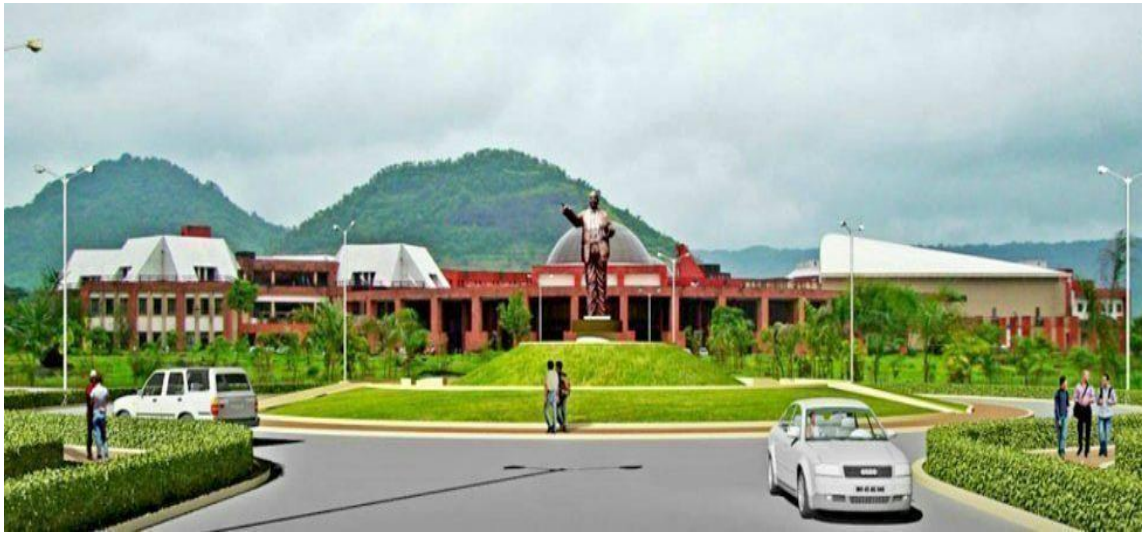
Dr. Babasaheb Ambedkar Technological University
(Established as a University of Technology in the State of Maharashtra)
(Under Maharashtra Act No. XXIX of 2014)
P.O. Lonere, Dist. Raigad, Pin 402 103, Maharashtra
Telephone and Fax. 02140 - 275142
www.dbatu.ac.in

CURRICULUM
POST GRADUATE PROGRAMME FOR
M.TECH

CYBER SECURITY

WITH EFFECT FROM THE ACADEMIC YEAR

2022-23



Semester –I (Cyber Security)

Course Category	Course Code	Course Title	Weakly Teaching Hrs.			Evaluation Scheme					Credit
			L	T	P	CA	MSE	ESE	OR	Total	
	MTCS1101	Mathematical Foundations for Cyber Security	3	1	-	20	20	60	-	100	4
	MTCS1102	Advanced Data Structures and Algorithms	3	1	-	20	20	60	-	100	4
	MTCS1103	Operating Systems and Security	3	1	-	20	20	60	-	100	4
	MTCS1104	Elective - I	3	-	-	20	20	60	-	100	3
	MTCS1105	Elective – II	3	-	-	20	20	60	-	100	3
	MTCSL1106	Information Security Lab	-	-	4	50	-	-	50	100	2
TOTAL			**15**	**3**	**4**	**150**	**100**	**300**	**50**	**600**	**20**

Elective –I

MTCS1104A	Cryptographic Protocols and Standards
MTCS1104B	E-Commerce
MTCS1104C	Neural Networks
MTCS1104D	Data Privacy

Elective –II

MTCS1105A	Information Risk Management
MTCS1105B	Mobile Network Security
MTCS1105C	Data Mining and Machine Learning
MTCS1105D	Coding and Information Theory

Semester –II (Cyber Security)

Course Category	Course Code	Course Title	Weakly Teaching Hrs.			Evaluation Scheme					Credit
			L	T	P	CA	MSE	ESE	OR	Total	
	MTCS1201	Cyber Forensics	3	1	-	20	20	60	-	100	4
	MTCS1202	Secure Coding	3	1	-	20	20	60	-	100	4
	MTCS1203	Ethical Hacking	3	1	-	20	20	60	-	100	4
	MTCS1204	Elective - III	3	-	-	20	20	60	-	100	3
	MTCS1205	Elective – IV	3	-	-	20	20	60	-	100	3
	MTCSL1206	Ethical Hacking And Digital Forensic Tools Lab	-	-	3	50	-	-	50	100	2
	MTCSS1207	Seminar			4	50			50	100	2
TOTAL			**15**	**3**	**7**	**200**	**100**	**300**	**100**	**700**	**22**

Elective - III

MTCS1204A	Digital Watermarking
MTCS1204B	Identity and Access Management
MTCS1204C	Cryptanalysis
MTCS1204D	Storage Management and Security

Elective - IV

MTCS1205A	Cyber Laws and Security Policies
MTCS1205B	Disaster Recovery
MTCS1205C	IT Governance
MTCS1205D	IoT Security

Semester –III (Cyber Security)

Course Category	Course Code	Course Title	Weakly Teaching Hrs.			Evaluation Scheme					Credit
			L	T	P	CA-I	MSE	ESE	OR	Total	
	MTCE2101	Project Management and Intellectual Property Rights (Self Study)*	-	-	-	50	-	-	50	100	2
	MTCS2102	Project Phase-I	-	-	-	50	-	-	50	100	10
TOTAL			**-**	**-**	**-**	**100**	**-**	**-**	**100**	**200**	**12**

*Student may select this course either from NPTEL/SWAYAM/MOOC pool or any other reputed source approved by the BoS. The submission of course completion certificate is mandatory. If the course is not available in online mode, University may conduct exam for the same.

Semester –IV (Cyber Security)

Course Category	Course Code	Course Title	Weakly Teaching Hrs.			Evaluation Scheme					Credit
			L	T	P	CA-II	MSE	ESE	OR	Total	
	MTCS2202	Project Phase-II				100	-	-	100	200	20
TOTAL			**-**	**-**	**-**	**100**	**-**	**-**	**100**	**200**	**20**

Detailed Syllabus

MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY
MTCS1101

COURSE OBJECTIVES:

1. Introduce basic concepts and knowledge in number theory, together with a wide variety of interesting applications of discrete mathematics.
2. Train students to solve problems from algorithm design and analysis, coding theory etc. and to apply techniques of number theory in cryptography.

COURSE OUTCOMES:

1. Understand the ideas of group, ring and an integral domain and be aware of examples of these structures in mathematics.
2. Introduce students to number theoretic problems and to different areas of number theory.
3. Apply coding methods to generate error detection and correction codes.
4. Use the concept of randomness in the domain of cryptography

Syllabus

Unit I

ALGEBRAIC STRUCTURES: Groups – Subgroup, Cyclic groups, group homomorphism, Permutation groups, Cosets, Modulo groups – Primitive roots – Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Rings of polynomials, factorization of polynomials over a field. Fields – Finite fields – GF (pn), GF (2n) - Classification – Structure of finite fields

Unit II

NUMBER THEORY**:** 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. Modular Arithmetic and Caesar cipher, quadratic residues, Legendre symbol, Jacobi symbol. Gauss's lemma, Quadratic Reciprocity.

Unit III

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.

Unit IV

STOCHASTIC PROCESS Random Variables – discrete and continuous- Central Limit Theorem-Stochastic Process- Markov Chain.

Unit V

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. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
2. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
3. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
4. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
5. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990. 6. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.

ADVANCED DATA STRUCTURES AND ALGORITHMS
MTCS1102

COURSE OBJECTIVES:

1. Familiarize with advanced data structures based on trees and heaps.
2. Learn to choose the appropriate data structure and algorithm design method for a specified application.
3. Study approaches used to analyze and design algorithms and to appreciate the impact of algorithm design in practice.
4. Learn different advanced algorithms in dynamic programming, flow network and computational geometry.

COURSE OUTCOMES: After completion of the course, the students will be able to

1. Compare different implementations of data structures and to recognize the advantages and disadvantages of the different implementations.
2. Determine which algorithm or data structure to use in different scenarios.
3. Design and analyze the performance of an algorithm.
4. Demonstrate different advanced algorithms in dynamic programming, flow network and computational geometry.

Syllabus

Unit I

Trees -Threaded Binary Trees, Selection Trees, Forests and binary search trees, Counting Binary Trees, Red-Black Trees, Splay Trees, Suffix Trees, Digital Search Trees, Tries- Binary Tries-patricia, Multiway Tries.

Unit II

Priority Queues - Single and Double Ended Priority Queues, Leftist Trees, Binomial Heaps, Fibonacci Heaps, Pairing Heaps, Symmetric Min-Max Heaps, Interval Heaps.

Unit III

Analysis of Algorithms-review of algorithmic strategies, asymptotic analysis, solving recurrence relations through Substitution Method, Recursion Tree, and Master Method. Dynamic Programming-Rod cutting-top down and bottom up approach, matrix chain multiplication-recursive solution, longest common subsequence problem

Unit IV

Maximum Flow-Flow Networks, Ford-Fulkerson method-analysis of Ford-Fulkerson, Edmonds-Karp algorithm, maximum bipartite matching, Betweenness Centrality algorithm.

Unit V

Computational Geometry - Line segment properties, Finding the convex hull, finding the closest pair of points. Implementations using Python.

REFERENCES:

1. Ellis Horowitz, SartajSahni, Susan Anderson Freed, Fundamentals of Data Structures in C, Second Edition, University Press, 2008
2. Yedidyah Langsam, Moshe J. Augenstein, Aaron M. Tenenbaum, Data Structures using

C and C++, Second Edition, PHI Learning Private Limited, 2010
3. Thomas Cormen, Charles, Ronald Rives, Introduction to algorithm,3rd edition, PHI Learning
4. Ellis Horowitz and SartajSahni, Sanguthevar Rajasekaran, Fundamentals of Computer Algorithms, Universities Press, 2nd Edition, Hyderabad.
5. Sara Baase & Allen Van Gelder, Computer Algorithms – Introduction to Design and Analysis, Pearson Education..
6. Anany Levitin, Introduction to The Design & Analysis of Algorithms, Pearson Education, 2nd Edition, New Delhi, 2008.
7. Berman and Paul, Algorithms, Cenage Learning India Edition, New Delhi, 2008.
8. S.K.Basu , Design Methods And Analysis Of Algorithms ,PHI Learning Private Limited, New Delhi,2008.
9. Jon Kleinberg and Eva Tardos, Algorithm Design, Pearson Education, New Delhi, 2006.
10. Hari Mohan Pandey, Design Analysis and Algorithms, University Science Press, 2008.
11. R. Panneerselvam, Design and Analysis of Algorithms, PHI Learning Private Limited, New Delhi, 2009.
12. UditAgarwal, Algorithms Design and Analysis, Dhanapat Rai & Co, New Delhi, 2009.
13. Aho, Hopcroft and Ullman, The Design And Analysis of Computer Algorithms, Pearson Education, New Delhi, 2007.
14. S.E.Goodman and S. T. Hedetmiemi, Introduction To The Design And Analysis Of Algorithms, McGraw-Hill International Editions, Singapore 2000.
15. Richard Neapolitan, Kumarss N, Foundations of Algorithms, DC Hearth &company.
16. Sanjay Dasgupta, Christos Papadimitriou, Umesh Vazirani, Algorithms, Tata McGraw-Hill Edition.

OPERATING SYSTEMS AND SECURITY
MTCS1103

COURSE OBJECTIVES:

1. Introduce students to the field of threats and vulnerabilities in OS and how to provide security in different OS.
2. Focuses on the study of techniques of fundamentals of protection systems, Information flow and Security kernels. This course also deals with a couple of case studies.

COURSE OUTCOMES: Upon completion, the student will be able to

1. Understand the basic of securing an operating system.
2. Understand the principles of trusted systems, Information flow integrity and securing commercial OS.
3. Understand the security challenges with the help of case studies

Syllabus

Unit I

Introduction: Secure OS, Security Goals, Trust Model, Threat Model. Access Control Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system. Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis

Unit II

Verifiable security goals: Information flow, information flow secrecy models, information flow integrity model, the challenges of trusted process, covert channels.

Unit III

Security Kernels: The Security Kernels, secure communications processor, Securing commercial OS: Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX Era- IX, domain and type enforcement

Unit IV

Case study - Solaris Trusted extensions: Trusted extensions access control, Solaris compatibility, trusted extension mediations, process rights management, role based access control.

Unit V.

Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

REFERENCES:

1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008
2. Michael Palmer, Guide to Operating system Security Thomson
3. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition
4. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont
5. Paxson, Bro: A System for Detecting Network Intruders in Real-Time. Proc. 7th USENIX Security Symposium, San Antonio, TX, January 1998.

CRYPTOGRAPHIC PROTOCOLS and STANDARDS
MTCS1104A

COURSE OBJECTIVES:

1. To provide learners with the concepts of symmetric and asymmetric cipher models.
2. To enable learners to understand fundamental concepts of authentication.

COURSE OUTCOMES: At the end of the course, students will be able

1. To explain classical encryption techniques.
2. To demonstrate encryption techniques and key exchange methods.
3. To differentiate between types of cryptosystems.
4. To compare various authentication techniques and signature schemes.

Syllabus

Unit I

Introduction to concepts of security, Cryptographic goals, Classical encryption techniques: Shift cipher, Substitution cipher,Vigenere cipher, Hill cipher, Permutation cipher, Stream ciphers, LFSR, Cryptanalysis of Vigenere cipher and LFSR.

Unit II

Modern Block Ciphers: Block ciphers principles, Shannon's theory of confusion and diffusion, Feistel cipher, Data Encryption Standard, 3- DES, Advanced Encryption Standard and Modes of operation, IDEA

Unit III

Hash Functions and Data Integrity: Classification and framework, Cryptographic hash functions, message authentication code, Hash based MAC, Case study: SHA 256. Introduction to Public Key Cryptography: Integer factorization problem, Discrete logarithm problem.

Unit IV

Public key cryptosystems- RSA cryptosystem, Attacks on RSA, Diffie-Hellman Key agreement scheme, ElGamal cryptosystem,

Unit V

Elliptic curve cryptography. Signature schemes: RSA signature, Digital Signature Algorithm, ECDSA. X.509 certification standard.

REFERENCES:

1. William Stallings, Cryptography and Network Security, Pearson Education, 2014.
2. Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw-Hill. 2010.
3. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network security", 2nd edition, Pearson India Education Services.
4. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
5. Abhijith Das and C.E. VeniMadha van, "Public-key Cryptography, Theory and Practice", Pearson Education, 2009.

E-COMMERCE
MTCS1104B

Syllabus

Unit I
Traditional commerce and E commerce – Internet and WWW – role of WWW – value chains strategic business and Industry value chains – role of E commerce.

Unit II
Packet switched networks – TCP/IP protocol script – Internet utility programmes, HTML, XML, XAML, SOA – web client and servers – Web client/server architecture – intranet and extranets.

Unit III
Web server – performance evaluation - web server software feature sets – web server software and tools – web protocol – search engines – intelligent agents –EC software – web hosting – cost analysis, Google and Facebook Ads case study

Unit IV
Computer security classification – copy right and Intellectual property – electronic commerce threats – protecting client computers – electronic payment systems – electronic cash – strategies for marketing – sales and promotion – cryptography – authentication.

Unit V
Definition and capabilities – limitation of agents – security – web based marketing – search engines and Directory registration – online advertisements – Portables and info mechanics – website design issues, BotNet and its infrastructure.

REFERENCES:

1. Ravi Kalakota, " Electronic Commerce", Pearson Education,
2. Gary P Schneider "Electronic commerce", Thomson learning & James T Peny Cambridge USA, 2001
3. Manlyn Greenstein and Miklos "Electronic commerce" McGraw-Hill, 2002.
4. EfraimTurvanJ.Lee, David kug and chung, "Electronic commerce" Pearson Education Asia 2001.
5. Brenda Kienew E commerce Business Prentice Hall, 2001.
6. E - Commerce : Business, Technology, Society- 2016 Edition 10 by by Kenneth C. Laudon,Pearson Education

NEURAL NETWORKS
MTCS1104C

Syllabus

Unit I

Neural network, Human Brain, Models of a Neuron, Neural networks as Directed Graphs, Network Architectures, Knowledge Representation, Artificial Intelligence and Neural Networks. Learning Error Correction learning, Memory based learning, Hebbian learning

Unit II

Learning: Competitive, Boltzmann learning, Credit Assignment Problem, Memory, Adaption, Statistical nature of the learning process. Single Layer Perceptron's: – Adaptive filtering problem, Unconstrained Organization Techniques, Linear least square filters, least mean square algorithm, learning curves, Learning rate annealing techniques, perception –convergence theorem, Relation between perception and Bayes classifier for a Gaussian Environment

Unit III

Multi-Layer Perceptron's – Back propagation algorithm XOR problem, Heuristics, Output representation and decision rule, Computer experiment, feature detection Back Propagation - back propagation and differentiation, Hessian matrix, Generalization, Cross validation, Network pruning Techniques, Virtues and limitations of back propagation learning, Accelerated convergence, supervised learning

Unit IV

Self-Organization Maps: Two basic feature mapping models, Self-organization map, SOM algorithm, properties of feature map, computer simulations, learning vector quantization, Adaptive patter classification, Hierarchal Vector quantilizer, contexmel Maps

Unit V

Neuro Dynamics: Dynamical systems, stavility of equilibrium states, attractors, neuro dynamical models, manipulation of attractors' as a recurrent network paradigm. Hopfield models and experiments

REFERENCES:

1. Neural networks A comprehensive foundations, Simon Haykin, Pearson Education 2nd
2. Edition 2004
3. Artificial neural networks - B.Vegnanarayana Prentice Halll of India P Ltd 2005
4. Neural networks in Computer intelligence, Li Min Fu TMH 2003
5. Neural networks James A Freeman David M S kapura Pearson Education 2004

DATA PRIVACY
MTCS1104D

COURSE OBJECTIVES:

1. To create architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals, the confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

COURSE OUTCOMES: After successful completion of this course, students will be able to:

1. Understand the concepts of privacy in today's environment.
2. Obtain the understanding of how automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security.
3. Obtain the knowledge of the role of private regulatory and self-help efforts.
4. Have an understanding of how emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices.

SYLLABUS

Unit I Introduction- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc.

Unit II Data explosion- Statistics and Lack of barriers in Collection and Distribution of Person-specific information. Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness.

Unit III Protection Models- Null-map, k-map, Wrong map Survey of techniques- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases. Computation systems for protecting delimited data- MinGen, Datafly, Mu-Argus, k-Similar, Protecting textual documents: Scrub.

Unit IV Technology, Policy, Privacy and Freedom- Medical privacy legislation, policies and best practices

Unit V Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.

REFERENCES:

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation, Auerbach Pub, 2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.

INFORMATION RISK MANAGEMENT
MTCS1105A

COURSE OBJECTIVES:

1. To understand the processes and measures that is used to manage risk to business critical information in an increasingly challenging cyber security environment.
2. Examine the way in which business and society make an assessment of, control and transfer risk.
3. To engage students in active discovery of risk management principles.

COURSE OUTCOMES: Upon completion, the student will be able to

1. Understand the structured process that is used to manage risk to information and data.
2. Realize what a business must, should or could do to address its risks.
3. Recognize the challenges unique to deploying the security measures.

SYLLABUS

Unit I

Information Risk Management: Definitions and relationships among different security components - threat agent, threat, vulnerability, risk, asset, exposure and safeguards; Governance models such as COSO and COBIT, ISO 27000 series of standards for setting up security programs.

Unit II

Risk analysis and management, policies, standards, baselines, guidelines and procedures as applied to Security Management program, Information strategy objectives.

Unit III

Security awareness and training. Security Architecture and Design: review of architectural frameworks (such as Zachman and SABSA), concepts of Security Models (such as Bell LaPadula, Biba and Brewer-Nash), vulnerabilities and threats to information systems (such as traditional on premise systems, web based multi-tiered applications, distributed systems and cloud based services), application of countermeasures to mitigate against those threats and security products evaluation.

Unit IV

Business Continuity and Disaster Recovery: Business Continuity Management (BCM) concepts, Business Impact Analysis, BC/ DR Strategy development.

Unit V

Backup and offsite facilities and types of drills and tests. An introduction to Operational Security and Physical security aspects.

REFERENCES:

1. Alan Calder and Steve G. Watkins, "Information Security Risk Management for IS027001 /IS027002", IT Governance Ltd, 2010.
2. Susan Snedaker, "Business Continuity and Disaster Recovery Planning for IT Professionals", Elsevier Science & Technology Books, 2007.

3. Harold F Tipton and Micki Krause, "Information Security Management Handbook", Volume 1, Sixth Edition, Auerbach Publications, 2003.
4. Andreas Von Grebmer, "Information and IT Risk Management in a Nutshell: A Pragmatic Approach to Information Security" Books on Demand, 2008.
5. Evan Wheeler, “Security Risk Management”, Elsevier, 2011.
6. Ian Tibble,"Security De-Engineering: Solving the Problems in Information Risk Management", CRC Press, 2012.

MOBILE NETWORK SECURITY
MTCS1105B

COURSE OBJECTIVES:

1. Creates Understanding about the basics of wireless technologies and security
2. Gain in - depth knowledge on wireless and mobile network security and its relation to the new security based protocols
3. Apply proactive and defensive measures to counter potential threats, attacks and intrusions.
4. Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks.

COURSE OUTCOMES: Upon completion, the student will be able to

1. Identify and investigate in-depth both early and contemporary threats to mobile and wireless networks security.
2. Apply proactive and defensive measures to deter and repel potential threats, attacks and intrusions.
3. Develop a clear view of integrated security environments consisting of both similar and diverse wireless access technologies and security architectures.

SYLLABUS

Unit I

Transmission Fundamentals: Antennas and Wave Propagation. Cellular Wireless networks, Third Generation Systems, 4G Long Term Evolutions, Signal Encoding Techniques, Spread Spectrum, Coding and Error Control, Multiple Access in Wireless Systems

Unit II

Satellite Networks, Wireless System Operations and Standards, Wi-Max an Ultra Wide Band technologies, Mobile IP and Wireless Access Protocol. Wireless LAN Technology, Wi-Fi and IEEE 802.11 Wireless LAN Standard, Blue-tooth and IEEE 802.15 standard.

Unit III

Threats to Wireless networks, ESM, ECM and ECCM, Proliferation of device and technologies, Practical aspects, Wireless availability, Privacy Challenges, Risks: Denial of Service, Insertion Attacks, Interception and monitoring wireless traffic, MIS configuration, Wireless Attacks, Surveillance, War Driving, Client-to-Client Hacking, Rogue Access Points, Jamming and Denial of Service.

Unit IV Authentication, Encryption/Decryption in GSM, Securing the WLAN, WEP Introduction, RC4 Encryption, Data Analysis, IV Collision, Key Extraction, WEP Cracking, WPA/ WPA2, AES, Access Point-Based Security Measures

Unit V Third- Party Security Methods, Funk's Steel-Belted Radius, WLAN Protection Enhancements, Blue-tooth Security Implementation, Security in Wi- MAX, UWB security, Satellite network security.

REFERENCES:

1. Kaveh Pahlavan and Prashant Krishnamurthy, "Principles of Wireless Networks",

Prentice Hall, 2006.
2. Cyrus Peikari and Seth Fogie, "Maximum Wireless Security" Sams, 2002.
3. Hideki lmai, Mohammad Ghulam Rahman and Kazukuni Kobari "Wireless Communications Security", Universal Personal Communications of Artech House, 2006.
4. Stallings William, "Wireless Communications and Networks" Second Edition, Pearson Education Ltd, 2009.
5. Jon Edney and William A. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Addison-Wesley Professional, 2003.

DATA MINING AND MACHINE LEARNING
MTCS1105C

COURSE OBJECTIVES:

1. Introduce students to the field of data mining and machine learning process.
2. Focuses on the study of techniques of clustering, classification, association finding, feature selection and visualization to real world data and determining whether a real world problem has a data mining solution
3. Introduce students to areas where data mining and machine learning can be applied to provide solutions to cyber security problems.

COURSE OUTCOMES: Upon completion, the student will be able to

1. Understand the basic data mining and machine learning algorithms.
2. Apply supervised and unsupervised learning algorithms to prediction problems.
3. Accurately evaluate the performance of algorithms, as well as formulate and test hypotheses.

SYLLABUS

Unit I

Introduction- Cybersecurity, Data Mining, Machine Learning. Classical Machine Learning Paradigms for Data Mining - Fundamentals of Supervised Machine Learning Methods, Popular Unsupervised Machine Learning Methods, Improvements on Machine Learning Methods, Challenges in Data Mining, Challenges in Machine Learning

Unit II

Supervised Learning for Misuse/Signature Detection - Machine Learning Applications in Misuse Detection- Rule-Based Signature Analysis, Artificial Neural Network, Support Vector Machine, Genetic Programming, Decision Tree and CART, Bayesian Network. Machine Learning for Anomaly Detection - Anomaly Detection - Machine Learning in Anomaly Detection Systems

Unit III

Machine Learning for Hybrid Detection - Hybrid Detection, Machine Learning in Hybrid Intrusion Detection Systems, Machine Learning Applications in Hybrid Intrusion Detection - Anomaly-Misuse sequence Detection System, Association Rules in Audit Data Analysis and Mining. Machine Learning for Scan Detection - Scan and Scan Detection, Machine Learning in Scan Detection, Machine-Learning Applications in Scan Detection, Other Scan Techniques

Unit IV

Machine Learning for Profiling Network Traffic - Network Traffic Profiling and Related Network Traffic Knowledge, Machine Learning and Network Traffic Profiling,

Unit V

Data Mining and Machine Learning Applications in Network Profiling. Emerging Challenges in Cyber security - Network Monitoring, Profiling, and Privacy Preservation, Challenges in Intrusion Detection.

REFERENCES:

1. Sumeet Dua and Xian Du, “Data Mining and Machine Learning in Cyber security” CRC press, Auerbach Publications 2011.
2. Christopher Westphal,” Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies” CRC Press, 2008.
3. Marcus A. Maloof, “Machine Learning and Data Mining for Computer Security: Methods and Applications” Springer Science & Business Media, 2006.
4. Jesus Mena,” Machine Learning Forensics for Law Enforcement, Security, and Intelligence”, CRC Press, 2011.
5. Ian H. Witten, Eibe Frank, Mark A. Hall,” Data Mining: Practical Machine Learning Tools and Techniques”, Elsevier, 2011.
6. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, MIT Press, 2016.
7. Tom M Mitchell, Machine Learning, McGraw Hill, 1997.
8. Jiawei Han, Micheline Kamber, Jian Pei, Data Mining: Concepts and Techniques, 3rd edition, 2011.
9. D. K. Bhattacharyya and J. K. Kalita, Network Anomaly Detection: A Machine Learning Perspective, 1st Edition, Chapman and Hall/CRC, 2013.
10. T. Dunning and E. Friedman, Practical Machine Learning - A New Look at Anomaly Detection, O'Reilly, 1st edition, 2014

CODING and INFORMATION THEORY
MTCS1105D

COURSE OBJECTIVES:

1. Covers information theory and coding within the context of modern digital communications applications.
2. To help students in quantify the notion of information in a mathematically and intuitively sound way.
3. Explaining how this quantitative measure of information may be used in order to build efficient solutions to multitudinous engineering problems

COURSE OUTCOMES: By the end of the course students will

1. Learn various coding methods.
2. Learn various error control methods.

SYLLABUS

Unit I

Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.

Unit II

Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDScodes.

Unit III

Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.

Unit IV

Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, Viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding.

Unit V

Trellis Coded Modulation - concept of coded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.

REFERENCES:

1. Lin S. and D. J. Costello, "Error Control Coding — Fundamentals and Applications", Second Edition, Pearson Education Inc., NJ., USA, 2004.

2. Shu Lin and Daniel J. Costello, "Error Control Coding", Second Edition, Prentice Hall, 1983. 3. E. R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New York, 1968.
3. R. E. Blahut, "Algebraic Codes for Data Transmission", Cambridge University Press Cambridge, UK, 2003.
4. Ranjan Bose, “Information theory, coding and cryptography”, Tata McGraw Hill, 2002.
5. Viterbi, “Information theory and coding”, McGraw Hill, 1982.
6. John G. Proakis, “Digital Communications”, 2nd Edition, McGraw Hill, 1989

INFORMATION SECURITY LAB
MTCSL1106

COURSE OBJECTIVES:

1. The main objective of this practical session is that students will get the exposure to various tools and programming methods using in information security.

COURSE OUTCOMES: By the completion of this laboratory session student

1. Will gain the knowledge on Perl and Shell scripting languages to implement various security attacks.
2. Will get the ideas in various ways to trace an attacker.
3. Will get the practical exposure to software firewall, port monitoring

SYLLABUS

Transmission, functions and security attacks implementation with Perl and shell scripting, Cryptographic algorithms and security protocols in C/C++, Firewall, Port monitoring.

The following programs should be implemented preferably on platform Windows/ Linux through Perl, shell scripting language and other standard utilities available with LINUX systems.

List of Experiments

1. Write a Perl script to concatenate ten messages and transmit to remote server
   a. Using arrays
   b. Without using arrays.
2. Write a Perl script to implement following functions:
   a. Stack functions
   b. File functions
   c. File text functions
   d. Directory functions
   e. Shift, unshift, Splice functions.
3. Write a Perl script to secure windows operating systems and web browser by disabling Hardware and software units
4. Write a Perl script to implement Mail bombing and trace the hacker.
5. Write a shell script to crack LINUX login passwords and trace it when breaking is happened.
6. Working with Sniffers for monitoring network communication (Ethereal)
7. Understanding of cryptographic algorithms and implementation of the same in C or C++.
8. Using open SSL for web server - browser communication
9. Using GNU PGP
10. Performance evaluation of various cryptographic algorithms
11. Using IP TABLES on Linux and setting the filtering rule
12. Configuring S/MIME for e-mail communication

13. Understanding the buffer overflow and format string attacks
14. Using NMAP for ports monitoring
15. Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication

Twelve experiments to complete mandatory

REFERENCES:

1. http://linuxcommand.org/man_pages/openssl1.html
2. http://www.openssl.org/docs/apps/openssl.html
3. http://www.queen.clara.net/pgp/art3.html
4. http://www.ccs.ornl.gov/~hongo/main/resources/contrib/gpg-howto/gpghowto.html
5. https://netfiles.uiuc.edu/ehowes/www/gpg/gpg-com-0.htm
6. http://www.ethereal.com/docs/user-guide

CYBER FORENSICS
MTCS1201

COURSE OBJECTIVES:

1. The main objective of the course is to introduce the students to bring awareness in crimes and tracing the attackers.
2. Define digital forensics from electronic media.
3. Describe how to prepare for digital evidence investigations and explain the differences between law enforcement agency and corporate investigations.
4. Explain the importance of maintaining professional conduct

COURSE OUTCOMES: Upon completion, the student will be able to

1. Utilize a systematic approach to computer investigations
2. Utilize various forensic tools to collect digital evidence.
3. Perform digital forensics analysis upon networks and network devices.
4. Perform web based investigations.

SYLLABUS

Unit I

Cyber forensics Introduction to Cyber forensics, Type of Computer Forensics Technology-Type of Vendor and Computer Forensics Services. Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases, Analyzing Malicious software

Unit II

Digital Evidence in Criminal Investigations. The Analog and Digital World, Training and Education in digital evidence, the digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies. Computer Forensics Evidence and Capture- Data Recovery Evidence collection and Data Seizure-Duplication and preservation of Digital Evidence-Computer image verification and Authentication

Unit III

Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics. Computer Forensics Analysis- Discovery of Electronic Evidence- Identification of data- Reconstructing Past events-networks

Unit IV

Countermeasure: Information warfare- Surveillance tool for Information warfare of the future-Advanced Computer Forensics.

Unit V

Cyber forensics tools and case studies

REFERENCES:

1. Understanding Cryptography: A Textbook for Students and Practitioners: Christofpaar, Jan Pelzl.
2. Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts Ali Jahangiri

3. Handbook of Digital and Multimedia Forensic Evidence [Paperback] John J. Barbara
4. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics)
5. Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk
6. Information warfare : Information warfare and security: (ACM Press) by Dorothy Elizabeth Robling Denning
7. Cyberwar and Information Warfare : Springer's by Daniel Ventre
8. Computer forensics: computer crime scene investigation, Volume 1 (Charles River Media, 2008) By John R. Vacca

SECURE CODING
MTCS1202

COURSE OBJECTIVES:

1. Students shall understand vulnerabilities in coding, identify, and remediate them.

COURSE OUTCOMES: Upon completion, the student will be able

1. To utilize a systematic approach to secure coding and web applications.

SYLLABUS

Unit I

Introduction, Security concepts, Security Architecture - Principles, coding in C and C++, String Characteristics, Common String Manipulation Errors, String Vulnerabilities, Process Memory Organization, Stack Smashing, Code Injection, Arc Injection, Notable Vulnerabilities. Pointer Subterfuge - Data Locations, Function Pointers, Data Pointers, Modifying the Instruction Pointer, Global Offset Table, The .dtors Section , Virtual Pointers, The at exit() and on exit() Functions, Thelongjmp() Function, Exception Handling

Unit II

Dynamic Memory Management - Common Dynamic Memory Management Errors, Doug Lea's Memory Allocator, RtlHeap, Integer Security - Integers, Integer Conversions, Integer Error Conditions, Integer Operations, Vulnerabilities, Non-exceptional Integer Logic Errors, Notable Vulnerabilities in Dynamic Memory Management and Integer Security.

Unit III

Formatted Output - Variadic Functions, Formatted Output Functions, Exploiting Formatted Output Functions, Stack Randomization. File I/O - Concurrency, Time of Check, Time of Use, Files as Locks and File Locking, File System Exploits.

Unit IV

Web Application, SQL Injection, Web Server–Related Vulnerabilities (XSS, XSRF, and Response Splitting), Web Client–Related Vulnerabilities (XSS), Use of Magic URLs,

Unit V

Predictable Cookies, and Hidden Form Fields:- Overview, CWE References, Affected Languages, Spotting the Pattern, Code Review, Testing Techniques, Redemption Steps.

REFERENCES:

1. Robert C. Seaford, "Secure Coding in C and C++", Addison-Wesley Professional, 2005.
2. Mark G. Graff, Kenneth R. van Wyk, "Secure Coding: Principles & Practices" O'Reilly, 2003
3. Michael Howard, David LeBlanc, and John Viega, "24 DEADLY SINS OF SOFTWARE SECURITY" McGraw-Hill Companies, 2010.
4. James A. Whittaker and Herbert H. Thompson, "How to Break Software Security",
5. Addison Wesley, 2003. John C. Mitchell and Krzysztof Apt, "Concepts in Programming Languages", Cambridge University Press, 2001.

ETHICAL HACKING
MTCS1203

COURSE OBJECTIVES:

1. To understand steps in ethical hacking.
2. To render all the techniques used for penetration testing for performing security auditing.
3. To transform the internet security industry by infusing professionalism and efficiency.

COURSE OUTCOMES: By the end of the course students will

1. Learn various hacking methods.
2. Perform system security vulnerability testing.
3. Perform system vulnerability exploit attacks.
4. Produce a security assessment report
5. Learn various issues related to hacking.

SYLLABUS

Unit I

Introduction, Casing the establishment- What is foot printing Internet Foot printing, Scanning- Enumeration - basic banner grabbing, Enumerating Common Network services. Case study- Network security monitoring securing permission. Securing file and folder permission using the encrypting file system.

Unit II

Dial-up, PBX, Voicemail, and VPN hacking - Preparing to dial up. War- Dialing. Brute-Force Scripting. Voice mail hacking. VPN hacking. Network Devices – Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability. Detecting Layer 2 Media.

Unit III

Wireless Hacking - Wireless Foot printing. Wireless Scanning and Enumeration. Gaining Access. Tools that exploiting WEP Weakness. Denial of Services Attacks. Firewalls- Firewalls landscape Firewall Identification-Scanning Through firewalls- packet Filtering- Application Proxy Vulnerabilities. Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. UNIX and Windows DoS

Unit IV

Remote Control Insecurities - Discovering Remote Control Software. Connection. Weakness. VNC. Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans.

Unit V

Cryptography. Subverting the systems Environment. Social Engineering. Web Hacking. Web server hacking web application hacking. Hacking the internet User - Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global Counter measures to Internet User Hacking.

REFERENCES

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.

2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.
3. Michael T. Simpson, “Ethical Hacking and Network Defense”, Cengage Learning, New Delhi, 2012.
4. Kevin Beaver, “Hacking for Dummies”, Wiley Publication, India, 2007.
5. Ankit Fadia, “Unofficial Guide to Ethical Hacking”, Macmillan Company, New Delhi, 2001.

DIGITAL WATERMARKING
MTCS1204A

COURSE OBJECTIVES:

1. To make the students aware of the basic mathematical concept behind watermarking theory and its main applications.
2. Provides the knowledge about the applications of watermarking techniques used and teaches about Watermark security and cryptographic methods used.

COURSE OUTCOMES: Upon completion, the Students will be able to

1. Understand and identify digital watermarking from other related fields.
2. Explain different types of watermarking applications and watermarking frameworks.
3. Design digital watermarking systems according to application domains
4. Analyze the different type of watermarking security issues.

SYLLABUS

Unit I

Watermarking host signals: Image, Video, and Audio. Multimedia compression and decompression, Lossless compression, Models watermarking, Communication-based models of watermarking, Geometric models of watermarking, modeling watermark detection by correlation

Unit II Basic message coding, Mapping message in message vectors, Error correction coding, detecting multi-symbol watermarks, Watermarking with side information, Information embedding, informed coding.

Unit III Structured dirty-paper codes, Analyzing errors, Message errors, ROC curves, The effect of whitening on error rates, Analysis of normalized correlation, Using perceptual mode, Evaluating perceptual impact of watermarks.

Unit IV General forms of perceptual model, Perceptual adaptive watermarking, and Robust watermarking

Unit V

Watermark security, Watermark security and cryptography, Content authentication, Exact authentication, Selective, authentication, Localization, Restoration.

REFERENCES

1. Cox I., M. Miller, J. Bloom, J. Fridrich and T Kalker, "Digit Watermarking and Steganography", Second Edition, Morg Kaufmann Publishers, 2008.
2. E. Cole, R. Krutz, and J. Conley, Network Security Bible, Wiley-Dreamtech, 2005.
3. W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003.
4. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3/e, Pearson Education, 2003.
5. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.

IDENTITY and ACCESS MANAGEMENT
MTCS1204B

COURSE OBJECTIVES:

1. To provide basics of Identity and Access Management and its concepts
2. Understand multi-factor Authentication to configure strong authentication for users at sign-in.
3. To Manage and secure web applications with OAuth 2.0.

COURSE OUTCOMES: Students should be able to

1. Understand the semantics and principles behind terms and concepts in Identity & Access Management
2. Understand the players and building blocks of Identity Management frameworks
3. Identify different components of IAM in a given implementation.
4. Implement secure networking solutions using OAuth 2.0.

SYLLABUS

Unit I

Introduction to IAM, Types of business cases for IAM, IAM Framework, IAM Capability maturity framework, Differences from traditional IT. Implementation Methodology and Approach - Plan and Diagnose, Define and Design, Develop and Deliver, Adopt and Sustain, IAM Implementation Toolkit, Life cycle for Identity and Access - Request, Approve, Create, Grant, Delete, Revoke, Request system, Workflow system, Provisioning system, HR system, IAM Data Management.

Unit II

Identity and Access Intelligence - Risk based approach to IAM, Roles and Rules - RBAC Key concepts, Rules and enforcement, RBAC Model and Access management, RBAC implementation considerations. Authentication methods - Cloud IAM identities, B2C and B2E, MFA, Passwords and API keys, Shared IDs, Federated identity, Instance Metadata, Identity documents, Secrets management, LDAP - basics, LDIF, LDAP security, LSC, SAML - assertions, protocols, bindings, profiles, OAuth - roles, tokens, grants, Overview of OpenID and connection chains.

Unit III

Strong authentication - OTPs, HOTP, TOTP, Mutual SSL/TLS, FIDO, User managed access - UMA Grant, Federated authorization. Implementing identity management - SSO, Credential management systems, integrating identify services, Managing sessions, AAA protocols.

Unit IV

Need of OAuth 2.0, Roles, Authorisation flow, Tokens, Clients and endpoints, Security considerations, Additional security with SAML.

Unit V

Case study: OAuth 2.0 for web server applications, Client side applications, Mobile applications.

REFERENCES:

1. Ertem Osmanoglu, “Identity and Access Management: Business Performance Through Connected Intelligence”, Elsevier Syngress 2014
2. Mike Chapple, James Michael Stewart, Darril Gibson, “(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide”, Wiley Sybex, 2018
3. Chris Dotson, “Practical Cloud Security: A Guide for Secure Design and Deployment”, O’Reilly 2019
4. Michael Schwartz, Maciej Machulak, “Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software”, APress, 2018
5. Steve Martinelli, Henry Nash, Brad Topol, “Identity, Authentication, and Access Management in OpenStack”, O’Reilly, 2016
6. Martin Spasovski, “OAuth 2.0 Identity and Access Management Patterns”, Packt Publishing.

CRYPTANALYSIS
MTCS1204C

COURSE OBJECTIVES:

1. To enable learner to understand various risks, threats and vulnerabilities in a system. 2. Also gives security awareness and countermeasures to mitigate various risks, threats and vulnerabilities in a system.

COURSE OUTCOMES:

1. Students will be able to design and analyze the security architecture designed for any system.
2. Students will be able to identify the security flows in any multi-tiered applications, distributed systems and cloud based services and mitigate it.

SYLLABUS

Unit I

Cryptanalysis of classical ciphers: Vigenere cipher, Affine cipher, Hill cipher, Linear Shift Register Random Bit Generator: Berlekamp- Massey algorithm for the cryptanalysis of LFSR, Correlation attack on LFSR based stream ciphers, Cryptanalysis of ORYX, Fast algebraic attack.

Unit II

Cryptanalysis of Block Ciphers: Man in the middle attack double DES, Linear and Differential cryptanalysis. Algorithmic Number Theory: Stein's binary greatest common divisor algorithm, Shanks Tonelli algorithm for square roots in Fp, Stein's greatest common divisor algorithm for polynomials.

Unit III

Algorithms for DLP: Pollard Rho method for DLP, Shank's baby step Giant step algorithm for DLP Silver-Pohling-Hellman algorithm for DLP, Index calculus for DLP algorithms: Trial division, Fermat method, Legendre-congruence, Continued fraction method, Pollard Rho method, Elliptic curve method, Quadratic sieve.

Unit IV

Lattice based Cryptanalysis. Direct attacks using lattice reduction, Coppersmith's attacks. Attacks on cryptographic hash functions: Birth day paradox, Birthday for paradox for multi collisions,

Unit V

Birthday paradox in two groups, Application of Birthday paradox in Hash functions, Multicollisions attack on hash functions.

REFERENCES:

1. Antoine Joux, "Algorithmic Cryptanalysis", Chapman & Hall/CRC Cryptography and Series, 2009.
2. Song Y Yang, "Number Theory for Computing", Second Edition,SpringerVerlag, 2010.
3. Gregory V. Bard, "Algebraic Cryptanalysis", Springer, 2009.
4. Hoffstein, Jeffray, Pipher, Jill and Silverman, "An Introduction to Mathematical Cryptography",Springer, 2010. APJ

STORAGE MANAGEMENT and SECURITY
MTCS1204D

COURSE OBJECTIVES:

1. To enable students to understand, explore and acquire a critical understanding about managing information in storage system and effective security implementation on the corresponding platforms.

COURSE OUTCOMES:

1. Introduce the students to various types of storage systems available and understand the importance of storage networking.
2. To explain the basic information storage and retrieval concepts in a storage system.
3. To understand the issues those are specific to efficient information retrieval.
4. To implement security issues while storing and retrieving information.

SYLLABUS

Unit I

Introduction, History: computing, networking, storage, Need for storage networking, SAN, NAS, SAN/NAS Convergence, Distributed Storage Systems, Mainframe/proprietary vs. open storage, Storage Industry Organizations and Major Vendors Market, Storage networking strategy (SAN/NAS) Technology

Unit II

Storage components, Data organization: File vs. Block, Object; Data store; Searchable models; Storage Devices (including fixed content storage devices), File Systems, Volume Managers, RAID systems, Caches, Prefetching. Error management: Disk Error Management, RAID Error Management, Distributed Systems Error Management

Unit III

Large Storage Systems: Google FS/Big Table, Cloud/Web - based systems (Amazon S3), FS+DB convergence, Programming models: Hadoop. Archival Systems: Content addressable storage, Backup: server less, LAN free, LAN Replication issues, Storage Security, Storage Management, Device Management, NAS Management, Virtualization, Virtualization solutions, SAN Management: Storage Provisioning, Storage Migration

Unit IV

Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking.

Unit V

Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice.

REFERENCES:

1. EMC Education Services “Information Storage and Management: Storing, Managing, and Protecting Digital Information”, John Wiley & Sons, 2010.
2. John Chirillo, ScottBlaul, “Storage Security: Protecting SANs, NAS and DAS”, Wiley,

2003.
3. David Alexander, Amanda French, Dave Sutton “Information Security Management Principles” BCS, The Chartered Institute, 2008.
4. Gerald J. Kowalski, Mark T. Maybury, “Information Storage and Retrieval Systems: Theory and Implementation, Springer, 2000.
5. Foster Stockwell, “A history of information storage and retrieval” McFarland, 2001.
6. R. Kelly Rainer, Casey G. Cegielski, “Introduction to Information Systems: Enabling and Transforming Business, John Wiley & Sons, 2010.

CYBER LAWS and SECURITY POLICIES
MTCS1205A

COURSE OBJECTIVES:

1. To enable learner to understand, explore, and acquire a critical understanding cyber law.
2. Develop competencies for dealing with frauds and deceptions (confidence tricks, cams) and other cybercrimes for example, child pornography etc.

COURSE OUTCOMES: Learner will be able to

1. Be conversant with the social and Intellectual Property issues emerging from Cyberspace.
2. Explore the legal and Policy developments in various countries to regulate Cyberspace
3. Develop the understanding of relationship between commerce and cyberspace
4. Gain in-depth knowledge of Information Technology Act and legal framework of Right to Privacy, Data Security and Data Protection.

SYLLABUS

Unit I

Emergence of Cyber space. Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace-Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access..

Unit II

Overview of IT Act 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication.

Unit III

Patent Law, Trademark Law, Copyright, Software – Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution , Online Dispute Resolution (ODR).

Unit IV

Evolution and development in E-commerce, paper vs paper less contracts E-Commerce models- B2B, B2C, E security. Application area: Business, taxation, electronic payments, supply chain, EDI, E-markets, Emerging Trends.

Unit V

Case Study On Cyber Crimes: Harassment Via E-Mails, Email Spoofing (Online A Method Of Sending E-Mail Using A False Name Or E-Mail Address To Make It Appear That The E-Mail Comes From Somebody Other Than The True Sender, Cyber Pornography

(Exm.MMS),Cyber-Stalking.

REFERENCES:

1. K.Kumar," Cyber Laws: Intellectual property & E Commerce, Security", 1st Edition, Dominant Publisher, 2011.
2. Rodney D. Ryder, "Guide to Cyber Laws", Second Edition, Wadhwa And Company, New Delhi, 2007.
3. Information Security policy &implementation Issues, NIIT, PHI.
4. Vakul Sharma, "Handbook of Cyber Laws" Macmillan India Ltd, 2nd Edition, PHI, 2003. 5. Justice Yatindra Singh, "Cyber Laws", Universal Law Publishing, 1st Edition, New Delhi, 2003.
5. Sharma, S.R., "Dimensions Of Cyber Crime", Annual Publications Pvt. Ltd., 1st Edition, 2004.
6. Augastine, Paul T.," Cyber Crimes and Legal Issues", Crecent Publishing Corporation, 2007.

DISASTER RECOVERY
MTCS1205B

COURSE OBJECTIVES:

1. Understanding of the roles of the various phases of disaster management and issues concerning planning and policies in those phases.
2. Understanding of comprehensive emergency management from a planning and policy Perspective, role of federal, state, and local governments in disaster planning and policies.
3. Knowledge of mitigation planning and policy strategies.
4. Understanding of comprehensive emergency management and related plans.
5. Understanding of the factors that give rise to disaster vulnerabilities (e.g. natural, physical, social, economic, policies, and governance, factors that give rise to differential vulnerabilities and levels of community resilience
6. Data, methods, tools, and geospatial techniques (including GIS) that can enhance vulnerability assessments and knowledge building.

COURSE OUTCOMES: After completing this course, you will be able to:

1. Affirm the usefulness of integrating management principles in disaster mitigation work
2. Distinguish between the different approaches needed to manage pre- during and post-disaster periods
3. Explain the process of risk management

SYLLABUS

Unit I

Introduction: Hazards and Disasters: Planning and Policies, Disaster Mitigation Policies and Planning. Mitigation Planning and Policy Strategies: Local, State, and Federal Level.

Unit II

Measuring and Mapping Vulnerability, Social, Economic, and Political Vulnerabilities, Community Resilience, Emergency Management Planning Communication and Risk Management (Policies and Plans)

Unit III

Disaster Response: Planning for Response, Supporting Emergency Response Operations using Geospatial Technologies Collaboration and Coordination in Emergency Response Planning & Management

Unit IV

Disaster Recovery and Rebuilding, Long-term recovery

Unit V

Post Disaster Recovery Planning and Reconstruction, Post-Disaster Housing Planning.

REFERENCES:

1. Waugh, William L. Jr. (2000). Living with Hazards, Dealing with Disasters: An Introduction to Emergency Management. Armonk, New York: M.E. Sharpe.
2. Burby, Raymond (1998). Cooperating with Nature: Confronting natural hazards with land use planning for sustainable communities. Joseph Henry Press.
3. Birkland, Thomas. 2006. Lessons of Disaster: Policy Change after Catastrophic Events. Washington, D.C.: Georgetown University Press.
4. Drabek, Thomas. 2010. The Human Side of Disaster. Taylor and Francis

IT GOVERNANCE
MTCS1205C

COURSE OBJECTIVES:

1. Definition, establishment, and management of a framework for the governance of enterprise IT in alignment with the mission, vision and values of the enterprise
2. Enterprise objectives through the integration and alignment of IT strategic plans with enterprise strategic plans.
3. Performance measurement are established, evaluated and the reporting of progress to stakeholders
4. IT risk management is in alignment with the enterprise risk management (ERM) framework

COURSE OUTCOMES: After learning this course, students will be able to

1. Identify the requirements and objectives for the framework for governance of enterprise IT.
2. Understand frameworks like COBIT, ITIL, and COSO for governance.
3. Apply Service Oriented Architectures for proper governance.
4. Understand the concept of KPIs and their application in planning.
5. Apply continuity planning for risk mitigation.

SYLLABUS

Unit I

Strategies and Models for IT Governance - IT Governance explained, Role of IT Governance, Structures, Processes, and Relational Mechanisms, Process measurement, Implementation Status, Sarbanes - Oxley Rules. COBIT Framework, Control objectives, Management guidelines, Maturity Models, Adaptation.

Unit II

Service Oriented Architecture - SOA applications and Service-driven IT applications, SOA Governance, Internal control, Risks, SOA Implementation blueprint, SOA and IT governance, Operation-level agreement, Service-level agreement, Analysis models - SWOT, BCG Matrix.

Unit III

IT Governance and COSO internal controls, ITIL- fundamentals, service strategy components, service design, service translation management, service operation process, best practices. COSO ERM - definitions and objectives, ERM framework, other dimensions. Key Performance Indicators - Four types of performance measures, 10/80/10 Rule, Importance of timely measurement, Relation between Critical Success Factors and KPIs.

Unit IV

IT Continuity management - Effective IT Security environment, IT continuity planning, Business continuity plan and IT governance.

Unit V

IT Governance in Practice: Case Studies - KBC, AGF Belgium, Huntsman, Sidemar Arcelor.

REFERENCES:

1. Alan Calder, IT Governance: A Pocket Guide, IT Governance publishing
2. David Clifford, ISO/IEC 20000: An Introduction to the global standard for service management, IT Governance Publishing, 2011.

IOT SECURITY
MTCS1205D

COURSE OBJECTIVES:

1. To give an overview of security in IoT system in security.
2. To provide knowledge about security risks IoT domain faces and countermeasures available for the known issues

COURSE OUTCOMES: On successful completion of this course the student will be able to

1. Understand IoT general models and security challenges
2. Recognize IoT security and vulnerability threats
3. Understand different IoT protocols and their security measures.
4. Interpret how to secure an IoT environment
5. Interpret different types of attacks

SYLLABUS

Unit I

Fundamentals, Architecture of IoTs, Sensing, Actuation; Basics of networking IoT devices; Interoperability in IoT; IoT design methodology, Domain specific IoTs: Home automation, Agriculture, Smart cities; IoT enabling technologies-WSNs, Cloud computing, Big data analytics, Embedded systems; WSN and IoT.

Unit II

IoT protocols-Link layer protocols, Network layer protocols IPV4, IPV6, 6LoWPAN, Transport layer protocols , Infrastructure-IPv6 -LowPAN , Identification-Electronic Product Code -uCode, Transport-Bluetooth - LPWAN, Data -MQTT – CoAP.

Unit III

IoT Security Requirements -Data Confidentiality -Data Encryption -Data Authentication - Secured Access Control –IoT-Vulnerabilities – Secret-Key Authentication/Authorization for Smart Devices - Constrained System Resources -Device Heterogeneity -Fixed Firmware. IoT Attacks -Side-channel Attacks -Reconnaissance -Spoofing -Sniffing -Neighbour -Discovery - Rogue Devices-Man-in-Middle

Unit IV

Threat modelling in an IoT system; Secure IoT system implementation life cycle, Identity and access management solutions for IoT- IoT life cycle

Unit V

Authentication credentials, Authorization and access control; Identity relationship management and context in IoT

REFERENCES:

1. Fei HU, “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations”, CRC Press, 2016.
2. Russell, Brian and Drew Van Duren, “Practical Internet of Things Security”, Packt Publishing, 2016.
3. Ollie Whitehouse, “Security of Things: An Implementers' Guide to Cyber-Security for

Internet of Things Devices and Beyond", NCC Group, 2014.

4. "Internet of Things: A Hands-on Approach", by Arshdeep Bahga and Vijay Madisetti (Universities Press).
5. Online Resources https://www.postscapes.com/internet-of-things-protocols/ https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities

ETHICAL HACKING and DIGITAL FORENSIC TOOLS LAB
MTCSL1206

COURSE OBJECTIVES:

1. The main objective of this practical session is that students will get the exposure to various hacking and forensic tools.

COURSE OUTCOMES: By the completion of this laboratory session Student

1. Will gain the knowledge to implement various security attacks.
2. Will get the ideas in various ways to trace an attacker.
3. Will get the practical exposure to forensic tools.

Experiment List

Part A: Ethical hacking

1. Working with Trojans, Backdoors and sniffer for monitoring network communication
2. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.
3. Penetration Testing and justification of penetration testing through risk analysis
4. Password guessing and Password Cracking.
5. Malware – Keylogger, Trojans, Keylogger countermeasures
6. Understanding Data Packet Sniffers
7. Windows Hacking – NT LAN Manager, Secure 1 password recovery
8. Implementing Web Data Extractor and Web site watcher.
9. Email Tracking.
10. Configuring Software and Hardware firewall.
11. Firewalls, Packet Analyzers, Filtering methods.

Part B: Exposure on Digital Forensic tools

1. Backup the images file from RAM using Helix3pro tool and show the analysis.
2. Introduction to Santhoku Linux operating system and features extraction
3. Using Santoku operating system generates the analysis document for any attacked file from by taking backup image from RAM.
4. Using Santoku operating system generates the attacker injected viewing java files.
5. Using Santoku operating system shows how attackers opened various Firefox URL‟s and pdf document JavaScript files and show the analysis.
6. Using Santoku operating System files show how an attacker connected to the various network inodes by the specific process.
7. Using exiftool (-k) generate the any picture hardware and software.
8. Using deft_6.1 tool recover the attacker browsing data from any computer.
9. Using Courier tool Extract a hacker secret bitmap image hidden data.
10. Using sg (Steganography) cyber Forensic tool hide a message in a document or any file.
11. Using sg cyber Forensic tool unhide a message in a document or any file.
12. Using Helix3pro tool show how to extract deleted data file from hard disk or usb device.
13. Using Ghostnet tool hide a message into a picture or any image file.
14. Using kgbkey logger tool record or generate an document what a user working on system
15. Using pinpoint metaviewr tool extract a metadata from system or from image file.
16. Using Bulk Extractor tool extract information from windows file system.

SEMINAR
MTCSS1207

COURSE OBJECTIVES:

1. To introduce the students to research, make them understand research papers and prepare presentation material.
2. To understand cutting edge technology in the chosen area
3. To improve oral communication skills through presentation.
4. To prepare original technical write up on the presentation.

COURSE OUTCOMES: After completion of course, students will be able to:

1. Develop skills in doing literature survey, technical presentation and report preparation
2. Improve the proficiency in English
3. Improve presentation skills
4. Improve analytical and reasoning ability
5. Improve technical writing skills

SYLLABUS

The aim of this course is to introduce the student to research, and to acquaint him with the process of presenting his work through seminars and technical reports. Students have to register for the seminar and select a topic in consultation with any faculty member offering courses for the programme. The student is expected to do an extensive literature survey and analysis in an area related to the area of specialization. The study should preferably result in design ideas, designs, algorithms, and theoretical contributions in the form of theorems and proofs, new methods of proof, new techniques or heuristics with analytical studies, implementations and analysis of results.

The presentation shall be of 30 minutes duration and a committee with the Head of the Department as the chairman and two faculty members from the department as members shall evaluate the seminar based on the coverage of the topic, presentation and ability to answer the questions put forward by the committee.

Students shall individually prepare and submit a seminar report based on experimental study / industrial training on the corresponding topic, in the prescribed format given by the Department. The reference shall include standard journals (ACM/ IEEE), conference proceedings and equivalent documents, reputed magazines and textbooks, technical reports and web based material, approved by the supervisor. The references shall be incorporated in the report following IEEE standards reflecting the state-of-the-art in the topic selected.

PROJECT PHASE-I
MTCS2102

COURSE OBJECTIVES:

1. To undertake research in an area related to the program of study.
2. To acquaint students to literature survey and design of a project.

COURSE OUTCOMES: Student should be able to

1. Identify the topic, objectives and methodology to carry out the project.
2. Finalize the project plan for their course project.

SYLLABUS

Every student should carry out project, under the supervision of a Supervisor(s). The project work shall commence in the third semester and shall be completed by the end of fourth semester. Candidates are required to undertake a suitable research project work; the topic shall be approved by a committee constituted by the Head of the concerned Department. Every student will be required to present the topic at the beginning of the Phase-I to illustrate the scope of the work and to finalize the topic. The third semester includes the design phase and the fourth semester includes the implementation and final thesis submission.

The student should report the status of their progress weekly to the concerned supervisor. Students should submit the project report at the end of the respective semesters, on dates announced by the college/department. Project evaluation will be based on presentations, viva voce, demonstration, review reports, design reports and final thesis. Progress of the project work is to be evaluated at the end of the third semester. For this a committee headed by the head of the department with two other faculty members in the area of the project, of which one shall be the project supervisor. If the project is done outside the college, the external supervisor associated with the student will also be a member of the committee.

Normally students are expected to do the project within the college. However they are permitted to do the project in an industry or in a government research institute under a qualified supervisor from that organization. This is only possible in the fourth semester and the topic of investigation should be in line with the project part planned in the 3rd semester.

PROJECT PHASE-II
MTCS2202

COURSE OBJECTIVES:

1. To undertake research in an area related to the program of study.
2. To enable students to implement and deploy a system and carry out performance analysis.

COURSE OUTCOMES: Student should be able to

1. Get a good exposure to a domain of interest.
2. Get a good domain and experience to pursue future research activities.

SYLLABUS

The Phase II work shall be based on the work in Phase I. Normally students are expected to do the project within the college. However they are permitted to do the project in an industry or in a government research institute under a qualified supervisor from that organization; the topic of investigation should be in line with the project part planned in the 3rd semester. Student should apply for this through the project supervisor indicating the reason for this well in advance, preferably at the beginning of the 3rd semester. This application is to be vetted by a departmental committee constituted for the same by the Principal and based on the recommendation of the committee the student is permitted to do the project outside the college. The same committee should ensure the progress of the work periodically and keep a record of this. The application for this shall include the following:- Topic of the Project, Project work plan in the 3rdSemester, Reason for doing the project outside, Institution/Organization where the project is to be done, External Supervisor Name, Designation, Qualification and Experience, Letter of consent of the External Supervisor as well as from the organization.

The concerned head of the department shall be the chairman of this committee. It shall have two senior faculty members from the same department, project supervisor and the external supervisor, if any, of the student and an external expert either from an academic/R&D organization or from Industry as members. Final project grading shall take into account the progress evaluation done in the third semester and the project evaluation in the fourth semester. If the quantum of work done by the candidate is found to be unsatisfactory, the committee may extend the duration of the project up to one more semester, giving reasons for this in writing to the student. Normally further extension will not be granted and there shall be no provision to register again for the project.

Students are required to publish their work in reputed national/ International Journals/ Conference Proceedings etc. which will carry weightage in final marks.