

RAMAKRISHNA MISSION VIDYAMANDIRA

(Residential Autonomous College under University of Calcutta)

THIRD YEAR

B.A./B.SC. SIXTH SEMESTER (January – June) 2013

Mid-Semester Examination, March 2013

Date : 19/03/2013

COMPUTER SC. (Honours)

Time : 11 am – 1 pm

Paper - VII

Full Marks : 50

[Use Separate Answer Books for each Group]

Group A (Computer Graphics & Multimedia)

Answer *any two* from the following

1. a) Give the architectural view of a raster-graphics system with a display processor. [3]
b) Write the operating characteristics for plasma panels display technologies. [2]
c) Consider three different raster systems with resolutions of 640 x 480, 1280 x 1024 and 2560 x 2048. What size frame buffer in kilo bytes is needed for each of these systems to store 24 bits per pixel ? How long would take to load a 1280 x 1024 frame buffer in the same system, if 104 bits can be transferred per second ? [3+2]
2. a) Write down the Midpoint circle algorithm. [4]
b) “For a given object, using odd-even rule one area is marked as interior would not always be marked as interior by using Non zero winding number rule.” - true or false? Justify. [3]
c) A y-direction shear of amount $\frac{1}{2}$, relative to the line $x_{ref} = -1$ is applied on the square with vertices (0,0), (1,0), (1,1), (0,1). What will be the new position of the vertices (0,0) and (1,1)? [3]
3. a) Rotate an object through an angle of 45 degree with center of the object on (1,2,3). The axis of rotation is given by the direction vector (1,1,1) passing through (1,0,0). Determine the transformation matrix and calculate new position of the centre of this object. [6]
b) Show that the transformation matrix for a reflection about the line $y = -x$, is equivalent to a reflection relative to the y-axis followed by a counterclockwise rotation of 90 degree. [4]

Group B (Cryptography)

Answer *question no. 4* and *any one* from the rest

4. Using RSA algorithm, what is the value of cipher text C and value of public key, if the plain text $M = 5$ and $p = 3$, $q = 11$ & $d = 7$? [2½ + 2½]
- OR**
- Suppose two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Find the D-H key. [5]
5. a) Justify, whether Diffie-Hellman key exchange is suitable for encryption or description. [8]
b) What do you mean by EDE mode? [2]
 6. a) Briefly differentiate between the key features of Symmetric & Asymmetric key cryptography. [5]
b) Write a short note on the following:
i) Block ciphers acting as Stream cipher (any one). [3]
ii) Confusion & Diffusion [2]

Group C (Artificial Intelligence)

Answer *question no. 7* and *any two* from the rest

7. Answer *any two* from the following: [2½ x 2]
a) Briefly discuss various types of Agent environments.
b) Define the term Heuristics in for informed search strategies with proper example.

c) What is Conjunctive Normal Form? Convert the following FOL into CNF:

$$\forall x \forall y ((P(x) \wedge Q(y)) \rightarrow \exists z R(x,y,z))$$

8. a) What are Intelligent agents? [2]

b) Consider that a user of an Intelligent agent asks the agent for a place to sit in a room, and the agent can point a chair of the user.

- What are the percepts/sensors for this agent?
- Characterize the operating environment.
- What are the actions the agent can take?
- How can one evaluate the performance of the agent?

[6]

c) Define Uninformed Search.

[2]

9. a) What are the properties of A* search?

[3]

b) Consider the following classroom scheduling problem: There are 4 classes, C1, C2, C3, and C4, and 3 class rooms, R1, R2, and R3. The following table shows the class schedule:

Class	Time
C1	8 a.m – 10.30 a.m
C2	9 a.m – 11.30 a.m

Class	Time
C3	10 a.m – 12.30 p.m
C4	11 a.m – 1.30 p.m

In addition, there are the following restrictions:

- Each class must use one of the 3 rooms, R1, R2, and R3.
- R3 is too small for C3.
- R2 and R3 are too small for C4.

i) Show the initial possible values for each variable, (C1... C4) maintaining the restrictions above.

ii) Express formally all the constraints in this problem.

[5]

c) In what kind of problems Bi- directional search works well?

[2]

10. a) Consider the following intermediate state in a TIC-TAC-TOE game:

O	O	X
	X	
O	X	

Draw the remaining Game tree for the given scenario and suggest a path which X should follow to win the game. Consider from the point of view of the Maximizing player which is X and next is X's turn. [6]

b) What is the difference between Intelligent Backtracking and Chronological backtracking? Give an example where Intelligent Backtracking improves the performance in a search problem as compared to Chronological backtracking. [4]

11. a) Let p denote the statement, "The weather is nice" and q denote the statement, "We have a picnic." Translate the following in English:

i) $p \rightarrow \bar{q}$

ii) $\bar{q} \leftrightarrow \bar{p}$

[4]

b) Prove or disprove $p \wedge (p \wedge q) \vdash q$

[3]

c) Deduce the difference between a function and a predicate in FOL with proper example.

[3]