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

Question Paper Code : 71657

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2017.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6004 — CYBER FORENSICS

(Common to Information Technology)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Draw the IPsec Authentication Header and List the fields.
2. State compression and decompression using SSL Reco protocol.
3. Suppose the string of octets [0008 02fe] forms an MPI. The length of the MPI in bits [00000000 00001001] or 9 (= 23 + 20) in octets. Identify the actual integer value of the MPI.
4. List the types and importance of firewalls.
5. Define 'Hacking'.
6. Discuss RAID Data acquisition.
7. Label any three types of field kit to be used in crime scene.
8. Classify and compare hardware and software Forensic tools.
9. Name any three standard procedures used in Network Forensics.
10. Decide the roles of Client and Servers in E-mail investigations.

PART B — (5 × 16 = 80 marks)

11. (a) Illustrate briefly and compute the HMAC-SHA-1 and HMAC-MD5 using RFC Method and alternative method in IPsec security. (16)

Data 0 × 7104f218 a3192f65 1cf7225d 7011bf79 4a19

Key : 0 × 31fa7062 a45113e3 2679fd13 53b71264

Or

(b) Design a Pseudo Random Function (PRF) generation scheme using the parameters (16)

Seed : 0× 80 af 12 5c 7e 36 f3 21

label = rocky mountains = 0× 82 6f 63 6b 69 20 6d 6e 75 6f 74 61 69 6e 73

secret = 0× 35 79 bf 12 c4

12. (a) (i) Explain in detail the basic concept of Confidentiality vs. Encryption with the computational scheme. (8)

(ii) Convert the encoding process from 8-bit input groups to character string using Radix-64 alphabet.

Input raw text : 0× 15 d0 2f 9e b7 4c (4)

Input raw text : 0× 14 f2 d2 87 c2 2b. (4)

Or

(b) Compute the dual signature and perform merchant's and Banker's verification for the given Order Message(OM) and Payment Message(PM)

Order Message (OM) = 315a46f51283e7c647

Payment Message (PM) = 1325e46568. (16)

13. (a) Discuss in detail the systematic approach in computer investigations and conducting an Investigation in Computer Organizations. (16)

Or

(b) Discuss the investigation of Employee termination case, Internet abuse investigation, Attorney Client Privilege investigation in corporate high tech investigation. (16)

14. (a) Explain in detail about how the understanding NTFA, FAT, FAT32 file system plays a Crucial role in cyber forensic. (16)

Or

(b) Explain briefly the RAID architecture and its types with the data acquisition structure. Also explain the data centers used in processing the RAID systems. (16)

15. (a) (i) Discuss the procedure to validate the hexadecimal editors. (8)

(ii) Briefly explain any one steganography algorithm to hide data in a image. (8)

Or

(b) Examine and list the procedure to analyze the UNIX and Microsoft E-mail server logs. (16)
