FORMAL LANGUAGES AND AUTOMATA THEORY

Module - 1 (Introduction to Formal Language Theory and Regular Languages)
Introduction to formal language theory– Alphabets, Strings, Concatenation of strings, Languages.

Regular Languages - Deterministic Finite State Automata (DFA) (Proof of correctness of construction not required), Nondeterministic Finite State Automata (NFA), Equivalence of DFA and NFA, Regular Grammar (RG), Equivalence of RGs and DFA.

Module - 2 (More on Regular Languages)
Regular Expression (RE), Equivalence of REs and DFA, Homomorphisms, Necessary conditions for regular languages, Closure Properties of Regular Languages, DFA state minimization (No proof required).

Module - 3 (Myhill-Nerode Relations and Context Free Grammars)
Myhill-Nerode Relations (MNR)- MNR for regular languages, Myhill-Nerode Theorem (MNT) (No proof required), Applications of MNT.
Context Free Grammar (CFG)- CFG representation of Context Free Languages (proof of correctness is required), derivation trees and ambiguity, Normal forms for CFGs.

Module - 4 (More on Context-Free Languages)
Nondeterministic Pushdown Automata (PDA), Deterministic Pushdown Automata (DPDA), Equivalence of PDAs and CFGs (Proof not required), Pumping Lemma for Context-Free Languages (Proof not required), Closure Properties of Context Free Languages.

Module - 5 (Context Sensitive Languages, Turing Machines)
Context Sensitive Languages - Context Sensitive Grammar (CSG), Linear Bounded Automata.

Turing Machines - Standard Turing Machine, Robustness of Turing Machine, Universal Turing
Machine, Halting Problem, Recursive and Recursively Enumerable Languages.
Chomsky classification of formal languages.

Text Book
1. Dexter C. Kozen, Automata and Computability, Springer (1999)
Reference Materials
1. John E Hopcroft, Rajeev Motwani and Jeffrey D Ullman, Introduction to Automata Theory, Languages, and Computation, 3/e, Pearson Education, 2007
2. Michael Sipser, Introduction To Theory of Computation, Cengage Publishers, 2013.

COMPUTER NETWORKS

Module - 1 (Introduction and Physical Layer)
Introduction – Uses of computer networks, Network hardware, Network software. Reference models – The OSI reference model, The TCP/IP reference model, Comparison of OSI and TCP/IP reference models.

Physical Layer – Modes of communication, Physical topologies, Signal encoding, Repeaters and hub, Transmission media overview. Performance indicators – Bandwidth, Throughput, Latency, Queuing time, Bandwidth–Delay product.

Module - 2 (Data Link Layer)
Data link layer - Data link layer design issues, Error detection and correction, Sliding window protocols, High-Level Data Link Control(HDLC) protocol. Medium Access Control (MAC) sublayer –Channel allocation problem, Multiple access protocols, Ethernet, Wireless LANs - 802.11, Bridges & switches - Bridges from 802.x to 802.y, Repeaters, Hubs, Bridges, Switches, Routers and Gateways.

Module - 3 (Network Layer)
Network layer design issues. Routing algorithms - The Optimality Principle, Shortest path routing, Flooding, Distance Vector Routing, Link State Routing, Multicast routing, Routing for mobile hosts. Congestion control algorithms. Quality of Service (QoS) - requirements, Techniques for achieving good QoS.

Module - 4 (Network Layer in the Internet)
IP protocol, IP addresses, Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP). Open Shortest Path First(OSPF) Protocol,
Border Gateway Protocol (BGP), Internet multicasting, IPv6, ICMPv6.

Module – 5 (Transport Layer and Application Layer)
Transport service – Services provided to the upper layers, Transport service primitives. User Datagram Protocol (UDP). Transmission Control Protocol (TCP) – Overview of TCP, TCP segment header, Connection establishment & release, Connection management modeling, TCP retransmission policy, TCP congestion control.
Application Layer –File Transfer Protocol (FTP), Domain Name System (DNS), Electronic mail, Multipurpose Internet Mail Extension (MIME), Simple Network Management Protocol (SNMP), World Wide Web(WWW) – Architectural overview.

Text Books
1. Andrew S. Tanenbaum, Computer Networks, 4/e, PHI (Prentice Hall India).
2. Behrouz A Forouzan, Data Communication and Networking, 4/e, Tata McGraw Hill

Reference Books
1. Larry L Peterson and Bruce S Dave, Computer Networks – A Systems Approach, 5/e, Morgan Kaufmann.

2. Fred Halsall, Computer Networking and the Internet, 5/e.
3. James F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach, 6/e.
4. Keshav, An Engineering Approach to Computer Networks, Addison Wesley, 1998. 5. W. Richard Stevens. TCP/IP Illustrated Volume 1, Addison-Wesley, 2005. 6. William Stallings, Computer Networking with Internet Protocols, Prentice-Hall, 2004. 7. Request for Comments (RFC) Pages - IETF -https://www.ietf.org/rfc.html

SYSTEMS & NETWORK SECURITY

Module-1 (Principles of Network Security)
Network Security Terminologies, Network Security and Data Availability, Components of Network Security, Network Security Policies.
Network segments-Perimeter Defense, NAT, Basic architecture issues, Subnetting,Switching and VLANs, Address Resolution protocol and media access control, Dynamic Host Configuration Protocol and Addressing Control.

Module-2(Windows Security)
Windows Security at the heart of the defense, Out-ofthe-box Operating system hardening, Installing applications, Putting the workstation on the network, Operating Windows safely, Upgrades and Patches, Maintain and test the security, Attacks against the Windows workstation.

Linux Security- Physical security, Controlling the configuration, Operating Linux safely, Hardening Linux.

Module-3 (Web Browser Security)
Web Browser and Client risk- How a web browser works, Web browser attacks, Operating safely, Web security- How HTTP works, Server and Client contents, State, Attacking Web servers, Web Services. E-mail security- The e-mail risk, Protocols, Authentication, Operating safely when using email, Domain Name System – DNS basics, Purpose of DNS, Security Issues with DNS, DNS attacks.

Module-4 (Cryptography and Steganography)
Cryptography- Principles, four cryptographic primitives, Proprietary versus open source algorithms. Steganography - overview, Core areas of network security and their relation to steganography, Principles of Steganography, Types of Steganography, Steganography Versus Digital Watermarking, Types of Digital Watermarking, Goals of Digital Watermarking.

Module-5 (Network Security)
Security In Data Networks: Wireless Device security issues-GPRS security, GSM security, IP security. Wireless Transport Layer Security: Secure Socket Layer - Wireless Transport Layer Security - WAP Security Architecture - WAP Gateway.
Firewalls-types, rules, personal firewalls, Intrusion detection systems, responses to intrusion detection, Penetration testing, Auditing and Monitoring.

Text Books
1. Eric Cole, Ronald Krutz, James W. Conley, “Network Security Bible”, First Edition Wiley

India Pvt Ltd, 2010
2. Michael A Whitman, Herbert J.Mattord, “Principles of Information Security”,Cengage Learning, Fourth Edition, 2016.
References
1. William Stallings, “Network Security Essentials”,Pearson Education, 4th Edition, 2011
2. Eric Maiwald, ”Fundamentals of Network Security”, Tata McGraw-Hill, 2011

APPLIED CRYPTOGRAPHY / FOUNDATIONS OF CRYPTOGRAPHY

Module -1(Basic Concepts of Cryptography)
Attacks on Computers and Computer Security-Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms.

Cryptography: Concepts and Techniques-Introduction, plaintext and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, stenography, key range and key size, possible types of attacks.

Module-2 (Symmetric and Asymmetric Cryptography)
Symmetric key Ciphers-Block Cipher principles & Algorithms (DES, AES, Blowfish),Differential and Linear Cryptanalysis, Block cipher modes of operation, Stream ciphers,RC4,Location and placement of encryption function, Key distribution.

Asymmetric key Ciphers- Principles of public key cryptosystems, Public key Infrastructure, Algorithms (RSA, Diffie-Hellman, ECC), Key Distribution.

Module-3 (Message Authentication Algorithms)
Message Authentication Algorithms and Hash Functions- Authentication requirements, Authentication functions, Message authentication codes (MAC), Hash functions, Security of Hash functions and MAC, Message Digest 5 (MD5), Secure Hash Algorithm (SHA)-512, Hash-based Message Authentication Code (HMAC), Cipher-based Message Authentication Code (CMAC), X.509 Authentication services.

Module-4(Cryptographic Applications)
Authentication Applications- Kerberos, X.509 Authentication Service, Public – Key Infrastructure, Biometric Authentication, Multi factor Authentication.
Cryptographic Protocols-Types of protocols, Trust and computation, Validating Cryptographic protocols and attacks.Digital Signatures and Certificates-Digital Signatures, Digital Certificates,PKI and Certificate Authorities.

Module -5(Applications of Cryptography)

User authentication- password, challenge-response and zero-knowledge protocols, server authentication; application secure online banking; digital cash, application keeping/storing secrets, blockchain, application crypto currencies, implementation aspects: weakest key, key modularity, key management in cryptography, clear text cryptography.

Quantum computing, quantum-resistant cryptography, implementation aspects: creating correct and secure programs, quality of code, side-channel attacks, implementation flaws, Quantum safe cryptography, Cloud security.

Text Books

1. William Stallings, “Cryptography and Network Security Principles and Practice”, Pearson Education, 6th Edition, 2013.
2. Bruce Schneier, “Applied Cryptography Protocols, Algorithms and source code in C”, JohnWiley, 2nd Edition,1995.

References

1. Behrouz A. Forouzan,“Cryptography and Network Security”, McGraw Hill, 2nd Edition, 2010.
2. Hans Delfs and HelmutKnebl, “Introduction to Cryptography: Principles and Applications”,
3. 2nd Edition, 2007. Douglas R and Stinson, “Cryptography Theory and Practice”, Chapman & Hall/CRC, 3rd Edition, 2006.
4. Bernard Menezes, “Network Security and Cryptography”, Cengage Learning, First Edition, 2010
5. Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography”, Chapman and Hall/CRC, First Edition,2007.

MANAGEMENT OF SOFTWARE SYSTEMS

Module 1 : Introduction to Software Engineering (7 hours)

Introduction to Software Engineering - Professional software development, Software engineering
ethics. Software process models - The waterfall model, Incremental development. Process activities - Software specification, Software design and implementation, Software validation, Software evolution. Coping with change - Prototyping, Incremental delivery, Boehm's Spiral Model. Agile software development - Agile methods, agile manifesto - values and principles. Agile development techniques, Agile Project Management. Case studies : An insulin pump control system. Mentcare - a patient information system for mental health care.

Module 2 : Requirement Analysis and Design (8 hours)

Functional and non-functional requirements, Requirements engineering processes. Requirements elicitation, Requirements validation, Requirements change, Traceability Matrix. Developing use cases, Software Requirements Specification Template, Personas, Scenarios, User stories, Feature identification. Design concepts - Design within the context

of software engineering, Design Process, Design concepts, Design Model. Architectural Design - Software Architecture, Architectural Styles, Architectural considerations, Architectural Design Component level design - What is a component?, Designing Class-Based Components, Conducting Component level design, Component level design for web-apps. Template of a Design Document as per “IEEE Std 1016-2009 IEEE Standard for Information Technology Systems Design Software Design Descriptions”. Case study: The Ariane 5 launcher failure.

Module 3 : Implementation and Testing (9 hours)

Object-oriented design using the UML, Design patterns, Implementation issues, Open-source development - Open-source licensing - GPL, LGPL, BSD. Review Techniques - Cost impact of Software Defects, Code review and statistical analysis. Informal Review, Formal Technical Reviews, Post-mortem evaluations. Software testing strategies - Unit Testing, Integration Testing, Validation testing, System testing, Debugging, White box testing, Path testing, Control Structure testing, Black box testing, Testing Documentation and Help facilities. Test automation, Test-driven development, Security testing. Overview of DevOps and Code Management - Code management, DevOps automation, Continuous Integration, Delivery, and Deployment (CI/CD/CD). Software Evolution - Evolution processes, Software maintenance.

Module 4 : Software Project Management (6 hours)

Software Project Management - Risk management, Managing people, Teamwork. Project Planning, Software pricing, Plan-driven development, Project scheduling, Agile planning. Estimation techniques, COCOMO cost modeling. Configuration management, Version management, System building, Change management, Release management, Agile software management - SCRUM framework. Kanban methodology and lean approaches.

Module 5 : Software Quality, Process Improvement and Technology trends (6 hours)

Software Quality, Software Quality Dilemma, Achieving Software Quality Elements of Software Quality Assurance, SQA Tasks , Software measurement and metrics. Software Process Improvement(SPI), SPI Process CMMI process improvement framework, ISO 9001:2000 for Software. Cloud-based Software - Virtualisation and containers, Everything as a service(IaaS, PaaS), Software as a service. Microservices Architecture - Microservices, Microservices architecture, Microservice deployment.

Text Books

1. Book 1 - Ian Sommerville, Software Engineering, Pearson Education, Tenth edition, 2015.
2. Book 2 - Roger S. Pressman, Software Engineering : A practitioner’s approach, McGraw Hill publication, Eighth edition, 2014
3. Book 3 - Ian Sommerville, Engineering Software Products: An Introduction to Modern Software Engineering, Pearson Education, First Edition, 2020.

References

1. IEEE Std 830-1998 - IEEE Recommended Practice for Software Requirements SpeciÞcations
2. IEEE Std 1016-2009 IEEE Standard for Information Technology—Systems Design—Software Design Descriptions

CRYPTOGRAPHY LAB

*mandatory

1. Represent a string (char pointer) with a value “Hello world”. The program should XOR each character in this string with 0 and displays the result.*
2. Represent string (char pointer) with a value “Hello world” The program should AND or and XOR each character in this string with 127 and display the result.
3. Perform encryption and decryption using the following algorithms*
    a. Ceaser cipher
    b. Substitution cipher
    c. Hill Cipher
4. Implementation of Encryption and Decryption using DES*
5. Implementation of RSA Encryption Algorithm
6. Implementation of Hash Functions*
7. Implementation of Blowfish algorithm logic*
8. Implement the Diffie-Hellman Key Exchange mechanism
9. Implement RC4 logic using Java*
10. Encrypt the text “Hello world” using Blowfish.
11. Implement the SIGNATURE SCHEME –Digital Signature Standard*

DATABASE MANAGEMENT SYSTEMS LAB

1. Design a database schema for an application with ER diagram from a problem description **.
2. Creation, modification, configuration, and deletion of databases using UI and SQL Commands **.
3. Creation of database schema - DDL (create tables, set constraints, enforce relationships, create indices, delete and modify tables). Export ER diagram from the database and verify relationships** (with the ER diagram designed in step 1).
4. Database initialization - Data insert, Data import to a database (bulk import using UI and SQL Commands)**.
5. Practice SQL commands for DML (insertion, updating, altering, deletion of data, and viewing/querying records based on condition in databases)**.
6. Implementation of built-in functions in RDBMS**.
7. Implementation of various aggregate functions in SQL**.
8. Implementation of Order By, Group By & Having clause **.
9. Implementation of set operators nested queries, and join queries **.
10. Implementation of queries using temp tables.
11. Practice of SQL TCL commands like Rollback, Commit, Savepoint **.
12. Practice of SQL DCL commands for granting and revoking user privileges **.
13. Practice of SQL commands for creation of views and assertions ** .
14. Implementation of various control structures like IF-THEN, IF-THEN-ELSE, IF-THEN ELSIF, CASE, WHILE using PL/SQL **.
15. Creation of Procedures, Triggers and Functions**.

16. Creation of Packages **.
17. Creation of Cursors **.
18. Creation of PL/SQL blocks for exception handling **.
19. Database backup and restore using commands.
20. Query analysis using Query Plan/Show Plan.
21. Familiarization of NoSQL Databases and CRUD operations**.
22. Design a database application using any front end tool for any problem selected. The application constructed should have five or more tables**.

** mandatory