Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 08-12- 2025 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** B.TECH	
Course Code: CIT2502	**Course Name:** PRIVACY AND SECURITY IN IOT	
Semester: V	**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 one way property?	**2 Marks**	**L1**	**CO1**
2.	List the exchange operations in AMQP	**2 Marks**	**L2**	**CO3**
3.	Write Commutative 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 applications of ECC	**2 Marks**	**L2**	**CO2**
7.	How ECC is Secured than RSA?	**2 Marks**	**L2**	**CO2**
8.	List four types of Messages in COAP	**2 Marks**	**L2**	**CO3**
9.	List the differences between Piconet and Scatternet	**2 Marks**	**L2**	**CO3**
10.	Explain the use of Retain Flag in MQTT	**2 Marks**	**L2**	**CO3**

Part B

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

11.	**a.**	Identify P+Q, 2P and 5P When P=(2,9), Q=(8,6) for E11(2,3)	**20 Marks**	**L3**	**CO1**
	b.	Identify all points which fall on the elliptic curve y^2=x^3+x+2 mod 13		**L3**	**CO1**
		Or			
12.	**a.**	Identify 2P, 3P and -P When P=(3,8) for E11(1,1)	**20 Marks**	**L3**	**CO1**
	b.	Identify all points fall on the curve y^2=x^3+2x+1 mod 11		**L3**	**CO1**

13.	**a.**	Explain Elgamal Digital Signature algorithm to create Signature components and verification components.	**20 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		**L3**	**CO2**
		Or			
14.	**a.**	Explain Elliptic Curve Cryptography algorithm based Encryption and Decryption.	**20 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)		**L3**	**CO2**

15.	**a.**	Illustrate how Bluetooth layered architecture supports for packet transmission among communication devices?	**20 Marks**	**L2**	**CO3**
	b.	Explain MQTT header with various message types, retain and QOS flags in it.		**L2**	**CO3**
		Or			
16.	**a.**	Explain COAP Methods/Responses to collect a temperature data using COAP Protocol.	**20 Marks**	**L2**	**CO3**
	b.	Explain in detail about AMQP Components and various frame types.		**L2**	**CO3**

17.	**a.**	Explain RFID Architecture with Message Format.	**20 Marks**	**L2**	**CO3**
	b.	Explain in detail on XML Stream Features		**L2**	**CO3**
		Or			
18.	**a.**	Explain Elliptic Curve Digital Signature algorithm (ECDSA)	**20 Marks**	**L2**	**CO2**
	b.	Write an algorithm to perform Encryption and Decryption using Elgamal approach		**L2**	**CO2**