Code No: R05320504 **Set No. 1**

III B.Tech II Semester Regular Examinations, Apr/May 2008
INFORMATION SECURITY
(Computer Science & Engineering)

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Define a Security attack. Explain in detail about the various types of attacks an Internetwork is vulnerable to.
   (b) Write about Man-in-the-middle attacks. [10+6]
2. (a) Differentiate between the symmetric block ciphers and symmetric stream ciphers.
   (b) Write about Key distribution. [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) 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. (a) Draw the diagrams showing the relative location of security facilities in TCP/IP protocol stack? Discuss the advantages of each?
   (b) What is SSL session? Can a session be shared among multiple connections? What are the parameters that define a session state? [8+8]
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) List the characteristics of a good firewall implementation?
   (b) Explain in detail the two broad categories of statistical anomaly detection? [6+10]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: R05320504 **Set No. 2**

III B.Tech II Semester Regular Examinations, Apr/May 2008
INFORMATION SECURITY
(Computer Science & Engineering)

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What is a Security attack? Give the classification of the Security attacks. Discuss the following terms in detail with relevant examples:
   i. Interruption
   ii. Interception
   iii. Modification
   iv. Fabrication
   (b) Explain UDP hijacking. [10+6]
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) 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) Explain about the routing applications of IPSec?
   (b) Give the formats of ISAKMP header and Generic payload header? Explain various fields? [6+10]
6. (a) List the sequence of events that are required for a secure electronic transaction?
   (b) Explain the concept of dual signature? [8+8]
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 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: R05320504 **Set No. 3**

III B.Tech II Semester Regular Examinations, Apr/May 2008
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) 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) Discuss the purpose of SA selectors?
   (b) Enumerate on the five default ISAKMP exchange types? [8+8]
6. (a) Draw the diagrams showing the relative location of security facilities in TCP/IP protocol stack? Discuss the advantages of each?
   (b) What is SSL session? Can a session be shared among multiple connections? What are the parameters that define a session state? [8+8]
7. (a) What is an access policy? On what factors does access determination depends?
   (b) Discuss the two techniques for developing an effective an efficient proactive password checker? [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: R05320504 **Set No. 4**

III B.Tech II Semester Regular Examinations, Apr/May 2008
INFORMATION SECURITY
(Computer Science & Engineering)

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Define a Security attack. Explain in detail about the various types of attacks an Internetwork is vulnerable to.
   (b) Write about Man-in-the-middle attacks. [10+6]
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) 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) The IPSec architecture document states that when two transport mode SAs are bounded to allow both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate. Performing the ESP protocol before performing the AH protocol. Why this approach is recommended rather authentication before encryption?
   (b) Discuss the advantages and disadvantages of Diffie-Helman key exchange protocol? What is the specific key exchange algorithm mandated for use in the initial version of ISAKMP [8+8]
6. (a) What is WWW? What are the challenges web presents? Discuss?
   (b) Explain how SSL makes use of TCP to provide a reliable end-to-end secure service. [6+10]
7. (a) Discuss in detail about network management architecture?
   (b) What are the deficiencies of SNMPV1?
   (c) Give a brief note of distributed network management. [8+4+4]
8. (a) With neat diagrams show the differences between screened host firewall single homed bastion and screened host firewall dual homed bastion?
   (b) Discuss in detail about multilevel security? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆