TB205700V **Reg. No :.....**

Name :.....

BCA DEGREE (C.B.C.S.) EXAMINATION, NOVEMBER 2022

2020 ADMISSIONS REGULAR AND 2019, 2018 ADMISSIONS SUPPLEMENTARY

SEMESTER V - CORE COURSE (CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)

BCA5B18B18 - CRYPTOGRAPHY FUNDAMENTALS

Time : 3 Hours **Maximum Marks : 80**

Part A

I. Answer any Ten questions. Each question carries 2 marks **(10x2=20)**

1. Define key and keyspace.
2. Find the gcd (816,2260).
3. “Passive attacks are very difficult to detect”. Explain.
4. Define Transposition cipher.
5. Write the security features of HMAC over SHA-1.
6. How is Initial permutation performed on DES algorithm?
7. Write the important aspects of key management.
8. Why key management is important in Cryptography?
9. What are the drawbacks of Kerberos?Explain.
10. What are the benefits of the Payment gateway?
11. Explain briefly about the vulnerabilities affected in a cryptographic system.
12. Explain the generic model of network security.

Part B

II. Answer any Six questions. Each question carries 5 marks **(6x5=30)**

13. Find the inverse of 5 mod 133.
14. Explain the hashed message authentication in cryptographic system.
15. Write the algorithm of ECC encryption and decryption.
16. Explain the procedures involved in verifying the certificate.
17. Write a short note on management of keys.
18. How to build an IPsec security association in ISAKMP?
19. How MIME differ from S/MIME? Explain the benefits of S/MIME certificates.
20. Differentiate between Virus and threats.
21. Explain Intruders and their functions.

Part C

III. Answer any Two questions. Each question carries 15 marks **(2x15=30)**

22. Write the Procedures of MD5 Algorithms and How is it differ from HMAC Algorithm. Explain with the help of figures.
23. Discuss the Key hierarchy and its key functions in cryptography.
24. Draw the format of X.509 certificate and X.509 revoked certificate. Explain its fields.
25. Explain the process involved in vulnerability analysis in Cryptographic functions.