2021

COMPUTER SCIENCE — GENERAL

Paper : SEC-B-X-2

(Information Security)

Full Marks : 80

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer ***questions no.*** **1** and **2** and ***any five*** from the rest.

1. Answer ***any five*** questions : 2×5

(a) What do you understand by network security attack?

(b) Distinguish between active and passive attacks.

(c) Name different types of active attacks.

(d) Name different types of passive attacks.

(e) List different types of cryptanalytic attacks.

(f) Identify any model for internetwork security.

(g) What is cipher?

(h) What is the difference between an unconditionally secure cipher and computationally secure cipher?

2. Write short notes on ***any four*** of the following : 5×4

(a) authentication

(b) access control

(c) data confidentiality

(d) data integrity

(e) non repudiation.

3. Describe different security attacks (passive and active) with detail subcategories from each. 5+5

4. Describe different possible security services provided by a system. 10

5. (a) What are the essential ingredients of symmetric encryption scheme?

(b) What do you mean by public key cryptography? 7+3

6. Describe the structure of DES and its key generation Algorithm. 5+5

7. What is confusion and diffusion in Shannon theory of block cipher? 5+5

8. What is permutation and substitution in DES. What is avalanche effect in DES. 8+2

9. List the public key cryptographic algorithms used in digital signature, encryption/decryption, and key exchange. 4+3+3