RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security/Cyber Security, V-Semester

CY501- OS Internals for Security Support

Unit-1: 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, System calls - OPEN, READ, CLOSE, WRITE, CREATE, CHMOD, CHOWN, Pipes, Mounting and Un-mounting.

Unit-2: Process - Layout System Memory, Process Description, Process control, process creation, signals, Process scheduling, Privileges, Threats, intruders, malicious software, time, clock, Principals of Concurrency, Inter-Process Communications - Process tracing, System V IPC, Shared Memory, Semaphores.

Unit-3: Security and Protection in Operating Systems - access control, auditing, trusted computing, Multics and the commercial Operating Systems, Malware analysis, protection-viruses, worms and Trojans, Root-kits, Ransomware, Polymorphic malware, Malware capture and analysis using honey-pots.

Unit-4: Common vulnerabilities and Exposures- Secure system configuration, Virtualization techniques for security, Mobile Operating Systems security, Systems security in Android, Application Security, Secure wallets, secure co-processors.

Unit-5: Windows Operation System - versions, Concepts and tools, Windows internals, System Architecture, System worker threads, Windows global flags, Local procedural calls, Socket, Sockets Programming, Winsock, functions, data structures, descriptors, Connections, Socket elements, Stream and Datagram Sockets.

TEXT BOOKS:
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.

REFERENCES:
1. W. Stallings: "*Operating Systems*: *Internals* and Design Principles", 5th Edition, Prentice Hall, 2005.
2. A. Tanenbaum, A. Woodhull: "Operating Systems Design and Implementation", 3rd Edition, Prentice Hall, 2006.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security/Cyber Security, V-Semester

CY502- Design& Analysis of Algorithms

COURSE OUTCOMES:

After completing the course student should be able to:

1. Describe complexity of an algorithm and various notations to represent it.
2. Apply and evaluate different algorithm design techniques for getting the effective solutions of specified problems.
3. Compare and contrast different graph/tree algorithms with its applications.
4. Explain computability and non-computability and various complexity classes.

Unit I : Definitions of algorithms and complexity, Time and Space Complexity; Time space tradeoff, various bounds on complexity, Asymptotic notation, Recurrences and Recurrences solving techniques, Introduction to divide and conquer technique, example: binary search, merge sort, quick sort, heap sort, strassen's matrix multiplication etc, Code tuning techniques: Loop Optimization, Data Transfer Optimization, Logic Optimization, etc.

Unit II : Greedy Algorithms: strategy, examples of greedy method like optimal merge patterns, Huffman coding, minimum spanning trees, knapsack problem, job sequencing with deadlines, single source shortest path algorithm etc. Correctness proof of Greedy algorithms.

Unit III : Dynamic programming: characteristics, problems based on dynamic programming such as 0/1 knapsack, multistage graph, reliability design, Floyd-Warshall algorithm etc.

Unit IV : Backtracking: concept and its examples like 8 queen's problem, Hamiltonian cycle, Graph colouring problem etc. Introduction to branch & bound method, examples of branch and bound method like travelling salesman problem etc. Meaning of lower bound theory and its use in solving algebraic problem, introduction to parallel algorithms.

Unit V : Advanced tree and graph algorithms, NP-hard and NP-complete problems, Approximations Algorithms, Data Stream Algorithms, Introduction to design and complexity of Parallel Algorithms.

Books Recommended:

1. Cormen, Leiserson, Rivest, Stein, "Introduction to Algorithms", Second Edition, Prentice Hall of India.

2. Aho A.V., Hopcroft J.E., J. Ullman, "Design and Analysis of Computer Algorithms", Addison Wesley.

3. Horowitz E. and Sahani, "Fundamentals of Computer Algorithms", Galgotia Publications.

4. Knuth D., "Fundamental algorithms: The Art of Computer programming", Volume – I, Pearson Education.

5. Knuth D., "Sorting and Searching: The Art of Computer programming", Volume – III, Pearson Education.

6. John Kleinberg, Trades E., "Algorithm Design", Pearson Education.

7. A. Papoulis, S.U. Pillai, "Probability, Random Variables and Stochastic Processes", McGraw Hill.

CY503 (A) – Biometric Techniques for Security

Unit-1: Biometrics- Introduction- benefits of biometrics over traditional authentication systems - benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems.

Unit-2: Physiological Biometric Technologies: Fingerprints - Technical description – characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan - Technical description - characteristics - weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern.

Unit-3: Technical description – characteristics - strengths – weaknesses – deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics. Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics.

Unit-4: signature and handwriting technology - Technical description – classification – keyboard / keystroke dynamics- Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses-deployment.

Unit-5: Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan.

TEXT BOOKS:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : "Biometrics -Identity verification in a network", 1st Edition, Wiley Eastern, 2002.

2. John Chirillo and Scott Blaul : "Implementing Biometric Security", 1st Edition, Wiley Eastern Publication, 2005.

REFERENCES:

1. John Berger: "Biometrics for Network Security", 1st Edition, Prentice Hall, 2004.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security/Cyber Security, V-Semester

CY503 (B) - Network Security

UNIT I:
Review of Cryptography: Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Random and Pseudorandom Numbers, Stream Ciphers and RC4, Cipher Block Modes of Operation, Approaches to Message Authentication, Secure Hash Function, Message Authentication Codes, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures.

UNIT II:
Hardware and Software Security: Hardware Security, Smart Cards, Biometrics, Virtual Private Networks, Types of VPNs, Trusted Operating Systems, Pretty Good Privacy (PGP), Security Protocols, Security Socket Layer, Transport Layer Security, IPSec, S/MIME.

UNIT III:
Intrusion Detection Systemand Firewalls: IDS- Infrastructure of IDS, Classification of IDS, Host-based IDS, Network based IDS, Anomaly v/s Signature Detection, Normal Behavior, Patterns-Anomaly Detection, Misbehaviour Signatures-Signature Detection, Parameter Pattern Matching, Managing an IDS. Malicious Software, Safeguards, Firewalls, Packet-Filtering Firewalls, State full Inspection Firewalls, Proxy firewalls, Guard, Personal Firewalls, Limitations of Firewalls.

UNIT IV:
Wireless Security: Wireless Application Protocol, WAP Security, Authentication, Integrity, Confidentiality, Security Issues with Wireless Transport Layer Security (WTLS), Wireless LAN, WLAN Configuration, WLAN Technology consideration, Wireless LAN Security, Access Point Security, Work Station Security, Safeguarding Wireless LANs.

UNIT V:
Web Security: Client/Server Architecture, Security considerations and Threats, Web traffic security approaches, SSL/TLS for secure web services, The Twin concept of "SSL Connection" and "SSL Session", SSL session state, SSL Connection State, SSL Record Protocol, SSL Handshake Protocol, S-HTTP, Secure Electronic Transaction(SET), Business Requirements, SET Participants, SET Transaction Flow.

Books Recommended:

[1] Network Security Essentials: Applications and Standards, William Stallings, Pearson Education.

[2] Network Security and Management, Brijendra Sing, PHI.

[3] Network Security Bible, Eric Cole, Wiley.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security/Cyber Security, V-Semester

CY503 (C) – Data Security

Unit-1: Introduction: History of Cryptography. Mathematical background: Probability theory - Information theory – Complexity theory, Number theory. Symmetric (Private) Key Cryptographic Systems: Caesar – Aff ine – Monoalphabetic Substitution – Transposition – Homophonic substitution – Vignere – Beauford and DES Family – Product ciphers – Lucifer and DES.

Unit-4: Asymmetric (Public) Key Cryptographic Systems: Concept of PKCS, RSA Cryptosystem- Variants of RSA – Primality testing – Security of RSA – Merkle – Hellamn – Security of Merkle – Hellaman, ElGamal. Elliptical Curve Cryptography.

Unit-3: Stream ciphers and block ciphers: The one time pad – Synchronous stream ciphers – Self-synchronizing stream ciphers – Feedback shift registers – Linear Complexity – Non-linear feedback shift registers – Stream ciphers based LFSRs. Non-linear Combination generators – Non linear filter generators – Clock controlled generators – The alternating step generators – The shrinking generators.

Unit-4: Digital Signatures: Properties, Generic signature schemes – Rabin Lamport – Matyasmeyer, RSA – Multiple RSA and ElGamal Signatures – Digital signature standard – Blind Signatures- RSA Blind.

Unit-5: Secret Sharing Algorithms: Threshold secret sharing – Shamir scheme, Blakley scheme and modular Scheme. Pseudo random number generators: Definition of randomness and pseudo-randomness – Statistical tests of randomness – Linear congruential generator – Modern PRNGs (a brief description).

Reference Book:

1.   Padmanabhan T R, Shyamala C and Harini N, "Cryptography and Security", Wiley Publications 2011.

2.   Josef Pieprzyk, Thomas Hardjono and Jenifer Seberry, "Fundamentals of Computer Security", Springer 2010.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security/Cyber Security, V-Semester

CY 504(A) Cyber Law & Intellectual Property Rights

UNIT - I
Evolution of the IT Act, Genesis and Necessity, Salient features of the IT Act, 2000, Various authorities under IT Act and their powers; Penalties & Offences, Amendments Impact on other related Acts: IPC, Indian Evidence Act, Bankers Book Evidence Act, RBI Act. Cyber Space Jurisdiction: Traditional principals of Jurisdiction, issues under IT Act, 2000, Extra terrestrial Jurisdiction. Cyber Tribunal & Appellate Tribunal, Cyber Regulations, Internet Service Providers and their liabilities.

UNIT - II
E – Commerce and Laws in India, Digital/Electronic Signature in Indian Laws; Issues and provisions in Indian Law related to E-Commerce. E – Governance: Concept and practicality in India, E–Taxation issues in Cyberspace. Cyber crime: Types of cyber crime, Cyber crime under IPC. E – Contracts and its validity in India.

UNIT – III
Indian Evidence Law - Cyber crimes under the Information Technology Act, 2000 - Cyber crimes
under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc.,   Cyber Terrorism, Violation of Privacy on Internet - Data Protection and
Privacy – Indian Court cases.

UNIT - IV
Intellectual Property Rights, Domain Names and Trademark Disputes: Concept of Trademarks in Internet Era, Cyber Squatting, Reverse Hijacking, Jurisdiction in Trademark Disputes, Copyright in the Digital Medium, Copyright in Computer Programmes, Copyright and WIPO Treaties, Concept of Patent Right, Relevant Provisions of Patent Act 1970, Sensitive Personal Data or Information (SPDI) in Cyber Law, SPDI Definition and Reasonable Security Practices in India.

UNIT - V
International Cyber Laws: International Perspective, EDI: Concept and legal Issues, UNCITRAL Model Law, Electronic Signature Laws of Major Countries, Cyber Laws of Major Countries.

Text Books

1. Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co., New Delhi
2. Farouq Ahmed, Cyber Law in India, New Era publications, New Delhi
3. S.R.Myneni: Information Technology Laws (Cyber Laws), Asia Law House, Hyderabad.
4. Chris Reed, Internet Law-Text and Materials, Cambridge University Press.
5. Pawan Duggal: Cyber Law- the Indian perspective, Universal Law Publishing Co., New Delhi.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security/Cyber Security, V-Semester

CY 504(B) Internet of Things

Unit-1: Fundamentals of IoT - Evolution of Internet of Things, Enabling Technologies, IoT Architectures, oneM2M, IoT World Forum (IoTWF) and Alternative IoT models, Simplified IoT Architecture and Core IoT Functional Stack, Fog, Edge and Cloud in IoT, Functional blocks of an IoT ecosystem Sensors, actuators, Smart objects and connecting smart objects.

Unit-2: IoT Protocols - IoT Access Technologies, Physical and MAC layers, topology and Security of IEEE 802.15.4, 802.15.4g, 802.15.4e, 1901.2a, 802.11ah and LoRaWAN, Network Layer, IP versions, Constrained Nodes and Constrained Networks, Optimizing IP for IoT, From 6LoWPAN to 6Lo, Routing over Low Power and Lossy Networks, Application Transport Methods, Supervisory Control and Data Acquisition , Application Layer Protocols, CoAP and MQTT

Unit-3: Design and Development- Design Methodology, Embedded computing logic, Microcontroller, System on Chips, IoT system building blocks, Arduino Board details, IDE programming, Raspberry Pi, Interfaces and Raspberry Pi with Python Programming.

Unit-4: Data Analytics And Supporting Services- structured vs unstructured Data and Data in Motion vs Data in Rest, Role of Machine Learning, No SQL Databases, Hadoop Ecosystem, Apache Kafka, Apache Spark, Edge Streaming Analytics and Network Analytics, Xively Cloud for IoT, Python Web Application Framework, Django AWS for IoT, System Management with NETCONF-YANG

Unit-5: Case Studies/Industrial Applications - Cisco IoT system, IBM Watson IoT platform, Manufacturing, converged plant-wide Ethernet Model (CPwE), Power Utility Industry, Grid-Blocks Reference Model, Smart and Connected Cities: Layered architecture, Smart Lighting, Smart Parking Architecture and Smart Traffic Control

TEXT BOOK:

1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, ―IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, Cisco Press, 2017

REFERENCES:

1. Arshdeep Bahga, Vijay Madisetti, ―Internet of Things – A hands-on approach‖, Universities Press, 2015

2. Olivier Hersent, David Boswarthick, Omar Elloumi , ―The Internet of Things – Key applications and Protocols‖, Wiley, 2012 (for Unit 2).

3. Jan Ho¨ ller, Vlasios Tsiatsis , Catherine Mulligan, Stamatis , Karnouskos, Stefan Avesand. David Boyle, "From Machine-to-Machine to the Internet of Things - Introduction to a New Age of Intelligence", Elsevier, 2014.

4. Dieter Uckelmann, Mark Harrison, Michahelles, Florian (Eds), ―Architecting the Internet of Things‖, Springer, 2011.

5. Michael Margolis, Arduino Cookbook, Recipes to Begin, Expand, and Enhance Your Projects, 2nd Edition, O'Reilly Media, 2011.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security/Cyber Security, V-Semester

CD504 (C) Computer Organization & Architecture

Unit I:
Review of Digital Logic Circuits, Digital Logic Components and Data representation.Computer Arithmetic**:** Integer and Floating Point Arithmetic operations.
Computer Organization v/s Architecture,Milestonesin Computer Architecture, Basic Structure of Computer System, Componentsof Computer System-CPU;Memory;System Bus- Bus width, Bus Operations;I/O subsystem. CPU Organization: General Register Organization-Memory Register, Instruction Register; Control Word, Stack Organization; ALU, Control Unit.

Unit II:
(A) Machine Language Level/Instruction Set Architecture (ISA) level: Instruction Set-Machine Instruction Characteristics, Types of operands, Types of operations**;** Instruction Types, Instruction Formats, Addressing Modes; Registers, Program Counter; Instruction Execution Cycle;Interrupts and Traps, Sources of interrupts, Interrupt identification and priorities, Interrupt servicing.Case Study of 8086 Microprocessor.
(B) Control Unit: Hardwired Control Unit;Micro-programmed Control Unit-Micro Instructions, Micro Instruction Formats, Micro Instruction Control, Micro program sequencer, Execution of Micro Instructions.

Unit III:
Memory Organization: Memory   Hierarchy,   Main memory-RAM, ROM; Memory Technologies; Memory Addresses, Memory Address Map; Flash Memory; Associative Memory, Cache Memory: Cache Structure and Design, Mapping Schemes, Replacement Algorithms, Improving Cache Performance; Concept of L1, L2, L3 Cache.
Secondary Memory –Magnetic Tape, Magnetic Disk, Optical Disks, Solid State Disk.

Unit IV:
I/O Organization: Data Transfer- Serial, Parallel, Synchronous, Asynchronous Modes of Data Transfer, I/O Techniques- Programmed I/O,   Interrupt driven I/O,Direct   Memory Access(DMA); External Interconnection Standards **(**I/O Interfaces): PCI Bus,PCI Express, SCSI Bus, USB; I/O Channels and I/O Processors; I/O Instructions**.**

Unit V:
Parallel Architectures:On-chip parallelism, Thread level parallelism, Instruction level parallelism; Multicore Processor Architecture;Processor level parallelism; Overview of Pipelining, Vector Processing and Array Processing. RISC vs CISC Architectures. Introduction to ARM processor and its architecture. Introduction to Assembly Language Programming.

Books Recommended:

1. William Stallings, "Computer Organization and architecture", Pearson.
2. Tannenbaum and Austin, "Structured Computer Organization", PHI.
3. V. Carl Hamacher, "Computer Organization", McGraw Hill.
4. John P. Hayes, "Computer Architecture and Organization", TMH.
5. Morris Mano, "Computer System Architecture", PHI.
6. David A. Patterson and John L. Hennessy, "Computer Organization and Design: The Hardware/Software Interface", Morgan Kauffman.
7. M. Usha, T.S. Shrikant: "Computer System Architecture and Organization", Willey India.
8. Chaudhuri, P.Pal: "Computer Organization and Design",PHI
9. Sarangi: "Computer Organization and Architecture", McGraw Hill.