R16

Reg. No:

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR
(AUTONOMOUS)
B.Tech IV Year I Semester Supplementary Examinations July-2022
INFORMATION SECURITY
(Computer Science & Information Technology)

Time: 3 hours   Max. Marks: 60

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

UNIT-I

1	**a**	Describe in detail about Conventional Encryption Model.	**6M**
	b	Determine the security mechanisms required to provide various types of security services.	**6M**

OR

2	**a**	Explain about the Encryption and decryption functions Triple DES.	**6M**
	b	Explain how diffusion and confusion are used in Block Ciphers.	**6M**

UNIT-II

3	**a**	Determine the GCD(24140,16762) using Euclid's algorithm.	**8M**
	b	Compare conventional encryption with public key encryption.	**4M**

OR

4	**a**	What are the requirements and applications of public key cryptography?	**7M**
	b	Discuss about Euler's theorem.	**5M**

UNIT-III

5	**a**	List out applications of cryptographic hash functions.	**6M**
	b	Explain the characteristics are needed in secure hash function.	**6M**

OR

6	**a**	Compare different types of SHA algorithms with parameters.	**5M**
	b	Discuss about the objectives of HMAC and its security features.	**7M**

UNIT-IV

7	What is secret key distribution? Explain secret key distribution with confidentiality and authentication.	**12M**

OR

8	Write and explain Client/ Server Authentication Exchange service in Kerberos version.	**12M**

UNIT-V

9	**a**	What are the different types of viruses? How do they get into the systems?	**6M**
	b	Explain Intrusion detection in detail.	**6M**

OR

10	**a**	Explain ESP Header of IPSec.	**6M**
	b	What is meant by stateful packet inspection? What are the advantages and disadvantages.	**6M**

*** END ***