Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025

Date: 27-10-2025 **Time:** 11.00am to 12.30pm

School: SOE/SOCSE	**Program:** B-Tech	
Course Code : CSE3063	**Course Name:** Privacy and Security in IoT	
Semester: VII	**Max Marks**: 50	**Weightage**: 25%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**36**	**14**			

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	Define an Elliptic Curve.	**2 Marks**	**L1**	**CO1**
2	State the Abelian group property of elliptic curves.	**2 Marks**	**L1**	**CO1**
3	Differentiate between point addition and point doubling.	**2 Marks**	**L2**	**CO1**
4	What is Elliptic Curve Cryptography (ECC)?	**2 Marks**	**L2**	**CO2**
5	What is the purpose of the Diffie-Hellman key exchange?	**2 Marks**	**L2**	**CO2**

Part B

Answer the Questions. **Total Marks 40M**

6.	**a.**	Discuss the role of elliptic curves in cryptography.	**10 Marks**	**L3**	**CO1**
		Or			
7.	**a.**	Explain elliptic curves over finite fields with suitable examples.	**10 Marks**	**L2**	**CO1**

8.	**a.**	Compare ECC with other public-key cryptosystems like RSA and Diffie–Hellman.	**10 Marks**	**L4**	**CO1**
		Or			
9.	**a.**	Describe the method of Diophantus and its relation to elliptic curves.	**10 Marks**	**L2**	**CO1**

10.	**a.**	Describe scalar multiplication and its importance in ECC key generation.	**10 Marks**	**L3**	**CO1**
		Or			
11.	**a.**	Derive the general form and Weierstrass equation of an elliptic curve.	**10 Marks**	**L4**	**CO1**

12.	**a.**	Discuss the Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm with a neat diagram and suitable example.	**10 Marks**	**L5**	**CO2**
		Or			
13.	**a.**	Explain Elliptic Curve Cryptography (ECC) in detail.	**10 Marks**	**L2**	**CO2**