Code No: R2032053 **R20** SET -1

III B. Tech II Semester Supplementary Examinations, December -2023
CRYPTOGRAPHY AND NETWORK SECURITY
(Com. To CSE & IT)

Time: 3 hours Max. Marks: 70

Answer any **FIVE** Questions **ONE** Question from **Each unit**
All Questions Carry Equal Marks
*****

UNIT-I

1.	a)	List and briefly define categories of Security Services and attacks.	[7M]
	b)	Explain integer arithmetic operations in Cryptography.	[7M]
		(OR)	
2.	a)	Describe the model for network security with a neat sketch.	[7M]
	b)	Explain Extended Euclidean Algorithm.	[7M]
		UNIT-II	
3.	a)	Explain in detail about Symmetric Cipher Model.	[7M]
	b)	Discuss about DES algorithm.	[7M]
		(OR)	
4.	a)	What is substitution ciphers and explain any two methods.	[7M]
	b)	Explain about p-boxes in modern block cipher.	[7M]
		UNIT-III	
5.	a)	Summarize the public key cryptographic principles. Explain RSA algorithm for given example, where p = 3 and q = 11.	[7M]
	b)	State and Describe Fermat's theorem.	[7M]
		(OR)	
6.	a)	Explain about MAN-in the Middle Attack (MITM).	[7M]
	b)	Discuss ECC (Elliptical curve cryptography) in detail.	[7M]
		UNIT-IV	
7.	a)	What is HMAC function? Summarize the design objectives of HMAC.	[7M]
	b)	What is the symmetric key distribution? Explain in detail with a suitable example.	[7M]
		(OR)	
8.	a)	What is the role of message authentication in cryptography? Explain.	[7M]
	b)	Discuss about RSA digital signature schemes.	[7M]
		UNIT-V	
9.	a)	Explain in detail Transport Layer Security protocol.	[7M]
	b)	What is SSL (Secure Socket Layer)? Explain in detail with a neat sketch.	[7M]
		(OR)	
10.	a)	Enumerate the functionalities of Secure Shell protocol.	[7M]
	b)	Discuss Tunnel Modes in IPSec with a neat sketch.	[7M]

|'''|'|'|''||'''||||