Code: 9A05709

R09

B.Tech IV Year I Semester (R09) Regular & Supplementary Examinations December 2015

INFORMATION SECURITY

(Common to CSE & CSS)

Time: 3 hours Max. Marks: 70

Answer any FIVE questions

All questions carry equal marks

*****

1 (a) List the three fundamental security properties and for each give an example of a failure.
(b) Illustrate columnar transposition cipher with an example.

2 Write notes on the following:
(a) Buffer overflows.
(b) Incomplete mediation.
(c) Time – check to time-of-use errors.

3 (a) What basic arithmetic and logical functions are used in SHA and WHIRLPOOL?
(b) Explain Diffie-Hellman key exchange algorithm with an example.

4 (a) What is digital signature? Explain the benefits of digital signature.
(b) What are relay attacks? Give examples. Explain the approaches to deal with these attacks.

5 (a) Describe about revocation of public keys in PGP.
(b) Explain how Kerberos supports inter realm authentication.

6 (a) Give the format of authentication header and explain the significance of various fields.
(b) For the Oakley aggressive key exchange, indicate which parameters in each message go in which ISAKMP payload type.

7 (a) Describe the sequence of events that are required for a transaction. Explain the cryptographic details.
(b) What is the significance of change cipher specification protocol?

8 (a) What are the advantages and disadvantages of using audit records for intrusion detection?
(b) Discuss in detail the three firewall configurations.

*****