Syllabus

Course Name: Network Security & Cryptography [3:0:0=3]

Course Content:

Introduction: Attack, Services and Mechanism, Model for Internetwork Security. Cryptography: basic concepts, cryptanalytic attacks, classical techniques and cryptanalysis. Cryptography: symmetric algorithms, basic concepts and principles, block cipher modes of operation, DES, AES. Introduction to number theory. Cryptography: asymmetric algorithms (public-key cryptography), basic concepts and principles. RSA. Key management. Message Authentication, Hash function and MAC Algorithm. Digital signature, DSS. Certificates, certificate authority. Network Security Applications: Authentication Application, Kerberos, X.509, Directory Authentication Service, Pretty Good Privacy, S/MIME. IP Security Architecture: Overview, Authentication header, Encapsulating Security Pay Load combining Security Associations, Key Management. Web Security: Requirement: Secure Sockets Layer, Transport Layer Security, Secure Electronic Transactions. Network Management Security: Overview of SNMP Architecture, SNMPV1 Communication Facility, SNMPV3. System Security: Intruders, Viruses and Related Threats, Firewall Design Principles, Comprehensive examples using available software platforms/case tools, Configuration Management.

Course Outcomes:

CO1: Understand cryptography and network security concepts with their applications.

CO2: Apply security principles to design a variety of secure systems.

CO3: Analyse and design network security protocols.

Text Book:

1) Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill Education, 4e, 2019

2) Behrouz A Forouzan & Debdeep Mukopadhyaya, "Cryptography and Network security", 3rd Edition, McGraw Hill, 2015.

3) William Stallings: Cryptography and Network Security, 7th Edition, Prentice-Hall / Pearson Education, Englewood Cliffs /New Delhi, 2017.

Reference Book:

1) Michael Goodrich & Roberto Tamassia, "Introduction to Computer Security", Prentice-Hall/ Pearson Education, Englewood Cliffs/ New Delhi, 2010.

Course Name: Theory of Computation **[3:0:0=3]**

Course Content:

Computation, Alphabet, Languages and grammars, productions and derivations, Chomsky hierarchy of languages, Finite State Machine, Deterministic finite automata (DFA), Non-Deterministic Finite Automata (NDFA), NDFA with ε moves, Converting NDFA to DFA, Eliminating ε transitions, Minimization of Finite Automata, Finite Automata with output: Mealy machine, Moore Machine, Conversion of Mealy machine to Moore machine and vice-versa, Regular Expression, Conversion of Regular expression to Finite Automata and Vice-versa, Pumping Lemma for regular sets, Application of pumping Lemma, Closure properties of regular sets, Introduction to Context Free Grammar (CFG), Derivation Trees, Ambiguity in CFG, Simplification of CFG, Normal forms for CFG, Pumping Lemma for CFG, Closure properties of CFG, Definition of Pushdown Automata (PDA), Deterministic PDA, Non-deterministic PDA, PDA Corresponding to given CFG and vice-versa, Context Sensitive Languages, Linear Bounded Automata, Turing Machine model, Representation of Turing machines, Design of Turing Machines, Variants of Turing Machine, Turing machine as enumerator, Properties of recursive and recursive enumerable languages, Decidable and Undecidable problems.

Course Outcomes:

CO1: Understand the definitions of several specific models of computation including finite automata, context-free grammars, and Turing machines, learn tools for analyzing their power and limitations, and understand how they are used in other areas of computer science.

CO2: Analyze the conversion of NFA to DFA, Mealy to Moore, Moore to Mealy, regular expression to DFA, DFA to regular expression, and minimization of DFA.

CO3: Develop the PDA for the context free language and context free grammar and design the Turing machine for the real-world application.

Textbook:

1) K.L.P Mishra & N. Chandrasekaran, "Theory of Computer Science", PHI Learning.2015.
2) C. K. Nagpal, "Formal Languages and automata theory", Oxford.

Reference Book:

1) John E. Hopcroft, Jeffery Ullman, "Introduction to Automata theory, Languages & computation", Pearson.
2) John C Martin, "Introduction to languages and theory of computation", McGraw Hill.

Course Name: NoSQL Database Management **[2:0:2=3]**

Course Content:

Introduction to Databases and NoSQL: Overview of traditional relational databases, Limitations of relational databases, Introduction to NoSQL databases, Types of NoSQL databases (document-oriented, key-value, column-family, graph), Data modeling in NoSQL databases, Sharding and scalability, Consistency and CAP theorem, Performance tuning and optimization. Document-oriented Databases: MongoDB and its architecture, Document-oriented data model, BSON (Binary JSON) format, CRUD operations in MongoDB, Indexing and querying in MongoDB. Key-Value Stores: Introduction to key-value stores, Redis and its architecture, Data structures in Redis (strings, lists, sets, hashes), Redis persistence and replication. Column-family Stores: Apache Cassandra and its architecture, Data model in Cassandra, Cassandra's distributed architecture, Consistent Hashing, Managing Cluster Nodes, Data modeling and query language (CQL) in Cassandra. Graph Databases: Introduction to graph databases, Neo4j and its architecture, Graph data model and relationships, Querying and traversal in graph databases.

Course Outcomes:

CO1: Understand the characteristics and drawbacks of NoSQL databases in comparison to relational databases

CO2: Apply the principles of designing NoSQL database management systems in practical scenarios.

CO3: Analyze real-world case studies of successful NoSQL implementations.

Text Book:

1) Dan Sullivan. NoSQL for Mere Mortals. Addison-Wesley Professional. 2015. ISBN: 0134023218 (DS)
2) Guy Harrison. Next-Generation Databases. Apress. 2016. ISBN: 9781484213292 (GH)
3) Shannon Bradshaw, Eoin Brazil, Kristina Chodorow, MongoDB: The Definitive Guide: Powerful and Scalable Data Storage, 2019
4) Perkins, Luc, Jim Wilson, and Eric Redmond. Seven databases in seven weeks: a guide to modern databases and the NoSQL movement. 2018