

| | | |
|---|---|---|
| L | T | P |
| 3 | 1 | - |

Class Work: 50

Exam: 100

Total: 150

Duration of Exam: 3 Hrs.

NOTE: For setting up the question paper, question no 1 will be set up from all the four sections which will be compulsory and of short answer type. Two questions will be set from each of the four sections. The students have to attempt first common question, which is compulsory, and one question from each of the four sections. Thus students will have to attempt 5 questions out of 9 questions.

Section A

Introduction: Codes and Ciphers – Some Classical 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 encryption and encoding. Block Ciphers – DES and variant, modes of use of DES.

Section B

Public key systems – Knapsack systems – RSK – Diffie Hellman Exchange – 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.

Section C

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 electronics transactions. Firewalls Design principle, established systems.

Section D

Telecommunication Network Architecture, TMN management layers, Management information Model, Management servicing and functions, Structure of management information and TMN information model, SNMP v1, SNMP2 & SNMP3, RMON1 & 2, Broadband Network Management (ATM, HFC, DSL), ASN

Text Books:

1. Cryptography and Network Security: Principal & Practices, 2nd Edition by Upper Saddle River, PHI
2. Network Management Principles & Practices by Subramanian, Mani (AWL)
3. SNMP, Stalling, Willian (AWL)

Reference Books:

1. SNMP: A Guide to Network Management (MGH)
2. Telecom Network Management by H.H. Wang (MGH)
3. Network Management by U. Dlack (MGH)