U.S.N.										

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

Autonomous Institute Affiliated to VTU

June 2025 Semester End Main Examinations

Programme: B.E. **Semester: VI**
Branch: Institutional Elective **Duration: 3 hrs.**
Course Code: 23IS6OECNS / 22IS6OECNS **Max Marks: 100**
Course: Cryptography and Network Security

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)		(i) Compare specific and pervasive security mechanisms. (ii) Identify the types of attacks on encrypted messages.	*CO1*	*PO1*	**4 +6**
	b)		Use Hill Cipher to encrypt and decrypt the message "SHORTER EXAMPLE". The key for encryption is "HILL" and a 2x2 matrix.	*CO2*	*PO1*	**10**
			OR			
2	a)		Differentiate between (i) Block and Stream Ciphers (ii) Passive and Active Attacks	*CO1*	*PO1*	**10**
	b)		Use Playfair Cipher to encrypt the message "instrumentsz".	*CO2*	*PO1*	**10**
			UNIT - II			
3	a)		Analyze Feistel Cipher Structure with a neat diagram.	*CO3*	*PO2*	**10**
	b)		Explain in detail RC4 stream cipher along with its strength	*CO1*	*PO1*	**10**
			OR			
4	a)		Analyze and explain in detail the design principles of Block Cipher.	*CO3*	*PO2*	**10**
	b)		Illustrate Stream cipher and Block cipher with suitable examples.	*CO1*	*PO1*	**10**
			UNIT - III			
5	a)		Explain the working of Diffie Hellman algorithm. Compute (secret) keys with following values q=23, $\alpha = 7$ A and B discrete private keys $X_A=21$ and $X_B=4$ Calculate Y_A and Y_B	*CO2*	*PO1*	**10**
	b)		Use RSA Algorithm to generate key and encrypt the message M=HI consider values for **p=53, q=59, e=3**	*CO2*	*PO1*	**10**

			OR			
	6	a)	Explain Man-in-the-middle attack with suitable example.	*CO2*	*PO1*	**10**
		b)	Explicate Secure Hash Algorithm (SHA).	*CO2*	*PO1*	**10**
			UNIT - IV			
	7	a)	Describe the key features of Session Key lifetime, Hierarchical key control, transparent key control scheme and decentralized key control	*CO1*	*PO1*	**10**
		b)	Identify the steps trailed for secret key distribution with Confidentiality and Authentication.	*CO2*	*PO1*	**10**
			OR			
	8	a)	Illustrate the simple Use of Public-Key Encryption to Establish a Session Key	*CO4*	*PO3*	**10**
		b)	With suitable diagrams explain the coupling and decoupling processes for key control using control vector Encryption and Decryption.	*CO4*	*PO3*	**10**
			UNIT - V			
	9	a)	Describe Heartbeat Protocol with various subsystems involved in it.	*CO1*	*PO1*	**10**
		b)	Analyze SSL/TLS Attacks. Explain in detail how SSL/TLS helps in protecting advanced persistent malwares.	*CO3*	*PO2*	**10**
			OR			
	10	a)	Explain in detail DSA Signing and Verifying functions with suitable diagram	*CO5*	*PO2*	**10**
		b)	Analyze the benefits and services of IPsec under RFC 430.	*CO5*	*PO2*	**10**

****