2022

COMPUTER SCIENCE — HONOURS

Paper : SEC-B-1

(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 **question nos.** 1 **& 2** and **any four** questions from the rest.

1. Answer **any ten** questions. 2×10

   (a) What do you mean by proxy server?

   (b) What do you mean by proxy firewall?

   (c) Which of the layers of OSI model ensure that data is successfully sent and received between two computers?

   (d) Briefly define field.

   (e) Write short note on stegonography.

   (f) Define 'Worm'.

   (g) What is Block cipher?

   (h) Justify the use of prime numbers in RSA Algorithm.

   (i) Which topology is referred to as Hub-and-Spoke topology?

   (j) Give an example of DDoS attack.

   (k) What are the features of networking?

   (l) What is the functionality of Socket?

   (m) What is 'Trojan'?

   (n) What is Digital Watermarking?

   (o) What is called the Logic Bomb?

2. Answer **any four** questions. 5×4

   (a) Write short note on OS-hardening.

   (b) Distinguish between Block cipher and Stream cipher.

   (c) Distinguish between FTP and DNS server.

Please Turn Over

(d) Explain the concept of Information Security and describe its principles.

(e) State and prove Fermat's Little Theorem.

(f) Explain the Deffie-Hellman Key Exchange Algorithm.

(g) Explain the purpose of S-boxes in DES.

3. (a) Describe S/MIME.

(b) How does the Firewall help to build a secure system?   5+5

4. (a) What is a virus? What are its symptoms?

(b) Explain P2P Network topology.   (2+3)+5

5. (a) Explain basic security threats.

(b) What are the Frameworks available for Network Management? – Explain.   5+5

6. (a) Why SSL layer is positioned between application layer and transport layer?

(b) Name four key steps in the creation of a Digital Certificate.   5+5

7. (a) What is Malware? What kind of precautions can be used to overcome the various problems?

(b) How can the TSR programs be used to override the ISR's of OS? Explain with an example.

                                                                                      (2+3)+5

8. Write short notes on *any two* of the following :   5×2

   (a) DHCP Server

   (b) Hill cipher

   (c) DNS Server

   (d) Digital Signature

   (e) Network Attacks.