Code No: V3225

R07

Set No: 1

III B.Tech. II Semester Supplementary Examinations, April/May - 2013
INFORMATION SECURITY
(Computer Science and Engineering)

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

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

1. a) Explain Network security model with neat diagram.
    b) Describe internet standards .   [8M+8M]

2. a) Explain classification of cryptographic systems.
    b) Explain various types of cryptanalytic attacks based on the amount of information known
    to crypto analysts.   [8M+8M]

3. a) What is message authentication? Explain the message without message encryption?
    b) What is a Kerberos? What are the requirements of a Kerberos?   [8M+8M]

4. Describe PGP services in detail.   [16M]

5. a) Explain IP Sec documents in detail.
    b) Explain Oakley Key Distribution Protocol.   [8M+8M]

6. Explain Secure Electronic Transaction in detail.   [16M]

7. a) Explain network management protocol architecture.
    b) Explain SNMPv3 applications.   [8M+8M]

8. a) Describe different classes of intruders.
    b) Explain the Trusted Systems.   [8M+8M]

*****

|''|'||'|''|'|''|'|''''|

Code No: V3225

R07

Set No: 2

III B.Tech. II Semester Supplementary Examinations, April/May - 2013
INFORMATION SECURITY
(Computer Science and Engineering)

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

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

1. a) Explain various security attacks in detail.
    b) Explain security services in detail.   [8M+8M]

2. Explain classical Feistel structure encryption and decryption with neat diagram.   [16M]

3. a) What is a MAC? Explain message authentication code using MAC.
    b) Describe Kerberos Realms and multiple Kerberi.   [8M+8M]

4. a) Explain PGP cryptographic functions with a diagram.
    b) Describe MIME format.   [8M+8M]

5. a) Explain benefits of IP Sec.
    b) Explain key management of IP sec.   [8M+8M]

6. a) Explain various web traffic Security approaches.
    b) Briefly explain TSL.   [8M+8M]

7. a) Explain key elements of SNMP.
    b) Explain SNMPV1 authentication service.   [8M+8M]

8. a) Describe password protection.
    b) Explain Trojan Horse defense.   [8M+8M]

*****

|''|'|||'|''|'|''''|

R07

Set No: 3

Code No: V3225

III B.Tech. II Semester Supplementary Examinations, April/May - 2013
INFORMATION SECURITY
(Computer Science and Engineering)

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

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

1. a) Explain various passive and active attacks.
    b) Explain internet standardization process.   [8M+8M]

2. a) Describe the following.
        (i) Cryptography.
        (ii) Cryptanalysis.
        (iii) Cryptology.
        (iv) Conventional encryption.
    b) Describe various cipher block modes of operations.   [8M+8M]

3. a) Compare the principle characteristics of secure Hash Functions.
    b) Explain differences between Kerberos version 4 and 5.   [8M+8M]

4. a) Explain transmission and reception of PGP with a diagram.
    b) Explain traditional e-mail format.   [8M+8M]

5. a) Explain the applications of IPSec
    b) Explain IP Sec authentication service for transport and tunnel modes.   [8M+8M]

6. Explain Secure Socket layer in detail.   [16M]

7. a) Briefly describe basic frame work for SNMP.
    b) Compare SNMPV1 and SNMPV2 protocol data units.   [8M+8M]

8. a) Explain Distributed Intrusion Detection.
    b) Describe the capabilities and limitations of firewall.   [8M+8M]

*****

|''|'||'|''|'|''''|

Code No: V3225

R07

Set No: 4

III B.Tech. II Semester Supplementary Examinations, April/May - 2013
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 following
       (i) Confidentiality   (ii) Authentication   (iii) Access control   (iv) Integrity
    b) Describe internet Society.   [8M+8M]

2. a) Explain the requirements for secure use of conventional encryption.
    b) Explain Advanced Encryption standard.   [8M+8M]

3. Describe X.509 Authentication service in detail.   [16M]

4. a) Explain the limitations of the SMTP/822 scheme.
    b) Describe S/MIME.   [8M+8M]

5. a) Describe IP Sec.
    b) Explain IPSEC ESP format.   [8M+8M]

6. a) Explain various Web security threats.
    b) Briefly explain SSL architecture.   [8M+8M]

7. a) Explain SNMP protocol architecture.
    b) Explain SNMPV3 applications.   [8M+8M]

8. a) Describe Intrusion detection in detail.
    b) Explain design goals for a fire walls.   [8M+8M]

*****

1 of 1