

QP CODE: 21100315



Reg No :

Name :

BSc DEGREE (CBCS) EXAMINATION, FEBRUARY 2021

Fifth Semester

B.Sc Computer Science Model III

Core Course - CC5CRT05 - COMPUTER SECURITY

2017 Admission Onwards

C4558AAF

Time: 3 Hours

Max. Marks : 80

Part A

*Answer any **ten** questions.*

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

1. Which are the approaches to Information Security implementation?
2. What is the difference between spoofing and sniffing?
3. What are the three factors that make Caesar cipher vulnerable to cryptanalytic attacks?
4. What are the two principal methods used in substitution ciphers to avoid elements of plain text in cipher text?
5. What is the main drawback of Playfair cipher?
6. Define alarm clustering and compaction?
7. Explain how IDPS helps in intrusion detection?
8. Define PGP.
9. What is IPsec?
10. List any four threats which compromise the confidentiality on the web.
11. Name the four protocols used on top of SSL.
12. List any four key features of SET.

(10×2=20)

Part B

*Answer any **six** questions.*

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

13. Explain deliberate software attacks.
14. With suitable block diagram, explain a symmetric cipher model.





15. Explain asymmetric encryption with private key and express mathematically the relationship between plain text and cipher text?
16. What are the main components in PKI? Explain its functioning.
17. List the advantages of HIDPS?
18. Discuss the importance of SPD and SAD in IPsec architecture.
19. Compare AH and ESP.
20. Write short notes on Packet Filtering Routers.
21. Write short notes on Application Level gateway.

(6×5=30)

Part C

*Answer any **two** questions.*

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

22. With suitable examples, explain substitution and transposition ciphers?
23. Explain different password selection strategies?
24. Define S/MIME and discuss the services provided by S/MIME.
25. Explain about firewalls and its types in detail.

(2×15=30)

