15623

Reg. No. | | | | | | | | |

VI Semester BCA Degree Examination, September/October - 2022

COMPUTER SCIENCE

Cryptography and Network Security

(CBCS Scheme)

Time : 3 Hours

Maximum Marks : 100

Instructions to Candidates :

Answer All Sections.

SECTION - A

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

1. What is Stegnography?
2. Differentiate between active and passive attack.
3. Mention two security goals.
4. What is Shift Cipher?
5. Write any two differences between Block Cipher and Stream Cipher.
6. What is expansion D box?
7. Define residue class.
8. What is one way function in Knapsack Cryptosystem?
9. Define Kerberos.
10. What is cryptographic hash function?
11. Define digital signature.
12. What is S/MIME?

[P.T.O.

SECTION- B

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

13. Explain the various security mechanisms.
14. Explain extended Euclidean algorithm with example.
15. Explain encryption and decryption.
16. Write general design of DES.
17. Explain two types of attacks to Elgamal Cryptosystem.
18. Write a note on X.509 Certificate.
19. Explain various phases of Handshaking process in SSL?
20. Briefly explain the architecture of SSL.

SECTION- C

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

21. a) Explain asymmetric key model with a neat diagram. (10)
    b) What is divisibility? List four properties of divisibility. (5)
22. a) Explain Triple DES algorithm with a neat diagram. (10)
    b) Compare AES and DES. (5)
23. a) State and explain Chinese reminder theorem. (8)
    b) Explain different attacks in RSA. (7)
24. a) What is Hijacking? Explain. (6)
    b) Explain Diffie-Hellman Key Agreement. (9)
25. a) Explain SSL Protocol stack. (8)
    b) Differentiate between Tunnel mode and Transport mode. (7)

SECTION- D

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

26. Explain different cryptographic attacks.
27. Explain Internet exchange key.
