R09

Code No: C5709

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.TECH I - SEMESTER EXAMINATIONS, APRIL/MAY-2012
NETWORK SECURITY AND CRYPTOGRAPHY
(VLSI SYSTEM DESIGN)

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

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

1.a) Discuss about Security Services defined in X.800.
b) With a block diagram explain conventional Encryption Model and entities involved.

2.a) What are drawbacks of double – DES? How is it handled by Triple DES?
b) List characteristics of Advanced Symmetric block ciphers.

3.a) What are the requirements of pure random number generator? Explain about any one pseudo random number generator.
b) Explain uses of RSA algorithm. With an example explain RSA algorithm.

4.a) State and prove Fermat's Theorem. Give Example and list its uses.
b) List authentication requirements. What are methods of offering authentication service?

5.a) Explain about Message Digest algorithm.
b) What is Digital Signature? Explain Digital Signature requirements.

6.a) What is X.509 certificate format? Explain significance of fields in X.509 certificate.
b) What are the Security Services offered in PGP? Explain how PGP works.

7.a) Discuss about two modes of usage by AH and ESP in IPSEC.
b) Explain web security threats and web Traffic Security Approaches.

8.a) What is Virus? Give a general depiction of virus structure.
b) Explain different types of Firewalls.

* * * * * *