Name of the program: M. Tech. in Information and Cyber Security

Department: Computer Science and Engineering

Semester I				
S. No.	**Subject Code**	**Title of the course**	**L-T-P**	**Credits**
1	CS-601	Modelling and Simulation	3-0-0	3
2	CS-602	Fundamentals of Cryptography	3-1-0	4
3	CS-603	Advanced Computer Networks and Security	3-0-2	4
4	CS-604	Implementation Techniques for Advanced Algorithms	3-0-2	4
5	CS-605	Cyber Laws and Information Crime	3-0-0	3
			Total credits	**18**

Semester II				
S. No.	**Subject code**	**Title of the course**	**L-T-P**	**Credits**
1	-----	Art of Engineering Research	2-0-2	3
2	-----	Machine learning	3-0-2	4
3	CS-608	Cyber Forensics: Tools and Techniques	3-0-2	4
4	CS-609	Formal Verification of Security Protocols	3-1-0	4
5	CS-6XX	Elective I	3-0-0	3
6	CS-6XX	Elective II	3-0-0	3
			Total credits	**21**

Semester III				
S. No.	**Subject code**	**Title of the course**	**L-T-P**	**Credits**
1	CS-6XX	Elective-III/MOOC	3-0-0	3
2	CS-6XX	Elective-IV/ MOOC	3-0-0	3
3	CS-698	Major Project part I		12
			Total credits	**18**

Semester IV				
S. No.	**Subject Code**	**Title of the course**	**L-T-P**	**Credits**
1	CS-6XX	Elective-V OR Elective-VI/MOOC	3-0-0	3
2	CS-699	Major Project part II		15*
			Total credits	**18**

For students going on internship in Semester IV: Major Project part II: 12 credits and additional Colloquium/Industrial Seminar: 3 credits.

Semester-1	**Semester-1**	**Semester-3**	**Semester-4**	**Total Credits**
18	21	18	18	**75**

S. No.	Electives I, III and V Category: Network Security Electives
CS-611	Wireless & Mobile Security
CS-612	Intrusion Detection and Prevention
CS-613	Web application and Cloud security
CS-614	Malware Analysis
CS-615	Authentication and Access Control
CS-616	Digital Watermarking and Steganalysis
CS-617	IoT protocols and Security
CS-618	Data privacy in Social Networks
CS-619	Blockchain Technology

S. No.	Electives II, IV and VI Category: System Security Electives
CS-621	Software System Design
CS-622	Modern Cryptography
CS-623	Database Security
CS-624	Hardware Security
CS-625	Operating Systems Security
CS-626	Fault Tolerant System
CS-627	Quantum Cryptography
CS-628	Big Data and Cyber fraud analysis
CS-629	Secure System Engineering

Course Contents

1	**Semester**	I
2	**Type of course**	Core
3	**Code of the subject**	CS-601
4	**Title of the subject**	Modelling and Simulation
5	**Any prerequisite**	Basic Mathematics
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Develop mathematical models to represent real-world systems and problems. Apply simulation tools to solve complex problems in engineering, science, and management. Develop critical thinking skills in problem-solving and model validation.
6	**Brief Contents**	Introduction to probability: Joint and Conditional Probability, Random Variables, Bayesian Networks. Optimization: System Modelling and Optimization, Optimizing Linear Systems, Nonlinear Constrained Optimization. Game Theory: Concepts and Terminology, Solving a Game, Mechanism Design, Limitations of Game Theory.
7	**Contents for lab**	No

1	**Semester**	I
2	**Type of course**	Core
3	**Code of the subject**	CS-602
4	**Title of the subject**	Fundamental of Cryptography
5	**Any prerequisite**	Computer networks, Information systems security
6	**L-T-P**	3-1-0
7	**Learning Objectives of the subject**	Describe the major security goals. Define security attacks that threaten security goals. Explain how various counter measures are used to protect security goals
8	**Brief Contents**	Introduction, Prime number generation, Shannon's theory of perfect secrecy, Traditional symmetric and asymmetric – key, Cryptographic attacks, Techniques, Substitution ciphers, Transposition ciphers, Stream ciphers, RSA cryptosystems, Rabin, El Gamal, Elliptic curve cryptosystems, Data Encryption Standard (DES) and Advanced Encryption Standard (AES), Message integrity, Message authentication and key management, Message integrity, Message authentication, Symmetric-key, Distribution, Kerberos, Public-key distribution.
9	**Contents for lab**	NA

1	**Semester**	I
2	**Type of course**	Core
3	**Code of the subject**	CS-603
4	**Title of the subject**	Advanced Computer Networks and Security
5	**Any prerequisite**	Computer networks
6	**L-T-P**	3-0-2
7	**Learning Objectives of the subject**	The aim of the course is to enable students to develop specialized theoretical and practical knowledge of different computer network protocols, security risks and threats, weaknesses in communication systems and computer networks and the corresponding methods of protection and detection of attacks.
8	**Brief Contents**	CIA triad, User authentication, Access controls: security model, policy, and mechanisms, High performance switching and routing: introduction, Performance considerations, IP address lookup, Network security-threats, Weaknesses, Attacks and countermeasures, Honeypots, Domain key identified mail, Pretty good privacy, S/MIME
9	**Contents for lab**	Wireshark, Implementation of DoS attacks, detection and analysis; Implementation of IP spoofing attack; DoS attack with spoofed IP address, detection and analysis.

1	**Semester**	I
2	**Type of course**	Core
3	**Code of the subject**	CS-604
4	**Title of the subject**	Implementation Techniques for Advanced Algorithms
5	**Any prerequisite**	Data structure and programming
6	**L-T-P**	3-0-2
7	**Learning Objectives of the subject**	To implement and learn the basic data structures and learn the appropriate algorithmic approach to a problem and implement various search and sorting techniques. To learn the appropriate algorithmic approach to a problem and implement various search and sorting techniques. Solve problems using fundamental algorithms. Demonstrate the ability to evaluate algorithms, justify that selection, and implement the algorithm in a particular context.
8	**Brief Contents**	Basics of linear and non-linear data structures, Asymptotic analysis, Recurrence relations, and Analysis of iterative and recursive algorithms. Searching and Sorting: Linear Search, Binary Search, Graph Algorithms, Introduction to recent research topics: Approximation Algorithms, Online Algorithms, Parameterized Algorithms.
9	**Contents for lab**	Implement linear and non-linear data structures, Binary trees, and Sorting techniques. Implementation of graph algorithms.

1	**Semester**	I
2	**Type of course**	Core
3	**Code of the subject**	CS-605
4	**Title of the subject**	Cyber Laws and Information Crime
5	**Any prerequisite**	No
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	To understand the basics of cyber law and its related issues. To explain the basic information on cyber security To understand the issues those are specific to amendment rights. To have knowledge on copy right issues of software. To understand ethical laws of computer for different countries and Information and Technology Act, 2000.
8	**Brief Contents**	Introduction-cyber security, Private ordering solutions, Regulation and jurisdiction for global cyber security, Copyright-source of risks, Pirates, Internet infringement, Fair use, Postings, Criminal liability, First amendments, Data losing, Trademarks, Defamation, Privacy- common law privacy, Constitutional law, Federal statutes, Anonymity, Technology expanding privacy rights, Duty of care, Criminal liability, Procedural issues, Electronic contracts & digital signatures, Misappropriation of information, Civil rights, Tax, Evidence, Ethics, Legal developments, Late 1990 to 2000, Cyber security in society, Security in cyber laws case studies, General law and cyber law-a swift analysis. Evolution of the IT act, Genesis and necessity, Salient features of the it act, 2000, Various authorities under it act and their powers-penalties & offences, Amendments, Impact on other related acts (amendments), Cyber space jurisdiction, E – commerce and laws in India, Intellectual property rights, Domain names and trademark disputes, Sensitive personal data or information (SPDI) in cyber law, Cloud computing & law, Cyber law : international perspective, Cyber forensic and Computer crimes and types, Case laws: Indian & international cases
9	**Contents for lab**	No

1	**Semester**	II
2	**Type of course**	Core
3	**Code of the subject**	-----
4	**Title of the subject**	Art of Engineering Research
5	**Any prerequisite**	No
6	**L-T-P**	2-0-2
7	**Learning Objectives of the subject**	To enable a student to develop their theoretical, methodological and research skills to enhance their ability to conduct rigorous research and reach to sound evidence-based conclusions. Understanding the nature of problem to be studied and identifying the related area of knowledge. Reviewing literature to understand how others have approached or dealt with the problem. Collecting data in an organized and controlled manner to arrive at valid decisions.
8	**Brief Contents**	Introduction to research, Analytical vs. Empirical methods, surveys, Controlled experiments, Ethnography and action research, Quantitative, Qualitative, and mixed methods, Choosing research methods, Validity threats. An empirical research framework, Research problems, Literature reviews, Introduction to quantitative research, Study designs, Controlled experiments, Elements and methods, Example experiments, Data collection techniques, Analysis and interpretation of quantitative data, Descriptive statistics, sampling, Sampling distribution, Parameter estimation, statistical inference, Confidence interval and hypothesis testing, Tests of significance, Test of difference of mean and proportions, T-tests, ANOVA, Chi-square tests, Correlation, and regression, Review process, Review guidelines, Validity threats, Review decisions, Qualitative methods, Study designs, Elements, and methods, Data collection methods - primary and secondary sources, Types of data analysis methods, Survey research, Sampling methods, Survey study designs, Case studies, Introduction to mixed methods research, Study designs and method, Writing research papers, Purpose, nature and evaluation, Content and format, Research presentations, The art of scientific and technical writing.
9	**Contents for lab**	Problem statement practice Literature survey practice Technical paper writing – practice Presentation – practice

1	**Semester**	II
2	**Type of course**	Core
3	**Code of the subject**	------
4	**Title of the subject**	Machine learning
5	**Any prerequisite**	Linear algebra
6	**L-T-P**	3-0-2
7	**Learning Objectives of the subject**	To understand popular ML algorithms with their associated mathematical foundations for appreciating these algorithms. To help connect real-world problems to appropriate ML algorithm(s) for solving them and to enable formulating real world problems as machine learning tasks.
8	**Brief Contents**	Introduction to ML, Fundamentals of ML - PCA and Dimensionality reduction, Nearest neighbours and KNN, Linear regression, Decision tree classifiers, Notion of generalization and concern of overfitting, Notion of training, Validation, and testing; Connect to generalization and overfitting. Selected algorithms - ensembling and RF, Linear SVM, K means, Logistic regression, Naive bayes, Neural network learning - Role of loss functions and optimization, Gradient descent and Perceptron/Delta learning, MLP, Backpropagation, MLP for classification and regression, Regularization, Early Stopping, Kernels (with SVM), Bayesian methods, Generative methods, HMM, EM, PAC learning, Introduction to Deep Learning, CNNs, Popular CNN architectures, RNNs, GANS and Generative models, Advances in backpropagation and optimization for neural networks adversarial learning.
9	**Contents for lab**	To implement basic algorithms using basic machine learning libraries mostly in python. Gain hands-on experience in applying ML to problems encountered in various domains. In addition, obtain exposure to high-level ML libraries or frameworks such as TensorFlow, PyTorch.

1	**Semester**	II
2	**Type of course**	Core
3	**Code of the subject**	CS-608
4	**Title of the subject**	Cyber Forensics: Tools and Techniques
5	**Any prerequisite**	Cryptography, network security
6	**L-T-P**	3-0-2
7	**Learning Objectives of the subject**	Overview of windows forensics; file system analysis; overview of memory forensics; anti-forensic techniques; hypervisor files and formats; forensic analysis of a virtual machine ; overview of cloud forensics
8	**Brief Contents**	**Windows Forensics** - Volatile data collection, Non-volatile data collection, Registry Analysis, Browser Usage, Hibernate File Analysis, Crash Dump Analysis, File System Analysis, File Metadata and Timestamp Analysis, Event Viewer Log Analysis, MFT analysis, Timeline Creation, Evidence Collection in Operating system, **Memory Forensics** - History of Memory Forensics, x86/x64 architecture, Data structures, Volatility Framework & plugins Memory acquisition, File Formats – PE/ELF/Mach-O, Processes and process injection, Command execution and User activity, Networking, sockets, paged memory and advanced registry artifacts, Related tools – Bulk Extractor and YARA, Timelining memory, Recovering and tracking user activity, Recovering attacker activity from memory, Introduction to Anti-forensics, tools and techniques, **Virtual Machine Forensics** - Types of Hypervisors, Hypervisor Files and Formats, Use and Implementation of Virtual Machines in Forensic Analysis, Use of VMware to establish working version of suspect's machine, Networking and virtual networks within Virtual Machine, Forensic Analysis of a Virtual Machine, **Cloud Forensics** - Cloud Storage Forensic Framework, Dropbox analysis: Data remnants on user machines, Evidence source identification and analysis, Collection of evidence from cloud storage services, Examination and analysis of collected data. Google Drive: Forensic analysis of Cloud storage and data remnants, Evidence source identification and analysis - Collection of evidence from cloud storage services, Examination and analysis of collected data, Issues in cloud forensics.
9	**Contents for lab**	No

1	**Semester**	II
2	**Type of course**	Core
3	**Code of the subject**	CS-609
4	**Title of the subject**	Formal Verification of Security Protocols
5	**Any prerequisite**	Basic knowledge of computer security and discrete mathematics
6	**L-T-P**	3-1-0
7	**Learning Objectives of the subject**	To understand the theoretical foundation behind a security protocol. To Understand the principles of formal verification and its application to security protocols. To Understand the various types of security protocols and their vulnerabilities. To Learn how to specify security properties and verify their correctness using formal verification tools.
8	**Brief Contents**	Basic of Logics: BNF, Labelled transition systems, Operational semantics, Protocol specification, describing protocol execution, Security properties: secrecy, authentication, Aliveness, Synchronization, the analysis of security protocols: abstract state machines, Belief logics, Constraint, Provable security, modelling guessable numbers, Modelling time, The BAN Kerberos Protocol, modelling ban Kerberos, Verifying ban Kerberos.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-611
4	**Title of the subject**	Wireless & Mobile Security
5	**Any prerequisite**	Mobile computing & wireless networks, security fundamentals
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Issues and technologies involved in designing a wireless and mobile system that is robust against various attacks. Broad knowledge of the state-of-the-art and open problems in wireless and mobile security, enhancing potential to do research or pursue a career in this rapidly developing area. Learn various security issues related to GPRS and 4G/5G.
8	**Brief Contents**	Mobile communication history, Security – wired vs wireless, Security issues in wireless and mobile communications, Security requirements in wireless and mobile communications, Security for mobile applications, advantages and disadvantages of application – level security, Mobile devices security requirements, Mobile wireless network level security, Server level security. Application-level security in wireless networks: application of WLANs, Wireless threats, Some vulnerabilities and attach methods over WLANs, Security for wi-fi, Generations of cellular networks, Security issues and attacks in cellular networks, GSM security for applications, GPRS security for applications, UMTS security for applications, 3G security for applications, Some of security and authentication solutions, MANET, Some applications of MANETs, MANET features, Security challenges in MANET, Security attacks on MANET, External threats for MANET applications, Internal threats for MANET applications, Some of the security solutions. Ubiquitous computing, Need for novel security schemes for ubiquitous computing, Security challenges for ubiquitous computing, and security attacks on ubiquitous computing networks, Some of the security solutions for ubiquitous computing.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-612
4	**Title of the subject**	Intrusion detection and prevention
5	**Any prerequisite**	Computer networks, Operating systems, Information systems security
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	To give students practical, working knowledge in intrusion detection and traffic analysis. To gain an understanding of the workings of TCP/IP, methods of network traffic analysis and popular network intrusion detection systems.
8	**Brief Contents**	IDS/IPS definition and classification -Basic elements of attacks and their detection -Misuse detection systems, Anomaly detection systems and supervised learning in IDS, Testing IDS and measuring their performances, Computational complexity, Theoretic IDS models and quality criteria, Intrusion detection in virtual networks, Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-613
4	**Title of the subject**	Web application and cloud security
5	**Any prerequisite**	Operating system, Distributed system, Information security
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Cloud services facilitate access to server infrastructure which is managed by the provider, which includes data storage and access, security and scalability and updates. This course aims at providing the students an insight into the operations of cloud and introduces them to different cloud providers available.
8	**Brief Contents**	Introduction to cloud computing, Cloud service delivery models, Cloud deployment models, Cloud computing security, Scalable application on AWS, Provisioning application resources with cloud formation, AWS security, AWS directory service, AWS key management service, Cloud deployment models – Public, Private and hybrid, Trusted cloud initiative (TCI) and cloud trust protocol (CTP), Transparency as a service (TaaS) and Security as a service (SaaS), cloud security, Top threats to cloud security, Comparison of traditional it and cloud security.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-614
4	**Title of the subject**	Malware analysis
5	**Any prerequisite**	Information system security, Machine learning
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Learn how to dissect malware to gather information about the malware functionality, perform analysis on all major file types and understand how the system was compromised so that you can defend against future attacks.
8	**Brief Contents**	Introduction to malware, Types and goals of malware analysis process, Virtual machine setup, Analyzing malicious windows programs, Static analysis and dynamic analysis, Analysis of malicious documents, Malware defences.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-615
4	**Title of the subject**	Authentication and access control
5	**Any prerequisite**	Information system security
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Introduce the concept of access control to information systems in applications, authentication, and accounting for end users and system administrators. Learn the security controls for access control including tokens, biometrics, and use of public key infrastructures (PKI).
8	**Brief Contents**	Access control and assessing risk, Business drivers and access control policies standards, Procedure and guidelines, unauthorized access – security breaches and mapping business challenges, Human nature – organizational behaviour and access control for information systems, Physical security and access control in the enterprise, Access control implementation for systems and remote workers, PKI infrastructure and encryption, Testing access control systems and assurance
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-616
4	**Title of the subject**	Digital watermarking and steganalysis
5	**Any prerequisite**	Image processing, Information security
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	To learn about the watermarking models and message coding. To learn about watermark security and authentication. To learn about steganography and perceptual models.
8	**Brief Contents**	Applications and properties, evaluating watermarking systems, Models of watermarking, Communication based watermarking, Geometric models of watermarking, Modelling watermarks detection by correlation, Informed embedding, Informed coding, Dirty paper codes, Perceptual model, Watson's model, Adaptive watermarking, Robust watermarking, Watermark security secret writing and steganography, Watermarking for copyright protection.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-617
4	**Title of the subject**	IoT protocols and security
5	**Any prerequisite**	Programming in C, Computer network fundamentals
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	The advanced topics of IoT security and privacy challenges. systematic analysis of IoT security hardware, communication, and system perspectives.
8	**Brief Contents**	Fundamentals, Architecture of IoTs, IoT security requirements, IoT privacy preservation issues, Attack Models – attacks to sensors in IoTs, Attacks to RFIDs in IoTs, Attacks to network functions in IoTs, Attacks to back-end systems, Security in front-end sensors and equipment, Prevent unauthorized access to sensor data, M2M security, RFID security, Cyber-physical object security, Hardware security, Front-end system privacy protection, Networking function security- IoT networking protocols, Secure IoT lower layers, Secure IoT higher layers, Secure communication links in IoTs, Back-end security -secure resource management, Secure IoT databases, Security products-existing testbed on security and privacy of IoTs, Commercialized products
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-618
4	**Title of the subject**	Data privacy in social network
5	**Any prerequisite**	Fundamental knowledge of computing and programming
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Increase the understanding of privacy aspects on various online platforms. Understand the threats and defend user privacy through real-time and scalable systems.
8	**Brief Contents**	Various privacy breaches and its effects; Privacy cases, litigations, and outcomes, Difference between data security and data privacy; Contextual integrity theory and applications, Online Social Networks (OSN), Data collection from social networks, Challenges, Opportunities, and pitfalls in online social networks, Image and location privacy; Ethics; Conducting studies; Privacy from 3rd party trackers and advertisers, Phishing in OSM and identifying fraudulent entities in online social networks, Privacy policies.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-619
4	**Title of the subject**	Blockchain technology
5	**Any prerequisite**	Basic cryptography and data structure
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Get an overview of blockchain technology, its history, benefits, drawbacks, and future. Examine the nascent blockchain technology and make an initial pass at identifying some of its major vulnerabilities. Design, build, and deploy distributed applications. Equip students with the skills necessary to create e-governance applications for the public good.
8	**Brief Contents**	Overview of blockchain technology, Peer-to-Peer networking, Blockchain categories, Mining mechanism, Blockchain architecture: Pros & Cons, Bitcoin & protocol, Architecture of blockchain- Block, Byzantine General problem and Fault tolerance, Merkle tree, transactions and fee, Anonymity, Reward, Private and public blockchain, Bitcoin transaction structure, Double spending problem, Introduction to consensus Problem real time of application of blockchain.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-621
4	**Title of the subject**	Software system design
5	**Any prerequisite**	Basic software engineering course
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Outline the software design process and demonstrate how the essential design principles are applied within it. Illustrate the essential elements of software structure and architecture in terms of styles, patterns and families of programs and frameworks. Demonstrate the application of quality analysis and evaluation principles. Employ function, object, data-structure, and component-based design methodologies in a typical software design project.
8	**Brief Contents**	Software design fundamentals, Key issues in software design, Concurrency, Control and handling of events, Error exception handling and fault tolerance, Software structure and architecture, design patterns, architecture design decisions, User interface design, Metaphors and conceptual models, Software design quality analysis and evaluation, Structural descriptions (static view), Behavioural descriptions (dynamic view), Software design strategies and methods
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-622
4	**Title of the subject**	Modern cryptography
5	**Any prerequisite**	Fundamental knowledge of cryptography
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	To develop a framework to understand and implement cryptographic aspects. To enhance an ability to analyze a problem and identify and define the computing requirements for data security.
8	**Brief Contents**	Classical encryption techniques, Security attacks, Block cipher principles, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), Block cipher modes of operation, Blowfish, RC4 algorithm, Principles of public key cryptosystems, The RSA algorithm, Diffie Hellman key exchange, ElGamal Encryption, Elliptic curve cryptography, Authentication, MAC, Hash functions, Digital signatures, Authentication protocols, SHA, MD5, Zero-knowledge proof systems, Oblivious transfer, Multi-party secret sharing, Two-party computation using garbled circuits, fully homomorphic encryption.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-623
4	**Title of the subject**	Database security
5	**Any prerequisite**	Knowledge of database management system
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Learn techniques to protect databases against compromises of their confidentiality, integrity and availability. Explain the place of database security in the context of security analysis and management.
8	**Brief Contents**	Database design and use of DBMS, Relational models, Relational algebra and design principles, Datalog, Physical security, Information system access control, Authorization, identification, Authentication, Accountability, Access control matrix, Use of views, Security logs and audit trails, SQL data control language (authorization graphs), Statistical database security, SQL injection, Proxy servers, Firewalls, Digital signatures, Certification authorities (SSL, Kerberos), Micro-databases, Linking attacks, k-anonymity, l-diversity, t-closeness, Differential privacy.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-624
4	**Title of the subject**	Hardware security
5	**Any prerequisite**	Digital logic design, Information system security, Computer programming, Cryptography
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	This course covers basic concepts in the security of hardware systems. Understand the vulnerabilities in current digital system design process and various attacks to the hardware designs. Get acquainted with the tools and skills to build secure and trusted hardware.
8	**Brief Contents**	Digital system design: Basics and vulnerabilities, Active and passive attacks, reverse engineering, Counterfeiting, and design of hardware security primitives, Side channel attacks and countermeasures, Hardware trojan detection and trusted IC design
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-625
4	**Title of the subject**	Operating system security
5	**Any prerequisite**	Operating systems
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	This course is a study of the principles and concepts of Network Security from the perspective of the Operating System (OS). Students will examine the principles, practices, and policies related to hardening and securing Operating Systems, so they are impervious to security threats. It focuses on the vulnerabilities and the related countermeasures of various Operating Systems and Network Devices.
8	**Brief Contents**	System security, MS windows security, Linux security, UNIX security, Embedded and real-time OS, System reliability, OS security mechanisms, Security administration, Delegation of authority, Group policy design, Security configuration, Password requirements, security services, Protection models, Protection levels, protection domains, Capabilities, Sharing, System kernel security, Resource control, Secure booting, Firewalls and border security, Security models and policies, Security levels, Authentication, Confidentiality, Integrity, Access control strategies access matrix, Access control list, mandatory, Discretionary, Monitoring, Auditing, accountability, Privilege, account security, File system protection, Registry security, Threat analysis, Security attacks, Security-hardened operating, New risks, Threats, and vulnerabilities associated with the Microsoft Windows operating system. Emphasis on Windows latest versions, on the desktop, and windows Server latest versions. Emphasis on how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft windows operating systems and applications, OS hardening, Application security, and incident management, among other issues.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-626
4	**Title of the subject**	Fault tolerant systems
5	**Any prerequisite**	Probability and statistics
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	This course introduces basic concepts of design and implementation of fault tolerance in general systems. The purpose of this course is to establish fault tolerance as a measure to improve the dependability of systems in the presence of faults and correlating this dependability with the effects to the system and functional safety. The students will be exposed with the quantitative and qualitative methodology used for computation of fault tolerance.
8	**Brief Contents**	Basic concept of reliability, Fundamentals of dependability, Dependability evaluation, Test generation, Fault diagnosis and self-repair, Fault-Tolerant design of Digital Systems, Self- checking and Fail-safe logic, Design for testability, Verification and validation, Software fault tolerance, Case studies
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-627
4	**Title of the subject**	Quantum cryptography
5	**Any prerequisite**	Familiarity with basic notions in cryptography (encryption, authentication, security definitions.
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Basic understanding about Quantum Information and Computation. Getting an overall understanding about Quantum Key Distribution and Secret Sharing protocols. To obtain the flavour of quantum supremacy over classical computation. Design reliability models for software systems.
8	**Brief Contents**	Introduction to quantum computing, Quantum money and its attacks, Mathematical model for quantum mechanics, Quantum algorithms (Lattice cryptography, Dihedral Hidden Subgroup Problem, Other Post-quantum Cryptosystems) and their attacks, Quantum encryption and notions of security. The quantum one-time pad, Measuring randomness, Extractors and privacy amplification, Information reconciliation, Two-party quantum cryptography, Quantum true random number generators, Other cryptologic issues.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-628
4	**Title of the subject**	Big data and cyber fraud analysis
5	**Any prerequisite**	Basic concepts of mathematics and information security
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Formulate and evaluate reasons for using data analysis to detect frauds in the cyberspace. Make users familiar with different types of cybercrimes and acquire necessary knowledge and skill to prevent the occurrence of such crimes in organizations.
8	**Brief Contents**	Cyberspace, Attack, Attack vector, Attack surface, Threat, risk, Vulnerability, Exploit, Exploitation, Hacker, Non-state actors, Cyber terrorism, Introduction to cybercrime: Concepts and techniques, Channels of cybercrimes, Cybercrime methods, Computer insecurity, Computer fraud protection, Incident of cybercrimes, Cybercrime risk management, Cyber forensics, Online transactions, Global payment processing, Payment cards & data security, electronic card frauds - ATM cards, Credit cards, Smart cards, Cyber law in India, Information technology act – 2000, Regulatory compliance.
9	**Contents for lab**	No

1	**Semester**	II/III/IV
2	**Type of course**	Elective
3	**Code of the subject**	CS-629
4	**Title of the subject**	Secure System Engineering
5	**Any prerequisite**	Basic Software Engineering course
6	**L-T-P**	3-0-0
7	**Learning Objectives of the subject**	Assess software security requirements to prevent data loss. Design software to meet software security requirements. Develop strategies to mitigate security vulnerabilities. Develop guidelines for operational security. Conduct software security reviews and audits. Develop a software security monitoring policy.
8	**Brief Contents**	Software vulnerabilities, Software security and software quality assurance, Security requirement gathering principals and guidelines, Secure software architecture, Architecture risk analysis, Software security knowledge for architecture and design, Security guideline and attack patterns, Testing software vulnerability in SDLC, Mitigating Software Vulnerabilities in SDLC, Static analysis techniques, Security testing, Operating software security, Maintaining software security
9	**Contents for lab**	No