H.T.No: | | | | | | | | | | |

Course Code: 201CS6T03

ADITYA ENGINEERING COLLEGE (A)

CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 hours **Max. Marks: 70**

Answer ONE question from each unit
All Questions Carry Equal Marks
All parts of the questions must be answered at one place only

UNIT – I					
1	a	Discuss different security mechanisms .	L2	CO1	[7M]
	b	Explain Cryptographic attacks in detail.	L2	CO1	[7M]
		OR			
2	a	Illustrate the model of network security with a neat diagram.	L2	CO1	[7M]
	b	State the difference between passive and active security attacks.	L2	CO1	[7M]
UNIT – II					
3	a	Explain the encryption and decryption techniques for AES with neat diagrams.	L2	CO2	[7M]
	b	Explain the types of Symmetric Key Ciphers.	L2	CO2	[7M]
		OR			
4	a	Explain the key generation process of DES with a neat diagram.	L2	CO2	[7M]
	b	Outline the Block cipher design principles.	L2	CO2	[7M]
UNIT – III					
5	a	Illustrate the principles of Public key cryptosystem and its applications.	L2	CO3	[7M]
	b	Perform the Encryption and decryption for p =7, q = 11, e = 17 and m = 8 using RSA algorithm.	L3	CO3	[7M]
		OR			
7	a	Discuss in detail about Elgamal Cryptosystem.	L2	CO3	[7M]
	b	Explain Fermat's little theorem.	L2	CO3	[7M]
UNIT – IV					
7	a	Describe signing and verification in Digital Signature Algorithm.	L2	CO4	[7M]
	b	Briefly describe about the overall processing of Message Digest Generation using MD5 with necessary block diagram.	L2	CO4	[7M]
		OR			
8	a	Explain different Authentication Procedures in X.509 Certificate.	L2	CO4	[7M]
	b	Discuss in detail about the Secure Hash Algorithm	L2	CO4	[7M]
UNIT – V					
9	a	Describe Encapsulating Security Payload (ESP) format.	L2	CO5	[7M]
	b	Give an overview on S/MIME functionality.	L2	CO5	[7M]
		OR			
10	a	Explain the TLS record format with a neat diagram.	L2	CO6	[7M]
	b	Briefly explain Encapsulating Security payload in IP security.	L2	CO6	[7M]

*****