Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SET-B

SCHOOL OF ENGINEERING

END TERM EXAMINATION –MAY/JUNE 2024

Semester : Semester VI - B.Tech CSE - 2021	**Date :** JUNE06-2024
Course Code : CSE3063	**Time :** 01:00 PM- 04:00 PM
Course Name : Privacy and Security in IoT	**Max Marks :**100
Program : B.Tech. Computer Science and Engineering	**Weightage :** 50%

Note: **1. Answer ALL 5 FULL Questions.**
2. Each Full Question carries 20 Marks
3. Scientific and non-programmable calculator are permitted.
4. Do not write any information on the question paper other than Roll Number.

1.a.	Find how many primitive root for 17 **[Knowledge]**	**(CO1)**	**(04 Marks)**
1.b.	Using point addition calculate P+Q when P=(1,11) and Q=(8,3) for x^3+2x+1 mod 13 **[Comprehension]**	**(CO1)**	**(06 Marks)**
1.c.	Using various approach Find 2P, 3P and -P When P=(3,8) for E11(1,1) **[Application]**	**(CO1)**	**(10 Marks)**

or

2.a.	Check 3 is a primitive root of 5? **[Knowledge]**	**(CO1)**	**(04 Marks)**
2.b.	Find all the points on Elliptic curve as given as y^2=X^3+2x+5 mod 11 **[Comprehension]**	**(CO1)**	**(06 Marks)**
2.c.	Calculate 2P, 3P and 5P When P=(6,5) for E11(1,1) using point addition and doubling approach **[Application]**	**(CO1)**	**(10 Marks)**
3.a.	List the Properties of ECC **[Knowledge]**	**(CO2)**	**(04 Marks)**
3.b.	Write in detail about Elgamal Digital Signature algorithm to create Signature components and verification components. **[Comprehension]**	**(CO2)**	**(06 Marks)**
3.c.	When P=11,Q=10,G=2,XA=8,K=9, H(M)=12, Perform Elgamal Digital Signature Algorithm to generate signature and verification component **[Application]**	**(CO2)**	**(10 Marks)**

or

4.a.	List the applications of ECC **[Knowledge]**	**(CO2)**	**(04 Marks)**
4.b.	Explain in detail about the Diffie Helman Key Exchange algorithm with appropriate example. **[Comprehension]**	**(CO2)**	**(06 Marks)**

4.c. when P=19, g=10, XA=5,K=6,M=17 to find encryption and decryption component using Elgamal Encryption and Decryption algorithm **[Application]** (CO2) (10 Marks)

5.a. Find the value of x where 17x^2≅ 10 mod 29 when 2 is a Primitive Root of 29, **[Knowledge]** (CO2) (04 Marks)

5.b. Explain about Elliptic Curve Based Diffie Helmen key Exchange algorithm (ECDHA) **[Comprehension]** (CO2) (06 Marks)

5.c. Perform Elgamal Digital Signature Algorithm to generate signature and verification component for P=19,Q=18,G=10,XA=16,K=5, H(M)=14 **[Application]** (CO2) (10 Marks)

or

6.a. Compare ECC with RSA **[Knowledge]** (CO2) (04 Marks)

6.b. Explain in detail about the Public key cryptosystem with neat diagram to achieve confidentiality and authentication **[Comprehension]** (CO2) (06 Marks)

6.c. When y^2=x^3+2x+3 mod 11, G=(2,1), XA=2, XB=3, Apply EC DH key exchange algorithm for sharing Secret key **[Application]** (CO2) (10 Marks)

7.a List AMQP Frame types **[Knowledge]** (CO3) (04 Marks)

7.b. Write in detail about Remaining length flag and its format in MQTT **[Comprehension]** (CO3) (06 Marks)

7.c Explain RFID Architecture with Message Format with neat diagram **[Application]** (CO3) (10 Marks)

or

8.a Explain various COAP Status Code **[Knowledge]** (CO3) (04 Marks)

8.b. Explain the architecture of XMPP with neat sketch **[Comprehension]** (CO3) (06 Marks)

8.c Explain in detail about the Principles of RFID **[Application]** (CO3) (10 Marks)

9.a List the Benefits of RFID **[Knowledge]** (CO3) (04 Marks)

9.b List the comparison between MQTT with COAP with table. **[Comprehension]** (CO3) (06 Marks)

9.c Describe in detail about various frame types and Components of AMQP **[Application]** (CO3) (10 Marks)

or

10.a What are the feature of XMPP? **[Knowledge]** (CO3) (04 Marks)

10.b Explain about COAP Security Aspects. **[Comprehension]** (CO3) (06 Marks)

10.c Describe in detail about XML Stream Features with applications **[Application]** (CO3) (10 Marks)