Roll No. ....

14353

B.C.A. EXAMINATION

(For Batch 2021 & Onwards)

(Sixth Semester)

INFORMATION SECURITY

BCA-63

Time : *Three Hours*　　　*Maximum Marks :* 80

Note : Attempt Five questions in all. Q. No. **1** is compulsory. Attempt *four* more questions selecting *one* question from each Unit. All questions carry equal marks.

1. (i) What is substitution cipher ?

   (ii) Define AES encryption.

   (iii) Explain PGP.

   (iv) What is system security ?

   (v) Define pretty good privacy.

(vi) Explain transport layer security.

(vii) What are viruses ?

(viii) Explain encryption.

Unit I

2. (a) Define information security. Discuss the main security goals.

   (b) What are security attacks ? Explain its types with the help of examples.

3. Discuss various components of wireless networks. Also explain the security issues in wireless networks.

Unit II

4. Explain the RSA algorithm in detail, highlighting its key generation, encryption, and decryption processes.

5. (a) Discuss the secure architecture of an open system.

   (b) Define transposition cipher. Explain its techniques.

B-14353

Unit III

6. What is Secure Socket Layer (SSL) ? Explain the various protocols used in SSL.

7. What is S/MIME ? How does S/MIME work ? Discuss S/MIME encrypted email.

Unit IV

8. What is IPsec ? Discuss the role of IPsec (IP Security) in enhancing network security.

9. Discuss the following :
   (a) Malicious Programs
   (b) Worms
   (c) Malware.