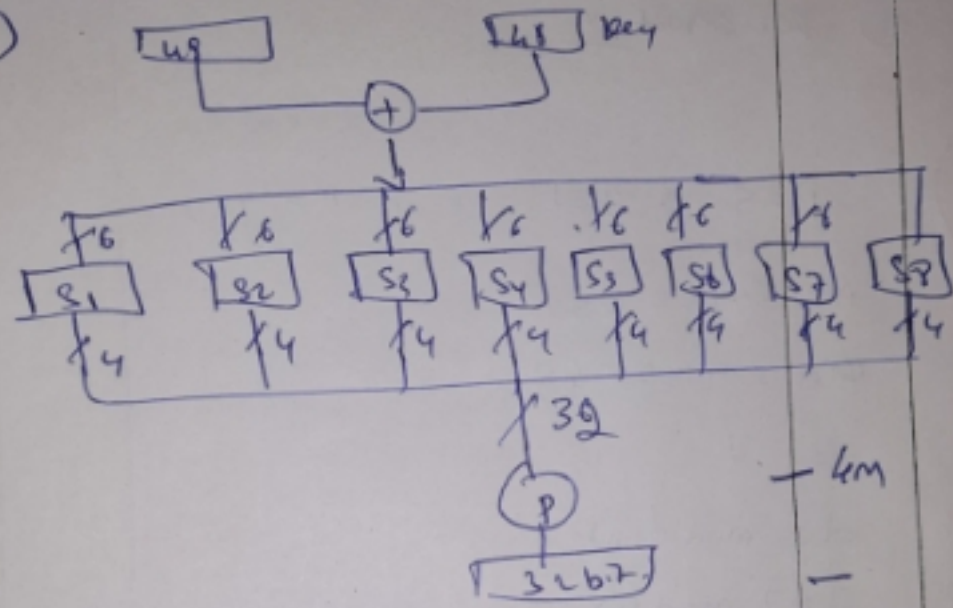


Q. No.	Description	Marks Distribution
7)	<p>① public announcement - 2 2 m</p> <p>② public Directory - 2 2 m</p> <p>③ public Authority - 3 m</p> <p>④ public certificate - 3 m</p> <p>Explanation with neat diagram</p>	10 M

7

Q no.	Description	Marks
6)	<p>a) diff Any four difference b/w diffusion & Confusion -4m</p> <p>b)</p>  <p>-4m</p> <p>-</p> <p>-> 1st & last bit represents row information</p> <p>-> middle 4 bit represents column information</p> <p>Example and show</p> <p>11- 3 - row</p> <p>1000 - 8 - column</p>	<p>-4m</p> <p>-</p> <p>-2M</p>

Q no.	Description	Marks
	<p><u>Explanation of Working of AES</u></p> <ol style="list-style-type: none"> Substitute byte operation Shift rows operation Mix column operation Key Expansion <p>4m</p>	
5)	<p> $p=5$ & $q=13$ $e=7$ $m=14$ $n = 5 \times 13 = 65$ $\phi(n) = 4 \times 12 = 48$ $e = 7$ $d \cdot e \bmod \phi(n) = 1$ $7 \times 7 \bmod 48 = 1$ $d = 7$ $C = M^e \bmod n$ $= 14^7 \bmod 65$ $C = 14$ </p> <p> $M = C^d \bmod n$ $= 14^7 \bmod 65$ $m = 14$ </p> <p>10m</p>	

Q no.	Description	Marks
3)	<p> $q = 11$ 25 </p> <p> $x_A = 4$ $x_B = 7$ </p> <p> $y_A = 2^4 \bmod 11$ $y_B = 2^7 \bmod 11$ </p> <p> $y_A = 5$ $y_B = 7$ </p> <p> $K_A = 7 \bmod 11$ $K_B = 5 \bmod 11$ </p> <p> $= 3$ $K_B = 3$ </p>	10M
4)	<p> </p>	6M

Q no.	Description	Marks
	<p> $\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 1 & 0 & 1 \end{array} \quad \begin{array}{ccc} 1 & 1 & 0 & 0 \end{array}$ </p> <p> $E/p = 11101011$ </p> <p> $\begin{array}{r} \oplus \\ 01000011 \\ \hline 10101000 \\ \hline \end{array}$ </p> <p> $\begin{array}{cc} \text{row} = 2 & \text{row} = 2 \\ \text{col} = 1 & \text{col} = 0 \end{array}$ </p> <p> $\begin{array}{c} S_0 \rightarrow 10 \\ S_1 \rightarrow 11 \end{array}$ </p> <p> $\begin{array}{c} \downarrow \\ P \\ \downarrow \\ 0111 \\ \oplus \\ 1100 = 1011 \end{array}$ </p> <p> $\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{array}$ </p> <p> $\begin{array}{c} \downarrow \\ \boxed{1011} \end{array}$ </p> <p> $\begin{array}{c} \downarrow \\ \boxed{11110011} \end{array}$ </p>	<p>10M</p> <p>③</p>

Q. No.	Description	Marks
1)	$P = S$	1
	$P.T = 1 \overset{1}{0} \overset{2}{0} \overset{3}{1} \overset{4}{0} \overset{5}{1} \overset{6}{0} \overset{7}{1}$	
2)	$P.T = 10010101 \quad K_1 = 10100100$	
	$K_2 = 01000011$	
	$S.P = 0 \overset{1}{1} \overset{2}{0} \overset{3}{1} \overset{4}{1} \overset{5}{1} \overset{6}{0} \overset{7}{0}$	
	$E/P = 01101001$	
	\oplus 10100100 $\hline 11001101$	
	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> $\overbrace{1100}$ row 2 col = 2 </div> <div style="text-align: center;"> <div style="border: 1px solid black; padding: 2px;">S₀</div> 01 </div> <div style="text-align: center;"> <div style="border: 1px solid black; padding: 2px;">S₁</div> 00 </div> <div style="text-align: right;"> row 3 col = 2 </div> </div>	
	$\overset{1}{0} \overset{2}{1} \overset{3}{0} \overset{4}{0}$ \downarrow <div style="border: 1px solid black; padding: 2px;">P</div> 1000	
	\oplus 0101 $\hline 1101$	

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Approved by AICTE & ISO 9001:2008 Certified)
Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

DEPARTMENT OF TELECOMMUNICATION ENGINEERING

Accredited by National Board of Accreditation Council (NBA)

SCHEME & SOLUTION: CONTINUOUS INTERNAL ASSESSMENT- 2

Date: 18/11/2020

Course: CNS

Course Code: 13TE7DECNS

Semester & Section: 8th 'A' & 'B'

Total no of Pages: 7

Scheme & Solution prepared by: VENKATESH

Signature

Q. No.	Description	Marks
		Distribution
1a) i)	128, 192 or 256	1
b) ii)	Substitution	1
c) iii)	Feistel Cipher Structure	1
d) i)	positive integer & relative prime	1
e) ii)	Greatest Common divisor	1
f) iii)	Confusion	1
g) iv)	ECB	1
h) i)	Authenticated	1
i) ii)	CBF	1