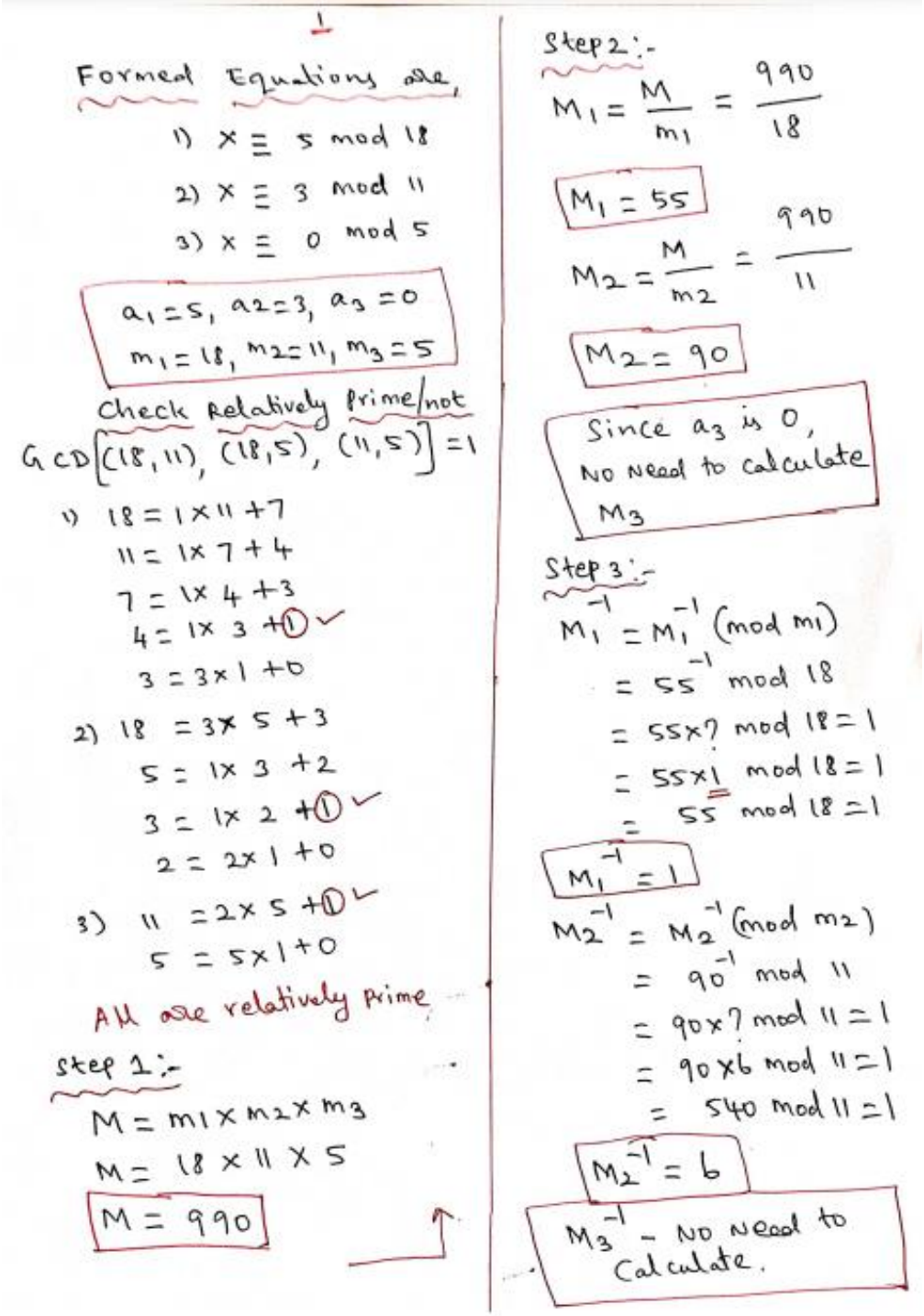
$= [88 \times 62 \times 35] \bmod 97$

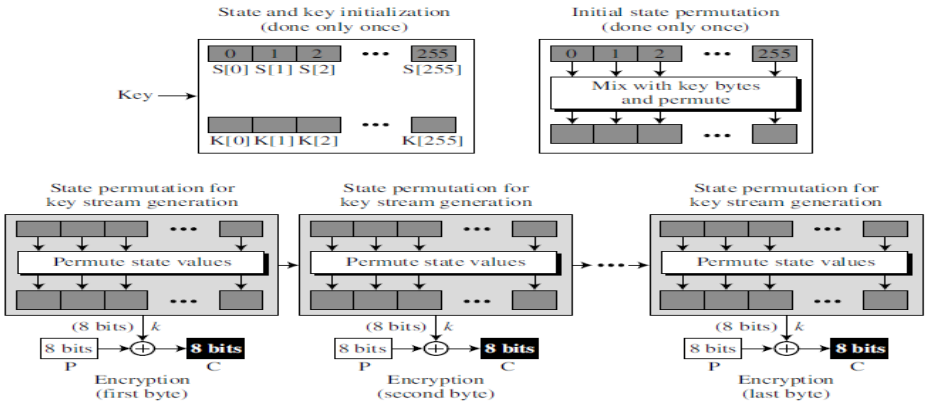
$= 190960 \bmod 97$

$15^{276} \bmod 97 = 64$

	b) Compute ϕ (8820) using the property of Euler's Totient Function. Describe your steps clearly. **Answer:** **Property formulae: 1 mark** **Detailed steps and correct answer: 2 marks**  $\phi(8820)$ Divide by least prime factor 2 | 8820 2 | 4410 3 | 2205 3 | 735 5 | 245 7 | 49 7 | 7 1 $8820 = 2^2 \times 3^2 \times 5^1 \times 7^2$ Apply the following property $\phi(n) = n \times \left(1-\frac{1}{P_1}\right) \times \left(1-\frac{1}{P_2}\right) \cdots\cdots$ $\phi(8820) = 8820 \times \left[1-\frac{1}{2}\right] \times \left[1-\frac{1}{3}\right] \times \left[1-\frac{1}{5}\right] \times \left[1-\frac{1}{7}\right]$ $= 8820 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7}$ $\phi(8820) = 2016$	3		

2.	a) Solve the following congruent equations and find the X value using Chinese Remainder Theorem. $X \equiv 5 \pmod{18}$ $X \equiv 3 \pmod{11}$ $X \equiv 0 \pmod{5}$ Answer: Relatively prime check, M, M1, M2 & M3 – 3 marks M1, M2, M3 Inverse values, X value – 4 marks	7		



	Step 4 :- $X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$ $= (5 \times 55 \times 1 + 3 \times 90 \times 6) \bmod 990$ $= (275 + 1620) \bmod 990$ $= 1895 \bmod 990$ $X = 905$			
	b) Write the algorithm steps of Miller-Robin algorithm. Answer: The below answer is one of the algorithm's steps. Some other alternate algorithm steps also there. You can follow any algorithm. **Miller–Rabin Primality Test** Algorithm Step 1: Find $n-1 = 2^k \times m$ Step 2: Choose 'a' such that $1<a<n-1$ Step 3: Compute $b_0 = a^m \pmod n$, … , $b_i = b^2_{i-1} \pmod n$ +1 ⟶ Composite -1 ⟶ Probably Prime	3		
3.	Explain in detail the state and key initialization, initial state permutation, key stream generation and encryption process of RC4 algorithm with diagram and algorithm steps. Answer: state and key initialization (Diagram + Algorithm steps + Explanation) – 2.5 marks initial state permutation (Diagram + Algorithm steps + Explanation) – 2.5 marks key stream generation (Diagram + Algorithm steps + Explanation) – 2.5 marks encryption process (Diagram + Algorithm steps + Explanation) – 2.5 marks Diagram:  	10		

	Algorithm steps: state and key initialization: • for (i = 0 to 255) • { • S[i] ← i • K[i] ← Key [i mod KeyLength] • } Initial state permutation: $j \leftarrow 0$ for ($i = 0$ to 255) { $j \leftarrow (j + S[i] + K[i]) \bmod 256$ **swap** (S[i] , S[j]) } key stream generation: $i \leftarrow (i + 1) \bmod 256$ $j \leftarrow (j + S[i]) \bmod 256$ **swap** (S [i] , S[j]) $k \leftarrow S[(S[i] + S[j]) \bmod 256]$ Encryption process: **// Key is ready, encrypt** input P C ← P ⊕ k output C			
4.	Construct the shift row matrix from the given sub byte matrix (given in Hex) in AES algorithm. Also, find X and Y values in the given output of mix column matrix using the given fixed matrix and determined shift row matrix (Hint: when finding X & Y values, consider fixed matrix as first matrix and shift row matrix as second matrix) $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$ Fixed matrix $\begin{bmatrix} 63 & 09 & cd & ba \\ 53 & d0 & 30 & 20 \\ 72 & ca & 94 & 6d \\ 04 & 84 & 85 & 25 \end{bmatrix}$ Sub byte matrix $\begin{bmatrix} X & - & - & - \\ Y & - & - & - \\ - & - & - & - \\ - & - & - & - \end{bmatrix}$ Mix column matrix Answer: Output of Shift Row: 2 marks Finding X value in the output of Mix column: 4 marks Finding Y value in the output of Mix column: 4 marks	10		

AES

1

Sub byte matrix

$$\begin{bmatrix} b3 & 09 & cd & ba \\ 53 & d0 & 30 & 20 \\ 72 & ca & 94 & bd \\ 04 & 84 & 85 & 25 \end{bmatrix}$$

o/p of shift row

No change $\begin{bmatrix} b3 & 09 & cd & ba \\ d0 & 30 & 20 & 53 \\ 94 & bd & 72 & ca \\ 25 & 04 & 84 & 85 \end{bmatrix}$

1 byte shift

2 byte "

3 byte "

Fixed matrix

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \otimes \begin{bmatrix} b3 & 09 & cd & ba \\ d0 & 30 & 20 & 53 \\ 94 & bd & 72 & ca \\ 25 & 04 & 84 & 85 \end{bmatrix}$$

o/p of shift row

Step 1 | Row 1

$02 \times b3 \oplus 03 \times d0 \oplus 01 \times 94 \oplus 01 \times 25$

$02 \times b3 = 0000\ 0010 \times 0110\ 0011$

$= x\left[x^6 + x^5 + x + 1\right]$

$= x^7 + x^6 + x^2 + x$ — (1)

$03 \times d0 = 0000\ 0011 \times 1101\ 0000$

$= x+1\left[x^7 + x^6 + x^4\right]$

$= x^8 + x^7 + x^5 + x^7 + x^6 + x^4$

$= x^8 + x^6 + x^5 + x^4$

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

$= x^6 + x^5 + x^3 + x + 1$ — (2)

2

$01 \times 94 = 0000\ 0001 \times 1001\ 0100$

$= 1[x^7 + x^4 + x^2]$

$= x^7 + x^4 + x^2$ ——— (3)

$01 \times 25 = 0000\ 0001 \times 0010\ 0101$

$= 1[x^5 + x^2 + 1]$

$= x^5 + x^2 + 1$ ——— (4)

$= x^7 + x^6 + x^2 + x$ — (1)

$= x^6 + x^5 + x^3 + x + 1$ — (2)

$= x^7 + x^4 + x^2$ ——— (3)

$= x^5 + x^2 + 1$ ——— (4)

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

$= 0001\ 1100$

$x = 1C$

Step 2 | Row 2

01×63 (1) $02 \times d0$ (5) 03×94 (5) 01×25

$01 \times 63 = x^6 + x^5 + x + 1$ ——— (1)

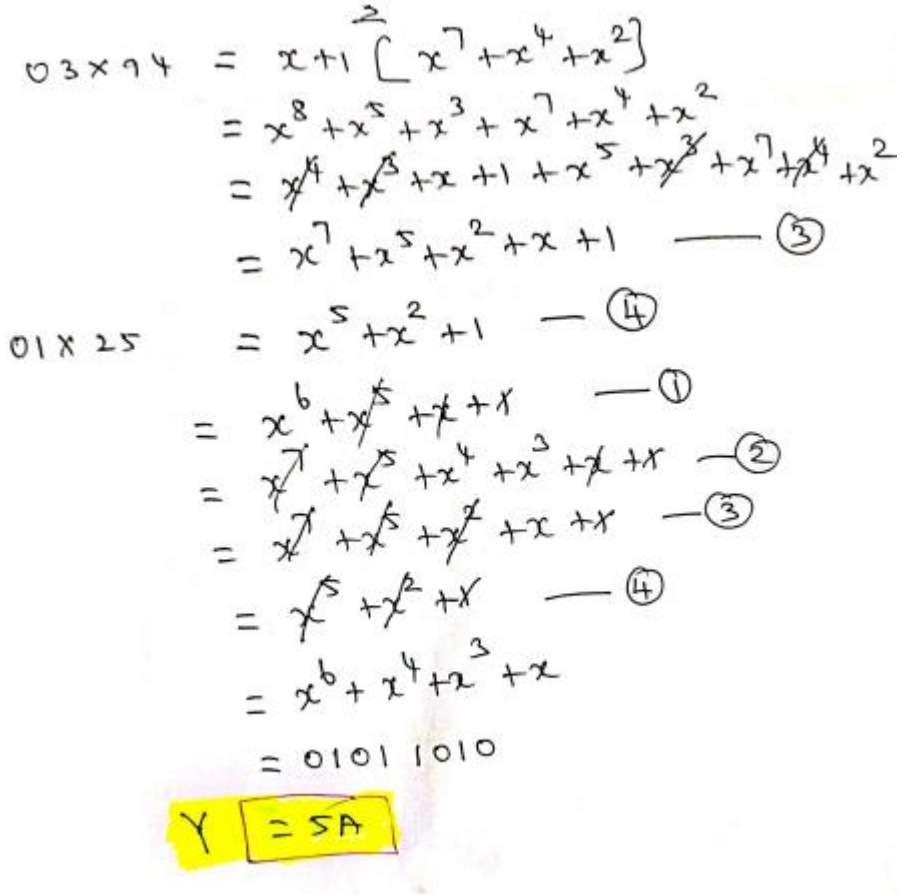
$02 \times d0 = 0000\ 0010 \times 1101\ 0000$

$= x[x^7 + x^6 + x^4]$

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

$= x^4 + x^3 + x + 1 + x^7 + x^5$

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



5.	Describe the operation of S-Box group and S-Box rule. Also, Find the output of S box group from the output of the whitener (XOR) operation of DES function using given S-Box tables. The output of the whitener is 48-bit values, which serves as the input to the S-boxes. The 48-bit values are given as follows: 110011101010011001110110000011111000101011011110 Answer: Operation of S-box group: 1 mark S-Box Rule: 1 mark Output of the S box group (Each s-box:1 mark): 8 marks Operation of S-box group: (Either draw this diagram or theoretically, they can explain) 48-bit input Array of S-Boxes S-Box S-Box S-Box S-Box S-Box S-Box S-Box S-Box 32-bit output **Fig. 6.7** *S-boxes*	10		

S-Box Rule:
(Either draw this diagram or theoretically, they can explain)

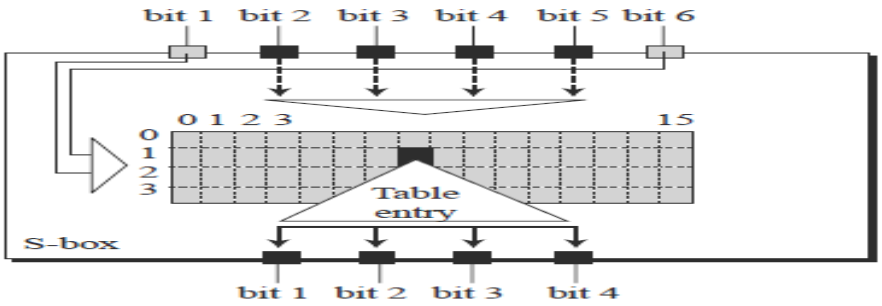


Fig. 6.8 S-box rule

Output of the S-Box Group:

Inputs

110011 (S box 1) 101010 (S2) 011001 (S3) 110110 (S4)

000011 (S5) 111000 (S6) 101011 (S7) 011110 (S8)

S Box 1 :-

110011 → 11 (Binary) – 3 (Decimal) → Row

110011 → 1001 (B) – 9 (D) – column

check in Row 3 & column 9

Result is 11 (D) → 1011 (B)

S Box 2 :-

101010 → 10 (B) – 2 (D)

101010 → 0101 (B) – 5 (D)

Row 2 & column 5

Result is 04 (D) → 0100 (B)

S Box 3 :-

011001 → 01 (B) – 1 (D) → R

011001 → 1100 (B) – 12 (D) – C

12 (D) → 1100 (B)

S Box 4 :-

110110 → 10 (B) – 2 (D) → R

110110 → 1011 (B) – 11 (D) → C

14 (D) → 1110 (B)

S Box 5:-

000011 → 01 (B) — 1 (D) → R
000011 → 0001 (B) — 1 (D) → C

11 (D) — 1011 (B)

S Box 6:-

111000 → 10 (B) — 2 (D) → R
111000 → 1100 (B) — 12 (D) → C

01 (D) — 0001 (B)

S Box 7:-

101011 → 11 (B) — 3 (D) → R
101011 → 0101 (B) — 5 (D) → C

04 (D) — 0100 (B)

S Box 8:-

011110 → 00 (B) — 0 (D) → R
011110 → 1111 (B) — 15 (D) → C

07 (D) — 0111 (B)

Final Answer:-

1011 0100 1100 1110 1011 0001 0100 0111

****