U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

January 2024 Semester End Main Examinations

Programme: B.E. **Semester: VII**
Branch: ES – Cluster Elective **Duration: 3 hrs.**
Course Code: 19EC7CE2NC **Max Marks: 100**
Course: Networks Security and Cryptography

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

			CO	PO	Marks
		UNIT - I			
1	a)	With the help of diagram explain the model of network security. List the basic tasks in designing a particular security service.	*CO1*	*PO1*	**6**
	b)	Describe the OSI Security Architecture in detail.	*CO1*	*PO1*	**10**
	c)	Define cryptology and Denial of service	-	-	**4**
		UNIT - II			
2	a)	What is a digital signature? List the requirements for a digital signature and also the different types of digital signature functions	-	-	**10**
	b)	Find the keys obtained using the diffie hellman key exchange algorithm for the values given: n=29, g=13, x=5,y=8.Also document the steps involved in detail.	*CO2*	*PO2*	**10**
		OR			
3	a)	Explain the modes of block cipher operation in detail.	-	-	**10**
	b)	Analyze and Encrypt an 8-bit Plain text-"10010111" with 10-bit key "1010000010" using Simplified Data Encryption Standard given: P_{10} =3,5,2,7,4,10,1,9,8,6 P_8 =6,3,7,4,8,5,10,9 IP = 2,6,3,1,4,8,5,7 IP^{-1}=4,1,3,5,7,2,8,6 E/P=4,1,2,3,2,3,4,1 P4=2,4,3,1 $S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$ $S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$	*CO2*	*PO2*	**10**

			UNIT - III			
	4	a)	Illustrate the life cycle of virus with relevant phases.	***CO1***	***PO1***	**10**
		b)	Describe the different types of firewall.	***CO1***	***PO1***	**10**
			OR			
	5	a)	Describe the different approaches to intrusion detection in detail	***CO1***	***PO1***	**10**
		b)	Elaborate the key requirements of secure electronic transaction. List its features.	***CO1***	***PO1***	**10**
			UNIT - IV			
	6	a)	What is the goal of an incident response? Discuss the distinct phases of a good Incident Response plan.	-	-	**10**
		b)	Outline the possible steps to be taken for digital forensics or cybercrime investigation. Discuss about the volatility in digital forensics.	***CO1***	***PO1***	**10**
			UNIT - V			
	7	a)	Using JAVA implement a practical cryptographic application.	***CO2***	***PO2***	**10**
		b)	Illustrate the practical cryptographic implementation using Microsoft.NET.	***CO1***	***PO1***	**10**

****