F 6668

Reg. No....................................

Name....................................

B.TECH. DEGREE EXAMINATION, NOVEMBER 2017

Eighth Semester

Information Technology

CS 010 802—CRYPTOGRAPHY AND NETWORK SECURITY (IT)

(New Scheme—2010 Admission onwards)

[Supplementary]

Time : Three Hours

Maximum : 100 Marks

Part A

Answer all questions.
Each question carries 3 marks.

1. What is the difference between integer and modular arithmetic ?

2. What are stream ciphers ?

3. What is a 'key' in cryptography ?

4. What is lP security ?

5. What are trusted systems ?

(3 × 5 = 15 marks)

Part B

Answer all questions.
Each question carries 5 marks.

6. Define congruence and compare it with equality.

7. Explain symmetric cipher model.

8. What is the purpose of using two prime numbers in RSA ?

9. What are the three types of messages defined in PGP ? Explain the purpose of using it.

10. Explain various counter measures for virus attacks ?

(5 × 5 = 25 marks)

Turn over

Part C

*Answer **all** questions.*

Each question carries 12 marks.

11. Write the multiplication and addition table for Z_9.

Or

12. Define determinants. With an example, calculate determinant of 2×2 and 3×3 matrix.

13. Explain the encryption process of AES algorithm.

Or

14. What are the drawbacks of DES ? Explain how triple DES overcomes the same.

15. Explain Hashed MAC function. Compare it with CMAC.

Or

16. With the help of flow chart/ block diagram explain RSA digital signature scheme.

17. Explain key distribution process using controlled trusted centre.

Or

18. Define kerberos and name its servers. Briefly explain the duties of each server.

19. How to detect and overcome from DDoS attacks ? Explain.

Or

20. Write a note on :

    (a) Firewall design.

    (b) Intrusion detection.

(5 × 12 = 60 marks)

F 6703 (Pages : 2) Reg. No...............................

Name.....................................

B.TECH. DEGREE EXAMINATION, NOVEMBER 2017

Eighth Semester

Branch : Information Technology

IT 010 804 L01—SOFTWARE TESTING (Elective III) (I.T.)

(New Scheme—2010 Admission onwards)

[Supplementary]

Time : Three Hours   Maximum : 100 Marks

Part A

Answer all questions.
Each question carries 3 marks.

1. Why software testing is essential ?

2. What is kick-off audit ?

3. Define alpha testing.

4. What is software quality ?

5. List the information a meaningful test report must contain.

(5 × 3 = 15 marks)

Part B

Answer all questions.
Each question carries 5 marks.

6. Explain mutation testing with an example.

7. Discuss the root causes of defects.

8. Why acceptance testing is done? What are the characteristics of acceptance testing ?

9. How boundary value analysis can be used for selection of test data? Give example.

10. Explain process metrics with examples.

(5 × 5 = 25 marks)

Turn over

Part C

Answer **all** *questions.*
Each question carries 12 marks.

11. (a) List the basic principles of software testing.

(4 marks)

(b) List and explain the important features of the software testing process.

(8 marks)

Or

12. What is configuration management ? Explain the configuration management process.

13. Explain with diagrammatic illustration V model (validation model) for testing.

Or

14. What is a defect ? Classify defects and discuss the same.

15. Explain with diagrammatic illustration the software testing stages. Clearly explain the need and importance of each stage.

Or

16. What is an acceptance plan ? Present the template for acceptance plan and discuss the same.

17. What is a test case ? What are the characteristics of a good test case ? How to write a good test case ? Discuss.

Or

18. What are test scripts ? What information test scripts must contain ? What activities are involved in execution of test scripts ? Discuss.

19. What is benchmarking ? List and explain the benchmarking process steps.

Or

20. (a) What is brainstorming ? Explain the guidelines for conducting successful brainstorming.

(6 marks)

(b) What is a Pareto chart ? Discuss with an example.

(6 marks)

[5 × 12 = 60 marks]

B.TECH. DEGREE EXAMINATION, NOVEMBER 2017

Eighth Semester

Branch : Information Technology

IT 010 805 G04—ELECTRONIC BUSINESS AND SERVICES (Elective IV) (I.T.)

(New Scheme—2010 Admission onwards)

[Supplementary]

Time : Three Hours   Maximum : 100 Marks

Part A

Answer all *questions.*
Each question carries 3 marks.

1. Define Symmetric Data Encryption and Asymmetric Data Encryption.

2. What are the main requirements of EFT systems ?

3. List the different kinds of card related faults.

4. What is public key certification ? Explain.

5. What are the main principles of Cryptography ?

(5 × 3 = 15 marks)

Part B

Answer all *questions.*
Each question carries 5 marks.

6. Describe the four models of E-commerce, with an example each.

7. Write a note on the E-commerce layered architecture.

8. Explain the working of the f(R,K) function in DES.

9. Explain the concepts of Mobile banking and the challenges involved in implementing such systems.

10. Discuss the need for Triple DES.

(5 × 5 = 25 marks)

Part C

Answer all questions.
Each question carries 12 marks.

11. What is Public Key Cryptography ? Discuss the main problems that it tries to solve and any one method of achieving this objective.

Or

12. Describe the objectives of the IT Act of 2000. Explain in detail the shortcomings of this Act, and how they have been remedied.

13. What types of computational intelligence techniques are available for CCFD ? Explain any one in detail.

Or

14. Discuss the main concepts of the Dempster-Shafer theory in details.

15. Discuss in detail Electronic Cash Payment Systems. Explain the main components and their role, with a neat diagram.

Or

16. Discuss in detail Electronic Cheque Payment Systems. Explain the main components and their role, with a neat diagram.

17. Explain in detail, the AES algorithm, with a detailed example

Or

18. What are Digital Signatures ? Why are they needed and how are they used in a real-world scenario. Explain in detail.

19. Write a note on EDI standards. What is their purpose and how are they implemented ?

Or

20. Write a note on Bayesian Inferencing for CCFD.

(5 × 12 = 60 marks)