Roll No. | | | | | | | | | | |

B.E / B.Tech (FT) END SEMESTER EXAMINATIONS – APRIL / MAY 2019

INFORMATION TECHNOLOGY

Semester VII

IT8702 & Information Security

(Regulation 2012)

Time: 3 Hours | Answer ALL Questions | Max. Marks 100

PART-A (10 x 2 = 20 Marks)

1. What do you understand by Risk, Vulnerability & Threat in a network?
2. Define viruses, worms and logic bombs.
3. What are the two basic functions used in encryption algorithms?
4. Differentiate between symmetric and asymmetric encryption.
5. What is the purpose of X.509 standard?
6. What are the services provided by PGP services?
7. What are the deliverables of risk assessment?
8. What are the key elements of a disaster recovery plan?
9. What are the principles of secure programming? What is OWASP?
10. What is a canonical data model? What are the benefits and downsides of it?

Part – B (5 x 16 = 80 marks)
(Question No.11 is Compulsory)

11. i) Explain the need and principles of security. (10)
ii) What is access control? How does Bell-Lapadula model achieve access control? Brief over it. (6)

12. a) i) Explain about AES in detail. (10)

a) ii) Perform encryption and decryption using RSA algorithm for the following. (6)
P=17; q=11; e=7; M=88.

(OR)

12. b) i) Explain the steps followed in creating digital signature. (10)

b) ii) User A & B exchange the key using Diffie Hellman algorithm. (6)
Assume á=5 q=11 X_A=2 X_B=3. Find Y_A, Y_B, K.

13. a) i) Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved? Explain. (10)

a) ii) Describe about SSL/TLS Protocol. (6)

(OR)

13. b) i) Explain the architecture of IP Security. (10)

b) ii) What are the steps involved in SET transaction? (6)

14. a) i) What is vulnerability? Explain the techniques for detecting vulnerabilities, NRL taxonomy and Aslam's model. (16)

(OR)

14. b) i) Define intrusion detection and the different types of detection mechanisms, in detail. (10)

b) ii) Briefly describe about the components in the anatomy of an auditing system. (6)

15. a) Briefly describe about, (16)

- Buffer overflow attack
- Cross site scripting and how can it be prevented
- Incomplete mediation
- Command injection attack

(OR)

15. b) Explain the phases in Secured SDLC model. Compare and contrast with SDLC. (16)