25173

Reg. No.

VI Semester B.Voc. (IT) Degree Examination, September - 2021
INFORMATION TECHNOLOGY
Cryptography and Network Security
(CBCS Scheme)

Time : 3 Hours   **Maximum Marks : 70**

Instructions to Candidates:

Answer all sections.

SECTION - A

Answer any **TEN** questions.   (10×2=20)

1. State Network Security Goals.

2. Write the primary functions of cryptography.

3. What is one time pad?

4. What are the variants of Vigenere cipher?

5. What is Co-prime? Give example.

6. What is Modular Arithmetic?

7. Define Caesar cipher.

8. Define composite number. Give example.

9. Write the usage of change cipher spec protocol.

10. Draw the IPV6 ESP datagram Format in Transport mode.

11. Define ISAKM.

12. Define steganography

SECTION - B

Answer any **FIVE** questions.   (5×10=50)

13. Explain the working principle of DES Algorithm with example.   **(10)**

14. Explain Elliptic curve cryptosystem with example?   **(10)**

15. Explain Digital signatures in detail.   **(10)**

16. a. Explain PGP in detail.   (5)

     b. Explain IPsec protocols.   (5)

17. a. Write a note on security Attacks.   (5)

     b. Discuss on security Engineering.   (5)

18. a. Explain Rabin cryptosystem.   (5)

     b. Explain SHA - 512   (5)

19. a. Write a note on information security services.   (5)

     b. Describe security Association.   (5)

20. a. Write a note on key management.   (5)

     b. Explain Transpositional Cipher.   (5)

_____