

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY-GURUJADA VIZINAGARAM

III B. Tech I Semester Supplementary Examinations November -2025

CRYPTOGRAPHY AND NETWORK SECURITY

(COMPUTER SCIENCE & ENGINEERING)

Time: 3 hours

Max. Marks: 70

Answer any **FIVE** Questions **ONE** Question from **Each unit**

All Questions Carry Equal Marks

UNIT-I			
1.	a)	Describe the different types of cryptographic attacks. How can these attacks be mitigated using cryptographic services and mechanisms?	[7M]
	b)	Explain the fundamental security goals in cryptography and network security. Discuss how these goals are achieved through various cryptographic mechanisms.	[7M]
(OR)			
2.	a)	Discuss the mathematical foundations of cryptography, including modular arithmetic, prime numbers, and finite fields. How are these concepts applied in cryptographic algorithms?	[7M]
	b)	Explain the working principle of symmetric and asymmetric cryptography. Discuss the mathematics involved in both types of cryptographic systems.	[7M]
UNIT-II			
3.	a)	Describe the structure and operation of the Advanced Encryption Standard (AES). How does AES improve upon the security and efficiency of DES?	[7M]
	b)	Write the pseudo code for Miller Rabin primality testing. Test whether 61 is prime or not using the same Miller Rabin test.	[7M]
(OR)			
4.	a)	Discuss the design of S-Box of AES. How it differs from the S-Boxes of DES?	[7M]
	b)	Differentiate between monoalphabetic ciphers and polyalphabetic ciphers and give one example for each.	[7M]
UNIT-III			
5.	a)	Explain the concept of public key infrastructure (PKI). How does PKI facilitate secure communication in asymmetric cryptography?	[7M]
	b)	Define Euler's Totient Function. Prove that, $\phi(pq) = (p-1)(q-1)$, where p and q are prime numbers.	[7M]
(OR)			
6.	a)	Give the encryption/decryption procedures using Elliptic Curve Cryptography (ECC).	[7M]
	b)	In a public key system using RSA, you intercept the cipher text C=8 sent to a user whose public key is e=13, n=33. What is the plain text M?	[7M]
UNIT-IV			
7.	a)	Compare and contrast message authentication codes (MACs) and digital signatures. How are they used to ensure message	[7M]

		integrity and authenticity?	
	b)	Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. What is the implication if same K (secret per message) is used to sign two different message using DSA?	[7M]
		(OR)	
8.	a)	Discuss the challenges in key management in cryptographic systems. What are the best practices for secure key generation, distribution, and storage?	[7M]
	b)	Describe how Diffie-Hellman algorithm used for key exchange is vulnerable to man in middle attack? Determine the shared secret key in a Diffie-Hellman scheme with a common prime 71 and primitive root 7. Given the private keys of the communicating parties A and B are 5 and 12 respectively.	[7M]
		<u>UNIT-V</u>	
9.	a)	Explain the sequence of steps involved in the message generation and reception in Pretty Good Privacy (PGP) with block diagrams.	[7M]
	b)	Explain Hash Function? Discuss SHA- 512 with all required steps, round function & block diagram.	[7M]
		(OR)	
10.	a)	Discuss the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. How do they provide secure communication over the internet?	[7M]
	b)	Explain the sequence of steps used in Secure Socket Layer handshake Protocol for establishing a new session. Draw a diagram which shows the action of Handshake Protocol.	[7M]
