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

Question Paper Code: 37024

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2017

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. List the different security policies and types of access control.
2. What is Chinese wall model?
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 is the difference between vulnerability and exposure?
8. What are computer viruses? What are the types of viruses?
9. List out the components of user policies.
10. What are the components of user's security policies?

PART - B (5 x 16 = 80 Marks)

11. (a) What is access control matrix? Explain about protection and state transition in access control. (16)

Or

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

12. (a) Explain single round of DES algorithm. (16)

Or

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

13. (a) Explain secure hashing algorithm. (16)

Or

(b) Describe hash functions and MAC. (16)

14. (a) Explain the different approaches to intrusion detection. (16)

Or

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

15. (a) Explain the use of cryptographic and network security techniques for an online shopping application. (16)

Or

(b) Explain about system security in detail. (16)

———————