Code No: 2320504 **Set No. 1**

III B.Tech II Semester Regular Examinations, April/May 2009
INFORMATION SECURITY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) "Internetwork security is both fascinating and complex" - Justify the statement with valid reasoning.
   (b) Explain the terms related to Buffer overflow:
      i. Stack dumping
      ii. Execute Payload. [8+8]
2. (a) Explain with a neat illustration the automatic key distribution.
   (b) Explain the various steps involved in the HMAC algorithm. [8+8]
3. (a) Explain the procedure involved in RSA public-key encryption algorithm.
   (b) Explain what Kerberos is and give its requirements. [8+8]
4. (a) Explain the following terms in relation with the e-mail software - PGP:
      i. E-mail compatibility
      ii. Segmentation and reassembly.
   (b) Describe how authentication and confidentiality are handled in S/MIME. [8+8]
5. (a) When tunnel mode is used, a new outer IP header is constructed. For both IPV4 and IPV6, indicate the relationship of each outer IP header field and each extension header in the outer packet to the corresponding field or extension header of the inner IP packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values?
   (b) IP Sec Architecture document mandates support for two types of key management. What are they? [12+4]
6. Explain how the following threats to web security can be defended by SSL.
   (a) Known plaintext dictionary attack
   (b) Replay attack
   (c) Password sniffing
   (d) SYN flooding. [16]
7. (a) Explain how proxy accommodates devices that do not implement SNMP?
   (b) Discuss SNMPV1 administrative concepts. [8+8]

8. (a) What are two default policies that can be taken in a packet filter if there is no match to any rule? Which is more conservative? Explain with example rule sets both the policies?

   (b) What are the advantages of decomposing a user operation into elementary actions?

   (c) What are false negatives and false positives? [6+6+4]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: 2320504 **Set No. 2**

III B.Tech II Semester Regular Examinations, April/May 2009
INFORMATION SECURITY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) "Gaining control over the Routing tables at layer 3 is one of the attacks" - explain how Route tables modification is crucial.
   (b) Explain how Buffer overflow is created for any known platforms (eg., WINDOWS NT / LINUX). [8+8]
2. (a) Describe the various steps of encryption and decryption in an AES algorithm.
   (b) Write about Message authentication. [10+6]
3. (a) What is Key exchange? What is its importance? Discuss the Diffie-Hellman key exchange algorithm.
   (b) Explain the Digital Signature Algorithm (DSA) with a relevant example. [8+8]
4. (a) Explain the importance and usage of the following in relation to PGP:
      i. Session key
      ii. Signature
      iii. Public / Private keys.
   (b) Describe how S/MIME works towards emerging as an industry standard for e-mail security at commercial and organizational use levels. [8+8]
5. (a) When tunnel mode is used, a new outer IP header is constructed. For both IPV4 and IPV6, indicate the relationship of each outer IP header field and each extension header in the outer packet to the corresponding field or extension header of the inner IP packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values?
   (b) IP Sec Architecture document mandates support for two types of key management. What are they? [12+4]
6. (a) With a neat diagram explain SSL record protocol operation?
   (b) Discuss about the passive attacks and active attacks in WWW? [10+6]
7. (a) Draw the figure showing VACM logic and explain?
   (b) The encryption scheme used for UNIX passwords is one way; it is not possible to reverse it. Therefore, would it be accurate to say that this is, in fact, a hash code rather than an encryption of the password. [8+8]
8. (a) What is a bastion host? List the common characteristics of a bastion host?
   (b) Explain the concept of reference monitor in detail with a neat sketch? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: 2320504 **Set No. 3**

III B.Tech II Semester Regular Examinations, April/May 2009
INFORMATION SECURITY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Explain about how the Internet standards and RFCs.
   (b) Explain how Address Resolution Protocol table becomes a victim for attacks. [8+8]
2. (a) Compare AES cipher versus RC4 encryption algorithm.
   (b) Compare and contrast SHA-1 and HMAC functions. [8+8]
3. (a) Alice and Bob wish to share private messages, where each of them of two separate keys generated. What kind of strategy would you suggest to ensure confidentiality, key management and authentication for the conversation between Alice and Bob? Explain the strategy and also highlight the design issues related to the strategy proposed.
   (b) Describe the X.509 version 3 in detail. [8+8]
4. (a) Explain how the exchange of secret key takes place between 'X' and 'Y' users with PGP.
   (b) Write about the MIME Content types. [8+8]
5. (a) Discuss about the documents regarding IPSec protocol?
   (b) Describe any four ISAKMP payload types listing the parameters of the payload? [8+8]
6. Describe how brute-force attack and man-in-the-middle attack can be counted by SSL? [16]
7. (a) Draw the figure indicating the relationship among the different versions of SNMP by means of the formats involved. Explain.
   (b) Discuss in detail the advanced anti virus techniques? [6+10]
8. (a) What can be the two main attacks on corporate networks?
   (b) Give a detailed description of the two approaches to intrusion detection? [4+12]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: 2320504 **Set No. 4**

III B.Tech II Semester Regular Examinations, April/May 2009
INFORMATION SECURITY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) "Information Security is a major concern for the software industry today as the number of Internal threats is nearly 80%" - Discuss on the statement, highlighting the various security attacks.
   (b) Write a sample program to demonstrate the Buffer overflow and explain. [8+8]
2. (a) With neat illustration explain Advanced Encryption Standard algorithm (AES).
   (b) Explain the importance of Secure Hash functions with relevant examples. [8+8]
3. (a) Explain the procedure involved in RSA public-key encryption algorithm.
   (b) Explain what Kerberos is and give its requirements. [8+8]
4. (a) Explain why PGP generates a signature before applying the compression.
   (b) Discuss the requirement of segmentation and reassembly function in PGP. [8+8]
5. (a) Discuss the scope of ESP encryption and authentication in both IPV4 and IPV6?
   (b) Explain about transport adjacency and transport tunnel bundle? [8+8]
6. Discuss the features of SSL that counters man-in-the-middle attack, IP spoofing, IP hijacking and brute-force attacks to web security? [16]
7. (a) With a neat diagram explain SNMPV3 message format with USM?
   (b) Discuss about the four generations of the anti virus software? [10+6]
8. (a) What are two default policies that can be taken in a packet filter if there is no match to any rule? Which is more conservative? Explain with example rule sets both the policies?
   (b) What are the advantages of decomposing a user operation into elementary actions?
   (c) What are false negatives and false positives? [6+6+4]

⋆ ⋆ ⋆ ⋆ ⋆