www.FirstRanker.com www.FirstRanker.com www.FirstRanker.com

Code: 9A05709

1

B.Tech IV Year II Semester (R09) Regular Examinations, March/April 2013

INFORMATION SECURITY

(Common to ECE and ECC)

Time: 3 hours Max. Marks: 70

Answer any FIVE questions

All questions carry equal marks

*****

1 (a) Explain how banks protect money.
(b) Write a note on substitution ciphers and their cryptanalysis.

2 (a) Write a detailed note on covert channels.
(b) Explain how viruses completely replace a program.

3 (a) Discuss how public-keys are distributed.
(b) What the categories of the use of public key crypto systems?

4 Describe in detail direct digital signatures and arbitrated digital signatures.

5 Compare and contrast S-MIME and PGP protocols.

6 (a) Explain the function areas of IP security.
(b) Give the application of IP security.

7 (a) What protocol is used to convey SSL-related alerts to the peer entity? Give the protocol format? Describe the fields.
(b) What are the advantages of using IP security to provide web security? How advantageous is application-specific web security services?

8 (a) Identify a few malicious programs that need a host program for their existence?
(b) Describe the familiar types of firewall configurations.

*****

FirstRanker

www.FirstRanker.com

www.FirstRanker.com www.FirstRanker.com www.FirstRanker.com

Code: 9A05709

2

B.Tech IV Year II Semester (R09) Regular Examinations, March/April 2013

INFORMATION SECURITY

(Common to ECE and ECC)

Time: 3 hours Max. Marks: 70

Answer any FIVE questions

All questions carry equal marks

*****

1 (a) Explain the characteristics of computer intrusion.
(b) Explain in detail one-time pads

2 (a) Give examples of salami attacks. Why do they persist?
(b) What the goals of virus and describe how each goal can be addressed?

3 Discuss the approaches to message authentication.

4 (a) What is digital signature? How are they different from hand written signatures?
(b) Explain the symmetric encryption approaches for authentication and key exchange using timestamps.

5 Explain various flags present in Kerberos version 5.

6 Explain in detail about authentication header.

7 Explain the following:
(a) Change Cipher Spec protocol.
(b) Handshake protocol.

8 (a) What is the logic for compression virus?
(b) Explain Trojan Horse and Secure operating system.

*****

FirstRanker

www.FirstRanker.com

www.FirstRanker.com www.FirstRanker.com www.FirstRanker.com

Code: 9A05709

3

B.Tech IV Year II Semester (R09) Regular Examinations, March/April 2013

INFORMATION SECURITY

(Common to ECE and ECC)

Time: 3 hours Max. Marks: 70

Answer any FIVE questions

All questions carry equal marks

*****

1 (a) Briefly describe data vulnerabilities.
(b) Illustrate columnar transposition cipher with an example.

2 (a) Explain the working of code red worm.
(b) What is "covert channel"? Explain different types of covert channels.

3 (a) Discuss the applications for public key crypto system.
(b) Discuss about message authentication using a message authentication code.

4 What is one-way authentication? Explain the approaches for one-way authentication.

5 (a) Define S/MIME. What are the elements of MIME?
(b) What are the headers fields define in MIME?
(c) What is MIME content type and explain?

6 Explain in detail about Oakley algorithm.

7 (a) Explain handshake protocol actions of SSL.
(b) Discuss in detail secure electronic transaction.

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?

*****

FirstRanker

www.FirstRanker.com

www.FirstRanker.com www.FirstRanker.com www.FirstRanker.com

Code: 9A05709

4

B.Tech IV Year II Semester (R09) Regular Examinations, March/April 2013

INFORMATION SECURITY

(Common to ECE and ECC)

Time: 3 hours Max. Marks: 70

Answer any FIVE questions

All questions carry equal marks

*****

1 Explain various methods of defense.

2 (a) Describe the viruses that can change its appearance.
(b) Give the taxonomy of program flaws.

3 (a) Discuss how public-keys are distributed.
(b) What the categories of the use of public key crypto systems.

4 (a) What are relay attacks? Give examples. Explain the approaches to deal with these attacks.
(b) What is the difference between direct and arbitrated digital signatures?

5 Explain about Kerberos.

6 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.

7 Discuss the features of SSL that counters man-in-the-middle attack, IP spoofing, IP hijacking and brute-force attacks to web security?

8 (a) With neat diagrams show the differences between screened host firewall single homed bastion and screened host firewall dual homed bastion?
(b) Discuss in detail about multilevel security?

*****

FirstRanker

www.FirstRanker.com