No. of Printed Pages : **1**

Sl. No.

C8-R4 : INFORMATION SECURITY

NOTE :

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

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

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

1. (a) Describe any 10 cyber-crime prevention tips.
(b) What are the five principles of security ?
(c) Explain the main properties of "Trustworthy" Encryption Systems.
(d) What is a private key crypto system ? Explain with a suitable example.
(e) How many permutations are used in a DES cipher algorithm ? How many permutations are used in the round-key generator ?
(f) Discuss the key management issues of public key cryptography.
(g) What is PSEUDO-RANDOMNESS ? Explain its importance in security system.

(7x4)

2. (a) Explain different types of attack that can happen on digital signature.
(b) Describe briefly about direct digital signature.
(c) Explain SCHNORR digital signature scheme with a suitable example.

(6+6+6)

3. (a) Explain two categories of attack that can occurred in MAC.
(b) Explain Birthday paradox problem in cryptography with a suitable example.
(c) Explain HMAC algorithm with a suitable example.

(6+6+6)

4. (a) Explain about PRNGs.
(b) Discuss about Linear Congruential Generators.
(c) Explain stream cipher with an example.

(6+6+6)

5. (a) Explain computer algebra system and its role in information security.
(b) Explain Euclidean algorithm and its use with a suitable example.
(c) Discuss linear congruence. What algorithm can be used to solve an equation of type $ax \equiv b(mod\ n)$?

(6+6+6)

6. (a) Describe briefly about Diffie–Hellman key exchange algorithm.
(b) Explain RSA algorithm in detail.
(c) Explain Elgamal Cryptographic System.

(6+6+6)

7. (a) Differentiate between DES and Triple DES.
(b) Explain Chinese Remainder Theorem in detail.
(c) Describe a model for network security.

(6+6+6)

- o O o -