RAMAKRISHNA MISSION VIDYAMANDIRA

(Residential Autonomous College affiliated to University of Calcutta)

B.A./B.Sc. THIRD SEMESTER EXAMINATION, DECEMBER 2019

SECOND YEAR [BATCH 2018-21]

Date : 17/12/2019 **COMPUTER SCIENCE (General)**

Time : 11 am – 1 pm **Paper : III** Full Marks : 50

(Use a separate Answer book for each Group)

Group - A

Answer **any one** question from question no. **1 to 2**: [1×5]

1. Draw an Entity Relationship Diagram of "Airline Reservation System". (5)
2. Discuss Hierarchical data Model with their pros and cons. (5)

Answer **any two** questions from question no. **3 to 6**: [2×10]

3. a) Briefly discuss about DDL and DML in the context of SQL.
   b) What do you mean by cardinality of a relation? Discuss different types of mapping cardinality. ((2.5+2.5)+(2+3))
4. a) Describe data independence in DBMS.
   b) Consider the database scheme given below and answer the queries in the relational algebra:

   Teacher (t_name, dept, tel_no)

   Subject (s_title, credit)

   Student (s_name, course,hostel)

   Taught-by (t_name, s_title)

   Taken-by (s_name, s_title, status, grade)

   i) Find the names of students who take DBMS (subject) as elective (status) and secure A-grade.

   ii) Student of Aurobindo hostel who do not study DBMS

   iii) Name of students who study all subjects taught by Prof X.

   iv) Find the names of students of BSc course living in Netaji hostel who study no subject taught by Prof X. (2+(4×2))
5. a) What is Data Independence? Explain the terms logical and physical data independence with suitable examples.
   b) Discuss the basic relational operators in DBMS in brief. ((2+3)+5)
6. a) Consider the Relation R(ABCDEF) and Functional Dependency set

   $F = \{A \to B, B \to C, C \to D, E \to F\}$ decomposed into

   $D = R_1(AB), R_2(BCD), R_3(DEF)$.

   Find whether D is Lossless or Lossy?

   b) Let R(ABCD) be a relational schema with the following functional dependencies:

   $F = \{A \to B, B \to C, C \to D, D \to B\}$. The decomposition of R into

   $D = \{AB, BC, BD\}$

   Check whether the decomposition D is preserving dependency or not? (5+5)

Group – B

Answer **any one** question from question no **7 to 8**: [1×5]

7. Use playfair cipher to encrypt the message "THE KEY IS HIDDEN UNDER THE DOOR PAD." Make the secret key by filling the first row and part of the second row with the word "GUIDANCE" from left hand side to right hand side in each row and filling the rest of the matrix with the rest of the alphabet. Ignore space between words. (5)
8. Explain different types of attack on confidentiality & Integrity. (5)

Answer **any two** questions from question no **9 to 12**: [2×10]

9. a) Explain the key-expansion operation of AES-256 algorithm.
   b) Differentiate between symmetric key cryptography and asymmetric key cryptography. (6+4)
10. Explain Diffie-Hellman key exchange algorithm. Also explain the problem that may be associated with this algorithm. (6+4)
11. a) Why ECB mode of operation is called "Electronic Codebook"?
    b) Explain the term "cryptology" in brief.
    c) Explain round-key generation operation of DES algorithm with suitable diagram. (2+2+6)
12. Explain the following terms in brief. (2.5×4)
    i) Strength of RSA algorithm.
    ii) Authentication.
    iii) Use of Modular Arithmetic in Cryptography.
    iv) Block Cipher.

———— × ————