65623

Sixth Semester B.C.A. Degree Examination, September/October 2021

(CBCS Scheme)

Computer Science

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours] *[Max. Marks : 100*

Instructions to Candidates : Answer all Sections.

SECTION – A

I. Answer any **TEN** questions. Each question carries **2** marks : **(10 × 2 = 20)**

1. What are the basic properties of divisibility?
2. Define cipher text with example.
3. What is Brute force attack?
4. Write any two applications of RSA algorithm.
5. What is Trap door one way function?
6. What is Kerberos?
7. What is PGP?
8. Define Session State.
9. Define Digital Signature.
10. What is IKE?
11. What is ESP protocol?
12. What is Whirlpool cipher?

SECTION – B

Answer any **FIVE** questions. Each carries **5** marks : **(5 × 5 = 25)**

13. Explain symmetric key encryption model with a neat diagram.
14. Discuss the classification of security goals.

15. Explain Euclid's algorithm with example.

16. Explain Fermat's little theorem.

17. Explain digital signature process with a neat diagram.

18. Explain CBC mode of operation.

19. Compare SSL and TLS protocols.

20. Explain the importance of Cryptography.

SECTION – C

Answer any **THREE** questions. Each question carries **15** marks : **(3 × 15 = 45)**

21. (a) Explain key elements of public key encryption. **(8)**

    (b) Differentiate equality and congruence with examples. **(7)**

22. (a) Explain steps in DES algorithm. **(8)**

    (b) Discuss any two modes of operations in DES. **(7)**

23. (a) Explain the rules of play fair cipher with an example. **(8)**

    (b) Differentiate between symmetric and asymmetric key cryptography. **(7)**

24. (a) Write a note on Kerberos. **(8)**

    (b) Write a note on PGP services. **(7)**

25. (a) Explain Diffie-Helman key exchange technique with an example. **(8)**

    (b) Explain SSL Handshake protocol action. **(7)**

SECTION – D

Answer any **ONE** question. It carries **10** marks : **(1 × 10 = 10)**

26. Explain SHA-512 algorithm with a neat diagram. **(10)**

27. Explain RSA cryptosystem. **(10)**

———————