Code No: 07A7EC39 **R07** **Set No. 2**

IV B.Tech I Semester Examinations,May 2011
INFORMATION SECURITY
Information Technology

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Discuss why Encryption is the most resorted security tool. Explain the conventional encryption principles.
   (b) Explain how message authentication is provided without message encryption. [8+8]
2. (a) With a neat diagram explain various fields of IP-Sec authentication header?
   (b) List the application of IPSec? Also mention IPSec routing applications. [8+8]
3. (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]
4. (a) Explain the RSA algorithm with an example.
   (b) Write about Digital Signatures. [8+8]
5. (a) "Phil Zimmerman's 'Pretty Good Privacy' (PGP) provides confidentiality and authentication" - Justify the statement with valid evidence.
   (b) Explain how the S/MIME Messages are prepared. [8+8]
6. (a) Discuss in detail firewall characteristics?
   (b) Explain the techniques that detect intrusion by observing events in the system and applying a set of rules? [6+10]
7. Consider the following threats to web security and describe how each is connected by a particular feature of SSL.
   (a) password sniffing
   (b) IP Spoofing
   (c) IP hijacking
   (d) SYN flooding. [16]
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: 07A7EC39 **R07** **Set No. 4**

IV B.Tech I Semester Examinations,May 2011
INFORMATION SECURITY
Information Technology

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Explain various web traffic security approaches?
   (b) Discuss in detail about SSL session and SSL connection? [8+8]
2. (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]
3. (a) Explain about the Security Mechanisms.
   (b) Explain TCP session hijacking with Packet Blocking. [8+8]
4. (a) Discuss in detail firewall characteristics?
   (b) Explain the techniques that detect intrusion by observing events in the system and applying a set of rules? [6+10]
5. (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]
6. (a) Perform the RSA algorithm on the given data and explain how encryption and decryption are performed on the message: p = 7; q = 11; e = 17; M = 8.
   (b) Explain Kerberos and the various servers it uses to provide authentication. Also briefly explain the duties of each server in this scenario. [8+8]
7. (a) Show how RC4 algorithm exhibits the symmetric stream cipher concept.
   (b) Discuss the requirements for Hash function. [8+8]
8. (a) End-to-end authentication and encryption are desired between two hosts. Draw figures that show
      i. Transport adjacency, with encryption applied before authentication.
      ii. A transport SA bundled inside a tunnel SA, with encryption applied before authentication.
      iii. A transport SA bundled inside a tunnel SA, with authentication applied before authentication.
   (b) What is the purpose of padding field in ESP packet? [12+4]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: 07A7EC39 **R07** **Set No. 1**

IV B.Tech I Semester Examinations,May 2011
INFORMATION SECURITY
Information Technology

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What are the things that need to be avoided for key management in SNMPV3?
   (b) Give the classification of Intruders?
   (c) Explain the various types of viruses? [4+6+6]
2. (a) What is the data base that defines the parameter associated with each SA? What are the parameters defined in the database?
   (b) Explain how encapsulating security payload provides confidentiality services? [8+8]
3. (a) With a suitable example show how the Digital Signature provides security. Also highlight the disadvantages of Digital signature.
   (b) Explain the terms used in relation with X.509 certificate:
      i. Version
      ii. Serial number
      iii. Signature algorithm identifier
      iv. Issuer unique identifier
      v. Subject unique identifier
      vi. Signature. [8+8]
4. (a) Explain the Feistel cipher structure.
   (b) With a clear diagram explain how Cipher Block Chaining mode is performed. [8+8]
5. (a) What action is taken by SSL when a fatal alert is received?
   (b) Discuss in detail the four phases of handshake protocol? [4+12]
6. (a) How is a circuit level gateway different from an application gateway?
   (b) Discuss about the measures that may be used for intrusion detection? [8+8]
7. (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]
8. (a) Describe clearly the Public key management in PGP.
   (b) Show how the S/MIME certification process is carried out. [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: 07A7EC39 **R07** **Set No. 3**

IV B.Tech I Semester Examinations,May 2011
INFORMATION SECURITY
Information Technology

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Discuss the common characteristics of a bastion host?
   (b) Discuss about distributed intrusion in detail? [6+10]
2. (a) Explain the procedure involved in RSA public-key encryption algorithm.
   (b) Explain what Kerberos is and give its requirements. [8+8]
3. (a) Make a comparison of transport and tunnel modes?
   (b) Mention the encryption and authentication algorithms used in ESP service? Discuss the purpose of padding in ESP protocol? [8+8]
4. (a) Define Information Security and explain its significance in today's world. Also clearly bring out the meaning of the following related terms: Computer Security, Network Security and Internet Security with relevant examples.
   (b) Write about UDP hijacking with suitable examples. [8+8]
5. (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]
6. (a) Explain how PGP uses the concept of trust.
   (b) Discuss the key management functions a User Agent Role of S/MIME performs.
   (c) Write about VeriSign Certificates. [16]
7. (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]
8. (a) List advantages and disadvantages of Cipher Feedback (CFB) mode.
   (b) Write about the One-way Hash function. [8+8]

⋆ ⋆ ⋆ ⋆ ⋆