Code No.: ETIT 412	**L**	**T**	**C**
Paper: Network Security	**3**	**1**	**4**

INSTRUCTIONS TO PAPER SETTERS: **MAXIMUM MARKS: 75**

1. Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 25 marks.
2. Apart from question no. 1, rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be of 12.5 marks.

UNIT – I

Introduction: Codes and Ciphers – Some Classifical systems – Statistical theory of cipher systems – Complexity theory of Crypto systems – Stream ciphers, Block ciphers.

Stream Ciphers: Rotor based system – shift register based systems – Design considerations for stream ciphers – Cryptanalysis of stream ciphers – Combined eneryption and encoding.

Block Ciphers – DES and variant, modes of use of DES. **[No. of Hrs.: 11]**

UNIT – II

Public Key systems – Knacksack systems – RSK – Diffle Hellman Exchange 0 Authentication and Digital signatures, Elliptic curve based systems.

System Identification and clustering

Cryptology of speech signals – narrow band and wide band systems – analogue & digital systems of speech encryption. **[No. of Hrs.: 11]**

UNIT – III

Network Security: Hash function – Authentication:

Protocols – Digital Signature standards.
Electronics Mail Security – PGP (Pretty Good Privacy) MIME, Data Compression technique.
IP Security: Architecture, Authentication Leader, Encapsulating security Payload – Key management.
Web Security: Secure Socket Layer & Transport Layer security, Secure electronic transactions.
Firewalls Design principle, established systems. **[No. of Hrs.: 12]**

UNIT – IV

Telecommunication Network architecture, TMN management layers, Management information Model, Management servicing and functions, Structure of management information and TMN information model. **[No. of Hrs.: 10]**

TEXT BOOKS:

1. William Stallings, “Network Security Essentials, 2nd Edition, 2002.
2. William Stallings, “Cryptography & Network Security”, 3rd Edition, 1999.