Roll No: | | | | | | | | | | | |

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Mid Term Examinations - October 2026

Date: 06/10/2026 **Time:** 11:45 AM - 01:15 PM

Course Code: CIT2502 **Course Name:** Privacy and Security in IoT

Semester: Fifth Semester **Max. Marks:** 50 **Weightage:** 50%

CO - Levels	CO1	CO2
Marks	92	88

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	Write Commutative law of Modular Arithmetic?	2	CO1	BT1
2	What is one way property?	2	CO1	BT1
3	Write the properties of ECC.	2	CO1	BT1
4	Check (3,8) is point which fall on curve y2 = x3+x+1 mod 11.	2	CO2	BT1
5	Find Multiplicative inverse of -1/2 mod 23.	2	CO2	BT1

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Find all points which fall on the elliptic curve y^2=x^3+3x+2 mod 13.	10	CO1	BT3
7	Add two points in E13(3,2) when P= (3,8) and Q= (9,11)	10	CO1	BT3

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Find all points which fall on the elliptic curve y^2=x^3+3x+2 mod 11.	10	CO1	BT3
9	Find 4P when P= (6,4) where E11(3,2).	10	CO1	BT3

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	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	CO2	BT3
11	Explain in detail about the applications and security of Elliptic Curve Cryptography.	10	CO2	BT2

PART E: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
12	Perform Encryption and Decryption using Elgamal Algorithm when P=19, g=10, XA=5, M=17 and k=6.	10	CO2	BT3
13	Explain how the ElGamal encryption scheme is simulated using Elliptic Curve Cryptography. Describe the key generation, encryption and decryption steps.	10	CO2	BT2