Computer Networks

Unit - I

Introduction – Uses – Network Hardware and Software – Reference models – Network standards - OSI reference models: Physical layer: Theoretical basis – Wireless transmission – Communication satellites – Mobile telephone system.

(Chapters: 1.1 to 1.4, 1.6, 2.1, 2.3 to 2.4, 2.6)

Unit – II

Data link layer: Design Issues - Error Detection and Correction - Elementary protocol – Sliding window protocols – Protocol verification. MAC sub layer: Channel allocation – multiple access protocol.

(Chapters: 3.1 to 3.5, 4.1 to 4.2)

Unit – III

Network Layer: Design Issues –Network Layer in the Internet. Transport Layer: Services – Internet transport protocol – Performance Issues: Application Layer: DNS – WWW: Architectural overview – Static and dynamic web documents - Security: Cryptography – Symmetric key and Public key algorithms.

(Chapters: 5.1, 5.6, 6.1, 6.4 to 6.5)

Unit – IV

TCP / IP: Introduction to Network Layer - IPv4 Addresses - Delivery and Forwarding of IP – Packets - Internet Protocol Version 4 (IPv4) - Mobile IP - Unicast Routing Protocols (RIP, OSPF and BGP) - Multicasting and Multicast Routing Protocol. Transport layer: Introduction to the Transport Layer - User Datagram Protocol (UDP) - Transmission Control Protocol (TCP)

(Chapters: 4 – 8, 11 - 15)

Unit – V

Application layer: Introduction – Host configuration – DNS – Remote login – File transfer – Network management. Next generation: IPV6 addressing – protocol – ICMVP6.

(Chapters: 17-21, 24, 26 - 28)

**Text Book**

1. Andrew S Tanenbaum, “Computer Networks”, Fourth Edition, PHI Private Limited, 2005. (Unit I – III)
2. [Behrouz Forouzan](http://www.tatamcgrawhill.com/cgi-bin/same_author.pl?author=Behrouz+Forouzan), TCP/IP Protocol Suite, Fourth Edition, TMGH, 2010

(Unit IV and V)

**Reference Books:**

1. Uyless Black, Computer Networks, Second Edition, PHI, 2005

2. B.A. Forouzan, “Data Communication and Networking”, Third Edition,

Tata McGraw Hill, 2004.

3. Vivek Acharya, TCP / IP and Distributed system, Firewall media 2006

Computer Graphics

Unit I

Overview: Video display devices – Raster and Random scan system – Input devices Output primitives: Points and Lines – Line drawing algorithms – Loading the frame buffer – Line function.

Unit II

Circle generating and Ellipse generating algorithm Pixel addressing and object geometry – Filled area primitives – Fill area function – Cell array – Character generation. Attributes of output primitives: Line attributes – Color and Grayscale levels – Area fill and Character attributes – Antialiasing. 2D Geometric transformations: Basic transformations – Composite – Reflection and Shear – Transformations between Coordinate systems.

Unit III

Affine transformations – Functions – Raster methods 2D Viewing: Viewing Pipeline – Coordinate reference frame – Window to Viewport – Viewing functions – Clipping operations – Line, Polygon, Text and Exterior clipping – GUI and Interactive input methods: User dialogue – Input of Graphical data – Input functions – Initial value – Picture construction – Virtual reality environments..

Unit IV

3D Concepts: Display methods Object Representations – Polygon surface – Curved lines and surface – Quadratic – Spline representation. 3D Geometric and Modeling transformations: Translation – Rotation – Scaling – Reflections – Shears – Composite transformations – functions. 3D Viewing: Pipeline – Coordinates – Projections – Clipping – Functions..

Unit V

Visible surface detection methods: Classification – Back face – Depth buffer – A buffer – Depth sorting – BSP – Area subdivision – Octree – Ray casting Color models and Applications: Properties of light – Standard primaries and Chromaticity diagram – RGB, YIQ, CMY, and HSV color models. Computer animations: Design – functions – Raster animations – Key frame systems – Motion specifications.

**Text Book**

1. Donald Hearn M. Pauline Baker, “Computer Graphics”, Second Edition, PHI Private Limited, 2004.

(Chapters: 2.1- 2.3, 2.5, 3.1 - 3.6, 3.10 - 3.14, 4.1, 4.3 - 4.5, 4.8, 5.1, 5.3 - 5.8, 6.1 - 6.8, 6.10 – 6.11, 8.1 – 8.6, 9.1, 10.1 – 10.3, 10.6, 11.1 – 11.6, 12.1 – 12.3, 12.5, 12.7, 13.1 – 13.10, 15.1 – 15.2, 15.4 – 15.7, 16.1 – 16.3, 16.5 – 16.6)

**Reference Books:**

1. F.S Hill, JR, “Computer Graphics using Open GL”, Second Edition, PHI, 2005

2. R.G.S Asthana, N. K. Sinha, “Computer Graphics for Scientists and Engineers” Second Edition, New Age international Publishers, 2003

**NETWORK SECURITY**

Unit - I

Introduction: Primer on Networking-Active vs. Passive Attacks- Layers and Cryptography – Authentication – Viruses, Worms, Trojan Horses – The Multi-level Model of security – Legal Issues. Cryptography: Introduction to cryptography: What is cryptography- Breaking an Encryption Scheme – Types of Cryptographic Functions – Secret Key Cryptography – Public Key Cryptography – Hash Algorithms. Security Key Cryptography: Generic Block Encryption – Data Encryption Standard (DES).

Chapters: 1.5 to 1.8, 1.12 to 1.14, 2.1 to 2.6

Unit - II

Security Key Cryptography: Generic Block Encryption – Data Encryption Standard (DES) -International Data Encryption Algorithm (IDEA) – Advanced Encryption Standard (AES). Mode of Operation: Encrypting a Large Message – Generating MACs – Multiple Encryption DES. Public Key Algorithm: Introduction - Modular Arithmetic – RSA –Diffie-Hellman – Digital Signature Standards (DSS) - Elliptic Curve Cryptography (ECC) - Zero Knowledge Proof System.

Chapters: 3.2 to 3.5, 4.2 to 4.4, 6.1 to 6.5, 6.7, 6.8

Unit - III

Authentication: Password-Based Authentication – Address-Based Authentication – Cryptographic Authentication Protocols –– Passwords as Cryptographic Keys – Eavesdropping and Server Database Reading – Trusted Intermediaries – Session Key Establishment – Delegation. Authentication of People: Password – On-Line Password Guessing - Off-Line Password Guessing –– Eavesdropping – Initial Password Distribution – Authentication Tokens – Physical Access – Biometrics. Security Handshake Pitfalls: Login Only – Mutual Authentication – Integrity/Encryption for Data – Mediated Authentication (with KDC) –Nonce Types – Picking Random Numbers – Performance Consideration – Authentication Protocol Checklist.

Chapters: 9.1 to 9.3, 9.5 to 9.7, 10.1 to 10.3, 10.5, 10.7 to 10.10, 11.1 to 11.3

Unit - IV

Mediated Authentication (with KDC) –Nonce Types – Picking Random Numbers – Performance Consideration – Authentication Protocol Checklist. Standards: Kerberos V4: Introduction – Tickets and Ticket-Granting Tickets – Configuration – Logging Into the Network. Kerberos V5: ASN.1 – Names – Delegation of Rights – Ticket Lifetimes – Key Versions – Making Master Keys in Different Realms Different – Optimizations – Cryptographic Algorithms. Real time Communication Security: Session Key Establishment – Perfect Forward Secrecy – PFS Foilage – Denial of Service/Clogging Protection – Endpoint Identifier Hiding – Live Partner Reassurance – Arranging for Parallel Computation – Session Resumption –Plausible Deniability – Data Stream Protection – Negotiation Crypto Parameters.

Chapters: 11.4 to 11.8, 13.1 to 13.4, 14.1 to 14.8, 16.2 to 16.12

Unit - V

Electronic Mail Security: Distribution Lists – Store and Forward –Security Services for Electronic Mail – Establishing Keys – Privacy – Authentication of Source – Message Integrity – Non-Repudiation – Proof of Submission – Proof of Delivery – Anonymity – Containment – Annoying Text Format Issues – Names and Addresses – Verifying When a Message Was Really Sent. Firewalls: Packet Filters – Application Level Gateway – Encrypted Tunnels – Comparisons – Why Firewalls Don’t Work – Denial-of-Service Attacks – Web Issues: Introduction – URLs/URIs – HTTP – HTTP Digest Authentication – Cookies – Other Web Security Problems.

Chapters: 20.1 to 20.10, 20.12 to 20.16, 23.1 to 23.6, 25.1 to 25.6.

Text Book:

1. Charlie Kaufman, Radia Perlman, Mike Speciner, “NETWORK SECURITY Private Communication in a PUBLIC World”, Second Edition, 2005, Prentice-Hall of India Pvt,Ltd.

Reference Books:

1. William Stallings, “CRYPTOGRAPHY AND NETWORK SECURITY Principles and Practice”,Fifth Edition, 2007, Prentice-Hall of India Pvt, Ltd.
2. **William Stallings,**“NETWORK SECURITY ESSENTIALS”,Third Edition, 2007, Prentice-Hall of India Pvt, Ltd.