RAMAKRISHNA MISSION VIDYAMANDIRA

(Residential Autonomous College affiliated to University of Calcutta)

B.A./B.Sc. THIRD SEMESTER EXAMINATION, DECEMBER 2016

SECOND YEAR [BATCH 2015-18]

Date : 16/12/2016 **COMPUTER SCIENCE [General]**

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

[Use a separate Answer Book for each Group]

Group – A

Answer <u>any one</u> question : [1×5]

1. Explain the 3-level architecture of DBMS with proper diagram.
2. Define Key of a relation. Why do we need to define Key of a relation?

Answer <u>any two</u> questions : [2×10]

3. Draw an ER diagram of a hospital. It maintains all patients visited, including age and address. It also keeps track of the information about the billing, visits, reason for visit and treatment. State any important assumptions you made in reaching the design. Show whether relationships are 1 – 1, 1 – M or N – M. [10]

4. a) Explain different types of Database Languages with example. [4]
   b) What are logical and physical data independence? [3]
   c) What is data dictionary? [3]

5. a) What is the disadvantage of normalization? [2]
   b) Explain First, Second and Third normal forms with a suitable example. [6]
   c) Define multivalued attribute with example. [2]

6. a) Define the following algebraic operations and explain each of these with suitable example.
      i) Selection ii) Projection [4]
   b) Explain ternary relationship in ER diagram with a suitable example. [3]
   c) Give the difference between primary and secondary Indexing. [3]

Group – B

Answer <u>any one</u> question : [1×5]

7. What are the different types of attacks possible on different principle of security?
8. What is the difference between symmetric key cryptography and asymmetric key cryptography? Also write down their advantages and disadvantages. [2·5+2·5]

Answer <u>any two</u> questions : [2×10]

9. a) Explain Diffie-Hellman Key exchange algorithm. What is the problem associated with it? [4+4]
   b) What is residue matrix? [2]

10. a) Decrypt the following message using Mono-alphabetic Substitution Cipher with Key = 4
       wigyvmxc rixiv gsqiw jsv joii [3]
    b) What would be the transformation of a message "Happy birthday to you" using Rail Fence technique? [3]
    c) What is the role of modular arithmetic in cryptography? [2]
    d) Differentiate between Z_n and Z_{n}^{*}. [2]

11. a) Using Euclidean algorithm, calculate greatest common divisor of 25 and 60. [3]

b) State the advantage of Cipher Feed Back (CFB) mode of operation of block cipher by explaining it also. [2+3]

c) What is traffic analysis? [2]

12. a) Given two prime numbers P = 17 and Q = 29, find out N, E and D in an RSA encryption process, where N is the modulus, D is the multiplicative inverse of E modulo $\phi(N)$. ϕ is Euler's Phi function. [3]

b) What is the real strength of RSA? [3]

c) Encrypt the message "RKMV IS AT BELUR" by using playfair cipher. Make the secret key by filling the first and part of the second row by the keyword "COMPUTER". Write the keyword from left hand side to right hand side in each row and fill the rest of the matrix in the same way. [4]

———— × ————