Reg. No. : □□□□□□□□□□

Question Paper Code: 47204

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

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 (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 (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) (i) Explain in detail about Lipner’s Integrity Matrix Model. (8)

(ii) What is a Security Policy? Explain the types of Security Policies. (8)

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) Explain MD5 Algorithm and compare its performance with SHA- I . (16)

Or

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

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

19. (a) Summarize the different types of Computer Viruses. (16)

Or

(b) (i) Draw the architecture of Intrusion detection system and explain its types. (8)

(ii) Explain State-Based auditing and Transition-Based Auditing? (8)

20. (a) (i) Pointout the ways the user can protect access to their accounts. (8)

(ii) Explain the requirements and policy of Program Security (8)

Or

(b) Write about Program Security aspects in detail with example. (16)