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

Question Paper Code: 31274

B.E. / B.Tech. DEGREE EXAMINATION, MAY 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. What is access control matrix?
2. Define Security policy.
3. Explain how the avalanche effect is achieved in DES.
4. How many keys are used in triple encryption?
5. List the requirements of MAC functions.
6. Distinguish between directed and arbitrated digital signature.
7. What is the difference between vulnerability and exposure?
8. List and briefly define three classes of intruders.
9. Can routers and bridges be used as firewalls? How?
10. What are the components of user'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) (i) Describe the different types of security policies. (8)

(ii) Write the goals of security. (8)

12. (a) (i) How AES is used for encryption/decryption? Explain with example. (8)

(ii) Discuss in detail about CBC and OFB mode of DES operations. (8)

Or

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

13. (a) (i) Explain the MD5 message digest algorithm by giving suitable diagrams for message digest generation and message processing of 512 bit block and MD5operation. (10)

(ii) Discuss about the process of signature verification in DSS. (6)

Or

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

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

Or

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

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

Or

(b) Briefly explain the common security-related programming problems. (16)

———————