SavitribaiPhule Pune University
T.Y.B.Sc. (Computer Science) Sem - V
Course Code: DSEC - I Course Code : CS - 352
Course Title :Computer Networks - II

Teaching Scheme	No. of Credits	Examination Scheme
03 Lect/ week	2	IE :15 marks UE: 35 marks

Prerequisites:
Prerequisites: Basic knowledge of Networking and ISO/OSI model

Course Objectives

- To understand different protocols of application layer.
- To understand concepts of multimedia.
- Explore the different methods used for Network/INTERNET security.

Course Outcomes

On completion of the course, student will be able to–

- Student will understand the different protocols of Application layer.
- Develop understanding of technical aspect of Multimedia Systems
- Develop various Multimedia Systems applicable in real time.
- Identify information security goals.
- Understand, compare and apply cryptographic techniques for data security.

Course Contents

Chapter 1	**Application Layer**	**10 Lect**

Domain Name System

- Name space-Flat name space, Hierarchical name space
- Domain Name Space -Label ,Domain name, FQDN,PQDN
- Distribution of Domain Name Space-Hierarchy of name servers, zone, Root server, Primary and secondary servers.
- DNS in the Internet: Generic domains, Country domains,inverse domain
- Resolution-Resolver,mapping names to address,mapping addresses to names,recursive resolution,iterative resolution,caching

Electronic Mail-

- Architecture-First scenario, second scenario, Third scenario, Fourth scenario
- User agent-services of user agent, types of UA Format of e-mail
- MIME-MIME header
- Message transfer agent-SMTP
- Message Access Agent: POP and IMAP

File Transfer

FTP-Communication over data control connection,File type,data structure,Transmission mode,anonymous FTP

Chapter 2	**Multimedia**	**08 Lect**

Digitizing audio and video, Audio and Video compression

Streaming Stored audio/video

- First approach
- Second approach
- Third approach
- Fourth approach

Streaming live audio/video

Real time interactive audio/video- Characteristics, Time relationship, timestamp, Playback buffer, ordering multicasting, translation

RTP-Packet format

RTCP-Message types

Voice over IP-SIP,SIP sessionH.323-

Architecture, Protocols

Chapter 3	**Cryptography and Network Security**	**09 Lect**

Terminology: Cryptography, plain text and cipher text, cipher key, categories of cryptography-Symmetric key, asymmetric key

Encryption model

Symmetric key cryptography

- Traditional ciphers – substitution cipher, shift cipher, Transposition cipher
- Simple Modern ciphers-XOR, Rotation cipher, s-box,p-box
- Modern round ciphers-DES
- Mode of operation-ECB,CBC,CFB,OFB

Asymmetric key cryptography-RSA

Security Services

- Message confidentiality-With Symmetric key cryptography, with asymmetric key cryptography
- Message integrity-Document and fingerprint, message and message digest
- Message authentication-MAC,HMAC
- Digital signature
- Entity Authentication-Passwords, Fixed passwords challenge-response

Chapter 4	**Security in the Internet**	**09 Lect**

IPSecurity(IPSec)

- Two modes
- Two security protocols
- Services provided by IPSec
- Security association
- Internet key exchange
- Virtual private network

SSL/TLS

- SSL services
- Security parameters
- Sessions and connections
- Four protocols
- Transport layer security

PGP

- Security parameters
- Services
- PGP algorithms
- Key rings
- PGP certificates

Firewalls

- Packet filter firewall
- Proxy firewall

Reference Books:

1. Data communications and networking by Behrouz Forouzan 4th/5th edition, McGraw Hill Pvt Ltd.
2. Computer Networks by Andrew S Tanenbaum, 4th/5th edition, Pearson Education
3. Cryptography and Network Security: Principles and Practice, William Stallings, 7th edition, Pearson Education
4. Network Security Essentials: Applications and Standards (For VTU), William Stallings, 3rd edition, Pearson Education