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.

Group - A

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

(a) What are three independent dimensions in a Cryptographic system?

(b) What is Brute force attack?

(c) Write the main differences between block and stream cipher.

(d) Briefly define a ring.

(e) Find the value of 321 mod 11 using Fermat's theorem.

(f) What is the difference between diffusion and confusion?

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

(h) What is the OSl security architecture?

Group - B

Answer ***any four*** questions. 5×4

2. Draw a simplified model of Symmetric Encryption technique and explain it in brief.

3. Give example each for substitution and transposition ciphers.

4. Explain Fermat's theorem with suitable example.

5. What is the purpose of Digital Signature? How does it provide additional security?

6. What is the purpose of P-box in DES?

7. Write about the different principles of Security.

Group - C

Answer ***any five*** questions.

8. (a) Write a short note on different types of Wireless Network threats.

(b) What is PGP with respect to Electronic mail security? 5+5

9. (a) What is Anti-Replay Service? Why it is needed?

(b) Write the different benefits of IPSec. 4+6

10. (a) What is IP sniffing and IP spoofing?

(b) Explain Diffie-Hellman key exchange algorithm with example. 4+6

11. (a) Explain substitution technique with suitable example.

(b) What are the principles of Public-Key Cryptosystems? 5+5

12. (a) What is Message digest? Why is it used?

(b) What are the roles of the public and private key? 5+5

13. Write short notes on (***any two***) : 5×2

(a) Use of Public-Key Certificates

(b) Network Access Control (NAC)

(c) Transposition Techniques

(d) RSA Algorithm.