U.S.N.										

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

Autonomous Institute Affiliated to VTU

January / February 2025 Semester End Main Examinations

Programme: B.E. **Semester: VII**
Branch: Electronics and Communication Engineering **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.

			UNIT - I	CO	PO	Marks
1	a)		With a neat diagram, explain the model of network security	-	-	6
	b)		Illustrate the working of the Caesar cipher with an example	CO1	PO1	6
	c)		Define active and passive security attacks. Discuss the functionality of following attacks. a. Masquerade c. Replay b. Modification of messages d. Denial of service	CO1	PO1	8
			OR			
2	a)		Describe the x.800 Security services in detail	-	-	6
	b)		Illustrate the working of the Playfair cipher with an example	CO1	PO1	6
			Illustrate the working of the Hill cipher with an example	CO1	PO1	08
			UNIT - II			
3	a)		Indicate the stages tp produce the sub keys for S-DES Key Generation. Assume 8 block input of plain text 10111101 and 10 bit key.	CO2	PO2	6
	b)		What is the motivation for the Feistal Cipher structure	-	-	4
	c)		How many modes of operation of Block Cipher operations are there? Indicate the advantages for the same.	CO1	PO1	10
			OR			
4	a)		With a neat schematic, explain the single round of DES encryption model.	CO2	PO2	6
	b)		In S-DES, 10 bit key is 1000100010.Find the sub keys K_1 and K_2 if P_{10} = 3 5 2 7 4 10 1 9 8 6 P_8 = 6 3 7 4 8 5 10 9	CO2	PO2	4
	c)		Explain Diffie Hellman key exchange with an example? Discuss advantages and disadvantages?	CO1	PO1	10

			UNIT - III			
	5	a)	Briefly describe the three classes of Intruder?	-	-	**6**
		b)	Illustrate the various approaches to intrusion detection system	***CO1***	***PO1***	**4**
		c)	Give the detailed account on UNIX password Management system	***CO1***	***PO1***	**10**
			OR			
	6	a)	Compare the types of firewalls in detail with necessary sketch	-	-	**6**
		b)	Compare the four generations of antivirus software	***CO1***	***PO1***	**4**
		c)	Explain the key requirements and features of Secure Electronic Transaction	***CO1***	***PO1***	**10**
			UNIT - IV			
	7	a)	Highlight the legal aspects of forensic investigation and its objectives.	***CO1***	***PO1***	**6**
		b)	Illustrate the process of forensic data recovery? What are the 4 types of data recovery?	***CO1***	***PO1***	**6**
		c)	Illustrate Evidence Analysis with an suitable example	***CO1***	***PO1***	**8**
			OR			
	8	a)	Elaborate the different phases of a good IR plan.	***CO1***	***PO1***	**6**
		b)	Describe the different methods for extracting evidence from systems and provide examples of helpful and relevant tools.	***CO1***	***PO1***	**6**
		c)	Illustrate the process of forensic data recovery? What are the 4 types of data recovery?	***CO1***	***PO1***	**8**
			UNIT - V			
	9	a)	Explain the framework used for cryptography in Java?	-	-	**8**
		b)	How is JCE different from JCA?	***CO1***	***PO1***	**4**
		c)	Discuss the challenges in implementation of cryptographic algorithms for security?	***CO1***	***PO1***	**8**
			OR			
	10	a)	Analyze the framework used for cryptography in Java using a flow chart?	***CO2***	***PO2***	**8**
		b)	JCE builds on JCA to provide a broader range of cryptographic features. Justify	***CO1***	***PO1***	**4**
		c)	Contrast the practical cryptographic implementation using Microsoft.NET	***CO1***	***PO1***	**8**

****