

R09

Code No: C5709

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech I - Semester Examinations, March/April-2011
NETWORK SECURITY AND CRIPTOGRAPHY
(VLSI SYSTEM DESIGN)**

Time: 3hours

Max. Marks: 60

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

- - -

- 1.a) Describe briefly about the model for internet work security.
- b) Explain the various classical encryption techniques. [12]
2. Explain in detail about Blowfish algorithm. [12]
- 3.a) Briefly explain Diffie-Hellman key exchange.
- b) Explain in detail about the RSA algorithm. [12]
- 4.a) Explain in detail about the Chinese remainder theorem.
- b) What are the various requirements of message authentication? [12]
- 5.a) Explain in detail about RIPEMD-160 algorithm.
- b) What are the differences between direct and arbitrated digital signatures? [12]
- 6.a) Explain about PGP.
- b) Explain about the Kerberos with a neat diagram. [12]
- 7.a) Explain in detail about SSL architecture.
- b) Explain the requirements of web security. [12]
- 8.a) Explain the design principles of firewalls.
- b) Explain the four techniques used by firewalls to control access and enforce a security policy. [12]
