**M. TECH DEGREE (FULL TIME) PROGRAMME**

**in**

# COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

## SCHEME OF EXAMINATION & SYLLABUS

**SCHOOL OF ENGINEERING**
**COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY**
**COCHIN– 682 022**

**NOVEMBER – 2025**

**M.TECH Degree (Full Time) programme in COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)**

**Number of seats: 18**

## Eligibility Requirement for Admission

**Candidates for admission to M-Tech degree (full time) programme in Computer Science and Engineering (Cyber Security) shall be required to possess the following qualifications.**

a) **Shall have passed B.Tech or equivalent degree in Computer Science and Engineering or Electronics and communication or Information Technology branch or MCA , with a minimum of 60% marks or CGPA 6.5 in 10-point scale from any recognised University in Kerala or any other University/Institution accepted by this University as equivalent there to.**
b) **A Valid GATE score.**
c) **In the absence of sufficient number of candidates with GATE score, candidates without GATE score shall also be considered subject to passing an admission test conducted by the University.**

**Credit patterns are as per the existing regulation for the full time M.Tech Programmes offered by the School of Engineering.**

**The Regulation of this programme will be the regulation applicable to the M.Tech Degree (Full Time) courses offered by School of Engineering, Cochin University of Science and Technology from 2020 admission onwards.**

**M. Tech Degree (Full Time) Programme in Computer Science and Engineering**
**(CYBER SECURITY)**

| SEMESTER I | | | | | | |
|---|---|---|---|---|---|---|
| **Sl No.** | **Course Code** | **Course Name** | **Hours/Week** | | | **Credits** |
| | | | **L** | **T** | **P** | |
| 1 | 25-506-0101 | Mathematical Foundation for Cyber Security | 3 | 1 | 0 | 4 |
| 2 | 25-506-0102 | Cryptography and Network Security | 3 | 1 | 0 | 4 |
| 3 | 25-506-0103 | Biometric System and Image Processing | 3 | 1 | 0 | 4 |
| 4 | 25-506-01** | Elective I | 3 | 1 | 0 | 3 |
| 5 | 25-506-01** | Elective II | 3 | 1 | 0 | 3 |
| 6 | 25-506-0112 | Research Methodology and Intellectual Property Rights | 2 | 1 | 0 | 2 |
| 7 | 25-506-0113 | Network Programming and Cryptography Lab | 0 | 0 | 3 | 1 |
| 8 | 25-506-0114 | Seminar I | 0 | 0 | 3 | 1 |
| **Total** | | | **17** | **6** | **6** | **22** |

| SEMESTER II | | | | | | |
|---|---|---|---|---|---|---|
| **Sl No.** | **Course Code** | **Course Name** | **Hours/Week** | | | **Credits** |
| | | | L | T | P | |
| 1 | 25-506-0201 | Software Vulnerability Analysis | 3 | 1 | 0 | 4 |
| 2 | 25-506-0202 | Ethical Hacking and Cyber Forensics | 3 | 1 | 0 | 4 |
| 3 | 25-506-0203 | Cyber Crime Investigation and Digital Forensic | 3 | 1 | 0 | 4 |
| 4 | 25-506-02** | Elective III | 3 | 1 | 0 | 3 |
| 5 | 25-506-02** | Elective IV | 3 | 1 | 0 | 3 |
| 6 | 25-506-0212 | Ethical Hacking Digital Forensic Lab | 0 | 0 | 3 | 1 |
| 7 | 25-506-0213 | Seminar II | 0 | 0 | 3 | 1 |
| **Total** | | | **15** | **5** | **6** | **20** |

| SEMESTER III | | | | | | |
|---|---|---|---|---|---|---|
| **Sl No.** | **Course Code** | **Course Name** | **Hours/Week** | | | **Credits** |
| | | | L | T | P | |
| 1 | 25-506-0301 | Internship / MOOC Course | 0 | 0 | 6 | 2 |
| 2 | 25-506-0302 | Dissertation Phase - I | 0 | 0 | 24 | 13 |
| **Total** | | | **0** | **0** | **30** | **15** |

| SEMESTER IV | | | | | | |
|---|---|---|---|---|---|---|
| **Sl No.** | **Course Code** | **Course Name** | **Hours/Week** | | | **Credits** |
| | | | L | T | P | |
| 1 | 25-506-0401 | Dissertation Phase - II | 0 | 0 | 30 | 15 |
| Total | | | **0** | **0** | **30** | **15** |

Total credits for the programme = 72

***Electives must be selected from the following list for the corresponding semester*

**ELECTIVES I & II (Semester I)**

| | |
|---|---|
| 25-506-0104 | Applied Cryptography |
| 25-506-0105 | Advances in data science |
| 25-506-0106 | Web Security |
| 25-506-0107 | IT Security metrics |
| 25-506-0108 | Information Storage Management |
| 25-506-0109 | Digital Watermarking and Steganography |
| 25-506-0110 | Database Security |
| 25-506-0111 | Embedded Systems Security |

**ELECTIVES III & IV (Semester II)**

| | |
|---|---|
| 25-506-0204 | Intrusion Detection and Prevision System |
| 25-506-0205 | Operating Systems and Security |
| 25-506-0206 | Information Theory and Coding |
| 25-506-0207 | Cyber Laws and Security Policies |
| 25-506-0208 | Cloud Computing |
| 25-506-0209 | Deep Learning |
| 25-506-0210 | Security and Privacy in Internet of Things |
| 25-506-0211 | Block Chain and Information Security |

Students must complete one MOOC Course, which is compulsory under the University's MOOC regulations. It should be related to any one course from the list marked as Elective III and IV from second semester.

**Syllabus For**
**M. Tech Degree (Full Time) Programme in Computer Science and Engineering**
**(CYBER SECURITY)**

## 25-506-0101 Mathematical Foundation for Cyber Security

COURSE OUTCOMES

After completion of course, students will be able to:

1. Able to apply Number theory in data security.
2. Understand the ideas of group, ring and an integral domain and be aware of examples of these structures in mathematics.
3. Understand probability and statical methods.
4. Understand coding theory and its use in data security.

**Module-1**

Theory of Numbers: Introduction - Divisibility - Greatest common divisor - Prime numbers – Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem -Euler totient function - Euler's theorem. Congruences: Definition - Basic properties of congruences -Residue classes - Chinese remainder theorem

**Module-2**

Probability and Statistics: introduction to probability concepts, random variables, probability distributions (continuous and discrete), Bayesian approach to distributions, mean and variance of a distribution, joint probability distributions, theory of estimation,Bayesian methods of estimation. Random Processes: general concepts, power spectrum, discrete-time processes, random walks and other applications, Markov chains, transition probabilities.

**Module-3**

Algebraic Structures: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields .
Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.

**Module-4**

Coding Theory: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes. Pseudorandom Number Generation: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator.

**References:**


1. David Burton, "Elementary Number Theory",7th edition, McGraw Hill Education,2017 .ISBN : 978-1259025761
2. G.H.Hardy, E.M.Wright , "An Introduction to Theory of Numbers",6th edition, Oxford University Press,2008. ISBN : 978-0199219865
3. Douglas C. Montgomery and George C. Runger, "Applied Statistics and Probability for Engineers" , Wiley, 6th edition , 2016. ISBN : 978-8126562947
4. Howard Anton. "Elementary Linear Algebra:Applications Version " , 11th edition, John Wiley & Sons Inc, 2013. ISBN : 978-1118434413
5. Douglas R. Stinson , "Cryptography: Theory and Practice" ,standard edition, CRC Press, 2018. ISBN : 978-1138197015
6. Kenneth H Rosen . "Discrete Mathematics and Its Applications with Combinatorics and Graph Theory" ,7th edition, McGraw Hill Education, 2017. ISBN : 978-0070681880

## 25-506-0102 Cryptography and Network Security

COURSE OUTCOMES

After completion of course, students will be able to:

1. Analyse vulnerabilities in any computing system and design and propose a security solution.
2. Identify security issues in the network and provide data security over the network.
3. Impart knowledge on Encryption techniques, Digital signatures and message authentication code.
4. Understand various protocols for network security used to protect against threats in the networks.
5. Examine the issues and structure of Authentication Service and Electronic Mail Security.

**Module-1**

Attack on computers and computer security – Principles of security -Types of attacks – Cryptography - Concepts and Techniques – Symmetric key cryptography - Algorithms.

**Module-2**

Asymmetric key algorithms – Digital Signatures – Message Digests – Message Authentication Code – Digital Certificates and Public key infrastructure.

**Module-3**

Internet security Protocols – SSL- TLS – Secure Electronic Transaction – 3D secure protocols – Electronic money – E-mail security – WAP security.

**Module-4**

User Authentication – Authentication Tokens – Certificate based Authentication – Kerberos – Firewalls and Virtual private networks.

**References:**


1. William Stallings, “Cryptography and Network Security Principles and Practice”, 7th Edition, Pearson, 2017.
2. Behrouz A Forouzan, Debdeep Mukhopadhyay, “ Cryptography and Network Security”, 3rd Edition, McGraw Hill, 2015.
3. Atul Kahate, “Cryptography and Network Security”, 3rd Edition, McGraw Hill, 2013.

## 25-506-0103 Biometric System and Image Processing

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand the need for biometric technologies versus traditional ones.
2. Understand the strengths and weaknesses of behavioural biometric techniques.
3. Gain knowledge about image processing and enhancement.
4. Understand the architecture of recent technologies used in biometric authentication.

**Module-1**

Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques -Characteristics of a good biometric system – Benefits of biometrics – Key biometric processes: verification,identification and biometric matching – Performance measures in biometric systems, FAR, FRR, FTE rate, EER and ATV rate, Applications of Biometric Systems, Security and Privacy Issues.

Physiological Biometrics : Leading technologies : Finger-scan – Facial-scan – Iris-scan – Voice-scan – components, working principles, competing technologies, strengths and weaknesses – Other physiological biometrics : Hand-scan, Retina-scan –components, working principles, competing technologies, strengths and weaknesses – Automated fingerprint identification systems.

**Module-2**

Behavioural Biometric techniques : Signature-scan – Keystroke scan – components, working principles, strengths and weaknesses.

Privacy and Standards in Biometrics: Assessing the Privacy Risks of Biometrics – Designing Privacy-Sympathetic Biometric Systems – Need for standards – different biometric standards.

**Module-3**

Image Processing basics : Digital Image representation - Fundamental steps in Image Processing Image Enhancement: The Spatial Domain Methods, The Frequency Domain Methods - Image Segmentation: Pixel Classification by Thresholding, Histogram Techniques, Smoothing and Thresholding - Gradient Based Segmentation: Gradient Image, Boundary Tracking, Laplacian Edge Detection.

**Module-4**

Fingerprint and Iris Biometrics: Fingerprint Patterns, Fingerprint Features, Fingerprint Image, width between two ridges - Fingerprint Image Processing - Minutiae Determination - Fingerprint Matching: Fingerprint Classification, Matching policies. Iris System Architecture, Definitions and Notations - Iris Recognition: Iris location, Doubly Dimensionless Projection, Iris code, Comparison - Coordinate System: Head Tilting Problem, Basic Eye Model, Searching Algorithm, Texture Energy Feature.

**References:**


1. Anil K Jain, Arun A Ross, Karthik Nandakumar, “Introduction to Biometrics”, Springer, 2011. ISBN : 978-0387773254
2. Arun A. Ross Anil Jain, Patrick Flynn , “Handbook of Biometrics” , Springer, 2018 .ISBN : 978-1493977284
3. Marina L. Gavrilova, Maruf Monwar , “ Multimodal Biometrics and Intelligent Image Processing for Security Systems”, IGI Global,2013. ISBN13: 9781466636460
4. Rafael Gonzalez , Richard Woods , “Digital Image Processing” , 4th edition , Pearson, 2017. ISBN : 978-0133356724

## 25-506-0104 Applied Cryptography

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand various encryption standards and protocols used in cryptography.
2. Apply the knowledge in discriminating ciphers.
3. Design various hash algorithms.
4. Visualise different types of signature schemes.

**Module-1**

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

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.

**Module-2**

Cryptographic techniques-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 - PublicKey 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.

**Module-3**

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) - OneWay Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes.

**Module-4**

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.

**References:**


1. Bruce Schneier , "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C" ,2nd edition ,John Wiley & Sons, Inc. 1995, ISBN : 978-0471117094
2. Douglas R. Stinson, "Cryptography: Theory and Practice" , 3rd edition ,CRC press ,2005. ISBN : 978-1584885085
3. Wenbo Mao, "Modern Cryptography Theory and Practice", Prentice Hall, 2003. ISBN : 978-0132887410

**25-506-0105 Advances in data science**

COURSE OUTCOMES

After completion of course, students will be able to:

1. Analyse various types of data, and its preprocessing.
2. Illustrate and analyse various applications of data mining.
3. Analyse and compare various classification models in data mining.
4. Understand developments in big data technologies.
5. Familiarize the concepts of machine learning using R/Python.
6. Analyse and make use of deep learning using R/Python.
7. Familiarize concepts of social network analysis and sentiment analysis

Module-1

Data Mining-Purpose-Various phases of data mining - supervised vs. unsupervised - learning - Data Warehouses - OLAP - Multidimensional databases - Data Pre-processing-Case studies in data pre-processing-Dimensionality reduction techniques-Chisquare, PCA, LDA. Different applications of data mining..Introduction to machine learning concepts of pattern recognition,.

**Module-2**

Association Rules mining-Apriori algorithm-Examples-Improvements for apriori algorithm-Classification concepts, mathematical notions and case studies-Decision trees, Neural networks, Naïve Bayes classifier, KNN, Support vector machines, Maximum likelihood classifier

**Module-3**

Cluster Analysis-K-Means algorithm-Example and suggestions for improvements- A Categorization ofMajor Clustering Methods, Partitioning Methods, Hierarchical Methods, Density-Based Methods (DBSCAN), Time series mining, Graph Mining, Reinforcement learning, Hidden markov models-Case studies-Introduction to rough sets-Mathematical
Notions.

**Module-4**

Introduction to cloud computing-Services from a cloud- Big Data-definition-data bases for the big data platform-Introduction to Hadoop its architecture and ecosystem. MapReduce-basic concepts-Introduction to Spark-Deep learning-Concepts-CNN and RNN- Typical use cases. Introduction to social network analysis, sentiment analysis

**References:**


1. Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques – 3rd Edition, Elsevier, 2011. ISBN: 9780123814807
2. Ian H.Witten et.al, Data Mining: Practical Machine Learning Tools and Techniques, Morgan Kofman publishers. 4th edition, 2016. ISBN: 978-0123748560
3. Ian Good fellow et.al, Deep learning, First edition, MIT Press, 2016. ISBN:978-0262035613
4. Tom White, Hadoop: The definitive guide, 3rd edition, OReilly Publishers, 2012. ISBN : 978-1449311520
5. Karau. H. et.al, Learning Spark: lightning-fast big data analysis, OReilly Publishers, 2015 hadoop, tom white. ISBN: 978-9351109945

**25-506-0106 Web Security**

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand various web server technologies.
2. Identify the need for security in e-commerce and payment gateways.
3. Adopt the recent technologies implemented to handle security threats.
4. Impart knowledge about the different mechanisms implemented for securing user data.

**Module-1**

Introduction- A web security forensic lesson, Web languages, Introduction to different web attacks. Overview of N-tier web applications, Web Servers: Apache, Nginx, Database Servers. Configuring Ngix and Apache to avoid security threats.

**Module-2**

Review of computer security, Public Key cryptography, RSA. Review of Cryptography Basics, e-commerce security - Payment Gateways.

**Module-3**

Web Hacking Basics HTTP & HTTPS URL, Web Under the Cover Overview of Java security Reading the HTML source, Applet and Servletsc Security. Symmetric and Asymmetric Encryptions, Network security Basics, Firewalls & IDS.

**Module-4**

Digital Certificates, Hashing, Message Digest, & Digital Signatures. Securing databases, Secure JDBC and ODBC, Securing Large Applications, Cyber Graffiti.

**References:**


1. Stuart McClure , Saumil Shah, Shreeraj Shah , " Web Hacking: Attacks and Defense" ,Addison Wesley , 2003. ISBN : 978-0201761764 .

2. Michael D. Bauer , " Building Secure Servers with Linux" , O'Reilly Media, 2002. ISBN : 978-0596002176
3. The Open SSL Project (SDKs for free download): http://www.openssl.org/.

## 25-506-0107 IT Security metrics

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand the recent developments in security metrics.
2. Understand various phases of the security process management framework.
3. Understand the challenges in implementing various security operations.

**Module-1**

Metric and Measurement, Security Metrics Today, The Dissatisfying State of Security Metrics, Reassessing Our Ideas About Security Metrics. Designing Effective Security Metrics:Choosing Good Metrics, GQM for Better Security Metrics, More Security Uses for GQM, Summary.

**Module-2**

Data Sources for Security Metrics; We Have Metrics and Data -Now what, Summary, Case Study 1. The Security Process Management Framework: Managing Security as a Business Process, the SPM Framework, Before You Begin SPM, Summary. The Analyzing Security Metrics Data: The Most Important Step, Analysis Tools and Techniques, Summary. Designing the Security Measurement Project: Before the Project Begins, Phase One: Build a Project Plan and Assemble the Team, Phase two: Gather the Metrics Data, phase Three: Analyze the Metrics Data and Build Conclusions,
phase Four: Present Results, Phase Five: Reuse the Results, Project Management Tools, Summary.

**Module-3**

Measurements Security Operations: Sample Metrics for Security Operations, Sample Measurement Project for Security Operations, Summary. Measuring Compliance and Conformance: The Challenges of Measuring Compliance, Sample Measurement Projects for Compliance and Conformance, Summary. Measuring Security Cost and Value: Sample Measurement Projects for Compliance and Conformance, The Importance of Data to Measuring Cost and Value, Summary. Measuring People, Organizations, and Culture: Sample Measurement Projects for People, Organizations, and Culture, Summary.

**Module-4**

The Security Improvement Program: Moving from Projects to Programs, Managing Security Measurement with a Security, Requirements for a SIP, Measuring the SIP. Summary. Learning Security: Different Contexts for Security Process Management: Organizational Learning, Three Learning Styles for IT Security Metrics.

**References:**


1. Lance Hayden, “IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data” , McGraw Hill, 2010. .ISBN : 978-0071713405

2. Caroline Wong , “Security Metrics, A Beginner's Guide” , McGraw Hill, 2011. ISBN : 978-0071744003

## 25-506-0108 Information Storage Management

COURSE OUTCOMES

After completion of course, students will be able to:

1. Impart knowledge on basic storage management skills and activities.
2. Familiarise with recent technological developments in storage systems architecture.
3. Understand about the implementation and management of networked storage.
4. Understand the need for disaster recovery mechanisms.
5. Understand the need for securing storage and the various threat handling mechanisms.

**Module-1**

Introduction to Storage Technology: Data proliferation and the varying value of data with time & usage, Sources of data and states of data creation, Data center requirements and evolution to accommodate storage needs, Overview of basic storage management skills and activities, The five pillars of technology,Overview of storage infrastructure components, Evolution of storage, Information Lifecycle Management concept, Data categorization within an enterprise, Storage and Regulations.

**Module-2**

Storage Systems Architecture: Intelligent disk subsystems overview, Contrast of integrated vs. modular arrays, Component architecture of intelligent disk subsystems, Disk physical structure- components, properties, performance, and specifications, Logical partitioning of disks, RAID & parity algorithms, hot sparing, Physical vs. logical disk organization, protection, and back end management, Array caching properties and algorithms, Front end connectivity and queuing properties, Front end to host storage provisioning, mapping, and operation, Interaction of file systems with storage, Storage system connectivity protocols.

**Module-3**

Introduction to Networked Storage: JBOD, DAS, SAN, NAS, & CAS evolution, Direct Attached Storage (DAS) environments: elements, connectivity, & management, Storage Area Networks (SAN): elements & connectivity, Fibre Channel principles, standards, & network management principles, SAN management principles, Network Attached Storage (NAS): elements, connectivity options, connectivity protocols (NFS,CIFS, ftp), & management principles, IP SAN elements, standards (iSCSI, FCIP, iFCP), connectivity principles, security, and management principles, Content Addressable Storage (CAS): elements, connectivity options, standards, and management principles, Hybrid Storage - solutions overview including technologies like virtualization & appliances.Introductions to Information Availability: Business Continuity and Disaster Recovery Basics, Local business continuity techniques, Remote business continuity techniques, Disaster Recovery principles & techniques.

**Module-4**

Managing & Monitoring: Management philosophies (holistic vs. system & component), Industry management standards (SNMP, SMI-S, CIM), Standard framework applications, Key management metrics (thresholds, availability, capacity, security, performance), Metric analysis methodologies & trend analysis, Reactive and pro-active management best practices, Provisioning & configuration change planning, Problem reporting, prioritization, and handling techniques, Management tools overview. Securing Storage and Storage Virtualization: Define storage security. , List the critical security attributes for information systems, describe the elements of a shared storage model and security extensions, Define storage security domains, List and analyze the common threats in each domain, Identify different virtualization technologies, describe block-level and file level virtualization technologies and processes.

**References:**


1. Marc Farley Osborne, "Building Storage Networks", Mac Graw Hill, 2001. ISBN : 978-0072130720
2. G.Somasundaram , Alok Shrivastava, "Information Storage and Management" , Wiley,2009. ISBN : 978-0470294215
3. Robert Spalding and Robert Spalding, "Storage Networks: The Complete Reference", McGraw Hill, 2003. ISBN : 978-0072224764
4. Meeta Gupta, "Storage Area Network Fundamentals", CISCO Press, 2002. ISBN : 978-1587050657


## 25-506-0109 Digital Watermarking and Steganography

COURSE OUTCOMES

After completion of course, students will be able to:

1. Analyse the need for information coding and information hiding.
2. Gain knowledge about different watermarking techniques and issues.
3. Differentiate between watermarking and cryptography.
4. Gain in-depth knowledge on different steganographic methods.

**Module-1**

Introduction: Information Hiding, Steganography and Watermarking – History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems Watermarking Models & Message Coding: Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.

**Module-2**

Watermarking with Side Information & Analyzing Errors: Informed Embedding – Informed Coding – Structured dirty-paper codes - Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates.

**Module-3**

Perceptual Models: Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients.Watermark Security & Authentication: Security requirements – Watermark security and cryptography – Attacks – Exact authentication – Selective authentication – Localization – Restoration.

**Module-4**

Steganography: Steganography communication – Notation and terminology – Information-theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis.

**References:**


1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, "Digital Watermarking and Steganography", Margan Kaufmann Publishers, New York, 2008.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, "Digital Watermarking", Margan Kaufmann Publishers, New York, 2003.
3. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, "Techniques and Applications of Digital Watermarking and Contest Protection", Artech House, London, 2003.
4. Peter Wayner, "Disappearing Cryptography – Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.

## 25-506-0110 Database Security

COURSE OUTCOMES

After completion of course, students will be able to:

1. Visualise the importance of the need for database security.
2. Identify the security architecture of typical database management systems.
3. Identify the possible threats and vulnerabilities.
4. Identify mechanisms against data exploitation.
5. Gain knowledge on security audit mechanisms.

**Module-1**

Importance of database security -malware - Security Architecture – security policies .
Database Structure Components-Database Models-Database Types-Database Management Systems-Architecture of MySQL, Oracle and MS SQL server. Installation of database server is Linux and Windows environments.

**Module-2**

Password, Profiles, Privileges, and Roles- Authentication- Authorization – Inference . SQL Injection: Understanding SQL Injections - Identifying Vulnerabilities.

**Module-3**

SQL Injection Exploitation and Defense : Exploitation and Information Gathering - Extracting the Real Data - Exploitation of Privileges and Passwords - Defending Against Exploitation .

**Module-4**

Security Auditing -audit Classification - goal of an Audit-The Auditing Process- - Database Auditing - Security Testing -Classification -Testing Methodology .

**References:**


1. Alfred Basta, Melissa Zgola , “Database Security” ,Cengage Learning, 2011. ISBN: 9781133708148
2. Ron Ben Natan, “Implementing Database Security and Auditing” ,Elsevier Science, 2010. ISBN: 9780080470641
3. Michael Gertz, Sushil Jajodia, “Handbook of Database Security” ,Springer , 2008. ISBN: 9780387485331
4. Indrakshi Ray, Pierangela Samarati ,”From Database to Cyber Security” , Springer , 2018 .ISBN: 9783030048341

## 25-506-0111 Embedded Systems Security

COURSE OUTCOMES

After completion of course, students will be able to:

1. Identify the issues and threats in embedded systems and the need for a robust security mechanism.
2. Do a case study analysis of secure embedded software implementation.
3. Gain knowledge about cryptographic mechanisms employed in embedded systems.
4. Impart knowledge about various data protection protocols for embedded systems.

**Module-1**

Embedded Security: Security Policies-Security Threats .Systems Software Considerations: The Role of the Operating System- Multiple Independent Levels of Security- Microkernel versus Monolith-Core Embedded Operating System Security Requirements- Access Control and Capabilities- Hypervisors and System Virtualization-I/O Virtualization- Remote Management- Assuring Integrity of the TCB.

**Module-2**

Secure Embedded Software Development: Introduction to PHASE—Principles of High-Assurance Software Engineering- Minimal Implementation- Component Architecture-Least Privilege- Secure Development Process- Independent Expert Validation-Case Study: HAWS—High-Assurance Web Server- Model-Driven Design.

**Module-3**

Embedded Cryptography- The One-Time Pad-Cryptographic Modes-Block Ciphers-Authenticated Encryption-Public Key Cryptography- Key Agreement-Public Key Authentication-Elliptic Curve Cryptography- Cryptographic Hashes- Message Authentication Codes- Random Number Generation-Key Management for Embedded Systems

**Module-4**

Data Protection Protocols for Embedded Systems: Data-in-Motion Protocols Data-at-Rest Protocols. Emerging Applications-Embedded Network Transactions- Automotive Security-Secure Android- Next-Generation Software-Defined Radio.

**References:**


1. David Kleidermacher,Mike Kleidermacher, "Embedded Systems Security", Elsevier, 2012. ISBN: 978-0-12-386886-2
2. Catherine H. Gebotys, "Security in Embedded Devices" ,Springer, 2010. ISBN: 9781441915306
3. Amjad Gawanmeh, Joel J. P. C. Rodrigues, "Cyber-Physical Systems for Next-Generation Networks" ,IGI Global ,2018. ISBN: 9781522555117
4. Timothy Stapko , "Practical Embedded Security" ,Elsevier Science, 2011. ISBN: 9780080551319

## 25-506-0112 Research Methodology and Intellectual Property Rights

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand research problem formulation
2. Analyse research related information
3. Follow research ethics
4. Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity
5. Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular
6. Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits

**Module-1**

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem.

Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations.

**Module-2**

Effective literature studies approaches, analysis, Plagiarism, Research ethics. Effective technical writing, how to write report, Paper. Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee.

**Module-3**

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.

**Module-4**

Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications. New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

**References:**


1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students", Goddard Publisher, 1996.
2. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction", Juta and Company, 2004.
3. Ranjit Kumar, 2 nd Edition, "Research Methodology: A Step by Step Guide for beginners", Pearson, 2005.
4. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd ,2007.
5. Mayall , "Industrial Design", McGraw Hill, 1992.
6. Asimov, "Introduction to Design", Prentice Hall, 1962.
7. Robert P. Merges, Peter S. Menell, Mark A. Lemley, " Intellectual Property in New Technological Age", 2016.
8. T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008.

**25-506-0113 Network Programming and Cryptography Lab**

COURSE OUTCOMES

After completion of course, students will be able to:

1. Apply packet capturing and analysis methods.
2. Familiarise network simulation tools.
3. Familiarise different encryption and hashing algorithms

**Experiments**

1. Programming using Python Pexpect and Paramiko Libraries.
2. Programming with Python Scapy.
3. Programming with OpenFlow, OpenStack and OpenDaylight
4. Programming in python using pcap libraries.
5. Familiarise wireshark.
6. Implementation of symmetric cipher algorithm(AES and RC4).
7. Implementation of RSA based signature system.
8. Testing various hashing algorithms (md5,sha etc..)
9. Implementation of Diffie-Hellman algorithm
10. Implementation of Kerberos cryptosystem.
11. Implementation of a trusted secure web transaction.
12. Digital Certificates and Hybrid (ASSY/SY) encryption, PKI.
13. Message Authentication Codes.
14. Elliptic Curve cryptosystems
15. Implementation of Goldwasser-Micali probabilistic public key system.

**References:**


1. Eric Chou, "Mastering Python Networking", Packt Publishing 2017.ISBN 978-1-78439-700-5.
2. W.R. Stevens, "Unix Network Programming, Vol 1&II", 2nd ed., Prentice-Hall Inc., 1998.
3. Douglas E.Comer, Hands on Networking with Internet Technologies, 2nd edition,Addison-Wesley,2004. ISBN: 978-0-13148-696-6

## 25-506-0114 Seminar I

COURSE OUTCOMES

After completion of course, students will be able to:

1. Identify and familiarize with some of the good technical publications and journals in his/her field / topic of study.
2. Acquaint oneself with preparation of independent reports, name them based on a central theme and write abstracts, main body, conclusions and references.
3. Understand effective use of tools for presentation, generate confidence in presenting a report before an audience and improve his/her skills in the same.
4. Develop skills like time management, leadership quality and rapport with audience.

Students shall individually prepare and submit a seminar report on a topic of current relevance related to the field of Cyber Forensics and information security . The reference shall include standard journals, conference proceedings, reputed magazines and textbooks and technical reports. The references shall be incorporated in the report following IEEE standards reflecting the state-of-the-art in the topic selected. Each student shall present a seminar for about 45 minutes duration on the selected topic. The report and presentation shall be evaluated by a team of internal experts comprising of 3 teachers based on style of presentation, technical content, adequacy of references, depth of knowledge and overall quality of the seminar report.

**References:**


1. David F. Griffiths,Desmond J. Higham "Learning LaTeX", Society for Industrial and Applied Mathematics,2016. ISBN:978-1611974416
2. Lalit Mali, "Libre office 5.1 Impress, Draw, Base book-Vol-2" ,Notion Press, 2017. ISBN:9781947027299.

## 25-506-0201 Software Vulnerability Analysis

COURSE OUTCOMES

After completion of course, students will be able to:

1. Identify and classify different types of software vulnerabilities.
2. Identify various prevention mechanisms.
3. Identify the vulnerabilities in file systems of typical operating systems.
4. Understand the overview of web technology and the common vulnerabilities.

**Module-1**

Software Vulnerability Fundamentals:Vulnerabilities-The Necessity of Auditing-Classifying Vulnerabilities-Common Threads.Software Design Fundamentals- Enforcing Security Policy-Threat Modeling.Operational Review:Exposure-Web Specific Considerations -Protective Measures- Overview of the Application Review Process:Preassessment- Application Review-Documentation and Analysis Reporting and Remediation Support-Code Navigation-Code-Auditing Strategies Code-Auditing Tactics-Code Auditor's Toolbox-Case Study: OpenSSH

**Module-2**

Software Vulnerabilities: Memory Corruption- Identifying and Preventing Software Vulnerabilities-Buffer Overflows-Shellcode-Protection Mechanisms- Assessing Memory Corruption Impact.C Language Issues:Introduction-Data Storage Overview-Arithmetic Boundary Conditions-Type Conversions-Type Conversion Vulnerabilities-Operators-Pointer Arithmetic-Other C Nuances

Program Building Blocks: Auditing Variable Use- Auditing Control Flow- Auditing Functions-Auditing Memory Management. Strings and Metacharacters: C String Handling-Metacharacters-Common Metacharacter Formats-Metacharacter Filtering-Character Sets and Unicode.

**Module-3**

UNIX/LINUX: Privileges and Files-Privilege Model-Privilege Vulnerabilities-File Security-File Internals-Links-Race Conditions -Temporary Files -The Stdio File Interface. Processes:Program Invocation- Process Attributes-Interprocess Communication-Remote Procedure Calls.

Windows: Objects and the File System-Objects-Sessions -Security Descriptors- Processes and Threads -File Access -The Registry. Interprocess Communication:Windows IPC Security- Window Messaging -Pipes -Mailslots -Remote Procedure Calls -COM.

**Module-4**

Software Vulnerabilities in Practice:Network Protocols-Internet Protocol-User Datagram Protocol-Transmission Control Protocol .Firewalls: Overview of Firewalls-Stateless Firewalls. Software Security Assessment:Identifying and Preventing Software Vulnerabilities -Simple Stateful Firewalls - Stateful Inspection Firewalls -Spoofing Attacks . Network Application Protocols-Auditing Application Protocols-Hypertext Transfer Protocol-Internet Security Association and Key Management Protocol-Abstract Syntax Notation (ASN.1)-Domain Name System. Web Technology Overview: HTTP -State and HTTP Authentication- Architecture - Problem Areas - Common Vulnerabilities -Harsh Realities of the Web -Auditing Strategy - Web Services and Service-Oriented Architecture .

Security metrics for measuring severity: NIST-CVSS.

**References:**


1. Mark Dowd, John McDonald, Justin Schuh, "The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities" , Addison Wesley Professional,2006. Print ISBN: 978-0-321-44442-4
2. John Viega & Gary McGraw, "Building Secure Software: How to Avoid Security Problems the Right Way" , Addison-Wesley, 2011. ISBN : 978-0321774958
3. Michael Howard, David LeBlanc, John Viega, "Deadly Sins of Software Security: Programming Flaws and How to Fix Them" ,McGraw-Hill Education, 2005.ISBN : 978-0072260854


## 25-506-0202 Ethical Hacking and Cyber Forensics

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand the types of hackers, the common threats, attacks and vulnerabilities.
2. Understand the modus operandi of various types of attacks.
3. Understand various spoofing attacks.
4. Impart knowledge on computer forensics services.

**Module-1**

Ethical Hacking–Overview-Hacker types-Threats and attacks ,Vulnerabilities, Phases of hacking-Reconnaissance-Scanning-Maintaining Access with Backdoors and Rootkits-Clearing aces.System Hacking-Hacking Windows-Hacking UNIX-Remote connectivity and VoIP Hacking. Software Hacking-Hacking code-Web Hacking-Hacking the Internet User.

**Module-2**

Password Hacking-Dictionary attack-Hybrid Dictionary attack-Brute force attack-Rainbow tables.A study on various attacks– Input validation attacks – SQL injection attacks – Buffer overflow attacks - Privacy attacks.

**Module-3**

TCP / IP – IP Spoofing, port scanning, DNS Spoofing. Dos attacks – SYN attacks, Smurf attacks, UDP flooding, DDoS – Models. Batch File Programming. Hacking wireless networks.

**Module-4**

Overview of computer forensics technology: computer forensics services-Data seizure-Data duplication and preservation-Data recovery-Document searches-Media conversion-Expert witness services-Computer evidence service options-Other miscellaneous services.

**References:**


1. Patrick Engebretson, "The Basics of Hacking and Penetration Testing", 2nd edition Syngress, 2013.ISBN : 978-0124116443
2. Stuart McClure, Joel Scambray,George Kurtz ,"Hacking Exposed: Network Security Secrets & Solutions", 3rd edition , McGraw-Hill Education, 2001. ISBN : 978-0072193817
4. John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition. Laxmi Publications, 2015. ISBN : 978-8170083412

## 25-506-0203 Cyber Crime Investigation and Digital Forensic

COURSE OUTCOMES

After completion of course, students will be able to:

1. Identify the nature and types of Cyber Crimes.
2. Impart knowledge on the legal aspects of Cyber Crimes.
3. Understand various investigation methods and evidence collection.
4. Get an overview of digital forensics and tools used.

**Module-1**

Introduction: Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime. Cyber Crime Issues: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

**Module-2**

Investigation: Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

**Module-3**

Digital Forensics: Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

**Module-4**

Laws and Acts: Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.

**References:**


1. Amelia Phillips, Frank Enfinger, Bill Nelson , “Computer Forensics and Investigations”, CBS publishers & distributors , 2009. ISBN : 978-1592003822
2. Jason T. Luttgens , Matthew Pepe, Kevin Mandia , “Incident Response and Computer Forensics “, Tata McGraw -Hill, New Delhi, 2006.
3. Robert M Slade,” Software Forensics”, Tata McGraw - Hill, New Delhi, 2005.
4. Anthony Reyes (Author), Richard Brittson , Kevin O'Shea , James Steele , “Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors”, Syngress, 2007.ISBN : 978-1597491334

## 25-506-0204 Intrusion Detection and Prevision System

COURSE OUTCOMES

After completion of course, students will be able to:

1. Get an overview of intrusion detection and prevention.
2. Understand the architecture and implementation methods of various intrusion detection mechanisms.
3. Impart knowledge on various tools used and their applications.
4. Get an overview of the legal side, issues and organisational standardizations.

**Module-1**

Introduction: Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anamoly detection – specification based detection – hybrid detection. Theoretical Foundations of Detection: Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering.

**Module-2**

Architecture and Implementation: Centralized – Distributed – Cooperative Intrusion Detection – Tiered. Justifying Intrusion Detection: Intrusion detection in security – Threat Briefing – Quantifying risk –Return on Investment (ROI).

**Module-3**

Applications and Tools: Tool Selection and Acquisition Process - Bro Intrusion Detection – Prelude Intrusion Detection - Cisco Security IDS - Snorts Intrusion Detection – NFR security.

**Module-4**

Legal issues and Organizations Standards: Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.

**References:**


1. Ali A. Ghorbani, Wei Lu,Mahbod Tavallaee, “Network Intrusion Detection and Prevention: Concepts and Techniques”,Springer, 2010. ISBN : 978-0387887708
2. Carl Endorf, Gene Schultz, Jim Mellander , “Intrusion detection and Prevention”, McGraw Hill, 2004. ISBN : 978-0072229547
3. Paul E. Proctor, “The Practical Intrusion Detection Handbook “,Prentice Hall , 2001. ISBN : 978-0130259608

**25-506-0205 Operating Systems and Security**

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand the need for a secure operating system, various threats and protection models.
2. Understand the security implementation of a typical operating system and its vulnerabilities.
3. Gain knowledge on implementation of a secure kernel.
4. Get an overview of secure virtual machines.

**Module-1**

Introduction: Secure Operating Systems - Security Goals - Trust Model -Threat Model .Access Control:Protection System - Lampson's Access Matrix -Mandatory Protection Systems -Reference Monitor - Secure Operating System Definition . Multics : The Multics System - Multics Fundamentals - Multics Security Fundamentals -Multics Protection System Models - Multics Protection System -Multics Reference Monitor -Multics Security -Multics Vulnerability Analysis

**Module-2**

Security in Ordinary Operating Systems: UNIX History- Windows History- UNIX Security- UNIX Protection System -UNIX Authorization -UNIX Security Analysis -UNIX Vulnerabilities. Windows Security - Windows Protection System - Windows Authorization -Windows Security Analysis - Windows Vulnerabilities .

Verifiable Security Goals: Information Flow- Information Flow Secrecy Models - Denning's Lattice Model -Bell-LaPadula Model - Information Flow Integrity Models -Biba Integrity Model - Low-Water Mark Integrity - Clark-Wilson Integrity -The Challenge of Trusted Processes- Covert Channels - Channel Types -Noninterference

**Module-3**

Security Kernels: The Security Kernel - Secure Communications Processor - Scomp Architecture - Scomp Hardware - Scomp Trusted Operating Program - Scomp Kernel Interface Package -Scomp Applications - Scomp Evaluation - Gemini Secure Operating System

Securing Commercial Operating Systems: Retrofitting Security into a Commercial OS-History of Retrofitting Commercial OS's - Commercial Era -Microkernel Era- UNIX Era -IX - Domain and Type Enforcement .

**Module-4**

Case Study: Building a Secure Operating System for Linux-Linux Security Modules - LSM History -LSM Implementation -Security Enhanced Linux -SELinux Reference Monitor -SELinux protection State -SELinux Labeling State - SELinux Transition State - SELinux Administration- SELinux Trusted Programs - SELinux Security Evaluation

Secure Capability Systems : Capability System Fundamentals - Capability Security - Challenges in Secure Capability Systems- Capabilities and the *-Property -Capabilities and Confinement -Capabilities and Policy Changes -Building Secure Capability Systems -Enforcing the *-Property - Enforcing Confinement - Revoking Capabilities

Secure Virtual Machine Systems: Separation Kernels - VAX VMM Security Kernel - VAX VMM Design - VAX VMM Evaluation - VAX VMM Result - Security in Other Virtual Machine Systems .

**References:**

1. Trent Jaeger, "Operating System Security", Morgan & Claypool, 2008. ISBN: 978-1598292121
2. Michael J. Palmer, "Guide to Operating Systems Security" ,Thomson/Course Technology, 2004. ISBN: 9780619160401
3. Enrico Perla, Massimiliano Oldani, "A Guide to Kernel Exploitation", Elsevier Science, 2010. ISBN: 9781597494878.
4. Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes , "Linux Security Cookbook" , O'Reilly Media, 2003. ISBN: 9781449366766
5. Darril Gibson, "Microsoft Windows Security Essentials", Wiley , 2011. ISBN: 9781118114575

## 25-506-0206 Information Theory and Coding

COURSE OUTCOMES

After completion of course, students will be able to:

1. Enhance their knowledge about the elements of modern probability theory.
2. Understand the elements of information theory with emphasis on its basic roots in probability theory.
3. Understand the relationships of entropy, relative entropy, and mutual information.
4. Understand the role of coding in communication and data storage system design and the need for implementation of error control coding methods.
5. To gain knowledge about various data compression techniques and their implementations.

**Module-1**

Random Variables and Processes: Events - Random variables - Distribution and density functions - Operations on random variables - Covariance - Correlation functions - Random process - Stationarity - Spectral decomposition - Response of linear system to random inputs, Relation between information and probability.

**Module-2**

Information Entropy Fundamentals: Self information measure - mutual and self information - Entropy function - Characteristics of Entropy function - Conditional Entropies - Derivation of the noise characteristics of a channel - Redundancy - Efficiency and channel capacity - capacities of channels with symmetric noise structure. Huffman coding: Implementation of Huffman code, Shannon's theorem, Code design, Shannon - Fano coding.

**Module-3**

Error Control Coding :Backward error correction linear block codes, BCH codes, Golay codes, efficiency of LBC, forward correction codes-Convolution coding decoding algorithms, Viterbi decoding optimum decoding performance measures.

**Module-4**

Data and Voice Coding: Context dependent coding, arithmetic codes, overall efficiency consideration. Voice coding, Delta Modulation and adaptive delta modulation, linear predictive coding, silence coding, sub-band coding. Compression Techniques: Principles – Text compression –Static Huffman Coding - Dynamic Huffman coding. Arithmetic coding – Image Compression – Graphics Interchange format – Tagged Image File Format – Digitized documents – Introduction to JPEG standards.

**References:**


1. Fazlollah M. Reza , "An Introduction to Information Theory", Dover Publications Inc, 2003.ISBN : 978-0486682105 .
2. Thomas M Cover, Joy A Thomas, "Elements of Information theory", 2nd edition, Wiley-Interscience, 2006.
3. Ron Roth , "Introduction to Coding theory", Cambridge University Press, 2006.ISBN : 978-0521845045
4. Peter Sweeney, "Error Control Coding: From Theory to Practice", John Wiley & Sons, 2002.ISBN : 978-0470843567


## 25-506-0207 Cyber Laws and Security Policies

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand the need for security in cyberspace.
2. Identify the components of Information System and challenges in Information System Security.
3. Gain knowledge about information security policies and procedures.
4. Identify the role of human experts in implementing information security.

**Module-1**

Introduction to Computer Security: Definition, Threats to security, Government requirements, Information . Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

**Module-2**

Secure System Planning and administration, Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Red book and Government network evaluations.

**Module-3**

Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

**Module-4**

Information security: fundamentals-Employee responsibilities- information classification- Information handling- Tools of information security- Information processing-secure program administration. Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.

**References:**


1. Nilakshi Jain , Ramesh Menon, "Cyber Security and Cyber Laws" , Wiley, 2020. ISBN : 978-9390395750
2. G.T. Gangemi Sr, Rick Lehtinen , "Computer Security Basics: Computer Security for the 21st Century ", 2ndEdition, Shroff, 2006. ISBN : 978-8184041583
3. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Auerbach Publications, 2004. ISBN : 978-0849319587
4. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer , CBS publishers & distributors, 2011. ISBN : 978-1461284840
5. James Graham, Ryan Olson, Rick Howard , " Cyber Security Essentials" ,Auerbach Publications, 2010. ISBN : 978-1439851234

## 25-506-0208 Cloud Computing

COURSE OUTCOMES

After completion of course, students will be able to:

1. Identify benefits and challenges of cloud computing and services.
2. Gain in-depth knowledge about cloud architecture.
3. Gain knowledge about cloud virtualization concepts.
4. Understand different cloud infrastructures.

**Module-1**

Cloud Computing Fundamental: Cloud Computing definition- private, public and hybrid cloud. Cloud types: IaaS, PaaS, SaaS. Benefits and challenges of cloud computing - public vs private clouds - role of virtualization in enabling the cloud - Business Agility: Benefits and challenges to Cloud architecture - Application availability – performance -security and disaster recovery Cloud Applications: Technologies and the processes required when deploying web services- Deploying a web service from inside and outside a cloud architecture - advantages and disadvantages.

**Module-2**

Cloud Services Management: Reliability, availability and security of services deployed from the cloud - Performance and scalability of services - tools and technologies used to manage cloud services deployment. Application Development: Service creation environments to develop cloud based applications - Development environments for service development.

**Module-3**

Virtual Data Centre: Environments-concept-planning and design-business continuity and disaster recovery principle-. Managing VDC and cloud environments and infrastructures. Information Storage Security & Design : Storage strategy and governance - security and regulations – Designing secure solutions - the considerations and implementations involved - Securing storage in virtualized and cloud environments - Monitoring and management - security auditing and SIEM.

**Module-4**

Storage Network Design: Architecture of storage, analysis and planning - Storage network design considerations - NAS and FC SANs - hybrid storage networking technologies (iSCSI, FCIP, FcoE) - design for storage virtualization in cloud computin - host system design considerations. Cloud Optimized Storage: Global storage management locations – scalability – operational efficiency - Global storage distribution - terabytes to petabytes and greater -Policy based information management - metadata attitudes - file systems or object storage. Designing backup/recovery solutions to guarantee data availability in a virtualized environment.

**References:**


1. Gautam Shroff, “Enterprise Cloud Computing: Technology, Architecture, Application”, Cambridge University Press,2010. ISBN: 978-1-10766-854-6.
2. Nick Antonopoulos, Lee Gillame, “Cloud Computing-rinciples, Systems and Application”, Springer,2010. ISBN: 978-1-84996-241-4.
3. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, McGrawhill, 2009. ISBN: 978-0-07162-694-1.
4. Greg Schulz , “Cloud and Virtual Data Storage Networking” , Auerbach Publications, 2011. ISBN: 978-1-43985-173-9.
5. Volker Herminghaus, Albrecht Scriba, “ Storage Management in Data Centers”, Springer, 2009. ISBN: 978-3-54085-022-9.

## 25-506-0209 Deep Learning

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand the basics of mathematical aspects of machine learning.
2. Apply fundamental principles and frameworks of deep neural networks.
3. Design and analyse various deep learning algorithms and techniques.
4. Explore Deep learning techniques and various deep network architectures.
5. Design and develop an application using suitable tools.

**Module-1**

Review of Machine Learning- The math behind machine learning- Linear algebra, Statistics. Foundations of Neural networks and deep learning – Neural networks- Activation functions, Loss functions, Hyper parameters.

**Module-2**

Fundamentals of Deep Networks – Definition, Common architectural principles, Building blocks.
Major architectures of deep networks- Unsupervised pre trained networks, Convolutional Neural Networks, Recurrent Neural networks, Recursive Neural networks.

**Module-3**

Training Deep Neural nets – Reusing pre trained layers, faster optimisers, avoiding overfitting through regularisation. Distributing Tensorflow across devices and servers- Multiple devices on a single machine, multiple devices across multiple servers. Parallelising Neural networks on a Tensorflow cluster.

**Module-4**

Autoencoders- Stacked autoencoders, denoising autoencoders,sparse autoencoders, variational autoencoders.Reinforcement Learning – Temporal difference learning and Q-Learning. Vectorization – Introduction to vectorization in machine learning, Vectorising image data, Working with Text in vectorisation. Attention mechanisms-Language translators- Vision transformers and image classification. Case study: Deep learning using TensorFlow Library.

**References:**


1. Josh Patterson, Adam Gibson, “Deep Learning: A Practitioner's Approach”, 1st Edition,O'Reilly ISBN : 978-1491914250,ISBN-10 : 1491914254.
2. Ian Goodfellow,Yoshua Bengio,Aaeron Courvill , “Deep Learning “,The MIT Press, Cambridge, Massachusetts,London, England,2017
3. Aurélien Géron, “Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems”, 1st Edition, O'Reilly. ISBN:978-1491962299, ISBN-10:1491962291


## 25-506-0210 Security and Privacy in Internet of Things

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand the basic architecture of IoT.
2. Understand various security implementation methodologies.
3. Understand various cryptographic methods used in IoT.
4. Identify various mechanisms for implementing user level authentication and device level authentication.

**Module-1**

Evolution of IoT- IoT Architecture and Taxonomy -Standardization Efforts - IoT Applications . IoT Security**:**Attacks and Countermeasures - Perception Layer -Network Layer - Application Layer -Authentication and Authorization - Authentication at IoT Layers - The Simplified Layer Structure - Middleware - Cross-Layer Security Problem - Privacy - Risk Mitigation - Blockchain - 5G - Fog and Edge Computing - Quantum Security, AI, and Predictive Data Analytics - Network Slicing .IoT Network and Communication Authentication: System Model and Assumptions - Attack Model - Group Node Key -Individual Cluster Key - Pairwise Key Derivation - Multicast Key - Group Cluster Key - Authentication by CN -Authenticated Broadcast by the CH - Authenticated Broadcast by the BS - Scheme in Change Mode - Capture of CN -Capture of CH -Packet Fragmentation .

**Module-2**

Public Key Based Protocols : ECC for Authentication and Key Management - ECC Based Implicit Certificates -Authentication and Key Management Using ECC Implicit Certificates - ECC-Based Signcryption - Security Features - ECC-Based Group Communication -Implementation Aspects . Lattice-Based Cryptography and Internet of Things : Lattice-Based Cryptography – Lattice Based Primitives - One-Way and Collision-Resistant Hash Functions - Passively Secure Encryption - Actively Secure Encryption - Trapdoor Functions - Gadget Trapdoor - Digital Signatures without Trapdoors - Pseudorandom Functions (PRF) - Homomorphic Encryption - Identity-Based Encryption (IBE) - Attribute-Based Encryption - Lattice-Based Cryptography for IoT

**Module-3**

IoT User Level Authentication: Network Model - Adversary Model - System Setup for the Edge Nodes Registration at the Registration Center -User Registration Phase - Login and User Authentication Phase - Password Update Phase - Security and Performance Evaluation .Biometric-Based Robust Access Control Model for Industrial IoT Applications: Network Model - Threat Model - Security Goals - Authentication and Key Establishment -Security and Performance Evaluations .

**Module-4**

IoT Device Level Authentication: PUF-Based Authentication and Key Exchange for IoT **-** Key Agreement from IoT Device to Server - Key Agreement between Two IoT Devices -System Architecture -Attack Model - Cryptographic Operations -Registration Phase -Security Association Phase -Authentication and Key Agreement Phase -Security Evaluation . Hardware-Based Encryption : System Scheme: Synchronization without Correlation - The Delay-Filter-Permute Block - Steady-State Dynamics of the DFP - DFP-Bitstream Generation - Sensitivity to Changes in the Permutation Table - The Chaotic Followers - The Permute-Filter Block - Brute Force Attack - PF-Bitstream Generation .Case Study: Remote Patient Monitoring -Blockchain-Based Cyber Physical Trust Systems .

**References:**


1. Madhusanka Liyanage , An Braeken, Pardeep Kumar, Mika Ylianttila (Editors), “IoT Security: Advances in Authentication” ,Wiley, 2020. ISBN: 978-1-119-52792-3

2. Brian Russell, Drew Van Duren , “Practical Internet of Things Security” ,Packt Publishing, 2016. ISBN: 9781785880292

3. Debdutta Barman Roy, Rituparna Chaki (Editors) , "Security in IoT-The Changing Perspective" ,CRC Press, 2022. ISBN: 9781000531299.

## 25-506-0211 Block Chain and Information Security

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand the fundamentals of block chain
2. Block chain based security
3. IoT security using block chain.

**Module-1**

Cyber Threat Landscape and Security Challenges : Distributed denial-of-service (DDoS) attacks - Insider threats - Data breaches - Advanced persistence threat (APT) .The security ecosystem -The zero-trust approach - The assume breach approach - Evolution at the foundation layer .

Introducing Blockchain and Ethereum: What is blockchain -Internet versus blockchain -How blockchain works -The building blocks of blockchain -Ethereum: What is Ethereum -Smart contract -EVM -Gas -dApp -Private versus public blockchain. Introduction to Etherium framework and case studies.

**Module-2**

Hyperledger : Blockchain for Businesses - Technical requirements -Hyperledger overview -Blockchain-as-a-service (BaaS) -Architecture and core components - Hyperledger Fabric model -Hyperledeger Fabric core components - Workings of Hyperledger and transaction processing - Bitcoin versus Ethereum versus Hyperledger - Hyperledger Fabric capabilities Blockchain on the CIA Security Triad: What is the CIA security triad -Understanding blockchain on confidentiality - Blockchain on integrity - Understanding blockchain on availability.

**Module-3**

Deploying PKI-Based Identity with Blockchain : PKI -Components- Architecture - Challenges of the existing PKI model - How can blockchain help - Decentralized infrastructure - Deployment method

Two-Factor Authentication with Blockchain : What is 2FA - Blockchain for 2FA

Blockchain-Based DNS Security Platform : DNS -Understanding DNS components - DNS structure and hierarchy - DNS topology for large enterprises - Challenges with current DNS - Blockchain-based DNS solution - X.509 PKI replacement - MITM-proof DNS infrastructure

**Module-4**

Deploying Blockchain-Based DDoS Protection :DDoS attacks -What is a DDoS attack - Types of DDoS attacks - Attacks targeting network resources - User datagram protocol (UDP) flood - ICMP flood - Internet Group Management Protocol (IGMP) flood - Amplification attacks -Attacks targeting server resources - TCP SYN Flood - TCP RST attack - Secure sockets layer (SSL)-based attack - Encrypted HTTP attacks - Attacks targeting application resources - DNS flooding - Challenges with current DDoS solutions – Using blockchain for DDoS protection .Decision path for blockchain - When should use blockchain - When should not use blockchain - Challenges with blockchain . Blockchain-Based Cyber Physical Trust Systems

**References:**

1. Rajneesh Gupta, "Hands-On Cybersecurity with Blockchain" ,Packt Publishing , 2018. ISBN: 9781788990189
2. Chandan Trivedi, Piyush Kumar Shukla, Sweta Gupta, Udai Pratap Rao, Zelalem Sintayehu

Shibeshi (Editors) , "Blockchain for Information Security and Privacy" ,CRC Press, 2021. ISBN: 9781000483109
3. Madhusanka Liyanage , An Braeken, Pardeep Kumar, Mika Ylianttila (Editors), "IoT Security: Advances in Authentication" ,Wiley, 2020. ISBN: 978-1-119-52792-3

4. Ali Dehghantanha, Kim-Kwang Raymond Choo, Reza M. Parizi (Editors) , "Blockchain Cybersecurity, Trust and Privacy", Springer , 2020. ISBN: 9783030381813

## 25-506-0212 Ethical Hacking Digital Forensic Lab

COURSE OUTCOMES

After completion of course, students will be able to:

1. Understand Hacking method.
2. Familiarise ethical hacking tools.
3. Understand how to create malware.
4. Understand how to create anti-malware.
5. Understand how to secure network,applications and servers.
6. Familiarise with security auditing and generating reports.

**Experiments**

1. Creating Phishing. Pages.
2. Implement DoS attacks and its detection.
3. Implement different web attacks and intrusion.
4. Write codes for identifying web attacks.
5. System hacking
6. Password hacking
7. Worms, Viruses and Trojans
8. Hacking wireless networks.
9. Email tracking
10. Securing web servers to defend attacks.
11. Penetration tests.
12. Familiarise security auditing softwares and generating reports.

**References:**

1. Thomas Wilhelm , "Professional Penetration Testing: Creating and Learning in a Hacking Lab ", 2nd edition, Syngress, 2013. ISBN : 978-1597499934
2. Jeremy Martin, "Hacking Lab with Kali", Amazon Digital Services LLC, 2018. ISBN : 978-1522086437
3. Vivek Ramachandran, "BackTrack 5 Wireless Penetration Testing Beginner's Guide" , Packt Publishing Limited ,2011.ISBN : 978-1849515580

4. Michael sikorski , andrew honig, "Practical malware analysis the hands-on guide to dissecting malicious software", No Starch Press, 2012. ISBN : 978-1593272906

## 25-506-0213 Seminar II

COURSE OUTCOMES

After completion of course, students will be able to:

1. Identify and familiarize with some of the good technical publications and journals in his/her field / topic of study.
2. Acquaint oneself with preparation of independent reports, name them based on a central theme and write abstracts, main body, conclusions and references.
3. Understand effective use of tools for presentation, generate confidence in presenting a report before an audience and improve his/her skills in the same.
4. Develop skills like time management, leadership quality and rapport with audience.

Students shall individually prepare and submit a seminar report on a topic of current relevance related to the field of Cyber forensics and information security. The reference shall include standard journals, conference proceedings, reputed magazines and textbooks and technical reports. The references shall be incorporated in the report following IEEE standards reflecting the state-of-the-art in the topic selected. Each student shall present a seminar for about 45 minutes duration on the selected topic. The report and presentation shall be evaluated by a team of internal experts comprising of 3 teachers based on style of presentation, technical content, adequacy of references, depth of knowledge and overall quality of the seminar report.

**References:**


1. David F. Griffiths,Desmond J. Higham "Learning LaTeX", Society for Industrial and Applied Mathematics,2016. ISBN:978-1611974416
2. Lalit Mali, "Libre office 5.1 Impress, Draw, Base book-Vol-2" ,Notion Press, 2017. ISBN:9781947027299.

## 25-506-0301 Internship

COURSE OUTCOMES

After completion of course, students will be able to:

1. Gain exposure to professional work culture and practices.
2. Apply and correlate theory and practice in the area of structural engineering.
3. Develop domain specific problem solving and critical thinking in day to day operation.
4. Create proper documentation of the work and present it before a committee.

The objective of this training is to expose the students to industry environment and practices. The students have to undergo training for duration of 4 weeks in IT Industries / Consultancy organizations / R & D organizations after the completion of second semester. The students shall submit a report of the training undergone and present the contents of the report before the evaluation Committee. Evaluation committee will award the marks based on training quality, contents of the report and presentation.

**MOOC COURSE**

Those students opting for MOOC course shall credit a MOOC course of minimum 8 weeks duration after getting prior approval from the division.

## 25-506-0302 Dissertation Phase-I

COURSE OUTCOMES

After completion of course, students will be able to:

1. Conduct literature survey in the field of Cyber forensics and Information security and identify and concentrate on a research / industry related problem in the specified field.
2. Formulate a project proposal through extensive study of the literature and / or discussion with learned resource persons in academy, industry or around
3. Generate a proper execution plan of the project work to be carried out in Phase-II through deliberations.
4. Improve presentation skills.

Each student shall identify a project in the field of Cyber forensics and Information security . The project work has to be carried out within the department itself. There is a project guide allotted to each student by the head of the division / course coordinator. The project work shall be reviewed and evaluated periodically by the project guide during third semester and be continued in the fourth semester. Under special cases, student can carry out a project in a reputed Industry / R&D institutions with the permission of course coordinator / HOD.

At the end of the semester, each student shall submit a project report comprising of the following.

1. Literature Review.
2. Application and feasibility of the project.
3. Objectives.
4. Detailed documentation including diagrams and algorithms .
5. Project implementation action plan.
6. References.

The project must be evaluated by a team comprising of 3 internal examiners including the project guide, coordinator & a senior faculty member.

## 25-506-0401 Dissertation Phase-II

COURSE OUTCOMES

After completion of course, students will be able to:

1. Apply required theory and experiments on the problem related to industry / research identified in Phase-I and solve it.
2. Realize various steps involved in completing a project work like literature survey, methodology adopted ( field study / survey / experiments / numerical work), analysis of the data to arrive at final results and conclusions.
3. Present and defend self-prepared report, verified by the project guide to a peer audience.

The project work started in the third semester shall be reviewed and evaluated periodically in the fourth semester by the guide. At the end of the semester, each student shall submit a project report comprising of the following.

1. Literature Review
2. Objectives
3. Detailed documentation including diagrams and algorithms
4. Result / Output
5. Future scope
6. Conclusion
7. References

The thesis will be examined by an oral examination committee. The committee shall consist of the thesis supervisor (project guide), one faculty member from the department ( course coordinator or faculty appointed by HOD) and one expert from outside the institute or within the department. The course coordinator will act as the Convener of the Committee. The final evaluation of the project shall include the following.

1. Presentation of the work
2. Oral examination
3. Demonstration of the project against objectives
4. Quality and content of the project report