Q.P. Code: 16IT611 **R16**

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

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR

(AUTONOMOUS)

B.Tech IV Year I Semester Supplementary Examinations February-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	Discuss in detail about various types of Security attacks with neat diagrams.	**6M**
	b	What is symmetric key cryptography? Discuss its advantages and limitations?	**6M**

OR

2	a	Describe in detail about Conventional Encryption Model.	**6M**
	b	Consider the following: Plaintext: "ACT" Secret key: "GYBNQKURP" Compute the cipher text from given plain text and key using hill cipher method	**6M**

UNIT-II

3	a	Explain the Chinese Remainder theorem.	**8M**
	b	State Fermat's theorem.	**4M**

OR

4	a	State modular arithmetic operations with example.	**7M**
	b	State Fermat's theorem with example.	**5M**

UNIT-III

5		Describe HMAC algorithm in detail.	**12M**

OR

6		Explain the classification of authentication function in detail.	**12M**

UNIT-IV

7	a	Enumerate the differences between Kerberos Version 4 and 5.	**6M**
	b	Explain the authentication procedures defined by X.509 certificate.	**6M**

OR

8	a	Write short notes on PGP.	**6M**
	b	Write short notes on S/MIME.	**6M**

UNIT-V

9	a	What is the use of SSL protocol? Explain SSL record protocol operation with SSL record format.	**6M**
	b	With a neat sketch explain the IPSec scenario and IPSec Services.	**6M**

OR

10	a	Why Internet Key Exchange is used? Write and explain header and payload formats of it.	**6M**
	b	Write and explain TLS functions and alert codes of Transport Layer Security.	**6M**

*** END ***