# RAMAKRISHNA MISSION VIDYAMANDIRA

**(Residential Autonomous College affiliated to University of Calcutta)**

**B.A./B.Sc. THIRD SEMESTER EXAMINATION, DECEMBER 2017**

**SECOND YEAR (BATCH 2016-19)**

Date : 16/12/2017 **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. What are the advantages and disadvantages of DBMS over traditional file processing system?

2. Draw an ER diagram of Banking Information System.

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

3. a) Consider a relation R (A, B, C, D, E) on which following functional dependencies hold: F= {A→ BC, A→C, B→D, C→E, CD→E, E→A} what is the key of R? Decompose R into 3NF relation with proper explanation. (1 + 4)

   b) Write down at least four (4) features of relational database management system (RDBMS). (2)

   c) Define the following algebraic operation of Relational algebra. (2 + 1)
   (i) Division (ii) Projection

4. a) Consider the relation R (A, B, C, D, E) and set of FD'S F= {A→ BC, CD→E, B→D, E→A} obtain a lossless join decomposition. Is dependency preserving decomposition of R is possible? (3 + 3)

   b) What are the advantages and disadvantages of Network Data Model? (2)

   c) Define super key with an example? (2)

5. a) What is the disadvantage of normalization? (2)

   b) What is generalization? (2)

   c) What do you mean by DBA? Explain the role of DBA. (2 + 4)

6. a) Consider the following relation schema :
   EMP (eid, ename, add, sal, supervisional, deptid)
   DEPT (deptid, dname, mgrid)
   DEPT_LOC ( deptid, deptloc )
   PROJECT (pno, pname, ploc, deptid )
   WORK_ON (eid, pno )
   Write down the Relation Algebra and SQL for the following query:
   (i) Find the department which has highest salary. (2 + 2)
   (ii) For every project in Kolkata, find the project name, controlling dept id and dept. manager's name. (2 + 2)

   b) What do you mean by Partial Participation? (2)

## Group – B

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

7. a) How many possible keys does the Playfair cipher have ? Ignore the fact that same keys might produce identical encryption results. Explain the answer. (3)

   b) The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key. (2)

8. Give the difference between symmetric and asymmetric cryptosystem with example in each type. (5)

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

9. a) What is residue matrix? (2)

   b) Explain any two non- cryptanalytic attacks. (3)

   c) Using extended Euclidean algorithm, find the greatest common divisor of 400 and 60. (3)

   d) Explain chosen plaintext attack. (2)

10. a) Encrypt the message "meet me at usual place" using Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show the calculations. (6)

   b) Explain the polyalphabetic cipher system with an example. (4)

11. a) Explain Cipher Block chaining (CBC) mode of operation. (3)

   b) Differential between S-Box and P-Box and explain their significance in symmetric key cryptography. (3)

   c) What is the problem associated with Diffie-Hellman key exchange algorithm? Explain. (4)

12. a) Explain steps of RSA algorithm with an example. (4)

   b) What is the advantage of Transposition Cipher over Monoalphabetic Cipher? (2)

   c) Explain the ShiftRows operation of AES algorithm. (3)

   d) What is the difference between different versions of AES algorithm? (1)

———— × ————