Paper Code: BCA 314 | **L** | **T** | **C**
Paper Id: 20314 | **3** | **1** | **4**
Paper: Computer Network & Information Security

Pre-requisite: Basic knowledge of Computer networks and various network protocols
Aim: The aim of this course is to provide an overview of information security and network security and management.
Objectives

- The course covers a broad range of security related concepts and issues that face industries today.
- The course will also examine the practical aspects of the issues involved in secure systems and networks and industry practices being adopted to protect information systems.
- Students will gain the knowledge, skills and abilities to incorporate good information security practice in any organization.

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 12.5 marks

Unit I
Information security
Attributes of Information Security: Confidentiality, Integrity, Availability. Threats & Vulnerabilities: Unauthorized Access, Impersonation, Denial of Service, Malicious Software; Trap Doors, Logic Bomb, Trojan Horses; Viruses, Worms & Bacteria; Cryptography Basics: Plain Text, Cipher Text, Encryption Algorithm, Decryption Algorithm; Requirements for Cryptography, Symmetric vs Asymmetric, Block and Stream ciphers, DES. T[1], T[2]

Unit – II
Public Key Infrastructure &. Message Authentication
Public Key Cryptography Principles & Applications, Algorithms: RSA, Message Authentication: One way Hash Functions: Message Digest, MD5, SHA1. Public Key Infrastructure: Digital Signatures, Digital Certificates, Certificate Authorities. T[1], T[2]

Unit-III
Network Security
Network Attacks: Buffer Overflow, IP Spoofing, TCP Session Hijacking, Sequence Guessing, Network Scanning: ICMP, TCP sweeps, Basic Port Scans; Denial of Service Attacks: SYN Flood, Teardrop attacks, land, Smurf Attacks.
IP security Architecture: Overview, Authentication header, Encapsulating Security Pay Load, combining Security Associations, Key Management. Virtual Private Network Technology: Tunneling using IPSEC. T[1], T[2]

Unit – IV
Web Security
Requirements, Secure Socket Layer, and Secure Electronic Transactions,
Network Management Security: Overview of SNMP Architecture- SNMPV1, SNMPV3.
Firewall Characteristics & Design Principles, Types of Firewalls: Packet Filtering Router, Application Level Gateway or Proxy, Content Filters, Bastion Host. T[1], T[2]