K24U 2876

Reg. No. : .....

Name : .....

V Semester B.C.A. Degree (CBCSS – OBE – Regular/ Supplementary/ Improvement) Examination, November 2024
(2019 to 2022 Admissions)
Core Course
5B16BCA-E01 : INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

PART – A
Short Answer

Answer **all** questions : (6×1=6)

1. What is confidentiality in information security ?
2. Define cryptography.
3. Name two types of passive attacks.
4. What is meant by transposition cipher ?
5. Define the term non-repudiation.
6. What is steganography ?

PART – B
Short Essay

Answer **any 6** questions : (6×2=12)

7. Explain the principle of integrity in information security.
8. What is the purpose of the avalanche effect in cryptographic algorithms ?
9. Differentiate between a block cipher and a stream cipher.
10. Describe the concept of public-key cryptosystem.
11. What are the security services provided by a digital signature ?
12. What is a brute-force attack and why is it a threat to cryptography ?
13. Explain the role of key management in cryptographic systems.
14. How does DES provide confidentiality ?

P.T.O.

PART – C
Essay

Answer **any 4** questions : **(4×3=12)**

15 Apply the RSA algorithm to encrypt a message using a public key.

16. Analyze the weaknesses in DES and how they are addressed by Triple DES.

17. Differentiate between active and passive attacks with examples .

18. How does Kirchhoff's principle influence modern cryptography ?

19. Explain how a digital certificate works in securing communication.

20. Compare and contrast monoalphabetic and polyalphabetic substitution ciphers.

PART – D
Long Essay

Answer **any 2** questions : **(2×5=10)**

21. Compare symmetric key cryptography with asymmetric key cryptography, focusing on their strengths and limitations.

22. Evaluate the RSA digital signature scheme and explain its security benefits.

23. Discuss the various types of cryptanalysis techniques used to break cryptographic systems.

24. Explain the concept of digital signatures. How do they ensure integrity, authentication and non-repudiation in digital communication ?