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

III B.Tech Supplimentary Examinations, Aug/Sep 2008
INFORMATION SECURITY
(Computer Science & Engineering)

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Describe the various Security Services.
   (b) Compare TCP session hijacking and UDP hijacking. [8+8]
2. (a) Differentiate between the symmetric block ciphers and symmetric stream ciphers.
   (b) Write about Key distribution. [8+8]
3. (a) Perform the RSA algorithm on the given data and explain how encryption and decryption are performed on the message: p = 3; q = 11; e = 7; M = 5.
   (b) Describe the Digital certificates. [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) Explain about the routing applications of IPSec?
   (b) Give the formats of ISAKMP header and Generic payload header? Explain various fields? [6+10]
6. 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]
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) With a neat diagram explain the working principle of packet-filtering router?
   (b) What is a reference monitor? What are the rules that it has to enforce? Discuss its properties? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

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

III B.Tech Supplimentary Examinations, Aug/Sep 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) Compare AES cipher versus RC4 encryption algorithm.
   (b) Compare and contrast SHA-1 and HMAC functions. [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) Compare and contrast the key management in PGP and S/MIME.
   (b) Write about how PGP messages are created. [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) Discuss in detail the messages exchanged during the phase of handshake protocol used to establish the security capabilities that are associated with it?
   (b) Explain how SSL record protocol provides basic security services to various higher layer protocols? [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) With a neat diagram explain the working principle of packet-filtering router?
   (b) What is a reference monitor? What are the rules that it has to enforce? Discuss its properties? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: R05320504 **Set No. 3**

III B.Tech Supplimentary Examinations, Aug/Sep 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) Compare and contrast between Cryptography and Cryptology.
   (b) Explain the various Key distribution methods. [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) What is the default length of Authentication data field? On what fields is it calculated?
   (b) Explain how Diffie-Hellman protocol is vulnerable to man-in-the-middle attack? How is rectified in Oakley protocol? [8+8]
6. (a) What protocol is used to convey SSL-related alerts to the peer entity? Give the protocol format? Describe the fields?
   (b) What are the advantages of using IP security to provide web security? How advantageous is application-specific web security services? [10+6]
7. (a) Discuss the key elements included in the model of network management used for SNMP?
   (b) Explain the functional enhancements made in SNMPV2 over SNMPV1 [8+8]
8. (a) Explain the working of Packet-filtering router?
   (b) Explain the general model of access control as exercised by DBMS? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: R05320504 **Set No. 4**

III B.Tech Supplimentary Examinations, Aug/Sep 2008
INFORMATION SECURITY
(Computer Science & Engineering)

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Explain how Data integrity and Data confidentiality is provided as a part of Information security.
   (b) Explain the terms related to Buffer overflow:
      i. Stack frame
      ii. Execute Payload. [8+8]
2. (a) Differentiate between the symmetric block ciphers and symmetric stream ciphers.
   (b) Write about Key distribution. [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 are the fields present in SSL record protocol header? Mention their sizes and purpose?
   (b) Discuss the purpose of change cipher spec protocol and alert protocol in detail? [6+10]
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) Taking your own packet filtering rule set, explain the working packet-filtering router?

   (b) "One way to secure against Trojan horse attacks is the use of a secure, trusted OS". Explain? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆