R09

Code No: D6108, D3808, D7008, D5510, D6508

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.TECH II - SEMESTER EXAMINATIONS, APRIL/MAY 2012
NETWORK SECURITY AND CRYPTOGRAPHY
(COMMON TO COMMUNICATION SYSTEMS, DIGITAL ELECTRONICS & COMMUNICATION SYSTEMS, ELECTRONICS & COMMUNICATION ENGINEERING, EMBEDDED SYSTEMS, WIRELESS & MOBILE COMMUNICATIONS)

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

Answer any five questions
All questions carry equal marks

\- - -

1.a) What are the essential ingredients of symmetric cipher? Explain.
b) Give a brief account on Security attacks.

2. Explain DES encryption algorithm with a neat diagram.

3.a) Give a brief account on key distribution for symmetric encryption.
b) Explain Fermat's theorem with an example.

4.a) Explain the compression function of SHA algorithm with a neat diagram.
b) What is the difference between direct and arbitrated digital signature?

5.a) Explain the role of Authentication server (AS) and Ticket-granting server (TGS) in Kerberos.
b) Write short notes on S/MIME.

6.a) Write notes on IPSec document.
b) What are the basic approaches to building SAs?

7.a) What are the requirements of SET?
b) What steps are involved in the SSL Record Protocol transmission?

8.a) List and briefly define three classes of intruders.
b) Write short notes on circuit-level gateway.

****