Reg. No. : □□□□□□□□□□

Question Paper Code: 37204

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2018

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. 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. What are computer viruses? What are the types of viruses?
9. Can routers and bridges be used as firewalls? How?
10. Define application gateway.

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

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) Explain secure hashing algorithm. (16)

Or

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

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

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