Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025

Date: 07-10-2025 **Time:** 09.30am to 11.00am

School: SOCSE	**Program:** B.Tech	
Course Code : CIT2502	**Course Name:** PRIVACY AND SECURITY IN IOT	
Semester: V	**Max Marks**:50	**Weightage**:25%

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	26	24			

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. **5Q x 2M=10M**

1	What is primitive Root?	**2 Marks**	**L1**	**CO1**
2	Prove 3 is a Primitive Root of 7.-CO1	**2 Marks**	**L1**	**CO1**
3	What is an Elliptic Curve Cryptography?	**2 Marks**	**L1**	**CO1**
4	Prove (3,3) is point on curve y2 = x3+x+1 mod 11	**2 Marks**	**L1**	**CO2**
5	Find λ for point doubling when P= (4,6) where E11(1,1)	**2 Marks**	**L1**	**CO2**

Part B

Answer the Questions. Total Marks 40M

6.	**a.**	Find all points which fall on the elliptic curve y^2=x^3+2x+2 mod 11	**10 Marks**	**L3**	**CO1**
	b.	Add two points in E11(2,2) when P= (5,4) and Q= (9,1)	**10 Marks**	**L3**	**CO1**
Or					
7.	**a.**	Find all points which fall on the elliptic curve y^2=x^3+2x+1 mod 11	**10 Marks**	**L3**	**CO1**
	b.	Find 4P when P= (10,3) where E11(2,1)	**10 Marks**	**L3**	**CO1**

8.	**a.**	Write in detail about the public key cryptography to attain Confidentiality and Authentication	**10 Marks**	**L2**	**CO2**
	b.	Perform Encryption and Decryption using Elgamal Algorithm when Prime no=23, Primitive Root=11, Private Key =6 and Plain Text=10, Random no=3	**10 Marks**	**L3**	**CO2**
Or					
9.	**a.**	Explain in detail about the applications and security of Elliptic Curve Cryptography.	**10 Marks**	**L2**	**CO2**
	b.	Calculate the Secret session using DH Key Exchange using P=13, g=6, XA=7, XB=5	**10 Marks**	**L3**	**CO2**