CST Fourth Semester Midterm Examination, May 2021

Analysis and Design of Algorithms (CS-2201)

Answer any four questions.

Two marks are reserved for neatness.

Full Marks 50 Time 90 minutes

Marks distribution for each question is **4+4+4=12**.

Explanation and steps need to be mentioned for all the problems.

Write your roll number in every page for ready reference.

- Let the last 3 digits of your registration number be x, y and z respectively, with z being the rightmost digit.
- In any problem, reference to these variable names are to be interpreted accordingly.

1. Show the mapping of the following problems by identifying their properties and correspondence:
   (a) Minimum spanning tree problem in terms of Matroid set theory
   (b) Polygon triangulation problem in terms of matrix chain multiplication
   (c) Clique of a graph in terms of Boolean formula satisfiability

2. Explain how choice of data structure influences the complexity of the following algorithms:
   (a) Finding the connected components of a graph
   (b) Searching of elements belonging to a dynamic set
   (c) Multiplying two polynomials of degree n

3. Show the solution steps in sequence for the following problems:
   (a) Miller Rabin test to check primality of the number 561 for base 2.
   (b) Minimum spanning tree using Kruskal algorithm
   (c) Minimum spanning tree using Prim algorithm
   solved for the following complete graph with five vertices and relevant edge weights indicated in the adjacency table below:

Vertex	A	B	C	D	E
A	-	y+2	z+3	2	5
B	-	-	4	3	6
C	-	-	-	x+4	5
D	-	-	-	-	7
E	-	-	-	-	-

4. Consider two small prime numbers 11 and 13 to generate a 7-bit toy RSA cryptosystem.

(a) First describe how to choose your public key e as the nearest integer of $10y + z$ obeying the property requirements of the public key.
(b) Now describe an algorithm that finds your private key. What values of public key and private key have you obtained?
(c) Suppose you want to send a message 'N' with first alphabet of your name as signature to one of your friends. Describe briefly the encryption scheme based on the keys obtained above.

5. Prove/Solve the following mathematically:
(a) Complexity of comparison based Sorting algorithm is bounded by $O(n\ lg\ n)$.
(b) Solve for $T(n) = 2T(n/2) + O(n^2)$.
(c) If any problem belonging to the NP complete set is solvable in P-time, then $P = NP$.