Karunya University
(Karunya Institute of Technology and Sciences)
(Declared as Deemed to be University under Sec.3 of the UGC Act, 1965)

End Semester Examinations - 2015-16 Even Semester - May 2016

14CS3064 Network Security

Set B

Time : 3 hrs
Total Marks: 100

1. Identify the design objectives of HMAC and illustrate the overall operation of HMAC algorithm (20)

OR

2. a) Sketch the message digest generation of SHA-512 and provide step by step algorithm for SHA-512. (13)

   b) Sketch the SHA-512 processing of a single 1024 bit block? (7)

3. Sketch the general format of X.509 structure and certificate revocation list? What is unique in X.509 Version 3? Highlight the applicability of X.509 certificate on real life applications? (20)

OR

4. a) Illustrate with an example Man-in-the middle attack? (8)

   b) Summarize the Kerberos Version 4 message exchanges? (12)

5. a) Identify the unique differences in TLS when compared to SSLv3? (5)

   b) Highlight the requirements of email security and illustrate the PGP message generation and PGP message reception with neat sketches? (15)

OR

6. a) When IPsec is implemented, each outbound packet is processed by the IPsec logic before transmission and each inbound packet is processed by the IPsec logic after reception. Represent pictorially using a flowchart, the processing model for outbound and incoming IP packets? (10)

   b) Illustrate the operations of SSL handshake protocol ? (10)

7. a) Sketch the ESP packet format? (6)

   b) Highlight the essential features of IKE key determination algorithm? (6)

   c) What are the different types of viruses and highlight few advanced antivirus techniques? (8)

OR

8. a) Consider a problem where an attacker uses a commercially available tool and falsify the origin address of email messages thereby making it difficult for the receiver to filter this spam email based on the originating address. How will you address this problem? (10)

   b) Write short notes on i) Packet Filtering Firewall ii) Stateful inspection firewall iii) Application Proxy firewall iv) Circuit level proxy firewall (10)

9. In an organization, an intruder is attempting to gain access to a system or is attempting to increase the range of priviledges accessible on a system. How will you design an intrusion detection system and solve this issue? (20)

Wishing you All the Best