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: V**
Branch: Information Science and Engineering **Duration: 3 hrs.**
Course Code: 23IS5PCCNS **Max Marks: 100**
Course: Cryptography and Network Security

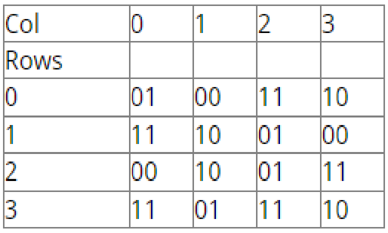
Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

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)	Discuss Security attacks recommended by X.800 Security architecture for OSI.	*CO1*	*PO1*	**8**
	b)	Encrypt the given plain text “This is the final exam” with the key guidance using Playfair cipher.	*CO2*	*PO1*	**6**
	c)	Using Double Transposition, Perform Encryption for the given plaintext: “THIS IS A SECRET MESSAGE” with the keys: K1 = keyword and K2 = Secret.	*CO2*	*PO2*	**6**
		OR			
2	a)	Encrypt and decrypt the plaintext: ATTACK using HILL CIPHER for the given key [2 3] [3 6]	*PO2*	*PO1*	**10**
	b)	Discuss the Specific Security mechanisms (any five) defined by X.800.	*CO1*	*PO1*	**5**
	c)	Explain the model of Network Security with a neat diagram.	*CO1*	*PO1*	**5**
		UNIT – II			

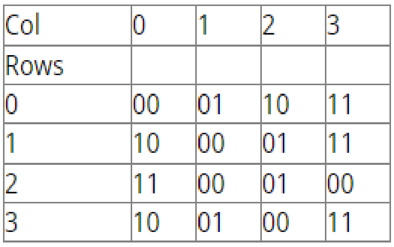
3	a)	Perform Key generation and Encryption using S-DES. Details are given below, Plaintext:00111000, Key: 1111100000
		IP = { 2 6 3 1 4 8 5 7} E/P = { 4 1 2 3 3 4 1 }
		P10 = { 3 5 2 7 4 10 1 9 8 6 }
		P4 = { 2 4 3 1 } IP^{-1} = { 4 1 3 5 7 8 6 }
			CO3	*PO2*	**10**

S-0



Col	0	1	2	3
Rows				
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1



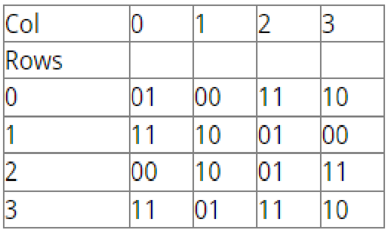
Col	0	1	2	3
Rows				
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Show the steps for Calculation of Key generation and Encryption.

	b)	Write the algorithm for initialization of state vector ‘S’ and Stream generation in RC4 algorithm,	*CO2*	*PO1*	**6**
	c)	List and explain the design principles of the Block Cipher.	*CO1*	*PO1*	**4**
		OR			
4	a)	Illustrate Fiestal Cipher Structure with a neat diagram.	*CO3*	*PO2*	**10**

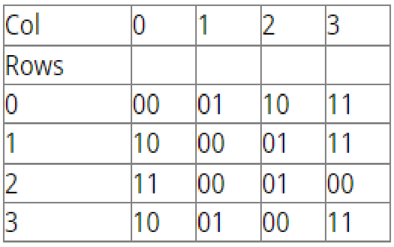
	b)	Perform Key generation and Decryption using S-DES. Details are given below, Ciphertext: 0 0 1 1 1 0 0 0 , Key: 1 0 1 0 0 0 0 0 1 0
		IP = { 2 6 3 1 4 8 5 7} E/P = { 4 1 2 3 3 4 1 }
		P10 = { 3 5 2 7 4 10 1 9 8 6 }
		P4 = { 2 4 3 1 } IP^{-1} = { 4 1 3 5 7 8 6 }
			CO3	*PO2*	**10**

S-0



Col	0	1	2	3
Rows				
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1



Col	0	1	2	3
Rows				
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Show the steps for Calculation of Key generation and Decryption.

		UNIT - III			
5	a)	With a neat diagram, write the steps associated with SHA-512 Logic	*CO3*	*PO2*	**8**
	b)	Illustrate how man in middle attack happens in Diffie Hellman algorithm.	*CO2*	*PO1*	**6**
	c)	In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. Derive the plaintext M.	*CO3*	*PO2*	**6**
		OR			
6	a)	Users A and B use the Diffie Hellman key exchange technique. A common prime q=17 and a primitive root alpha=5 is chosen. (i) If user A has private key XA=4.What is A’s public key YA? (ii) If user B has private key XB=6 What is B’s public key YB? (iii) What is the shared secret key?	*CO3*	*PO2*	**8**

		b)	Identify and explain the attacks on RSA.			**6**
		c)	Demonstrate with a neat diagram how Public Key Cryptosystems provide Secrecy.			**6**
			UNIT - IV			
	7	a)	Illustrate the scenario, how public key is distributed involving public key authority.	***CO3***	***PO2***	**8**
		b)	Describe Secret Key distribution with Confidentiality and Authentication with a neat diagram.	***CO3***	***PO2***	**6**
		c)	List and explain fatal alerts(any six)which is conveyed by TLS to the peer entity using Alert protocol.	***CO1***	***PO1***	**6**
			OR			
	8	a)	Demonstrate the various phases used to establish a secure session using TLS Handshake protocol with a neat diagram.	***CO3***	***PO2***	**10**
		b)	Explain the steps involved in automatic key distribution for the connection-oriented protocol.	***CO1***	***PO1***	**5**
		c)	Describe TLS Record protocol.	***CO1***	***PO1***	**5**
			UNIT - V			
	9	a)	Elucidate Digital Signature algorithm along with signing and Verifying functions.	***C03***	***PO2***	**10**
		b)	List and discuss the benefits of IPsec?	***CO1***	***PO1***	**5**
		c)	Identify how Security Association are used by IPSec to enforce a security policy.	***CO2***	***PO1***	**5**
			OR			
	10	a)	Explain IPsec processing for Outbound and Inbound traffic with a neat diagram.	***CO3***	***PO2***	**10**
		b)	In what order should the signature function and the confidentiality function be applied to a message and why?	***C03***	***PO2***	**5**
		c)	State and describe the requirements for a Digital Signature.	***CO1***	***PO1***	**5**

******