Q.P. Code: 19CI0605 **R19**

Reg. No: | | | | | | | | | | |

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR

(AUTONOMOUS)

B.Tech IV Year I Semester Regular Examinations November/December-2022

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.	L4	6M
	b	Explain about steganography.	L2	6M
		OR			
2	a	Illustrate different types of Security Attacks and Services in Detail .	L2	6M
	b	List and briefly define the fundamental security design principles.	L1	6M
		UNIT-II			
3	a	Extend the Diffie-Hellman Key Exchange.	L2	6M
	b	What are the principle elements of a public key cryptosystem?	L1	6M
		OR			
4	a	Explain the block cipher modes of operations.	L2	5M
	b	Explain about IDEA with neat diagram.	L2	7M
		UNIT-III			
5	a	Describe Secure hash Algorithm in detail.	L2	6M
	b	What are the requirements for message authentication.	L1	6M
		OR			
6	a	What is a key distribution center?	L1	4M
	b	What is Kerberos? Define the requirements of a Kerberos.	L1	8M
		UNIT-IV			
7	a	Evaluate the different protocols of SSL. Explain Handshake protocol in detail.	L5	6M
	b	What is the difference between a TLS connection and a TLS session?	L1	6M
		OR			
8	a	Elaborate different level of awareness of a connection in HTTPS.	L6	6M
	b	What steps are involved in the TLS Record Protocol transmission?	L1	6M
		UNIT-V			
9	a	Explain in detail about the security services for E-mail	L2	6M
	b	Explain the operation description of PGP.	L2	6M
		OR			
10	a	Why is base64 conversion useful for an email application?	L4	6M
	b	Explain about internet key exchange.	L2	6M

***** END *****