U.S.N.										

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

Autonomous Institute Affiliated to VTU

January / February 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.

B.M.S.C.E. - ODD SEM 2024-25

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)	With a neat block diagram, describe the model for network security. Explain the different types of attacks on encrypted messages.	*CO1*		**8**
	b)	Encrypt the plaintext “I LOVE INDIA” using Playfair cipher with the key “BANGALORE”.	*CO1*		**6**
	c)	Using the Monoalphabetic Cipher technique, encrypt the plaintext "SECURITY" with a substitution pattern of your choice. Discuss the challenges associated in breaking such a cipher.	*CO1*		**6**
		OR			
2	a)	Define passive and active security attacks. Describe the functioning of the following attacks with a suitable diagrams i) Masquerade ii) Replay iii) Modification of messages iv) Denial of service	*CO1*		**8**
	b)	Derive the cipher text using Ceaser cipher for the following plain text message “Enabling Transformation”.	*CO1*		**6**
	c)	Use a columnar transposition cipher with the keyword "NETWORK" to encrypt the plaintext "COMMUNICATION SYSTEMS". Describe the steps involved in the encryption and decryption process.	*CO1*		**6**
		UNIT - II			
3	a)	Explain the working principle of the Feistel Cipher. Discuss why is it possible to use the same algorithm for both encryption and decryption.	*CO2*	*PO1*	**6**
	b)	Describe the difference between ECB (Electronic Codebook) and CBC (Cipher Block Chaining) modes in block ciphers. Provide the potential vulnerabilities of ECB mode.	*CO3*	*PO2*	**7**

		c)	Provide the role of the keystream in stream ciphers. Discuss why randomness of the keystream critical for the security of the cipher.	*CO1*		**7**
			OR			
	4	a)	Identify the roles of confusion and diffusion in block cipher design. Provide examples of operations used to achieve these properties.	*CO2*	*PO1*	**6**
		b)	Define the Avalanche Effect in block cipher design. How does it ensure that small changes in plaintext or key result in significant changes in ciphertext.	*CO1*		**7**
		c)	Describe how the RC4 stream cipher combines the keystream with the plaintext to produce ciphertext. Discuss the roles of XOR in this process.	*CO2*	*PO1*	**7**
			UNIT - III			
	5	a)	Compare public-key and private-key cryptosystems. Describe the use of a public-private key pair in enhancing security.	*CO2*	*PO1*	**6**
		b)	Given an RSA system where n=33 and e=3, decrypt a ciphertext C=27 Calculate the private key d and demonstrate the decryption process.	*CO4*	*PO3*	**8**
		c)	Illustrate the concept of message digest in the context of SHA-512. Explain how a message of arbitrary length is compressed into a fixed-length hash.	*CO2*	*PO1*	**6**
			OR			
	6	a)	Describe how a public-key cryptosystem enables digital signatures. Provide the process of signing and verification using the public and private keys.	*CO2*	*PO1*	**6**
		b)	Demonstrate the Diffie-Hellman Key Exchange protocol using p= (a prime number) and g = 5 (a primitive root). Assume Alice selects a = 6 and Bob selects b= 15. Calculate the shared secret key.	*CO4*	*PO2*	**8**
		c)	Explain the key properties of cryptographic hash functions, such as pre-image resistance, second pre-image resistance, and collision resistance. Discuss why these properties are important for security.	*CO1*		**6**
			UNIT - IV			
	7	a)	Describe the role of Public Key Infrastructure (PKI) in the distribution and management of public keys. How does PKI ensure the integrity and authenticity of public keys.	*CO2*	*PO1*	**6**
		b)	Describe the concept of a Key Distribution Center (KDC) in symmetric encryption and discuss how does it ensure secure key distribution between two communicating parties.	*CO3*	*PO2*	**7**

B.M.S.C.E. - ODD SEM 2024-25

		c)	Describe the Handshake Protocol in TLS. Identify the key steps involved and how does it establish a secure session between the client and server.	*CO4*	*PO1*	**7**
			OR			
	8	a)	Discuss the role of Certificate Authorities (CAs) in public-key distribution. How does a CA ensure the trustworthiness of a public key?	*CO4*	*PO1*	**6**
		b)	Describe the Heartbeat Protocol in TLS. Discuss its purpose and how it maintains session liveliness during a TLS connection.	*CO4*	*PO1*	**7**
		c)	Explain the concept of a Man-in-the-Middle (MITM) attack on SSL/TLS connections. How can such attacks compromise the security of encrypted communication?	*CO4*	*PO2*	**7**
			UNIT - V			
	9	a)	Provide the role of a private key in generating a digital signature. How does the corresponding public key verify the authenticity of the signature?	*CO5*	*PO1*	**6**
		b)	Discuss how NIST Digital Signature Algorithm combines cryptographic hash functions and modular arithmetic to create secure signatures.	*CO3*	*PO2*	**7**
		c)	Explain the format of the Encapsulating Security Payload (ESP) in IPsec. Provide the fields included and their contribution towards encryption and authentication.	*CO5*	*PO2*	**7**
			OR			
	10	a)	Describe the core security services provided by IPsec: confidentiality, authentication, integrity, and replay protection. How do these services ensure secure communication?	*CO5*	*PO2*	**6**
		b)	Explain the working of the SCHNORR Digital Signature Scheme. How does it achieve security and efficiency in signing and verification?	*CO3*	*PO2*	**7**
		c)	Discuss the difference between transport mode and tunnel mode in ESP. How does each mode impact the encapsulation and protection of IP packets?	*CO5*	*PO2*	**7**

B.M.S.C.E. - ODD SEM 2024-25

******