RAMAKRISHNA MISSION VIDYAMANDIRA

(Residential Autonomous College affiliated to University of Calcutta)

B.A./B.Sc. THIRD SEMESTER EXAMINATION, DECEMBER 2018

SECOND YEAR (BATCH 2017-20)

Date : 18/12/2018 **COMPUTER SCIENCE (General)**

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

(Use a separate Answer Book for each Group)

Group – A

Answer **any one** question from **Question nos. 1 & 2** : (1 × 5)

1. Draw an ER diagram of College Management System.
2. Discuss about view level, logical level and physical level of DBMS with the help of a diagram.

Answer **any two** questions from **Question nos. 3 to 6** : (2 × 10)

3. a) What is data dictionary? Explain with example. 3

   b) What is partial key, candidate key, super key and primary key. 1+1+1+1

   c) Write down the advantage and disadvantage of Hierarchical Model. 1½+1½

4. a) Define the following algebric operation of Relational Algebra with example table.

      i) Right outer join

      ii) Set difference 2+2

   b) What is lossless join decomposition? 1

   c) Relation $R(ABC)$, $F = \{A \to B, A \to C\}$ decomposed into $D = R_1(AB), R_2(BC)$. Find whether D is Lossless or Lossy? 5

5. a) What are the disadvantages of normalization? 2

   b) Explain Primary & Secondary Index. 2

   c) Decompose the following relation 6

   R till *BCNF*.

   R (*ABCDEFGHIJ*)

   $FD: \{AB \to C,\ A \to DE,\ B \to F,\ F \to GH,\ D \to IJ\}$

6. a) Consider the following schema :

   PERSON (driver_id, name, address)
   CAR (license, model, year)
   ACCIDENT (report_number, date, location)
   OWNS (driver_id, license)
   PARTICIPATED (driver_id, report_number, damage_amount)

Answer the following SQL Queries.

(i) Find the total number of people who owned Cars that were involved in accident in 2017.

(ii) Delete the Mazda belonging to "Mr. X".

(iii) Find the number of accidents in which the Cars belongs to "Mr. X". 3×2

b) What do you mean by partial and total participation? 1+1

c) What is composite attribute? 2

Group – B

Answer **any one** question from **Question nos. 7 & 8** : (1×5)

7. a) Differentiate between symmetric key cryptography and asymmetric key cryptography.

b) Explain the term 'cryptanalysis'. 3+2

8. What are the different types of attack over different principle of security – explain each. 5

Answer **any two** questions from **Question nos. 9 to 12** : (2 × 10)

9. a) Explain the key-expansion operation of AES-128 algorithm.

b) Explain the importance of Modular Arithmetic, Congruence & Residue Matrix in cryptography. 5+(2½+2½)

10. a) Use playfair cipher to encipher the message "The key is hidden under the door pad." The secrete key can be made by filling the first and part of the second row with the word 'guidance' and filling the rest of the matrix with the rest of the alphabet.

b) Write the advantages and disadvantages of CBC mode of operation. 6+(2+2)

11. a) Perform cryptanalysis of affine cipher with respect to chosen plaintext attack.

b) Explain the following terms:

i) Confusion ii) Traffic analysis 6+(2+2)

12. a) Explain the strength of DES algorithm. What are the versions of DES algorithm? Explain any one of them.

b) Explain Diffie-Hellman key exchange algorithm. 5+5

———— × ————