PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – MAY 2025

Date: 27-05-2025 **Time:** 09:30 am – 12:30 pm

School: SOCSE	**Program:** B. Tech -CSE(Internet of Things)	
Course Code: CSE 3063	**Course Name:** PRIVACY AND SECURITY IN IOT	
Semester: VI	**Max Marks**: 100	**Weightage**: 50%

CO – Levels	CO1	CO2	CO3
Marks	26	36	38

Instructions:

    (i) Read all questions carefully and answer accordingly.
    (ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks.   **10Q x 2M=20M**

1.	Define Multiplicative inverse	2 Marks	L1	CO1
2.	List the exchange operations in AMQP	2 Marks	L2	CO3
3.	Write Associative law of Modular Arithmetic	2 Marks	L2	CO1
4.	What is primitive Root?	2 Marks	L1	CO1
5.	What is an Elliptic Curve Cryptography?	2 Marks	L1	CO2
6.	List the Operation using ECC	2 Marks	L2	CO2
7.	List the differences between RSA & ECC?	2 Marks	L2	CO2
8.	List four types of Messages in MQTT	2 Marks	L2	CO3
9.	List the differences between MQTT and COAP	2 Marks	L2	CO3
10.	Define Message Queuing	2 Marks	L2	CO3

Part B

Answer the Questions.   **Total Marks 80M**

11.	a.	Identify P+Q, 2P and 5P When P=(4,9), Q=(9,6) for E11(1,2)	**10 Marks**	L3	CO1
	b.	Identify all points which fall on the elliptic curve y^2=x^3+x+2 mod 13	10 Marks	L3	CO1

		Or			
12.	**a.**	Identify 2P, 3P and -P When P=(9,5) for E11(1,2)	10 Marks	**L3**	**CO1**
	b.	Identify all points fall on the curve y^2=x^3+2x+1 mod 11	10 Marks	**L3**	**CO1**

13.	**a.**	Explain Elgamal Digital Signature algorithm to create Signature components and verification components.	**10 Marks**	**L2**	**CO2**
	b.	Apply Elgamal Digital Signature Algorithm to Find signature and verification components and prove V1=V2 where P=13, g=2, k=7, XA=9, H(M)=20	10 Marks	**L3**	**CO2**
		Or			
14.	**a.**	Explain Elliptic Curve Cryptography algorithm based Encryption and Decryption.	**10 Marks**	**L2**	**CO2**
	b.	Apply Elliptic Curve Cryptography algorithm to Identify the Encryption Components using when E11(1,2) with point G (4,2), random integer k=2, nb=3 and Plaint text point (6,9)	**10 Marks**	**L3**	**CO2**

15.	**a.**	Illustrate how Bluetooth layered architecture supports for packet transmission among communication devices?	**10 Marks**	**L2**	**CO3**
	b.	Explain MQTT header with various message types, retain and QOS flags in it.	**10 Marks**	**L2**	**CO3**
		Or			
16.	**a.**	Explain COAP Methods/Responses to collect a temperature data using COAP Protocol.	**10 Marks**	**L2**	**CO3**
	b.	Explain in detail about AMQP Components and various frame types.	**10 Marks**	**L2**	**CO3**

17.	**a.**	Write an algorithm to perform Encryption and Decryption using Elgamal approach	**10 Marks**	**L2**	**CO2**
	b.	Explain RFID Architecture with Message Format.	**10 Marks**	**L2**	**CO3**
		Or			
18.	**a.**	Explain Elliptic Curve Digital Signature algorithm (ECDSA)	**10 Marks**	**L2**	**CO2**
	b.	Explain in detail on XML Stream Features	**10 Marks**	**L2**	**CO3**