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

Question Paper Code: 37204

B.E. / B.Tech. DEGREE EXAMINATION, DEC 2020

Seventh Semester

Computer Science and Engineering

01UCS704 - FUNDAMENTALS OF INFORMATION SECURITY

(Regulation 2013)

Duration: One hour Maximum: 30 Marks

PART A - (6 x 1 = 6 Marks)

(Answer any six of the following questions)

1. Which of the following principle ensure that the sender of a message cannot claim that the message was never sent?

   (a) Access Control (c) Availability

   (b) Authentication (d) Non-Repudiation

2. A _____ is anything that can cause harm.

   (a) Vulnerability (b) Phish (c) Threat (d) Spoof

3. The DES algorithm has a key length of

   (a) 128 bits (b) 32 bits (c) 64 bits (d) 16 bits

4. Which one of the algorithm is not used in asymmetric-key cryptography?

   (a) RSA (b) Diffie-Hellman (c) Electronic code book (d) None of the above

5. Another name for Message Authentication Code

   (a) Cryptographic codebreak (b) Cryptographic codesum

   (c) Cryptographic checksum (d) Cryptographic checkbreak

6. SHA-1 has a message digest of

(a) 160 bits (b) 512 bits (c) 628 bits (d) 820bits

7. Which of the following is independent malicious program that need not any host program?

(a) Trap door (b) Trojan Horse (c) Virus (d) Worm

8. Which method uses the assumption that unexpected behavior is evidence of an intrusion?

(a) Rule based (b) Anomaly Detection (c) Attack tool (d) None

9. ____ is a portion of network that separates a purely internal network from an external network.

(a) Firewall (b) DMZ (c) Proxy (d) DNS

10. A firewall needs to be _____ so that it can grow with the network it protects.

(a) Robust (b) Expensive (c) Fast (d) Scalable

PART – B (3 x 8= 24 Marks)

(Answer any three of the following questions)

11. What is access control matrix? Explain about protection and state transition in access control. (8)

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

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

14. Explain about penetration analysis in detail with any two examples. (8)

15. Explain the use of cryptographic and network security techniques for an online shopping application. (8)