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

Question Paper Code: 49214

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

Elective

Computer Science and Engineering

14UCS914 – CYBER FORENSICS

(Regulation 2014)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 1 = 10 Marks)

1. Name the parameter that uniquely identifies the Security Association:

   (a) IP Source Address (b) IP Destination Address

   (c) Initialization Vector (d) Session Identifier

2. State the purpose of alert message:

   (a) Identify input labels (b) Key generation

   (c) Connection termination (d) Information exchange

3. What is S/MIME?

   (a) Secure/Multipurpose Internet Mail Extension

   (b) Secure/Multipurpose Internet Mail Exchange

   (c) Secure/ Multipurpose Internet Mail Encryption

   (d) Secret/Multipurpose Internet Mail Extension

4. State which of the following is the attribute certificate with respect to PKIX:

   (a) X.509 AC (b) X.502 AC (c) X.508 AC (d) X.507 AC

5. To be considered a computer crime, what needs to be involved in the crime?

   (a) Technology (b) Computers

   (c) Data (d) Networks

6. Identify the password recovery methods

(a) Rainbow Attack (b) Script kiddies

(c) Cyberpunks (d) Hackers

7. State which of these is an open source encryption encryption tool:

(a) DPMI (b) Cross crypt (c) EFS (d) ZBR

8. Which of the following would be a method of recording the crime scene?

(a) Note-taking

(b) Sketching the crime scene

(c) Both A and B

(d) Having a witness describe the scene to a crime scene investigator

9. State the use of bit shifting

(a) Hiding data (b) Digital Watermarking

(c) Track Network (d) Examining Tool

10. What piece of legislation makes it a crime to send e-mail using false headers?

(a) CAN-SPAM Act (b) CFAA

(c) FERPA (d) USA PATRIOT Act

PART - B (5 x 2 = 10 Marks)

11. Distinguish between HMAC and MAC.

12. List the algorithms used in PGP 5.X

13. How will you specify the rules for computer Forensics in investigation ?

14. Point out the tools used in validation and discrimination in Forensics.

15. Define Network Forensics.

PART - C (5 x 16 = 80 Marks)

16. (a) Describe TLS Protocol with suitable example. (16)

Or

(b) Discuss about Key Management Protocol for IPSec. (16)

17. (a) Describe the transaction protocols required for secure Payment Processing in SET (16)

Or

(b) Demonstrate the SET system Participants with a diagram. (16)

18. (a) Examine the traditional Computer crimes associated with CyberForensics (16)

.

Or

(b) Examine in detail the roles of the following in detail:-

(i) Forensics Technology. (8)

(ii) Forensics Systems. (8)

19. (a) Illustrate how will the processing of an incident or a crime scene takes place in cyberforensics. (16)

Or

(b) Explain in detail about the following:-

(i) Computer Forensics Software Tools. (8)

(ii) Computer Forensics Hardware Tools. (8)

20. (a) Describe in detail about using specialized E-mail Forensics Tools. (16)

Or

(b) Give a brief description of the following data-hiding techniques: (16)

(i) Hiding Partitions

(ii) Bit-Shifting