(Affiliated to University of Mumbai)	***End Semester Examination (R-24/R-25) SH 2026 Answer Key with marking scheme***	
Branch: IT	Course: Cryptography and Network Security	
Year/ Semester: TE V	Course code: ITC501	
Time: 03 hours	Marks: 80	
		Marks
Q. 1	All questions are compulsory.	**30**
A.	Discuss CIA Traid and security services. Define the CIA Triad-3M security services, such as authentication, access control, data confidentiality, data integrity, and non-repudiation -2M	5
B.	Explain the role of Hardware Security Modules (HSMs) in secure key storage and management. Define HSM and its purpose 3M secure generation and storage of cryptographic keys 2M	5
C.	Describe IPsec Authentication Header (AH) and Encapsulating Security Payload (ESP). Define IPsec and its purpose 3M AH: connectionless integrity, data-origin authentication, and anti-replay support; no confidentiality 1M ESP: confidentiality through encryption and optional integrity/authentication and anti-replay protection 1M	5
D.	Explain multi-factor authentication (MFA) with suitable example. Define MFA withexplaination 3M Example 2M.	5
E.	Explain Identity and Access Management (IAM) federation and its role in cloud security. Define IAM federation 1M Explain identity provider (IdP) and service provider/cloud relying party 2M Explain authentication and exchange of trusted assertions 2M	5
F.	Write short note on AI/ML in Threat Detection Explain the role of AI/ML in cybersecurity threat detection 2M Describe data sources, such as network traffic, logs, and endpoint telemetry2M anomaly detection or classification of suspicious activities 1M	5
Q.2A	Compare and Contrast DES and AES. Each difference carry 2M	
	OR	
Q.2B.	Encrypt “Communicate” with Playfair Cipher using key “COMPUTER”. Step 1 Construct the 5 × 5 key matrix. (3 marks) Remove repeated letters from the key and combine I/J in the alphabet. Insert the remaining unused letters in alphabetical order.	

	Step 2 Prepare the plaintext pairs. (2 marks) Plaintext: COMMUNICATE Repeated letters in a pair are separated using X. The plaintext is divided as: CO | MX | MU | NI | CA | TE Step 3: Apply Playfair encryption rules. (4 marks) • Same row: replace each letter with the letter to its right, wrapping around if necessary. • Same column: replace each letter with the letter immediately below it, wrapping around if necessary. • Rectangle: replace each letter with the letter in its own row and the other letter's column. **Plaintext pair Rule Ciphertext pair** CO Same row OM MX Same column RM MU Same row PC NI Rectangle SG CA Rectangle PT TE Same row ER Step 4: Final ciphertext. OMRMPCSGPTER (1 mark)	
Q.3A	Explain the principles of public-key cryptography and distinguish it from symmetric-key cryptography. principles of public-key cryptography-6M Compare public-key and symmetric-key cryptography 4M	
	OR	
Q.3B	Describe Diffie-Hellman Key Exchange algorithm, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged? Description 4M Demonstration of secret key they exchanged 6M	
Q.4A	A company has experienced email spoofing and unauthorized disclosure of confidential attachments. Analyze how PGP and S/MIME can address these threats. PGP 5M S/MIME 5M	
	OR	

Q.4B	Describe Zero Trust Network Architecture (ZTNA), focusing on identity-based access and continuous verification. Definition of Zero Trust Network Architecture (ZTNA) 2M Identity-based authentication least-privilege and application-specific access Device posture and contextual access checks Continuous verification Monitoring, logging, and threat response Example Any 5 Points -2M for each point.	
Q.5A	Differentiate between Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC). Define access control and explain its purpose Explain Discretionary Access Control (DAC) Explain Mandatory Access Control (MAC) Explain Role-Based Access Control (RBAC) Explain Attribute-Based Access Control (ABAC) Give a suitable comparison or application-based conclusion. Valid 5 points carry 10M	
	OR	
Q.5B	Define Privileged Access Management (PAM) and explain its major functions. Define PAM and privileged accounts Privileged credential storage and vaulting Password rotation and credential lifecycle management Privileged session management and monitoring least privilege, just-in-time access, and approval workflows auditing, alerting, and compliance support example Any 5 Points -2M for each point.	
Q.6A	Explain Private Information Retrieval (PIR) and how it protects a user's query privacy. Definiftion How PIR protects query privacy Types of PIR Example Advantages Any 5 Points -2M for each point	
	OR	
Q.6B	Differentiate between Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) Any 5 differences 10M	
	*********** All the Best***********	