

## **MS-101: MICROPROCESSOR ARCHITECTURE & ASSEMBLY LANGUAGE PROGRAMMING**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT-I**

Microprocessors, Microcomputers, and Assembly Language, The 8085 Programming Model, Instruction, Data Format, and Storage, 8085 Microprocessor Architecture and its operation, Microprocessor initiated operation, Bus organization of 8085, Registers, Memory unit of 8085, Instruction decoding & execution, 8085-Based single board Microcomputer, Pin out Diagram of 8085, Bus timings, ALU of 8085 and its flags.

### **UNIT-II**

Instruction set of 8085, Classification of Instructions, Addressing Modes, Data transfer operation commands, Arithmetic operation commands, Logic operation commands, Branch operation commands, Writing and debugging simple assembly Language Program, developing assembly Language Program, Writing programs using an assembler, Branching looping and Indexing. Programming Techniques, Looping, Counting and Indexing, Additional Data Transfer and 16-Bit Arithmetic Instructions, Arithmetic Operations Related to Memory, Logic Operations: Rotate, Logic Operations: Compare, Dynamic Debugging

### **UNIT-III**

Counters and Time Delays, Stack, Subroutine, Restart, Conditional Call, and Return Instructions, Advanced instructions - LHLD, SHLD, XCHG, PUSH, POP, XTHL, PCHL, Assembly Programs of addition, subtraction, multiplication and division of multi byte signed and unsigned numbers, Interrupts, Microprocessor-Based Software Development Systems, Operating Systems and Programming Tools, Assemblers and Cross-Assemblers, Writing Programs Using a Cross-Assembler.

### **UNIT – IV**

I/O device, Interfacing devices, I/O ports, 8255 programmable peripherals interfacing, Basic Interfacing concepts, Interfacing output display, Interfacing input key board, Memory mapped I/O, I/O mapped I/O, Data Transfer (synchronize and asynchronies), 8085 Interrupts (Hardware and Software), 8085 Vectored Interrupts

### **UNIT-V**

Basic Concepts in Programmable Devices, 8253 programmable interfacing timer, DMA (Direct memory Access), DMA Controller, Extending 8-Bit Microprocessor Concepts to Higher Level Processors and Microcontrollers, 16-Bit Microprocessors, BASICS OF 8086, High-End-High-Performance Processors, Single-Chip Microcontrollers

### **TEXT & REFERENCE BOOKS :**

- MICROPROCESSOR ARCHITECTURE, PROGRAMMING & APPLICATIONS WITH 8085. RAMESH GAONKAR, PENRAM PUBLISHING LTD.
- MICROPROCESSORS AND INTERFACING BY D.V. HALL TMH, 2ND EDITION.
- IBM PC ASSEMBLY LANGUAGE PROGRAMMING BY PETER ABLE, PHI

## **MS-102: OPERATING SYSTEM DESIGN PRINCIPLES**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT– I**

Definitions, Components and types of Operating system, Operating System Services, System Calls, System Programs, System Structure, System Design and Implementation, System Generations. I/O subsystem Overview, I/O hardware, Application I/O interface, Kernel I/O Subsystem.

### **UNIT–II**

Process Concepts, Process State & Process Control Block, Process Scheduling, Scheduling Criteria, Scheduling Algorithms, Multiple-Processor Scheduling, Real-Time Scheduling, Threads Introduction

### **UNIT–III**

The Critical Sections Problem, Semaphores, Classical Problem of Synchronization, Deadlock Characterizations, Method for Handling Deadlocks, Deadlock Prevention, Deadlock Avoidance, Deadlock Detection, Recovery from Deadlock, Combined Approach to Deadlock.

### **UNIT–IV**

Storage management Logical Versus Physical Address Space, Swapping, Contiguous Allocating, Paging, Segmentation, Virtual Memory, Demand Paging, Performance of Demand Paging, Page Replacement, Page Replacement Algorithms, Thrashing, Demand Segmentation.

### **UNIT–V**

Disk Scheduling, Disk Management, Swap Space Management, Disk Reliability, Stable Storage Implementation, File Concepts, Directory Structure, Protecting, File system in Linux & Windows NT

### **TEXT & REFERENCE BOOKS :**

- OPERATING SYSTEM CONCEPTS By SILBERSCHATZ & GALVIN, ADDISON WESLEY PUBLICATION 6th Edition.
- OPERATING SYSTEM CONCEPTS & DESIGN By MILAN MILEN KOVIC, TMH PUBLICATION
- OPERATING SYSTEMS By WILLIAM STALLINGS

## **MS-103: FUNDAMENTALS OF INFORMATION SECURITY**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT-I**

Basics of Communication Systems- Computer Networks types, Transmission Media, Network Topology, Network Protocols, ISO/OSI and TCP/IP Protocol Stacks, Local Area Networks, Wide Area Networks, Internetworking, LAN, WAN and Wireless Networks , The Internet.

### **UNIT-II**

What is Network Security, Security Services, Security Standards, Elements of Security, Security Threats to Computer Networks, Sources of Security Threats, Security Threat Motives, Security Threat Management, Computer Network Vulnerabilities, Sources of Vulnerabilities, Vulnerability assessment, Computer Viruses, Types of viruses, prevention and protection mechanisms-scanning, filtering and blocking, Virus filtering, Contents filtering, Spam,

### **UNIT-III**

Cyber Crimes and hackers, Dealing with Cyber crimes, Hostile scripts, Security Assessment, Analysis and Assurance, Security Requirements Specifications, Threat Identification, Threat Analysis, Vulnerability Identification and Assessment, Security Certification, Security Monitoring and Auditing, Products and Services.

### **UNIT-IV**

Security Access Control and Authorization—Access Rights, Access Control Systems, Authorization, Types of authorization Systems, Authorization principles, Authorization granularity, web access and authorization, Authentication –Authentication elements, Types of authentication, Authentication methods.

### **UNIT-V**

Cryptography, Definition, Symmetric encryption, Public key encryption, Key Management: Generation, Transportation and Distribution, Public Key Infrastructure, Firewalls, Types of Firewalls, Improving Security through Firewalls.

### **Text Books:**

- Computer Network Security, by Joseph M. Kizza, Publisher: Springer International Edition. 2007
- Computer Security, 2nd. ed. by Dieter Gollmann Publisher: John Wiley & Sons, 2006 ISBN: 0-470-86293-9
- Security in Computing, Fourth Edition Author: Charles P. Pfleeger, Shari Lawrence Publisher: Pearson India
- Cryptography and Network Security Principles and Practices 3rd. ed. by William Stallings Publisher: Pearson Education

## MS\_104: MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

**Max. Marks for theory:60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### UNIT-I

Topics in elementary number theory:  $O$  and  $_$  notations – time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruences: Definitions and properties – linear congruences, residue classes, Euler's phi function – Fermat's Little Theorem – Chinese Remainder Theorem – Applications to factoring – finite fields – quadratic residues and reciprocity: Quadratic residues – Legendre symbol – Jacobi symbol.

### UNIT-II

Simple Cryptosystems: Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric Cryptosystems – Cryptanalysis – Block ciphers –Use of Block Ciphers – Multiple Encryption – Stream Ciphers –Affine cipher – Vigenere, Hill, and Permutation Cipher – Secure Cryptosystem.

### UNIT-III

Public Key Cryptosystems: The idea of public key cryptography – The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem – Bit security of RSA – ElGamal Encryption – Discrete Logarithm – Knapsack problem – Zero-Knowledge Protocols – From Cryptography to Communication Security - Oblivious Transfer.

### UNIT-IV

Primality and Factoring: Pseudoprimes – the rho ( $\rho$ ) method – Format factorization and factor bases – the continued fraction method – the quadratic sieve method.

### UNIT-V

Number Theory and Algebraic Geometry: Elliptic curves – basic facts – elliptic curve cryptosystems – elliptic curve primality test – elliptic curve factorization.

**Note:** Theorem Proofs are excluded for examination but the statements of the theorems and solving problems are included.

### REFERENCES

1. Neal Koblitz, "A Course in Number Theory and Cryptography", 2<sup>nd</sup> Edition, Springer, 2002
2. Johannes A. Buchman, "Introduction to Cryptography", 2<sup>nd</sup> Edition, Springer, 2004.
3. Serge Vaudenay, "Classical Introduction to Cryptography – Applications for Communication Security", Springer, 2006.
4. Victor Shoup, "A Computational Introduction to Number Theory and Algebra", Cambridge University Press, 2005.
5. A. Manezes, P. Van Oorschot and S. Vanstone, "Hand Book of Applied Cryptography", CRC Press, 1996.
6. S.C. Coutinho, "The Mathematics of Ciphers – Number Theory and RSA Cryptography", A.K. Peters, Natick, Massachusetts, 1998.

## **MS-201: INTERNALS OF OPERATING SYSTEMS**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT-I**

Introduction to Kernel - Architecture of the UNIX operating system, System concepts, Data structures. Buffer Cache: Buffer header, Structure of Buffer pool, Reading and writing disk blocks. Files INODES, Structure of a regular file, Directories, Super block, Inode assignment.

### **UNIT-II**

System calls - OPEN, Read, Close, Write, Create, CHMOD, CHOWN, Pipes, Mounting and Unmounting. Process - Layout the system memory, Context, Process control, process creation, signals, Process scheduling, time, clock.

### **UNIT-III**

Inter-Process Communications - Process tracing, System V IPC, Shared Memory, Semaphores. Network Communications - Socket programming: Sockets, descriptors, Connections, Socket elements, Stream and Datagram Sockets.

### **UNIT-IV**

Windows Operating system - versions, Concepts and tools, Windows internals, SystemArchitecture, Requirements and design goals, Operating system model, Architecture overview, Key system components. System mechanisms - Trap dispatching, object manager, Synchronization, System worker threads, Windows global flags, Local procedural calls, Kernel event tracing.

### **UNIT-V**

Windows Management Mechanisms - The registry, Registry usage, Registry data types, Localstructure, Trouble shooting Registry problems, Registry Internals, Services, Applications, Accounts, Service control Manager, Windows Management Instrumentation, Processes, Threads, and Jobs: Process Internals, Flow of create process, Thread Internals, Examining Threadcreation, Thread Scheduling, Job Objects.

### **REFERENCES**

1. Maurice J. Bach, "The Design of the Unix Operating System", Prentice Hall of India, 1991.
2. Mark E. Russinovich and David A. Solomon, "Microsoft® Windows® Internals", 4th Edition, Microsoft Press, 2004.
3. William Stallings, "Operating Systems: Internals and Design Principles", 5th Edition, Prentice Hall, 2005.

## **MS-202: COMPUTER NETWORKS**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT-I**

Users of Computer Network, Network Hardware, Network software, Protocol , Hierarchies, Design issue for the layers, Interfaces and services, connection oriented and connection-less services, service primitives, the relationship of services, to protocols, Reference Models, comparison of OSI and TCP/IP Reference models, Data communication services, SMDS, X.25, Frame Relay, Broadband ISDN, ATM and comparison of services.

### **UNIT-II**

Physical layer, Theoretical Basis for data communication, Bandwidth-limited signals. Maximum Data Rate of a Channel, Transmission media, Magnetic media, Wireless, Transmission, The telephone systems, Narrowband and Broadband ISDN and ATM, communication satellites.

### **UNIT-III**

Data Link layer, Design issues, Services provided to the Network layer, error detection and correction, elementary data link protocols, sliding window protocols, Protocol specification and verification, Case studies, HDLC and the Data link layer in the Internet.

### **UNIT-IV**

Network layer design issues, routing algorithms, the optimality principle, shortest path routing, Flooding, Flow-based Routing, Distance-vector and link-state routing broadcast and Multicast Routing, Congestion control algorithms, general principles of congestion control, Traffic shaping, choke packets, load shedding, jitter control.

### **UNIT-V**

The transport layer, The transport service, Quality of service, Transport service Primitives, Addressing establishing a connection, Releasing a connection, Flow-Control and Buffering, Multiplexing, crash Recovery, The Internet Transport protocols, TCP service model, TCP protocol, TCP segment header, TCP connection management, TCP transmission policy, TCP congestion control, TCP timer management UDP.

### **Text Books:**

1. Computer Networks, third edition, 1997 A.S. Tanenbaum, P.H.I.

### **Reference Books:**

1. Data and Computer Communication 1996 William Stallings, P.H.I

## **MS-203: ADVANCED DATA STRUCTURES AND ALGORITHMS**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT-I**

INTRODUCTION: Basic concepts of OOPs – Templates – Algorithm Analysis – ADT -List (Singly, Doubly and Circular) Implementation - Array, Pointer, Cursor, Implementation

### **UNIT-II**

BASIC DATA STRUCTURES: Stacks and Queues – ADT, Implementation and Applications - Trees – General, Binary, Binary Search, Expression Search, AVL, Splay, B-Trees – Implementations - Tree Traversals.

### **UNIT -III**

ADVANCED DATA STRUCTURES: Set – Implementation – Basic operations on set – Priority Queue – Implementation - Graphs – Directed Graphs – Shortest Path Problem- Undirected Graph - Spanning Trees – Graph Traversals

### **UNIT-IV**

MEMORY MANAGEMENT ; Issues - Managing Equal Sized Blocks – Garbage Collection Algorithms for Equal Sized Blocks - Storage Allocation for Objects with Mixed Sizes - Buddy Systems - Storage Compaction

### **UNIT-V**

SEARCHING, SORTING AND DESIGN TECHNIQUES: Searching Techniques, Sorting – Internal Sorting – Bubble Sort, Insertion Sort, Quick Sort, Heap Sort, Bin Sort, Radix Sort – External Sorting – Merge Sort, Multi-way Merge Sort, Polyphase Sorting - Design Techniques - Divide and Conquer - Dynamic Programming - Greedy Algorithm – Backtracking - Local Search Algorithms

### **REFERENCES :**

1. Mark Allen Weiss, “Data Structures and Algorithm Analysis in C++”, Pearson P
2. Marry E Loomis , Data Structure
3. Aho, Hopcroft, Ullman, “Data Structures and Algorithms”, Pearson Education P
4. Drozdek, Data Structures and algorithm in Java, Cengage (Thomson)
5. Gilberg, Data structures Using C++, Cengage
6. Horowitz, Sahni, Rajasekaran, “Computer Algorithms”, Galgotia,
7. Tanenbaum A.S., Langram Y, Augestien M.J., ”Data Structures using C & C++”, Prentice Hall of India, 2002-

## **MS-204:COMPUTER FORENSICS ANALYSIS AND INVESTIGATIONS**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **Unit-I**

Determining what data to collect and analyze. Addressing data hiding techniques, Hiding partitions, Marking bad cluster, Bit –shifting, using steganography to hide data, Examining encrypted files, Recovering Passwords, Performing Remote Acquisitions, Remote Acquisitions with Runtime Software.

### **Unit-II**

Understanding vector Graphics, Understanding graphics file formats .Lossless and lossy compression. Identifying graphics file fragments, Repairing Damaged Headers, Searching for and carving data from unallocated space. Understanding steganography in graphics files. Using steganalysis tools. Understanding copyright issues with graphics.

### **Unit-III**

Performing live acquisitions, Performing a live acquisition in windows, Developing standard procedures for network forensics, Reviewing network logs. Using network tools, using Unix/Linux tools. Using packet sniffers, examining the honey net projects.

### **Unit-IV**

Exploring the role of email investigation, Exploring the role of client and server in email, Investigating E-mail crimes and violations, Examining E-mail Messages, Viewing E-mail headers, Examining E-mail headers, Examining additional E-mail files. Tracing an e-mail message, Using network E-mail logs, Understanding E-mail servers, Examining Unix e-mail server logs, Examining Microsoft email server logs.

### **Unit-V**

Understanding mobile device forensics, Mobile phone basics, inside mobile devices, inside PDAs, Understanding acquisition procedures for cell phones and mobile devices, Mobile forensics equipment.

### **REFERENCES:**

1. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations", Fourth Edition, Course Technology.
2. Angus M. Marshall, "Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008.



## **MS-301: SECURE SOFTWARE ENGINEERING**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT I**

Problem, Process, and Product - Problems of software practitioners – approach through software reliability engineering- experience with SRE – SRE process – defining the product – Testing acquired software – reliability concepts- software and hardware reliability. Implementing Operational Profiles - Developing, identifying, crating, reviewing the operation – concurrencerate – occurrence probabilities- applying operation profiles

### **UNIT II**

Engineering “Just Right” Reliability - Defining “failure” for the product - Choosing a common measure for all associated systems. - Setting system failure intensity objectives -Determining user needs for reliability and availability., overall reliability and availability objectives, common failure intensity objective., developed software failure intensity objectives. – Engineeringsoftware reliability strategies. Preparing for Test - Preparing test cases. - Planning number of new test cases for current release. -Allocating new test cases. - Distributing new test cases among new operations - Detailing test cases. - Preparing test procedures

### **UNIT III**

Executing Test - Planning and allocating test time for the current release. - Invoking testidentifyingidentifying failures - Analyzing test output for deviations. – Determining which deviations are failures. Establishing when failures occurred. Guiding Test - Tracking reliability growth - Estimating failure intensity. - Using failure intensity patterns to guide test - Certifying reliability. Deploying SRE - Core material - Persuading your boss, your coworkers, and stakeholders. - Executing the deployment - Using a consultant.

### **UNIT IV**

Using UML for Security - UML diagrams for security requirement -security business processphysicalsecurity - security critical interaction - security state. Analyzing Model - Notation - formal semantics - security analysis - important security opportunities. Model based security engineering with UML - UML sec profile- Design principles for secure systems - Applying security patterns

### **UNIT V**

Applications - Secure channel - Developing Secure Java program- more case studies. Toolsupport for UML Sec - Extending UML CASE TOOLS with analysis tools - Automated tools for UML SEC. Formal Foundations - UML machines - Rely guarantee specifications- reasoning about security properties.

## **REFERENCES**

1. John Musa D, “Software Reliability Engineering”, 2nd Edition, Tata McGraw-Hill, 2005 (Units I, II and III)
3. Jan Jürjens, “Secure Systems Development with UML”, Springer; 2004 (Unit IV and V)

## **MS-302: E-COMMERCE SECURITY**

**Max Marks for Theory:60 Internal Assessment :40 (Min., Passing Marks 40% in each)**

### **UNIT-I**

Introduction to E-commerce: Operating System Services, Advantages and Disadvantages of E – Commerce, Developer Services, Data Services, Application Services, Store Services, Client Services, Types of E-Commerce Solutions- Direct Marketing and Selling, Supply Chain Integration, Corporate Procurement.

### **UNIT-II**

Business Models for E-Commerce: E-Business models based on Relationship of Transaction Parties, Brokerage Model, Aggregator Model, Info-mediary model, Community Model, Value chain model, Manufacturer model, Advertising Model, Subscription model, E- Marketing – Identifying Web Presence Goals, Browsing Behaviour Model, Building Customer Relationship Based on One – to – One Marketing, E – branding, Elements of Branding, Spiral Branding.

### **UNIT-III**

Electronic Data Interchange: Evolution, uses, Benefits, Working of EDI, EDI Standards (includes variable length EDI standards), Cost Benefit Analysis of EDI, Electronic Trading Networks, EDI Components, File Types, EDI Services, EDI Software, Business Approach of EDI, EDIFACT (Overview, Structure, EDIFACT Software), Business Future of EDI, EDI Administration. EDI Security, Digital signatures, Digital Certificates, Cryptography export restrictions, Secure Sockets Layer (SSL), Secure Electronic Transactions (SET), Smart Cards and its applications, WAP, WAP Architecture, WAP Programming Model.

### **UNIT-IV**

Electronic Payment Security: Electronic Payment Systems – Electronic Commerce, Offline Versus Online, Debit Versus Credit, Macro versus Micro, Payment Instrument, Electronic Wallet, Smart Cards, Electronic Payment Security. Payment Security Services – Payment Transaction Security, Digital Money Security, Electronic Check Security, Availability and Reliability, Electronic Payment Framework.

### **UNIT-V**

Security on the Web & Mobile : Network and Website Security Risks, HTTP Cache Security Issues, HTTP Client Authentication, Web Transaction Security, Web Server Security, Web Client Security, Mobile Agent Security – mobile Agents, Security Issues, Protecting Platforms from Hostile Agents, Smart Card Security, Firewall Concept, Firewall Components, Benefits of an Internet Firewall, Enterprise-Wide Security Framework, Secure Physical Infrastructure.

### **REFERENCES:**

- 1) E-Commerce: Fundamentals and Applications, Henry Chan, Wiley India
- 2) E-Commerce An Indian Perspective, P.T. Joseph, S.J., PHI.

- 3) Electronic Commerce: Greenstein, Merylin, Tata Mc.Graw Hill.
- 4) E-Commerce Business.Technology. Society, Kenneth C. Laudon, Carol Guerico Traver, Pearson

## **MS-303: DIGITAL FORENSICS & TOOLS**

**Max Marks for Theory:60 Internal Assessment:40 (Min,. Passing Marks 40% in each)**

### **UNIT-I**

Computer forensics and investigations as a profession, Understanding computer forensics, computer forensics versus other related disciplines, A brief History of computer Forensics, Understanding case laws, Developing computer forensics resources, Preparing for computer investigations, Understanding law enforcement agency investigations, Following the legal process, Understanding corporate investigations, Establishing company policies, Displaying warning Banners.

### **UNIT-II**

Windows Systems and Artifacts:Introduction, Windows File Systems, File Allocation Table, New Technology File System, File System Summary, Registry, Event Logs, Prefetch Files, Shortcut Files, Windows Executables.

### **UNIT-III**

Linux Systems and Artifacts:Introduction, Linux File Systems, File System Layer, File Name Layer , Metadata Layer, Data Unit Layer, Journal Tools, Deleted Data, Linux Logical Volume Manager, Linux Boot Process and Services, System V , BSD, Linux System Organization and Artifacts, Partitioning, File system Hierarchy, Ownership and Permissions, File Attributes, Hidden Files, User Accounts , Home Directories, Shell History GNOME Windows Manager Artifacts, Logs, User Activity Logs, Syslog, Command Line Log Processing, Scheduling Tasks.

### **UNIT- IV**

Evaluating Computer Forensics Tool Needs, Types of Computer Forensics Tools, Tasks Performed by Computer Forensics Tools, Tool Comparisons, Other Considerations for Tools, Computer Forensics Software Tools, Command-Line Forensics Tools, UNIX/Linux Forensics Tools, Other GUI Forensics Tools, Computer Forensics Hardware Tools, Forensic Workstations, Using a Write-Blocker.

### **UNIT-V**

Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events: How to Become a Digital Detective, Useable File Formats ,Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime ,Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks ,Router Forensics. Cyber forensics tools and case studies.

### **REFERENCES:**

1. Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Syngress imprint of Elsevier.

2. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations", Fourth Edition, Course Technology.
3. Angus M. Marshall, "Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008.

## **MS-304 :CRYPTOGRAPHY & NETWORK SECURITY**

**Max Marks for Theory:60 Internal Assessment:340 (Min., Passing Marks 40% in each)**

### **UNIT I**

Introduction to Security in Networks – Characteristics of Networks – Intrusion – Kinds of security breaches – Plan of attack - Points of vulnerability – Methods of defense – Control measures – Effectiveness of controls

### **UNIT II**

Basic encryption and decryption – Encryption techniques – Characteristics of good encryption systems – Secret key cryptography – Data Encryption Standard – International Data Encryption Algorithm – Advanced Encryption Standard – Hash and MAC algorithms

### **UNIT III**

Public Key encryptions – Introduction to number theory - RSA algorithm – Diffie-Hellman – Digital Signature standard – Elliptic Curve cryptography - Digital signatures and authentication – Trusted intermediaries – Security handshake pitfalls

### **UNIT IV**

Secure sockets – IPsec overview – IP security architecture – IPsec-Internet Key, Exchanging(IKE) – IKE phases – encoding – Internet security – Threats to privacy – Packet sniffing – Spoofing - Web security requirements – Real Time communication security – Security standards–Kerberos.X.509AuthenticationService.

### **UNIT V**

Security protocols – Transport layer protocols – SSL – Electronic mail security – PEM and S/MIME security protocol – Pretty Good Privacy – Web Security - Firewalls design principles – Trusted systems – Electronic payment protocols. Intrusion detection – password management – Viruses and related Threats – Virus Counter measures, Virtual Private Networks.

### **REFERENCES**

1. William Stallings, "Cryptography and Network Security: Principles and Standards", Prentice Hall India, 3<sup>rd</sup> Edition, 2003.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security: Private Communication in a public world", Prentice Hall India, 2<sup>nd</sup> Edition, 2002.
3. Charles P. Pleeger, "Security in Computing", Pearson Education Asia, 5<sup>th</sup> Edition, 2001.
4. William Stallings, "Network Security Essentials: Applications and standards", Person Education Asia, 2000.

## **MS-401:ETHICAL HACKING**

**Max. Marks for theory: 60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT I**

Casing the Establishment - What is footprinting- Internet Footprinting. -Scanning-Enumeration - basic banner grabbing, Enumerating Common Network services. Case study- Network Security Monitoring

### **UNIT II**

Securing permission - Securing file and folder permission. Using the encrypting file system. Securing registry permissions. Securing service- Managing service permission. Default services in windows 2000 and windows XP. Unix - The Quest for Root. Remote Access vs Local access. Remote access. Local access. After hacking root.

### **UNIT III**

Dial-up ,PBX, Voicemail, and VPN hacking - Preparing to dial up. War-Dialing. Brute-Force Scripting PBX hacking. Voice mail hacking . VPN hacking. Network Devices – Discovery,Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability.  
Detecting Layer 2 Media.

### **UNIT IV**

Wireless Hacking - Wireless Footprinting. Wireless Scanning and Enumeration. Gaining Access. Tools that exploiting WEP Weakness. Denial of Services Attacks. Firewalls- Firewallslandscape- Firewall Identification-Scanning Through firewalls- packet Filtering- Application Proxy Vulnerabilities . Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS

### **UNIT V**

Remote Control Insecurities - Discovering Remote Control Software. Connection.Weakness.VNC . Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans. Cryptography . Subverting the systems Environment. Social Engineering. Web Hacking. Web server hacking web application hacking. Hacking the internet User - Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.

### **REFERENCES:**

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.
2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.

## **MS-402 : CYBER LAWS AND INFORMATION SECURITY**

**Max. Marks for theory:60 Internal Assessment: 40 (Min Passing Marks 40% in each)**

### **UNIT-I**

**Cyber Law:** Fundamentals of Cyber Law, History of Internet, Introduction to Indian Cyber Law, Need for Cyber Laws, Jurisprudence of Cyber Law, Objective and Scope of the IT Act 2000, UNCITRAL Model Law, Intellectual property issues, Overview of Intellectual property related legislation in India Rationale behind Intellectual Property, Underlying premises of IP, Balancing the Rights of the Owner of the IP and the Society, Enforcement of IPRS, IP and Constitution of India Patent, The Patent System, Patentable Invention?, Non-patentable, Procedure for Obtaining Patent, Copyright, Trademark law, Law related to semiconductor layout and design.

### **UNIT-II**

**Security in E-Commerce:** E-Commerce Issues of privacy, Security Threats to E – Commerce, Physical Security: Incidents of Physical Security Violations, Disaster and Controls, Basic Tenets of Physical Security, Challenges in Ensuring Physical Security, Physical Entry Controls, Steps to Perform after Physical Security Breach; Spyware Technology: Lock Down USB Ports, Device Lock, Tracking Device; Access Control: Biometrics, Benefits, Criteria for selection of Biometrics, Interoperability Issues, Economic and Social Aspects, Legal Challenges; Digital Signatures: Requirements of Digital Signature System, Components of Digital Signature, Technical issues, Legal issues, Electronic Records, Digital Certificates, Applications of Digital Signatures; Certificate Issuance, Cardholder Certificates, Trader Certificates, Acquirer and Issuer Certificates

### **UNIT-III**

**Investigation and Ethics:** Cyber crime, Cyber resource Theft, types of cyber crimes/frauds, cyber frauds in India, Cyber jurisdiction, dealing with cyber crimes in various countries, Ethical issues in data and software privacy, Plagiarism, pornography, Tampering computer documents/system hacking, Data privacy and protection, software piracy, social engineering and Phishing, Types of social engineering, exploring methods of phishing; Issues in ethical hacking, Internet security threats: Hacking and Cracking, Malicious code, Viruses, Worms, Trojan Horses; certifying authorities need and power, appointment function, generation, suspension and revocation of certifying authorities; cyber crime forensic.

### **UNIT-IV**

**Information Security:** Information system, Information Systems, Computer Literacy and IS Literacy, IS Components, Trends in IS, Classification of IS Framework of IS in an Organization, IS and Business Organisation, Human Body as an Information System, IS Failures and Causes,

Developing Information System, introduction to various models, Role of security in internet and web services, securing web services, principles of information security, ISMS and its benefits, classification of Threats and attacks,, Security Implication for organizations, Information classification and their roles, access control, authentication of hosts, vulnerability, stages of vulnerability management.

### **UNIT-V**

**Cryptography:** Understanding Cryptography and Encryption, Private Key Encryption, Public Key Encryption, Secret-Key Encryption, Understanding Cryptographic Algorithms: MD5, SHA,RC4, RC5, Blowfish, Understanding Cryptanalysis, Describing Code Breaking Methodologies, Describing Cryptographic Attacks, Firewalls Types of Firewall Techniques, How to Identify a Firewall, Issues in Documents Security, Basic concepts of Network Security, Sniffing, Sniffing Objectives, Protecting from Sniffing Attacks, Perimeters of Network protection and Network attack, Scoping an Attack, Enumerating Network, Querying Registrar, Querying Domain, Querying Network, Interrogating DNS, Exploring Network Reconnaissance, Common Attacks: Wiretaps, Eavesdropping, Portscan, Need of Intrusion Monitoring and Detection Network-based IDS Host-based IDS, Honeypot Types and Placement, VPN: Insecure Storage of Authentication Credentials by VPN Clients, VPN Fingerprinting, Username Enumeration Vulnerabilities, Offline Password Cracking, Lack of Account Lockout, Denial of Service Attacks, Benefits, Use of Tunnelling with VPN, Authentication Mechanism, Types of VPN, Security Concerns in VPN.

### **TEXT & REFERENCE BOOKS :**

- Cyber law and information security by Faiyaz Ahamed, Dreamtech Publication.
- Information Security and Cyber laws by Saurabh Sharma, Vikas Publishing House Pvt Ltd.
- Information Security and Cyber laws by Pankaj Sharma, S.K. Kataria and Sons

### **REFERENCES:**

- The Indian Cyber law with Cyber glossary, Suresh T. Vishwanathan, New Delhi, Bhart Law House,2000.
- Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives, Nina Godbole, Sunit Belapure, Wiley India
- Law of Cyber Crimes and Information Technology Law, S.V. Joga Rao, 2007.
- Cyber Law, Cyber Crime Internet and E-Commerce, Vimlendu Tayal.
- Information Technology Law and Practice, Vakul Sharma.

