RAMAKRISHNA MISSION VIDYAMANDIRA

(Residential Autonomous College affiliated to University of Calcutta)

SECOND YEAR [2015-18]

B.A./B.Sc. THIRD SEMESTER (July – December) 2016

Mid-Semester Examination, September 2016

Date : 16/09/2016 **COMPUTER SCIENCE (General)**

Time : 12 noon – 1 pm Paper : III Full Marks : 25

[Use a separate Answer Book for each group]

Group – A

*Answer **any one** questions* [1×12·5]

1. a) Define DBA. Explain the roles of DBA. [5]
   b) Explain Data Abstraction. [3]
   c) Explain relational schema with a suitable example. [4·5]

2. a) Define super key, candidate key and primary key with proper example. [5]
   b) What are several types of attributes can be represented in E-R diagram? [3]
   c) Explain various mapping cardinality constraints with suitable example. [4·5]

Group – B

*Answer **any one** questions* [1×12·5]

3. a) Explain fabrication with an example. [1+1]
   b) How modular arithmetic is useful in cryptography? Explain with an example. [1+1]
   c) Find out multiplicative inverse of 132 in Z_{180} using extended Euclidean algorithm. [3]
   d) Do a cryptanalysis of Hill cipher in terms of known-plaintext attack. [3]
   e) What is the use of compression D-box in cryptography? [1·5]
   f) What is the advantage of CFB mode over CBC mode? [1]

4. a) Differentiate between passive attack and active attack with proper example. [1+1]
   b) What is residue matrix? [2]
   c) What is the difference between Z_n and Z_n^* ? Explain with an example. [1+1]
   d) Why ECB mode of operation for block cipher is called 'Electronic Codebook'? [2]
   e) Use playfair cipher to encrypt the message "THE KEY IS HIDDEN UNDER THE DOOR PAD." Make the secret key by filling the first and part of the second row with the word "GUIDANCE" from Left Hand Side (LHS) to Right Hand Side (RHS) in each row and filling the rest of the matrix with the rest of the alphabet. [3·5]
   f) What is the size of the key space of monoalphabetic substitution cipher? [1]

——— × ———