2023

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 is 'trojen'?

(b) What is Symmetric Key Cryptography?

(c) What is avalanche effect in DES?

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

(e) How 'denial of service' prevents the management of communication facilities?

(f) Find the value of 3 to the power (201) mod 11.

(g) What are the services provided by PGP?

(h) What is proxy firewall?

(i) What is the purpose of HTTPS?

(j) What is data confidentiality?

(k) What is brute force attack?

(l) What are the benefits of IPSec?

(m) What are the limitations of Firewall?

(n) What is S/MIME?

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

2. Answer ***any four*** questions : 5×4

(a) Why SHA is more secure than MD5? Explain.

(b) What is the purpose of digital signature? How does it provide additional security?

(c) How firewall is used to protect a private network?

(d) What do you mean by Cryptanalysis and Cryptography?

(e) Explain Secure Hash Algorithm (SHA).

(f) List and briefly define the SSH protocols.

(g) Draw and explain the IP security architecture.

3. (a) What characteristics are needed in a secure hash function?

(b) Why is SSL layer positioned between application layer and transport layer? 5+5

4. (a) Explain Diffie-Hellman Key Exchange Algorithm.

(b) Briefly explain the ESP packet format with diagram. 5+5

5. (a) State and prove Chinese Remainder theorem.

(b) Use Vigenere cipher with keyword 'HEALTH' to encipher the message "Life is full of surprises". 5+5

6. (a) Explain the Fermat's theorem with suitable example.

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

7. (a) State Euler's theorem.

(b) What are symmetric cipher and asymmetric cipher? 5+5

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

(a) MAC

(b) Kerbcros

(c) Transposition cipher

(d) Message digest

(e) SSL attacks.