2022

COMPUTER SCIENCE — GENERAL

Paper : SEC-B-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 ***question nos.*** **1** and **2** and ***any four*** questions from the rest.

1. Answer ***any ten*** questions : 2×10

(a) What is brute force attack?

(b) What is proxy firewall?

(c) Find the value of 3^(201) mod 11.

(d) Briefly define a group.

(e) What is data confidentiality?

(f) What are the different types of passive attack?

(g) What do you mean by cryptography?

(h) Write the main difference between block cipher and stream cipher.

(i) What is non-repudiation?

(j) What is message authentication?

(k) What is Secure Electronic Transaction (SET)?

(l) What is ring? Give an example.

(m) What is cipher?

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

(a) Message digest

(b) RSA algorithm

(c) Substitution technique

(d) Firewall

(e) Benefits of IPScc.

(f) Wireless network threats.

(g) Public key cryptography.

3. (a) Explain the Fermat's theorem with suitable example.
   (b) What is the purpose of P-box in DES? 5+5

4. (a) What is PGP with respect to E-mail security?
   (b) Briefly explain the symmetric encryption technique with its simplified model diagram. 5+5

5. (a) What are the roles of public and private key?
   (b) Briefly explain the key generation algorithm used in DES. 4+6

6. (a) What are the limitations of firewall?
   (b) Explain Secure Socket Layer. 4+6

7. (a) Explain Diffie Hellman Key Exchange with suitable example.
   (b) What is the purpose of HTTPS? 8+2

8. (a) Discuss the advantage of public key encryption.
   (b) Differentiate symmetric and asymmetric encryption with suitable examples. 4+6

9. (a) State Euler's theorem.
   (b) Solve 3^{302} mod 13 using Euler's theorem. 5+5
