RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

Computer Science and Engineering, VII-Semester

Open Elective – CS703 (A) Cryptography & Information Security

COURSE OUTCOMES:

CO1: Understanding of the basics of Cryptography and Network Security and working knowledge of Mathematics used in Cryptology.
CO2: Understanding of previous attacks on cryptosystems to prevent future attacks from securing a message over an insecure channel by various means.
CO3: Knowledge about how to maintain the Confidentiality, Integrity and Availability of a data.
CO4: Understanding of various protocols for network security to protect against the network threats.
CO5: Getting hands-on experience of various Information Security Tools.

UNIT I:

Mathematical Background for Cryptography: Abstract Algebra, Number Theory, Modular Inverse, Extended Euclid Algorithm, Fermat's Little Theorem, Euler Phi-Function, Euler's theorem.
Introduction to Cryptography: Principles of Cryptography, Classical Cryptosystem, Cryptanalysis on Substitution Cipher (Frequency Analysis), Play Fair Cipher, Block Cipher. Data Encryption Standard (DES), Triple DES, Modes of Operation, Stream Cipher.

UNIT II:

Advanced Encryption Standard (AES), Introduction to Public Key Cryptosystem, Discrete Logarithmic Problem, Diffie-Hellman Key Exchange Computational & Decisional Diffie-Hellman Problem, RSA Assumptions & Cryptosystem,RSA Signatures & Schnorr Identification Schemes, Primarily Testing, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime., Chinese Remainder Theorem.

UNIT III:

Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function. Universal Hashing, Cryptographic Hash Function, MD, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS), Cryptanalysis: Time-Memory Trade-off Attack, Differential Cryptanalysis. Secure channel and authentication system like Kerberos.

UNIT IV:

Information Security: Threats in Networks, Network Security Controls–Architecture, Wireless Security, Honey pots, Traffic Flow Security, Firewalls – Design and Types of Firewalls, Personal Firewalls, IDS, **Email Security:** Services Security for Email Attacks Through Emails, Privacy-Authentication of Source Message, Pretty Good Privacy(PGP), S-MIME. **IP Security**: Overview of IPSec, IP& IP version 6 Authentication, Encapsulation Security Payload ESP, Internet Key Exchange IKE, **Web Security:** SSL/TLS, Basic protocols of security. Encoding –Secure Electronic Transaction SET.

UNIT V:Cryptography and Information Security Tools: Spoofing tools**:** like Arping etc., **Foot printing Tools** (ex-nslookup, dig, Whois,etc..), **Vulnerabilities Scanning Tools** (i.e. Angry IP, HPing2, IP Scanner, Global Network Inventory Scanner, Net Tools Suite Pack.), NetBIOS Enumeration Using NetView Tool, **Steganography** Merge Streams, Image Hide, Stealth Files, Blindsideusing:**STools, Steghide, Steganos**.Stegdetect, Steganalysis - Stego Watch- Stego Detection Tool, **StegSpy**.**Trojans Detection Tools**(i.e. Netstat, fPort, TCPView, CurrPorts Tool, Process Viewer), Lan Scanner Tools (i.e.look@LAN, Wireshark, Tcpdump). **DoS Attack Understanding Tools-** Jolt2, Bubonic.c, Land and LaTierra, Targa, Nemesy Blast, Panther2, Crazy Pinger, Some Trouble, UDP Flood, FSMax.

Recommended Text:

1. Cryptography and Network Security Principles and Practice Fourth Edition,William Stallings, Pearson Education.
2. Network Security Essentials: Applications and Standards, by William Stallings.Prentice Hall.
3. Behrouz A Ferouzan, “Cryptography and NetworkSecurity” Tata Mc Graw Hills, 2007
4. Charles PPfleeger, Shari Lawrence Pfleeger “Security in Computing”, 4th Edition Prentice Hall of India, 2006.
5. Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell, Chapman and Hall/CRC

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

Computer Science and Engineering, VII-Semester

Open Elective – CS703 (B) Data Mining and Warehousing

COURSE OBJECTIVES

- Student should understand the value of Historical data and data mining in solving real-world problems.
- Student should become affluent with the basic Supervised and unsupervised learning algorithms commonly used in data mining .
- Student develops the skill in using data mining for solving real-world problems.

---

1. Data Warehousing: Introduction, Delivery Process, Data warehouse Architecture, Data Preprocessing: Data cleaning, Data Integration and transformation, Data reduction. Data warehouse Design: Datawarehouse schema, Partitioning strategy Data warehouse Implementation, Data Marts, Meta Data, Example of a Multidimensional Data model. Introduction to Pattern Warehousing.

2. OLAP Systems: Basic concepts, OLAP queries, Types of OLAP servers, OLAP operations etc. Data Warehouse Hardware and Operational Design: Security, Backup And Recovery,

3. Introduction to Data& Data Mining :Data Types, Quality of data, Data Preprocessing, Similarity measures, Summary statistics, Data distributions, Basic data mining tasks, Data Mining V/s knowledge discovery in databases. Issues in Data mining. Introduction to Fuzzy sets and fuzzy logic.

4. Supervised Learning: Classification: Statistical-based algorithms, Distance-based algorithms, Decision tree-based algorithms, Neural network-based algorithms, Rule-based algorithms, Probabilistic Classifiers

5. Clustering & Association Rule mining : Hierarchical algorithms, Partitional algorithms, Clustering large databases – BIRCH, DBSCAN, CURE algorithms.Association rules : Parallel and distributed algorithms such as Apriori and FP growth algorithms.

Books Recommended:

Text Books:

1. Pang – ningTan , Steinbach & Kumar, *"Introduction to Data Mining"*, Pearson Edu, 2019.
2. Jaiwei Han, Micheline Kamber, "*Data Mining : Concepts and Techniques*", Morgan Kaufmann Publishers.

Reference Books:

1. Margaret H. Dunham, "*Data Mining : Introductory and Advanced topics*", Pearson Edu., 2009.
2. Anahory& Murray, "*Data Warehousing in the Real World"*, Pearson Edu., 2009.

COURSE OUTCOMES

After completion of this course, the students would be able to:

CO1. Understand the need of designing Enterprise data warehouses andwill be enabled to approach business problems analytically by identifying opportunities to derive business.

CO2. Compare and contrast, various methods for storing & retrieving data from different data sources/repository.

CO3. Ascertain the application of data mining in various areas and Preprocess the given data and visualize it for a given application or data exploration/mining task

CO4. Apply supervised learning methods to given data sets such as classification and its various types.
CO5. Apply Unsupervised learning methods to given data sets such as clustering and its various types.
CO6 Apply Association rule Mining to various domains.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

Computer Science and Engineering, VII-Semester

Open Elective – CS703 (C) Agile Software Development

Pre-Requisite: Software Engineering

Course Outcomes:
After completing the course student should be able to:

5. Describe the fundamental principles and practices associated with each of the agile development methods.
6. Compare agile software development model with traditional development models and identify the benefits and pitfalls.
7. Use techniques and skills to establish and mentor Agile Teams for effective software development.
8. Apply core values and principles of Agile Methods in software development.

Course Contents:

Unit-I: Fundamentals of Agile Process: Introduction and background, Agile Manifesto and Principles, Stakeholders and Challenges, Overview of Agile Development Models: Scrum, Extreme Programming, Feature Driven Development, Crystal, Kanban, and Lean Software Development.

Unit-II: Agile Projects: Planning for Agile Teams: Scrum Teams, XP Teams, General Agile Teams, Team Distribution; Agile Project Lifecycles: Typical Agile Project Lifecycles, Phase Activities, Product Vision, Release Planning: Creating the Product Backlog, User Stories, Prioritizing and Estimating, Creating the Release Plan; Monitoring and Adapting: Managing Risks and Issues, Retrospectives.

Unit-III: Introduction to Scrum: Agile Scrum Framework, Scrum Artifacts, Meetings, Activities and Roles, Scrum Team Simulation, Scrum Planning Principles, Product and Release Planning, Sprinting: Planning, Execution, Review and Retrospective; User story definition and Characteristics, Acceptance tests and Verifying stories, Burn down chart, Daily scrum, Scrum Case Study.

Unit-IV: Introduction to Extreme Programming (XP): XP Lifecycle, The XP Team, XP Concepts: Refactoring, Technical Debt, Timeboxing, Stories, Velocity; Adopting XP: Pre-requisites, Challenges; Applying XP: Thinking- Pair Programming, Collaborating, Release, Planning, Development; XP Case Study.

Unit-V: Agile Software Design and Development: Agile design practices, Role of design Principles, Need and significance of Refactoring, Refactoring Techniques, Continuous Integration, Automated build tools, Version control; Agility and Quality Assurance: Agile Interaction Design, Agile approach to Quality Assurance, Test Driven Development, Pair programming: Issues and Challenges.

Recommended Books:

1. Robert C. Martin, Agile Software Development- Principles, Patterns and Practices, Prentice Hall, 2013.
2. Kenneth S. Rubin, Essential Scrum: A Practical Guide to the Most Popular Agile Process, Addison Wesley, 2012.
3. James Shore and Shane Warden, The Art of Agile Development, O'Reilly Media, 2007.
4. Craig Larman, ―Agile and Iterative Development: A manager's Guide, Addison-Wesley, 2004.
5. Ken Schawber, Mike Beedle, Agile Software Development with Scrum, Pearson, 2001.
6. Cohn, Mike, Agile Estimating and Planning, Pearson Education, 2006.
7. Cohn, Mike, User Stories Applied: For Agile Software Development Addison Wisley, 2004.

Online Resources:

1. IEEE Transactions on Software Engineering
2. IEEE Transactions on Dependable and Secure Computing
3. IET Software
4. ACM Transactions on Software Engineering and Methodology (TOSEM)
5. ACM SIGSOFT Software Engineering Notes