

1. Answer any five questions

a. State the existing Functional Dependencies based on following instance.

(5 x 2 = 10)

X	Y	Z
1	4	2
1	5	3
1	6	3
3	2	2

b. R(A,B,C,D) is a relation. Which of the following does not have a lossless join, dependency preserving BCNF decomposition?

- i. $A \rightarrow B, B \rightarrow CD$ ii. $A \rightarrow B, B \rightarrow C, C \rightarrow D$ iii. $AB \rightarrow C, C \rightarrow AD$ iv. $A \rightarrow BCD$

c. The following functional dependencies are given.

$AB \rightarrow CD, AF \rightarrow D, DE \rightarrow F, C \rightarrow G, F \rightarrow E, G \rightarrow A$. What will be the Key?

d. The following functional dependencies hold true for the relational schema R (V,W,X,Y,Z).

$V \rightarrow W, VW \rightarrow X, Y \rightarrow VX, Y \rightarrow Z$.

Find the irreducible equivalent FD set for the given relation R.

e. Consider the set of FDs. $F = \{ A \rightarrow BC, CD \rightarrow E, E \rightarrow C, D \rightarrow AEH, ABH \rightarrow BD, DH \rightarrow BC \}$.

Find out the canonical cover of F.

f. If an index contains data records as 'data entries', is it clustered or unclustered? Dense or sparse?

2. Answer any five from the following.

(5 x 4 = 20)

a. Consider a relation stored as a randomly ordered file for which the only index is an unclustered index on a field called salary. If you want to retrieve all records with salary > 20000, is using the index always the best alternative? Explain.

b. Consider the following figure 1.

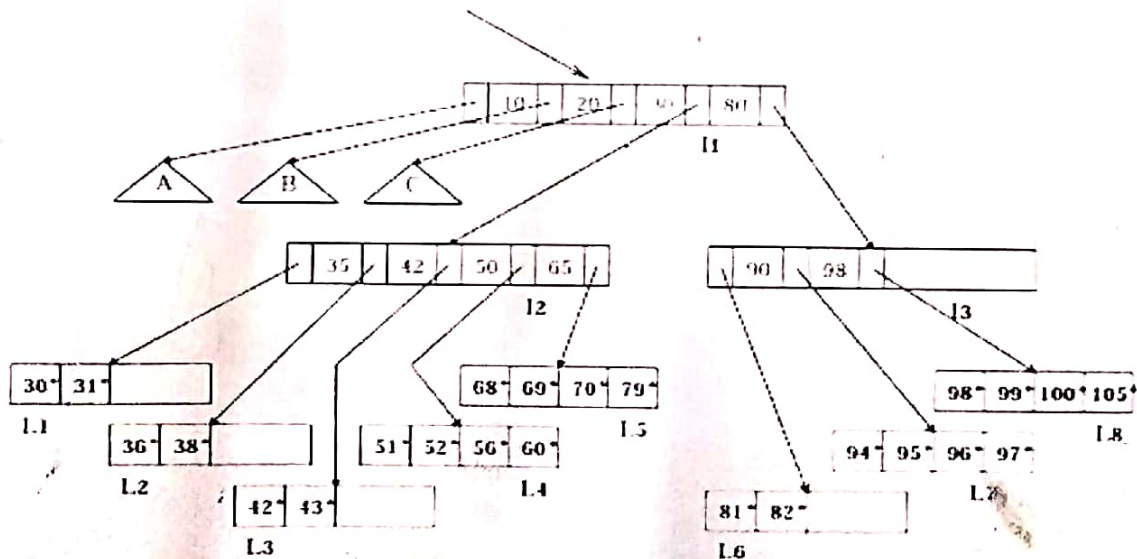


Figure 1

Insert a record with search key 109 into the tree.

Delete the record with search key 81 from the (original) tree.

c. Deduce the expression for computing the cost of external sort algorithm that contains N records and four buffer pages.

d. Consider the following relational schema and the given query.

Employees (eno,ename, add, salary), Projects (pno, pname, pjob), Workin (eno,pno)

Select ename

Where eno IN

(Select eno

From Workin

Where Pno =

(Select Pno

From Projects

Where Pname = "DBMS"))

Order by ename

Give a detailed account of steps involved in optimizing the following query.

e. Consider a relation R (a,b,c,d,e) containing 5,000,000 records, where each data page of the relation holds 10 records. R is organized as a sorted file with dense secondary indexes. Assume that R:a is a candidate key for R, with values lying in the range 0 to 4,999,999, and that R is stored in R:a order.

For each of the following relational algebra queries, state which of the following three approaches is most likely to be the cheapest:

Access the sorted file for R directly.

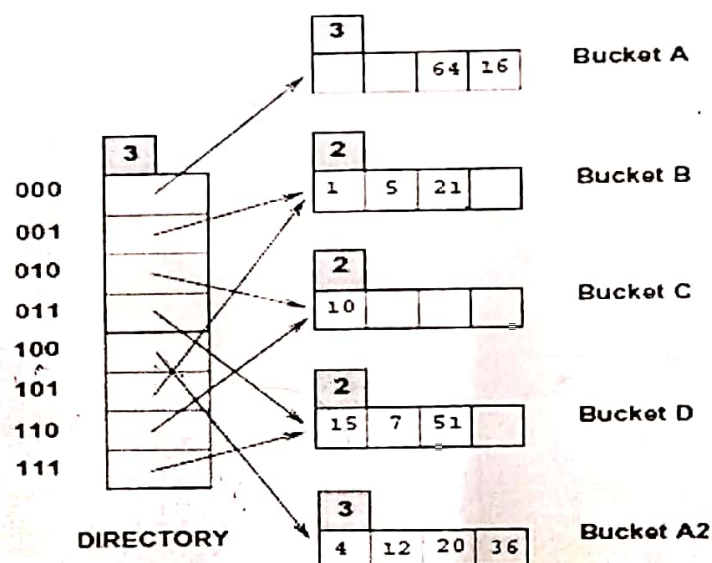
Use a (clustered) B+ tree index on attribute R:a.

Use a linear hashed index on attribute R:a.

1. $a > 50000 \wedge a < 50010(R)$

4. $a < > 50000(R)$

f. Consider the following figure 2.



Show the index after inserting an entry with hash value 68. Suppose you have told that there have been no deletions from the index so far. What can you say about the last entry whose insertion into the index causes a split?

Full Marks-30

M. Sc Sem-II, 2022 Mid-semester examination
Subject- Cryptography & Network Security (CSMC204)

Time - 1 hour

1. Answer any five.

[5 x 2 marks = 10 marks]

- a) Explain the use of S-box in DES algorithm.
- b) State the prime difference between symmetric and asymmetric key cryptography.
- c) Find the value of x and y for $a=5$, $b=10$, which satisfy the equation $ax+by=\gcd(a,b)$.
- d) What is substitution in cryptography?
- e) What is LFSR?
- f) What is passive attack?
- g) What is monoalphabetic cipher? Give an example. (1+1)

2. Answer any four.

[4 x 5 marks = 20 marks]

- a) State Fermat's Little Theorem for prime numbers. Find an a and p pair such that Fermat's theorem is satisfied, but p is not a prime. (3+2)
- b) Explain the steps of RSA algorithm with an example.
- c) Describe the Diffie-Hellman key exchange protocol.
- d) How can Diffie-Hellman key exchange protocol be vulnerable to the man in the middle attack?
- e) Why is 3-DES more secure than 2-DES?
- f) Find the euler totient function value for 43 and 24. (2+3)

[4 x 2 marks = 8 marks]

1. Answer any four.

- (i) Differentiate between tokens, patterns and lexemes.
- (ii) What is a viable prefix? Give an example.
- (iii) Write a CFG to represent palindromes.
- (iv) What do you mean by "Pass" of a compiler? How can you reduce the number of passes?
- (v) Write a grammar which generates strings of 0s and 1s with an unequal number of 0s and 1s.

$S \rightarrow 0A1 \mid 1A0 \mid A$
 $A \rightarrow 011S$

[3 x 4 marks = 12 marks]

2. Answer any three.

- (i) Eliminate left recursion (direct and indirect) from the following grammar :

$S \rightarrow (L) \mid a$
 $S \rightarrow L, S \mid S$

- (ii) Consider the following grammar :

$rexp \rightarrow rexp \mid rexp$
 $rexp \rightarrow rexp rexp$
 $\quad \mid rexp *$
 $\quad \mid (rexp)$
 $\quad \mid letter$

where, \mid , $*$, $($, $)$ and letter are terminals.

- (c) What type of language will be derived by the grammar?

- (d) Show whether the grammar is ambiguous or not. If it is ambiguous, convert it into an unambiguous one.

$(0+11)^* + (1+00)^*$

- (iii) There are some CFG for which shift-reduce parsing cannot be used. Comment.

- (iv) Consider the following grammar :

$A \rightarrow Ba$
 $B \rightarrow dab \mid CB$
 $C \rightarrow d \mid b$

where, A , B , C are non-terminals and the other symbols are terminals. Find the FIRST and FOLLOW sets for all the non-terminals in the grammar.

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, UNIVERSITY OF CALCUTTA
CLASS TEST FOR M. SC. SEMESTER-II

Full Marks: 30

Subject: Advance Operating System (CSMC202)

Time: 1 hour

2x5=10

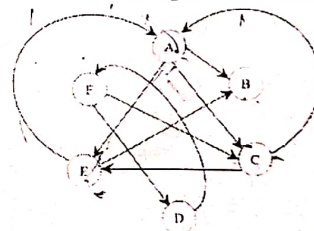
1. Answer any five of the following:

- ☒ a) Define condition of consistency for a distributed system.
- ☒ b) Define global state of a system.
- ☒ c) Define user mobility, and access transparency.
- ☒ d) Compare syntactic versus semantic distribution transparency.
- ☒ e) Define forward and backward intersection of cuts.
- ☒ f) Can a node with in-degree zero act as initiator node for diffusion computation process? Justify your opinion within 150 words.

2. Answer each of the following:

4x5=20

- a) How clocks in nodes are synchronized for Lamport's logical clock model in a distributed system?
- ☒ b) "Chandy-Lamport's state recording algorithm is not an example of diffusion computation model for algorithms" - do you agree with this comment? Justify your opinion within 150 words.
- ☒ c) Is it possible to follow a Master clock in a Master node as the system's clock for an entire distributed system? Justify your opinion within 150 words.
- b) What would be the impact for finding initiator nodes if the network has more than one node with in-degree zero? Justify your opinion within 150 words.
- ☒ e) Identify the node set that can be reached from node A in the figure attached, in a maximum of 2 hops. Also identify the node(s) for the attached figure that can act as possible initiator node(s) for diffusion computation algorithms. Also, for each of the possible initiator nodes(s), identify the order in which the nodes will be traversed till all nodes in the network are reached.



A → C → E
A → F → B