Code No: V3225 **R07** **Set No: 1**

III B.Tech. II Semester Supplementary Examinations, November/December - 2012

INFORMATION SECURITY

(Computer Science and Engineering)

Time: 3 Hours **Max Marks: 80**

Answer any FIVE Questions

All Questions carry equal marks

*****

1. a) Describe in detail about TCP session hijacking and UDP hijacking.
   b)"Gaining control over the Routing tables at layer 3 is one of the attacks" - explain how Route tables modification is crucial. [8+8]

2. a) Explain about key distribution approaches of message authentication.
   b) Explain about Data Encryption Standard and also discuss about the strength of DES. [8+8]

3. a) Explain the procedure involved in RSA public-key encryption algorithm.
   b) List two disputes that can arise in the context of message authentication. What are the properties that digital signature should have? [8+8]

4. a) Explain why PGP generates a signature before applying the compression.
   b) Write down the functions provided by S/MIME. [8+8]

5. a) Explain in detail about the IP Security Architecture.
   b) List the default ISAKMP exchange types? [8+8]

6. a) Explain about Payment Processing which is supported by SET
   b) Explain how SSL makes use of TCP to provide a reliable end-to-end secure service. [8+8]

7. a) Define Honey pots. How are they designed? Explain.
   b) What are the deficiencies of SNMPV1?
   c) What is the role of compression and encryption in the operation of a virus? [5+5+6]

8. a) What does stateful inspection firewall mean? Explain.
   b) In the context of access control, what is the difference between subject and an object. [8+8]

*****

Code No: V3225 **R07** **Set No: 2**

III B.Tech. II Semester Supplementary Examinations, November/December - 2012

INFORMATION SECURITY

(Computer Science and Engineering)

Time: 3 Hours **Max Marks: 80**

Answer any FIVE Questions

All Questions carry equal marks

*****

1. a) Explain the terms related to Buffer overflow:
   i. Stack dumping
   ii. Execute Payload.

   b) Describe in detail about model for internetwork security. [8+8]

2. a) With neat illustration explain Advanced Encryption Standard 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) What is the "realm" in Kerberos environment? Explain with suitable diagram how a service between two realms takes place. [8+8]

4. a) Discuss the requirement of segmentation and reassembly function in PGP.
   b) Define S/MIME. What are the key algorithms used in S/MIME? [8+8]

5. a) What does authentication header provide? Explain in detail about fields of authentication header.
   b) Explain briefly how IPSec documents are categorized. [8+8]

6. a) What are services SET provides? Give an overview of SET.
   b) Explain about the Web Security Considerations. [8+8]

7. a) Suggest any three password selection strategies and identify their advantage and disadvantages if any.
   b) Discuss in detail about the model of network management that can be SNMP and explain about key elements. [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? [5+5+6]

*****

Code No: V3225 **R07** **Set No: 3**

III B.Tech. II Semester Supplementary Examinations, November/December - 2012

INFORMATION SECURITY

(Computer Science and 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) Explain about how the Internet standards and RFCs. [8+8]

2. a) Draw the general structure of DES and explain the encryption decryption process.
   b) Explain the importance of Secure Hash functions with relevant examples. [8+8]

3. a) Perform encryption and decryption using RSA algorithm P=7, Q=11, E=17 ;M=18.
   b) Describe the X.509 version 3 Directory Authentication Service in detail. [8+8]

4. a) Explain how the exchange of secret key takes place between 'X' and 'Y' users with PGP.
   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 packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values?
   (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) Explain how the following threats to web security can be defended by SSL.
   i)Replay attack ii) SYN flooding
   b) Discuss about the usage of TLS Pseudorandom functions in detail. [8+8]

7. a) Draw the figure indicating the relationship among the different versions of SNMP by means of the formats involved. Explain.
   b) Report the techniques for learning passwords by password crackers. [8+8]

8. a) Discuss on service controls on which firewalls focused.
   b) With a simple scenario explain about Trojan horse defense and secure operating system. [8+8]

*****

Code No: V3225 **R07** **Set No: 4**

III B.Tech. II Semester Supplementary Examinations, November/December - 2012

INFORMATION SECURITY

(Computer Science and Engineering)

Time: 3 Hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks
*****

1. a) Explain different security attacks and security services in detail.
   b) Describe in detail about buffer overflow and format string vulnerabilities. [8+8]

2. a) Describe in detail about cipher block modes of operation .
   b) Describe about HMAC in detail and mention any one of its application. [8+8]

3. a) Alice and Bob want to establish a secret key using the Diffie - Hellman key exchange protocol using n = 11, g = 5, x = 2 and y = 3. Find the values A and B and the secret key.
   b) List the approach used by X.509 for user authentication . [8+8]

4. a) Write about the MIME Content types? Describe in detail.
   b) Describe how PGP provides confidentiality and authentication service for email applications. [8+8]

5. a) Explain about tunnel mode ESP and also discuss about where transport mode is suitable and where tunnel mode is useful.
   b) Define security association bundle. Discuss different ways of combining security associations. [8+8]

6. a) With a neat diagram explain SSL record protocol operation?
   b) Describe about how the merchant verifies customer Purchase request in detail. [8+8]

7. a) Why does SNMP use unreliable UDP datagram? What would be the reason for the designers to choose UDP instead of TCP for transport protocol for SNMP?
   b) Give a detailed description of the two approaches to intrusion detection? [8+8]

8. a) Discuss about attacks that can be made on packet filtering router and appropriate counter measures.
   b) Discuss in detail about firewall design principles. [8+8]

*****