

R09

Code No: C6809

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M.TECH I SEMESTER EXAMINATIONS, APRIL/MAY-2012
NETWORK SECURITY AND CRYPTOGRAPHY
(VLSI & EMBEDDED SYSTEMS)**

Time: 3hours

Max.Marks:60

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

- - -

- 1.a) Give the model of conventional crypto system and explain the function of each element.
- b) Explain Transposition and Substitution techniques.
2. Explain DES Encryption and Decryption algorithms in detail.
- 3.a) List out the characteristics of advanced symmetric block ciphers.
- b) Explain Blow fish encryption algorithm.
- 4.a) State and prove Fermat's and Euler's theorems.
- b) Write a brief note on discrete algorithms.
- 5.a) List out the authentication requirements and functions.
- b) What is Hash function? What are its basic uses?
- 6.a) Explain MD-5 Message digest algorithm.
- b) Explain various functions of PGP.
- 7.a) What are the requirements of web security?
- b) Explain requirements and key features of secure electronic transaction.
- 8.a) Explain Rule-based Intrusion detection technique.
- b) Explain various types of viruses and its counter measures.
