www.firstranker.com

Code No: 07A60503 **R07** **Set No. 2**

III B.Tech II Semester Examinations,December 2010
INFORMATION SECURITY
Computer Science And Engineering

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Discuss about the SSL protocol stack?
   (b) List the services provided by TLS?
   (c) Explain the significance of dual signature in SET? [8+4+4]
2. Explain the IDEA algorithm? [16]
3. Explain the various MIME content types? [16]
4. (a) List and briefly explain the three classes of intruders?
   (b) Write a short note on macro virus? [8+8]
5. (a) Give an overview of IPSec document?
   (b) Explain the selectors that determine an Security Policy Database(SPD) entry in IPSec? [8+8]
6. (a) Explain the intrusion detection tool: audit records?
   (b) What are the services provided by Firewalls? [8+8]
7. (a) Perform the RSA algorithm on the given data and explain how encryption and decryption on the message: p =5; q=11;e=3;M=9.
   (b) Describe the digital certificates. [8+8]
8. Write short notes on:
   (a) Security services
   (b) TCP session hijacking. [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

FIRSTRANKER

www.firstranker.com

www.firstranker.com

Code No: 07A60503 **R07** **Set No. 4**

III B.Tech II Semester Examinations,December 2010
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 key management in IP security?
   (b) Explain the Oakley key determination protocol? [8+8]
2. (a) Explain how confidentiality and authentication services are achieved in public key cryptography?
   (b) Describe the dialogue conversation of Kerberos? [8+8]
3. (a) Differentiate between the symmetric block ciphers and symmetric stream ciphers.
   (b) Write about Key distribution in symmetric key algorithms. [8+8]
4. Write short notes on:
   (a) Second generation of antivirus
   (b) intruders. [16]
5. (a) Distinguish between cryptography and steganography?
   (b) Explain how Data integrity and Data confidentiality is provided as a part of Information security.
   (c) Explain the terms related to Buffer overflow:
      i. Stack frame.
      ii. Execute Payload. [4+4+8]
6. (a) What is R64 conversion? Why is R64 conversion useful for an e-mail application?
   (b) Discuss the functions provided by S/MIME? [8+8]
7. (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. [8+8]
8. (a) What properties are required of a reference monitor?
   (b) Explain the working of application-level gateway? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

FIRSTRANKER

www.firstranker.com

www.firstranker.com

Code No: 07A60503 **R07** **Set No. 1**

III B.Tech II Semester Examinations,December 2010
INFORMATION SECURITY
Computer Science And Engineering

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What are the various antivirus approaches? Explain?
   (b) Write short notes on:
   (a) Intruders
   (b) virus. [8+4+4]
2. Explain the pretty good privacy (PGP). [16]
3. (a) Explain the public key cryptographic principles?
   (b) Describe Kerberos? [8+8]
4. (a) What are the applications of IPSec?
   (b) Give an overview of IPSec document? [8+8]
5. (a) Explain the various web security threats?
   (b) Explain the significance of dual signature in SET? [8+8]
6. (a) What is man-in-the-middle attack? Explain with an example?
   (b) List and explain the different internet standards related to information security? [8+8]
7. (a) What is the difference between diffusion and confusion?
   (b) Which parameters and design choices determine the actual algorithm of a fiestel cipher?
   (c) What is the purpose of the S-boxes in DES? [4+8+4]
8. Write short notes on:
   (a) Rule-based penetration identification: intrusion detection
   (b) Application-level gateway: firewall. [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

FIRSTRANKER

www.firstranker.com

www.firstranker.com

Code No: 07A60503 **R07** **Set No. 3**

III B.Tech II Semester Examinations,December 2010
INFORMATION SECURITY
Computer Science And Engineering

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

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What are the characteristics of firewall?
   (b) Explain the general model of access control as exercised by DBMS? [8+8]
2. (a) What is TCP session hijacking?
   (b) Explain UDP hijacking? [8+8]
3. Explain SNMP? [16]
4. (a) Briefly explain about DES design criteria?
   (b) What are the approaches of message authentication? [8+8]
5. Explain ISAKMP protocol? [16]
6. (a) List the participants of SET? Explain?
   (b) Explain the SSL record protocol? [8+8]
7. (a) In the context of Kerberos, what is a realm? Explain?
   (b) What are the requirements of public key cryptography? [8+8]
8. (a) Explain how bob finds out what cryptographic algorithms alice has used when he receives an S/MIME message from her?
   (b) In PGP, explain how bob and alice exchange the secret key for encrypting messages? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

FIRSTRANKER

www.firstranker.com