R09

Code No: D0509, D5809, D4003

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M.TECH II - SEMESTER EXAMINATIONS, APRIL/MAY 2012

INFORMATION SECURITY

(COMMON TO COMPUTER SCIENCE, COMPUTER SCIENCE & ENGINEERING, INFORMATION TECHNOLOGY)

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

Answer any five questions

All questions carry equal marks

- - -

1.a) Explain the model for Network Security.

b) What are the different types of Security Attacks? Give the mechanisms to counter them.

2.a) Explain DES Algorithm, and security of its s-boxes.

b) Show that Inverse of DES algorithm is again DES.

3.a) Explain the RSA Algorithm Completely.

b) In a public key system using RSA, you intercept the cipher text c=10 sent to a user whose public key is e=5, n=35. What is the plaintext M?

4. Explain SHA-512 Message Digest Algorithm with a flow diagram. Also explain the intermediate results.

5. Explain X.509 Authentication Service. Give the format for PKI certificates.

6. Explain SSL Security in detail. How is it used in practical applications?

7.a) What is Virus and specify different types of viruses?

b) Explain different types of Firewall Configurations.

8. Explain the following.

(a) ELGAMAL

(b) Pretty Good Privacy

(c) SNMP

(d) CBC mode.

****