Name: Student University Roll No.:	Printed Pages:1

School of Engineering
Second Theory Sessional Examination
Odd Semester (AS: 2024-25)

B. Tech: CSE/CCML **[Year :IV]** **[Semester :VII]**

Course Title: Network Security and Cryptography **Course Code:** BCS3702	**Max Marks: 30** **Time: 1*hrs***

Instructions if any: Read the question Carefully.

SECTION 'A' **Q.N.1. Attempt all parts of the following:**		**Course Objective**	**Marks**
a)	What you meant by MAC?	CO2	1
b)	What are the properties of Digital Signature?	CO3	1
c)	What is discrete logarithmic problem?	CO2	1
d)	Define Kerberos.	CO3	1
e)	What do you understand by Digital Certificate?	CO3	1
SECTION 'B' **Q.N.2. Attempt any two parts of the following:**		**Course Objective**	**Marks**
a)	Perform encryption and decryption using RSA Algorithm for the following. P=7; q=11; e=17; M=8	CO2	7.5
b)	What do you understand by Digital Certificate? What are the services provided by PGP?	CO3	7.5
c)	What is Hash function? List the requirements of a Hash function.	CO4	7.5
SECTION 'C' **Q.N.3. Attempt any one part of the following:**		**Course Objective**	**Marks**
a)	What are the operations used in AES?	CO2	10
b)	Find gcd (24140, 16762) using Euclid's algorithm?	CO2	10
c)	Give the benefits of IP security? What are the protocols used to provide IP security?	CO4	10

Table 1: Mapping between COs and questions

Cos	Questions Numbers	Total Marks
CO2	1.a,1.c,2.a,3.a,3.b	29.5
CO3	1.b,1.d,1.e,2.b	10.5
CO4	2.c,3.c	17.5

02.12.2024