Code No: 20IT6T02-20IT6O01 **R20**

III B. TECH II SEMESTER REGULAR EXAMINATIONS APRIL - 2023
CRYPTOGRAPHY AND NETWORK SECURITY
(COMMON TO CSE & INF BRANCHES)

Time: 3 hours Max. Marks: 70

Note: Answer **ONE** question from each unit **(5 × 14 = 70 Marks)**

~~~~~~

UNIT-I

1.	a)	Classify various types of security attacks.	[7M]
	b)	Apply Caesar cipher to encrypt the message "NETWORK SECURITY".	[7M]
		(OR)	
2.	a)	Explain a model for symmetric cryptosystem with a neat diagram.	[7M]
	b)	Encrypt the message "MEET ME AFTER THE TOGA PARTY" by using Rail fence technique with a depth of 3.	[7M]
		UNIT-II	
3.	a)	Explain AES Algorithm in detail.	[7M]
	b)	What are the Block Cipher Modes of Operations.	[7M]
		(OR)	
4.	a)	Explain about IDEA algorithm with an example.	[7M]
	b)	With a neat diagram explain the internal structure of single round in DES algorithm.	[7M]
		UNIT-III	
5.	a)	Explain Diffie-Hellman Key exchange for encryption and decryption with suitable example.	[7M]
	b)	Discuss about El Gammal Key exchange algorithm in detail.	[7M]
		(OR)	
6.	a)	Illustrate Principles of Public Key Cryptosystems.	[7M]
	b)	Describe Chinese Remainder Theorem with an example.	[7M]
		UNIT-IV	
7.	a)	Write about basic uses of Message Authentication Codes with diagrams.	[7M]
	b)	Demonstrate how the message exchange mechanism in Kerberos 5.	[7M]
		(OR)	
8.	a)	Mention the properties of digital signature.	[7M]
	b)	List and explain the steps used in SHA 512 message digest generation process.	[7M]
		UNIT-V	
9.	a)	Illustrate various types of password management techniques.	[7M]
	b)	Sketch SSL Record Format and explain.	[7M]
		(OR)	
10.	a)	Explain ESP Packet format with a neat diagram.	[7M]
	b)	Write about MIME header fields.	[7M]

* * * * *
~~~~~~