EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 3 | - | - | 3 |
| Subject Name | | Mathematical Foundations of Computer Science | | | | |
| Subject Code | | MCSCS20S101 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**

1. To introduce the concepts of mathematical logic.
2. To introduce the concepts of sets, relations, and functions.
3. To perform the operations associated with sets, functions, and relations.
4. To introduce generating functions and recurrence relations.
5. To relate practical examples to the appropriate set, function, or relation model, and interpret the associated operations and terminology in context. To use Graph Theory for solving problems.

**Course Outcomes:**

**CO1**. To learn the difference between optimal reasoning vs human like reasoning.
**CO2**. To understand the notions of state space representation, exhaustive search, heuristic search along with the time and space complexities.
**CO3**. To learn different knowledge representation techniques.
**CO4**. To understand the applications of AI: namely Game Playing.
**CO5**. To understands theorem proving, expert systems, machine learning and natural language processing.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | Probability mass, density, and cumulative distribution functions, Parametric families of distributions, Expected value, variance, and conditional expectation, Applications of the univariate and multivariate Central Limit Theorem, Probabilistic inequalities, Markov chains. | 15 |
| UNIT-II | Random samples, sampling distributions of estimators, Methods of Moments and Maximum Likelihood. | 10 |

| | | |
|---|---|---|
| **UNIT-III** | Statistical inference**,** Introduction to multivariate statistical models: regression and classification problems, principal components analysis**,** The problem of overfitting model assessment. | **15** |
| **UNIT-IV** | Graph Theory: Isomorphism, Planar graphs, graph colouring, Hamilton circuits and Euler cycles. permutations and combinations with and without repetition. Specialized techniques to solve combinatorial enumeration problems. | **15** |
| **UNIT-V** | Recent trends in various distribution functions in mathematical field of computer science for varying fields like bioinformatics, soft computing, and computer vision. | **10** |

**TEXT BOOKS:**

1. John Vince, Foundation Mathematics for Computer Science, Springer.
2. K. Trivedi. Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Wiley.

**REFERENCE BOOKS:**

1. M. Mitzenmacher and E. Upfal. Probability and Computing: Randomized Algorithms and Probabilistic Analysis.
2. Alan Tucker, Applied Combinatorics, Wiley.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 3 | - | - | 3 |
| Subject Name | | Advanced Data Structures | | | | |
| Subject Code | | MCSCS20S102 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**

1. To introduce the fundamental concept of data structures and to emphasize the importance of data structures in developing and implementing efficient algorithms.
2. In addition, another objective of the course is to develop effective software engineering practice, emphasizing such principles as decomposition, procedural abstraction, and software reuse.

**Course Outcomes:**

**CO1.** Understand the implementation of symbol table using hasing techniques.
**CO2.** Compare and contrast the benefits of dynamic and static data structures implementations.
**CO3.** Develop and analyze algorithms for red-black trees, B-trees and Splay trees.
**CO4.** Develop algorithms for text processing applications.
**CO5.** Demonstrate different methods for traversing trees.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | **Dictionaries:** Definition, Dictionary Abstract Data Type, Implementation of Dictionaries. Hashing: Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing | 15 |
| UNIT-II | **Skip Lists:** Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists. | 10 |
| UNIT-III | **Trees:** Binary Search Trees, AVL Trees, Red Black Trees, 2-3 Trees, B-Trees, Splay Trees, Recent trends in Hashing, trees, and various computational geometry methods for efficiently solving the new evolving problem. | 15 |

| | | |
|---|---|---|
| **UNIT-IV** | **Text Processing:** Sting Operations, Brute-Force Pattern Matching, The Boyer- Moore Algorithm, The Knuth-Morris-Pratt Algorithm, Standard Tries, Compressed Tries, Suffix Tries, The Huffman Coding Algorithm, The Longest Common Subsequence Problem (LCS), Applying Dynamic Programming to the LCS Problem. | **15** |
| **UNIT-V** | Computational Geometry: One Dimensional Range Searching, Two Dimensional Range Searching, Constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quad trees, k-D Trees. | **10** |

**TEXT BOOKS:**

1. Mark Allen Weiss, “Data Structures and Algorithm Analysis in C++”, Pearson P.
2. Aho, Hopcroft, Ullman, “Data Structures and Algorithms”, Pearson Education.

**REFERENCE BOOKS:**

1. Drozdek, Data Structures and algorithm in Jawa, Cengage (Thomson).
2. Gilberg, Data structures Using C++, Cengage.
3. Horowitz, Sahni, Rajasekaran, “Computer Algorithms”, Galgotia,
4. Tanenbaum A.S., Langram Y, Augestien M.J., ”Data Structures using C & C++”,Prentice Hall of India, 2002.

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 3 | - | - | 3 |
| Subject Name | | Ethical Hacking | | | | |
| Subject Code | | MCSCS20S103 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**

1. Ethical hacking validates that an organization's cyber security strategy is effective.
2. This session will introduce participants to the process an ethical hacker follows when testing a target.
3. We will cover the different tools, techniques, and methodologies a tester and threat actor will employ during a test or breach attempt.

**Course Outcomes:**

After completion of course, students would be able to:

**CO1.** Understand the core concepts related to vulnerabilities and their causes.
**CO2**. Understand ethics behind hacking and vulnerability disclosure.
**CO3**. Appreciate the impact of hacking.
**CO4.** Determine the techniques and tools used in system hacking.
**CO5**. Describe the characteristics of Trojans, worms, and malware.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | Ethical hacking process, Hackers behaviour& mind set, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Physical security vulnerabilities and countermeasures. Internal and External testing. Preparation of Ethical Hacking and Penetration Test Reports and Documents. | 15 |

| | | |
|---|---|---|
| **UNIT-II** | Social Engineering attacks and countermeasures. Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS Spoofing.<br>Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access(hacking 802.11), WEP, WPA, WPA2. | **10** |
| **UNIT-III** | DoS attacks, Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege. Exploiting vulnerabilities in Mobile Application. | **15** |
| **UNIT-IV** | Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads, Metrpreter, Introduction to Armitage, Installing and using Kali Linux Distribution, Introduction to penetration testing tools in Kali Linux. | **15** |
| **UNIT-V** | Case Studies of recent vulnerabilities and attacks. | **10** |

**TEXT BOOKS:**


1. Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press,2015.
2. Beaver, K., Hacking for Dummies, 3rd ed. John Wiley &sons.,2013.
3. Council, Ec. , Computer Forensics: Investigating Network Intrusions and Cybercrime,Cengage Learning, Second Edition, 2010
4. McClure S., Scambray J., and Kurtz G, Hacking Exposed, Tata McGraw-Hill Education, 6th Ed.


**REFERENCE BOOKS:**


1. International Council of E-Commerce Consultants by Learning, Penetration Testing Network and Perimeter Testing Ec-Council/ Certified Security Analyst Vol. 3 of Penetration Testing, Cenage Learning, 2010.
2. Davidoff, S. and Ham, J., Network Forensics Tracking Hackers through Cyberspace, Prentice Hall, 2012.
3. Michael G. Solomon, K Rudolph, Ed Tittel, Broom N., and Barrett, D., Computer, Forensics Jump Start, Willey Publishing, Inc, 2011.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 3 | - | - | 3 |
| Subject Name | | Intrusion Detection | | | | |
| Subject Code | | MCSCS20S104 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:
1. State the function of an Intrusion Detection System (IDS).
2. Evaluate exterior and interior sensor placement effectiveness.
3. Consider trade-offs that influence exterior IDS design effectiveness.
4. Identify factors that influence interior sensor effectiveness.

**Course Outcomes:**
After completion of course, students would be able to:

**CO1.** Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.

**CO2**. Evaluate the security an enterprise and appropriately apply Intrusion Detection tools and techniques in order to improve their security posture.

**CO3**. Perform vector differentiation and integration, analyze the vector fields and apply to Electro-Magnetic fields.

**CO4**. Use Vector differentiation and integration required in Electro-Magnetics and Wave theory.

**CO5**. Solve higher order linear differential equation using appropriate techniques for modelling and analyzing electrical circuits.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | The state of threats against computers, and networked Systems-Overview of computer security solutions and why they Fail-Vulnerability assessment, firewalls, VPN's, Overview of Intrusion Detection and Intrusion Prevention- Network and Host-based IDS. | **15** |
| **UNIT-II** | Classes of attacks – Network layer: scans, denial of service, penetration – Application layer: software exploits, code Injection-Human layer: identity theft, root access-Classes of attackers-Kids/hackers/sop Hesitated groups-Automated: Drones, Worms, and Viruses. | **10** |
| **UNIT-III** | A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS. | **15** |
| **UNIT-IV** | Attack trees and Correlation of Alerts-Autopsy of Worms and Botnets-Malware detection-Obfuscation, Polymorphism-Document vectors Email/IM security Issues-Viruses/Spam-From signatures to thumbprints to zero day Detection-Insider Threat Issues-Taxonomy-Masquerade and Impersonation- Traitors, Decoys and Deception-Future: Collaborative Security. | **15** |
| **UNIT-V** | Anomaly Detection Systems and Algorithms-Network Behaviour Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors-Software Vulnerabilities- State transition, Immunology, Payload Anomaly Detection. | **10** |

**TEXT BOOKS:**

**1.** Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defense, Symantec Press, 2008, ISBN: 978-0-321-50195.

**REFERENCE BOOKS:**

1. Peter Szor, The Art of Computer Virus Research and Defense, Symantec Press, 2010, ISBN 0- 321-30545.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 3 | - | - | 3 |
| Subject Name | | Data Encryption & Network Security | | | | |
| Subject Code | | MCSCS20S105 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:
1. Exhibit knowledge to secure corrupted systems, protect personal data, and secure computer networks in an organization.
2. Practice with an expertise in academics to design and implement security solutions. Understand key terms and concepts in Cryptography, Governance and Compliance.

**Course Outcomes:**
After completion of course, students would be able to:
**CO1**. At the end of this course the student will have the knowledge of plaintext, cipher text, RSA and other cryptographic algorithm.
**CO2.** Key Distribution, Communication Model, Network Perimeter Security, Access Control Lists and Virtual Private Networks.
**CO3**. Analyze and evaluate the cyber security needs of an organization.
**CO4**. Determine software vulnerabilities and security solutions to reduce the risk of exploitation.
**CO5**. Design and develop security architecture for an organization.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | **Introduction to Security:** Need for security, Security approaches, Principles of security, Types of attacks.<br>**Encryption Techniques:** Plaintext, Cipher text, Substitution & Transposition Techniques, Encryption & Decryption, Types of attacks, Key range & Size. | **15** |
| **UNIT-II** | **Symmetric & Asymmetric Key Cryptography:** Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital signature, Knapsack algorithm.<br>**User Authentication Mechanism:** Authentication basics, Passwords, Authentication tokens, Certificate based & Biometric authentication, Firewall. | **10** |
| **UNIT-III** | **Case Studies Of Cryptography:** Denial of service attacks, IP spoofing attacks, Secure inter branch payment transactions, Conventional Encryption and Message Confidentiality, Conventional Encryption Principles, Conventional Encryption Algorithms, Location of Encryption Devices, Key Distribution.<br>**Public Key Cryptography and Message Authentication:** Approaches to Message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Digital, Signatures, Key Management. | **15** |
| **UNIT-IV** | **Network Perimeter Security Fundamentals:** Introduction to Network Perimeter, Multiple layers of Network Security, Security by Router.<br>**Firewalls:** Firewall Basics, Types of Firewalls, Network Address Translation Issues. | **15** |
| **UNIT-V** | **Access Control Lists:** Ingress and Egress Filtering, Types of Access Control Lists, ACL types: standard and extended, ACL commands.<br>**Virtual Private Networks:** VPN Basics, Types of VPN, IPsec Tunneling, IPsec Protocols. VLAN: introduction to VLAN, VLAN Links, VLAN Tagging, VLAN Trunk Protocol (VTP). | **10** |

**TEXT BOOKS:**


1. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education,2010.
2. Kahate, A. Cryptography and Network Security. McGraw-Hill Higher Ed.,2009.
3. Godbole, N., Information Systems Security: Security Management, Metrics, Rameworks and Best Practices. 1st Ed. John Wiley & Sons India,2009.
4. Riggs, C., Network Perimeter Security: Building Defence In-Depth, AUERBACH, USA, 2005.


**REFERENCE BOOKS:**


1. Northcutt S., Inside Network Perimeter Security, 2nd Ed., Pearson Education,2005.
2. Stallings, W., Network Security Essentials: applications and standards. 3rd ed. Pearson Education India, 2007.
3. Stallings, W., Cryptography and Network Security: Principles and Practice. 6th ed. Pearson, 2004.
4. Kim. D., and Solution, M.G., Fundamentals of Information System Security. Jones &Bartlett Learning, 2010.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 3 | - | - | 3 |
| Subject Name | | Information Theory | | | | |
| Subject Code | | MCSCS20S106 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**

After completing this module, you should be able to:

1. Understand the basics of information theory and coding theories.
2. Introduce the concept of amount of information, entropy, channel capacity, error detection and error-correction codes, block coding, convolution coding, and Viterbi decoding algorithm.
3. Understand and explain the basic concepts of information theory, source coding, channel and channel capacity, channel coding and relation among them.
4. Describe the real life applications based on the fundamental theory.

**Course Outcomes:**

After completion of course, students would be able to:

**CO1**. Understand the basics of information and coding theories.

**CO2**. Discuss the various capacity reduction based coding techniques for text, audio and speech type of data.

**CO3**. Compare various capacity reduction based coding techniques for image and video type of data.

**CO4**. Illustrate various security oriented coding techniques for Block codes.

**CO5.** Implement various error control techniques for Convolutional codes.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | Information and entropy information measures, Shannon's concept of Information. Channel coding, channel mutual information capacity (BW). Theorem for discrete memory less channel, information capacity theorem, Error detecting and error correcting codes. | **15** |
| **UNIT-II** | Types of codes: block codes, Hamming and Lee metrics, description of linear block codes, parity check Codes, cyclic code, Masking techniques. | **10** |
| **UNIT-III** | Compression: loss less and lossy, Huffman codes, LZW algorithm, Binary Image c compression schemes, run length encoding, CCITT group 3 1- D Compression, CCITT group 3 2D compression, CCITT group 4 2DCompression. | **15** |
| **UNIT-IV** | Convolutional codes, sequential decoding. Video image Compression: CITT H 261 Video coding algorithm, audio (speech) Compression. Cryptography and cipher. | **15** |
| **UNIT-V** | Case study of CCITT group 31-D Compression, CCITT group 32 D compression. Case Study of Advanced compression technique and Audio compression. | **10** |

**TEXT BOOKS:**


1. Monica Borda, Fundamentals in information theory and coding, Springer, 2011.
2. Singh and Sapre, Communication Systems: Analog and digital, Tata McGraw Hill, 2007.


**REFERENCE BOOKS:**


1. Fred Halsall, Multimedia Communications, Addition-Wesley, 2001.
2. Ranjan Bose, Information Theory, Coding and Cryptography, Tata McGraw Hill, 2001.
3. Prabhat K Andleigh and KiranThakrar, Multimedia system Design, Prentice Hall PTR, 1996.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 3 | - | - | 3 |
| Subject Name | | MACHINE LEARNING | | | | |
| Subject Code | | MCSCS20S107 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:
1. To introduce students to the basic concepts and techniques of Machine Learning.
2. To become familiar with regression methods, classification methods, clustering methods.
3. To become familiar with Dimensionality reduction Techniques.

**Course Outcomes:**
After completion of course, students would be able to:
**CO1.** Gain knowledge about basic concepts of Machine Learning.
**CO2.** Identify machine learning techniques suitable for a given problem.
**CO3**. Solve the problems using various machine learning techniques.
**CO4**. Apply Dimensionality reduction techniques.
**CO5**. Design application using machine learning techniques.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | **Introduction to learning Techniques Supervised Learning (Regression/Classification)**<br>Basic methods: Distance-based methods, Nearest-Neighbours, Decision Trees, Naive Bayes . Linear models: Linear Regression, Logistic Regression, Generalized Linear Models Support Vector Machines, Nonlinearity and Kernel Methods Beyond Binary Classification: Multi-class/Structured Outputs, Ranking. | 15 |

| | | |
|---|---|---|
| **UNIT-II** | **Unsupervised Learning**<br>Clustering: K-means/Kernel K-means Dimensionality Reduction: PCA and kernel PCA Matrix Factorization and Matrix Completion Generative Models (mixture models and latent factor models). | **10** |
| **UNIT-III** | Evaluating Machine Learning algorithms and Model Selection, Introduction to Statistical Learning Theory, Ensemble Methods (Boosting, Bagging, Random Forests).<br>Sparse Modeling and Estimation, Modeling Sequence/Time-Series Data, Deep Learning and Feature Representation Learning | **15** |
| **UNIT-IV** | Scalable Machine Learning (Online and Distributed Learning) A selection from some other advanced topics, e.g., Semi-supervised Learning, Active Learning, Reinforcement Learning, Inference in Graphical Models, Introduction to Bayesian Learning and Inference. | **15** |
| **UNIT-V** | Simulation Tool for Machine Learning, Hands on with recent tools WEKA, R, MATLAB.<br>Recent trends in various learning techniques of machine learning and classification methods for IOT applications. Various models for IOT applications. | **10** |

**TEXT BOOKS:**

1. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press,2012
2. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer 2009 (freely available online).

**REFERENCE BOOKS:**

1. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.
2. ShaiShalev-Shwartz, Shai Ben-David, Understanding Machine Learning: From Theory to Algorithms, Cambridge University Press; 1 edition (May 19, 2014).

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 3 | - | - | 3 |
| Subject Name | | Malware Analysis & Reverse | | | | |
| Subject Code | | MCSCS20S108 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**

**1.** Understand how malware hides its execution, including process injection, process replacement and user-space rootkits.
**2.** Grasp how shellcode works, including position independence, symbol resolution and decoders.
**3.** Comprehend the inner workings and limitations of disassemblers such as IDA Pro as well as how to circumvent the anti-disassembly mechanisms that malware authors use to thwart analysis.

**Course Outcomes:**

After completion of course, students would be able to:
**CO1**. To understand the concept of malware and reverse engineering.
**CO2**. Implement tools and techniques of malware analysis.
**CO3**. Evaluate and demonstrate a critical and systematic understanding of malicious software, malicious code implementation and the methods of detecting software vulnerabilities.
**CO4**. Critically evaluate the design, code and the implementation of a malicious component.
**CO5**. Employ network and system-monitoring tools to examine and assess how malware interacts.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM).Methodology,BriefOverviewofMalwareanalysislabsetupandconfiguration,Introduction to key MA tools and techniques, Behavioural Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining Clam AV Signatures. | 15 |

| | | |
|---|---|---|
| **UNIT-II** | Introduction to Python ,Introduction to x86 Intel assembly language, Scanners: Virus Total, Jotti, and No Virus Thanks, Analyzers: Threat Expert, CWS and box, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, Handle Diff, Analysis Automation Tools: Virtual Box, VM Ware, Python , Other Analysis Tools Malware Forensics Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg RipperPlu-gins.BypassingPoisonIvy'sLockedFiles,BypassingConficker'sFileSystemACL Restrictions, Detecting Rogue PKI Certificates. | **10** |
| **UNIT-III** | **Malware and Kernel Debugging** Opening and Attaching to Processes, Configuration of JIT Debugger for Shell code Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands**,** DLL Export Enumeration, Execution, and Debugging**,** Debugging a VMware Workstation Guest (on Windows)**,** Debugging a Parallels Guest (on Mac OSX). Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbg Scripts**,** Kernel Debugging with IDA Pro. | **15** |
| **UNIT-IV** | **Memory Forensics and Volatility**<br>Memory Dumping with MoonSols Windows Memory Toolkit**,** Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps**,** Code Injection and Extraction**,** Detecting and Capturing Suspicious Loaded DLLs**,** Finding Artefacts in Process Memory**,** Identifying Injected Code with Malfind and YARA. Using WHOIS to Research Domains**,** DNS Hostname Resolution**,** Querying, Passive DNS**,** Checking DNS Records**,** Reverse IP Search New Course Form**,** Creating Static Maps**,** Creating Interactive Maps. Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA | **15** |
| **UNIT-V** | Creating Custom Clam AV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser'sREMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks. | **10** |

**TEXT BOOKS:**

1. Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software publisher, William Pollock, 2012.

**REFERENCE BOOKS:**

1. Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, 1st Edition,2014.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 0 | - | 4 | 2 |
| Subject Name | | Ethical Hacking & Network Security Lab | | | | |
| Subject Code | | MCSCS20S109 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 50 | | | | |

**List of Experiments:**

1. To learn about hacking tools and skills.
2. To study about Foot printing and Reconnaissance.
3. To study about Fingerprinting.
4. To study about system Hacking.
5. To study about Wireless Hacking.
6. To learn & study about Sniffing & their tools.
7. Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.
8. Study of packet sniffer tools like Wireshark, ethereal, tcp dump etc. Use the tools to do the following 1. Observer performance in promiscuous as well as non-promiscuous mode. 2. Show that packets can be traced based on different filters.
9. Download and install NMAP. Use it with different options to scan open ports, perform OS finger printing, do a ping scan, TCP port scan, UDP port scan, etc.
10. Detect ARP spoofing using open source tool ARPWATCH.
11. Use the Nessus tool to scan the network for vulnerabilities.
12. Implement a code to simulate buffer overflow attack.
13. Set up IPSEC under LINUX 8 Install IDS (e.g. SNORT) and study the logs.
14. Use of ip tables in Linux to create firewalls. 10 Mini projects.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 2 | - | - | - |
| Subject Name | | English for Research Paper Writing(AE*) | | | | |
| Subject Code | | MCSER20S110 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | - | | | | |

**Course Objective:**
After completing this module, you should be able to:
1. Understand that how to improve your writing skills and level of readability.
2. Learn about what to write in each section.
3. Understand the skills needed when writing a Title Ensure the good quality of paper at very first-time submission.

**Course Outcomes:**
After completion of course, students would be able to:
**CO1**. Students will heighten their awareness of correct usage of English grammar in writing and Speaking.
**CO2**. Students will improve their speaking ability in English both in terms of fluency and comprehensibility.
**CO3**. Students will give oral presentations and receive feedback on their performance.
**CO4**. Students will increase their reading speed and comprehension of academic articles.
**CO5**. Students will improve their reading fluency skills through extensive reading.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | Planning and Preparation, Word Order, breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness | 10 |
| UNIT-II | Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticizing, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts. Introduction. | 15 |
| UNIT-III | Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check. | 10 |

| | | |
|---|---|---|
| **UNIT-IV** | key skills needed when writing a Title, key skills needed when writing an Abstract, key skills needed when writing an Introduction, skills needed when writing a Review of the Literature, skills needed when writing the Methods, skills needed when writing the Results, skills needed when writing the Discussion, skills are needed when writing the Conclusions. | 15 |
| **UNIT-V** | Useful phrases, how to ensure paper is as good as it could possibly be the first- time submission. | 10 |

**TEXT BOOKS:**


1. Highman N (1998), Handbook of Writing for the Mathematical Sciences, SIAM. Highman'sbook.
2. Adrian Wallwork , English for Writing Research Papers, Springer New York Dordrecht Heidelberg London,2011.


**REFERENCE BOOKS:**


1. Goldbort R (2006) Writing for Science, Yale University Press (available on Google Books).
2. Day R (2006) How to Write and Publish a Scientific Paper, Cambridge University Press.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 2 | - | - | 2 |
| Subject Name | | Research Methodology and IPR | | | | |
| Subject Code | | MMAT20S111 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:

1. Students will able to Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.

**Course Outcomes:**
After completion of course, students would be able to:

**CO1**. Understand research problem formulation.
**CO2**. Analyze research related information.
**CO3**. Follow research ethics.
**CO4**. Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
**CO5**. Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations. | **15** |
| **UNIT-II** | Effective literature studies approaches, analysis Plagiarism, Research ethics. | **10** |
| **UNIT-III** | Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee. | **15** |
| **UNIT-IV** | Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT. | **15** |
| **UNIT-V** | Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications**:** New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs. | **10** |

**TEXT BOOKS:**


1. Stuart Melville and Wayne Goddard, “Research methodology: an introduction for science &engineering students.
2. Wayne Goddard and Stuart Melville, “Research Methodology: An Introduction”.
3. Ranjit Kumar, 2nd Edition, “Research Methodology: A Step-by-Step Guide for beginners”
4. Halbert, “Resisting Intellectual Property”, Taylor & Francis Ltd, 2007.


**REFERENCE BOOKS:**


1. Mayall, “Industrial Design”, McGraw Hill,1992.
2. Niebel, “Product Design”, McGraw Hill,1974.
3. Asimov, “Introduction to Design”, Prentice Hall,1962.
4. Robert P. Merges, Peter S. Menell, Mark A. Lemley, “Intellectual Property in New Technological Age”, 2016.
5. T. Ramappa, “Intellectual Property Rights Under WTO”, S. Chand, 2008.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M.TECH./DS | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | I/I | 0 | 0 | 4 | 2 |
| Subject Name | | Advanced Data Structures | | | | |
| Subject Code | | MCSCSE20S112 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 50 | | | | |

### List of Experiments

1. Write a program that implements stack and Queue operations using
   a. Arrays. b. linked list
2. Write a program to perform the following operations on singly linked list and doubly linked list
   a. Creation. b. Insertion. c. Deletion. d. Traversal.
3. Implement recursive and non-recursive i) Linear search ii) Binary search
4. Study and Implementation of Different sorting algorithms and Find Time and Space complexities.
5. Implement Recursive functions to traverse the given binary tree in
   a. Preorder. b. Inorder. c. Postorder
6. Study and Implementation of different operations on
   a. Binary Search Tree
   b. AVL tree
   c. Red Black Tree
7. Perform the following operations
   a. Insertion into a B-tree
   b. Deletion from a B-tree
8. Implement Different Collision Resolution Techniques.
9. Study and Implementation of Following String Matching algorithms:
   a. Rabin-Karp algorithm
   b. Knuth-Morris-Pratt algorithm
   c. Boyer-Moore algorithm
10. Implement the following using java:
    1. Single Source Shortest Path algorithms
    2. All pairs shortest path algorithms
    3. Minimal Spanning Tree algorithms
    4. String and Pattern matching algorithms
    5. Maximum Flow/ Minimum cut algorithms.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 3 | - | - | 3 |
| Subject Name | | Advance Algorithms | | | | |
| Subject Code | | MCSCS20S201 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:

1. The course is intended to provide the foundations of the practical implementation and usage of Algorithms and Data Structures. One objective is to ensure that the student evolves into a competent programmer capable of designing and analysing implementations of algorithms and data structures for different kinds of problems.
2. The second objective is to expose the student to the algorithm analysis techniques, to the theory of reductions, and to the classification of problems into complexity classes like NP.

**Course Outcomes:**
After completion of course, students would be able to:

**CO1.** Design and analyze programming problem statements.
**CO2**. Choose appropriate data structures and algorithms, understand the ADT/libraries, and use it to design algorithms for a specific problem.
**CO3**. Understand the necessary mathematical abstraction to solve problems.
**CO4**. Come up with analysis of efficiency and proofs of correctness.
**CO5**. Comprehend and select algorithm design approaches in a problem specific manner.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | **Sorting:** Review of various sorting algorithms, topological sorting.<br>**Graph:** Definitions and Elementary Algorithms: Shortest path by BFS, shortest path in edge-weighted case (Dijkasra's), depth-first search and computation of strongly connected components, Emphasis on correctness proof of the algorithm and time/space analysis Introduction to greedy paradigm, algorithm to compute a maximum weight maximal independent set. Application to MST. | 15 |

| | | |
|---|---|---|
| **UNIT-II** | Strassen's algorithm and introduction to divide and conquer paradigm, inverse of a triangular matrix, relation between the time complexities of basic matrix operations. Floyd-Warshall algorithm and introduction to dynamic programming paradigm. More examples of dynamic programming. | **10** |
| **UNIT-III** | **Linear Programming:** Geometry of the feasibility region and Simplex algorithm, Decision Problems: P, NP. | **15** |
| **UNIT-IV** | One or more of the following topics based on time and interest: Approximation algorithms, Randomized Algorithms, Interior Point Method, Recent Trends in problem solving paradigms using recent searching and sorting techniques by applying recently proposed data structures. | **15** |
| **UNIT-V** | NP Complete, NP-Hard, NP Hard with Examples, Proof of NP-hardness and NP-completeness. | **10** |

**TEXT BOOKS:**


1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest Introduction to Algorithms, Stein, Third Edition, July2009.
2. AlfredV.Aho, JohnE. Hopcroft, JeffreyD. Ullman, The Design and Analysis of Computer Algorithms, 2002.


**REFERENCE BOOKS:**


1.Jon Kleinberg and Eva Tardos , Algorithm Design, First Edition,2014.

2.Juraj Hromkovic, Design and Analysis of Randomized Algorithms: Introduction to Design, Jun2005.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 3 | - | 0 | 3 |
| Subject Name | | Soft Computing | | | | |
| Subject Code | | MCSCS20S202 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:
1. Develop the skills to gain a basic understanding of neural network theory and fuzzy logic theory.
2. Introduce students to artificial neural networks and fuzzy theory from an engineering perspective.

**Course Outcomes:**
After completion of course, students would be able to:
**CO1**. Comprehend the fuzzy logic and the concept of fuzziness involved in various systems and fuzzy set theory.
**CO2**. Understand the concepts of fuzzy sets, knowledge representation using fuzzy rules, approximate reasoning, fuzzy inference systems, and fuzzy logic.
**CO3**. To understand the fundamental theory and concepts of neural networks, Identify different neural network architectures, algorithms, applications and their limitations .
**CO4**. Understand appropriate learning rules for each of the architectures and learn several neural network paradigms and its applications.
**CO5**. Reveal different applications of these models to solve engineering and other problems.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | **Introduction to Soft Computing and Neural Networks:** Evolution of Computing: Soft Computing Constituents, From Conventional AI to Computational Intelligence: Machine Learning Basics.Adaptive Resonance architectures, Advances in Neural networks.<br>**Neural Networks:** Machine Learning Using Neural Network, Adaptive Networks, Feed forward Networks, Supervised Learning Neural Networks, Radial Basis Function Networks: Reinforcement Learning, Unsupervised, and Learning Neural Networks. | 15 |

| | | |
|---|---|---|
| **UNIT-II** | Fuzzy Rules and Fuzzy Reasoning, Fuzzy Inference Systems, Fuzzy Expert Systems, Fuzzy Decision Making.<br>**Fuzzy Logic:** Fuzzy Sets, Operations on Fuzzy Sets, Fuzzy Relations, Membership Functions. | **10** |
| **UNIT-III** | **Genetic Algorithms:** Introduction to Genetic Algorithms (GA), Applications of GA in Machine Learning: Machine Learning Approach to Knowledge Acquisition. Introduction to other optimization techniques. | **15** |
| **UNIT-IV** | Study of neural network toolbox and fuzzy logic toolbox, Simple implementation of Artificial Neural Network and Fuzzy Logic.<br>Recent Trends in deep learning, various classifiers, neural networks and genetic algorithms. Implementation of recently proposed soft computing techniques. | **15** |
| **UNIT-V** | **Matlab/Python Lib:** Introduction to Matlab/Python, Arrays and array operations, Functions and Files. | **10** |

**TEXT BOOKS:**

1. Jyh-Shing Roger Jang, Chuen-Tsai Sun, Eiji Mizutani, Neuro - Fuzzy and Soft Computing, Prentice-Hall of India, 2003.

**REFERENCE BOOKS:**

1. George J. Klir and Bo Yuan, Fuzzy Sets and Fuzzy Logic - Theory and Applications, Prentice Hall,1995.
2. MATLAB Toolkit Manual Ross J.T., Fuzzy Logic with Engineering Applications John Wiley & Sons, 2001.

**List of Experiment**

1. Create a perceptron with appropriate number of inputs and outputs. Train it using fixed increment learning algorithm until no change in weights is required. Output the final weights.
2. Write a program to implement artificial neural network without back propagation. Write a program to implement artificial neural network with back propagation.
3. Implement Union, Intersection, Complement and Difference operations on fuzzy sets. Also create fuzzy relation by Cartesian product of any two fuzzy sets and perform max-min composition on any two fuzzy relations.
4. Implement travelling sales person problem (TSP) using genetic algorithms.
5. Plot the correlation plot on dataset and visualize giving an overview of relationships among data on soya bins data. Analysis of covariance: variance (ANOVA), if data have categorical variables on iris data.
6. Implement linear regression and multi-regression for a set of data points.
7. Implement crisp partitions for real-life iris dataset.
8. Write a program to implement Hebb's rule Write a program to implement Delta rule.
9. Write a program to implement logic gates.
10. Implement SVM classification by Fuzzy concepts.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 3 | - | - | 3 |
| Subject Name | | Steganography | | | | |
| Subject Code | | MCSCS20S203 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:

1. The objective of the course makes students familiar about Digital watermarking and steganography.

**Course Outcomes:**
After completion of course, students would be able to:

**CO1**. By the end of the course, students should be able understand how Digital Watermarking and Steganography works.
**CO2**. Able to understand the applications for making it more secure.
**CO3**. Learn the concept of information hiding.
**CO4**. Survey of current techniques of steganography and learn how to detect and extract hidden Information.
**CO5**. Learn watermarking techniques and through examples understand the concept.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | **Steganography:** Overview, History, Methods for hiding (text, images, audio, video, speech etc.), Issues: Security, Capacity and Imperceptibility,<br>Steganalysis: Active and Malicious Attackers, Active and passive steg analysis. | **15** |
| **UNIT-II** | Frameworks for secret communication (pure Steganography, secret key, public key steganography), Steganography algorithms (adaptive and non-adaptive). | **10** |
| **UNIT-III** | Steganography techniques: Substitution systems, Spatial Domain, Transform domain techniques, Spread spectrum, Statistical steganography, Cover Generation and cover selection, Tools: EzStego, FFEncode, Hide 4 PGP, Hide and Seek, S Tools etc.).<br>Detection, Distortion, Techniques: LSB Embedding, LSB Steganalysis using primary sets, Texture based. | **15** |
| **UNIT-IV** | **Digital Watermarking**: Introduction, Difference between Watermarking and Steganography, History, Classification (Characteristics and Applications), Types and techniques (Spatial-domain, Frequency-domain, and Vector quantization based watermarking), Attacks and Tools (Attacks by Filtering, Re modulation, Distortion, Geometric Compression, Linear Compression etc.), Watermark security & authentication. | **15** |
| **UNIT-V** | Recent trends in Steganography and digital watermarking techniques. Case study of LSB Embedding, LSB Stage analysis using primary sets. | **10** |

**TEXT BOOKS:**


1. Peter Wayner, Disappearing Cryptography–Information Hiding: Steganography & Watermarking, Morgan Kaufmann Publishers, New York,2002.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, TonKalker, Digital Watermarking and Steganography, Margan Kaufmann Publishers, New York,2008.


**REFERENCE BOOKS:**


1. Neil F. Johnson, ZoranDuric, SushilJajodia, Information Hiding: Steganographyand Watermarking-Attacks and Countermeasures, Springer,2012.
2. Stefan Katzenbeisser, Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Print on Demand, 1999.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| | | | | | | |
|---|---|---|---|---|---|---|
| **Class** | | **M-Tech.-Cyber Security** | **L** | **T** | **P** | **C** |
| **Semester/Year** | | **II/I** | **3** | **-** | **-** | **3** |
| **Subject Name** | | **Secure Software Design & Enterprise** | | | | |
| **Subject Code** | | **MCSCS20S204.** | | | | |
| **Paper** | **English** | | | | | |
| | **Hindi** | | | | | |
| **Max. Marks** | | **100** | | | | |

**Course Objective:**

After completing this module, you should be able to:

1. The course takes a software development perspective to the challenges of engineering software systems that are secure.
2. This course addresses design and implementation issues critical to producing secure software systems.
3. The course deals with the question of how to make the requirements for confidentiality, integrity, and availability integral to the software development process from requirements gathering to design, development, configuration, deployment, and ongoing maintenance.

**Course Outcomes:**

After completion of course, students would be able to:

**CO1**. Understand various aspects and principles of software security.

**CO2**. Devise security models for implementing at the design level.

**CO3**. Identify and analyse the risks associated with s/w engineering and use relevant models to mitigate the risks.

**CO4**. Understand the various security algorithms to implement for secured computing and computer networks.

**CO5**. Explain different security frameworks for different types of systems including electronic systems.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | **Secure Software Design**<br>Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance. | **15** |
| **UNIT-II** | **Enterprise Application Development**<br>Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Research technologies available for the presentation, business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Develop components at the different tiers in an enterprise system, Design and develop a multi-tier solution to a problem using technologies used in enterprise system, Present software solution. | **10** |
| **UNIT-III** | **Enterprise Systems Administration**<br>Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, Monitor server resource utilization for system reliability and availability, Install and administer network services (DNS / DHCP / Terminal Services / Clustering / Web / Email). | **15** |
| **UNIT-IV** | Obtain the ability to manage and troubleshoot a network running multiple services, Understand the requirements of an enterprise network and how to go about managing them. Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum Vulnerabilities and flaws. | **15** |
| **UNIT-V** | Case study of DNS server, DHCP configuration and SQL injection attack. | **10** |

**TEXT BOOKS:**

1. Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett, 2012.

**REFERENCE BOOKS:**

1. KennethR.vanWyk,MarkG.Graff,DanS.Peters,DianaL.Burley,EnterpriseSoftwareSecurity, Addison Wesley, 1st Edition, 2014

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 3 | - | - | 3 |
| Subject Name | | Big Data Analysis and Visualization | | | | |
| Subject Code | | MCSCS20S205 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:
1. Students will develop relevant programming abilities.
2. Students will demonstrate proficiency with statistical analysis of data.
3. Students will develop the ability to build and assess data-based models.
4. Students will execute statistical analyses with professional statistical software.
5. Students will demonstrate skill in data management.

**Course Outcomes:**
After completion of course, students would be able to:
**CO1.** Students will demonstrate an understanding of and ability to apply computer science principles relating to data representation, retrieval, programming and analysis.
**CO2**. Students will demonstrate an understanding of and ability to apply mathematical and statistical models and concepts to detect patterns in data, as well as draw inferences and conclusions supported by the data.
**CO3**. Students will demonstrate critical thinking skills associated with problem identification, problem solving and decision-making, assessing value propositions supported by data, and generating a logical synthesis of information from data.
**CO4**. Students will demonstrate the ability to apply knowledge gained from one area to problems and data in another.
**CO5**. Students will demonstrate the ability to communicate findings and their implications, and to apply them effectively in organizational settings.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | **Data Gathering and Preparation:** Data formats, parsing and transformation, Scalability and real-time issues. | **15** |
| **UNIT-II** | **Exploratory Analysis:** Descriptive and comparative statistics, Clustering and association, Hypothesis Generation,<br>**Visualization:** Designing visualizations, Time series, Geo-located data, Correlations and connections, Hierarchies and networks, interactivity. | **10** |
| **UNIT-III** | **Big Data Technology:** Fundamental of Big Data Types, Big data Technology Components, Big Data Architecture, Big Data Warehouse, Functional Vs. Procedural Programming Models for Big Data. | **15** |
| **UNIT-IV** | **Big Data Tools:** Hadoop: Introduction to Hadoop Ecosystem, HDFS, Map-Reduce programming, Spark, PIG, JAQL, Understanding Text Analytics and Big Data, Predictive Analysis of Big Data, Role of Data Analyst. | **15** |
| **UNIT-V** | **Data Cleaning:** Consistency checking, Heterogeneous and missing data, Data Transformation and segmentation. | **10** |

**TEXT BOOKS:**

1. Glenn J. Myatt, Making sense of Data: A practical Guide to Exploratory Data Analysis and Data Mining, Wiley- Blackwell,2006.

**REFERENCE BOOKS:**

1. Anil Maheshwari, Data Analytics Make Accesible, Orilley Publications, 2014.
2. Croll and B. Yoskovitz Lean Analytics: Use Data to Build a Better Startup Faster, Oreilley Publications, 1st Edition, 2013.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 3 | - | - | 3 |
| Subject Name | | Secure Coding | | | | |
| Subject Code | | MCSCS20S206 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:

1. Exhibit knowledge to secure corrupted systems, protect personal data, and secure computer networks in an Organization. Practice with an expertise in academics to design and implement security solutions.
2. Understand key terms and concepts in Cryptography, Governance and Compliance.• Develop cyber security strategies and policies.
3. Understand principles of web security and to guarantee a secure network by monitoring.
4. Analysing the nature of attacks through cyber/computer forensics software/tools.

**Course Outcomes:**
After completion of course, students would be able to:
**CO1**. Write secure programs and various risks in the software's.
**CO2.** Describe various possible security attacks.
**CO3.** Classify various errors that lead to vulnerabilities.
**CO4**. Real time software and vulnerabilities associated with them.
**CO5**. Describe various securities issues.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | Software Security: Security Concepts, Security Policy, Security Flaws, Vulnerabilities, Exploitation and Mitigations. Software Security problems, Classification of Vulnerabilities. Security Analysis: Problem Solving with static analysis: Type Checking, Style Checking, and Program.<br>Understanding, verifications and property checking, Bug finding and Security Review. | **15** |
| **UNIT-II** | Strings: Common String manipulating Errors, String Vulnerabilities and Exploits, Mitigation Strategies for strings, String handling functions, Runtime protecting strategies, Notable Vulnerabilities.<br>Integer Security: Integer data Type, Integer Conversions, Integer Operations, Integer Vulnerabilities, Mitigation Strategies. | **10** |
| **UNIT-III** | Handling Inputs: What to validate, How to validate, Preventing metadata Vulnerabilities, Buffer Overflow: Introduction, Exploiting buffer overflow vulnerabilities, Buffer allocation strategies, Tracking buffer sizes, buffer overflow in strings, Buffer overflow in Integers Runtime Protections.<br>Errors and Exceptions: Handling Error with return code, Managing exceptions, Preventing Resource leaks, Logging and debugging. | **15** |
| **UNIT-IV** | Web Applications: Input and Output Validation for the Web: Expect That the Browser Has Been Subverted, HTTP Considerations: Use POST, Not GET, Request Ordering, Error Handling, Request Provenance. | **15** |
| **UNIT-V** | Maintaining Session State: Use Strong Session Identifiers, Enforce a Session Idle Timeout and a Maximum Session Lifetime, Begin a New Session upon Authentication. | **10** |

**TEXT BOOKS:**


1. Seacord, R. C., Secure Coding in C and C++, Addison Wisley for Software Engineering Institute, 2nd edition, 2013.
2. Chess, B., and West, J., Secure Programming with static Analysis, Addison Wisley Software Security Series, 2007.


**REFERENCE BOOKS:**


1. Seacord, R. C., The CERT C Secure Coding Standard, Pearson Education, 2009.
2. Howard, M., LeBlanc, D., Writing Secure Code, 2nd Edition. Pearson Education, 2002.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 3 | - | - | 3 |
| Subject Name | | Security Assessment & Risk Analysis | | | | |
| Subject Code | | MCSCS20S207 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**

1. Exhibit knowledge to secure corrupted systems, protect personal data, and secure computer networks in an Organization. Practice with an expertise in academics to design and implement security solutions.
2. Understand key terms and concepts in Cryptography, Governance and Compliance.
3. Develop cyber security strategies and policies.
4. Understand principles of web security and to guarantee a secure network by monitoring.

**Course Outcomes:**

After completion of course, students would be able to:

**CO1**. Capable of recommending contingency strategies including data backup and recovery and alternate site selection for business resumption planning.

**CO2**. Skilled to be able to describe the escalation process from incident to disaster in case of security disaster.

**CO3**.Capable of Designing a Disaster Recovery Plan for sustained organizational operations.

**CO4**.Capable of Designing a Business Continuity Plan for sustained organizational operations.

**CO5**. Analysing the nature of attacks through cyber/computer forensics software/tools.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | **Security Basics**: Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security Countermeasures- education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security countermeasures-policy, procedures and practices, threats, vulnerabilities. | 15 |

| | | |
|---|---|---|
| **UNIT-II** | Threats to and Vulnerabilities of Systems: definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas, Countermeasures: assessments (e.g., surveys, inspections), Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis of controls, implementation of cost-effective controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or Inadvertent disclosure of information), threat and vulnerability assessment. | **10** |
| **UNIT-III** | Security Planning: directives and procedures for policy mechanism, Risk Management: acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process, Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for off-site processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation. | **15** |
| **UNIT-IV** | **Policies and Procedures**<br>Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms) Personnel Security Practices and Procedures: access authorization/verification (need-to-know), contractors, employee clearances, position sensitivity, | **15** |
| **UNIT-V** | Security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing, Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs.<br>Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption (e.g., point-to-point, network, link), cryptography-key management (to include electronic key),<br>Cryptography-strength (e.g., complexity, secrecy, characteristics of the key) Case study of threat and vulnerability assessment. | **10** |

**TEXT BOOKS:**


1. Whitman & Mattord, Principles of Incident Response and Disaster Recovery,Course Technology, ISBN: 141883663X (Web L.ink)http://www.cnss.gov/Assets/pdf/nstissi_4011,pdf


**REFERENCE BOOKS:**


1. Seacord, R. C., The CERT C Secure Coding Standard, Pearson Education, 2009.
2. Howard, M., LeBlanc, D., Writing Secure Code, 2nd Edition. Pearson Education, 2002.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 3 | - | - | 3 |
| Subject Name | | Digital Forensics | | | | |
| Subject Code | | MCSCS20S208. | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 100 | | | | |

**Course Objective:**
After completing this module, you should be able to:

1. Introduces computer security administrators to computer forensics. Includes setup and use of an investigator's laboratory.
2. computer investigations using digital evidence controls, processing crime and incident scenes, performing data acquisition, computer forensic analysis, e-mail investigations, image file recovery, investigative report writing, and expert witness testimony.

**Course Outcomes:**
After completion of course, students would be able to:
**CO1.** Understand relevant legislation and codes of ethics.
**CO2**. Computer forensics and digital detective and various processes, policies and procedures.
**CO3**. E-discovery, guidelines and standards, E-evidence, tools and environment.
**CO4**. Email and web forensics and network forensics.
**CO5**. Perform recovery of digital evidence from various digital devices using a variety of software utilities.

| Unit | Syllabus | Periods |
|---|---|---|
| **UNIT-I** | Digital Forensics Science: Forensics science, computer forensics, and digital forensics. Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber- criminalistics area, holistic approach to cyber-forensics.<br>Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008. | **15** |
| **UNIT-II** | Incident- Response Methodology, Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation. | **10** |
| **UNIT-III** | Image Capturing, Authenticating Evidence, Hidden Data Extraction, Data Storage, File Systems, Recovery of deleted files, Cracking Passwords,<br>Internet Crime Investigations, Web Attack Investigations. | **15** |
| **UNIT-IV** | Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, and Complete a case, Critique a case.<br>Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data. | **15** |
| **UNIT-V** | Mobile Forensics: mobile forensics techniques, mobile forensics tools. | **10** |

**TEXT BOOKS:**


1. John Sammons, The Basics of Digital Forensics, Elsevier, 1st Edition,2015.
2. Davidoff, S. and Ham, J., Network Forensics Tracking Hackers through Cyberspace, Prentice Hall, 2012.
3. MichaelG.Solomon, KRudolph, Ed Tittel Broom N.,and Barrett D.,Computer, Forensics JumpStart, Willey Publishing, Inc.,2011.


**REFERENCE BOOKS:**


1. Marcella,AlbertJ.,Cyberforensics:Afieldmanualforcollecting,examiningandpreservingevidence of computer crimes, New York, Auerbach publications,2008.
2. Davidoff, Sherri, Network forensics: Tracking hackers through cyberspace, Pearson education India private limited, 2017.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | - | - | 4 | 2 |
| Subject Name | | Mini Project | | | | |
| Subject Code | | MCSCS20S209 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 50 | | | | |

**Syllabus:**

- Mini Project will have mid semester presentation and end semester presentation. Mid semester presentation will include identification of the problem based on the literature review on the topic referring to latest literature available.

- End semester presentation should be done along with the report on identification of topic for the work and the methodology adopted involving scientific research, collection and analysis of data, determining solutions highlighting individuals ‘contribution.

- Continuous assessment of Mini Project at Mid Sem and End Sem will be monitored by the Departmental committee.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M.Tech/CSE | L | T | P | Credit |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 0 | 0 | 4 | 2 |
| Subject Name | | Advance Algorithms | | | | |
| Subject Code | | MCSCSE20S210 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 50 | | | | |

List of Experiments

1. Implement Recursive Binary search and Linear search and determine the time taken to search an element.
2. Sort a given set of elements using the Heap sort method and determine the time taken to sort the elements.
3. Sort a given set of elements using Merge sort method and determine the time taken to sort the elements. Repeat the experiment for different values of n, the number of elements in the list to be sorted and plot a graph of the time taken versusn.
4. Sort a given set of elements using Selection sort and hence find the time required to sort elements. Repeat the experiment for different values of n, the number of elements in the list to be sorted and plot a graph of the time taken versus n.
5. Implement All Pair Shortest paths problem using Floyd’s Algorithm .
6. Implement 0/1 Knapsack problem using dynamic programming.
7. From a given vertex in a weighted connected graph, find shortest paths to other vertices using Dijkstra's algorithm.
8. Sort a given set of elements using Quick sort method and determine the time taken to sort the elements. Repeat the experiment for different values of n, the number of elements in the list to be sorted and plot a graph of the time taken versusn.
9. Design, develop and run program in any language to implement the Bellman-Ford algorithm and determine its performance.
10. Design, develop and run a program in any language to implement a Edmond’s Blossom algorithm to compute augmenting path.
11. Design, develop and run program in any language to implement Strassen's algorithm to compute matrix.
12. Design, develop and write program to compute maximum flow using Edmond-Karp maximum-flow algorithm.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M-Tech.-Cyber Security | L | T | P | C |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 2 | - | - | - |
| Subject Name | | Stress Management by Yoga | | | | |
| Subject Code | | MCSYM20S211 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | - | | | | |

**Course Objective:**
After completing this module, you should be able to:
1. To achieve overall health of body and mind.
2. To overcome stress.

**Course Outcomes:**
After completion of course, students would be able to:
**CO1**. Develop healthy mind in a healthy body thus improving social health also.
**CO2**. Improve efficiency.

| Unit | Syllabus | Periods |
|---|---|---|
| UNIT-I | Definitions of Eight parts of yoga. (Ashtanga). | 15 |
| UNIT-II | Yam and Niyam. Do`s and Don't sin life.<br>i) Ahinsa, satya, astheya, bramhacharya and aparigraha.<br>ii) Shaucha, santosh, tapa, swadhyay,ishwarpranidhan. | 10 |
| UNIT-III | Asan and Pranayam:<br>i) Various yog poses and their benefits for mind & body.<br>ii)Regularization of breathing techniques and its effects-Types of pranayama. | 15 |

**REFERENCE BOOKS:**

1. Yogic Asanas for Group Tarining-Part-I": Janardan Swami Yogabhyasi Mandal, Nagpur.
2. Rajayoga or conquering the Internal Nature" by Swami Vivekananda, Advaita Ashrama (Publication Department), Kolkata.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishvavidyalaya (Sthapna Evam Sanchalana) Adhyadesh, 2020

# SCHOOL OF ENGINEERING

## SYLLABUS

## CYBER SECURITY

| Class | | M.Tech/CSE | L | T | P | Credit |
|---|---|---|---|---|---|---|
| Semester/Year | | II/I | 0 | 0 | 4 | 2 |
| Subject Name | | Soft Computing | | | | |
| Subject Code | | MCSCSE20S212 | | | | |
| Paper | English | | | | | |
| | Hindi | | | | | |
| Max. Marks | | 50 | | | | |

| List of Experiments |
|---|
| 1. To perform Union,Intersection and Complement operations.<br>2. To implement De-Morgan's Law.<br>3. To plot various membership functions.<br>4. To implement FIS Editor. Use Fuzzy toolbox to model tip value that is given after a dinner based on quality and service.<br>5. To implement FIS Editor.<br>6. Generate ANDNOT function using McCulloch-Pitts neural net.<br>7. Generate XOR function using McCulloch-Pitts neura net.<br>8. Hebb Net to classify two dimensional input patterns in bipolar with given targets.<br>9. Perceptron net for an AND function with bipolar inputs and targets.<br>10. To calculate the weights for given patterns using hetero associative neural net.<br>11. To store vector in an auto-associative net.Find weight matrix & test the net with input<br>12. To store the vector, find the weight matrix with no self-connection. Test this using a discrete Hopfield net. |