Code No: 07A71204 **R07** **Set No. 2**

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

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What is the contribution of Phil Zimmerman towards creation of PGP? Also explain reasons for the popularity of PGP.
   (b) Write about the functions of S/MIME and list the cryptographic algorithms adopted by S/MIME. [8+8]
2. (a) Discuss about user security model in detail.
   (b) How a viral infection happens initially?
   (c) Give a note of types of viruses. [8+2+6]
3. (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]
4. (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]
5. (a) Explain the following related to RSA cryptosystem:
      i. What is the one-way function in this system?
      ii. What is the trapdoor in this system?
      iii. Define the public and private keys in this system.
      iv. Describe the security in this system.
   (b) Define the X.509 recommendation. State and explain its purpose in detail. [8+8]
6. (a) "A bastion host is a critical strong point in the network's security". Justify?
   (b) Discuss in detail profile-based anomaly 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) 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 IP packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values?

(b) IP Sec Architecture document mandates support for two types of key management. What are they? [12+4]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: 07A71204 **R07** **Set No. 4**

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

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Explain about the Security Mechanisms.
   (b) Explain TCP session hijacking with Packet Blocking. [8+8]
2. (a) What is the purpose of a firewall? Discuss the limitations of firewalls?
   (b) What is the significance of audit records in intrusion detection? Explain the various fields of an audit record. [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) 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]
5. (a) Explain why AES algorithm is an example of symmetric block cipher algorithm.
   (b) Write about Simple Hash functions. [8+8]
6. (a) Discuss the scope of ESP encryption and authentication in both IPV4 and IPV6.
   (b) Explain about transport adjacency and transport tunnel bundle. [8+8]
7. Explain how the following threats to web security can be defended by SSL:
   (a) Known plaintext dictionary attack
   (b) Replay attack
   (c) Password sniffing
   (d) SYN flooding. [16]
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: 07A71204 **R07** **Set No. 1**

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

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) How is screened host firewall, dual-homed bastion different from screened host firewall, single home bastion?
   (b) What are the two types of audit records that can be used in intrusion detection? Explain the typical fields of an audit record. [8+8]
3. Write about the following terms related to PGP and S/MIME:
   (a) Radix-64
   (b) Session key
   (c) Compression
   (d) Encryption
   (e) Decryption. [16]
4. (a) Explain the Feistel cipher structure.
   (b) With a clear diagram explain how Cipher Block Chaining mode is performed. [8+8]
5. (a) Discuss how sequence number field of Authentication header is used to threat replay attacks?
   (b) What is a cookie? ISAKMP mandates that the cookie generation satisfy three basic requirements. What are they? Explain? [8+8]
6. (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]
7. (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]

8. 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]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: 07A71204 **R07** **Set No. 3**

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

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) With a neat diagram explain SNMPV3 message format with USM.
   (b) Discuss about the four generations of the anti virus software. [10+6]
2. (a) Discuss the common characteristics of a bastion host.
   (b) Discuss about distributed intrusion in detail. [6+10]
3. (a) Give the structure of HMAC and explain the HMAC algorithm.
   (b) Explain the location of Encryption devices to provide network security. [8+8]
4. (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]
5. (a) Explain clearly with relevant illustration how authentication is addressed in PGP.
   (b) Explain how the exchange of secret key takes place between 'X' and 'Y' users of S/MIME. [8+8]
6. (a) What is Man-in-the-middle attacks? Explain the same with a relevant example.
   (b) Explain the Format String vulnerabilities being exploited by 'C' language's 'printf' function with a suitable example. [8+8]
7. (a) Explain what a Certificate and Certificate Authority are.
   (b) Compare version 4 with version 5 of Kerberos in terms of the following:
      i. Authentication Service Exchange
      ii. Ticket-Granting Service Exchange
      iii. Client/Server Authentication Exchange. [8+8]
8. Describe how brute-force attack and man-in-the-middle attack can be counted by SSL. [16]

⋆ ⋆ ⋆ ⋆ ⋆