JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech. in CYBER FORENSICS & INFORMATION SECURITY / CYBER SECURITY

EFFECTIVE FROM ACADEMIC YEAR 2017- 18 ADMITTED BATCH

COURSE STRUCTURE AND SYLLABUS

I Semester

Category	Course Title	Int. marks	Ext. marks	L	T	P	C
PC-1	Secure Operating System	25	75	4	0	0	4
PC-2	Applied Cryptography	25	75	4	0	0	4
PC-3	Network and Wireless Security	25	75	4	0	0	4
PE-1	1. Database Security 2. Advanced Algorithms 3. Cloud Computing and Security 4. Information Systems Control And Audit	25	75	**3**	0	0	3
PE-2	1. Machine Learning 2. Web Security 3. Distributed Systems 4. Mobile Application Security	25	75	**3**	0	0	3
OE-1	***Open Elective – 1**	25	75	3	0	0	3
Laboratory I	Algorithms and Information Security Lab	25	75	0	0	3	2
Seminar I	Seminar-I	100	0	0	0	3	2
	Total	**275**	**525**	**21**	**0**	**6**	**25**

II Semester

Category	Course Title	Int. marks	Ext. marks	L	T	P	C
PC-4	IT Security-Threats and Vulnerability	25	75	4	0	0	4
PC-5	Ethical Hacking	25	75	4	0	0	4
PC-6	Computer Forensics	25	75	4	0	0	4
PE-3	1. Privacy and Security in Cyber Space 2. Cyber laws and Security Policies 3. Digital Watermarking and Steganography 4. Incident Response and Forensics	25	75	**3**	0	0	3
PE4	1. Software Security Engineering 2. IT Security Metrics 3. Intrusion Detection and Prevention Systems 4. Reverse Engineering and Malware Analysis	25	75	**3**	0	0	3
OE-2	***Open Elective – 2**	25	75	3	0	0	3
Laboratory II	Computer Forensics Tools and Ethical Hacking Lab	25	75	0	0	3	2
Seminar II	Seminar -II	100	0	0	0	3	2
	Total	**275**	**525**	**21**	**0**	**6**	**25**

III Semester

Course Title	Int. marks	Ext. marks	L	T	P	C
Technical Paper Writing	100	0	0	3	0	2
Comprehensive Viva-Voce	0	100	0	0	0	4
Project work Review II	100	0	0	0	22	8
Total	**200**	**100**	0	**3**	22	**14**

IV Semester

Course Title	Int. marks	Ext. marks	L	T	P	C
Project work Review III	100	0	0	0	24	8
Project Evaluation (Viva-Voce)	0	100	0	0	0	16
Total	**100**	**100**	**0**	**0**	**24**	**24**

***Open Elective subjects must be chosen from the list of open electives offered by OTHER departments.**

 # For Project review I, please refer 7.10 in R17 Academic Regulations.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

SECURE OPERATING SYSTEM (PC -1)

UNIT – 1

Introduction, Secure Operating Systems, Security Goals, Trust Model, Threat Model, Access Control Fundamentals, Protection System, Reference Monitor, Secure Operating System Definition, Assessment Criteria

UNIT- II

Security in Operating Systems -UNIX History, UNIX Security, UNIX Protection System, UNIX Authorization, UNIX Security Analysis, UNIX Vulnerabilities, Windows Security, Windows Protection System, Windows Authorization, Windows Security Analysis, Windows Vulnerabilities.

UNIT- III

Verifiable Security Goals, Information Flow, Information Flow Secrecy Models - Denning's Lattice Model, Bell-La Padula Model, Information Flow Integrity Models - Biba Integrity Model, Low-Water Mark, Clark-Wilson Integrity, the challenge of trusted processes

UNIT- IV

Security Kernel, Secure communication processor, securing commercial operating systems, **secure virtual machine systems** - separation kernels, VAX VMM design, VAX VMM evaluation, VAX VMM result, security in other virtual machine systems.

UNIT –V

Building a secure operating system for Linux, Linux security modules – history, implementation, security – enhanced Linux, SELinux reference monitor, SELinux protection state, SELinux labeling state, SELinux transition state, SELinux administration, SELinux trusted programs, SELinux security evaluation. System assurance – Orange book, common criteria - common criteria concepts, common criteria in action

TEXTBOOKS:

1. Operating System Security (Synthesis Lectures on Information Security, Privacy, and Trust), by Trent Jaeger.

REFERENCES:

1. Operating Systems: Principles and Practice, by Thomas Anderson and Michael Dahlin.
2. Fundamentals of Secure Computer Systems, by Brett Tjaden.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

APPLIED CRYPTOGRAPHY (PC -2)

Course Objectives:

- To understand the cryptography techniques
- To understand the protocols and information theory

Unit-I

Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols - Advanced Protocols -Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity -Blind Signatures - Identity-Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures - Esoteric Protocols

Unit-II

Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode - Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving - Block Ciphers versus Stream Ciphers - Choosing an Algorithm - PublicKey Cryptography versus Symmetric Cryptography - Encrypting Communications Channels - Encrypting Data for Storage - Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption - Detecting Encryption – Hiding and Destroying Information.

Unit- III

Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation - Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) – Lucifer -Madryga – New DES - GOST – 3 Way – Crab – RC5 - Double Encryption - Triple Encryption - CDMF Key Shortening - Whitening.

Unit- IV

Pseudo-Random-Sequence Generators and Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs - Nonlinear-Feedback Shift Registers - System-Theoretic Approach to Stream-Cipher Design - Complexity-Theoretic Approach to Stream-Cipher Design - N- Hash - MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) – One Way Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes

Unit- V

RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) - Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes - Ongchnorr-Shamir - Cellular Automata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -Shamir's Three-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture.

(Subject may be taught with implementation through JAVA)

REFERENCES

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley & Sons, Inc, 2nd Edition, 1996.
2. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004
3. Atul Kahate, "Cryptography and Network Security", Tata McGrew Hill, 2003.
4. William Stallings, "Cryptography and Network Security, Prentice Hall, New Delhi, 2006.
5. Bernard Menezes, "Network Security and Cryptography", Cengage Learning, New Delhi, 2010.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

NETWORK AND WIRELESS SECURITY (PC -3)

Course Objectives:

- To understand the network concepts and controls
- To understand the wireless technologies
- To understand the wireless threats.

Unit - I

Introduction: Network concepts – Threats in networks – Network security controls – Importance of security – Threat models – Security concepts – Common mitigation methods.

Electronic Mail Security: Store and forward – Security services for e-mail – Establishing keys – Privacy – Authentication of the Source – Message Integrity – Non-repudiation – Proof of submission and delivery - Pretty Good Privacy – Secure/Multipurpose Internet Mail Extension.

Unit - II

Wireless Technologies: Introduction to wireless technologies- Wireless data networks-Personal Area Networks -Transmission Media – WLAN standards - Securing WLANS - Countermeasures - WEP (Wired Equivalence Protocol).

Wireless Threats: - Kinds of security breaches - Eavesdropping - Communication Jamming - RF interference - Covert wireless channels - DOS attack – Spoofing - Theft of services - Traffic Analysis - Cryptographic threats - Wireless security Standards.

Unit - III

Security In Data Networks: Wireless Device security issues - CDPD security (Cellular Digital Packet Data)- GSM (Global System for Mobile Communication) security -GPRS security (General Packet Radio Service) -– IP security.

Unit - IV

Wireless Transport Layer Security: Secure Socket Layer - Wireless Transport Layer Security - WAP Security Architecture - WAP Gateway.

Unit -V

Bluetooth Security: Basic specifications – Piconets – Bluetooth security architecture – Scatternets – Security at the baseband layer and link layer – Frequency hopping – Security manager – Authentication – Encryption – Threats to Bluetooth security

REFERENCES:

1. Charles P. Fleeger, "Security in Computing", Prentice Hall, New Delhi, 2009
2. Behrouz A. Forouzan, “Cryptography & Network Security”, Tata McGraw Hill, India, New Delhi, 2009.
3. William Stallings, “Cryptography and Network Security, Prentice Hall, New Delhi, 2006.
4. Bruce Schneier, “Applied Cryptography”, John Wiley, & Sons, New York, 2004.
5. Nichols and Lekka, “Wireless Security-Models, Threats and Solutions”, Tata McGraw – Hill, New Delhi, 2006.
6. Merritt Maxim and David Pollino,”Wireless Security”, Osborne/McGraw Hill, New Delhi, 2005.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

DATABASE SECURITY
(Professional Elective- 1)

Course Objectives:

- To learn the security of databases
- To learn the design techniques of database security
- To learn the secure software design

Course Outcomes:

- Ability to carry out a risk analysis for large database.
- Ability to set up, and maintain the accounts with privileges and roles.

UNIT- I

Introduction: Introduction to Databases Security Problems in Databases Security Controls Conclusions

Security Models -1: Introduction Access Matrix Model Take-Grant Model Acten Model PN Model Hartson and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases

UNIT-II

Security Models -2: Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu's Model The Lattice Model for the Flow Control conclusion

Security Mechanisms: Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation Criteria

UNIT- III

Security Software Design: Introduction A Methodological Approach to Security Software Design Secure Operating System Design Secure DBMS Design Security Packages Database Security Design

Statistical Database Protection & Intrusion Detection Systems: Introduction Statistics Concepts and Definitions Types of Attacks Inference Controls evaluation Criteria for Control Comparison. Introduction IDES System RETISS System ASES System Discovery

UNIT- IV

Models for the Protection of New Generation Database Systems -1: Introduction A Model for the Protection of Frame Based Systems A Model for the Protection of Object-Oriented Systems SORION Model for the Protection of Object-Oriented Databases

UNIT- V

Models for the Protection of New Generation Database Systems -2: A Model for the Protection of New Generation Database Systems: the Orion Model ajodia and Kogan's Model A Model for the Protection of Active Databases Conclusions

TEXT BOOKS:

1. Database Security by Castano Pearson Edition (lie) Database Security and Auditing: Protecting Data Integrity and Accessibility, 1st Edition, Hassan Afyouni, THOMSON Edition.

REFERENCE BOOK:

1. Database security by Alfred basta, melissazgola, CENGAGE learning.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

ADVANCED ALGORITHMS
(Professional Elective- 1)

Course Objectives:

- The fundamental design, analysis, and implementation of basic data structures.
- Basic concepts in the specification and analysis of programs.
- Principles for good program design, especially the uses of data abstraction.
- Significance of algorithms in the computer field
- Various aspects of algorithm development
- Qualities of a good solution

Unit - I : Introduction - Role of algorithms in computing, Analyzing algorithms, Designing Algorithms, Growth of Functions, Divide and Conquer- The maximum-subarray problem, Strassen's algorithms for matrix multiplication, The substitution method for solving recurrences, The recurrence-tree method for solving recurrence, The master method for solving recursions, Probabilistic analysis and random analysis.

Unit - II: Review of Data Structures- Elementary Data Structures, Hash Tables, Binary Search Trees, Red-Black Trees.

Unit - III: Dynamic Programming - Matrix-chain multiplication, Elements of dynamic programming, Longest common subsequence, Greedy Algorithms **-** Elements of the greedy strategy, Huffman codes, Amortized Analysis - Aggregate analysis, The accounting method, The potential method, Dynamic tables.

Unit - IV: Graph Algorithms - Elementary Graph Algorithms, Minimal spanning trees, Single-Source Shortest Paths, Maximum flow.

Unit - V: NP-Complete & Approximate Algorithms-Polynomial time, Polynomial-time verification, NP-completeness and reducibility, NP-complete & approximation problems - Clique problem, Vertex-cover problem, formula satisfiability, 3 CNF Satisfiabilty, The vertex-cover problem, The traveling-salesman problem, The subset-sum problem.

TEXT BOOKS:

1. "Introduction to Algorithms", Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, Third *Edition*, PHI Publication.
2. "Data Structures and Algorithms in C++", M.T. Goodrich, R. Tamassia and D.Mount, Wiley India.

REFERENCES:

1. Fundamentals of Computer Algorithms, Ellis Horowitz, Sartaj Sahni, Sanguthevar Rajasekaran, Second Edition, Galgotia Publication
2. Data structures with C++, J. Hubbard, Schaum's outlines, TMH.
3. Data structures and Algorithm Analysis in C++, 3rd edition, M. A. Weiss, Pearson.
4. Classic Data Structures, D. Samanta, 2nd edition, PHI.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

CLOUD COMPUTING AND SECURITY
(Professional Elective- 1)

UNIT – I
CLOUD COMPUTING FUNDAMENTALS:
Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

UNIT – II
CLOUD APPLICATIONS:
Technologies and the processes required when deploying web services-Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages- Development environments for service development; Amazon, Azure, Google App.

UNIT – III
SECURING THE CLOUD:
Security Concepts - Confidentiality, privacy, integrity, authentication, nonrepudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud.

UNIT – IV
VIRTUALIZATION SECURITY:
Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file system security- storage considerations, backup and recovery- Virtualization System Vulnerabilities.

UNIT – V
CLOUD SECURITY MANAGEMENT:
Security management in the cloud – security management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage incloud.

TEXTBOOK:

1. Gautam Shroff, “Enterprise Cloud Computing Technology Architecture Applications”, Cambridge University Press; 1 edition [ISBN: 978-0521137355], 2010.

REFERENCES:

1. Toby Velte, Anthony Velte, Robert Elsenpeter, “*Cloud Computing, A Practical Approach”,* Tata McGraw-Hill Osborne Media; 1 edition 22, 2009.
2. Tim Mather, Subra Kumara swamy, Shahed Latif, “*Cloud Security and Privacy: an Enterprise Perspective on Risks and Compliance”,* O'Reilly Media; 1 edition, 2009.
3. Ronald L. Krutz, Russell Dean Vines, “*Cloud Security”,* Wiley, 2010.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

INFORMATION SYSTEMS CONTROL AND AUDIT
(Professional Elective- 1)

Course Objectives:

- To understand the foundations of information systems auditing
- To understand the management, application control framework
- To understand about the evidence collection and evidence evaluation process

Unit- I

Overview of Information System Auditing, Effect of Computers on Internal Controls, Effects of Computers on Auditing, Foundations of information Systems Auditing, Conducting an Information Systems Audit.

The management Control Framework-I: Introduction, Evaluating the planning Function, Evaluating the Leading Function, Evaluating the Controlling Function, Systems Development Management Controls, Approaches to Auditing Systems Development, Normative Models of the Systems Development Process, Evaluating the Major phases in the Systems Development Process, Programming Management Controls, Data Resource Management Controls.

Unit- II

The Management Control Framework-II: Security Management Controls, Operations management Controls Quality assurance Management Controls.

The Application Control Framework-I: Boundary Controls, Input Controls, and Communication Controls.

Unit-III

The Application Control Framework-II: Processing Controls, Database Controls, output Controls.

Unit- IV

Evidence Collection: Audit Software, Code Review, Test Data, and Code Comparison, Concurrent Auditing techniques, Interviews, Questionnaires, and Control Flowcharts. Performance Management tools.

Unit -V

Evidence Evaluation: Evaluating Asset Safeguarding and Data Integrity, Evaluating System Effectiveness, Evaluating System Efficiency.

REFERENCES:

1. Ron Weber, Information Systems Control and Audit, Pearson Education, 2002.
2. M. Revathy Sriram, Systems Audit, TMH, New Delhi, 2001.
3. Jalote : Software Project Management in Practice, Pearson Education
4. Royce: Software Project Management, Pearson Education.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

MACHINE LEARNING
(Professional Elective- 2)

Course Objectives:

- To be able to formulate machine learning problems corresponding to different applications.
- To understand a range of machine learning algorithms along with their strengths and weaknesses.
- To understand the basic theory underlying machine learning.
- To be able to apply machine learning algorithms to solve problems of moderate complexity.
- To be able to read current research papers and understands the issues raised by current research.

UNIT - I

Introduction - Well-posed learning problems, Designing a learning system, Perspectives and issues in machine learning

Concept learning and the general to specific ordering – Introduction, A concept learning task, Concept learning as search, Find-S: finding a maximally specific hypothesis, Version spaces and the candidate elimination algorithm, Remarks on version spaces and candidate elimination, Inductive bias

UNIT - II

Decision Tree learning – Introduction, Decision tree representation, Appropriate problems for decision tree learning, The basic decision tree learning algorithm, Hypothesis space search in decision tree learning, Inductive bias in decision tree learning, Issues in decision tree learning

Artificial Neural Networks – Introduction, Neural network representation, Appropriate problems for neural network learning, Perceptions, Multilayer networks and the back propagation algorithm, Remarks on the back propagation algorithm, An illustrative example face recognition

Advanced topics in artificial neural networks

Evaluation Hypotheses – Motivation, Estimation hypothesis accuracy, Basics of sampling theory, A general approach for deriving confidence intervals, Difference in error of two hypotheses, Comparing learning algorithms

UNIT - III

Bayesian learning – Introduction, Bayes theorem, Bayes theorem and concept learning, Maximum likelihood and least squared error hypotheses, Maximum likelihood hypotheses for predicting probabilities, Minimum description length principle, Bayes optimal classifier, Gibs algorithm, Naïve Bayes classifier, An example learning to classify text, Bayesian belief networks The EM algorithm

Computational learning theory – Introduction, Probability learning an approximately correct hypothesis, Sample complexity for Finite Hypothesis Space, Sample Complexity for infinite Hypothesis Spaces, The mistake bound model of learning - **Instance-Based Learning**- Introduction, k -Nearest Neighbour Learning, Locally Weighted Regression, Radial Basis Functions, Case-Based Reasoning, Remarks on Lazy and Eager Learning

Genetic Algorithms – Motivation, Genetic Algorithms, An illustrative Example, Hypothesis Space Search, Genetic Programming, Models of Evolution and Learning, Parallelizing Genetic Algorithms

UNIT - IV

Learning Sets of Rules – Introduction, Sequential Covering Algorithms, Learning Rule Sets: Summary, Learning First Order Rules, Learning Sets of First Order Rules: FOIL, Induction as Inverted Deduction, Inverting Resolution

Analytical Learning - Introduction, Learning with Perfect Domain Theories: Prolog-EBG Remarks on Explanation-Based Learning, Explanation-Based Learning of Search Control Knowledge

UNIT - V

Combining Inductive and Analytical Learning – Motivation, Inductive-Analytical Approaches to Learning, Using Prior Knowledge to Initialize the Hypothesis, Using Prior Knowledge to Alter the Search Objective, Using Prior Knowledge to Augment Search Operators,

Reinforcement Learning – Introduction, The Learning Task, Q Learning, Non-Deterministic, Rewards and Actions, Temporal Difference Learning, Generalizing from Examples, Relationship to Dynamic Programming

TEXT BOOKS:

1. Machine Learning – Tom M. Mitchell, - MGH
2. Machine Learning: An Algorithmic Perspective, Stephen Marsland, Taylor & Francis (CRC)

REFERENCE BOOKS:

1. Machine Learning Methods in the Environmental Sciences, Neural Networks, William W Hsieh, Cambridge Univ. Press.
2. Richard o. Duda, Peter E. Hart and David G. Stork, pattern classification, John Wiley & Sons Inc., 2001
3. Chris Bishop, Neural Networks for Pattern Recognition, Oxford University Press, 1995.
4. Machine Learning by Peter Flach , Cambridge.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

WEB SECURITY
(Professional Elective- 2)

Course Objectives:

- To learn web security objectives
- To learn about vulnerabilities in web hacking
- To learn about phishing, digital certificates, etc.

UNIT - I :

The Web Security Landscape: The Web Security Problem, Risk Analysis and Best Practices; **Cryptography and the Web:** Cryptography and Web Security, Working Cryptographic Systems and Protocols, What Cryptography Can't Do? , Legal Restrictions on Cryptography.

UNIT - II:

The Web's War on Your Privacy: Understanding Privacy, User-Provided Information, Log Files, Understanding Cookies, Web Bugs, Conclusion; **Privacy-Protecting Techniques:** Choosing a Good Service Provider, Picking a Great Password, Cleaning Up After Yourself, Avoiding Spam and Junk Email, Identity Theft; **Privacy-Protecting Technologies:** Blocking Ads and Crushing Cookies, Anonymous Browsing, Secure Email, **Backups and Anti Theft:** Using Backups to Protect Your Data, Preventing theft.

UNIT – III:

Physical security for Servers: Planning for the Forgotten Threats, Protecting Computer Hardware, Protecting Your Data, **Host Security for Servers:** Current Host Security Problems, Securing the Host Computer, minimizing Risk by Minimizing Services, Operating Securely, Secure Remote Access and Content Updating, firewalls and the Web, **Securing Web Applications:** A Legacy of Extensibility and Risk, Rules to Code By, Security Using Fields, Hidden Fields and Cookies, Rules for Programming languages, Using PHP Securely, Writing Scripts That Run with Additional Privileges, Connecting to Databases.

UNIT - IV:

Deploying SSL Server Certificates: Planning for your SSL Server, Creating SSL Servers with FreeBSD, Installing an SSL Certificate on Microsoft IIS, Obtaining a Certificate from a Commercial CA, When Things Go Wrong; **Securing Your Web Service:** Protecting Via Redundancy, Protecting Your DNS, Protecting Your Domain Registration.

UNIT - V:

Controlling Access to Your Web Content: Access Control Strategies, Controlling Access with Apache, Controlling Access with Microsoft IIS; **Client-Side Digital Certificates:** Client Certificates, A Tour of the VeriSign Digital ID Center; **Pornography, Filtering Software and Censorship:** Pornography Filtering, PICS, RSAC, **Privacy Policies, Legislation and P3P:** Policies that Protect Privacy and Privacy Policies, Children's Online Privacy Protection Act, P3P.

TEXT BOOKS:

1. Web Security, Privacy & Commerce: Simson Garfinkel, Gene Spafford, SPD O'reilly.

REFERENCE BOOKS:

1. Web Application Security: Bryan Sullivan, Vincent Liu, Mc Graw Hill.
2. Web Application Hacker's Handbook: Dafydd Stuttard, Marcus Pinto, 2nd Edition, Wiley India.
3. Hacking Exposed Web Applications 3: Joel Scambray, Vincent Liu, Caleb Sima, TMH.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

DISTRIBUTED SYSTEMS
(Professional Elective- 2)

Course Objectives:

- To explain what a distributed system is, why you would design a system as a distributed system, and what the desired properties of such systems are;
- To list the principles underlying the functioning of distributed systems, describe the problems and challenges associated with these principles, and evaluate the effectiveness and shortcomings of their solutions;
- To recognize how the principles are applied in contemporary distributed systems, explain how they affect the software design, and be able to identify features and design decisions that may cause problems;
- To design a distributed system that fulfills requirements with regards to key distributed systems properties (such as scalability, transparency, etc.), be able to recognize when this is not possible, and explain why;
- To build distributed system software using basic OS mechanisms as well as higher-level middleware and languages.

Unit-I

Characterization of Distributed Systems. Design Issues, User Requirement, Network Technologies and Protocols, IPC, Client-Server Communication, Group Communication, IPC in UNIX.
Remote Procedure Calling, Design issues, Implementation, Asynchronous RPC

Unit-II

Distributed OS, Its kernel, Processes and Threads, Naming and Protection, Communication and Invocation, Virtual Memory, File Service components, Design issues, Interfaces, implementation techniques, SUN network file systems

Unit-III

SNS – a name service model, its design issues, Synchronizing physical clocks, Logical time and logical clocks, Distributed coordination. Replication and its architectural model, Consistency and request ordering, Conversation between a client and a server, Transactions, Nested Transactions.

Unit-IV

Concurrency control Locks, Optimistic concurrency control, Timestamp ordering, Comparison of methods for concurrency control.
Distributed Transactions and Nested Transactions, Atomic commit protocols, Concurrency control in distributed transactions, distributed Deadlocks, Transactions with replicated data, Transaction recovery, Fault tolerance, Hierarchical, and group masking of faults.

Unit-V

Cryptography, Authentication and key distribution, Logics of Authentication, Digital signatures.
Distributed shared memory, Design and Implementation issues, Sequential consistency and ivy, Release consistency and Munin, Overview of Distributed Operating systems Mach, Chorus.

TEXT BOOK:

1. G Coulouris, J Dollimore and T Kindberg - Distributed Systems Concepts and Design, Third Edition, Pearson Education.

REFERENCE BOOKS:

1. M Singhal, N G Shivarathri - Advanced Concepts in Operating Systems, Tata McGraw Hill Edition.
2. A. S. Tanenbaum and M. V. Steen - Distributed Systems – Principles and Paradigms, Pearson education.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

MOBILE APPLICATION SECURITY
(Professional Elective- 2)

Course Objectives:

To understand the mobile issues and development strategies
To understand the WAP and mobile security issues
To understand the Bluetooth security issues.

UNIT - I:

Top Mobile Issues and Development Strategies: Top Issues Facing Mobile Devices, Physical Security , Secure Data Storage (on Disk), Strong Authentication with Poor Keyboards , Multiple-User Support with Security, Safe Browsing Environment , Secure Operating Systems, Application Isolation, Information Disclosure, Virus, Worms, Trojans, Spyware, and Malware , Difficult Patching/Update Process, Strict Use and Enforcement of SSL, Phishing , Cross-Site Request Forgery (CSRF), Location Privacy/Security, Insecure Device Drivers, Multifactor Authentication, Tips for Secure Mobile Application Development .

UNIT - II:

WAP and Mobile HTML Security :WAP and Mobile HTML Basics , Authentication on WAP/Mobile HTML Sites , Encryption , Application Attacks on Mobile HTML Sites ,Cross-Site Scripting , SQL Injection , Cross-Site Request Forgery , HTTP Redirects , Phishing , Session Fixation , Non-SSL Login , WAP and Mobile Browser Weaknesses , Lack of HTTPOnly Flag Support , Lack of SECURE Flag Support , Handling Browser Cache , WAP Limitations.

UNIT - III:

Bluetooth Security: Overview of the Technology , History and Standards , Common Uses , Alternatives , Future , Bluetooth Technical Architecture , Radio Operation and Frequency, Bluetooth Network Topology , Device Identification , Modes of Operation , Bluetooth Stack ,Bluetooth Profiles , Bluetooth Security Features , Pairing , Traditional Security Services in Bluetooth, Security “Non-Features” , Threats to Bluetooth Devices and Networks, Bluetooth Vulnerabilities , Bluetooth Versions Prior to v1.2, Bluetooth Versions Prior to v2.1.

UNIT - IV:

SMS Security: Overview of Short Message Service, Overview of Multimedia Messaging Service, Wireless Application Protocol (WAP), Protocol Attacks , Abusing Legitimate Functionality, Attacking Protocol Implementations, Application Attacks , iPhone Safari , Windows Mobile MMS, Motorola RAZR JPG Overflow, Walkthroughs ,Sending PDUs ,Converting XML to WBXML .

UNIT - V

Enterprise Security on the Mobile OS: Device Security Options , PIN , Remote , 346 Secure Local Storage , Apple iPhone and Keychain , Security Policy Enforcement ,Encryption ,Full Disk Encryption ,E-mail Encryption , File Encryption , Application Sandboxing, Signing, and Permissions , Application Sandboxing , Application Signing , Permissions , Buffer Overflow Protection ,Windows Mobile , iPhone ,Android ,BlackBerry , Security Feature Summary.

TEXT BOOK:

1. “Mobile Application Security”, Himanshu Dwivedi, Chris Clark, David Thiel, TATA McGRAW-Hill.

REFERENCES:

1. “Mobile and Wireless Network Security and Privacy”, Kami S. Makki, et al, Springer.
2. “Android Security Attacks Defenses”, Abhishek Dubey, CRC Press.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech- I Year – I Semester (Cyber Forensics & Information Security/Cyber Security)

ALGORITHMS LAB
PART-I

Course Objectives:

- The fundamental design, analysis, and implementation of basic data structures.
- Basic concepts in the specification and analysis of programs.
- Principles for good program design, especially the uses of data abstraction.

Sample Problems on Data structures:

1. Write Java programs that use both recursive and non-recursive functions for implementing the following searching methods:
   a) Linear search b) Binary search
2. Write Java programs to implement the following using arrays and linked lists
   a) List ADT
3. Write Java programs to implement the following using an array.
   a) Stack ADT b) Queue ADT
4. Write a Java program that reads an infix expression and converts the expression to postfix form. (Use stack ADT).
5. Write a Java program to implement circular queue ADT using an array.
6. Write a Java program that uses both a stack and a queue to test whether the given string is a palindrome or not.
7. Write Java programs to implement the following using a singly linked list.
   a) Stack ADT b) Queue ADT
8. Write Java programs to implement the deque (double ended queue) ADT using
   a) Array b) Singly linked list c) Doubly linked list.
9. Write a Java program to implement priority queue ADT.
10. Write a Java program to perform the following operations:
    a) Construct a binary search tree of elements.
    b) Search for a key element in the above binary search tree.
    c) Delete an element from the above binary search tree.
11. Write a Java program to implement all the functions of a dictionary (ADT) using Hashing.
12. Write a Java program to implement Dijkstra's algorithm for Single source shortest path problem.
13. Write Java programs that use recursive and non-recursive functions to traverse the given binary tree in
    a) Preorder b) Inorder c) Postorder.
14. Write Java programs for the implementation of bfs and dfs for a given graph.
15. Write Java programs for implementing the following sorting methods:
    a) Bubble sort d) Merge sort g) Binary tree sort
    b) Insertion sort e) Heap sort
    c) Quick sort f) Radix sort
16. Write a Java program to perform the following operations:
    a) Insertion into a B-tree b) Searching in a B-tree
17. Write a Java program that implements Kruskal's algorithm to generate minimum cost spanning tree.
18. Write a Java program that implements KMP algorithm for pattern matching.

REFERENCE BOOKS:

1. Data Structures and Algorithms in java, 3rd edition, A. Drozdek, Cengage Learning.

2. Data Structures with Java, J.R. Hubbard, 2nd edition, Schaum's Outlines, TMH.
3. Data Structures and algorithms in Java, 2nd Edition, R. Lafore, Pearson Education.
4. Data Structures using Java, D.S. Malik and P.S. Nair, Cengage Learning.
5. Data structures, Algorithms and Applications in java, 2nd Edition, S. Sahani, Universities Press.
6. Design and Analysis of Algorithms, P.H. Dave and H.B. Dave, Pearson education.
7. Data Structures and java collections frame work, W.J. Collins, Mc Graw Hill.
8. Java: the complete reference, 7th edition, Herbert Schildt, TMH.
9. Java for Programmers, P.J. Deitel and H.M. Deitel, Pearson education / Java: How to Program P.J. Deitel and H.M. Deitel , 8th edition, PHI.
10. Java Programming, D.S. Malik, Cengage Learning.
11. A Practical Guide to Data Structures and Algorithms using Java, S. Goldman & K. Goldman, Chapman & Hall/CRC, Taylor & Francis Group.

(Note: Use packages like java.io, java.util, etc

INFORMATION SECURITY LAB
PART-II

Course Objectives:

- To implement the cryptographic algorithms
- To implement the security algorithms.
- To implement cryptographic, digital signatures algorithms.

List of Experiments:

1. Implementation of symmetric cipher algorithm(AES and RC4)
2. Random number generation using a subset of digits and alphabets.
3. Implementation of RSA based signature system
4. Implementation of Subset sum
5. Authenticating the given signature using MD5 hash algorithm.
6. Implementation of Diffie-Hellman algorithm
7. Implementation EIGAMAL cryptosystem.
8. Implementation of Goldwasser-Micali probabilistic public key system
9. Implementation of Rabin Cryptosystem. (Optional).
10. Implementation of Kerberos cryptosystem
11. Firewall implementation and testing.
12. Implementation of a trusted secure web transaction.
13. Cryptographic Libraries-Sun JCE/Open SSL/Bouncy Castle JCE.
14. Digital Certificates and Hybrid (ASSY/SY) encryption, PKI.
15. Message Authentication Codes.
16. Elliptic Curve cryptosystems (Optional)
17. PKCS Standards (PKCS1, 5, 11, 12), Cipher modes.