

**2021**

**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.*

**Group - A**

1. Answer *any five* questions : 2×5
- (a) What is watermarking?
  - (b) What is proxy firewall?
  - (c) Find the value of  $3^{201} \bmod 11$ .
  - (d) List out the services provided by PGP.
  - (e) Find the value of  $3^{21} \bmod 11$  using Fermat's theorem.
  - (f) What is steganography?
  - (g) What is logic bomb?
  - (h) What is 'worm'?

**Group - B**

Answer *any four* questions. 5×4

- 2. What are the differences between block cipher and stream cipher?
- 3. Give example each for substitution and transposition ciphers.
- 4. Explain Elgamal crypto system.
- 5. Explain why SHA is more secure than MD5?
- 6. What is the purpose of X-boxes in DES?
- 7. Explain Kerberos.

**Please Turn Over**

**Group - C**

Answer *any five* questions.

8. (a) Discuss the various steps used in verification of digital certificate.  
(b) What do you mean by cryptanalysis and cryptography? 5+5
9. (a) Explain Diffie–Hellman key exchange algorithm.  
(b) What are symmetric cipher and asymmetric cipher? 5+5
10. (a) What is IP sniffing and IP spoofing?  
(b) What are the four main stages in AES operation? 5+5
11. (a) What are the limitations of firewall?  
(b) What is Brute-force-attack? Explain. 5+5
12. (a) What are the features of ITAA?  
(b) State and prove Fermat's little theorem. 5+5
13. Write short notes on (*any two*) : 5×2
- (a) S/MIME
  - (b) Firewall
  - (c) Digital Signature
  - (d) Secure Hash Algorithm (SHA)
-