

Reg. No. :

--	--	--	--	--	--	--	--	--	--

Question Paper Code: 49024

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

Elective

Computer Science and Engineering

14UCS914 – CYBER FORENSICS

(Regulation 2014)

Duration: 1:15hrs

Maximum: 30 Marks

PART A - (6 x 1 = 6 Marks)

(Answer any six of the following questions)

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 (3 x 8= 24 Marks)

(Answer any three of the following questions)

11. Explain in detail about IPSec Protocol Documents. (8)
12. Briefly explain the types of Firewalls with a neat diagram and examples. (8)
13. Explain in detail about Incident Response Methodology and the six steps associated with it. (8)
14. Describe about the following mechanisms:
- (i) Understanding File Systems. (8)
15. Describe in detail about using specialized E-mail Forensics Tools. (8)