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

Question Paper Code: 47204

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2019

Seventh Semester

Computer Science and Engineering

14UCS704 - FUNDAMENTALS OF INFORMATION SECURITY

(Regulation 2014)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 1 = 10 Marks)

1. Which of the following principle ensure that the sender of a message cannot claim that the message was never sent?
   (a) Access Control (b) Authentication
   (c) Availability (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. What kind of ciphers Electronic Codebook (ECB) mode and Cipher Block Chaining (CBC) mode are?
   (a) Block Cipher (b) Stream Cipher (c) Field Cipher (d) Both (A) and (B)
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. ---------- is the process that defines, identifies and classifies the security holes in a computer, network or communications infrastructure.

(a) Vulnerability Analysis (b) Network Analyzer

(c) Packet Tracer (d) Cryptanalysis

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. IPsec in _____ mode does not protect the IP header,it only protects the information coming from the transport layer.

(a) Tunnel mode (b) Transport mode (c)Network mode (d) Data mode

PART - B (5 x 2 = 10 Marks)

11. What is meant by Threat? Explain its types..

12. Write down the purpose of S-Boxes in DES

13. Differentiate Hash and MAC function.

14. List the steps in Flaw Hypothesis Methodology

15. Define devnet.

PART - C (5 x 16 = 80 Marks)

16. (a) Discuss in detail about Access Control Matrix with illustrative example (16)

Or

(b) Explain the concept of Security Policies with reference to any existing security model. (16)

17. (a) Discuss in detail various block cipher modes of operation (16)

Or

(b) (i) Explain RSA Algorithm to perform encryption and decryption to the system with p = 7, q = 11, e = 17, M = 8. (8)

(ii) Describe RC5 algorithm with neat diagram. (8)

18. (a) Describe HMAC algorithm in detail with an example. (16)

Or

(b) (i) Briefly explain about Digital Signature Algorithm. (8)

(ii) Explain Schnorr digital signature schemes. (8)

19. (a) Elaborate the concept of Vulnerability Analysis with an example (16)

Or

(b) Explain in detail about Intrusion Detection System with its types (16)

20. (a) Discuss about User Security concerns with suitable example. (16)

Or

(b) Discuss about Network and System Security. (16)

———————