O.P.Code: 20CI0612 | R20 | H.T.No. □□□□□□□□□□

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR

(AUTONOMOUS)

B.Tech IV Year I Semester Regular Examinations February-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**	Specify the components of encryption algorithm.	**CO1**	**L4**	**6M**
	b	Explain about steganography.	**CO1**	**L2**	**6M**
		OR			
2	**a**	What is security mechanism.	**CO1**	**L1**	**6M**
	b	Explain about a model for network security.	**CO1**	**L2**	**6M**
		UNIT-II			
3	**a**	What is the difference between block cipher and stream cipher?	**CO2**	**L1**	**6M**
	b	What requirements must a public key cryptosystem to fulfill to a secured algorithm?	**CO2**	**L1**	**6M**
		OR			
4	**a**	List the steps in RSA algorithm.	**CO2**	**L1**	**6M**
	b	Consider and Evaluate a Diffie-Hellman scheme with a common prime q=11 and a primitive root α=2 i. Show that 2 is a primitive root of 11. ii. If user A has public key Ya = 9, what is A's private key Xa? iii. If user B has public key Yb = 3, what is the secret key K shared with A?	**CO2**	**L5**	**6M**
		UNIT-III			
5	**a**	Differentiate MAC and Hash function.	**CO3**	**L2**	**6M**
	b	What are the applications of cryptographic hash function?	**CO3**	**L1**	**6M**
		OR			
6	**a**	Describe any one method of efficient implementation of HMAC.	**CO3**	**L2**	**6M**
	b	What types of attacks are addressed by message authentication?	**CO3**	**L1**	**6M**
		UNIT-IV			
7	**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?	**CO4**	**L1**	**6M**
		OR			
8	**a**	Describe transport level security in detail.	**CO5**	**L6**	**6M**
	b	Explain about web security considerations.	**CO5**	**L6**	**6M**
		UNIT-V			
9	**a**	Discuss in detail about S/MIME.	**CO5**	**L2**	**6M**
	b	Why does ESP include a padding field?	**CO5**	**L4**	**6M**
		OR			
10	**a**	Elaborate different categories of IPsec documents.	**CO5**	**L6**	**6M**
	b	List and briefly define different categories of IPsec documents	**CO5**	**L1**	**6M**

*** END ***