Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 09- 12-2025 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** B.Tech-Computer Science and Engineering (CSE)	
Course Code : CSE3063	**Course Name:** Privacy and Security in IoT	
Semester: VII	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**
Marks	**32**	**34**	**34**

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.	Write the formula for point addition on an elliptic curve.	**2 Marks**	**L1**	**CO1**
2.	Define primitive root in modular arithmetic.	**2 Marks**	**L1**	**CO1**
3.	What is the significance of the base point (generator) in ECC?	**2 Marks**	**L1**	**CO1**
4.	State any two advantages of using ECC over RSA.	**2 Marks**	**L1**	**CO1**
5.	What is the purpose of a hash function in digital signatures?	**2 Marks**	**L1**	**CO1**
6.	What is the discrete logarithm problem in ECC?	**2 Marks**	**L1**	**CO1**
7.	List the key components of ElGamal encryption system.	**2 Marks**	**L1**	**CO2**
8.	Mention two security goals of IoT systems.	**2 Marks**	**L1**	**CO2**
9.	List any two IoT communication protocols used for device-to-cloud communication.	**2 Marks**	**L1**	**CO3**
10.	Define piconet and scatternet in Bluetooth communication.	**2 Marks**	**L1**	**CO3**

Part B

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

11.	For the elliptic curve E:y^2=x^3+x+6" mod " 11, calculate 2P, 3P, and -P when P = (2, 7).	**10 Marks**	**L3**	**CO1**
	Or			
12.	Illustrate the concept of group operation on an elliptic curve with an example over finite field F_p.	**10 Marks**	**L3**	**CO1**

13.	Using $\boldsymbol{E}: \boldsymbol{y^2 = x^3 + 2x + 2} \bmod \mathbf{17}$, compute $\boldsymbol{2P}$ and $\boldsymbol{3P}$ for $\boldsymbol{P = (5, 1)}$.	**10 Marks**	**L3**	**CO1**
	Or			
14.	Demonstrate the method of Diophantus and its relation to elliptic curves.	**10 Marks**	**L3**	**CO1**

15.	Illustrate the process of Elliptic Curve Digital Signature Algorithm (ECDSA) with neat steps and suitable example.	**10 Marks**	**L3**	**CO2**
	Or			
16.	Compute the public and private keys for Alice and Bob using Diffie–Hellman key exchange for p=23, g=5, if X_A=6 and X_B=15.	**10 Marks**	**L3**	**CO2**

17.	Describe the complete architecture of Bluetooth including Radio, Baseband, LMP, and L2CAP layers.	**10 Marks**	**L2**	**CO3**
	Or			
18.	Explain the architecture and working of the MQTT protocol with neat diagram.	**10 Marks**	**L2**	**CO3**

19.	**a.**	Discuss the ElGamal Digital Signature scheme with algorithm steps for signature generation and verification.	**12 Marks**	**L2**	**CO2**
	b.	Determine the differences between ElGamal Signature and DSA with respect to efficiency and security.	**8 Marks**	**L2**	**CO2**
		Or			
20.	**a.**	Describe the Elliptic Curve Diffie–Hellman Algorithm (ECDH).	**12 Marks**	**L2**	**CO2**
	b.	Apply ECDH to compute shared secret key for given parameters p=17,a=2,b=2,G=(5,1),n_A=3,n_B=7.	**8 Marks**	**L3**	**CO2**

21.	**a.**	Discuss the working of RFID-based IoT systems including components and types of tags. Explain how RFID integrates with cloud-based IoT frameworks for real-time tracking.	**20 Marks**	**L2**	**CO3**
		Or			
22.	**a.**	Explain in detail the various IoT communication protocols — MQTT, COAP, and XMPP — with their architecture and use cases. Compare their advantages and limitations.	**20 Marks**	**L2**	**CO3**