776 Register No.:

October 2018

Time – Three hours
(Maximum Marks: 75)

[N.B: (1) Q.No. 8 in PART – A and Q.No. 16 in PART – B are compulsory. Answer any FOUR questions from the remaining in each PART – A and PART – B

(2) Answer division (a) or division (b) of each question in PART – C.

(3) Each question carries 2 marks in PART – A, 3 marks in Part – B and 10 marks in PART – C.]

PART – A

1. What is security?
2. Define integrity of information.
3. List out any three categories of threat.
4. What is spoofing?
5. Define mitigation in risk management.
6. What is hybrid VPN?
7. What is cipher text?
8. List out any three physical security controls.

PART – B

9. List out the components of an information system.
10. What is confidentiality?
11. Give expansion: (i)PIN (ii)UPS (iii)TCP.
12. Define brute force attack.
13. List out the risk control strategies.
14. Define cost benefit analysis.
15. What is encryption?
16. Define virus.

[Turn over.....

PART – C

17. (a) Explain in detail about SDLC with a neat sketch.

(Or)

(b) Explain any three critical characteristics of information.

18. (a) Define attack and explain any four types of attacks.

(Or)

(b) Explain in detail about any three software development security problems.

19. (a) Explain in detail about risk assessment.

(Or)

(b) Explain cost benefit analysis in detail.

20. (a) Explain any two firewall architectures in detail.

(Or)

(b) Explain: (i)Substitution cipher (ii)transposition cipher (iii)Vernam cipher.

21. (a) Explain any three physical security controls in detail.

(Or)

(b) Explain in detail about heating, ventilation and air conditioning.
