Reg. No. :

Question Paper Code: 37204

B.E. / B.Tech. DEGREE EXAMINATION, NOV 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 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 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) (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) 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 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)