MATHEMATICAL FOUNDATION OF COMPUTER SCIENCE
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	**18SFC11** / 18LNI11 / 18SCE11 / 18SCS11 / 18SCN11 / 18SSE11 / 18SIT11	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- To acquaint the students with mathematical/logical fundamentals including numerical techniques,
- To understand probability, sampling and graph theory that serve as an essential tool for applications of computer and information sciences.

Module 1	**Contact Hours**
Numerical Methods: Significant figures, Error definitions, Approximations and round off errors, accuracy and precision. Roots of Equations: Bairstow-Lin's Method, Graeffe's Root Squaring Method. Computation of eigen values of real symmetric matrices: Jacobi and Givens method. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Statistical Inference: Introduction to multivariate statistical models: Correlation and Regression analysis, Curve fitting (Linear and Non linear) **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Probability Theory: Probability mass function (p.m.f), density function (p.d.f), Random variable: discrete and continuous, Mathematical expectation, Sampling theory: testing of hypothesis by t-test and chi - square distribution. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Graph Theory: Isomorphism, Planar graphs, graph coloring, Hamilton circuits and Euler cycle. Specialized techniques to solve combinatorial enumeration problems. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Vector Spaces: Vector spaces; subspaces; Linearly independent and dependent vectors ; Bases and dimension; coordinate vectors-Illustrative examples. Linear transformations; Representation of transformations by matrices; linear functional; Non singular Linear transformations; inverse of a linear transformation- Problems. **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

- Understand the numerical methods to solve and find the roots of the equations.
- Utilize the statistical tools in multi variable distributions.
- Use probability formulations for new predictions with discrete and continuous RV's.
- To understand various graphs in different geometries related to edges.
- Understand vector spaces and related topics arising in magnification and rotation of images.

Question paper pattern:
The question paper will have ten questions.

There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Steven C. Chapra and Raymond P Canale: " Numerical Methods for Engineers, 7th Edition, McGraw-Hill Publishers, 2015.
2. T.Veerarajan: "Probability, Statistics and Random Process",3rd Edition,Tata Mc-Graw Hill Co.,2016.
3. David C.Lay, Steven R.Lay and J.J.McDonald: Linear Algebra and its Applications, 5th Edition, Pearson Education Ltd., 2015.

Reference Books:

1. **B.S. Grewal**: Higher Engineering Mathematics, Khanna Publishers, 44th Ed., 2017.
2. **John Vince :** "Foundation Mathematics for Computer Science", Springer International Publishing, Switzerland, 2015
3. **M.K.Jain, S.R.K.Iyengar and R.K.Jain:** Numerical Methods for Scientific and Engineering Computation. 6th Ed.,New Age Int.Publishers.2012.
4. **Norman L.Biggs**: Discrete Mathematics, 2nd Ed., Oxford University Press, 2017.

Web links and Video Contacts:

1. *http://nptel.ac.in/courses.php?disciplineId=111*
2. *http://www.class-central.com/subject/math(MOOCs)*
3. *http://ocw.mit.edu/courses/mathematics/*

ETHICAL HACKING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	**18SFC12**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Learn aspects of security, importance of data gathering, foot printing and system hacking.
- Learn tools and techniques to carry out a penetration testing.
- How intruders escalate privileges?
- Explain Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
- Compare different types of hacking tools.

Module 1	**Contact Hours**
Casing the Establishment: What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access, After hacking root. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, Brute-Force Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of Dos Attackers, Types of DoS attacks, Generic Dos Attacks, UNIX and Windows DoS. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking. **RBT:L1, L2, L3**	**10 Hours**
Course Outcomes	
The students should be able to:	

- Explain aspects of security, importance of data gathering, foot printing and system hacking.
- Explain aspects of security, importance of data gathering, foot printing and system hacking.
- Demonstrate how intruders escalate privileges.
- Demonstrate how intruders escalate privileges.
- Demonstrate how intruders escalate privileges.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata Mc Graw Hill Publishers, 2010.
2. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall of India, 2010.

Reference Books:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, "Hacking Exposed Network Security Secrets & Solutions", 5th Edition, Tata Mc Graw Hill Publishers, 2010.
2. Rafay Baloch, "A Beginners Guide to Ethical Hacking".
3. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, "Gray Hat Hacking The Ethical Hackers Handbook", 3rd Edition, McGraw-Hill Osborne Media paperback(January 27, 2011)

PRAGMATICS OF INFORMATION SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	**18SFC13**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain the fundamentals of Cryptography.
- Acquire knowledge on cryptographic tools used to provide confidentiality, integrity and authenticity.
- Differentiate the various user authentication methods, access control schemes and authentication applications.
- Acquire the knowledge on IP Security tools.
- Acquire the knowledge about malicious software.

Module 1	**Contact Hours**
Overview: Computer Security Concepts, Requirements, Architecture, Trends, Strategy Perimeter Security: Firewalls, Intrusion Detection, Intrusion Prevention systems, Honeypots Case Study: Readings, Intrusion and intrusion detection by John McHugh. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
User Authentication: Password, Password-based, token based, Biometric, Remote User authentication. Access Control: Principles, Access Rights, Discretionary Access Control, Unix File Access Control, Role Based Access Control Internet Authentication Applications: Kerberos, X.509, PKI, Federated Identity Management. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Cryptographic Tools: Confidentiality with symmetric encryption, Message Authentication & Hash Functions, Digital Signatures, Random Numbers. Symmetric Encryption and Message Confidentiality: DES, AES, Stream Ciphers, Cipher Block Modes of Operation, Key Distribution. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Internet Security Protocols: SSL, TLS, IPSEC, S/ MIME. Public Key Cryptography and Message Authentication: Secure Hash Functions, HMAC, RSA, Diffie Hellman Algorithms Case Study: Readings, Programming Satan's Computer Ross Anderson and Roger Needham. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Malicious Software: Types of Malware, Viruses & Counter Measures, Worms, Bots, Rootkits Software Security: Buffer Overflows, Stack overflows, Defense, Other overflow attacks Case Study. **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

The students should be able to:

- Explain the fundamentals of Cryptographic techniques.
- Identify the security issues in the network and resolve it.

- Implement security algorithms in the field of Information technology
- Identifying the type of malware attacks and implementing preventive measures.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Computer Security: Principles and Practice, William Stalling & Lawrie Brown, 2008, Indian Edition 2010, Pearson.

Reference Books:

1. Readings: Smashing The Stack For Fun And Profit, Aleph One http:// www.phrack.com/ issues.html ? issue = 49&id=14#article
2. Chuck Easttom, " Computer Security Fundamentals" Pearson, 2012.

CYBER CRIME AND CYBER FORENSICS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	18SCN321 / **18SFC14**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain the fundamentals of Cyber Crime.
- Analyze the nature and effect of cybercrime in society.
- Demonstrate Accounting Forensics.
- Explain Computer Crime and Criminals and Liturgical Procedures.

Module 1	**Contact Hours**
Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime, Social Engineering, Categories of Cyber Crime, Property Cyber Crime. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies, Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies. **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

The students should be able to:

- Explain the fundamentals and types of cybercrime.
- Distinguish various types of computer crime.
- Illustrate computer forensic techniques to identify the digital forensics associated with criminal activities.
- Apply forensic analysis tools to recover important evidence for identifying computer crime.

- Discuss laws and ethics involved in cyber crime.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004. "Understanding Forensics in IT ", NIIT Ltd, 2005.
2. Nelson Phillips and Enfinger Steuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.

Reference Books:

1. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics ", Tata McGraw -Hill, New Delhi, 2006.
2. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.

ACCESS CONTROLAND IDENTITY MANAGEMENT SYSTEM
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	**18SFC151**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Compute tasks with security contexts.
- Different classifications of identity management system.
- Various models for Trust paradigms.
- Discretionary access model and Access Matrix Model.
- Classify all the active entities of a protection system.

Module 1	**Contact Hours**
Access control: Introduction, Attenuation of privileges, Trust and Assurance, Confinement problem, Security design principles, Identity Management models, local, Network, federal , global web identity, XNS approach for global Web identity, Centralized enterprise level Identity Management. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Elements of trust paradigms in computing, Third party approach to identity trust, Kerberos, Explicit third party authentication paradigm, PKI approach to trust establishment, Attribute certificates, Generalized web of trust models, Examples. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Mandatory access control, comparing information flow in BLP and BIBA models, Combining the BLP and BIBA models, Chinese wall problem. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Discretionary access control and Access matrix model, definitions, Safety problem, The take grant protection model, Schematic protection model, SPM rules and operations, Attenuating, Applications **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Role based access control, Hierarchical Access Control, Mapping of a mandatory policy to RABC, Mapping discretionary control to RBAC, RBAC flow analysis, Separation of Duty in RBAC, RBAC consistency properties, The privileges perspective of separation of duties, Functional specification for RBAC. **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

The students should be able to:

- Analyze to compute tasks with security contexts.
- Categorize the identity management system into different classes.
- Measure the different elements of Trust paradigms for various models.
- Compare and contrast between Discretionary access model and Access Matrix Model.
- Categorize all the active entities of a protection system.

Question paper pattern:

The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.
Text Books: 1. Messoud Benantar, "Access Control Systems: Security, Identity 2. Management and Trust Models", Springer, 2009.
Reference Books: 1. Elena Ferrari and M. Tamer A-zsu , "Access Control In Data Management 2. Systems", Morgan & Claypool Publishers, 2010.

CLOUD SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	18LNI333 / 18SCE331 / 18SCN154 / **18SFC152**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Describe the fundamentals of Cloud Computing.
- Summarize the need of cloud compliance and existing cloud solutions.
- Explain the cloud security concepts.
- Demonstrate the operations of Data Centre.
- Distinguish the concepts of Identity management and virtualization.

Module 1	**Contact Hours**
Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated. **RBT:L1, L2**	**10 Hours**
Module 2	
Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP). **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Data Center Operations: Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Identity and Access Management: Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS , IDaaS Security Recommendations. Virtualization: Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage	**10 Hours**

Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations. **RBT:L1, L2, L3**	

Course Outcomes

The students should be able to:

- Demonstrate the growth of Cloud computing, architecture and different modules of implementation.
- Evaluate the different types of cloud solutions among IaaS, PaaS, SaaS.
- Access the security implementation flow, actions and responsibilities of stake holders.
- Generalize the Data Centre operations, encryption methods and deployment details.
- Provide recommendations for using and managing the customer's identity and choose the type of virtualization to be used.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance", Oreilly Media 2009.

Reference Books:

1. Vic (J.R.) Winkler, "Securing the Cloud, Cloud Computer Security Techniques and Tactics", Syngress, April 2011.

ADVANCED CRYPTOGRAPHY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	18LNI254 / **18SFC153**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- The concepts of principles and practice of cryptography and network security.
- Overview of the Feistel cipher, Distribution of Public Keys, digital signatures and Authentication protocols.
- How to analyze the security of multiple encryption schemes and Triples DES.
- Structure and Building of secure authentication systems using message authentication techniques.
- The concepts of principles and practice of visual cryptography.

Module 1	**Contact Hours**
OSI security architecture: Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Key management: Diffie Hellman key exchange, Elliptic curve architecture and cryptography, Introduction to number theory, Confidentiality using symmetric encryption, Public key cryptography and RSA. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Authentication requirements: Authentication functions, Message authentication codes, Hash functions, Security of hash functions and MACS, MD5 Message Digest algorithm, Secure hash algorithm, Ripend, HMAC digital signatures, Authentication protocols. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. non local interactions, entanglements, EPR paradox, Bell's theorem, Bell basis, teleportation of a single qubit theory and experiments. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Future trends: Review of recent experimental achievements, studyon technological feasibility of a quantum computer candidate physical systems and limitations imposed by noise. **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

The students should be able to:

- Explain the concepts of principles and practice of cryptography and network security.
- Present an overview of the Feistel cipher, Distribution of Public Keys, digital signatures and Authentication protocols.

- Analyze the security of multiple encryption schemes and Triples DES.
- Build secure authentication systems by use of message authentication techniques.
- Explain the concepts of principles and practice of visual cryptography.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. William Stallings, "Cryptography and Network Security -Principles and Practices", 3rd Edition, Prentice Hall of India, 2003.
2. Atul Kahate, "Cryptography and Network Security", Tata McGraw -Hill, 2003.
3. William Stallings, "Network Security Essentials: Applications and Standards", Pearson Education Asia, 2000.

Reference Books:

1. R. P. Feynman, "Feynman Contacts on computation", Penguin Books, 1996.
2. Gennady P. Berman, Gary D. Doolen, Ronnie Mainiri & Valdmis Itri Frinovich, "Introduction to quantum computers", World Scientific, Singapore, 1998.
3. Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography" Principles And Protocols",CRC Press.

APPLICATION AND WEB SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	**18SFC154**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Web application's vulnerability and malicious attacks.
- Basic web technologies used for web application development.
- Basic concepts of Mapping the application
- Illustrate different attacking illustrations.
- Basic concepts of Attacking Data Stores.

Module 1	**Contact Hours**
Web Application (In) security: The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications , Web Application Security. Core Defense Mechanisms: Handling User Access Authentication, Session Management, Access Control, Handling User Input, Varieties of Input Approaches to Input Handling, Boundary Validation. Multistep Validation and Canonicalization: Handling Attackers, Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, Client-Side Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks. **RBT:L1, L2**	**10 Hours**
Module 3	
Mapping the Application: Enumerating Content and Functionality, Web Spidering, User-Directed Spidering, Discovering Hidden Content, Application Pages Versus Functional Paths, Discovering Hidden Parameters, Analyzing the Application, Identifying Entry Points for User Input, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Attacking Authentication: Authentication Technologies, Design Flaws in Authentication Mechanisms, Bad Passwords, Brute-Forcible Login, Verbose Failure Messages, Vulnerable Transmission of Credentials, Password Change, Functionality, Forgotten Password Functionality, "Remember Me" Functionality, User Impersonation, Functionality Incomplete, Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords, Insecure Distribution of Credentials. Attacking Access Controls: Common Vulnerabilities, Completely Unprotected, Functionality Identifier-Based Functions, Multistage Functions, Static Files, Platform Misconfiguration, Insecure Access Control Methods. **RBT:L1, L2, L3**	**10 Hours**

Module 5	
Attacking Data Stores: Injecting into Interpreted Contexts, Bypassing a Login, Injecting into SQL, Exploiting a Basic Vulnerability Injecting into Different Statement Types, Finding SQL Injection Bugs, Fingerprinting the Database, The UNION Operator, Extracting Useful Data, Extracting Data with UNION, Bypassing Filters, Second-Order SQL Injection, Advanced Exploitation Beyond SQL Injection: Escalating the Database Attack, Using SQL Exploitation Tools, SQL Syntax and Error Reference, Preventing SQL Injection. **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

The students should be able to:

- Achieve Knowledge of web application's vulnerability and malicious attacks.
- Understand the basic web technologies used for web application development
- Understands the basic concepts of Mapping the application.
- Able to illustrate different attacking illustrations
- Basic concepts of Attacking Data Stores.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. The Web Application Hacker's Handbook: Finding And Exploiting Security
2. Defydd Stuttard, Marcus Pinto Wiley Publishing, Second Edition.

Reference Books:

1. Professional Pen Testing for Web application, Andres Andreu, Wrox Press.
2. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, "Web Application Security" Springer; 1st Edition
3. Joel Scambray, Vincent Liu, Caleb Sima ,"Hacking exposed", McGraw-Hill; 3rd Edition, (October, 2010).
4. OReilly Web Security Privacy and Commerce 2nd Edition 2011.
5. Software Security Theory Programming and Practice, Richard sinn, Cengage Learning.
6. Database Security and Auditing, Hassan, Cengage Learning.

ETHICAL HACKING LABORATORY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – I

Subject Code	**18SFCL16**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 02

Course objectives: This course will enable students to

- Evaluate modern tools
- Analyze packet capturing in network
- Define forensic analysis
- Security in various web applications

1. Wireshark: Experiment to monitor live network capturing packets and analyzing over the live network.
2. LOIC: DoS attack using LOIC.
3. FTK: Bit level forensic analysis of evidential image and reporting the same.
4. Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network. 4.
5. HTTrack: Website mirroring using Httrack and hosting on a local network.
6. XSS: Inject a client side script to a web application.
7. Emailtrackerpro: Email analysis involving header check, tracing the route. Also perform a check on a spam mail and non-spam mail.

Course Outcomes

The students should be able to:

- Evaluate modern tools
- Analyze packet capturing in network
- Define forensic analysis
- Security in various web applications

Conduction of Practical Examination:

All laboratory experiments (nos) are to be included for practical examination.
Students are allowed to pick one experiment from **each part and execute both**
Strictly follow the instructions as printed on the cover page of answer script for breakup of marks
Change of experiment is allowed only once and marks allotted to the procedure part to be made zero.

PRESERVING AND RECOVERING DIGITAL EVIDENCE
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	**18SFC21**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Different laws related to computer crime
- How to Secure Digital Evidences
- To Understand Investigation Process

Module 1	**Contact Hours**
Digital evidence and computer crime: history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room. **RBT:L1, L2**	**10**
Module 2	
Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems, forensic examination of Unix systems, forensic examination of Macintosh systems, and forensic examination of handheld devices. **RBT:L1, L2, L3**	**10**
Module 3	
Networks basics for digital investigators: applying forensic science to networks, digital evidence on physical and datalink layers, digital evidence on network and transport layers, digital evidence on the internet. **RBT:L1, L2, L3**	**10**
Module 4	
Investigating computer intrusions, investigating cyber stalking, digital evidence as alibi. **RBT:L1, L2, L3**	**10**
Module 5	
Handling the digital crime scene, digital evidence examination guidelines. **RBT:L1, L2, L3**	**10**

Course Outcomes

The students should be able to:

- Explain Digital evidence and computer crime and Laws
- Illustrate the Computer basics for digital investigators w.r.t Unix and Macintosh systems
- Illustrate the Networks basics for digital investigators
- Able to Investigating computer intrusions and cyber stalking
- Explain the basic concepts how to Handling the digital crime scene, digital evidence examination guidelines

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Digital Evidence and Computer Crime Forensic science, Computers and Internet -Eoghan Casey,

Elsevier Academic Press, Second Edition.

Reference Books:

1. A Electronic Discovery and Digital Evidence in a Nut Shell-Shira A scheindlin, Daniel J Capra, Th Sedona Conference, Academic Press, Third Edition (No where available).
2. Digital Forensic for Network, Internet, and Cloud Computing A forensic evidence guide for moving Targets and Data' – Terrence V.Lillard, Glint P.Garrison, Craig A..Schiller, James Steele, Syngress
3. The Best Damn Cybercrime and Digital Forensics Book Period' [Paperback] Jack Wiles , Anthony Reyes , Jesse Varsalone, Syngress Edition, 2007.

OPERATING SYSTEM SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	**18SFC22**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Define fundamental concepts and mechanisms for enforcing security in OS.
- Build a secure OS by exploring the early work in OS.
- Illustrate formal security goals and variety of security models proposed for development of secure operating systems.
- Explain architectures of various secure OS and retrofitting security feature on existing commercial OS's.
- Analyze variety of approaches applied to the development & extension services for securing operating systems.

Module 1	**Contact Hours**
Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system. **RBT:L1, L2, L3**	**10**
Module 2	
Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis. **RBT:L1, L2, L3**	**10**
Module 3	
Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels. **RBT:L1, L2, L3**	**10**
Module 4	
Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement. **RBT:L1, L2, L3**	**10**
Module 5	
Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration. **Case study:** Building secure OS for Linux: Linux security modules, security enhanced Linux. **RBT:L1, L2, L3**	**10**

Course Outcomes

The students should be able to:

- Gain the knowledge of fundamental concepts and mechanisms for enforcing security in OS.

- Analyze how to build a secure OS by exploring the early work in OS.
- Identify and compare different formal security goals and variety of security models proposed for development of secure operating systems.
- Interpret architectures of various secure OS and retrofitting security feature on existing commercial OS's.
- Shows variety of approaches applied to the development & extension services for securing operating systems.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008

Reference Books:

1. Michael Palmer, Guide to Operating system Security Thomson
2. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition
3. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont.

SECURED PROGRAMMING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	**18SFC23**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain the basics of secure programming.
- Demonstrate the most frequent programming errors leading to software vulnerabilities.
- Identify and analyze security problems in software
- Illustrate how to protect against security threats and software vulnerabilities

Module 1	**Contact Hours**
Validating all input & Designing secure programs: Command line and environment variables, File descriptors, names and contents, Web based application inputs, Locale selection and character encoding, Filtering represent able URIs, preventing cross site malicious input content, Forbidding HTTP Input to perform non-queries. Good security design principles: Securing the interface, separation of data and control. Minimize privileges: Granted, time, modules, resources etc, Using chroot, careful use of setuid/setgid, Safe default value and load initializations. Avoid race conditions, Trustworthy channels and trusted path, Avoiding semantics and algorithmic complexity attacks. **RBT:L1, L2, L3**	**10**
Module 2	
Declarations and Initializations and Expressions: Declare objects with appropriate storage durations, Identifier declaration with conflict linkage classifications, Using correct syntax for declaring flexible array member, Avoiding information leakage in structure padding, Incompatible declarations of same function or object. Dependence on evaluation order for side effects: Reading uninitialized memory and dereferencing null pointers, Modifying objects with temporary lifetime, Accessing variable through (pointer) incompatible type, Modifying constant objects and comparing padding data. **RBT:L1, L2, L3**	**10**
Module 3	
Integers and Floating Points: Wrapping of unsigned integers, Integer conversions and misrepresented data, Integer overflow and divide by zero errors, Shifting of negative numbers, Using correct integer precisions, Pointer conversion to integer and vice versa. Floating point values for counters: Domain and range errors in math functions, Floating point conversions and preserving precision. **RBT:L1, L2, L3**	**10**
Module 4	
Arrays , Strings and Memory Management: Out of bounds subscripts and valid length arrays, Comparing array pointers, Pointer arithmetic for non-array object, scaled integer, Modifying string literals, Space allocation for strings (Null terminator), Casting large integers as unsigned chars, Narrow and wide character strings and functions. Accessing freed memory: Freeing dynamically allocated memory, Computing memory allocation for an object, Copying structures containing flexible array members, Modifying object	**10**

alignment by using realloc. **RBT:L1, L2, L3**	
Module 5	
I/O, Signals and Error Handing: User input and format strings, Opening an pre-opened file, Performing device operations appropriate for files, Dealing with EOF, WEOF, Copying FILE object, Careful use of fgets, fgetws, getc, putc, putwc. Use of fsetops and fgetops, Accessing closed files. Using asynchronous safe functions and signal handlers: Shared objects and signal handlers, Using signal() within interruptible signal handlers, Returning computation exception signal handler. Using errno: check and set, Depending upon indeterminate values of errno, Handling standard library errors. **RBT:L1, L2, L3**	**10**
Course Outcomes	
The students should be able to: • How to respond to security alerts which identifies software issues • Identify possible security programming errors • Define methodology for security testing and use appropriate tools in its implementation • Apply new security-enhanced programming models and tools	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books 1. Robert C. Seacord, "The CERT ® C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems, Second Edition", Addison Wesley Professional, April 2014 2. David Wheeler, "Secure Programming for Linux and Unix HowTo", Linux Documentation project, Aug 2004	
Reference Books: 1. JohnViega, Matt Messier, "Secure Programming Cookbook for C and C++", O'Reilly Media, 1st Edition, July 2003.	

CYBER LAWS AND ETHICS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	**18SFC241**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain the Indian legal system, ITA 2000/2008, cyber security and related legal issues.
- Explain the Types of contract law, Digital signature and related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues
- Explain cyber crime investigation and prosecution in depth.

Module 1	**Contact Hours**
Introduction to Cyber Law and Cyber Ethics: Introduction to Cyber Crimes and Ethical Issues in IT**,** Basic concepts of Law and Information Security, overview of Information Security obligations under ITA 2008, Privacy and data protection concepts. **RBT:L1, L2, L3**	**10**
Module 2	
Law of Contracts applicable for Cyber Space transactions: introduction to Contract law, legal recognition of Electronic Documents, Authentication of Electronic Documents, Authentication of Electronic Documents, Cyber space contracts, Resolution of Contractual disputes, stamping of Contractual document. **RBT:L1, L2, L3**	**10**
Module 3	
Intellectual Property Law for Cyber Space: Concept of Virtual assests, nature of Intellectual property, Trademarks and domain names, copyright law, law of patents. **RBT:L1, L2, L3**	**10**
Module 4	
Intellectual Property Law for Cyber Space: Concept of Virtual assests, nature of Intellectual property, Trademarks and domain names, copyright law, law of patents. **RBT:L1, L2, L3**	**10**
Module 5	
Miscellaneous Issues in Cyber Crimes and Cyber Security: Cyber Crime Investigation and Prosecution, Digital evidence and Cyber forensics, Jurisdiction issues, Information Security Management in corporate Sector. **RBT:L1, L2, L3**	**10**

Course Outcomes

The students should be able to:

- Describe the Indian legal system, ITA 2000/2008, cyber security and related legal issues.
- Classify the Types of contract law, Digital signature , related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues, the types of cyber crimes and related legal issues.
- Interpret the cyber crime investigation and prosecution in depth.

Question paper pattern:
The question paper will have ten questions.

There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Cyber Laws for Engineers, Naavi, Ujvala Consultants Pvt Ltd, 2010.

Reference Books:

1. Deborah G Johnson, Computer Ethics, Pearson Education Pub., ISBN : 81-7758-593-2.
2. Earnest A. Kallman, J.P Grillo, Ethical Decision making and Information Technology: An Introduction with Cases, McGraw Hill Pub.
3. John W. Rittinghouse, William M. Hancock, Cyber security Operations Handbook, Elsevier Pub.
4. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 2nd Edition, Cengage Learning Pub.
5. Randy Weaver, Dawn Weaver, Network Infrastructure Security, Cengage Learning Pub

BIOMETRIC SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	**18SFC242**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain the principles used in biometrics algorithms and systems and most important biometric approaches.
- Illustrate the capability to select a suitable algorithm / system for a given application context (e.g. physical access control)
- Demonstrate a good understanding of the complex relationships between biometric systems and environmental conditions (e.g. illumination, pose variations etc.) and their impact on biometric performance.
- Illustrate of data privacy principles and the impact on the design and configuration of biometric systems.

Module 1	**Contact Hours**
Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy inbiometric systems. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Physiological Biometric Technologies: Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, weaknesses, deployment. Iris scan: Technical description, characteristics, strengths, weaknesses, deployment. Retina vascular pattern: Technical description, characteristics, strengths, weaknesses, deployment. Hand scan: Technical description, characteristics, strengths, weaknesses, deployment , DNA biometrics. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke Dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Case studies on Physiological, Behavioral and multifactor biometrics in identification systems. **RBT:L1, L2, L3**	**10 Hours**
Course Outcomes	

The students should be able to:

- Visualize traditional and biometric systems.
- Analyze different algorithms of biometric systems.
- Compare strengths and weaknesses of different biometric systems.
- Design different biometric system.
- Design multimodal biometric systems.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Biometrics –Identity verification in a networked World, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Eastern Publications, 2005.

Reference Books:

1. John Berger, Biometrics for Network Security, Prentice Hall, 2004.

INFORMATION SECURITY POLICIES IN INDUSTRY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	18SCN323 / **18SFC243**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

The objectives of this course is to make students to learn

- Explain management's responsibilities and role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines.
- Illustrate the differences between the organization's general information security policy and the needs and objectives of the various issue-specific and system-specific policies the organization will create.
- Know what an information security blueprint is and what its major components are.
- How an organization institutionalizes its policies, standards, and practices using education, training and awareness programs.
- Become familiar with what viable information security architecture is, what it includes, and how it is used.

Module 1	**Contact Hours**
Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goal Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in Organization, Business Objectives, Standards: International Standards. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Writing The Security Policies: Computer location and Facility construction, Contingency Planning, Periodic System and Network Configuration Audits, Authentication and Network Security, Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Telecommuting and Remote Access, Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Establishing Type of Viruses Protection: Rules for handling Third Party Software, User Involvement with Viruses, Legal Issues, Managing Encryption and Encrypted data, Key	**10 Hours**

Generation considerations and Management, Software Development policies, Processes Testing and Documentation, Revision control and Configuration management, Third Party Development, Intellectual Property Issues. **RBT:L1, L2, L3**	
Module 5	
Maintaining the Policies: Writing the AUP, User Login Responsibilities, Organization's responsibilities and Disclosures, Compliance and Enforcement, Testing and Effectiveness of Policies, Publishing and Notification Requirements of the Policies, Monitoring, Controls and Remedies, Administrator Responsibility, Login Considerations, Reporting of security Problems, Policy Review Process, The Review Committee, Sample Corporate Policies, Sample Security Policies. **RBT:L1, L2, L3**	**10 Hours**
Course Outcomes	
The students should be able to: • Explain the content, need, and responsibilities of information security policies. • Explain the standards, guidelines, Procedures, and key roles of the organization. • Able to write policy document for securing network connection and interfaces. • Explain the threats to the stored data or data in transit and able to write policy document. • Able to write, monitor, and review policy document.	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books 1. Scott Barman, Writing Information Security Policies, Sams Publishing, 2002. 2. Thomas.R.Peltier, Information Policies, Procedures and Standards, CRC Press, 2004.	
Reference Books: 1. Thomas R Peltier, Justin Peltier, John Backley, " Information Security Fundamentals", Auerbach publications, CRC Press, 2005. 2. Harold F. Tipton and Micki Krause "Information Security Management Handbook", Auerbach publications, 5th Edition, 2005.	

TRUST MANAGEMENT IN E-COMMERCE
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	**18SFC244** / 18SSE253	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain fundamental principles of E-Commerce
- Illustrate technologies & tools for E-Commerce with emphasis on Security
- Identify best techniques & practices for different types of legacy & partner requirements
- Handle & address risk management

Module 1	**Contact Hours**
Introduction to E-Commerce: Network and E-Commerce, Types of E-Commerce. Ecommerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models. Ecommerce Payment systems: Types of payment system, Credit card E-Commerce transactions, B2C E-Commerce Digital payment systems, B2B payment system. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Security and Encryption: E-Commerce Security Environment, Security threats in Ecommerce environment, Policies, Procedures and Laws. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Inter-organizational trust in E-Commerce: Need, Trading partner trust, Perceived benefits and risks of E-Commerce, Technology trust mechanism in E-Commerce, Perspectives of organizational, economic and political theories of inter-organizational trust, Conceptual model of inter-organizational trust in E-Commerce participation. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Introduction to trusted computing platform: Overview, Usage Scenarios, Key components of trusted platform, Trust mechanisms in a trusted platform. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Trusted platforms for organizations and individuals: Trust models and the E-Commerce domain. **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

The students should be able to:

- Explain the types of E-Commerce, E-Commerce business models and E-commerce payment systems.
- Illustrate the Policies, Procedures and Laws and Security threats in E-Commerce environment.
- Analysis and explain the issues, risks and challenges in inter-organisational trust in E-Commerce
- Explain the Key components and Trust mechanisms of trusted computing platform.

- Describe the Trusted platforms for organizations and individuals

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Kenneth C. Laudon and Carol Guercio Trave, Study Guide to E-Commerce Business Technology Society, Pearson Education, 2005.
2. Pauline Ratnasingam, Inter-Organizational Trust for Business-to-Business E- Commerce,IRM Press, 2005.

Reference Books:

1. Siani Pearson, et al, Trusted Computing Platforms: TCPA Technology in Context, Prentice Hall PTR, 2002.

DATA MINING & DATA WAREHOUSING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	18SCE154 / 18SCS244 / **18SFC251** / 18SIT23 / 18SSE241	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Define Data warehousing Architecture and Implementation
- Explain Data mining principles and techniques and Introduce DM as a cutting edge business intelligence
- Interpret association rule mining for handling large data
- Classification for the retrieval purposes
- Explain clustering techniques in details for better organization and retrieval of data

Module -1	**Contact Hours**
Introduction and Data Preprocessing :Why data mining, What is data mining, What kinds of data can be mined, What kinds of patterns can be mined, Which Technologies Are used, Which kinds of Applications are targeted, Major issues in data mining .Data Preprocessing: An overview, Data cleaning, Data integration, Data reduction, Data transformation and data discretization. **RBT:L1, L2, L3**	**10 Hours**
Module -2	
Data warehousing and online analytical processing: Data warehousing: Basic concepts, Data warehouse modeling: Data cube and OLAP, Data warehouse design and usage, Data warehouse implementation, Data generalization by attribute-oriented induction, **RBT:L1, L2, L3**	**10 Hours**
Module – 3	
Classification: Basic Concepts: Basic Concepts, Decision tree induction, Bays Classification Methods, Rule-Based classification, Model evaluation and selection, Techniques to improve classification accuracy **RBT:L1, L2, L3**	**10 Hours**
Module-4	
Cluster Analysis: Basic concepts and methods: Cluster Analysis, Partitioning methods, Hierarchical Methods, Density-based methods, Grid-Based Methods, Evaluation of clustering. **RBT:L1, L2, L3**	**10 Hours**
Module-5	
Data mining trends and research frontiers: Mining complex data types, other methodologies of data mining, Data mining applications, Data Mining and society. **RBT:L1, L2, L3**	**10 Hours**

Course outcomes:

The students shall able to:

- Demonstrate Storing voluminous data for online processing, Preprocess the data for mining applications
- Apply the association rules for mining the data

- Design and deploy appropriate classification techniques
- Cluster the high dimensional data for better organization of the data
- Discover the knowledge imbibed in the high dimensional system

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module.
The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Jiawei Han, Micheline Kamber, Jian Pei: Data Mining Concepts and Techniques, ELSEVIER(MK) 3rd edition 2012.

Reference Books: NIL

DATABASE SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	18SCE332 / **18SFC252**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Fundamental security concepts and architectures that serve as building blocks to database security
- Concepts of user account management and administration, including security risks
- To use current database management system to design and configure the user and data permissions
- Operational components necessary to maximize database security using various security models

Module 1	**Contact Hours**
Introduction: Introduction to Databases, Security Problems in Databases Security Controls Conclusions. Security Models 1: Introduction, Access Matrix Model, Take-Grant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases. **RBT:L1, L2**	**10 Hours**
Module 2	
Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion. Security Mechanisms: Introduction, User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation, Security Functionalities in Some Operating Systems, Trusted Computer System, Evaluation Criteria. **RBT:L1, L2**	**10 Hours**
Module 3	
Security Software Design: Introduction, A Methodological Approach to Security, Software Design, Secure Operating System Design, Secure DBMS Design, Security Packages, Database Security Design. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Statistical Database Protection & Intrusion Detection Systems: Introduction, Statistics, Concepts and Definitions, Types of Attacks, Inference Controls, evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System Discovery. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Models For The Protection Of New Generation Database Systems 1: Introduction, A Model for the Protection of Frame Based Systems, A Model for the Protection of Object-Oriented Systems, SORION Model for the Protection of Object-Oriented Databases. Models For The Protection Of New Generation Database Systems 2: A Model for the Protection of New Generation Database Systems, the Orion Model, Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions.	**10 Hours**

RBT:L1, L2, L3	
Course Outcomes	
The students should be able to: • Carry out a risk analysis for a large database • Implement identification and authentication procedures, fine-grained access control and data encryption techniques • Set up accounts with privileges and roles • Audit accounts and the database system	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books 1. Database Security and Auditing, Hassan A. Afyoun i, India Edition, CENGAGE Learning, 2009. 2. Database Security, Castano, Second edition, Pearson Education.	
Reference Books: 1. Database security by Alfred Basta, Melissa Zgola , CENGAGE learning..	

ENTERPRISE APPLICATION PROGRAMMING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	**18SFC253** / 18SIT12 / 18SSE22	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain Web Application Development and related terminologies
- Demonstrate persistent framework and other ORM tools.
- Illustrate solutions using Design Patterns
- Outline latest WEB frameworks

Module 1	**Contact Hours**
Web application and java EE 6: Exploring the HTTP Protocol, Introducing web applications, describing web containers, exploring web architecture models, exploring the MVC architecture. **Working with servlets 3.0** Exploring the features of java servlet, Exploring new features in servlet 3.0, Exploring the servlet API, explaining the servlet life cycle, creating a sample servlet, creating a servlet by using annotation, working with servlet config and servlet context objects, working with the HTTP servlet request and HTTP servlet response interfaces, Exploring request delegation and request scope, implementing servlet collaboration. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Handling sessions in servlet 3.0: Describing a session, introducing session tracking, Exploring the session tracking, mechanisms, using the java servlet API for session tracking, creating login application using session tracking. **Implementing event handling** Introducing events, Introducing event handling, working with the servlet events, developing the online shop web application. **Working with java server pages:** Introducing JSP technology, Exploring new features of JSP2.1, listing advantages of JSP over java servlet, Exploring the architecture of a JSP page, Describing the life cycle of a JSP page, working with JSP basic tags and implicit objects, working with the action tags in JSP, exploring the JSP unified EL, using functions with EL. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Implementing JSP tag extensions: Exploring the elements of tag extensions, Working with classic tag handlers, Exploring the tag extensions, Working with simple tag handlers. **Implementing java server pages standard tag library 1.2:** Introducing JSTL, Exploring the tag libraries JSTL, working with the core tag library. **Implementing filters:** Exploring the need of filters, exploring the working of filters, exploring filters API, configuring a filter, creating a web application using filters, using initializing parameter in filters. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Persistence Management and Design Patterns: Implementing java persistence using hibernate Introducing hibernate, exploring the architecture of hibernate, downloading hibernate, exploring HQL, understanding hibernate O/R mapping, working with hibernate, Implementing O/R mapping with hibernate. **Java EE design patterns:** Describing the java EE application architecture, Introducing a design patterns, discussing the role of design	**10 Hours**

patterns, exploring types of patterns. **RBT:L1, L2, L3**	
Module 5	
Web Frameworks: Working with struts 2 Introducing struts 2, understanding actions in struts 2.**Working with java server faces 2.0:** Introducing JSF, Explaining the features of JSF, Exploring the JSF architecture, describing JSF elements, Exploring the JSF request processing life cycle. **Working with spring 3.0:** Introducing features of the spring framework, exploring the spring framework architecture, exploring dependency injection & inversion of control, exploring AOP with spring, managing transactions. **Securing java EE 6 applications:** Introducing security in java EE 6, exploring security mechanisms, implementing security on an application server. **RBT:L1, L2, L3**	**10 Hours**
Course Outcomes	
The students should be able to: • Explain WEB basics and their functionalities • Develop JAVA support and API skills • Build a WEB application. • Build Security mechanisms	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books: 1. Kogent learning solution: JAVA SERVER PROGRAMMING JAVA EE6(J2EE 1.6), Dreamtech press 2014	
Reference Books: 1. **NIL**	

MACHINE LEARNING TECHNIQUES
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – II

Subject Code	18LNI322 / 18SCE321 / 18SCN324 / 18SCS31 / **18SFC254** / 18SIT322 / 18SSE334	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain basic concepts of learning and decision trees.
- Compare and contrast neural networks and genetic algorithms
- Apply the Bayesian techniques and instant based learning
- Examine analytical learning and reinforced learning

Module -1	**Contact Hours**
INTRODUCTION, CONCEPT LEARNING AND DECISION TREES Learning Problems – Designing Learning systems, Perspectives and Issues – Concept Learning – Version Spaces and Candidate Elimination Algorithm – Inductive bias – Decision Tree learning – Representation – Algorithm – Heuristic Space Search **RBT:L1, L2, L3**	**10Hours**
Module -2	
NEURAL NETWORKS AND GENETIC ALGORITHMS: Neural Network Representation – Problems – Perceptrons – Multilayer Networks and Back Propagation Algorithms – Advanced Topics – Genetic Algorithms – Hypothesis Space Search – Genetic Programming – Models of Evolution and Learning. **RBT:L1, L2, L3**	**10 Hours**
Module – 3	
BAYESIAN AND COMPUTATIONAL LEARNINGL Bayes Theorem – Concept Learning – Maximum Likelihood – Minimum Description Length Principle – Bayes Optimal Classifier – Gibbs Algorithm – Naïve Bayes Classifier– Bayesian Belief Network – EM Algorithm – Probably Learning – Sample Complexity for Finite and Infinite Hypothesis Spaces – Mistake Bound Model. **RBT:L1, L2, L3**	**10 Hours**
Module-4	
INSTANT BASED LEARNING AND LEARNING SET OF RULES: K- Nearest Neighbor Learning – Locally Weighted Regression – Radial Basis Functions –Case-Based Reasoning – Sequential Covering Algorithms – Learning Rule Sets – Learning First Order Rules – Learning Sets of First Order Rules – Induction as Inverted Deduction – Inverting Resolution **RBT:L1, L2, L3**	**10 Hours**
Module-5	
ANALYTICAL LEARNING AND REINFORCED LEARNING: Perfect Domain Theories – Explanation Based Learning – Inductive-Analytical Approaches - FOCL Algorithm – Reinforcement Learning – Task – Q-Learning – Temporal Difference Learning **RBT:L1, L2, L3**	**10 Hours**
Course outcomes:	
On Completion of the course, the students will be able to	

- Choose the learning techniques with this basic knowledge.
- Apply effectively neural networks and genetic algorithms for appropriate applications.
- Apply bayesian techniques and derive effectively learning rules.
- Choose and differentiate reinforcement and analytical learning techniques

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module.
The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Tom M. Mitchell, "Machine Learning", McGraw-Hill Education (INDIAN EDITION), 2013.

Reference Books:

1. Ethem Alpaydin, "Introduction to Machine Learning", 2nd Ed., PHI Learning Pvt. Ltd., 2013.
2. T. Hastie, R. Tibshirani, J. H. Friedman, "The Elements of Statistical Learning", Springer; 1st edition, 2001.

FILE SYSTEM FORENSIC ANALYSIS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	**18SFC31**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Computer file system and storage analysis
- Basics of Computer forensics
- Role of forensics in business world

Module 1	**Contact Hours**
Volume Analysis: Introduction, Background, Analysis Basics, Summary. PC-based Partitions: DOS Partitions, Analysis Considerations, Apple Partitions, Removable Media. Server-based Partitions: BSD Partitions, Sun Solaris Slices, GPT Partitions, Multiple Disk Volumes: RAID, Disk Spanning. **RBT:L1, L2, L3**	**10**
Module 2	
File System Analysis: What Is a File System?, File System Category, Content Category, Metadata Category, File Name Category, Application Category, Application-level Search Techniques, Specific File Systems FAT Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture, Other Topics. FAT Data Structures: Boot Sector, FAT32 FSINFO, FAT, Directory Entries, Long File Name Directory Entries **RBT:L1, L2, L3**	**10**
Module 3	
NTFS Concepts: Introduction, Everything is a File, MFT Concepts, MFT Entry Attribute Concepts, Other Attribute Concepts, Indexes, Analysis Tools. NTFS Analysis: File System Category, Content Category, Metadata Category, File Name Category, Application Category, The Big Picture. NTFS Data Structures: Basic Concepts, Standard File Attributes, Index Attributes and Data Structures, File System Metadata Files. **RBT:L1, L2, L3**	**10**
Module 4	
Ext2 and Ext3 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, Application Category. The Big Picture. Ext2 and Ext3 Data Structures: Superblock, Group Descriptor Tables, Block Bitmap, Inodes, Extended Attributes, Directory Entry, Symbolic Link, Hash Trees, Journal Data Structures **RBT:L1, L2, L3**	**10**
Module 5	
UFS1 and UFS2 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture. UFS1 and UFS2 Data Structures: UFS1 Superblock, UFS2 Superblock, Cylinder Group Summary, UFS1 Group Descriptor, UFS2 Group Descriptor, Block and Fragment Bitmaps, UFS1 Inodes, UFS2 Inodes, UFS2 Extended Attributes, Directory Entries **RBT:L1, L2, L3**	**10**

Course Outcomes

The students should be able to:

- Compare the different file systems for storing information
- Illustrate the role of computer forensics in the business and private world
- Identify some of the current techniques and tools for forensic examinations

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Brian Carrier, File System Forensic Analysis, Pearson Education, 2005

Reference Books:

1. Machtelt Garrels, "Introduction to Linux A Hands-On Guide", Third Edition, Fultus Corporation Publisher, 2010.

Laboratory Experiments

1. Design a simple experiment to test whether a bootable CD/DVD examination altered the hard disk of the suspect's computer system when the system was booted using the bootable CD/DVD.
2. Design a simple experiments that shows that the correct application of a virtual environment approa results in a less time spent on analysing the evidence, giving more chance of discovering important data, and allowing less qualified personnel to be involved in a more productive way.
3. Write a program to find a unique pattern in each sector of disk.
4. Write a program to compare two partitions.
5. Write a program to compare two disks.
6. Write a program to change or corrupt one byte in a file.

The above experiments can be simulated using freely available forensic tool.

SECURITY ARCHITECTURE DESIGN
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	**18SFC321**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Describe the intent of effective site security
- List different security zones
- Select appropriate elements to apply to specific security zones

Module 1	**Contact Hours**
Architecture and Security: Architecture Reviews, Software Process, Reviews and the Software Development Cycle, Software Process and Architecture Models, Software Process and Security, Architecture Review of System, Security Assessments, Security Architecture Basics, Architecture Patterns in Security **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Low-Level Architecture: Code Review, importance of code review, Buffer Overflow Exploits, Countermeasures Against Buffer Overflow Attacks, patterns applicable, Security and Perl, Bytecode Verification in Java-Good Coding Practices Lead to Secure Code, Cryptography, Trusted Code, Secure Communications. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Mid-Level Architecture: Middleware Security, Middleware and Security, The Assumption of Infallibility, The Common Object Request Broker Architecture, The OMG CORBA Security Standard, Vendor Implementations of CORBA Security, CORBA Security Levels, Secure Interoperability, Application, Unaware Security, Application, Aware Security, Application Implications, Web Security, Application and OS Security, Database Security. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
High-Level Architecture: Security Components, Secure Single Sign-On- Public-Key Infrastructures, Firewalls, Intrusion Detection Systems, LDAP and X.500 Directories, Kerberos, Distributed Computing Environment,The Secure Shell, or SSH, The Distributed Sandbox, Security and Other Architectural Goals, Metrics for Non-Functional Goals, Force Diagrams around Security, High Availability, Robustness, Reconstruction of Events, Ease of Use, Maintainability, Adaptability, and Evolution, Scalability, Interoperability, Performance, Portability. **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Enterprise Security Architecture: Security as a Process, Security Data, Enterprise Security as a Data Management Problem, Tools for Data Management, David Isenberg and the "Stupid Network", Extensible Markup Language,The XML Security Services Signaling Layer, XML and Security Standards, The Security Pattern Catalog Revisited, XML-Enabled Security Data-HGP: A Case Study in Data Management, Business Cases and Security,	**10 Hours**

Building Business Cases for Security **Case study:** Building secure OS for Linux: Linux security modules, security enhanced Linux. **RBT:L1, L2, L3**	

Course Outcomes

The students should be able to:

- Design the secured sites based on tools & techniques
- Map site zones with level of security
- Identify the components targeted for each zone

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Jay Ramachandran, Designing Security Architecture Solutions, Wiley Computer Publishing, 2010.

Reference Books:

1. Markus Schumacher, Security Patterns: Integrating Security and Systems Engineering, Wiley Software Pattern Series, 2010.

STEGANOGRAPHY AND DIGITAL WATERMARKING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	**18SFC322**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Basics of Data hiding by using Steganography & Watermarking
- Compare and contrast several different methods of steganography
- Apply digital watermarking as an authentication tool for distribution of content over the Internet

Module 1	**Contact Hours**
Introduction to Information hiding: Brief history and applications of information hiding, Principles of Steganography, Frameworks for secret communication, Security of Steganography systems, Information hiding in noisy data, Adaptive versus non adaptive algorithms, Laplace filtering, Using cover models, Active and malicious attackers, Information hiding in written text, Examples of invisible communications. **RBT:L1, L2**	**10 Hours**
Module 2	
Survey of steganographic techniques: Substitution system and bit plane tools, Transform domain techniques, Spread spectrum and information hiding, Statistical Steganography, Distortion and code generation techniques, Automated generation of English text. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Steganalysis: Detecting hidden information, Extracting hidden information, Disabling hidden information, Watermarking techniques, History, Basic Principles, applications, Requirements of algorithmic design issues, Evaluation and benchmarking of watermarking system. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Survey of current watermarking techniques: Cryptographic and psycho visual aspects, Choice of a workspace, binary image, audio, video. Formatting the watermark beds: Digital watermarking schemes, Spread Spectrum, DCT (Discrete Cosine Transform), Domain and Quantization schemes, Watermarking with side information, Robustness to temporal and geometric distortions. **RBT:L1, L2,L3**	**10 Hours**
Module 5	
Data Right Management: DRM Products and Laws, Fingerprints, Examples, Protocols and Codes, Boneh-Shaw finger printing Scheme, Steganography and watermarking applications, Military, Digital copyright protection and protection of intellectual property. **RBT:L1, L2, L3**	**10 Hours**
Course Outcomes	
The students should be able to:	

- Distinguish Stegnography & Digital watermarking from other related fields.
- Knowledge of how to use steganography techniques in conjunction with encryption systems to protect data.
- Explain different types of watermarking applications and watermarking frameworks.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, Information hiding techniques for Steganography and Digital Watermarking, ARTECH House Publishers, January 2004.
2. I.J. Cox, M.L. Miller, J.Fridrich and T.Kalker, Digital Water Marking and Steganography, 2nd Edition, Morgan Kauffman Publishers, 2008.
3. Johnson, Neil F. / Duric, Zoran / Jajodia, Sushil G , Information Hiding: Steganography and Watermarking -Attacks and Countermeasures (Advances in Information Security, Volume 1), 2001.

Reference Books:

1. Peter Wayner , "Disappearing Cryptography: Information Hiding, Steganography and Watermarking 2/e", Elsevier.
2. Practical Cryptography, N.Ferguson and B.Schneier, Wiley Publishing Inc., 2003.
3. Bolle, Connell et. al., "Guide to Biometrics", Springer
4. John Vecca, "Computer Forensics: Crime scene Investigation", Firewall Media
5. Christopher L.T. Brown, "Computer Evidence: Collection and Preservation", Firewall Media

MOBILE DEVICE FORENSICS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	**18SFC323**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Basic Concepts in Mobile Forensics
- Mobile Device Data Storage
- Identify, preserve, extract, analyze, and report data from mobile devices
- Acquiring Evidence from Mobile devices

Module 1	**Contact Hours**
Android and mobile forensics: Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Android hardware platforms: Overview of core components, Overview of different device types, Read-only memory and boot loaders, Manufacturers, Specific devices **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Android software development kit and android debug bridge: Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Android file systems and data structures: Data in the shell, Type of memory, File systems, Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques **RBT:L1, L2, L3**	**10 Hours**
Module 5	
Android device data and app security: Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies. Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

The students should be able to:

- Describe security risks and vulnerabilities from mobile devices and network access.
- Explain the methods and procedures used in forensics investigations.
- Have knowledge of the global security threats and vulnerabilities of mobile devices and networks.
- Carry out a forensics investigation of mobile and network devices.

Question paper pattern:
The question paper will have ten questions.

There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Android Forensics Investigation, Analysis, and Mobile security for Google Android, Andrew Hoog, John McCash, Technical Editor, Elsevier, 2011.

Reference Books:

1. Satish Bommisetty, Rohit Tamma, Heather Mahalik "Practical Mobile Forensics", Kindle Edition, Packt Publishing (21 July 2014).
2. Andrew Martin," Mobile Device Forensics", © SANS Institute 2009

SECURITY ASSESSMENT AND VERIFICATION
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	**18SFC324**	**IA Marks**	40
Number of Contact Hours/Week	04	**Exam Marks**	60
Total Number of Contact Hours	50	**Exam Hours**	03

CREDITS – 04

Course objectives: This course will enable students to

- Explain the role of assessment & verification for information security
- Demonstration of different existing tools and procedures for assessment planning
- Recall awareness of risk management

Module 1	**Contact Hours**
Evolution of information security: information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Security assessment planning: Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan. Initial information gathering, Initial preparation, analysis of gathered information. **RBT:L1, L2, L3**	**10 Hours**
Module 3	
Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation. **RBT:L1, L2**	**10 Hours**
Module 4	
Security Risk assessment project management, Security risk assessment approaches and methods. **RBT:L1, L2**	**10 Hours**
Module 5	
Information security standards, Information security Legislation, Formal security verification, Security verification with SSL. **RBT:L1, L2**	**10 Hours**

Course Outcomes

The students should be able to:

- Illustrate the roles information security and its management
- Select appropriate techniques to tackle and solve problems in the discipline of information security assessment
- Design an information security and validation system

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Sudhanshu Kairab, A practical guide to security assessments, CRC press, 2005.
2. Douglas J. Landoll, A Security risk assessment Handbook, Auerbach publications, 2006.

Reference Books:

1. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 2nd Edition, Cengage Learning Pub.
2. Thomas R Peltier, Justin Peltier and John Blackley, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996

MANAGING BIG DATA
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	18LNI251 / 18SCE21 / 18SCN252 / 18SCS21 / **18SFC331** / 18SIT31 / 18SSE322	IA Marks	40
Number of Lecture Hours/Week	03	Exam Marks	60
Total Number of Lecture Hours	40	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Deal with Big data using Hadoop and SPARK technologies
- Explain basic concepts of Map and Reduce
- Explain basic concepts of Hadoop Distributed File System
- Develop map-reduce analytics using Hadoop and related tools

Module -1	**Teaching Hours**
Meet Hadoop: Data!, Data Storage and Analysis, Querying All Your Data, Beyond Batch, Comparison with Other Systems: Relational Database Management Systems, Grid Computing, Volunteer Computing Hadoop Fundamentals MapReduce A Weather Dataset: Data Format, Analyzing the Data with Unix Tools, Analyzing the Data with Hadoop: Map and Reduce, Java MapReduce, Scaling Out: Data Flow, Combiner Functions, Running a Distributed MapReduce Job, Hadoop Streaming **The Hadoop Distributed Filesystem** The Design of HDFS, HDFS Concepts: Blocks, Namenodes and Datanodes, HDFS Federation, HDFS High-Availability, The Command-Line Interface, Basic Filesystem Operations, Hadoop Filesystems Interfaces, The Java Interface, Reading Data from a Hadoop URL, Reading Data Using the FileSystem API, Writing Data, Directories, Querying the Filesystem, Deleting Data, Data Flow: Anatomy of a File Read, Anatomy of a File Write. **RBT:L1, L2, L3**	**10 Hours**
Module -2	
YARN Anatomy of a YARN Application Run: Resource Requests, Application Lifespan, Building YARN Applications, YARN Compared to MapReduce, Scheduling in YARN: The FIFO Scheduler, The Capacity Scheduler, The Fair Scheduler, Delay Scheduling, Dominant Resource Fairness **Hadoop I/O** Data Integrity, Data Integrity in HDFS, LocalFileSystem, ChecksumFileSystem, Compression, Codecs, Compression and Input Splits, Using Compression in MapReduce, Serialization, The Writable Interface, Writable Classes, Implementing a Custom Writable, Serialization Frameworks, File-Based Data Structures: SequenceFile **RBT:L1, L2, L3**	**10 Hours**
Module – 3	
Developing a MapReduce Application The Configuration API, Combining Resources,	**10 Hours**

Variable Expansion, Setting Up the Development Environment, Managing Configuration, GenericOptionsParser, Tool, and ToolRunner, Writing a Unit Test with MRUnit: Mapper, Reducer, Running Locally on Test Data, Running a Job in a Local Job Runner, Testing the Driver, Running on a Cluster, Packaging a Job, Launching a Job, The MapReduce Web UI, Retrieving the Results, Debugging a Job, Hadoop Logs, Tuning a Job, Profiling Tasks, MapReduce Workflows: Decomposing a Problem into MapReduce Jobs, JobControl, Apache Oozie **How MapReduce Works** Anatomy of a MapReduce Job Run, Job Submission, Job Initialization, Task Assignment, Task Execution, Progress and Status Updates, Job Completion, Failures: Task Failure, Application Master Failure, Node Manager Failure, Resource Manager Failure, Shuffle and Sort: The Map Side, The Reduce Side, Configuration Tuning, Task Execution: The Task Execution Environment, Speculative Execution, Output Committers **RBT:L1, L2, L3**	
Module-4	
MapReduce Types and Formats: MapReduce Types, Input Formats: Input Splits and Record,s Text Input, Binary Input, Multiple Inputs, Database Input (and Output) Output Formats: Text Output, Binary Output, Multiple Outputs, Lazy Output, Database Output, **Flume** Installing Flume, An Example,Transactions and Reliability, Batching, The HDFS Sink, Partitioning and Interceptors, File Formats, Fan Out, Delivery Guarantees, Replicating and Multiplexing Selectors, Distribution: Agent Tiers, Delivery Guarantees, Sink Groups, Integrating Flume with Applications, Component Catalog **RBT:L1, L2, L3**	**10 Hours**
Module-5	
Pig Installing and Running Pig, Execution Types, Running Pig Programs, Grunt, Pig Latin Editors, An Example: Generating Examples, Comparison with Databases, Pig Latin: Structure, Statements, Expressions, Types, Schemas, Functions, Data Processing Operators: Loading and Storing Data, Filtering Data, Grouping and Joining Data, Sorting Data, Combining and Splitting Data. **Spark** An Example: Spark Applications, Jobs, Stages and Tasks, A Java Example, A Python Example, Resilient Distributed Datasets: Creation, Transformations and Actions, Persistence, Serialization, Shared Variables, Broadcast Variables, Accumulators, Anatomy of a Spark Job Run, Job Submission, DAG Construction, Task Scheduling, Task Execution, Executors and Cluster Managers: Spark on YARN **RBT:L1, L2, L3**	**10 Hours**
Course outcomes:	
The students shall able to: • Understand managing big data using Hadoop and SPARK technologies • Explain HDFS and MapReduce concepts • Install, configure, and run Hadoop and HDFS. • Perform map-reduce analytics using Hadoop and related tools • Explain SPARK concepts	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books: 1. Tom White, "Hadoop: The Definitive Guide", Third Edition, O'Reilley, 2012.	
Reference Books:	

1. Matei Zaharia and Bill Chambers, SPARK: The Definitive Guide, Oreilly, 2018
2. S. D'Souza and Steve Hoffman, Apache Flume: Distributed Log Collection for Hadoop, Oreilly. 2014

MOBILE APPLICATION DEVELOPMENT
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	18LNI323/ 18SCN244 **18SFC332** / 18SIT241	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Analyze system requirements for mobile applications.
- Apply of mobile development frameworks.
- Demonstrate mobile application design.
- Demonstrate and implement mobile application.

Module -1	**Contact Hours**
Introduction to mobile communication and computing: Introduction to mobile computing, Novel applications, limitations and GSM architecture, Mobile services, System architecture, Radio interface, protocols, Handover and security. Smart phone operating systems and smart phones applications. **RBT:L1, L2**	**10 Hours**
Module -2	
Fundamentals of Android Development: Introduction to Android., The Android 4.1 Jelly Bean SDK, Understanding the Android Software Stack, Installing the Android SDK, Creating Android Virtual Devices, Creating the First Android Project, Using the Text View Control, Using the Android Emulator. **RBT:L1, L2, L3**	**10 Hours**
Module – 3	
The Intent of Android Development, Four kinds of Android Components: Activity, Service, Broadcast Receiver and Content Provider. Building Blocks for Android Application Design, Laying Out Controls in Containers. Graphics and Animation: Drawing graphics in Android, Creating Animation with Android's Graphics API. **RBT:L1, L2, L3**	**10 Hours**
Module-4	
Creating the Activity, Working with views: Exploring common views, using a list view, creating custom views, understanding layout. Using Selection Widgets and Debugging Displaying and Fetching Information Using Dialogs and Fragments. Multimedia: Playing Audio, Playing Video and Capturing Media. Advanced Android Programming: Internet, Entertainment, and Services. **RBT:L1, L2, L3**	**10 Hours**
Module-5	
Displaying web pages and maps, communicating with SMS and emails. Creating and using content providers: Creating and consuming services, publishing android applications **RBT:L1, L2, L3**	**10 Hours**

Course outcomes:

The students should be able to:

- Describe the requirements for mobile applications
- Explain the challenges in mobile application design and development
- Develop design for mobile applications for specific requirements

- Implement the design using Android SDK
- Implement the design using Objective C and iOS
- Deploy mobile applications in Android and iPone marketplace for distribution

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module.
The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Mobile Computing: (technologies and Applications-N. N. Jani S chand
2. B.M.Hirwani- Android programming Pearson publications-2013
3. W. Frank Ableson, Robi Sen and C. E. Ortiz - **Android in Action**, Third Edition-2012 DreamTech Publisher

SOCIAL NETWORK ANALYSIS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	18LNI332 / 18SCN153 / **18SFC333**	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- The learning objective of the course Social Network Analysis is to discuss essential knowledge of network analysis applicable to real world data, with examples from today's most popular social networks.

Module 1	**Contact Hours**
Introduction to social network analysis and Descriptive network analysis: Introduction to new science of networks. Networks examples. Graph theory basics. Statistical network properties. Degree distribution, clustering coefficient. Frequent patterns. Network motifs. Cliques and k-cores. **RBT:L1, L2, L3**	**10 Hours**
Module 2	
Network structure, Node centralities and ranking on network: Nodes and edges, network diameter and average path length. Node centrality metrics: degree, closeness and betweenness centrality. Eigenvector centrality and PageRank. Algorithm HITS. **RBT:L1, L2**	**10 Hours**
Module 3	
Network communities and Affiliation networks: Networks communities. Graph partitioning and cut metrics. Edge betweenness. Modularity clustering. Affiliation network and bipartite graphs. 1-mode projections. Recommendation systems. **RBT:L1, L2, L3**	**10 Hours**
Module 4	
Information and influence propagation on networks and Network visualization: Social Diffusion. Basic cascade model. Influence maximization. Most influential nodes in network. Network visualization and graph layouts. Graph sampling. Low -dimensional projections **RBT:L1, L2**	**10 Hours**
Module 5	
Social media mining and SNA in real world: FB/VK and Twitter analysis: Natural language processing and sentiment mining. Properties of large social networks: friends, connections, likes, re-tweets. **RBT:L1, L2, L3**	**10 Hours**

Course Outcomes

The students should be able to:

- Define notation and terminology used in network science.
- Demonstrate, summarize and compare networks.
- Explain basic principles behind network analysis algorithms.
- Analyzing real world network.

Question paper pattern:
The question paper will have ten questions.

There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. David Easley and John Kleinberg. "Networks, Crowds, and Markets: Reasoning About a Highly Connected World." Cambridge University Press 2010.
2. Eric Kolaczyk, Gabor Csardi. “Statistical Analysis of Network Data with R (Use R!)”. Springer, 2014.
3. Stanley Wasserman and Katherine Faust. "Social Network Analysis. Methods and Applications." Cambridge University Press, 1994.

Reference Books:

1. **NIL**

SOFTWARE METRICS AND QUALITY ASSURANCE
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2018 -2019)
SEMESTER – III

Subject Code	**18SFC334** / 18SIT243 / 18SSE242	IA Marks	40
Number of Contact Hours/Week	04	Exam Marks	60
Total Number of Contact Hours	50	Exam Hours	03

CREDITS - 04

Course objectives: This course will enable students to

- Define metrics, measurement theory and related Terminologies
- Assess the quality level of internal and external attributes of the software product
- Explain of software reliability and to illustrate how to perform planning, executing and testing for software reliability
- Evaluate various metrics and models of software reliability
- Compare various models of software reliability based on its application

Module -1	**Contact Hours**
What Is Software Quality: Quality: Popular Views, Quality Professional Views, Software Quality, Total Quality Management and Summary. **Fundamentals Of Measurement Theory:** Definition, Operational Definition, And Measurement, Level Of Measurement, Some Basic Measures, Reliability And Validity, Measurement Errors, Be Careful With Correlation, Criteria For Causality, Summary. **Software Quality Metrics Overview:** Product Quality Metrics, In Process Quality Metrics, Metrics for Software Maintenance, Examples For Metrics Programs, Collecting Software Engineering Data. **RBT:L1, L2, L3**	**10Hours**
Module -2	
Applying The Seven Basic Quality Tools In Software Development : Ishikawa's Seven Basic Tools, Checklist, Pareo Diagram, Histogram, Run Charts , Scatter Diagram, Control Chart, Cause And Effect Diagram. **The Rayleigh Model:** Reliability Models, The Rayleigh Model Basic Assumptions, Implementation, Reliability And Predictive Validity. **RBT:L1, L2, L3**	**10 Hours**
Module – 3	
Complexity Metrics And Models: Lines Of Code, Halstead's Software Science , Cyclomatic Complexity Syntactic Metrics, An Example Of Module Design Metrics In Practice .**Metric And Lessons Learned For Object Oriented Projects:** Object Oriented Concepts And Constructs, Design And Complexity Metrics, Productivity Metrics, Quality And Quality Management Metrics, Lessons Learned For object oriented Projects. **RBT:L1, L2, L3**	**10 Hours**
Module-4	
Availability Metrics: Definition And Measurement Of System Availability, Reliability Availability And Defect Rate, Collecting Customer Outage Data For Quality Improvement, In Process Metrics For Outage And Availability .**Conducting Software Project Assessment :**Audit Ad Assessment , Software Process Maturity Assessment And Software Project Assessment , Software Process Assessment A Proponed Software Project Assessment Method. **RBT:L1, L2**	**10 Hours**

Module-5	
Dos And Don'ts Of Software Process Improvement : Measuring Process Maturity, Measuring Process Capability, Staged Versus Continuous Debating Religion, Measuring Levels Is Not Enough, Establishing The Alignment Principle , Take Time Getting Faster, Keep it Simple Or Face Decomplexification, Measuring The Value Of Process Improvement , Measuring Process Compliance , Celebrate The Journey Not Just The Destination. **Using Function Point Metrics to Measure Software Process Improvement: Software** Process Improvement Sequences, Process Improvement Economies, Measuring Process Improvement at Activity Levels **RBT:L1, L2, L3**	**10 Hours**
Course outcomes:	
Upon completion of the course, students shall be able to • Identify and apply various software metrics, which determines the quality level of software • Identify and evaluate the quality level of internal and external attributes of the software product • Compare and Pick out the right reliability model for evaluating the software • Evaluate the reliability of any given software product • Design new metrics and reliability models for evaluating the quality level of the software based on the requirement	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books: 1. Stephen H Khan: Metrics and Models in Software Quality Engineering, Pearson 2nd edition 2013.	
Reference Books: 1. Norman E-Fentor and Share Lawrence Pflieger." Software Metrics". International Thomson Computer Press, 1997. 2. S.A.Kelkar,"Software quality and Testing, PHI Learing, Pvt, Ltd., New Delhi 2012. 3. Watts S Humphrey, "Managing the Software Process", Pearson Education Inc, 2008. 4. Mary Beth Chrissis, Mike Konrad and Sandy Shrum, "CMMI", Pearson Education(Singapore) Pte Ltd, 2003 5. Philip B Crosby, " Quality is Free: The Art of Making Quality Certain ", Mass Market, 1992.	