NR

Code No: B5803, B7707

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.TECH II - SEMESTER EXAMINATIONS, APRIL/MAY 2012
NETWORK SECURITY AND CRYPTOGRAPHY
(COMMON TO COMPUTER SCIENCE AND ENGINEERING, EMBEDDED SYSTEMS & VLSI DESIGN)

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

Answer any five questions
All questions carry equal marks

\- - -

1.a) Explain various Security mechanisms.
b) Explain the following ciphers along with examples
(i) Hill Cipher
(ii) One-Time Pad.

2.a) Explain Conventional Encryption model.
b) Explain Block Cipher modes of operation.

3.a) Discuss Trusted systems.
b) List the design principles of firewalls.

4.a) Explain about Traffic Confidentiality.
b) Compare Secret Key, Private Key, Public Key.

5. Explain RSA Algorithm.

6.a) Prove Euler's Theorem.
b) Explain Security of MACs.

7.a) Explain RIPEMD-160 Algorithm.
b) Write a note on digital signature standards.

8a) Explain OAKLEY key management protocol.
b) Describe secure electronic transaction.

****