Reg. No. : | | | | | | | | | | |

Question Paper Code: A31724

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2016

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 a threat? List out the four broad classes of threats?
2. What is Chinese wall model?
3. What is public key certificate?
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) What is access control matrix? Explain about protection and state transition in access control. (8)

(ii) Explain about Bell-Lapadula model in detail. (8)

Or

(b) (i) Explain about biba integrity model. (8)

(ii) Write notes on lipner's integrity matrix model. (8)

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) (i) What are the properties of hashing function in cryptography. (8)

(ii) Explain secure hashing algorithm. (8)

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) Write short notes on (i) Anomaly modeling and (ii) Misuse modeling. (16)

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

Or

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

———————