|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |

 **Reg. No. :**

**Question Paper Code: 49024**

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2017

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. Identify the objective of computer forensics

 (a) Recover evidence (b) Analyze evidence

 (c) Present evidence (d) All the above

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. Encrypting File Systems are used to encrypt

 (a) Files (b) Folders (c) Disk volumes (d) All of the above

9. State the use of bit shifting

 (a) Hiding data(b) Digital Watermarking

 (c) Track Network (d) Examining Tool

10. What is the use of DiD?

 (a) Data registry (b) Traffic Monitoring

 (c) File processing (d) None of the above

PART - B (5 x 2 = 10 Marks)

11. Mention the two main transformation types that form the basis of IPsec.

12. List out the data fields contained in ASCII Armor Format.

13. Who can use Computer Forensic Evidence? .

14. Define Recovery Certificate.

15. What is meant by Data Hiding?

PART - C (5 x 16 = 80 Marks)

16. (a) (i) Explain in detail about IPSec Protocol Documents. (6)

 (ii) Explain in detail about HMAC with its structure and suitable example. (10)

Or

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

17. (a) Briefly explain the types of Firewalls with a neat diagram and examples. (16)

Or

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

18. (a) Explain in detail about Incident Response Methodology and the six steps associated

 with it. (16)

 Or

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

 (i) Forensics Technology. (8)

 (ii) Forensics Systems. (8)

19. (a) Describe about the following mechanisms:

 (i) Understanding File Systems. (6)

 (ii) Whole Disk Encryption. (10)

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:

 (i) Hiding Partitions. (8)

 (ii) Bit-Shifting. (6)

 (iii) Marking Bad Clusters. (2)