R09

Code No: D0606

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech II - Semester Examinations, March/April 2011
NETWORK SECURITY AND CRYPTOGRAPHY
(DIGITAL SYSTEMS & COMPUTER ELECTRONICS)

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

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

1. a. What are the goals of network security?
   b. Enumerate the difference between passive attacks and active attacks? Give examples for each.
   c. Describe the Internet work security model. [12]

2. a. What are block cipher design principles?
   b. Explain the operation of DES algorithm. [12]

3. Explain the working of Blowfish algorithm. [12]

4. a. How the key is distributed/managed in private key algorithms? Explain the different scenarios.
   b. What are principles of public key cryptography?
   c. List out the steps in RSA algorithm. [12]

5. Explain the following
   a) Euler’s theorem.
   b) Authentication requirements and functions. [12]

6. List and explain the sequence of steps followed in Message Digest (MD5) algorithm.[12]

7. a. Explain how security is provided to e– mails.
   b. Explain X.509 directory authentication service. [12]

8. Write short notes on:
   a. Secure socket layer(SSL)
   b. Trusted systems [12]

****