U.S.N.										

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

Autonomous Institute Affiliated to VTU

April 2025 Semester End Make-Up 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.

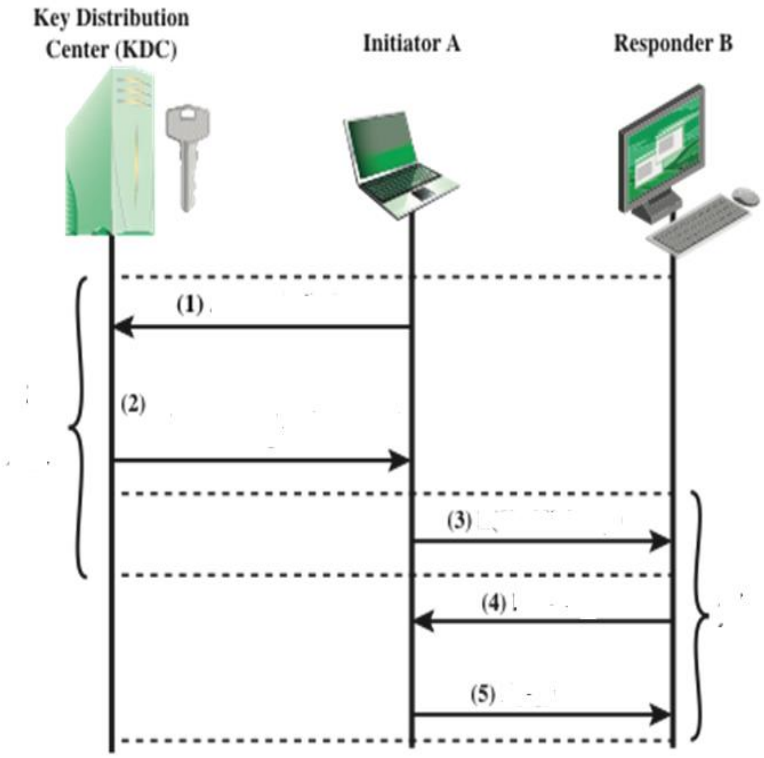
Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

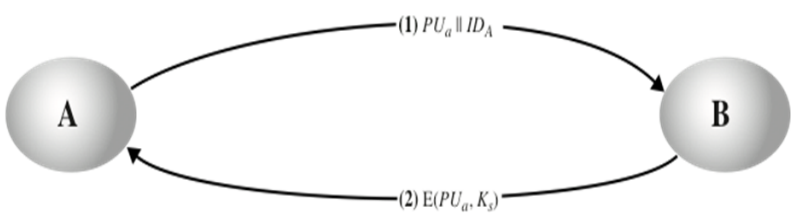
			UNIT - I	CO	PO	Marks
1	a)		Using Playfair cipher Alice wants to, encrypt the following PT : "hide the gold in the tree stump" with Key: "*playfair example"*	CO2	PO1	6
	b)		For the given Ciphertext "FINPOH" apply Hill Cipher and help Bob to decrypt the message using the following Key = $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$ Apply Hill Cipher. (assume a=0 and z=25)	CO2	PO1	8
	c)		Illustrate Network security model with a neat diagram.	CO1		6
			OR			
2	a)		Differentiate between Active and Passive attacks with suitable examples	CO2	PO1	6
	b)		For the given Plaintext "RETREATNOWXX" apply Hill Cipher and encrypt the message using 3*3 matrix using the following Key = "BACKUPABC"	CO2	PO1	8
	c)		Using Double transposition technique decrypt the message "thlfpbrhrgdeiyaaetoefroeortnt" applying the key: 413256	CO2	PO1	6
			UNIT – II			
3	a)		Explain in detail Feistel Cipher Structure with its design principles and parameters.	CO1		10
	b)		Perform Key generation and Encryption using S-DES. Details are given below, Plaintext:00111000 Key: 1111100000	CO2	PO1	10

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] P4 = [2, 4, 3, 1] IP^{-1} =[4, 1, 3, 5, 7, 2, 8, 6] S0 = | | c0 | c1 | c2 | c3 | r0 | 1 | 0 | 3 | 2 | r1 | 3 | 2 | 1 | 0 | r2 | 0 | 2 | 1 | 3 | r3 | 3 | 1 | 3 | 2 | S1 = | | c0 | c1 | c2 | c3 | r0 | 0 | 1 | 2 | 3 | r1 | 2 | 0 | 1 | 3 | r2 | 3 | 0 | 1 | 0 | r3 | 2 | 1 | 0 | 3 |			
		OR			
4	a)	Bhishma wants to secure his data by encrypting the message using stream cipher RC4 algorithm. Illustrate the process followed by Bhishma for key scheduling and Encryption process.	***CO3***	***PO2***	**6**
	b)	Differentiate between block cipher and stream cipher	***CO1***		**4**
	c)	Perform Key generation and Decryption using S-DES. Details are given below, Ciphertext:00111000 Key: 1010000010 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] P4 = [2, 4, 3, 1] IP^{-1} =[4, 1, 3, 5, 7, 2, 8, 6] S0 = | | c0 | c1 | c2 | c3 | r0 | 1 | 0 | 3 | 2 | r1 | 3 | 2 | 1 | 0 | r2 | 0 | 2 | 1 | 3 | r3 | 3 | 1 | 3 | 2 | S1 = | | c0 | c1 | c2 | c3 | r0 | 0 | 1 | 2 | 3 | r1 | 2 | 0 | 1 | 3 | r2 | 3 | 0 | 1 | 0 | r3 | 2 | 1 | 0 | 3 |	***CO2***	***PO1***	**10**
		UNIT – III			
5	a)	Applying RSA cryptosystem, Sita uses two prime numbers p = 13 and q =17 to generate her public and private keys. Given the public key of Sita is 35 and calculate the private key of Sita. Assume the message Sita sends Rama is 10. Find the encrypted format of the message sent by Sita and Rama decrypts the message after receiving and identifies the codeword what Sita have sent.	***CO3***	***PO2***	**10**
	b)	Suppose that two parties Krishna and Arjuna wish to setup a common secret key between themselves using the Diffie-Hellman Key exchange technique. They agree on 7 as the prime number and 3 as the primitive root. Party A chooses 2 and Party B chooses 5 as their respective secrets and calculate the Diffie Hellman Key at Krishna and Arjuna.	***CO3***	***PO2***	**6**
	c)	Sachin wants to send a message to his friend Rahul which should be authenticated. Sachin wants to maintain secrecy in the message transmission following a cryptosystem which addresses his requirements. Identify the cryptosystem and Illustrate the scenarios with a neat diagram.	***CO3***	***PO2***	**4**

			OR			
	6	a)	Illustrate with a diagram how man in middle attack can be performed in Diffie Hellman algorithm.	*CO2*	*PO1*	**8**
		b)	Provide the steps associated with SHA-512 Logic with a neat diagram.	*CO2*	*PO1*	**8**
		c)	Describe the security issues of RSA algorithm	*CO2*	*PO1*	**4**
			UNIT – IV			
	7	a)	Analyze the given figure and complete the steps from 1 to 5 and name the stages and explain the process of key distribution in detail. 	**10**	**10**	**10**
		b)	List and explain some alerts that are fatal in Alert Protocol	*CO1*		**5**
		c)	Compare between publicly available directory and exchange of Public-Key Certificate key distribution techniques.	*CO2*	*PO1*	**5**
			OR			
	8	a)	Elucidate the process of establishing a secure session by using TLS Handshake protocol with neat diagram.	*CO1*		**10**
		b)	Identify the key distribution technique followed in the below mentioned figure. Analyze the scenario where the adversary(attacker) is trying to intercept the messages sent from A to B and then relay the intercepted message or substitute another message man in the middle attack is possible in this scenario. Describe how this attack can be avoided with a diagrammatic representation.	*CO3*	*PO2*	**10**

						
			UNIT – V			
	9	a)	Distinguish between Transport-Mode and Tunnel-Mode techniques in IPsec.	***CO2***	***PO1***	**10**
		b)	Demonstrate the process of IP Traffic Processing with Outbound Packets and Inbound Packets.	***CO2***	***PO1***	**10**
			OR			
	10	a)	Elaborate the SCHNORR Digital Signature Scheme.	***CO2***	***PO1***	**8**
		b)	Explain the process of Digital Signature Algorithm key generation, signature creation and signature verification.	***CO1***		**6**
		c)	Identify the IPSec document categorization groups.	***CO2***	***PO1***	**6**

****