O.P.Code: 19CI0605	R19	H.T.No.									

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR
(AUTONOMOUS)
B.Tech IV Year I Semester Supplementary Examinations June-2024
CRYPTOGRAPHY & NETWORK SECURITY
(Computer Science & Information Technology)

Time: 3 Hours **Max. Marks: 60**

(Answer all Five Units **5 x 12 = 60** Marks)

UNIT-I

1	a	Illustrate different types of Security Attacks and Services in Detail.	CO3	L2	6M
	b	List and briefly define the fundamental security design principles.	CO1	L1	6M
		OR			
2	a	Compare Substitution and Transposition techniques.	CO1	L2	6M
	b	Explain about security approaches.	CO3	L2	6M

UNIT-II

3	a	Formulate the decryption and encryption using RSA algorithm with p=3 q=11 e=7 and N=5.	CO2	L6	6M
	b	List out the attacks to RSA and define each.	CO1	L1	6M
		OR			
4	a	Descover the working principles of simple DES with an example.	CO2	L3	6M
	b	What is the difference between block cipher and stream cipher ?	CO1	L1	6M

UNIT-III

5	a	Describe any one method of efficient implementation of HMAC.	CO1	L2	6M
	b	What types of attacks are addressed by message authentication?	CO1	L1	6M
		OR			
6	a	Explain X.509 Authentication Services.	CO2	L2	6M
	b	Explain the public key infrastructure.	CO3	L2	6M

UNIT-IV

7	a	What is the basic building block of an 802.11 WLAN?	CO5	L1	6M
	b	List some security threats related to mobile devices.	CO1	L1	6M
		OR			
8	a	Evaluate the different protocols of SSL. Explain Handshake protocol in detail.	CO4	L5	6M
	b	What is the difference between a TLS connection and a TLS session?	CO1	L1	6M

UNIT-V

9	a	Elaborate different categories of IPsec documents.	CO6	L6	6M
	b	List and briefly define different categories of IPsec documents.	CO1	L1	6M
		OR			
10	a	Describe the Encapsulating security payload.	CO6	L5	6M
	b	List and briefly describe some benefits of IPsec.	CO1	L1	6M

***** END *****