Code No: **R1941051** **R19** **Set No. 1**

IV B.Tech I Semester Advance Supplementary Examinations, March - 2023

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 75**

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.	[7]
	b)	Describe the model for network security with neat sketch.	[8]
		(OR)	
2	a)	Explain in detail about Symmetric Cipher Model.	[7]
	b)	Explain the following i) Cyber Threats ii) Phishing Attack	[8]

UNIT II

3	a)	Explain the Key Expansion process in AES.	[7]
	b)	Which four tasks are performed in each round of AES Cipher? Explain.	[8]
		(OR)	
4	a)	State and Describe Fermat's theorem.	[7]
	b)	Give a detailed description of key generation and encryption of IDEA algorithm.	[8]

UNIT III

5	a)	Summarize the public key cryptographic principles. Explain RSA algorithm for given example, where p = 3 and q = 11.	[7]
	b)	What is HMAC function? Summarize the design objectives of HMAC.	[8]
		(OR)	
6	a)	Explain about Elgamal NIST Digital Signature Algorithm.	[7]
	b)	Enumerate Diffie-Hellman Key exchange for encryption and decryption with suitable examples.	[8]

UNIT IV

7	a)	Analyze the Cryptographic algorithms used in S/MIME.	[7]
	b)	List and explain the PGP services and explain how PGP message generation is done with a neat diagram.	[8]
		(OR)	
8	a)	Describe IP security Architecture.	[7]
	b)	Briefly explain the scenario of IP security and its Policy.	[8]

UNIT V

9	a)	Explain in detail Transport Layer Security protocol.	[7]
	b)	Is it possible in SSL for the receiver to recorder SSL record blocks that arrive out of order? If so, explain how it can be done. If not, why not?	[8]
		(OR)	
10	a)	Enumerate the functionalities of Secure Shell.	[7]
	b)	Write the methodology involved in computing the keys in SSL/TLS protocol.	[8]