U.S.N.										

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

Autonomous Institute Affiliated to VTU

October 2024 Supplementary Examinations

Programme: B.E. **Semester: VI**
Branch: Information Science and Engineering **Duration: 3 hrs.**
Course Code: 22IS6PCCNS **Max Marks: 100**
Course: Cryptography and Network Security

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.

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)	Summarize the motives and objectives behind some of the common security-attacks.	CO 1	PO 1	5
	b)	With a neat diagram, explain the model for network security.	CO 1	PO 1	7
	c)	Find ciphertext for cipher system double transposition cipher using key1 "Crypto" key2=" system" for the plaintext=" cryptography needs mathematics background"	CO 1	PO 1	8
		UNIT - II			
2	a)	Explain the stages and single rounds of the DES encryption model with a neat diagram.	CO 3	PO 2	10
	b)	Distinguish between: Block ciphers and Stream ciphers with a neat diagram.	CO 3	PO 2	10
		UNIT - III			
3	a)	Illustrate the RSA algorithm for encryption and decryption. Perform encryption and decryption using RSA algorithms for prime numbers p=17, q=11, e=7, Key(Block) size=6 and message 00111011.	CO 2	PO 2	10
	b)	Explain the man in the middle attack on Diffie Hellman Key Exchange (DHKE) with neat diagram.	CO 2	PO 2	5
	c)	With a neat diagram, explain Message Digest Generation Using SHA-512.	CO 2	PO 2	5
		UNIT - IV			
4	a)	With a neat diagram, explain Automatic Symmetric Key Distribution for Connection-Oriented Protocol.	CO 3	PO 1	6
	b)	What is Transport Layer Security (TLS)? Explain TLS Record Protocol.	CO 3	PO 1	7
	c)	Explain in detail about the Key Distribution Center (KDC).	CO 3	PO 1	7
		OR			
5	a)	Explain the general schemes for the Distribution of Public Keys.	CO 3	PO 1	10

		b)	With a neat diagram, explain the Handshake Protocol Action.	***CO 3***	***PO 1***	**10**
			UNIT - V			
	6	a)	Explain the two DSA approaches for generating digital signatures used with RSA.	***CO 3***	***PO 1***	**10**
		b)	With a neat diagram, explain IPsec Architecture.	***CO 3***	***PO 1***	**10**
			OR			
	7	a)	Illustrate in detail about the ESP, with packet format.	***CO 3***	***PO 1***	**10**
		b)	Explain Schnorr digital signature scheme with neat diagram and algorithm.	***CO 3***	***PO 1***	**10**

****