Calcutta University
MSC 2nd Year
Advanced Database Management System (CSMC 201)
MID SEM
Full Mark=20

1. Answer any **four** Question: 4x2=8

a) What is normalization?

b) Define fully functional dependency with the help of suitable example.

c) Differentiate between extendible and static hashing.

d) Define query optimization.

e) What is conflict?

2. Answer any **Three** question: 3x4=12

a) A table has fields, F1,F2,F3,F4,F5, with the following functional dependencies:
F1→F3, F2→F4, F1.F2→F5 in terms of Normalization, this table is in which normal form? Break the table so that it can achieve BCNF.

b) Perform double hashing to store the data item:
First hash function is h1(k)=k% 7 and second is h2(k)=~~(h1(k)+(i*h2(k)))~~ $1+(k \bmod 5)$
%n $n=7$
Values are: 27, 43, 692,72

c) Explain cost-based query optimization with example.

d) Explain lost-update and dirty read problem with example.

M.Sc. 2nd Semester Midsem Examination

Subject:Automata and Compiler Design Paper Code: CSMC 202

(Full Marks – 20, Time: 1hr)

1. Answer any ***four***: 2×4=8

a) If there are n no. of inputs, how many outputs are generated by *Mealy* and *Moore* machines separately? Justify your answer.

b) Why do you need a *DFA* to be minimized?

c) Find a grammar in *Chomsky Normal Form* equivalent to $S \rightarrow aAbB$, $A \rightarrow aA \mid a$, $B \rightarrow bB \mid b$.

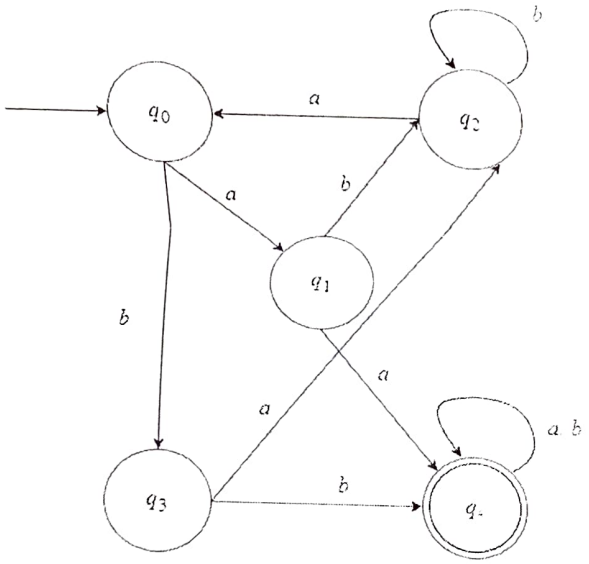
d) Derive the strings concretely generated by the *regular* expression $r = (1+01)^*(0+\lambda)$.

e) When is a production said to be *useless*? Explain with example.

2. Answer any ***three:*** 4×3=12

a) Construct a *Turing Machine* that accepts the language of 010 over $\Sigma = \{0, 1\}$.

b) Minimize the following *DFA*:



c) Construct a *Moore Machine* equivalent to the *Mealy Machine M* defined as follows:

Present State	Next State			
	G=0		G=1	
	State	Output	State	Output
$\rightarrow q_1$	q_1	1	q_2	0
q_2	q_4	1	q_4	1
q_3	q_2	1	q_3	1
q_4	q_3	0	q_1	1

d) Construct a grammar in *Greibach Normal Form* equivalent to the grammar $S \rightarrow AA \mid a$, $A \rightarrow SS \mid b$.

Mid term Examination M.Sc. (Second Semester) Cryptography & Network Security Full Marks: 30

Answer all Questions

a. Encrypt the message "meet me at hill" using the Hill cipher with the key .

9	5
4	7

Show your calculations and the result. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

b. "Hill cipher succumbs to a known plaintext attack if sufficient plaintext–ciphertext pairs are provided." --- Comment with necessary Justification.

c. Comment on the performance of Public Key Cryptography and Secret Key Cryptography for protecting spoofing attack.

d. Find the Multiplicative inverse of 23 in Z_{100}.

e. The encryption Key in a transposition cipher is [3,2,6,1,5,4]. Find the decryption key.

f. Consider a cipher. The cipher is affine, but the keys depend on the position of the character in the PT. If the PT character to be encrypted is in position i, the keys are defined as

The multiplicative key is the (i mod 12) th element in Z_{26}^*

The additive key is the (i mod 26)th element in Z_{26}

Encrypt the message "Exam is fun" using this cipher.

g. Illustrate the meet in the middle attack through an example.

h. Consider a desktop publishing system used to produce documents for various organizations.

- Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
- Give an example of a type of publication in which data integrity is the most important requirement.
- Give an example in which system availability is the most important requirement.

[6+2+2+5+1+5+6+3 = 30]

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, UNIVERSITY OF CALCUTTA

CLASS TEST FOR M. SC. SEMESTER-II, 2023

Full Marks: 30 Time: 1 hour

1. Answer any five of the following: 2x5=10

   a) In a distributed system, what is the significance of finding two or more events as concurrent?
   b) Define the global state of a system.
   c) Define name transparency and explain its significance in a distributed system.
   d) Compare syntactic versus semantic distribution transparency.
   e) Explain how the forward and backward intersection of cuts are related to consistent state recording.
   f) Why, in a distributed system, periodic synchronization of clocks in the participating sites is not considered good?

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) "It is required to record the state of the channel through which the first marker is delivered to any node as empty for the sake of consistent state record" - do you agree with this comment in the context of the Chandy-Lamport's state recording algorithm? 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.