Code No: M1222/R07 **Set No. 1**

IV B.Tech I Semester Supplementary Examinations, Feb/Mar 2011
INFORMATION SECURITY
(Common to Information Technology and Computer Science & Systems 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) Explain with a neat illustration the automatic key distribution.
   (b) Explain the various steps involved in the HMAC algorithm. [8+8]

3. (a) Differentiate between Public key cryptography and Digital signature with relevant examples.
   (b) Compare version 4 with version 5 of Kerberos. [8+8]

4. (a) What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed.
   (b) Describe the five principal services that Pretty Good Privacy (PGP) provides. [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. Explain in detail an open encryption and security specification designed to protect credit card transactions on the internet? [16]

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 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: M1222/R07 **Set No. 2**

IV B.Tech I Semester Supplementary Examinations, Feb/Mar 2011
INFORMATION SECURITY
(Common to Information Technology and Computer Science & Systems 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) 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 what each of the following means used in Kerberos:
      i. Authentication server
      ii. Ticket Granting server
      iii. Kerberos realm
      iv. Kerberos principal.
   (b) Explain the three alternative authentication procedures that X.509 uses across various applications. [8+8]
4. (a) What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed.
   (b) Describe the five principal services that Pretty Good Privacy (PGP) provides. [8+8]
5. (a) What are SA selectors? How there are used in filtering outgoing traffic to map it a particular SA?
   (b) What are the features of Oakley algorithm? Discuss the three basic requirements that must be satisfied in cookie generation. [8+8]
6. Write notes on:
   (a) Alert Protocol
   (b) SET Participants
   (c) Padding in SSL and TLS. [16]
7. (a) What are the goals for key management in SNMPV3?
   (b) Explain the nature of the virus?

(c) What are the deficiencies of SNMPV1? [6+6+4]

8. (a) What are the three main actions of a packet filter?
   (b) Give a detailed note on trusted systems? [6+10]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: M1222/R07 **Set No. 3**

IV B.Tech I Semester Supplementary Examinations, Feb/Mar 2011
INFORMATION SECURITY
(Common to Information Technology and Computer Science & Systems 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) What is a cipher block mode of operation? Explain the use of these modes of operation for the block ciphers for encipherment,
   (b) Describe the different methods of Message authentication. [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) What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed.
   (b) Describe the five principal services that Pretty Good Privacy (PGP) provides. [8+8]
5. (a) Distinguish between transport mode AH and tunnel mode AH. ?
   (b) For the Oakley aggressive key exchange, indicate which parameters in each message go in which ISAKMP payload type? [8+8]
6. Give a brief note on:
   (a) Business requirements for SET
   (b) Key features of SET
   (c) SET participants. [5+5+6]
7. (a) Draw the block diagram of traditional SNMP manager and explain its role?
   (b) With a neat diagram illustrate the typical steps in the Digital Immune System operation? [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?

Code No: M1222/R07 **Set No. 3**

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

⋆ ⋆ ⋆ ⋆ ⋆

Code No: M1222/R07 **Set No. 4**

IV B.Tech I Semester Supplementary Examinations, Feb/Mar 2011
INFORMATION SECURITY
(Common to Information Technology and Computer Science & Systems 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. Write about the following Secure hash functions:
   (a) SHA-1
   (b) MD5
   (c) HMAC. [6+5+5]

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 the general format of a PGP message with a pictorial representation.
   (b) What is a Certification Authority and explain its role in S/MIME. [8+8]

5. (a) What are the security services provided by IPSec at the IP layer?
   (b) Explain Authentication header protocol in detail? [6+10]

6. (a) Explain the concept of linking two messages intended for two different recipients adapted in SET?
   (b) Discuss SSL record protocol operation in detail? [8+8]

7. (a) Draw the block diagram of traditional SNMP manager and explain its role?
   (b) With a neat diagram illustrate the typical steps in the Digital Immune System operation? [8+8]

8. (a) What is a firewall? What is its functionality? What are its limitations?
   (b) What are the three main components of distributed intrusion detection? Discuss about agent architecture? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆