U.S.N.										

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

Autonomous Institute Affiliated to VTU

July 2023 Semester End Main Examinations

Programme: B.E. **Semester: VI**
Branch: Information Science and Engineering **Duration: 3 hrs.**
Course Code: 20IS6PCCNS **Max Marks: 100**
Course: Cryptography and Network Security **Date: 05.07.2023**

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 the main goals of security services in the context of network security.	*CO1*		**05**
	b)	Explain the operation of Ceaser Cipher with an algorithm. Derive the Cipher text using Ceaser cipher for the following plain text message "Enabling Transformation". Key value: 4	*CO2*	*PO1*	**05**
	c)	Encrypt the message "We will meet tomorrow" using playfair cipher with a key "STORY". Provide the rules of Encryption.	*CO2*	*PO1*	**06**
	d)	How do transposition techniques differ from substitution techniques?			**04**
		UNIT - II			
2	a)	Illustrate the process of DES encryption and decryption with suitable diagram. Explain the steps involved in a single round of DES algorithm.	*CO1*		**10**
	b)	Describe the fundamental design principles that should be considered when creating a block cipher.	*CO1*		**05**
	c)	Write the steps involved in initializing the permutation table (S-box) during the initialization of RC4 stream cipher. Provide a detailed illustration of the key mixing process and its impact on the S-box.	*CO3*	*PO3*	**05**
		UNIT - III			
3	a)	Explain Diffie-Hellman key exchange algorithm and solve the following scenario: In the Diffie-Hellman key exchange, users A and B agree on a common prime q=11 and a primitive root a=8. If user A's public key is YA=5, what is the corresponding private key XA? Similarly, if user B's public key is YB=4, what is the corresponding private key XB? What is the value of the shared secret key between A and B?	*CO2*	*PO1*	**08**
	b)	Outline the step-by-step procedure for generating a digest using SHA-512. Provide a comprehensive explanation of how an input message is handled, covering the padding scheme, processing of message blocks, utilization of the compression function, and the finalization steps.	*CO4*	*PO3*	**08**

		c)	List some common vulnerabilities or weaknesses in public-key cryptosystems that make them susceptible to cryptanalysis attacks?	*CO1*		**04**
			UNIT - IV			
	4	a)	Define a key distribution center (KDC). How does it facilitate symmetric key distribution in a network? Describe the role and functioning of a KDC in securely distributing symmetric keys.	*CO1*		**08**
		b)	Discuss Heartbeat protocol and its purpose in the context of SSL/TLS communication?	*CO1*		**06**
		c)	Explain the operations involved in TLS record protocol. Analyze how are application data segmented into records and encrypted for secure transmission?	*CO5*	*PO2*	**06**
			OR			
	5	a)	Describe the key distribution process in a transparent key control scheme. Explain the steps involved in securely distributing symmetric keys between the communicating parties.	*CO5*	*PO2*	**08**
		b)	Explain the concept of the Heartbeat message in the Heartbeat protocol. How does it enable the detection of a live connection between a client and a server?	*CO3*	*PO2*	**06**
		c)	Discuss TLS Alert Protocol and its purpose within the TLS protocol suite?	*CO4*	*PO3*	**06**
			UNIT - V			
	6	a)	Write the main services provided by IPsec (Internet Protocol Security) in securing IP communications. Discuss the significance of each service in ensuring confidentiality, integrity, and authenticity of data.	*CO1*		**06**
		b)	How does IPsec provide data confidentiality in Transport mode? Explain the process of encrypting the payload of an IP packet and the role of encryption algorithms and keys.	*CO1*		**06**
		c)	Identify the role of Security Associations (SAs) in the IPsec architecture? Analyze how SAs are established and maintained to enable secure communication between IPsec peers.	*CO5*	*PO2*	**08**
			OR			
	7	a)	Identify the role of IPsec in ensuring data integrity in Tunnel mode. How are integrity algorithms used to detect any modifications to the encapsulated IP packets?	*CO2*	*PO1*	**06**
		b)	Analyze the process of encapsulating an IP packet in Tunnel mode using ESP. Discuss the role of new IP header, ESP header, and ESP trailer.	*CO4*	*PO3*	**06**
		c)	Analyze the process of generating secure digital signatures using DSA (Digital Signature Algorithm) approach. Discuss the key steps involved in DSA process in ensuring security and integrity of digital signatures.	*CO5*	*PO2*	**08**

****