PONDICHERRY ENGINEERING COLLEGE, PUDUCHERRY – 605 014

CURRICULUM AND SYLLABI FOR AUTONOMOUS STREAM

M.TECH. (INFORMATION SECURITY) COURSES

(FOR STUDENTS ADMITTED FROM ACADEMIC YEAR 2015-16 ONWARDS)

CURRICULUM

I SEMESTER

Subject Code	Name of the Subject	Category#	Periods			Marks*			Credit
			L	T	P	CA	SE	TM	
CS162	Mathematical Foundations of Information Security	TY	3	1	-	40	60	100	4
CS163	Advanced Data Structure and Algorithms	TY	3	1	-	40	60	100	4
CS164	Security Threats and Trusted Computing	TY	3	1	-	40	60	100	4
CS165	Secure Software Engineering	TY	3	1	-	40	60	100	4
	Elective-I	TY	3	1	-	40	60	100	4
	Elective-II	TY	3	1	-	40	60	100	4
CS166	Information Security Laboratory-I	LB	-	-	3	60	40	100	2
Total Credits									**26**

II SEMESTER

Subject Code	Subject	Category#	Periods			Marks*			Credit
			L	T	P	CA	SE	TM	
CS167	Security Standards and Information Security Management	TY	3	1	-	40	60	100	4
CS168	Applied Cryptography	TCM	3	-	2	50	50	100	4
	Elective-III	TY	3	1	-	40	60	100	4
	Elective-IV	TY	3	1	-	40	60	100	4
	Elective-V	TY	3	1	-	40	60	100	4
	Elective-VI	TY	3	1	-	40	60	100	4
CS169	Information Security Laboratory-II	LB	-	-	3	60	40	100	2
CS159	Research Methodology	PR	-	-	3	100	-	100	1
Total Credits									**27**

III SEMESTER

Subject Code	Subject	Category#	Periods			Marks*			Credit
			L	T	P	CA	SE	TM	
CS170	Project Work (Phase I)	PR	-	-	-	150	150	300	9
	Total							**300**	**9**

IV SEMESTER

Subject Code	Subject	Category#	Periods			MARKS*			Credit
			L	T	P	CA	SE	TM	
CS171	Project Work (Phase II)	PR	-	-	-	200	200	400	14
-	Professional Development Courses *(2 one credit courses)*	PR	-	-	-	200	-	200	2
Total Credits									**16**

A representative list of *Professional Development Courses* is given below (*Limited to one credit*):

a) Industrial Training
b) Specific Field Knowledge Training
c) Seminar related with directed study
d) Paper Publication in SCI Journals

CA – Continuous Assessment, **SE** – Semester Examination, **TM** – Total Marks
*** TY** – Theory, **LB** – Laboratory**, TCM** – Theory with a Mini Project, **PR** –Practice

LIST OF ELECTIVES

Sl.No.	Subject Code	Subject	Category
1.	**CSE67**	Internals of Operating System	TY
2.	**CSE68**	Distributed System Security	TY
3.	**CSE69**	Ethical Hacking	TY
4.	**CSE70**	Embedded Systems	TY
5.	**CSE71**	Information Theory and Coding	TY
6.	**CSE72**	Digital and Cyber Forensics	TY
7.	**CSE73**	Mobile Wireless Security	TY
8.	**CSE74**	Security Assessment and Verification	TY
9.	**CSE75**	Internet Security Protocols	TY
10.	**CSE76**	Network Security Essentials	TY
11.	**CSE77**	Human Aspects in Information Security	TY
12.	**CSE78**	Game Theory	TY
13.	**CSE79**	Database Security and Auditing	TY
14.	**CSE80**	Intelligent Systems	TY
15.	**CSE81**	Cloud and Big Data Security	TY
16.	**CSE82**	Data Hiding and Biometric Security	TY
17.	**CSE83**	Intellectual Property Rights	TY
18.	**CSE84**	Information Security Policies	TY
19.	**CSE85**	Secure Coding	TY
20.	**CSE86**	Web Application Security	TY

SYLLABUS (Core Subjects)

Department : Computer Science and Engineering		**Programme:** M.Tech. (Information Security)						
Semester : One		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS162	Mathematical Foundations of Information Security	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To provide concepts of security and mechanisms • To learn mathematical background foundation insight of information security							
Outcomes	On successful completion of the course, the students will be able to: • apply the concepts in the implementation of security issues • mathematically prove the efficiency of the cryptography algorithms • perform crypt analysis							
UNIT – I								**Hours: 09**
Topics in elementary number theory: O and Ω notations – time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruences: Definitions and properties – linear congruences, residue classes, Euler's phi function – Fermat's Little Theorem – Chinese Remainder Theorem – Applications to factoring – finite fields – quadratic residues and reciprocity: Quadratic residues – Legendre symbol – Jacobi symbol.								
UNIT – II								**Hours: 09**
Simple Cryptosystems: Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric Cryptosystems – Cryptanalysis – Block ciphers –Use of Block Ciphers – Multiple Encryption – Stream Ciphers – Affine cipher – Vigenere, Hill, and Permutation Cipher – Secure Cryptosystem.								
UNIT – III								**Hours: 09**
Public Key Cryptosystems: The idea of public key cryptography – The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem – Bit security of RSA – ElGamal Encryption - Discrete Logarithm – Knapsack problem – Zero-Knowledge Protocols – From Cryptography to Communication Security - Oblivious Transfer.								
UNIT – IV								**Hours: 09**
Primality and Factoring: Pseudoprimes – the rho (γ) method – Format factorization and factor bases – the continued fraction method – the Quadratic Seieve method.								
UNIT – V								**Hours: 09**
Number Theory and Algebraic Geometry: Elliptic curves – basic facts – Elliptic Curve Cryptosystems – Elliptic Curve Primality Test – Elliptic Curve Factorization. **(*Theorem Proofs are excluded from all the units in this course of study)**								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			

Text Books:

1. Neal Koblitz, A Course in Number Theory and Cryptography, 2nd Edition, Springer, 2002.
2. Johannes A. Buchman, Introduction to Cryptography, 2nd Edition, Springer, 2004.

Reference Books:

1. Serge Vaudenay, Classical Introduction to Cryptography – Applications for Communication Security, Springer, 2006.
2. Victor Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press, 2005.
3. A. Manezes, P. Van Oorschot and S. Vanstone, Hand Book of Applied Cryptography, CRC Press, 2001.
4. S.C. Coutinho, The Mathematics of Ciphers – Number Theory and RSA Cryptography, A.K. Peters, Natick, Massachusetts, 1999.

Websites: -

Department : Computer Science and Engineering					**Programme :** M.Tech. (Information Security)			
Semester : One					**Category :** TY			
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS163	Advanced Data Structure and Algorithms	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To learn techniques for designing algorithms using appropriate data structures • To develop the data structures for implementing the algorithms • To identify a problem and analyze it in terms of its significant parts and the information needed to solve it							
Outcomes	On successful completion of the course, the students will be able to: • Familiarize the student with good programming design methods, particularly Top-Down design • Develop skills of design and analysis of algorithms in program development and organization • Solve problems using different data structures and design techniques, and compare their performance and tradeoffs • Prove correctness and analyze run time complexity of algorithms							
UNIT – I								**Hours: 09**
Mathematical Induction - Asymptotic Notations – Algorithm Analysis - NP-Hard and NP Completeness – Recurrence Equations – Solving Recurrence Equations – Memory Representation of Multi-dimensional Arrays – Time-Space Tradeoff.								
UNIT – II								**Hours: 09**
Heapsort – Quicksort – Topological sort - Sorting in Linear Time – Elementary Data Structures – Hash Tables – Binary Search Trees – AVL Trees – Red-Black trees – Multi-way Search Trees – B-Trees- Fibonacci Heaps – van Emde Boas Trees – Data Structures for Disjoint Sets.								
UNIT – III								**Hours: 09**
Divide-and-Conquer – Greedy – Dynamic Programming – Amortized Analysis - Backtracking – Branch-and-Bound techniques.								
UNIT – IV								**Hours: 09**
Elementary graph Algorithms – Minimum Spanning Trees – Single-Source Shortest Paths- All- Pairs Shortest Paths – Maximum Flow - Multithreaded Algorithms.								
UNIT – V								**Hours: 09**
Linear programming – Polynomials and FFT – Number-Theoretic Algorithms – NP-Completeness – Approximation Algorithms.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			
Text Books:								
1. Thomas H. Coreman, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, Introduction to Algorithms, PHI, 3rd Edition, 2010. 2. G. Brassard and P. Bratley, Algorithmics: Theory and Practice, Printice –Hall, 1997.								
Reference Books:								
1. E. Horowitz, S.Sahni and Dinesh Mehta, Fundamentals of Data structures in C++, Uiversity Press, 2007. 2. E. Horowitz, S. Sahni and S. Rajasekaran, Computer Algorithms/C++, 2nd Edition, University Press, 2007. 3. Alfred V. Aho, Jeffrey D. Ullman, John E. Hopcroft, Data Structures and Algorithms, Addison Wesley.								
Websites:								
1. http://nptel.ac.in/courses/106102064/ 2. http://www.radford.edu/~nokie/classes/360/								

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester : One		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS164	Security Threats and Trusted Computing	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To introduce the various types of threats to security, approaches for threat modeling and threat containment. • To familiarize the vulnerability scanning process and the tools available. • To introduce the concept of Trusted Computing.							
Outcomes	On successful completion of the course, the students will be able to: • Understand the various threats to security and their relation to vulnerabilities. • Perform threat modeling to identify, prioritize and mitigate threats. • Understand the operation of Trusted Computing.							
UNIT – I	**Introduction**							**Hours: 09**
Sources of security threats – Motives – Consequences of Threats – Target assets and vulnerabilities – Vulnerability Assessment – Vulnerability Assessment Tools – Vulnerability Databases – Network Scanning Tools – Penetration Testing – Insider Threats – Environmental Threats.								
UNIT – II	**Network Security Threats**							**Hours: 09**
Worms, Spams, Ad ware, Spy ware, Trojans and covert channels, Backdoors, Bots, Spoofing Attacks, Session Hijacking, Computer Sabotage, DoS and DDoS – Pharming Attacks – Phishing – Buffer Overflow – Format String Attacks – Cross - Site Scripting – Cross Site Request Forgery – SQL Injection– Wardialing – WarFlying – Wardriving – War Chalking – Network Reconnaisance – Cloud Threats.								
UNIT – III	**Threat Modeling**							**Hours: 09**
Approaches to threat modeling – Threat Identification – STRIDE method – Attack Trees – Managing and Addressing Threats – Threat Elicitation Approaches – Threat Prioritization – Threat Modeling Tools.								
UNIT – IV	**Trusted Computing**							**Hours: 09**
Introduction to Trusted Computing – Secure Co processors – Cryptographic accelerators – Dongles – Trusted platform modules – Motivating scenarios.								
UNIT – V	**Design Goals and Implementation**							**Hours: 09**
Design goals of Trusted Computing modules – Trusted computing and Secure Storage – Trusted Computing and Secure Identification – Administration of Trusted Devices.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			

Text Books:

1. John Vacca, Managing Information Security, 2 nd Edition, Syngress, 2014.
2. Adam Shostack, Threat Modeling, Designing for Security, John Wiley and Sons, 2014.
3. David Challener, Kent Yoder, Ryan Catherman, David Safford, Leendert Van Doorn , A Practical Guide to Trusted Computing, Pearson Education, 2007.

Reference Books:

1. EC-Council, Network Defense: Security Policy and Threats, Cengage Learning, 2010.
2. Sean Smith Trusted Computing Platforms: Design and Applications, Springer Science & Business Media, 2006.

Websites:

1. http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-hackers
2. https://msdn.microsoft.com/en-us/library/cc723507.aspx
3. https://www.uts.sc.edu/itsecurity/threats.shtml

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester : One		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS165	Secure Software Engineering	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To understand the security concerns that need to be taken care in every phase of the software development • To understand how the security requirements are incorporated into software systems							
Outcomes	On successful completion of the course, the students will be able to: • appreciate the importance of security considerations in software engineering • design and develop secure software systems							
UNIT – I	**Introduction to Secure Software Engineering**							**Hours: 09**
Security Issues in Software – Software Assurance and Software Security – Threats and Sources of Software Insecurity – Benefits of Detecting Software Security Defects Early – Managing Secure Software Development – Defining Properties of Secure Software – How to Influence, Assert and Specify Desired Security Properties.								
UNIT – II	**Requirements Gathering for Secure Software**							**Hours: 09**
Introduction – Misuse and Abuse Cases – The SQUARE Process Model – SQUARE Sample Outputs – Requirements Elicitation – Requirements Prioritization.								
UNIT – III	**Secure Software Architecture and Design**							**Hours: 09**
Software Security Practices for Architecture and Design: Architectural Risk Analysis – Software Security Knowledge for Architecture and Design: Security Principles – Security Guidelines and Attack Patterns.								
UNIT – IV	**Secure Coding and Testing**							**Hours: 09**
Code Analysis – Coding Practices – Software Security Testing – Security Testing Considerations Throughout the SDLC.								
UNIT – V	**Security – Complexity and Management for Secure Software**							**Hours: 09**
Security Failures – Functional and Attacker Perspectives for Security Analysis – System Complexity Drivers and Security – Deep Technical Problem Complexity – Governance and Security – Adopting an Enterprise Software Security Framework – Required Level of Security – Security and Project Management – Maturity of Practice.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			
Text Books:								
1. Allen Julia H, Specifications of Software Security Engineering: A Guide for Project Managers, SEI Series in Software Engineering, Addison-Wesley Professional, 2013.								
Reference Books:								
1. Mouratidis Haralambos, Software Engineering for Secure Systems: Industrial and Research Perspectives, Premier Reference Source, IGI Global, 2011.								
Websites:								
1. www.sis.pitt.edu/jjoshi/Devsec/secureSoftware.pdf 2. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/secure-software-engineering/secure-software-engineering-initiatives/L3SSE_ Final_Report_13May2011.pdf								

Department : Computer Science and Engineering				**Programme :** M.Tech. (Information Security)				
Semester : One				**Category :** LB				
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS166	Information Security Laboratory – I	-	-	3	2	60	40	100

Prerequisite	-
Objectives	• To gain a hands on experience of cryptographic algorithms • To inculcate logical and practical thinking towards security problem solving • To learn a hands on experience of threats and attacks
Outcomes	On successful completion of the course, students will be able to: • Implement cryptographic algorithms to solve specified problems • Solve Security Problem for the industry • Have the programming skills in the aspects of security

Cycle – I **Hours: 30**

Any Ten of the following exercises have to be Implemented

1. Understanding of cryptographic algorithms and implementation of the same in C or C++
2. Performance evaluation of various cryptographic algorithms
3. Illustrate Intrusion Detection and IPS
4. Program to implement AVL tree
5. Program to implement Dynamic Programming.
6. To verify the integrity of the message using Digital signature.
7. Penetration Testing and justification of penetration testing through risk analysis
8. Password guessing and Password Cracking
9. Configuring S/MIME for e-mail communication
10. Implementation of Access Control List
11. Develop an application which should include authentication, authorization and access control mechanism.
12. Implement Elliptic Curve Cryptosystems
13. Implement RSA Cryptosystem
14. Implement the Diffie–Hellman Key Agreement Protocol
15. Implement Zero-Knowledge Protocol
16. Implement Oblivious Transfer

Cycle – II **Hours: 15**

17. Any Five programs related to concern electives offered in this semester need to be implemented.

Total contact Hours: -	**Total Tutorials: -**	**Total Practical Classes: 45**	**Total Hours: 45**

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester : Two		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS167	Security Standards and Information Security Management	3	1	-	3	40	60	100
Prerequisite:	-							
Objectives	• To compile, analyze, and assess the applicability of best practices in addressing information security issues • To integrate principles and techniques of risk analysis, project planning and ethics in the development of information security strategies • To understand the security standards, laws and policies and practice in information security							
Outcomes	On successful completion of the course students will be able to: • Design information system with high level of security by planning and risk assessment • Have knowledge on security standards, laws and policies and practice in information security • Design information security by developing the Security Program using Management Models							

UNIT – I	**Introduction**	**Hours: 09**

Introduction to the Management of Information Security: Principles of Information Security Management – Applying Project Management to Security – Project Management Tools – Planning for Security: The Role of Planning – Precursors to Planning– Strategic Planning – Information Security Governance– Information Security Policy, Standards, and Practices – Planning for Information Security Implementation – Planning for Contingencies: Fundamentals of Contingency Planning–Components of Contingency Planning– Business Resumption Planning – Testing Contingency Plans.

UNIT – II	**Security Policy and Standards**	**Hours: 09**

Information Security Policy: Enterprise Information Security Policy – Issue-Specific Security Policy – System-Specific Security Policy – Guidelines for Effective Policy – Security Standards: Overview of ISO 17799/ISO 27001 Standards– System Security Engineering Capability Maturity Model (SSE-CMM) – Information Systems Security Certification and Accreditation NIST SP 800-37, NSTISS Instruction-1000, ISO 27001/27002 Systems Certification and Accreditation – Emerging Trends in Certification and Accreditation.

UNIT – III	**Risk Management and Auditing for Security**	**Hours: 09**

Overview of Risk Management: Identifying Risk – Assessing Risk – Controlling Risk– Risk Control Strategies– Selecting a Risk Control Strategy – Quantitative Versus Qualitative Risk Control Practices – Managing Risk – Feasibility and Cost-Benefit Analysis – Recommended Risk Control Practices – Introduction to Security Audits: Need for security audits – Organizational roles – Auditor's roles – Types of security audits – Audit approaches – Technology based audits.

UNIT – IV	**Information Security Management in Organizations**	**Hours: 09**

Developing the Security Program: Organizing for Security – Placing Information Security within an Organization – Components of the Security Program – Information Security Roles and Titles – Implementing Security Education, Training and Awareness Program – Security Management Models: Blueprints, Frameworks, and Security Models – Access Control Models – Security Architecture Models – Security Management Models– Security Management Practices: – Benchmarking – Performance Measures in Information Security Management. – Personnel and Security: Staffing the Security Function – Information Security Professional Credentials – Security Considerations for Nonemployees – Employment Policies and Practices.

UNIT – V	**Law, Ethics and Maintenance**	**Hours: 09**

Legal, Ethical, and Professional Issues in Information Security: Information Security and the Law – Laws and Legal Framework for Information Security – Indian IT Act– Indian Copyright Act – HIPAA of 1996, GLBA of 1999, and FISMA Acts – U.S. Laws – International Laws and Legal Bodies –Ethics in Information Security –Professional Organizations and their Codes of Ethics – Information Security Maintenance: Security Management Maintenance Models – Digital Forensics.

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, First Edition, Wiley India Pvt Ltd, 2008.
2. Michael Whitman and Herbert Mattord, Management of Information Security, Fourth Edition, Cengage Learning, 2014.

Reference Books:

1. Michael Whitman and Herbert Mattord, Principles of Information Security, Fifth Edition, Cengage Learning, 2015.
2. Harold F. Tipton, Information Security Management Handbook, Sixth edition, CRC Press, 2012.
3. Thomas R. Peltier, Information Security Policies and Procedures, 2nd Edition, Auerbach Publications, 2004.

Websites:

1. http://www.cert.org/octave/
2. http://www.isaca.org/
3. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
4. http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter18.html

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester : Two		**Category :** TCM						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS168	Applied Cryptography	3	-	2	4	50	50	100

Prerequisite	-
Objectives	• To understand the various cryptographic concepts, algorithms and various methods of analysis of the cryptographic algorithms • To understand the underlying mathematical structures of cryptographic algorithm • To get an overview of the various applications of the cryptographic algorithms and implement them in mini project
Outcomes	On successful completion of the course, the students will be able to: • Understand the theories and concepts of Cryptographic • Understand the Cryptographic Techniques • Design the Cryptographic Algorithms • Apply Cryptographic Algorithms in real world problems

UNIT – I	**Cryptographic Protocols**	**Hours: 09**

Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols – Advanced Protocols - Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity -Blind Signatures - Identity-Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures – Esoteric Protocols.

UNIT – II	**Cryptographic Techniques**	**Hours: 09**

Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode - Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving - Block Ciphers versus Stream Ciphers - Choosing an Algorithm - Public-Key Cryptography versus Symmetric Cryptography - Encrypting Communications Channels -Encrypting Data for Storage - Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption - Detecting Encryption – Hiding and Destroying Information.

UNIT – III	**Cryptographic Algorithms**	**Hours: 09**

Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation - Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) – Lucifer - Madryga - NewDES - GOST – 3 Way – Crab – RC5 - Double Encryption - Triple Encryption - CDMF Key Shortening - Whitening.

UNIT – IV	**Cryptographic Algorithms Design**	**Hours: 09**

Pseudo-Random-Sequence Generators and Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs - Nonlinear-Feedback Shift Registers - System-Theoretic Approach to Stream-Cipher Design - Complexity-Theoretic Approach to Stream-Cipher Design **-** N-Hash - MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) - One-Way Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes.

UNIT – V	**Cryptographic Algorithms Application**	**Hours: 09**

RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) - Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes – Ongchnorr - Shamir -Cellular Automata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -Shamir's Three-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture.

Mini Project		**Hours: 30**

The students need to form in teams with maximum 3 students and carry out the mini project. Each team has to take a real world security issues or problem. They have to analyze, design and solve the problem using the suitable cryptographic protocols and algorithms.

Total contact Hours: 45	**Total Tutorials: -**	**Total Practical Classes: 30**	**Total Hours: 75**

Text Books:

1. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc, 2nd Edition, 2007.

Reference Books:

1. Wenbo Mao, Modern Cryptography Theory and Practice, Pearson Education, 2004.
2. Atul Kahate, Cryptography and Network Security, Tata McGrew Hill, 2003.

3. William Stallings, Cryptography and Network Security, 3rd Edition, Pearson Education, 2003.

Websites:

1. http://cacr.uwaterloo.ca/hac/l
2. www.inderscience.com/jhome.php?jcode=IJACT

Department : Computer Science and Engineering				**Programme :** M.Tech. (Information Security)				
Semester : Two				**Category :** LB				
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS169	Information Security Laboratory – II	-	-	3	2	60	40	100
Prerequisite	-							
Objectives	• To gain a hands on experience of security design, analysis and testing tools • To asses and implement web application with Information security							
Outcomes	On successful completion of the course, students will be able to: • Design solution for to solve specified problems • Analyze and Design security solutions to problems in applications and network layers • calculate the strength of the generated password • asses and implement web application with Information security							
Cycle – I								**Hours: 15**

1. Any Four programs related to concern electives offered in this semester need to be implemented.
2. The following exercises have to be implemented using various software tools/utilities.
    - i. Passive Information Gathering
        - a. IP Address and Domain Identification of log entries
        - b. Information Gathering of a web site
        - c. Banner Grabbing
    - ii. Detecting Live Systems
        - a. Port Scanning
        - b. Passive Fingerprinting
        - c. Active Fingerprinting
    - iii. Enumerating Systems
        - a. SNMP Enumeration
        - b. Enumerating Routing Protocols
    - iv. Automated Attack and Penetration Tools
        - a. Vulnerability Assessment Tool
    - v. Defeating Malware
        - a. Building Trojans, Rootkit Hunter
        - b. Finding malware
    - vi. Securing Wireless Systems
        - a. Scan WAPs
    - vii. Network analysis
        - a. Analyze your network using any tool
        - b. Find the Vulnerabilities present in your Network
        - c. Perform Penetration Testing on your network
        - d. Implement Pro-active and Reactive measures to secure your network

Cycle – II	**Hours: 30**

3. Setting up the local security policy
4. Develop a web application with secure database using any hashing algorithm
5. Program to generate Password automatically which is easy to remember and calculate the strength the generated password
6. Develop a web application and perform penetration testing to detect the vulnerabilities present in it.
7. Suggest and implement measures to overcome the vulnerabilities identified in exercise 4

Total contact Hours: -	**Total Tutorials: -**	**Total Practical Classes: 45**	**Total Hours: 45**

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester : Two		**Category :** PR						
Subject code	**Subject**	**Hours/week**			**Credit**	**Maximum marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS159	Research Methodology	-	-	3	1	100	0	100
Prerequisite	-							
Objectives	• To educate students to methods of selection of research problems • To expose students to different research methods							
Outcomes	• Students will be capable to identify and narrow down to the area of research on the basis the requirements of industrial and global requirements • Students will exhibit the domain skill to choose suitable research methods to execute research effectively • Students will possess knowledge to further their academic program, namely, Ph.D program.							

- **Definition of research:** Research – Definition; Concept of Construct, Postulate, Proposition, Thesis, Hypothesis, Law, Principle. Definition and Dimension of a Theory, Functions and Characteristics; Types of Theory: General Theory and Particular/ Empirical Theory. Cases and their Limitations; Causal Relations. Philosophy and validity of research. Objective of research.
- **Characteristics of research:** Various functions that describe characteristics of research such as systematic, valid, verifiable, empirical and critical approach.
- **Types of research:** Pure and applied research. Descriptive and explanatory research. Qualitative and quantitative approaches.
- **Research procedure:** Formulating the Research Problem, Literature Review, Developing the objectives, Preparing the research design including sample. Design, Sample size.
- **Considerations in selecting research problem:** Relevance, interest, available data, choice of data, Analysis of data, Generalization and interpretation of analysis.
- **Outcome of research:** Significance of report writing – Layouts of the research report – Types of reports – Oral presentation – Mechanics of writing research report – Precautions for writing research reports – Plagiarism and copy right violation – Patent writing and filing.

Total contact hours: -	**Total tutorials: -**	**Total practical classes:15**	**Total hours: 15**

Reference books:

1. Dawson, Catherine, Practical Research Methods, UBS Publishers and Distributors, New Delhi, 2002
2. Kothari, C.R., Research Methodology-Methods and Techniques, Wiley Eastern Limited, New Delhi, 1985.
3. Kumar, Ranjit, Research Methodology, A Step-by-Step Guide for Beginners, (2nd.ed), Pearson Education, Singapore, 2005.

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester : Three		**Category :** PR						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS170	Project Work (Phase I)	-	-	-	9	150	150	300
Prerequisite	-							
Objectives	• To expose students with project-product development cycle using state-of-art technologies • To understand the Product Development Cycle through Project • To plan for various activities of the project							
Outcome	On successful completion of the course, the students will be able to: • Able to State problem definition clearly • Prepare SRS for projects and develop design • Exposure to Learning and knowledge access techniques using Conferences, Journal papers and participation in research activities							
PHASE – I								
The student is required to do the following: 1. Select a Research Problem. 2. Conduct a Survey in the chosen area. 3. Perform a feasibility study. 4. Study the limitations of the Existing System. 5. Define the Problem Statement and Objectives. 6. Choose the Research Methodology. 7. Finalize the Experimental Environment. 8. Choose the evaluation parameters. 9. Implement the Existing System. 10. Document the outcome of Phase I.								
Total contact Hours: -	**Total Tutorials: -**	**Total Practical Classes: -**			**Total Hours: -**			

Department : Computer Science and Engineering					**Programme :** M.Tech. (Information Security)			
Semester : Four					**Category :** PR			
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CS171	Project Work (Phase II)	-	-	-	14	200	200	400
Prerequisite	-							
Objectives	• To encourage and expose students for participation in National/ International paper presentation activities • Acquire in depth working knowledge in the chosen area of problem							
Outcomes	On successful completion of the course, the students will be able to: • Acquire knowledge and skills needed for the construction of highly software project • Enhance the technical presentation skills • Inculcate the practice of publishing in Conferences and Journal							
PHASE – II								
The student is required to do the following: 1. High level Design of the Proposed Solution. 2. Detailed Design of the Proposed Solution. 3. Implementation of the Proposed Solution. 4. Comparison of the performance with the existing system 5. Document the results in the Project Report.								
Total contact Hours: -	**Total Tutorials: -**	**Total Practical Classes: -**			**Total Hours: -**			

SYLLABUS (Elective Subjects)

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE67	Internals of Operating System	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To identify the necessity of various sub systems in UNIX operating system. • To analyze the mechanism of process communication and the differences in the organization of Unix and Windows operating systems • To design various data structures needed to develop an operating system							
Outcomes	On successful completion of the course, the students will be able to: • Explain the components in Unix and Windows operating system • Use the system calls whenever they are necessary • Know the storage of information of system usage and other information in Windows system and develop the algorithms to perform kernel functions							
UNIT – I	**Buffer cache and File sub-system**							**Hours: 09**
Introduction to Kernel - Architecture of the UNIX operating system, System concepts, Data structures. Buffer Cache: Buffer header, Structure of Buffer pool, Reading and writing disk blocks. Files INODES, Structure of a regular file, Directories, Super block, Inode assignment.								
UNIT – II	**System Calls and Process sub-system**							**Hours: 09**
System calls - OPEN, Read, Close, Write, Create, CHMOD, CHOWN, Pipes, Mounting and Unmounting. Process - Layout the system memory, Context, Process control, process creation, signals, Process scheduling, time, clock.								
UNIT – III	**Inter-Process Communications**							**Hours: 09**
Inter-Process Communications - Process tracing, System V IPC, Shared Memory, Semaphores. Network Communications - Socket programming: Sockets, descriptors, Connections, Socket elements, Stream and Datagram Sockets.								
UNIT – IV	**Windows System Components**							**Hours: 09**
Windows Operating system - versions, Concepts and tools, Windows internals, System Architecture, Requirements and design goals, Operating system model, Architecture overview, Key system components. System mechanisms - Trap dispatching, object manager, Synchronization, System worker threads, Windows global flags, Local procedural calls, Kernel event tracing.								
UNIT – V	**Registry and Process Management**							**Hours: 09**
Windows Management Mechanisms - The registry, Registry usage, Registry data types, Local structure, Trouble shooting Registry problems, Registry Internals, Services, Applications, Accounts, Service control Manager, Windows Management Instrumentation, Processes, Threads, and Jobs: Process Internals, Flow of create process, Thread Internals, Examining Thread creation, Thread Scheduling, Job Objects.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			

Text Books:

1. Maurice J. Bach, The Design of the Unix Operating System, Prentice Hall of India, 1991
2. Mark E. Russinovich and David A. Solomon, Microsoft® Windows® Internals, Microsoft Press, 2004.

Reference Books:

1. William Stallings, "Operating Systems: Internals and Design Principles", 5th Edition, Prentice Hall, 2005.

Websites:

1. https://technet.microsoft.com/en-in/sysinternals/bb963901.aspx
2. https://social.microsoft.com/Forums/en-us/home?category=windowsacademic
3. https://www.gnu.org/
4. http://www.linux.com/directory/Distributions/desktop
5. http://www.ubuntu.com/download
6. https://www.suse.com/download-linux/

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE68	Distributed System Security	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To understand the various threats, vulnerabilities, solutions and security standards for each layers of distributed systems • To understand the secure software development lifecycle process for distributed systems							
Outcomes	On successful completion of the course students will be able to: • Structure and design the distributed systems using multiple levels of security • Have knowledge on the threats, vulnerabilities and solution at various level of distributed systems							

UNIT – I	**Hours: 09**
Introduction: – Distributed Systems, Distributed Systems Security. Security in Engineering: Secure Development Lifecycle Processes - A Typical Security Engineering Process - Security Engineering Guidelines and Resources. Common Security Issues and Technologies: Security Issues – Common Security Techniques.	
UNIT – II	**Hours: 09**
Host-level Threats and Vulnerabilities: Transient code Vulnerabilities - Resident Code Vulnerabilities - Malware: Trojan Horse – Spyware - Worms/Viruses – Eavesdropping - Job Faults - Resource Starvation - Overflow - Privilege Escalation - Injection Attacks. Infrastructure-Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities - Grid Computing Threats and Vulnerabilities – Storage Threats and Vulnerabilities – Overview of Infrastructure Threats and Vulnerabilities.	
UNIT – III	**Hours: 09**
Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities -Injection Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues. Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-Level Attacks - Services Threat Profile.	
UNIT – IV	**Hours: 09**
Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code -Memory Firewall – Antimalware. Infrastructure-Level Solutions: Network-Level Solutions - Grid-Level Solutions - Storage-Level Solutions. Application-Level Solutions: Application-Level Security Solutions.	
UNIT – V	**Hours: 09**
Service-Level Solutions: Services Security Policy - SOA Security Standards Stack – Standards in Dept - Deployment Architectures for SOA Security - Managing Service-Level Threats - Compliance in Financial Services - SOX Compliance - SOX Security Solutions - Multilevel Policy-Driven Solution Architecture - Case Study: Grid - The Financial Application - Security Requirements Analysis. Future Directions - Cloud Computing Security – Security Appliances – Usercentric Identity Management - Identity-Based Encryption (IBE) - Virtualization in Host Security.	

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, Distributed Systems Security: Issues, Processes and Solutions, Wiley Pubilications, First Edition, 2009.

Reference Books:

1. Yang Xiao and Yi Pan, Security in Distributed and Networking Systems, World Scientific, 2007.
2. Rachid Guerraoui and Franck Petit, Stabilization, Safety, and Security of Distributed Systems, Springer, 2010.

Websites:

1. http://arxiv.org/ftp/arxiv/papers/1211/1211.2032.pdf
2. http://www.sans.org/reading-room/whitepapers/application/distributed-systems-security-java-corba-com-plus-28

Department : Computer Science and Engineering					**Programme :** M.Tech. (Information Security)			
Semester :					**Category :** TY			
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE69	Ethical Hacking	3	1	-	4	40	60	100

Prerequisite	-	
Objectives	• To immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems • To give students in-depth knowledge and practical experience with the current essential security systems • To learn how intruders escalate privileges and what steps can be taken to secure a system	
Outcomes	On successful completion of the course, the students will be able to: • Defend a computer against a variety of different types of security attacks using a number of hands-on techniques • Defend a LAN against a variety of different types of security attacks using a number of hands-on techniques Practice and use safe techniques on the World Wide Web	
UNIT – I	**Introduction to Ethical Hacking**	**Hours: 12**
Introduction-Importance of Security-Elements of Security-Phase of an Attack- Hacker Attacks –Hacktivism – Ethical Hackers – Computer Crimes and Implication.		
UNIT – II	**Footprints**	**Hours: 12**
Introduction – Information gathering methodology – Footprinting tools – WHOIS Tool- DNS Information tool – Locating the network range – E-mail spiders – Locating network activity – Meta Search Engines.		
UNIT – III	**Scanning and Enumeration**	**Hours: 12**
Scanning: Introduction – Objectives of scanning – Scanning methodologies – Tools – Enumeration: Introduction – Techniques – Procedures – Tools.		
UNIT – IV	**Social Engineering**	**Hours: 12**
Social Engineering: Introduction- Human weakness –Types – Human based social Engineering – Computer based social Engineering – Threats and Defense – Countermeasures- Case studies on Impersonating in Facebook, My Space and Orkut.		
UNIT – V	**System Hacking**	**Hours: 12**
Introduction – Cracking password – Password cracking websites – Password guessing Algorithms – Password cracking Tools – Countermeasure – Escalating Privileges- Executing Applications – Key loggers and spywares.		

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. EC- Council, Ethical Hacking and Countermeasures: Attack Phases, Cengage Learning, 2009.
2. EC- Council, Ethical Hacking and Countermeasures: Threats and Defense Mechanisms, Cengage Learning, 2009.

Reference Books:

1. Michael T. Simpson, Hands-On Ethical Hacking and Network Defense, Cengage Learning, 2012.

Websites:

1. https://www.udemy.com/learn-the-basics-of-ethical-hacking-and-penetration-testing/
2. http://breakthesecurity.cysecurity.org/

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE70	Embedded Systems	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To provide a clear understanding on the basic concepts, ARM processor and Architecture • To introduce on Embedded Process development Environment • To study on Basic of Processes and Operating systems							
Outcomes	On successful completion of the course, the students will be able to: • Have skills in the Embedded C Programming • Design Embedded System with real time constraints							
UNIT – I								**Hours: 09**
Embedded Computing - Challenges of Embedded Systems – Embedded system design process - Processor in Embedded System – Other Hardware Units in the Embedded System - Software Embedded into a System - ARM Architecture: ARM Design Philosophy - Registers - Program Status Register - Instruction Pipeline - Interrupts and Vector Table - Architecture Revision - ARM Processor Families.								
UNIT – II								**Hours: 09**
ARM Instruction Set - Data Processing Instructions - Addressing Modes - Branch, Load, Store Instructions - PSR Instructions - Conditional Instructions. Thumb Instruction Set - Register Usage - Other Branch Instructions - Data Processing Instructions - Single-Register and Multi Register Load-Store Instructions - Stack - Software Interrupt Instructions. ARM Programming using C: Simple C Programs using Function Calls – C-looping structures – Register allocation – Function calls – Pointer aliasing – Structures - Integer and Floating Point Arithmetic– inline functions and inline assembly– Portability issues.								
UNIT – III								**Hours: 09**
Optimizing Assembly Code - Profiling and cycle counting – instruction scheduling – Register allocation – conditional execution – looping constructs – bit manipulation – efficient switches – optimized primitives. Processes and Operating systems - Multiple tasks and processes – Context switching – Scheduling policies – Interprocess communication mechanisms – Exception and interrupt handling - Performance issues.								
UNIT – IV								**Hours: 09**
Introduction to RTOS- Meeting real time constraints –Defining RTOS - The Scheduler - Objects – Services - Characteristics of RTOS - Defining a Task - Tasks States and Scheduling - Task Operations – Structure – Synchronization - Communication and Concurrency. Defining Semaphores - Operations and Use - Defining Message Queue - States – Content – Storage - Operations and Use.								
UNIT – V								**Hours: 09**
Embedded System Development - Multi-state systems and function sequences. Embedded software development tools – Emulators and debuggers. Design methodologies – Case studies – Windows CE – Linux 2.6x and RTLinux – Coding and sending application layer byte stream on a TCP/IP network using RTOS Vxworks – Embedded system for a smart card.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			
Text Books:								
1. Andrew N Sloss, D. Symes and C. Wright, ARM System Developers Guide, Morgan Kaufmann / Elsevier, 2006. 2. Raj Kamal, Embedded Systems – Architecture, Programming and Design, 2nd Edition, McGraw-Hill companies, 2008. 3. Qing Li, Real Time Concepts for Embedded Systems, Elsevier, 2011.								
Reference Books:								
1. Michael J. Pont, Embedded C, Pearson Education, 2007. 2. Wayne Wolf, Computers as Component: Principles of Embedded Computer System Design, 2nd Edition, 2008. 3. Steve Heath, Embedded System Design, Elsevier, 2nd Edition, 2003.								
Websites: -								

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE71	Information Theory and Coding	3	1	-	4	40	60	100

Prerequisite	-
Objectives	• To support the analysis and research on information and information system systematically and comprehensively. • To strengthen the fundamental concepts of information theory and error control coding.
Outcomes	On successful completion of the course, the students will be able to: • understand how error control coding techniques are applied in communication systems • analyze the information and information system

UNIT – I	**Information Theory**	**Hours: 09**

Introduction to Information theory- Uncertainty and information – average mutual information, Average self information, Average conditional self information, Measures of information-Information content of a message-Average information content of symbols in long independent sequences – Average information content of symbols in long dependent sequences – Markoff statistical model for information sources, Entropy and information rate of Markoff sources, Information measure for continuous random variables.

UNIT – II	**Channels and Channel Capacity**	**Hours: 09**

Communication channels, Discrete communication channel-Rate of information transmission over a discrete channel-capacity of a discrete memoryless channel continuous channel – Shannon –Hartley theorem and its implications. Channel models- channel capacity –BSC ,BEC-cascade channels-symmetric channel –unsymmetric channel and their capacities-Information capacity theorem ,Shannon limit , channel capacity for MIMO system.

UNIT – III	**Source Coding**	**Hours: 09**

Purpose of coding, Uniquely decipherable codes ,Shannon's I and II fundamental theorem- Source coding theorem –Huffman coding – Shannon fano-Elias coding, Arithmetic coding –Lempel-Ziv algorithm-Run length encoding and PCX format-Rate distortion function-optimum quantizer design-JPEG standard for lossless and lossy compression.

UNIT – IV	**Channel Coding**	**Hours: 09**

Linear block codes and cyclic codes-Galois fields, Vector spaces and matrices, Noisy channel coding theorem, Matrix description of linear blocks codes-Equivalent codes-parity check matrix, Decoding of linear block codes , error detection and error correction capability perfect codes, Hamming codes, Low density parity check (LDPC) codes, Optimal linear codes, Maximum distance separable (MDS) codes-Bounds on minimum distance-space time block codes. Method fee generating cyclic codes- Matrix description of cyclic codes, syndrome calculation, Error detection and correction quasi cyclic codes and shortened cyclic codes and shortened cyclic codes, Fire codes, Golay codes ,CRC codes, BCH codes, RS codes.

UNIT – V	**Channel Coding - Convolution Codes**	**Hours: 09**

Convolution codes and Trellis codes-Tree codes and Trellis codes, polynomial description of convolutional codes-Viterbi decoding of convolutional codes distance bounds-performance bounds, Turbo codes-Turbo decoding-Interleaver design concept of coded modulation, Ungerboecks TCM-Design rules-Decoders, TCM for AWGN channel, TCM for fading channel, Space Time Trellis Codes.

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. J.Das, SK.Mullick and PK Chatterjee, Principles of Digital Communication, Wiley Eastern Limited, 2008.
2. Ranjan Bose, Information Theory Coding and Cryptography, Tata McGraw Hill, New Delhi, 2010.

Reference Books:

1. K. Sam Shanmugam, Digital and Analog Communication Systems, John Wiley and sons, 1994.
2. Simon Haykin, Digital Communications, John Wiley and sons, 1988.

Websites:

1. http://www.nptel.ac.in
2. http://www/aparallel.com

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE72	Digital and Cyber Forensics	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To introduce the fundamental concepts of computer fraud and threat concepts • To familiarize with Cyber forensics and Computer Forensics Technology • To know the concepts of Evidence Collection and Data Seizure							
Outcomes	On successful completion of the course, students will be able to: • Analyze digital forensics and use them to inference for security based problems • Design the new ideas of detecting the key fraud selection process • Design applications related to Computer Forensics techniques							

UNIT – I	**Hours: 09**
Fundamentals of Computer Fraud – Threat concepts – Framework for predicting inside attacks –Managing the threat – Strategic Planning Process. Architecture strategies for computer fraud prevention – Protection of Web sites – Intrusion detection system – NIDS, HIDS – Penetrating testing process – Web Services – Reducing transaction risks.	
UNIT – II	**Hours: 09**
Key Fraud Indicator selection process customized taxonomies – Key fraud signature selection process –Accounting Forensics – Computer Forensics – Journaling and it requirements –Standardized logging criteria – Journal risk and control matrix – Neural networks – Misuse detection and Novelty detection.	
UNIT – III	**Hours: 09**
Introduction to Cyber forensics: Computer Forensics fundamentals, Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems.	
UNIT – IV	**Hours: 09**
Types of Computer Forensics Systems: Internet Security Systems, Intrusion Detection Systems, Firewall Security Systems, Storage Area Network Security Systems, Network Disaster Recovery Systems, Public Key Infrastructure Systems, Wireless Network Security Systems, Satellite Encryption Security Systems, Instant Messaging (IM) Security Systems, Net Privacy Systems, Identity Management Security Systems, Identity Theft, Biometric Security Systems.	
UNIT – V	**Hours: 09**
Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies. Identification of Data, Reconstructing Past Events.	

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. Kenneth C.Brancik, Insider Computer Fraud, Auerbach Publications Taylor & Francis Group, 2008.
2. John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, Charles River Media, 2005.

Reference Books:

1. Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, 2nd edition, Springer, 2010.
2. Computer Forensics: Investigating Network Intrusions and Cyber Crime, Ec-Council Press Series, 2010.

Websites:

1. http://avniet.ac.in/adminpanel/material/book1.pdf
2. http://www.sciencelib.net/files/Brancik-Insider_Computer_Fraud_(Auerbach,2008).pdf

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE73	Mobile Wireless Security	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To focus security issues in the wireless networks • To differentiate between the issues in wired and wireless networks • To educate the students about the security vulnerabilities and counter measures.							
Outcomes	On successful completion of the course, the students will be able to: • Map the mathematical models of security algorithms onto wireless and mobile environment • Understand the specific vulnerabilities in wide range of wireless systems • Design robust systems against state-of-the-art security attacks							

UNIT – I	**Hours: 09**
Introduction to Mobile and Wireless Networks: Cellular Networks, 1G through 3G, IEEE Network - WLAN IEEE 802.11, WPAN IEEE 802.15, WMAN IEEE 802.16, IEEE 802.20, MIH IEEE 802.21, WRAN IEEE 802.22, Mobile Internet Networks – Macro and Micro mobility – Personal mobility – SIP – Identity based mobility, NEMO and MANETs – Vulnerabilities of Wireless Networks – Review of security basics – symmetric and asymmetric cryptography, Hash functions – Electronic signatures – MAC – PKI and electronic certificate – IPSec – AAA protocol – Firewalls – Intrusion detection.	
UNIT – II	**Hours: 09**
Wi-Fi Security Architectures – Hot Spot architecture – WIDS – Rogue AP detection – IEEE 802.11 geolocation techniques – Honeypots – Passive and Active attacks – DOS attacks – Trojan attack – Dictionary Attack. Bluetooth Security – Protocol architecture – Radio physical layer – Device addressing – SCO and ACL logical transports – Security mode – Authentication and pairing – Attacks – BlueSmack.	
UNIT – III	**Hours: 09**
Security in IEEE 802.11 – WEP – WEP2 – IV collisions – RC4 weakness – 802.1x authentication - 802.11i security architecture – policy negotiation – radio security policies – RADIUS – EAP – PKI – WiMAX security – TEK – KEK – IEEE 802.16e – PKMv2-RSA – Security Association – 3 way handshake – role of smart cards in WiMAX.	
UNIT – IV	**Hours: 09**
Security in Ad Hoc Networks – Attacks to routing protocols – Security mechanisms – Auto-configuration – Key management – Self-managed PKI – Resurrecting Duckling – Group key management – Wireless Sensor Networks – Attacks – Preventive mechanisms – Intrusion tolerance – SNEP - µTELSA – TinySec – key management in WSNs.	
UNIT – V	**Hours: 09**
Security in Mobile Telecommunication Networks – SS7 – GSM security – GRPS security – UMTS infrastructure and security – H.323 – SIP – Megaco – VoIP security flaws and countermeasure – IMS architecture – security flaws – 4G security – Protection of interception – Security issues in Mobile IP – HIP – NetLMM.	

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. Hakima Chaouchi and Maryline Laurent-Maknavicius, Wireless and Mobile Network Security: Security basics, Security in On-the-shelf and Emerging Technologies, 2nd Edition, John Wiley & Sons, 2009.
2. Pallapa Venkataram and Sathish Babu, Wireless and Mobile Network Security, 1st Edition, Tata McGraw Hill, 2010.

Reference Books:

1. Lei Chen, Jiahuang Ji, and Zihong Zhang, Wireless Network Security: Theories and Applications, Springer Higher Education Press, 2013.
2. Amitabh Mishra, Security and Quality of Service in Ad Hoc and Wireless Networks, 1st Edition, Cambridge University Press, 2008.
3. S. Kami Makki, Peter Reiher, Kia Makki, Niki Pissinou, Shamila Makki, Mobile and Wireless Security and Privacy, Springer Science, 2007.

Websites:

1. http://www.wi-fi.org/discover-wi-fi/security
2. http://www.netsec.ethz.ch/Publication

3. http:// www.radio-electronics.com/info/wireless/wimax/security-encryption-authentication.php

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE74	Security Assessment and Verification	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To understand the core business processes and the critical technologies that support core business processes • To introduce the methods available to perform risk analysis to identify process-related risks and controls to mitigate those risks • To introduce the key standards and legislations that is relevant for information security							
Outcomes	On successful completion of the course, the students will be able to: • Gain an in-depth understanding of the process, components, skills, and experience required and other factors required for a security risk assessment process • positioned to commission a security risk assessment for any organization that requires security service and address their risks in a cost-effective manner							
UNIT – I								**Hours: 09**
Role of Security assessment in an Information security Program, Need for Security assessment, Related Activities, Information Security Risk Assessment Basics, Security Project Definition, Security Risk Assessment Preparation.								
UNIT – II								**Hours: 09**
Data Gathering, Sampling, RIIOT Method, Administrative, Technical and Physical Data Gathering, Analysis of gathered information.								
UNIT – III								**Hours: 09**
Business process evaluation, Critical Business Processes, Organization, Interviews with Process Owners, Status Meeting with Client, Status Based on Project Plan, Discussion of Critical Technologies, Technology evaluation, Meet with Technology Owners, Hands-On Testing, Manual vs. Automated Testing, Tool Selection, Status Meeting with Client.								
UNIT – IV								**Hours: 09**
Risk Analysis, Determining Risk, Creating Risk Statements, Team Review of Risk Statements, Risk Mitigation, Selecting Safeguards, Establishing Risk Parameters, Risk Assessment Reporting, Report Structure, Risk Assessment Project Management, Assessment Approaches, Qualitative and Quantitative Analysis, Risk Assessment Methods.								
UNIT – V								**Hours: 09**
Information security standards, GAISP, COBIT, ISO17799, NIST Handbook, CC, ITIL, Information security Legislation, Sarbanes Oxley Act, Federal Information Security Management Act, HIPAA, Gramm-Leach-Bliley Act.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			

Text Books:

1. Douglas Landoll, The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, Second Edition, CRC Press, 2011.
2. Sudhanshu Kairab, A Practical Guide to Security Assessments, CRC Press, 2005.

Reference Books:

1. Thomas S. Coleman, A Practical Guide to Risk Management, Research Foundation, 2011.

Websites:

1. https://studentaid.ed.gov/sites/default/files/IVV_Handbook.docx
2. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/risk-assessment/risk-assessment-guideline.html

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE75	Internet Security Protocols	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To introduce some of the known security problems related to the protocols and applications of the Internet • To overview the contemporary security solutions on architectures and protocols. • To understand concepts and terminology associated System level security.							
Outcomes	On successful completion of the course, the students will be able to: • Develop a clear understanding of Internet security protocols • Understand clearly MAC, IP and Transport level protocols • Understand the general system level security							

UNIT – I	**Introduction**	**Hours: 09**

Overview of ISO OSI model and TCP/IP model, Key Management, X.509 certificates, Public-Key Infrastructure (PKI), Remote user authentication using symmetric key encryption, Kerberos, Remote user authentication using asymmetric key encryption Federated Identity management, Biometrics. Intruders, Intrusion detection, Password management, malicious software, Viruses and related threats, Virus countermeasures, Distributed denial of service attacks, Firewalls: Firewall design principles, trusted systems.

UNIT – II	**Wireless Network Security**	**Hours: 09**

IEEE 802.11 Wireless LAN Overview - The Wi-Fi Alliance, IEEE 802 Protocol Architecture, IEEE 802.11 Network Components and Architectural Model ,IEEE 802.11 Services, IEEE 802.11i Wireless LAN Security: IEEE 802.11i Services, IEEE 802.11i Phases of Operation, Discovery Phase, Authentication Phase, Key Management Phase, Protected Data Transfer Phase, The IEEE 802.11i Pseudorandom Function.

UNIT – III	**WAP Security**	**Hours: 09**

Wireless Application Protocol Overview: Operational Overview, WAP Architecture, Wireless Application Environment, WAP Protocol Architecture, Wireless Transport Layer Security: WTLS Sessions and Connections, WTLS Protocol Architecture, Cryptographic Algorithms, WAP End-to-End Security.

UNIT – IV	**Electronic Mail Security**	**Hours: 09**

Pretty Good Privacy: Notation, Operational Description, Cryptographic Keys and Key Rings, Public-Key Management, S/MIME: RFC 5322, Multipurpose Internet Mail Extensions, S/MIME Functionality, S/MIME Messages, S/MIME Certificate Processing, Enhanced Security Services, Domain Keys Identified Mail: Internet Mail Architecture, E-mail Threats, DKIM Strategy, DKIM Functional Flow.

UNIT – V	**Web and IP Security**	**Hours: 09**

Web security: Web security requirements, Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Electronic Transaction (SET), HTTPS, Secure Shell (SSH), IP Security: IP Security overview, Architecture, Authentication, Encapsulating security payload, Combining security associations, Key management. E-commerce security: SET and other e-cash and micropayment schemes.

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. William Stallings, Cryptography and Network Security: Principles and Practice, 5th Edition, Pearson Education, 2006.
2. Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw-Hill, 2011.

Reference Books:

1. R. Oppliger, Internet and Intranet Security, second edition, Artech House, 2002.
2. A. Rubin, D. Geer and M. Ranum, Web Security Sourcebook, Wiley, 1997.
3. W. Cheswick and S. Bellovin, Firewalls and Internet Security, Addison-Wesley, 1994.

Websites:

1. http://www.cert.org/
2. http://www.ietf.org/
3. http://www.setco.org/set_specifications.html

4. http://www.drizzle.com/~aboba/IEEE/
5. http://www.cerias.purdue.edu/coast/firewalls/
6. http://www.cerias.purdue.edu/coast/intrusion-detection/welcome.html

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE76	Network Security Essentials	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To introduce the security problems associated with malicious software and intruders • To familiarize the network security controls that help to protect the usability, integrity, reliability and safety of the network infrastructure and the data that travels through it							
Outcomes	On successful completion of the course, the students will be able to: • Identify the attacks against network infrastructure and the sources of attacks • Identify the various types of security controls available to protect the network infrastructure • Implement appropriate security controls to safeguard the network infrastructure							
UNIT – I	**Introduction**							**Hours: 09**
Characteristics of Networks, Need for network security, Intruders, Malicious Software, Reconnaissance, Eavesdropping, wiretapping, impersonation, traffic analysis, website defacement, DOS, active code or mobile code attacks, OSI Security Architecture, Security Services, Model for Network Security.								
UNIT – II	**Cryptography and Key Distribution**							**Hours: 09**
Classical Encryption Techniques, Symmetric Encryption Principles, Symmetric Encryption Algorithms, DES, AES, Stream Ciphers, Block Cipher Modes of Operation, Public Key Cryptography Principles, Public Key Cryptographic Algorithms, RSA,ECC, Key Distribution using Symmetric and Asymmetric Encryption, Kerberos, X.509, Public Key Infrastructure, trust models, revocation, directories.								
UNIT – III	**Message Authentication and Digital Signatures**							**Hours: 09**
Requirement of Authentication Functions, Message Authentication Codes, Hash and MAC Algorithms, MD2, MD4, MD5, SHA, HMAC, CMAC, Whirlpool, Address bases authentication, password based authentication, trusted intermediaries, digital Signatures, Digital Signature Standard.								
UNIT – IV	**IP Security, Transport Layer Security**							**Hours: 09**
IP Sec, Authentication header, Encapsulating Security Payload, IKE, ISAKMP/IKE Encoding, Web Security Issues, Secure Sockets Layer, Transport Layer Security, Negotiating cipher suites, compression methods , encoding, HTTPS, Secure Shell.								
UNIT – V	**Network Security Applications**							**Hours: 09**
Electronic Mail Security, Privacy enhanced mail, PGP, SMIME, Authorization and Access control, Firewalls, Intrusion Detection and Prevention Systems, Honeypots, honetnets, scanning and analysis tools, Antivirus Software, Virtual Private Network.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			

Text Books:

1. William Stallings, Cryptography and Network Security Principles and Practices, 6th Edition, Prentice Hall, 2013.
2. Behrouz A. Fourouzan, Cryptography and Network security, 2nd Edition, Tata McGraw-Hill, 2012.
3. Charlie Kaufman, Radia Peralman, Mike Speciner, Network Security: Private communication in public world, 2nd edition, Prentice Hall, 2002.

Reference Books:

1. Williams Stallings, Network Security Essentials: Applications and Standards, 4th Edition, Pearson Education, 2011.
2. Charles P. Pfleeger, Security in Computing, 4th Edition, Prentice Hall, 2006.

Websites:

1. http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/download-course-materials/
2. http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-875-cryptography-and-cryptanalysis-spring-2005/

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE77	Human Aspects in Information Security	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To learn and understand the human aspects and socio cultural aspects of security • To understand usable security and privacy • To understand security from the perspective of an organization							
Outcomes	On successful completion of the course, the students will be able to: • Understand the motivations for misuse • Recognize the importance of user acceptance of security policies and technologies • Realize the need for Non-intrusive security and organizational governance for information security							

UNIT – I	**Human and Psychological Aspects**	**Hours: 09**
Human and Social Aspects of Password Authentication- Human and Social Aspects of Password Authentication- Why Humans are the Weakest Link- Impact of the Human Element on Information Security- The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions- Trusting Computers Through Trusting Humans: Software Verification in a Safety-Critical Information Society.		
UNIT – II	**Social and Cultural Aspects**	**Hours: 09**
Information Security Culture as a Social System: Some Notes of Information Availability and Sharing- Social Aspects of Information Security: An International Perspective- Social and Human Elements of Information Security: A Case Study- Effects of Digital Convergence on Social Engineering Attack Channels- A Social Ontology for Integrating Security and Software Engineering.		
UNIT – III	**Usability Issues**	**Hours: 09**
Security Configuration for Non-Experts: A Case Study in Wireless Network Configuration - Security Usability Challenges for End-Users - CAPTCHAs: Differentiating between Human and Bots- Privacy Concerns when Modeling Users in Collaborative Filtering Recommender Systems.		
UNIT – IV	**Organizational Aspects**	**Hours: 09**
An Adaptive Threat-Vulnerability Model and the Economics of Protection- Bridging the Gap between Employee Surveillance and Privacy Protection- Aligning IT Teams' Risk Management to Business Requirements- Security Requirements Elicitation: An Agenda for Acquisition of Human Factors - Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis.		
UNIT – V	**Organizational Security**	**Hours: 09**
Responsibilities and Liabilities with respect to catastrophes-The complex new world of information security-Employee Surveillance based on Free Text Detection of Keystroke Dynamics-E-risk insurance product design: A Copula based Bayesian Belief Network-E-commerce Security and Honesty-credit-Towards a Scalable Role and Organization Based Access Control Model with Decentralized Security Administration-Enterprise Information System Security ; A Life-Cycle Approach.		

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. Raj Sharman and Manish Gupta, Social and Human Elements of Information Security: Emerging Trends and Countermeasures, IGI Global, 2008.
2. Manish Gupta and Raj Sharman, Handbook of research on social and organizational liabilities in information security, IGI Global, 2008.

Reference Books:

1. H. Raghav Rao and Shambhu Upadhyaya, Information Assurance, Security and Privacy Services, Emerald Group Publishing, 2009.
2. Hamid Nemati, Pervasive Information Security and Privacy Developments: Trends and Advancements, IGI Global, 2011.

Websites: -

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE78	Game Theory	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To train students in the logic and strategic decision making involved in the theory of games. • To learn the classification of games the course will move onto important definitions and concepts of game theory and teach students to solve strategic games between two and more agents in non-cooperative scenario. • To analyze and solve both simultaneous-moves and sequential-moves games and will be familiarized with different solution concepts like minimax, Nash equilibrium, dominant strategy equilibrium, Subgame perfect equilibrium, etc							
Outcomes	On successful completion of the course, the students will be able to: • Have knowledge to mixed strategy equilibria, and to repeated games • Apply game theory in voting and bargaining • Recognize and understand game theory in the world around them • Apply the concepts, ideas that constitute these various game types and their solutions, and apply them to the problems at hand							
UNIT – I	**Introduction on Game theory**							**Hours: 09**
Games and Solutions – Theory of competitive Equilibrium – Steady state and Deductive interpretation- Nash Equilibrium –Existence and properties of Nash Equilibrium- Interrelated strict dominance and Rationalizability- Correlated Equilibrium								
UNIT – II	**Dynamic games of complete information**							**Hours: 09**
Extensive form games –Commitment and perfection in multistage games – Strategies and Equilibria in extensive form – Backward induction and Subgame perfection – Critics of backward induction and Subgame perfection- Application of Multistage games with observed Actions – Open and closed Loop Horizons – Repeated Games.								
UNIT – III	**Static games of Incomplete information**							**Hours: 09**
Incomplete Information- The notations of Type and Strategy – Bayseian Equilibrium – Deletion of Strictlty dominated strategies – Distributed Approach – Bayseian game and mechanism design: Revelation Principle – Single Agent – feasible allocation –Optimization								
UNIT – IV	**Dynamic games of incomplete information**							**Hours: 09**
Dynamic games of incomplete information: Perfect Bayseian equilibrium in multistage games – Extensive form refinements – Strategic form refinements – Reputation effects – signaling gaming – Robust prediction under payoff stability- Coalitional games.								
UNIT – V	**Application of game theory in Networking**							**Hours: 09**
Routing game basics – Cooperation enforcement and learning using repeated games – Hierarchal routing using network function game – Auction theory – Basics of cooperation transmission – Non cooperative game for relay selection – Auction theory for resource allocation - Cooperative games for transmission								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			
Text Books:								
1. Drew Fudenberg and Jean Triole, Game theory, Princeton University press, 2013.								
Reference Books:								
1. Martin J. Osborne and Ariel Rubinstein, A Course in game theory,1994 2. Zhu Han, Dusit Niyato and Walid Sasd, Game Theory in Wireless and Communication networks, 2012.								
Websites:								
1. https://www.coursera.org/course/gametheory 2. http://gametheory101.com/								

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE79	Database Security and Auditing	3	1	-	4	40	60	100

Prerequisite	-
Objectives	• To understand the need to secure and audit the Databases • To get the knowledge of different methods of securing Databases • To know how to do auditing with Database
Outcomes	On successful completion of the course, the students will be able to: • Develop the applications with secured Databases • Auditing the Databases

UNIT – I	**Security Architecture and Operating System Security Fundamentals**	**Hours: 09**

Introduction – Security – Information Systems – Database Management Systems – Information Security – Information Security Architecture – Database Security – Asset Types and Their Values – Security Methods. Operating System Security Fundamentals: Introduction – Operating System Overview – Operating System Security Environment – The components of an Operating System Security Environment – Authentication Method – User Administration – Password Policies – Vulnerabilities of Operating Systems – E-mail Security.

UNIT – II	**Administration of Users, Profiles, Password Policies, Privileges and Roles**	**Hours: 09**

Introduction – Documentation of User Administration – Operating System Authentication – Creating Users – Creating a SQL Server User – Removing Users – Modifying Users – Default Users – Remote Users – Database Links – Linked Servers – Remote Servers – Practices for Administrators and Managers. Profiles, Password Policies, Privileges and Roles : Introduction – Defining and Using Profiles – Designing and Implementing Password Policies – Granting and Revoking User Privileges – Creating, Assigning and Revoking User Roles.

UNIT – III	**Database Application Security Models and Security Within the General Security Landscape**	**Hours: 09**

Introduction – Types of Users – Security Models – Application Types – Application Security Models – Data Encryption. Security Within the General Security Landscape: Defense-in-Depth – Security Software Landscape – Perimeter Security, Firewall, Intrusion Detections and Intrusion Preventions – Securing the Core – Application Security – Public Key Infrastructure (PKI) – Vulnerability Management – Patch Management and Incident Management.

UNIT – IV	**Auditing Categories and Auditing Database Activity**	**Hours: 09**

Auditing Categories. Auditing Database Activity: Introduction – Using Oracle Database Activity – Creating DLL Triggers with Oracle – Auditing Database Activity with Oracle – Auditing Server Activity with Microsoft SQL Server 2000 – Implementing SQL Profiler – Security Auditing with SQL Server.

UNIT – V	**Security and Auditing Case Studies**	**Hours: 09**

Introduction – Developing an Online Database – Taking Care of Payroll – Tracking Town Contracts – Tracking Database Changes – Developing a Secure Authorization Repository.

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. Hassan A. Afyouni, Database Security and Auditing, Thomson Course Technology, 2009.
2. Ron Ben Natan, Implementing Database Security and Auditing, Elsevier Digital Press, 2005.

Reference Books:

1. Alfred Basta, Melissa Zgoca, Dana Bullaboy, Thomas L.Whitlocksr, Database Security, 2011.
2. Mario Piattini, Auditing Information System,Idea Group Publishing, 2000.

Websites: -

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE80	Intelligent Systems	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To provide the ideas of fuzzy sets, fuzzy logic and use of heuristics based on human experience • To understand different Knowledge representation schemes for typical AI problems • To introduce soft computing techniques and intelligent control							
Outcomes	On successful completion of the course, students will be able to: • Construct intelligent and use them for inferencing solution to real world problems • Design fuzzy logic and implement the fuzzy sets and operations in fuzzy systems • Analyze uses of intelligent control problems • Design applications related to optimization techniques							
UNIT – I	**Artificial Intelligence**							**Hours: 09**
Introduction ,Intelligent Agents, Problem-solving: Solving Problems by Searching , Informed Search and Exploration, Constraint Satisfaction Problems, Adversarial Search								
UNIT – II	**Knowledge and reasoning**							**Hours: 09**
Logical Agents, First-Order Logic, Inference in First-Order Logic, Knowledge Representation ,Planning: Planning and Acting in the Real World , Uncertain knowledge and reasoning								
UNIT – III	**Intelligent Modeling**							**Hours: 09**
Introduction of soft computing techniques, Fuzzy logic systems; fuzzy sets, inferencing, fuzzy relation models, Tagaki-Sugeno models, Neural networks, Neuro-fuzzy systems, Modeling of dynamical systems								
UNIT – IV	**Optimization**							**Hours: 09**
Model building, Fuzzy inverse model development, Model-based forward optimization, Application of model-based optimization to numerical examples, Application of model-based optimization scheme to practical problems								
UNIT – V	**Intelligent Control**							**Hours: 09**
Neural control, Rule-based fuzzy control, Model-based fuzzy control, Stability analysis, Fuzzy control for SISO nonlinear systems, Fuzzy control application to practical problems								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			
Text Books:								
1. Stuart Russel, Peter Norvig, AI – A Modern Approach, 2nd edition, Pearson Education 2007. 2. Yung C. Shin and Chengying Xu, Intelligent Systems - Modeling, Optimization and Control, CRC Press, Taylor & Francis Group, 1st edition, 2009.								
Reference Books:								
1. Kevin Night, Elaine Rich, Nair B., Artificial Intelligence (SIE), McGraw Hill, 3rd edition ,2008. 2. Dan W. Patterson, Introduction to AI and ES, Pearson Education, 2nd edition 2007. 3. Patrick Henry Winston, Artificial Intelligence, 3rd edition, Pearson Edition, 1992.								
Websites:								
1. http://www.cs.utexas.edu/users/novak/cs381kcontents.html 2. www.ics.uci.edu/~smyth/courses/cs271/topic0_introduction.ppt 3. www.cs.utexas.edu/users/novak/cs381kcontents.html								

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE81	Cloud and Big Data Security	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To introduce the basics of Cloud and Big data • To explore the fundamental concepts of big data analytics • To learn to analyze the big data using intelligent techniques							
Outcomes	On successful completion of the course, the students will be able to: • Understand the basics concepts of cloud computing and its related techniques. • Analyze the big data analytic techniques for useful business applications. • Design efficient algorithms for mining the data from large volumes. • Analyze the HADOOP and Map Reduce technologies associated with big data analytics							
UNIT – I	**Security Concepts**							**Hours: 09**
Confidentiality – privacy – integrity – authentication – non-repudiation – availability – access control – defence in depth – least privilege – application in cloud – Security importance in PaaS, IaaS and SaaS – Cryptographic Systems- Symmetric cryptography – stream ciphers – block ciphers – modes of operation – public-key cryptography – hashing – digital signatures – public-key infrastructures – key management – X.509 certificates – OpenSSL.								
UNIT – II	**Multi-Tenancy Issues**							**Hours: 09**
Isolation of users/VMs – Virtualization System Security Issues- ESX and ESXi Security – ESX file system security – storage considerations – backup and recovery – Virtualization System Vulnerabilities- Management console vulnerabilities – management server vulnerabilities – administrative VM vulnerabilities – guest VM vulnerabilities – hypervisor vulnerabilities – hypervisor escape vulnerabilities –configuration issues – malware.								
UNIT – III	**Introduction to BigData**							**Hours: 09**
Introduction to BigData Platform – Challenges of Conventional Systems - Intelligent data analysis – Nature of Data - Analytic Processes and Tools - Analysis vs Reporting - Modern Data Analytic Tools - Statistical Concepts: Sampling Distributions - Re-Sampling - Statistical Inference - Prediction Error.								
UNIT – IV	**HADOOP**							**Hours: 09**
History of Hadoop- The Hadoop Distributed File System – Components of Hadoop – Analyzing the Data with Hadoop- Scaling Out- Hadoop Streaming- Design of HDFS-Java interfaces to HDFS Basics- Developing a Map Reduce Application-How Map Reduce Works-Anatomy of a Map Reduce Job run-Failures-Job Scheduling-Shuffle and Sort – Task execution - Map Reduce Types and Formats- Map Reduce Features.								
UNIT – V	**HADOOP Environment**							**Hours: 09**
Setting up a Hadoop Cluster - Cluster specification - Cluster Setup and Installation – Hadoop Configuration-Security in Hadoop - Administering Hadoop – HDFS – Monitoring Maintenance-Hadoop benchmarks- Hadoop in the cloud.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			

Text Books:

1. Guy Bunker and Darren Thomson, Delivering Utility Computing, John Wiley & Sons Ltd, 2012.
2. Tom White,Hadoop: The Definitive Guide, Third Edition, O'reilly Media, 2012.

Reference Books:

1. Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media; 1 edition, 2009.
2. Ronald L. Krutz, Russell Dean Vines, Cloud Security, 2010.
3. John Rittinghouse, James Ransome, Cloud Computing, CRC Press, 1 edition, 2009.
4. J.R. ("Vic") Winkler, Securing the Cloud, Syngress, 2011.
5. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing ,2009
6. Chris Eaton, Dirk DeRoos, Tom Deutsch, George Lapis, Paul Zikopoulos, Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data, McGrawHill Publishing, 2012.

Websites: -

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE82	Data Hiding and Biometric Security	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To understand existing security methods • To understand how biometric systems are implemented • To understand the intricacies involved							
Outcomes	On successful completion of the course, the students will be able to: • design new/existing security methods • compare and appreciate new/existing biometric systems, hiding techniques							
UNIT – I	**Introduction to Information hiding**							**Hours: 09**
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 – Using cover models – Active and malicious attackers – Information hiding in written text – Examples of invisible communications.								
UNIT – II	**Steganography and Steganalysis**							**Hours: 09**
Survey of steganographic techniques – Substitution system and bit plane tools – Transform domain techniques– Statistical Steganography – Distortion and code generation techniques – Steganalysis – Detecting hidden information – Extracting hidden information - Disabling hidden information.								
UNIT – III	**Watermarking techniques**							**Hours: 09**
History – Basic Principles – Applications – Algorithmic design issues – Evaluation and benchmarking of watermarking systems – Survey of current watermarking techniques – Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bets - Merging the watermark and the cover – Optimization of the watermark receiver – Extension of Watermarking techniques from still images to video – Robustness for copyright making systems.								
UNIT – IV	**Biometric Security**							**Hours: 09**
Introduction to Biometrics – 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 in biometric systems.								
UNIT – V	**Physiological and Behavioral Technologies**							**Hours: 09**
Classification of Physiological and Behavioral Biometric Technologies – (Technical description – characteristics – Competing technologies - strengths – weaknesses – deployment) for Fingerprints – Facial scan – Iris scan – Retina vascular pattern – Palm scan –– DNA biometrics - Handprint Biometrics – Signature – handwriting technology - keyboard / keystroke dynamics – Voice metrics.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			

Text Books:

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, Information hiding techniques for Steganography and Digital Watermarking, ARTECH House Publishers, January 2004.
2. Jessica Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University press, 2010.

Reference Books:

1. Ingemar Cox, Matthew Miller,Jeffrey Bloom,Jessica Fridrich and Ton Kalker, Digital Watermarking And Steganography, Morgan Kaufmann Publishers, Nov 2007.
2. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Biometrics -Identity verification in a network, Wiley Eastern, 2002.
3. John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Eastern Publications, 2005.

Websites: -

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE83	Intellectual Property Rights	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To understand the difference between intellectual and conventional property • To learn how to value intangible assets, taking into account their commercial potential and legal status. • To explore the legal and business issues surrounding marketing of new products related to technology							
Outcomes	On successful completion of the course, the students will be able to: • Apply for patents in India and Abroad • Develop a business plan that advances the value of their intellectual property portfolio • Develop a strategy of marketing their intellectual property and understand some negotiation basics. • Explain some of the limits of their intellectual property rights and comprehend some basic legal pitfalls							

UNIT – I	**Hours: 09**

Introduction: Intellectual Property Rights and their usefulness for Engineers - Intellectual Property -different forms- Usefulness of IPRs- new career opportunities/consultancy opportunities - Intellectual Property vs. Physical or conventional Property-concept of property-Intellectual Property vs Conventional Property- similarities and differences-Importance of Intellectual Property - Patents, Copyright, Trademarks, Industrial Designs-Registration of Plant Varieties, Registration of Semiconductor Integrated Circuit Layout Design)-Registration of Geographical Indications and Trade Secrets.

Patents: Patents-uses- preventing duplication of work- identification research- preventing exploitation-promoting revenue generation- access to rare technical information-preventing infringements and helping to avoid litigation-stimulating creativity. Patents- Significance for stakeholders - Patents- to file or not to file-Practical aspects of filing a Patent in India - Determination of patentability of inventions – the TRISHUL test of novelty- inventive step and industrial application-patent search map and performing a prior art search; literature and non-literature-Forms, Fee and time lines-Practical aspects of filing a Patent in Abroad – Various routes for international patenting-direct filing abroad-filing vide regional office route and filing under the Patent Cooperation Treaty (PCT)- New developments in Patent Law- Patent Law Treaty -Substantive Patent Law Treaty -TRIPS-Enforcement of Patent Rights at National and Global level-Case studies.

UNIT – II	**Hours: 09**

Copy right: Copyright and its uses - Subject matter of copyright- Artistic, Literary, musical and cinematographic works-Definition-History-International Copyright Treaties- Internet treaties-Amendments in Indian Copyright Law and their significance-Protection of Software and digital innovations-Rights afforded by copyright law; Rights of Distribution and Communication to the Public-Exceptions in copyright- Plagiarism vs Copyright Infringement- Dr.Mashelkar Committee Report and Kaavya Vishwanathan Case;-Case Studies-Practical aspects of Copyright Registration and Transfer - Procedural and practical aspects related to registration of copyright – Forms, Fee, Timeline- Ownership issues, transfer and duration. Enforcement at National and Global level-Remedies available under the Copyright Act.-Forms for copy rights

Design registration: Industrial Design Registration and its usefulness in Engineering – Importance of industrial design registration for engineers-Indian Law related to Registration of Industrial Designs-Essential Requirements for Registration of a Design in India- Limitations-American Law- International Agreements- The Hague System; Conflicts related to Registration of Design, Copyright or Trademark; Legal rights and advantages of Industrial Design Registration- The Tupperware Case-Practical aspects of Industrial Design Registration in India and Abroad - Practical aspects of Industrial Design Registration in India-Forms, Fee, Timelines. Procedural aspects. Enforcement at National and Global level. Guide and forms for registering the design

UNIT – III	**Hours: 09**

Trade Secrets and trademarks: Trade Secrets- Importance – Trade Secrets- Importance Elements of Trade Secrets-

what is a trade secret and what is not- Laws relating to protection of Trade Secrets-Spring Board Doctrine-Case Studies-agreement or NCA and Trade Secret Bonds or TSBs-Practical aspects of maintaining trade secrets-Maintaining Lab Notebooks as Trade Secret Documents. -Format of NDA/CDA and a Trade Secret Bond Trademarks- Importance in Engineering –

Trademarks- Importance in Engineering industry-National Trademark Filing- Practical aspects-forms, fee, timelines, procedural aspects. International Trademark Filing-Madrid System-Agreement and Madrid Protocol; Maintenance and Transfer; Dilution of ownership-likelihood of confusion; Case Study – Trademark related forms.

UNIT – IV		**Hours: 09**

Agreements and legislation: International Agreements and Organizations related to Intellectual Property –
Important IPR related treaties and international agreements and their implications for Engineers-Conventional and Agreements -GATT, TRIPS and Establishment of WTO, GATT vs WTO. Amendments in the Indian Patents Act after TRIPS; Salient features of the Patents (Amendment) Act, 2005 of India- Indian IPR legislations- difference between statutes and rules. WIPO–Objectives and Structure-Legislations and Policy - Supermacy of societal interests as the cornerstone for legislations, policy and legal judgments. Societal impact of IPRs. Handling IPR Related Conflicts. IPR Conflict Resolution - Role of Values and Ethics-IPR Conflict Resolution - Role of Alternative Dispute Resolution or ADR mechanisms-Arbitration in Intellectual Property Disputes-Indian Position Vs WTO and Strategies- Commitments to WTO. Patent Ordinance and the Bill – Protection and Utilization of Public Funded Intellectual Property Bill, 2008- Laws on Public Funded IP in other countries- National IP Policies (NIPP) and role of WIPO; NIPP and India; NIPP of Malaysia; Key elements of an Institutional IPR policy.- Model IPR Policy Document.

UNIT – V		**Hours: 09**

Digital Products and Law: Digital Innovations and Developments as Knowledge Assets – Significance of IP in Content for the Internet and Tech Sector- Symbols and trademarks as Business Assets in the Information Age; Internet and the WWW; Applications of computer technology - advantages/disadvantages-Cyber Technology- e-commerce and e-governance; Electronic records and digital signatures; The Employment Relationship in the Internet and Tech Sector - role of CDAs and contracts-Trolls, landmines and other metaphors-Cyber etiquette. IP Laws, Cyber laws and Digital Content Protection - IP laws and Cyberlaws- Linkages; IPR issues vs Regulatory issues-E-commerce and Cyber Laws-Cyber Crime and Legislation- Need, Objective and Scope; UNCITRAL model law –Objectives- its relevance to India; Objects of the IT Act, 2000; Information Technology and Information Security-Case studies.

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

Text Books:

1. Kompal Bansal and Parikshit Bansal, Fundamentals of Intellectual Property for Engineers, BS Publications/BSP Books, First Edition, 2013.

Reference Books:

1. Deborah E.Bouchoux, Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets, Third Edition, Cengage Learning India Pvt Ltd, New Delhi, 2012.
2. Prabuddha Ganguli, Intellectual Property Rights: Unleashing the Knowledge Economy, First Edition, McGraw Hill Education (India) Private Limited, 2008.

Websites:

1. http://www.ipindia.nic.in/
2. www.uspto.gov/

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE84	Information Security Policies	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To Introduce and understand the Information Security Policies with aspects of security • To understand how to write the Security Policies • To understand how to establish Viruses Protection in an organization							
Outcomes	On successful completion of the course, the students will be able to: • Maintain the Policies in an organization. • Have skill to write the Security Policies for an organization. • Asses the Viruses and suggest Protection mechanism for organization							

UNIT – I	**Hours: 09**
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 .	
UNIT – II	**Hours: 09**
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.	
UNIT – III	**Hours: 09**
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.	
UNIT – IV	**Hours: 09**
Establishing Type of Viruses Protection - Rules for handling Third Party Software - User Involvement with Viruses - Legal Issues- Managing Encryption and Encrypted data - Key Generation considerations and Management - Software Development policies -Processes - Testing and Documentation- Revision control and Configuration management - Third Party Development - Intellectual Property Issues.	
UNIT – V	**Hours: 09**
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.	

Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**	**Total Hours: 60**

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. Detmar W. Straub, Seymour E. Goodman and Richard Baskerville, Information Security: Policy, Processes, and Practices, M.E. Sharpe, 2008.
2. Thomas R. Peltier, Information Security Policies and Procedures: A Practitioner's Reference, Second Edition, CRC Press, 2004.

Websites:

1. http://www.sans.org/security-resources/policies/

2. http://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy
3. http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/home.aspx
4. www.csoonline.com/article/495017

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE85	Secure Coding	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To introduce basic concepts, policies, and mechanisms in designing and coding secure software systems • To examine the concepts that apply to programming "in the large" as well as specifics on things like buffer overflow • To deal with C and C++ code for secure software system development							
Outcomes	On successful completion of the course, the students will be able to: • Analyze the essential techniques for secure coding which are used in current practice • Apply and analyze techniques for secure coding used in current practice • Evaluate the use of type-safe languages, certifying compilers, proof-carrying code, run-time monitoring, and stack inspection, • Analyze legal and ethical issues underlying secure coding of software systems							
UNIT – I								**Hours: 09**
Introduction: Software security- Security concepts-Security policy-security flaws-vulnerabilities-exploits-mitigation-C and C++-Development Platforms-operating systems-compilers. Strings: Common String Manipulation Errors-String Vulnerabilities-Process Memory Organization-Stack Smashing- Code Injection- Arc Injection-Mitigation Strategies.								
UNIT – II								**Hours: 09**
Pointer Subterfuge: Data Locations-Function Pointers-Data Pointers-Modifying the Instruction Pointer-Global Offset Table-The .dtors Section-Virtual Pointers-atexit(), on-exit(), longjmp()-Exception Handling-Mitigation Strategies. Dynamic Memory Management: Common Dynamic Memory Management Errors-Doug Lea's Memory Allocator-RtlHeap Mitigation Strategies.								
UNIT – III								**Hours: 09**
Integer Security: Integers-Integer Conversions-Integer Error Conditions-Integer Operations-Vulnerabilities-Nonexceptional Integer Logic Errors-Mitigation Strategies. Formatted Output: Variadic Functions-Formatted Output Functions-Exploiting Formatted Output Functions-Stack Randomization-Mitigation Strategies.								
UNIT – IV								**Hours: 09**
Concurrency-Time of Check, Time of Use-Files as Locks and File Locking-File System Exploits-Mitigation Strategies. Recommended Practices: Secure Software Development Principles-System Quality Requirements Engineering-Threat Modeling-Use/Misuse Cases-Architecture and Design -Off-the-Shelf Software-Compiler Checks-Input Validation-Data Sanitization-Static Analysis-Quality Assurance-Memory Permissions-Defense in Depth-TSP-Secure.								
UNIT – V								**Hours: 09**
Proactive Security Development Process: Installing a Security Culture-The Defender's Dilemma and the Attacker's Advantage-Role of Education-Integrating Security into the Development Process-Security Principles. Language Independent Security Issues: Appropriate Access Control-Running with Least Privilege-Cryptographic Foibles Protecting Data-Input checking and canonicalization-Database input.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			

Text Books:

1. Robert C. Seacord, Secure Coding in C and C++. SEI Series (CERT Book), Addison-Wesley, 2006.

Reference Books:

1. Mark Dowd, John McDonald, and JustingSchuh, The ART of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, Addison Wesley, 2007.
2. Michael Howard and David LeBlanc, Writing Secure Code, Microsoft Press, 2003.
3. Tom Gallagher, Bryan Jeffries, Lawrence Landauer, Hunting Security Bugs, Microsoft Press, 2006.

Websites: -

Department : Computer Science and Engineering		**Programme :** M.Tech. (Information Security)						
Semester :		**Category :** TY						
Subject Code	**Subject**	**Hours / Week**			**Credit**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CA**	**SE**	**TM**
CSE86	Web Application Security	3	1	-	4	40	60	100
Prerequisite	-							
Objectives	• To Identify various components of an web application from the security view point • To have Knowledge of web application testing methodologies							
Outcomes	On successful completion of the course, the students will be able to: • design secured web application • build web testing tools							
UNIT – I								**Hours: 09**
Web Security Fundamentals- Input Validation, Attack surface reduction, principles-Authentication- Securing Password-Best Practices-Authorization-Access control - Session Management - securing web application								
UNIT – II								**Hours: 09**
Browser security principles- cross-site scripting - cross-site request forgery- Database security principles - SQL injection- setting database permission-stored procedure security- Insecure Direct object references.								
UNIT – III								**Hours: 09**
File security principles- source code secret- forceful browsing- directory traversal- secure development methodologies- application security - industry standard secure development methodologies and maturity models - SDL - CLASP- SAMM - BSIMM.								
UNIT – IV								**Hours: 09**
Web Applications Testing Fundamentals, Basic Observation HTML Page Source, Web-Oriented DataEncoding, Tampering with Input, Automated Bulk Scanning, Automating Specific Tasks with cURL.								
UNIT – V								**Hours: 09**
Automating with LibWWWPerl, Seeking Design Flaws, Attacking AJAX, Manipulating Sessions, Multifaceted Tests.								
Total contact Hours: 45	**Total Tutorials: 15**	**Total Practical Classes: -**			**Total Hours: 60**			
Text Books:								
1. Bryan Sullivan, Vincent Liu Web Application Security- A Beginner's Guide, McGrawHill Companies, 2012. 2. Paco Hope, Ben Walther, Web Security Testing Cookbook, O'Reilly Media, 2008.								
Reference Books:								
1. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press, 2014.								
Websites:								
1. https://www.owasp.org/								