QP CODE: 25020288

25020288

Reg No : .....

Name : .....

B.Sc DEGREE (CBCS)) REGULAR/ IMPROVEMENT/ REAPPEARANCE / MERCY CHANCE EXAMINATIONS, FEBRUARY 2025

Fourth Semester

B.Sc Cyber Forensic Model III

Core Course - CF4CRT12 - APPLIED CRYPTOGRAPHY

2017 Admission Onwards

B4CACAF1

Time: 3 Hours Max. Marks : 80

Part A

*Answer any **ten** questions.*

*Each question carries **2** marks.*

1. What is the main difference between passive and active cheaters?
2. Give an alternate name for ‘data authentication code’. Define it.
3. What is called (m,n)-threshold scheme?.
4. What are the different duties of an arbitrator?
5. Who is a trent?
6. Define secure multiparty protocol.
7. What do you mean by privacy in case of digital cash transaction?
8. What is called traffic flow security?
9. DES stands for_____.Draw it's structure..
10. How many S-boxes are present in the blowfish algorithm? Explain its usage.
11. What is private key? Write its usage?
12. What are the few major applications of cryptography in the modern world?

(10×2=20)

Part B

*Answer any **six** questions.*

*Each question carries **5** marks.*

13. Briefly explain different attack against cryptographic protocols.

14. Explain different characteristics of a digital signature.

15. Write short note on SKEY.

16. List out the various steps involved in Yahalom protocol.

17. What are the properties of completely blind signatures?

18. List some problems of voting with blind signatures.

19. List out the differences between asymmetric and symmetric keys.

20. Explain the security of MD5.

21. Given the values ,prime numbers (p=13,q=31),private key (d=7).Calculate public key ‘e’ using RSA approach.

(6×5=30)

Part C

*Answer any **two** questions.*

*Each question carries **15** marks.*

22. How Alice can send a message to Bob using asymmetric key cryptography?

23. Explain key exchanging with public-key cryptography.

24. Explain hardware encryption versus software encryption.

25. Explain with an appropriate algorithm ,how we can securely exchange keys between two parties?

(2×15=30)