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: 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.
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)	Compute play fair cipher Keyword : ATHENS Encrypt the plain text : COMMUNICATE	CO2	PO1	6
	b)	Compute hill cipher Keyword: [2 3 4 5] consider row wise Encrypt the plain text : INFORM	CO2	PO1	6
	c)	Using DOUBLE transposition cipher, Decrypt the message "TRESAAEHMSSEIEXCSISTG" using Key: "ANALYST" OR (1 4 2 3 7 5 6) for the first round and Key: "CENTURY" OR (1 2 3 5 6 4 7) for the second round.	CO2	PO1	8
		OR			
2	a)	Identify the types of attacks on encrypted messages.	CO1	PO1	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
	c)	Compare specific and pervasive security mechanisms	CO1	PO1	4
		UNIT - II			
3	a)	Analyze Feistel Cipher Structure with a neat diagram	CO1	PO2	10
	b)	Perform Key generation, Encryption using S-DES. Details are given below, Plaintext:11100110 Key: 1010101110 IP: 2 6 3 1 4 8 5 7 E/P: 4 1 2 3 2 3 4 1 P10 = [3, 5, 2, 7, 4, 10, 1, 9, 8, 6] P8 = [6, 3, 7, 4, 8, 5, 10, 9]	CO2	PO1	10

			P4 = [2, 4, 3, 1] IP^{-1} = [4, 1, 3, 5, 7, 2, 8, 6] $S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array}\begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$ $S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array}\begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$			
			OR			
4	a)		Explain stream generation of RC4 algorithm and give its strengths.	*CO3*	*PO3*	**10**
	b)		Perform Encryption and Decryption using S-DES. Details for computation are Plaintext: 10010111, Key : 1010000010 **P4**: 2 4 3 1 **IP**: 1 1 1 0 1 0 1 1 **IP^{-1}**: 4 1 3 5 7 2 8 6 **P8**: 6 3 7 4 8 5 10 9 **E/P**: 4 1 2 3 2 3 4 1 **P10**: 3 5 2 7 4 10 1 9 8 6 $S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array}\begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$ $S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array}\begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$	*CO2*	*PO1*	**10**
			UNIT - III			
5	a)		Consider a Diffie-Hellman scheme with a common prime q = 353 and a primitive root α = 3. If user A chooses X_A = 97, and if user B chooses X_B = 233, Compute their respective public keys and their shared session keys?	*CO4*	*PO2*	**6**
	b)		In a public- key system using RSA, you intercept the ciphertext C= 10 sent to a user whose public key is e=5, p=7, q=5. What is the plaintext M?	*CO3*	*PO2*	**6**
	c)		Illustrate the generation of message digest using SHA-512 Logic.	*CO3*	*PO3*	**8**
			OR			
6	a)		Compare Asymmetric and Symmetric Encryption	*CO3*	*PO2*	**6**

		b)	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*	**6**
		c)	Use RSA Algorithm to generate key and encrypt the message M=HI consider values for **p=53, q=59, e=3**	*CO2*	*PO1*	**8**
			UNIT - IV			
	7	a)	Illustrate the techniques for the distribution of public keys with a neat diagram.	*CO1*	*PO2*	**10**
		b)	Elucidate on SSL record protocol	*CO3*	*PO2*	**10**
			OR			
	8	a)	Explain : i) Key distribution using symmetric Encryption ii) Key distribution using asymmetric Encryption	*CO4*	*PO4*	**10**
		b)	Illustrate Handshake protocol with neat diagram and also explain all the phases in detail.	*CO1*	*PO3*	**10**
			UNIT - V			
	9	a)	Explain Direct digital signature algorithm and NIST digital signature algorithm	*CO2*	*PO2*	**10**
		b)	Elucidate on security associations and its database	*CO2*	*PO2*	**10**
			OR			
	10	a)	Provide SCHNORR Digital signature scheme. Elucidate on security policy database.	*CO2*	*PO2*	**10**
		b)	Derive protocol considerations in both INBOUND and OUTBOUND IP traffic processing	*CO3*	*PO3*	**10**

****