Reg. No. :

Question Paper Code: 37204

B.E. / B.Tech. DEGREE EXAMINATION, APRIL 2019

Seventh Semester

Computer Science and Engineering

01UCS704 - FUNDAMENTALS OF INFORMATION SECURITY

(Regulation 2013)

Duration: Three hours   Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1. What is access control matrix?

2. List the different security policies and types of access control.

3. Explain how the avalanche effect is achieved in DES.

4. Define ECC.

5. What are the requirements for message authentication?

6. Distinguish between directed and arbitrated digital signature.

7. What are computer viruses? What are the types of viruses?

8. How auditing is different from logging? Write the Syntactic issue related to auditing?

9. List out the components of user policies.

10. Define goal of Drib's security policies.

PART - B (5 x 16 = 80 Marks)

11. (a) (i) Explain in detail about access control matrix with examples.   (10)

    (ii) Discuss about clinical information systems security policy.   (6)

Or

(b) Describe the different types of security policies.   (16)

12. (a) (i) Explain single round of DES algorithm.   (8)

    (ii) Explain advance encryption standard.   (8)

Or

(b) Explain about Diffie Hellman key exchange algorithm with suitable example.   (16)

13. (a) Illustrate in detail MD5 algorithm.   (16)

Or

(b) (i) Write short notes on DSS.   (8)

    (ii) Explain digital signature with ElGamal public key cryptosystem.   (8)

14. (a) Explain about penetration analysis in detail with any two examples.   (16)

Or

(b) What is IDS? Explain in detail about various intrusion detection systems.   (16)

15. (a) Explain about system security in detail.   (16)

Or

(b) Discuss about requirements, design refinement and implementation in program security?   (16)

37204