No. of Printed Pages : **1**

Sl. No.

# C8-R4 : INFORMATION SECURITY

**NOTE :**

**1. Answer question 1 and any FOUR from questions 2 to 7.**

**2. Parts of the same question should be answered together and in the same sequence.**

**Time : 3 Hours** **Total Marks : 100**

**1.** (a) Explain the basic objectives of Information Security.
(b) What are hash functions ? Describe some applications where they are used ?
(c) What are the advantages and disadvantages of Asymmetric Cryptography ?
(d) Explain modular arithmetic and show the arithmetic operations of modular operations.
(e) What are some threats associated with a direct signature scheme ?
(f) Briefly explain the basic structure of stream cipher.
(g) What are weak keys in Data Encryption Standard (DES) ? Give examples of weak keys. **(7x4)**

**2.** (a) Explain the process of Miller-Rabin Algorithm of primality testing.
(b) Differentiate between DES and Triple DES Algorithms with an example. **(9+9)**

**3.** (a) Draw and Explain ANSI X9.17 Pseudorandom Number Generator.
(b) Describe any two standard hashes used in hash functions. **(9+9)**

**4.** (a) Why multiple encryption is needed ? What are the problems in AES ?
(b) What do you mean by Provable Security ? Is AES provably secure ?
(c) Explain how man-in the-middle attack affects the Deffie Hellman algorithm. **(6+6+6)**

**5.** (a) What is the EIGamal cryptosystem ? Explain.
(b) What do you mean by Entity based authentication ? Discuss its various types. **(8+10)**

**6.** (a) Explain the purpose of Digital Signature Schemes. Draw block diagram and discuss the properties of digital signature schemes.
(b) What is Fast Exponentiation ? Which cryptography algorithm requires fast exponentiation ? Write steps of one fast exponentiation algorithm. **(9+9)**

**7.** Write Short notes on **any three**.
(a) Euclidean Algorithm
(b) Message Integrity
(c) Birthday Attack
(d) Finite fields of the form GF ($2^n$ ) **(6x3)**

**- o O o -**