R09

Code No: **C8204**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.Tech I - Semester Examinations, March/April -2011
NETWORK SECURITY -I
(COMPUTER NETWORKS)

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

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

1. a) List and briefly define categories of security attacks.
    b) Explain substitutional and transpositional encryption methods.   [12]

2. a) Describe Block Cipher chaining Mode of Operation.
    b) Discuss about Diffie-Hellman Key exchange algorithm.   [12]

3. a) Explain Message Authentication code in detail.
    b) Describe about Euclid's Algorithm and how do you use in the context of
       security?   [12]

4. a) Explain Kerberos?
    b) Write about DSS (Digital Signature Standard) algorithm.   [12]

5. a) What Services are provided by IPSec?
    b) List three design goals for a Firewall? And Explain circuit-level gateway.[12]

6. a) Explain about PGP.
    b) Define Message Digest Algorithm.   [12]

7. a) What are typical phases of operation of a virus or warm?
    b) Explain RSA public key cryptography with appropriate numerical example.
                                                                               [12]
8. a) Explain Triple DES.
    b) What are the two basic functions used in encryption algorithms?   [12]

******