NR

Code No: B2501

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.TECH II SEMESTER EXAMINATIONS, APRIL/MAY 2012
INFORMATION SECURITY
(SOFTWARE ENGINEERING)

Time: 3hours **Max.Marks:60**

Answer any five questions
All questions carry equal marks
- - -

1.a) Define the three security goals.
b) Explain TCP session hijacking.
c) Write notes on man-in-middle attack.

2.a) Explain mono alphabetic cipher and poly alphabetic cipher with examples.
b) List ways in which secret keys can be distributed to two communicating parties. Explain them.

3.a) Explain ECC algorithm.
b) Explain X.509 directory services.

4.a) What are the five principal services provided by PGP? Explain.
b) Write notes on S/MIME functionality.

5.a) What parameters identify an SA and what parameters characterize the nature of a particular SA?
b) What are the roles of Oakley key determination protocol and ISAKMP in IPSec?

6.a) Write notes on SSL connection and SSL session.
b) What steps are involved in the SSL Record Protocol transmission?

7.a) What are the two common techniques used to protect a password file?
b) What are the key elements of SNMP model?
c) Write short notes on key localization.

8.a) What are the four techniques used by a firewall to control access and enforce a security policy?
b) What are the two rules that a reference monitor enforces?
c) What properties are required by a reference monitor?

****