

Code No: 07A60503

R07**Set No. 2****III B.Tech II Semester Examinations, APRIL 2011****INFORMATION SECURITY****Computer Science And Engineering****Time: 3 hours****Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

1. Discuss about
 - (a) security attacks
 - (b) security services
 - (c) security mechanisms. [16]
2. (a) Explain the rule-based intrusion detection?
(b) Discuss about data access control. [8+8]
3. Explain the AES algorithm? [16]
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 are the web security considerations
(b) What are the key features of SET?
(c) What are the elements involved in SET? Explain? 4+4+8]
6. (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]
7. (a) How does the encapsulating security payload work?
(b) How are the secure keys distributed in IPsec? [8+8]
8. (a) Explain the procedure involved in RSA public-key encryption algorithm?
(b) Explain what Kerberos is and give its requirements. [8+8]

Code No: 07A60503

R07**Set No. 4****III B.Tech II Semester Examinations, APRIL 2011****INFORMATION SECURITY****Computer Science And Engineering****Time: 3 hours****Max Marks: 80****Answer any FIVE Questions****All Questions carry equal marks**

1. (a) Distinguish between a packet-filtering router and a stateful inspection firewall?
(b) "One way to secure against Trojan horse attacks is the use of a secure, trusted OS". Explain? [8+8]
2. Explain the working of SSL protocol? [16]
3. (a) What is IPSec authentication header? Explain?
(b) Discuss the purpose of SA selectors? [8+8]
4. (a) How does PGP use the concept of trust?
(b) Discuss the functions provided by S/MIME? [8+8]
5. (a) With a neat diagram explain SNMPV3 message format with USM?
(b) Discuss about the four generations of the anti virus software? [8+8]
6. (a) What are the criteria used while designing the DES algorithm?
(b) In AES, how the encryption key is expanded to produce keys for the 10 rounds. [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) How IP spoofing and session hijacking work?
(b) Discuss the various types of security attacks? [8+8]

Code No: 07A60503

R07**Set No. 1****III B.Tech II Semester Examinations, APRIL 2011****INFORMATION SECURITY****Computer Science And Engineering****Time: 3 hours****Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

1. Explain the key distribution techniques in public key cryptographic algorithms? [16]
2. (a) Explain the key features of SET?
(b) What is SSL? Explain the advantages and disadvantages of SSL? [8+8]
3. (a) How is IP security achieved? Explain.
(b) What are various applications of IP Security?
(c) Explain the features of Oakley? [8+4+4]
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 is the difference between an unconditionally secure cipher and a computationally secure cipher?
(b) Briefly describe about the Strength of DES? [8+8]
6. (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? [8+8]
7. (a) Explain the route table modification vulnerability?
(b) Explain the security mechanisms? [8+8]
8. (a) What are the two rules that a reference monitor enforces?
(b) Explain the techniques used by a firewall to control access? [8+8]

Code No: 07A60503

R07**Set No. 3****III B.Tech II Semester Examinations, APRIL 2011****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 SNMP community facility?
(b) Explain the phases of a virus? [8+8]
2. Discuss about the public key management in PGP? [16]
3. (a) What are the limitations of a firewall? Explain.
(b) 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 of both the policies? [8+8]
4. (a) What are the requirements for the use of a public key certificate scheme?
(b) Briefly explain the X.509 authentication service. [8+8]
5. (a) Explain the buffer overflow attack with an example?
(b) Explain the format string vulnerability? [8+8]
6. (a) Explain about the authentication header?
(b) Explain the transport and tunnel modes of ESP? [8+8]
7. (a) In SSL and TLS, why is there a separate Change Cipher Spec Protocol, rather than including a change_cipher_spec message in the Handshake Protocol?
(b) Explain the significance of dual signature in SET? [8+8]
8. (a) Discuss the factors on which the strength of DES depends?
(b) Explain security over hash functions and MAC? [8+8]
