HINDUSTAN
INSTITUTE OF TECHNOLOGY & SCIENCE
(DEEMED TO BE UNIVERSITY)

CURRICULUM & SYLLABUS

2018-19

for

M. Tech.

Information Technology

Specialization in Cyber Security

DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING SCIENCES

HINDUSTAN INSTITUTE OF TECHNOLOGY AND SCIENCE
DEPARTMENT OF INFORMATION TECHNOLOGY
M.Tech. (INFORMATION TECHNOLOGY)
CURRICULUM 2018-2019

HINDUSTAN INSTITUTE OF TECHNOLOGY & SCIENCE
VISION AND MISSION

MOTTO

"TO MAKE EVERY MAN A SUCCESS AND NO MAN A FAILURE."

VISION

To be an International Institute of Excellence, providing a conducive environment for education with a strong emphasis on innovation, quality, research and strategic partnership blended with values and commitment to society.

MISSION

- To create an ecosystem for learning and world class research.
- To nurture a sense of creativity and innovation.
- To instill highest ethical standards and values with a sense of professionalism.
- To take up activities for the development of Society.
- To develop national and international collaboration and strategic partnership with industry and institutes of excellence.
- To enable graduates to become future leaders and innovators.

VALUE STATEMENT

- Integrity, Innovation, Internationalization

DEPARTMENT OF INFORMATION TECHNOLOGY
VISION AND MISSION

VISION

To be a globally renowned academic department for quality education and research in the field of Information Technology with ethical values and social commitment.

MISSION

M1: To impart comprehensive technical education to produce highly competent IT professionals and entrepreneurs.

M2: To provide an academic environment for state of the art research with ethical standards.

M3: To conduct knowledge transfer programs to enhance the technical knowledge in the field of Information Technology.

PROGRAMME EDUCATIONAL OBJECTIVES (PEO)

The program is expected to enable the students to

PEO I	Demonstrate comprehensive knowledge in IT solution development leading to excellence in professional career and/or higher education including research.
PEO II	Provide solutions making use of the knowledge gained in Artificial Intelligence, Cloud Computing, Big Data, Cyber Security and Communication.
PEO III	Adapt themselves to continuously changing technologies to develop innovative applications with ethical and social commitment.

PROGRAM OUTCOMES (ALIGNED WITH GRADUATE ATTRIBUTES) (PO)

At the end of this program, graduates will be able to

PO1	**Scholarship of knowledge** Acquire in-depth knowledge of specific discipline or professional area, including wider and global perspective, with an synthesize existing and new knowledge, and integration of the same for enhancement of knowledge.
PO2	**Critical Thinking** Analyze complex engineering problems critically, apply independent judgment for synthesizing information to make intellectual and/or creative advances for conducting research in a wider theoretical, practical and policy context.
PO3	**Problem Solving** Think laterally and originally, conceptualize and solve engineering problems, evaluate a wide range of potential solutions for those problems and arrive at feasible, optimal solutions after considering public health and safety, cultural, societal and environmental factors in the core areas of expertise.
PO4	**Research Skill** Extract information pertinent to unfamiliar problems through literature survey and experiments, apply appropriate research methodologies, techniques and tools, design, conduct experiments, analyze and interpret data, demonstrate higher order skill and view things in a broader perspective, contribute individually/in group(s) to the development of scientific/technological knowledge in one or more domains of engineering.

PO5 **Usage of modern tools** Create, select, learn and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and modeling, to complex engineering activities with an understanding of the limitations.

PO6 **Collaborative and Multidisciplinary work** Possess knowledge and understanding of group dynamics, recognize opportunities and contribute positively to collaborative-multidisciplinary scientific research, demonstrate a capacity for self-management and teamwork, decision-making based on open-mindedness, objectivity and rational analysis in order to achieve common goals and further the learning of themselves as well as others.

PO7 **Project Management and Finance** Demonstrate knowledge and understanding of engineering and management principles and apply the same to one's own work, as a member and leader in a team, manage projects efficiently in respective disciplines and multidisciplinary environments after consideration of economical and financial factors.

PO8 **Communication** Communicate with the engineering community, and with society at large, regarding complex engineering activities confidently and effectively, such as, being able to comprehend and write effective reports and design documentation by adhering to appropriate standards, make effective presentations, and give and receive clear instructions.

PO9 **Life-long Learning** Recognize the need for, and have the preparation and ability to engage in life-long learning independently, with a high level of enthusiasm and commitment to improve knowledge and competence continuously.

PO10 **Ethical Practices and Social Responsibility** Acquire professional and intellectual integrity, professional code of conduct, ethics of research and scholarship, consideration of the impact of research outcomes on professional practices and an understanding of responsibility to contribute to the community for sustainable development of society.

PO11 **Independent and Reflective Learning** Observe and examine critically the outcomes of one's actions and make corrective measures subsequently, and learn from mistakes without depending on external feedback.

SEMESTER I								
SL. NO	**COURSE**	**COURSE CODE**	**COURSE TITLE**	**L**	**T**	**P**	**C**	**TCH**
1	BS	MAA3706	Statistics for Computer Science	3	0	2	4	5
2	PC	CSA3701	Advanced Data Structures and Algorithms	2	0	2	3	4
3	PC	CSA3702	Machine Learning	2	0	2	3	4
4	PE	ITA****	Department Elective – I	3	0	0	3	3
5	PE	ITA****	Department Elective – II	3	0	0	3	3
6	HS	ZZZ3715	Research Methodology & IPR	2	0	0	2	2
PRACTICAL								
7	PE	ITA3780	Mini project	0	0	6	2	6
		Total Credits					20	27

- Research Methodology & IPR is a Compulsory Course.
- Professional Core and Basic Science Papers are common to M. Tech. CSE and M.Tech. IT

SEMESTER II								
SL. NO	**COURSE**	**COURSE CODE**	**COURSE TITLE**	**L**	**T**	**P**	**C**	**TCH**
1	PC	ITA3701	Integrated Software Engineering Methodology	2	0	2	4	4
2	PC	CSA3703	Advanced Operating Systems	2	0	2	3	4
3	PC	ITA3702	Cryptography and Network Security	2	0	2	3	4
4	PE	ITA****	MOOC Course	3	0	0	3	3
5	PE	ITA****	Department ELE III	3	0	0	3	3
6	OE		Open Elective	2	0	0	2	2
PRACTICAL								
7	PC	ITA3796	Seminar	0	0	3	2	3
		Total Credits					20	23

SEMESTER III								
SL. NO	**COURSE**	**COURSE CODE**	**COURSE TITLE**	**L**	**T**	**P**	**C**	**TCH**
1	PE	ITA****	Department ELE IV	3	0	0	3	3
PRACTICAL								
2	PC	ITA3897 ITA3781	Internship / Mini Project	0	0	6	2	6
3	PC	ITA3898	Project Phase –I	0	0	16	8	16
		Total Credits					13	25

*Internship to be undergone during the vacation between 2nd and 3rd semesters

SEMESTER IV								
SL. NO	**COURSE**	**COURSE CODE**	**COURSE TITLE**	**L**	**T**	**P**	**C**	**TCH**

PRACTICAL								
1	PC	ITA3899	Project Phase –II	0	0	24	12	24
		Total Credits					12	24

TOTAL CREDITS: 65

DEPARTMENT ELECTIVE I for Cyber Security Specialization (SEMESTER-I)								
SL. NO	**COURSE CODE**	**COURSE CATEGORY**	**COURSE TITLE**	**L**	**T**	**P**	**C**	**TCH**
1	ITB3721	PE	Concepts of Ethical Hacking	3	0	0	3	3
2	ITB3722	PE	Cyber Crime & Security	3	0	0	3	3
3	CSA3723	PE	Information Security Architecture	2	0	2	3	2

DEPARTMENT ELECTIVE II for Cyber Security Specialization (SEMESTER-I)								
SL. NO	**COURSE CODE**	**COURSE CATEGORY**	**COURSE TITLE**	**L**	**T**	**P**	**C**	**TCH**
1	ITB3723	PE	Ethical Hacking and Systems Defense	3	0	0	3	3
2	ITB3724	PE	Ethical Hacking and Digital Forensics	3	0	0	3	3
3	ITB3725	PE	Mobile and Digital Forensics	3	0	0	3	3

DEPARTMENT ELECTIVE III for Cyber Security Specialization (SEMESTER-II)								
SL. NO	**COURSE CODE**	**COURSE CATEGORY**	**COURSE TITLE**	**L**	**T**	**P**	**C**	**TCH**
1	ITB3726	PE	Ethical Hacking for Administrators	3	0	0	3	3
2	ITB3727	PE	Criminology and Analytics	3	0	0	3	3
3	ITB3728	PE	Cyber Threats	3	0	0	3	3
4	CSA3731	PE	Software Security	3	0	0	3	3

DEPARTMENT ELECTIVE IV for Cyber Security Specialization (SEMESTER-III)								
SL. NO	**COURSE CODE**	**COURSE CATEGORY**	**COURSE TITLE**	**L**	**T**	**P**	**C**	**TCH**
1	ITB3729	PE	Cyber Investigation and Laws	3	0	0	3	3
2	ITB3730	PE	Penetration Testing & Vulnerability Assessment	3	0	0	3	3
3	CSA3734	PE	Block Chain Technology	3	0	0	3	3
4	CSB3732	PE	Risk analysis and Management	3	0	0	3	3

SEMESTER I

COURSE TITLE	**STATISTICS FOR COMPUTER SCIENCE**			**CREDITS**	**4**
COURSE CODE	**MAA3706**	**COURSE**	**BS**	**L-T-P-C**	**3- 0- 2-**

		CATEGORY			**1**
CIA		**60%**		**ESE**	**40%**
LEARNING LEVEL		**BTL-3**			

CO	**COURSE OUTCOMES**	**PO**
1	Develop statistical models for business analytics	1,2
2	Use forecasting methods to support managerial, financial, and operational statistics.	1,2
3	Perform marketing analytics using statistical models.	1,2
4	Analyze customer data for customer acquisition, retention, and profitability	1,2
5	Analysis of variance	1,2

MODULE 1 : PROBABILITY **9**

Introduction to probability –Bayes theorem-Random variables-discrete random variable (Binomial, Poisson, Geometric), Continues random variable (Uniform, Exponential and Normal distribution). Moment generating function.

Suggested Activities: Basic knowledge on probability

Suggested sources: Introduction to probability

MODULE 2 : TWO DIMENSIONAL RANDOM VARIABLES **9**

Joint distribution –Marginal and conditional distribution covariance –correlation and regression (linear and Multiple). Central limit theorem, Chebyshev's inequality.

Suggested Activities: Basic knowledge on probability

Suggested sources: Probability, Statistics and Random Processes-T.Veerarajan

MODULE 3 : THEORY OF SAMPLING AND TEST OF HYPOTHESIS **9**

Introduction to hypothesis, Large and small samples test -mean and variance (single and double), ψ^2 test, Independent of attributes and contingency table.

Suggested Activities: Basic knowledge of sampling

Suggested sources: Probability, Statistics and Random Processes-T.Veerarajan

MODULE 4 : TIME SERIES ANALYSIS **9**

Introduction to Stochastic process, Time series as a discrete stochastic process. Stationarity, Main characteristics of stochastic process (mean, auto covariation and auto correlation function). Autoregressive models AR (p), Yull-Worker equation Auto regressive moving average models ARMA. Seasonality in Box –Jenkins model

Suggested Activities: Basic knowledge of Time series analysis

Suggested sources: Time series-Maurice George kendall,j.k.Ord

MODULE 5 : DESIGN OF EXPERIMENTS **9**

Analysis of variance (one way & two ways) classification – completely randomized design – randomized block design – Lattin square design.

Suggested Activities: Basic knowledge of design of experiments

Suggested sources: Probability, Statistics and Random Processes-T.Veerarajan

TEXT BOOKS

1	T.Veerarajan , "Probability, Statistics and Random Processes" Tata McGraw-Hill,Education 2008
2	Maurice George Kendall, J. K. Ord,"Time series" Oxford University Press, 1990

REFERENCE BOOKS

1	K.S.Trivedi.John , "Probability and statistics with reliability, Queuing and computer Science Application", Second edition, Wiley&Son, 2016.
2	Levin Richard and Rubin Davids, "Statistics for Management ", Pearson Publications,2016.
3	Robert Stine, Dean Foster ,"Statistical for Business: Decision Making and Analysis". Pearson Education, 2nd edition ,2013.
E-BOOKS	
1	http://www.math.harvard.edu/~knill/teaching/math144_1994/probability.pdf
2	http://www.dartmouth.edu/~chance/teaching_aids/books_articles/probability_book/book.pdf
MOOC	
1	https://nptel.ac.in/courses/IIT-MADRAS/Principles_of_Communication1/Pdfs/1_5.pdf
2	https://nptel.ac.in/courses/110104024/

COURSE TITLE	**ADVANCED DATA STRUCTURES AND ALGORITHMS**			**CREDITS**	**3**
COURSE CODE	**CSA3701**	**COURSE CATEGORY**	**PC**	**L-T-P-C**	**2- 0- 2- 1**
CIA	**60%**			**ESE**	**40%**
LEARNING LEVEL	**BTL-3**				

CO	**COURSE OUTCOMES**	**PO**
1	Estimate time and space complexities for a given algorithm.	1,2
2	Describe the heap property and the use of heaps as an implementation of priority queues.	1,2,3
3	Illustrate the various self- balanced trees and their operations.	1,2,3
4	Apply an appropriate algorithmic approach to a given problem.	1,2,3,
5	Illustrate parallel algorithm models.	1,2,3
6	Use a heuristic approach to solve an appropriate problem.	1,2,3

MODULE 1 : INTRODUCTION **9**

Abstract Data Types - Time and Space Analysis of Algorithms - Big Oh and Theta Notations - Average, best and worst case analysis - Simple recurrence relations – Mappings.

Suggested Activities: Find the time and space complexities of the following algorithms
1. Sum of n numbers **2**. Factorial of a n 3. Matrix multiplication 4. Insertion sort
Suggested sources: https://nptel.ac.in/courses/106105164/
https://nptel.ac.in/courses/106105085/18

MODULE 2 : HEAP STRUCTURES **9**

Min-max heaps - Heaps - Leftist heaps -Binomial heaps - Fibonacci heaps - Skew heaps - Lazy-binomial heaps.

Suggested Activities: Implement the following Heap structures using C, C++, Java or Python
1. Max-min Heap 2. Binomial Heap 3. Fibonacci Heap

Suggested sources: https://nptel.ac.in/courses/106102064/20, 21

MODULE 3 : SEARCH STRUCTURES **9**

Binary search trees - AVL trees - 2-3 trees - 2-3-4 trees - Red-black trees - B-trees - splay trees – k-d trees,Tries.

Suggested Activities: Implement the following tree structures using C, C++, Java or Python
1. AVL Tree 2. Red-Black tree 3. Splay Trees 4. K-d Trees 5. Tries
Suggested sources: https://nptel.ac.in/courses/106102064/11, 12,14,15,18

MODULE 4 : ALGORITHM DESIGN TECHIQUES **9**

Divide and Conquer and Greedy : Quicksort - Strassen's matrix multiplication - Convex hull - Tree-vertex splitting - Job sequencing with deadlines - Optimal storage on tapes Dynamic Programming and Backtracking: Multistage graphs - 0/1 knapsack - 8- queens problem - graph coloring, Palindrome portioning.

Suggested Activities: Solve the following problems
1. Quicksort 2. Strassen's matrix multiplication 3. 8-queens problem 4. Palindrome Partitioning

Suggested Sources:
https://nptel.ac.in/courses/106106131/15,
https://nptel.ac.in/courses/106102011/7

MODULE 5 : ADVANCED ALGORITHMS **9**

Parallel Algorithms: Basic Techniques- Work & Efficiency - Distributed Computation - Heuristic & Approximation Approaches.

Suggested Activities: Implement following heuristic algorithms
1. Hill Climbing 2. Simulated Annealing 3. Particle Swarm Optimization 4. Genetic Algorithm
Suggested sources: https://nptel.ac.in/courses/106104120/4, 5
https://nptel.ac.in/courses/106106126/9 - 15

TEXT BOOKS

1	Thomas H.Coremen, Charles E. Leiserson, Ronald L.Rivest, Clifford Stein , "Introduction to algorithms", Third edition, MIT press,2013

REFERENCE BOOKS

1	E. Horowitz, S.Sahni and Dinesh Mehta, Fundamentals of Data structures in C++, University Press, 2009.
2	E. Horowitz, S. Sahni and S. Rajasekaran, Computer Algorithms/C++, Second Edition, University Press, 2007.
3	Mark Allen Weiss, "Data Structures and Algorithm Analysis in C", Third Edition, Pearson Education, Asia.2007.
4	Ananth Grama, Anshul Gupta, George Karypis, Vipin Kuma, "Introduction to Parallel Computing ", Second Edition, Addison Wesley, 2003

E-BOOK

1	Omid Bozorg-Haddad, Mohammad Solgi, Hugo A. LoÃ¡iciga, "Meta-heuristic and Evolutionary Algorithms for Engineering Optimization 1st Edition", Wiley , 2017
2	Introduction To Parallel Computing - ResearchGate - Free Ebook, www.researchgate.net

MOOC

1	**Advanced Data structures and Algorithms ,** https://nptel.ac.in/courses/106105164/
2	Artificial Intelligence Search Methods for problem Solving, https://onlinecourses.nptel.ac.in/noc18_cs51/

COURSE TITLE	MACHINE LEARNING			CREDITS	3
COURSE CODE	CSA3702	COURSE CATEGORY	PC	L-T-P-C	2- 0- 2- 3
CIA	60%			ESE	40%
LEARNING LEVEL	BTL-3				

CO	COURSE OUTCOMES	PO
1	Apply multilayer perceptron using simple machine learning techniques.	1,2,3
2	Use decision trees and statistics models	1,2,3
3	Use data analysis for machine learning	1,2,3
4	Use Genetic algorithm and reinforced learning for appropriate applications	1,2,3
5	Have learnt machine learning tools in MATLAB, Python programming for ML	1,2,3

MODULE 1 : INTRODUCTION **9**

Learning - Types of machine learning - supervised learning - The brain and the neurons , Linear Discriminants -Perceptron - Linear Separability -Linear Regression,The multilayer perceptron- Examples of using MLP – Back propagation of error.

Suggested Activities: Design a Multilayer Perceptron for Rain Forecasting system

Suggested sources: Enrico C, Simon W, Jay R, Machine Learning Techniques for Space Weather, Elsevier, 2018

MODULE 2 : CLASSIFICATION ALGORITHMS **9**

Decision Tree – Constructing decision trees – Classification of Regression trees - Regression example .Probability and Learning: Turning data into probabilities - Some basic statistics - Gaussian mixture models - Nearest Neighbor methods.

Suggested Activities: Explore the Regression Examples in Machine Learning

Suggested sources: Norman Matlof, "Statistical Regression and Classification: From Linear Models to Machine Learning", CRC Press, 2017.

MODULE 3 : ANALYSIS **9**

The k-Means algorithm - Vector Quantizations - Linear Discriminant Analysis - Principal component analysis - Factor Analysis - Independent component analysis -Locally Linear embedding – Isomap. ill - Least squares optimisation - simulated annealing.

Suggested Activities: Simulated annealing / Modelling on any data science application.

Suggested sources: L.M. Rasdi, Simulated Annealing Algorithm for Deep Learning, Procedia Computer Science, Volume: 72, 2015.

MODULE 4 : OPTIMIZATION TECHNIQUES **9**

The Genetic algorithm - Genetic operators - Genetic programming - Combining sampling with genetic programming – Markov Decision Process - Markov Chain Monte Carlo methods: sampling - Monte carlo - Proposal distribution.

Suggested Activities: Design an Encryption algorithm using Genetic algorithm

Suggested sources: Harsh Bhasin, Application of Genetic Algorithms in Machine learning,, International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011.

MODULE 5 : PYTHON FOR MACHINE LEARNING **9**

Baysean Networks - Markov Random moFields - Hidden Markov Models -Tracking methods. Python: Installation - Python for MATLAB AND R users -Code Basics - Using NumPy and MatPolitB.

Suggested Activities: Design a simple application using NumPy and MatPolitB.

Suggested sources: Rakshith Vasudev, Introduction to Numpy -1 : An absolute beginners guide to Machine Learning and Data science., 2017.

TEXT BOOK	
1	Kevin P. Murphy, "Machine Learning – A probabilistic Perspective", MIT Pres, 2016.
2	Randal S, "Python Machine Learning, PACKT Publishing, 2016.
REFERENCE BOOKS	
1	Ethem Alpaydin, "Machine Learning: The New AI", MIT Press, 2016.
2	Shai Shalev-Shwartz, Shai Ben-David, "Understanding Machine Learning: From Theory to Algorithms", Cambridge University Press, 2014.
3	Sebastian Raschka, "Python Machine Learning", Packt Publishing Ltd, 2015.
E-BOOK	
1	http://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning/index.html
2	http://www.mlyearning.org/
MOOC	
1	https://www.coursera.org/learn/practical-machine-learning
2	https://www.coursera.org/learn/python-machine-learning

SEMESTER II

COURSE TITLE	**INTEGRATED SOFTWARE ENGINEERING METHODOLOGY**			**CREDITS**	**4**
COURSE CODE	**ITA3701**	**COURSE CATEGORY**	**PC**	**L-T-P-C**	**2- 0- 2-4**
CIA	**60%**			**ESE**	**40%**
LEARNING LEVEL	**BTL-3**				

CO	**COURSE OUTCOMES**	**PO**
1	Approach to the concept of continuous integration.	1, 3
2	Reduce risks with CI	1, 2
3	To implement CI with inspection and feedback.	1, 3

Prerequisites : Nil

MODULE 1 : CONTINUOUS INTEGRATION FUNDAMENTALS **12**

Features of CI - Building software at every change – Life of CI - Value of CI – Preventing teams from using CI – Getting to CI – Project Implementation of CI – Evolution of Integration – CI Complementation to development practices – Time for CI Setup – Commit code frequently – Not Commit broken code - All test and Inspections must pass – Run private builds.

MODULE 2 : RISK REDUCTION **12**

Risk: Lack of deployable software – Late discovery of defects – Lack of project visibility – Low quality software – Building software at every change – Automate builds – Build types and

Mechanisms – Dedicated integrated build machine – CI server – run manual integration builds – Run fast builds – Stage builds.	
MODULE 3 : CREATING CI SYSTEM	**12**
Continuous DB integration – Local DB Sandbox – Version control repository – Capability to modify the DB by developers – Team focuses on fixing broken builds – DB integration and Integrate button – Continuous Testing – Automate unit testing - Automate component testing – Automate system testing – Categorize developer tests.	
MODULE 4 : CONTINUOUS INSPECTION	**12**
Difference between inspection and testing – How often to run inspectors – Code metrics – Reduce code complexity – Perform design review continuously – Maintain organizational standards with code audits – Reduce duplicate code – Assess code coverage – Evaluate code quality continuously.	
MODULE 5 : CONTINUOUS DEPLOYMENT AND FEEDBACK	**12**
Release working software – Label repository assets – Produce clean environment – Label each build – Run all tests – create build feedback reports – Continuous feedback – Use continuous feedback mechanisms.	
REFERENCE BOOKS	
1	Jez Humble, David Farley, "Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation", Addison Wesley, 2nd Edition, 2014.
2	Paul M. Duvall, Steve Matyas, "Continuous Integration: Improving Software and Reducing Risks", 1st edition, Addison Wesley, 2007.

COURSE TITLE	**ADVANCED OPERATING SYSTEMS**			**CREDITS**	**3**
COURSE CODE	**CSA3703**	**COURSE CATEGORY**	**PC**	**L-T-P-C**	**2- 0-2- 1**
CIA	**60%**			**ESE**	**40%**
LEARNING LEVEL	**BTL-3**				

CO	**COURSE OUTCOMES**	**PO**
1	Design distributed operating system.	1,2
2	Detect, prevent and avoid the deadlocks in distributed environment.	1,2,3
3	Explain the need for load distribution and the corresponding techniques.	1,2,3
4	Design security mechanisms for distributed operating system.	1,2,3
5	Analyze and find out the requirements to construct a database operating systems	1,3

MODULE 1 : DISTRIBUTED OPERATING SYSTEM	**9**
Synchronization Mechanisms: Introduction – concept of a process – concurrent process – the critical section problem – Synchronization problems – language mechanisms for synchronization: Monitors. System Architecture types – issues in distributed operating systems – communication networks – communication primitives. Theoretical Foundations: inherent limitations of a distributed system – lamport logical clocks – vector clocks – casual ordering of messages – global state – cuts of a distributed computation – termination detection.	
MODULE 2 : DISTRIBUTED DEADLOCK DETECTION	**9**
Deadlock handling strategies in distributed systems – issues in deadlock detection and resolution – control organizations for distributed deadlock detection – centralized and distributed deadlock detection algorithms – hierarchical deadlock detection algorithms. Agreement protocols – introduction-the system model, a	

classification of agreement problems, solutions to the Byzantine agreement problem, applications of agreement algorithms.
MODULE 3 : DISTRIBUTED SHARED MEMORY 9
Architecture– algorithms for implementing DSM – memory coherence and coherence protocols – design issues. Distributed Scheduling: introduction – issues in load distributing – components of a load distributing algorithm – stability – load distributing algorithm – performance comparison – selecting a suitable load sharing algorithm – requirements for load distributing -task migration and associated issues. Failure Recovery and Fault tolerance: introduction – basic concepts – classification of failures – backward and forward error recovery approaches - recovery in concurrent systems – synchronous and asynchronous check pointing and recovery – check pointing for distributed database systems - recovery in replicated distributed databases systems.
MODULE 4 : MULTIPROCESSOR OPERATING SYSTEM 9
Basic multiprocessor system architectures – basic multiprocessor system architecture - inter connection networks for multiprocessor systems – caching – hypercube architecture – structures of multiprocessor operating system - operating system design issues – threads - process synchronization – processor scheduling – Memory management. The Mac OS.
MODULE 5 : DATABASE OPERATING SYSTEM 9
Requirements of a database operating system Concurrency control: theoretical aspects - introduction, database systems - a concurrency control model of database systems- the problem of concurrency control - Serializability theory- distributed database systems, concurrency control algorithms - introduction, basic synchronization primitives, lock based algorithms-timestamp based algorithms, optimistic algorithms - concurrency control algorithms, data replication.
PRACTICAL COMPONENT
1. Implementation of semaphores for multiprocessor OS 2. Implementation of multithreading for multiprocessor OS 3. Implementation of multiple sleeping barbers problem for synchronization in distributed OS 4. Implementation of network operating system. 5. Design a real time operating system to control the temperature of a boiler. 6. Implementation of transactions and concurrency in Database operating system. 7. Implement a banking application using distributed Operating system.

TEXT BOOKS	
1	Mukesh Singhal, Niranjan G.Shivaratri, "Advanced concepts in operating systems", TMH, 2011
REFERENCE BOOKS	
1	Abraham Silberschatz, Peter B. Galvin, G. Gagne, “Operating System Concepts”, Ninth Edition, Addison Wesley Publishing Co., 2013.
2	Andrew S.Tanenbaum, "Modern operating system", PHI, 3rd edition,2008
3	Pradeep K.Sinha, "Distributed operating system-Concepts and design", PHI, 2003.
4	Andrew S.Tanenbaum, "Distributed operating system", Pearson education, 2003
E- BOOKS	
1	https://books.google.co.in/books/about/Advanced_Concepts_In_Operating_Systems.html?id=nel4vdeLcqkC
2	http://www.cs.iit.edu/~sun/pdfd/cs550-lec1.pdf

COURSE TITLE	**CRYPTOGRAPHY AND NETWORK SECURITY**	**CREDITS**	**3**

COURSE CODE	ITA3702	COURSE CATEGORY	PC	L-T-P-C	2- 0- 2- 3
CIA	60%			ESE	40%
LEARNING LEVEL	BTL-4				

CO	COURSE OUTCOMES	PO
1	Understand Cryptography and bitcoin concept.	1, 2, 3
2	Understand key management techniques and algorithms.	1, 2
3	Understanding message authentication and hash algorithms.	1,2, 3
4	Understand security and authentication applications.	1, 2,3
5	Understand network attacks.	1, 2, 3

Prerequisites : Nil

MODULE 1 : **12**

Public Key Cryptography and Bitcoins Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis. Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining

MODULE 2 : **12**

Key Establishment Protocols Introduction, Key transport based on symmetric encryption, Key agreement based on symmetric techniques, Key transport based on public-key encryption, Key agreement based on asymmetric techniques, Secret sharing, Key Management Techniques, Techniques for distributing public keys, Techniques for controlling key usage, Key management involving multiple domains. Secret Key Cryptography Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family.

MODULE 3 : **12**

Message authentication code and Hash Functions Message authentication code Authentication functions, Hash functions-Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure.

MODULE 4 : **12**

Security practice Authentication applications - Kerberos - X.509 Authentication services - Internet Firewalls for Trusted System: Roles of Firewalls - Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions. Intruder - Intrusion detection system - Virus and related threats - Countermeasures - Firewalls design principles - Trusted systems - Practical implementation of cryptography and security.

MODULE 5 : **12**

Network Attacks Network Sniffing, Wireshark, packet analysis, display and capture filters, ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, Open VAS, Sparta, Network Scanning Report Generation, System hardening, secure system configurations, SSL Striping, Setup network IDS/IPS, Router attacks, VPN Pentesting, VOIP Pentesting

REFERENCE BOOKS

1	William Stallings, "Cryptography And Network Security", 6th Edition, Pearson Education, March 2013.
2	Monte, M.,"Network Attacks and Exploitation: A Framework" Wiley, 2015.
3	Bernard Menezes, "Network Security and Cryptography", Cengage Learning, India Edition, 2010
4	Kaufman, C . , Perlman, R., & Speciner, M., "Network Security, Private communication in public world", (2nd Ed.). PHI, 2002.
5	Delfs, H. & Knebl, H., "Introduction to Cryptography: Principles and Applications" Springer-Verlag Berlin and Heidelberg GmbH & Co, 2001
6	Menezes, A.J., Oorschot, P. Van & Vanstone, S.A. "The Handbook of Applied Cryptography", CRC Press, 1997.
7	Schneier, B., "Applied cryptography, Protocols, algorithms and source code in C", (2nd ed.). New York: John Wiley & Sons, 1995

DEPARTMENT ELECTIVE – I for Cyber Security Specialization

COURSE TITLE	**CONCEPTS OF ETHICAL HACKING**			**CREDITS**	**3**
COURSE CODE	**ITB3721**	**COURSE CATEGORY**	**PE**	**L-T-P-C**	**3- 0- 0- 3**
CIA	**60%**			**ESE**	**40%**
LEARNING LEVEL	**BTL-3**				

CO	**COURSE OUTCOMES**	**PO**
1	To known about hacking concepts.	1,3
2	Apply the System Hacking strategies in Ethical manner.	1,3
3	Awareness of Webserver and Wireless Hacking and its issues.	1,3
4	Undertake cyber defensive measures	1,2,3

Prerequisites : Nil

MODULE 1 : INTRODUCTION TO ETHICAL HACKING	**9**
Introduction-Ethical hacking Terminology-types of hacking technologies-phases of ethical hacking-Footprinting-Social Engineering-Scanning and enumeration.	
MODULE 2 : SYSTEM HACKING	**9**
Understanding the password hacking techniques-Rootkits-Trojans-Backdoors-Viruses and worms-sniffers-denial of service-Session hijacking.	
MODULE 3 : WEB SERVER HACKING	**9**
Hacking web servers-web application vulnerabilities –Buffer overflow-Wireless hacking-Physical Security.	
MODULE 4 : WIRELESS HACKING	**9**
WEP, WPA Authentication mechanism-wireless sniffers-Physical Security-factors affecting physical security-honeypots-Firewall types.	
MODULE 5 : PENETRATION TESTING	**9**
Cryptography-overview of MD5, SHA, RC4-penetration testing methodologies- steps-pen test legal framework-penetration testing tools.	
REFERENCE BOOKS	

1	Hands- On Ethical Hacking and Network Defense – By Michael T. Simpson, Kent Backman, James Corley
2	Official Certified Ethical Hacker Review Guide – By Steven DeFino, Barry Kaufman, Nick Valenteen.
3	The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series) [Paperback]
4	Hands- On Ethical Hacking and Network Defense [Print Replica] [Kindle Edition]

COURSE TITLE	**CYBER CRIME & SECURITY**			**CREDITS**	**3**
COURSE CODE	**ITB3722**	**COURSE CATEGORY**	**PE**	**L-T-P-C**	**3- 0- 0- 3**
CIA	**60%**			**ESE**	**40%**
LEARNING LEVEL	**BTL-3**				

CO	**COURSE OUTCOMES**	**PO**
1	Follow the cyber laws and solve issues if any	3
2	Ascertain the impacts on citizen security	1,2,3
3	Import security in the network activities.	1,3
4	Identify threat and perform intrusion analysis.	1,2,3

Prerequisites : Nil

MODULE 1 : CYBER CRIMES AND CYBER LAWS **9**

Introduction to IT laws & Cyber Crimes – Internet, Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits, and Cyber Security

MODULE 2 : COMPUTER AND CYBER FORENSIC BASICS **9**

Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Basic Computer Terminology, Internet, Networking, Computer Storage, Cell Phone / Mobile Forensics, Computer Ethics and Application Programs, Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology

MODULE 3 : DATA AND EVIDENCE RECOVERY **9**

Introduction to Deleted File Recovery, Formatted Partition Recovery, Data Recovery Tools, Data Recovery Procedures and Ethics, Preserve and safely handle original media, Document a "Chain of Custody", Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK) etc, Use computer forensics software tools to cross validate findings in computer evidence-related cases

MODULE 4 : CYBER FORENSICS INVESTIGATION **9**

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking

MODULE 5 : INTRUSION ANALYSIS **9**

Intrusion Analysis as a Core Skill set, Methods to Performing Intrusion Analysis, Intrusion Kill Chain, Passively Discovering Activity in Historical Data and Logs, Detecting Future Threat Actions and Capabilities, Denying Access to Threats, Delaying and Degrading Adversary Tactics and Malware, Identifying Intrusion Patterns and Key Indicators	
REFERENCE BOOKS	
1	Cybercrime and Digital Forensics: An Introduction, 2nd Edition, Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, CRC press
2	Cyber Security, Nina Godbole, Sunit Belapure, ISBN: 9788126521791, Wiley
3	Dan Shoemaker and Wm Arthur Conklin "Cyber Security – the Essential body of knowledge", Cengage Learning, 2012
4	Kim Andreasson "Cyber Security – Public Sector threats and responses", CRC Press, 2012

COURSE TITLE	**INFORMATION SECURITY ARCHITECTURE**			**CREDITS**	**3**
COURSE CODE	**CSA3723**	**COURSE CATEGORY**	**PE**	**L-T-P-C**	**3- 0- 0- 0**
CIA	**50%**			**ESE**	**50%**
LEARNING LEVEL	**BTL5- DESIGN**				

CO	**COURSE OUTCOMES**	**PO**
1	The basics of information security	3
2	Use the legal, ethical and professional issues in Information Security	1,2,3
3	Analyse Risk management	1,3
4	Design the logic of various standards	1,2,3
5	Implement Information Security procedures.	1,2,3

Prerequisites : Nil

MODULE 1 : INTRODUCTION	**9**
History, Information Security Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC.	
MODULE 2 : SECURITY INVESTIGATION	**9**
Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues **Suggested Activities**: Design a Secure Business Model **Suggested sources: https://dynomapper.com/blog/278-books-about-information-architecture**	
MODULE 3 : SECURITY ANALYSIS	**9**
Risk Management: Identifying and Assessing Risk, Assessing and Controlling Risk **Suggested Activities**: Identifying and Assess the Risk	
MODULE 4 : LOGICAL DESIGN	**9**
Blueprint for Security, Information Security Policy, Standards and Practices, ISO 17799/BS 7799, NIST Models, VISA International Security Model, Design of Security Architecture, Planning for Continuity. **Suggested Activities**: To prepare a blueprint for security design of an organisation	
MODULE 5 : PHYSICAL DESIGN	**9**
Security Technology, IDS, Scanning and Analysis Tools, Cryptography, Access Control Devices, Physical Security, Security and Personnel.	

TEXT BOOK	
1	Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi, 2012.
REFERENCE BOOKS	
1	Micki Krause, Harold F. Tipton, " Handbook of Information Security Management", Vol 1-3 CRC Press LLC, 2004.
2	Stuart Mc Clure, Joel Scrambray, George Kurtz, "Hacking Exposed", Tata McGraw-Hill, 2003.
3	Matt Bishop, " Computer Security Art and Science", Pearson/PHI, 2002.
MOOC	
1	https://dynomapper.com/blog/278-books-about-information-architecture
2	https://www.cyberark.com/blog/8-books-every-security-architect-must-read/

DEPARTMENT ELECTIVE – II for Cyber Security Specialization

COURSE TITLE	ETHICAL HACKING AND SYSTEMS DEFENSE			CREDITS	3
COURSE CODE	ITB3723	COURSE CATEGORY	PE	L-T-P-C	3- 0- 0- 3
CIA	60%			ESE	40%
LEARNING LEVEL	BTL-3				

CO	COURSE OUTCOMES	PO
1	To known about hacking concepts in defense.	1,3
2	Apply the Hacking strategies in Ethical manner.	1,2,3
3	Awareness of Security policies in defenses field.	3

Prerequisites : Nil

MODULE 1 : TCP/IP OVERVIEW CONCEPTS	9
Overview of TCP/IP-IP addressing-numbering systems-Denial of service attacks-distributed denial of service attacks.	
MODULE 2 : PORT SCANNING	**9**
Introduction to port scanning-types of port scan-port scanning tools-ping sweeps- Understanding scripting-Enumeration-Net BIOS basics-Enumeration tools.	
MODULE 3 : PROGRAMMING FOR SECURITY PROFESSIONALS	**9**
Introduction to programming fundamentals-Basics of C-Basics of HTML-Understanding perl-Understanding oops concepts.	
MODULE 4 : DESKTOP AND SERVER OS VULNERABILITIES	**9**
Windows OS vulnerabilities-tools for identifying vulnerabilities in windows-Linux OS vulnerabilities-vulnerabilities of embedded OS	
MODULE 5 : NETWORK PROTECTION SYSTEMS	**9**
Understanding routers-understanding firewalls-risk analysis tools for firewalls-understanding intrusion and detection and prevention systems-honeypots.	
REFERENCE BOOKS	

1	Michael T Simpson, Nicholas Antil, "Hands-On Ethical Hacking And Network Defense " 3rd Edition, Cengage Learning, 2012
2	James S. Tiller, "The Ethical Hack: A Framework for Business Value Penetration Testing", Auerbach Publications, 2004.

COURSE TITLE	ETHICAL HACKING AND DIGITAL FORENSICS			CREDITS	3
COURSE CODE	ITB3724	COURSE CATEGORY	PE	L-T-P-C	3- 0- 0- 3
CIA	60%			ESE	40%
LEARNING LEVEL	BTL-3				

CO	COURSE OUTCOMES	PO
1	Uderstand the history of hacking	3
2	Interpret hacking methods and remedial measures	1,2,3
3	Apply recovering digital evidences and forensics	1,2,3

Prerequisites : Nil

MODULE 1 : HISTORY OF HACKING **9**

History and current state of hacking and penetration testing-Profiles of hackers and cybercriminals-History of computer hacking-Common hacking methodologies-Ethical hacking and penetration testing in relation to black-hat and white-hat activities-Laws and ethical standards for penetration testers and ethical hackers

MODULE 2 : HACKING AND ATTACKS **9**

Hacking windows – Network hacking – Web hacking – Password hacking. A study on various attacks – Input validation attacks – SQL injection attacks – Buffer overflow attacks - Privacy attacks

MODULE 3 : COMPUTER NETWORKS **9**

TCP / IP – Checksums – IP Spoofing port scanning, DNS Spoofing. Dos attacks – SYN attacks, Smurf attacks, UDP flooding, DDOS – Models. Firewalls – Packet filter firewalls, Packet Inspection firewalls – Application Proxy Firewalls. Batch File Programming

MODULE 4 : COMPUTER FRAUD **9**

Fundamentals of Computer Fraud – Threat concepts – Framework for predicting inside attacks –Managing the threat – Strategic Planning Process. Architecture strategies for computer fraud Prevention – Protection of Web sites – Intrusion detection system – NIDS, HIDS – Penetrating testing process – Web Services – Reducing transaction risks

MODULE 5 : DIGITAL FORENSIC **9**

Key Fraud Indicator selection process customized taxonomies – Key fraud signature selection Process – Accounting Forensics – Computer Forensics – Journaling and it requirements – Standardized logging criteria – Journal risk and control matrix – Neural networks – Misuse detection and Novelty detection.

REFERENCE BOOKS

1	Kenneth C.Brancik "Insider Computer Fraud" Auerbach Publications Taylor & Francis Group, 2008
2	AnkitFadia" Ethical Hacking" 2nd Edition Macmillan India Ltd, 2006
3	Oriyano, Sean-Philip. (2016)Ethical hacking and systems defense,Burlington, MA: Jones Bartlett Learning

COURSE TITLE	MOBILE AND DIGITAL FORENSICS			CREDITS	3
COURSE CODE	ITB3725	COURSE CATEGORY	PE	L-T-P-C	3- 0- 0- 3
CIA	60%			ESE	40%
LEARNING LEVEL	BTL-3				

CO	COURSE OUTCOMES	PO
1	Understand the basics of wireless technologies and security	3
2	Become knowledgeable in mobile phone forensics and android forensics	1,2,3
3	Learn the methods of investigation using digital forensic techniques	1,2,3

Prerequisites : Nil

MODULE 1 : OVERVIEW OF WIRELESS TECHNOLOGIES AND SECURITY **9**

Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft

MODULE 2 : CIA TRIAD IN MOBILE PHONES **9**

Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues

MODULE 3 : MOBILE PHONE FORENSICS **9**

crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques

MODULE 4 : DIGITAL FORENSICS **9**

Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contamination

MODULE 5 : DIGITAL FORENSICS EXAMINATION PRINCIPLES **9**

Previewing, imaging, continuity, hashing and evidence locations- Seven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context

REFERENCE BOOKS

1	Gregory Kipper, "Wireless Crime and Forensic Investigation", Auerbach Publications, 2007
2	Iosif I. Androulidakis, " Mobile phone security and forensics: A practical approach", Springer publications, 2012
3	Andrew Hoog, " Android Forensics: Investigation, Analysis and Mobile Security for Google Android", Elsevier publications, 2011
4	Angus M.Marshall, " Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008

DEPARTMENT ELECTIVE – III for Cyber Security Specialization

COURSE TITLE	ETHICAL HACKING FOR ADMINISTRATORS			CREDITS	3
COURSE CODE	ITB3726	COURSE CATEGORY	PE	L-T-P-C	3- 0- 0- 3
CIA	60%			ESE	40%
LEARNING LEVEL	BTL-3				

CO	COURSE OUTCOMES	PO
1	Understand the ethics of hacking in a layman perspective	3
2	Employ pentesting tools and defend an attack	1,3
3	Discover different types of attacks and handle buffer overflow issues	1,3
4	Deduct and analyse malware using latest trending tools	1,3

Prerequisites : Nil

MODULE 1 : INTRODUCTION TO ETHICAL DISCLOSURE **9**

Ethics of Ethical Hacking – Recognizing the Gray Areas in Security – Vulnerability Assessment – Ethical Hacking and Legal System : The Rise of Cyberlaws – Electronic Communication Privacy Act – Digital Millennium Copyright Act (DCMA) - Cyber Security Enhancement Act - Understanding Individuals Cyberlaws .

MODULE 2 : PENETRATION TESTING AND TOOLS **9**

Social Engineering Attacks – Common Attacks used in Penetration Testing – Physical Penetration Attacks – Reconnaissance – Common ways into a Building – Defending against physical Penetrations. **Insider Attacks**: Conducting an Insider Attack – Defending Against Insider Attack.

MODULE 3 : TYPES OF ATTACKS **9**

Web Server Attacks - Database Attacks - Password Cracking -Network Devices & Attacks - Wireless Network Attacks - Trojans and Backdoor Applications -OS Specific Attacks - Buffer Overflows - Denial of Service Attacks

MODULE 4 : MALWARE ANALYSIS **9**

Malware – Latest Trends in Honeynet Technology – Catching Malware – Initial Analysis of Malware.

MODULE 5 : HACKING MALWARE **9**

Trends in Malware – De-obfuscating Malware – Reverse Engineering Malware – Malware Operation Phase – Automated Malware Analysis.

REFERENCE BOOKS

1	Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams, "Gray Hat Hacking: The Ethical Hackers Handbook : The Ethical Hacker's Handbook", 5th Edition, McGraw Hill , 2015.
2	Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy" , 2nd Edition , Syngress, 2013.

COURSE TITLE	CRIMINOLOGY AND ANALYTICS			CREDITS	3
COURSE CODE	ITB3727	COURSE CATEGORY	PE	L-T-P-C	3- 0- 0- 3

CIA	60%	ESE	40%
LEARNING LEVEL	BTL-3		

CO	COURSE OUTCOMES	PO
1	Know about advanced concepts and types of cyber crime.	1, 3
2	Describe the various analytical methods for identifying the cyber crimes.	1, 3
3	Identify the ways for mitigating the effects of cyber crimes.	1, 3

Prerequisites : Nil

MODULE 1 : DEVIANCE AND CRIMINAL SUBCULTURE IN CYBERSPACE **6**

Introduction to criminal subculture cyberspace – Café Culture and Heresy of Yahooboyism in Nigeria - Internet Gambling . Consolidate the analytics outcome.

MODULE 2 : PERPETRATORS' PERSPECTIVES AND OFFENDER USE OF THE INTERNET **10**

Identity Construction Among Hackers - Virtual Sex Offenders: A Clinical Perspective - Self-Reported Internet Child Pornography Consumers: A Personality Assessment Using Bandura's Theory of Reciprocal Determinism - Online Social Networking and Pedophilia: An Experimental Research "Sting" - Adult–Child Sex Advocacy Websites as Learning Environments for Crime - The Internet as a Terrorist's Tool: A Social Learning Perspective .

MODULE 3 : DIGITAL PIRACY **12**

Value and Choice: Examining Their Roles in Digital Piracy - Suing the Genie Back in the Bottle: The Failed RIAA Strategy to Deter P2P Network Users - Criminological Predictors of Digital Piracy: A Path Analysis - Change of Music Piracy and Neutralization: An Examination Using Short-Term Longitudinal Data - Digital File Sharing: An Examination of Neutralization and Rationalization Techniques Employed by Digital File Sharers.

MODULE 4 : VICTIMIZATION **9**

Cyber-Routine Activities: Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization - Adolescent Online Victimization and Constructs of Routine Activities Theory - Cyber Stalking: Typology, Etiology, and Victims - Online Social Networking and Women Victims - Malware Victimization: A Routine Activities Framework.

MODULE 5 : LEGAL AND POLICY ISSUES OF CYBER CRIMES **8**

Fatwas Chaos Ignites Cyber Vandalism: Islamic Criminal Law Prohibit Cyber Vandalism - Cyber Bullying: Legal Obligations and Educational Policy Vacuum - Human Rights Infringement in the Digital Age.

REFERENCE BOOKS

1	Jai Shankar, Cyber Criminology, "Exploring Internal Crimes and Criminal Behaviour", CRC Press, Taylor and Francis Group, 2016.
2	Colleen Mccue, "Data Mining and Predictive Analysis – Intelligence Gathering and Crime Analysis", Elsevier-Science Direct, 2015.

COURSE TITLE	CYBER THREATS			CREDITS	3
COURSE CODE	ITB3728	COURSE CATEGORY	PE	L-T-P-C	3- 0- 0- 3

CIA	60%	ESE	40%
LEARNING LEVEL	BTL-3		

CO	COURSE OUTCOMES	PO
1	Know about advanced types of cyber threats	3
2	Describe the various analytical methods for identifying the cyber threats.	1,3
3	Examine Cyber Threat Intelligence though advanced concepts	1,2,3

Prerequisites : Nil

MODULE 1 : INTRODUCTION **9**

Cyber Crime – Cyber Terrorism – Cyber Space – Cyber crime cost – Cyber Threat Strategies- Cyber Decline and Fall.

MODULE 2 : ORDER & DISORDER, CRIME, WAR AND TERRORISM **9**

Self organizing system – Order in human societies – Rules for modern human social systems – External order – Crime War – Crime and Terrorism.

MODULE 3 : CYBER THREAT ANALYSIS **9**

Cyber Threat Analysis Program – Client Confidentiality and Sensitivity – Cyber Security Expertise – CTAP Intelligence Catalogs, Infrastructure and Tools.

MODULE 4 : RESPONDING TO CYBER THREAT **9**

Cyber global concerns – Cyber trends and the future model – Cyber Security Model – Automation in analyzing the cyber threat.

MODULE 5 : CYBER THREAT INTELLIGENCE **9**

Know the Cyber threat – Technological Environment – Adversary tactics – Cyber Intelligence Framework – Strategic Assessment.

REFERENCE BOOKS

1	Susan W. Brenner “Cyber Threats”, Oxford Press, 2016.
2	White Paper on “Symantec Cyber Threat Analysis”, 2017.
3	Bob Gourley, “The Cyber Threat – know the threat to beat the threat”, 2017.

COURSE TITLE	SOFTWARE SECURITY			CREDITS	3
COURSE CODE	CSA3731	COURSE	PE	L-T-P-C	3- 0- 0- 3

		CATEGORY			
CIA	**50%**			**ESE**	**50%**
LEARNING LEVEL	**BTL-3,4,5 & 6**				

CO	COURSE OUTCOMES	PO
1	Describe software security fundamentals	1,3
2	Do code review with a tool	1,3
3	Perform Security Testing and identify the security gap	1,2,3
4	Analyse the files both statically and dynamically	3

Prerequisites : Security Software Engineering

MODULE 1 : SOFTWARE SECRITY FUNDAMENTALS	**9**
Defining a discipline : Security Problems in Software - The three pillars of software security -The rise of security engineering - Risk Management framework.	
MODULE 2 : TOUCH POINTS OF SOFTWARE SECURITY	**9**
Introduction to software security touch points -Code review with a tool	
MODULE 3 : SECURITY TESTING	**9**
Software penetration Testing - Risk Based Security Testing - Abuse Cases - Software Security meets security operations	
MODULE 4 : SOFTWARE SECURITY GAP	**9**
Enterprise Software Security Program -Knowledge for software security - Taxonomy of coding errors	
MODULE 5 : ANALYSIS OF FILES	**9**
Static and Dynamic analysis of files. Static analysis methods - feature selection, feature extraction and dataset creation - Dynamic analysis methods (use procmon)	

REFERENCE BOOKS

1	Gary R.McGraw, "Software Security : Building Security In", Addison Wesley, 2006
2	Sommerville, “Software Engineering”, Adison Wesley, 10th Edition, 2016
3	Pfleeger, “Software Engineering”, Prentice Hall, 4th Edition, 2010
4	Carlo Ghezzi, Mehdi Jazayari and Dino Mandrioli, “Fundamentals of Software Engineering”, Prentice Hall of India, 2th Edition, 2004
5	Craig Larman, “Agile and Iterative Development: A Manager’s Guide”, Pearson Education, 2009.
6	M.Shaw and D. Garlan, “Software Architecture: Perspectives on an Emerging Discipline”, Prentice Hall of India Private Limited , New Delhi 2010

E BOOKS

1	*https://www.amazon.com/Secure-Software-Design-Theodor-Richardson/.../14496263..*
2	*euref.kieskompas.nl/secure-software-design.pdf*

MOOC

1	*ceur-ws.org/Vol-1977/paper3.pdf*
2	https://pe.gatech.edu/courses/secure-software-development

DEPARTMENT ELECTIVE – IV for Cyber Security Specialization

COURSE TITLE	**CYBER INVESTIGATION & LAWS**	**CREDITS**	**3**

COURSE CODE	ITB3729	COURSE CATEGORY	PE	L-T-P-C	3- 0- 0- 3
CIA	60%			ESE	40%
LEARNING LEVEL	BTL-3				

CO	COURSE OUTCOMES	PO
1	Need for cyber issues there in and to apply a cyber law	1,3
2	Address e-trade and e-governance	1,2,3
3	Resolve the issues and problems arising out of online transactions	1,2,3
4	Understanding crimes with case law	3

Prerequisites : Nil

MODULE 1 : INRODUCTION **9**

Cyber Space- Fundamental definitions -Interface of Technology and Law – Jurisprudence and-Jurisdiction in Cyber Space - Indian Context of Jurisdiction -Enforcement agencies – Need for IT act - UNCITRAL – E-Commerce basics Information Technology Act, 2000 - Aims and Objects — Overview of the Act – Jurisdiction.

MODULE 2 : E-GOVERNANCE **9**

Electronic Governance – Legal Recognition of Electronic Records and Electronic Evidence -Digital Signature Certificates - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators under the Act -The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability– Powers of Police under the Act – Impact of the Act on other Laws

MODULE 3 : TYPES OF CYBER CRIMES **9**

Cyber Crimes -Meaning of Cyber Crimes –Different Kinds of Cyber crimes – Cyber crimes under IPC, Cr.P.C and Indian Evidence Law - Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber Terrorism Violation of Privacy on Internet - Data Protection and Privacy – Indian Court cases.

MODULE 4 : INTELLECTURAL PROPERTY RIGHTS **9**

Intellectual Property Rights – Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases, Patents

MODULE 5 : PATENTS **9**

Understanding Patents - European Position on Computer related Patents, Legal position on Computer related Patents - Indian Position on Patents – Case Law, Domain names -registration - Domain Name Disputes-Cyber Squatting-IPR cases.

REFERENCE BOOKS

1	Ashwani Kumar Bansal "Justice Yatindra Singh: Cyber Laws", Universal Law Publishing Co., New Delhi, 2010.
2	Farouq Ahmed, "Cyber Law in India", New Era publications, New Delhi, 2015.
3	S.R.Myneni, "Information Technology Law(Cyber Laws)", Asia Law House, 2017
4	Chris Reed, "Internet Law-Text and Materials", Cambride University Press, 2004.

5	Pawan Duggal, “Cyber Law- the Indian perspective” Universal Law Publishing Co., 2018

COURSE TITLE	**BLOCK CHAIN TECHNOLOGY**			**CREDITS**	**3**
COURSE CODE	**CSA3734**	**COURSE CATEGORY**	**PE**	**L-T-P-C**	**3- 0- 0- 0**
CIA	**50%**			**ESE**	**50%**
LEARNING LEVEL	**BTL-3(APPLY)**				

CO	**COURSE OUTCOMES**	**PO**
1	State the basic concepts of blockchain	3
2	Paraphrase the list of Consensus	1,3
3	Demonstrate and Interpret working of Hyperledger Fabric	1,2,3
4	Implement SDK composer tool	1,2,3
5	Demonstrate the supply chain.	1,2,3
6	Describe the Digital identity for government	1,3

Prerequisites : Basic idea in Networking, finance, Supply chain, Cryptography, Network Security

MODULE 1 : INTRODUCTION TO BLOCKCHAIN **9**

History: Digital Money to Distributed Ledgers -Design Primitives: Protocols, Security, Consensus, Permissions, Privacy- : Blockchain Architecture and Design-Basic crypto primitives: Hash, Signature-Hashchain to Blockchain-Basic consensus mechanisms

Suggested sources: http://https://onlinecourses.nptel.ac.in/noc18_cs47/unit?unit=6&lesson=55

MODULE 2 : CONSENSUS **9**

Requirements for the consensus protocols-Proof of Work (PoW)-Scalability aspects of Blockchain consensus protocols**:** Permissioned Blockchains-Design goals-Consensus protocols for Permissioned Blockchains

Suggested sources: https://onlinecourses.nptel.ac.in/noc18_cs47/unit?unit=18&lesson=64

MODULE 3 : HYPERLEDGER FABRIC **9**

Decomposing the consensus process-Hyperledger fabric components-Chaincode Design and Implementation: Hyperledger Fabric II:-Beyond Chaincode: fabric SDK and Front End-Hyperledger composer tool

Suggested sources: https://onlinecourses.nptel.ac.in/noc18_cs47/unit?unit=31&lesson=66
https://onlinecourses.nptel.ac.in/noc18_cs47/unit?unit=37&lesson=67

MODULE 4 : USE CASE I **9**

Blockchain in Financial Software and Systems (FSS): -Settlements, -KYC, -Capital markets-Insurance-Use case II: Blockchain in trade/supply chain: Provenance of goods, visibility, trade/supply chain finance, invoice management/discounting

Suggested sources: https://onlinecourses.nptel.ac.in/noc18_cs47/unit?unit=45&lesson=68

MODULE 5 : USE CASE II **9**

Blockchain for Government: Digital identity, land records and other kinds of record keeping between government entities, public distribution system / social welfare systems : Blockchain Cryptography : Privacy and Security on Blockchain

Suggested sources: https://onlinecourses.nptel.ac.in/noc18_cs47/unit?unit=49&lesson=69

TEXT BOOKS

1	Mark Gates, “Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money”, Wise Fox Publishing and Mark Gates, 2017.
2	Salman Baset, Luc Desrosiers, Nitin Gaur, Petr Novotny, Anthony O'Dowd, Venkatraman Ramakrishna, “Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer”, 2018.
3	Arshdeep Bahga, Vijay Madisetti, “Blockchain Applications: A Hands-On Approach”, Arshdeep Bahga, Vijay Madisetti publishers 2017.
REFERENCE BOOKS	
1	Andreas Antonopoulos, “Mastering Bitcoin: Unlocking Digital Cryptocurrencies”,O'Reilly Media, Inc., 2014.
2	Melanie Swa, “Blockchain ”,O'Reilly Media, 2014
E BOOKS	
1	Blockchain Applications- https://www.blockchain-books.com
2	Hyperledger Fabric - https://www.hyperledger.org/projects/fabric
3	Zero to Blockchain - An IBM Redbooks course, by Bob Dill, David Smits,2017 - https://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/crse0401.html
MOOC	
1	https://onlinecourses.nptel.ac.in/noc18_cs47/preview
2	https://www.udemy.com/blockchain-and-bitcoin-fundamentals/

COURSE TITLE	**RISK ANALYSIS AND MANAGEMENT**			**CREDITS**	**3**
COURSE CODE	**CSB3732**	**COURSE CATEGORY**	**PE**	**L-T-P-C**	**3- 0- 0- 0**
CIA	**50%**			**ESE**	**50%**
LEARNING LEVEL	**BTL-3**				

CO	**COURSE OUTCOMES**	**PO**
1	Identify, formulate, and solve engineering problems in risk management.	1,2,3
2	Apply knowledge of mathematics, science, and engineering to the assessment of risk.	1,2,3
3	Understand the environmental assessments and perception of risk assessment	1,2,3
4	Suggest risk reduction and risk management measures, also where there is a lack of information	1,2,3
5	Reflect upon ethical, subjective and societal dimensions of risk assessments.	1,2,3
6	Implement tools and techniques to evaluate risk in projects	1,2,3

Prerequisites : Nil

MODULE 1 : INTRODUCTION TO RISK ANALYSIS **9**

Introduction - Risk analysis –Variability and uncertainty of risk analysis-Risk analysis modeling-Probabilistic risk analysis for complex engineering system Ecological risk analysis-Economics of risk Privacy.

MODULE 2 : APPLICATION OF RISK ANALYSIS **9**

Role of risk assessment in human health – Role of risk analysis in pollution prevention-Integrated risk analysis and global climate change-Computer software programs-databases –www- Other online systems-

Use of internet.	
MODULE 3 : RISK PERCEPTION AND COMMUNICATION	**9**
Risk perception and trust- Insurability of risk – Setting environmental priorities based on risk— Comparative risk analysis – Law and risk assessment –Science and toxic risk assessment.	
MODULE 4 : RISK MANAGEMENT	**9**
Risk management process-Identify-assess-plan responses-Manage process –PRAM Process – Three cycles of strategic level risk management.	
MODULE 5 : RISK ORGANISATION AND CONTROL	**9**
Organizational structure- Responsibilities – Functional roles – Risk response actions - Control risk documentation – Risk reporting – Risk governance – Risk reviews –Behavioral influences.– Risk identification techniques –SWOT analysis.	
TEXT BOOKS	
1	Vlasta Molak, "Fundamentals of Risk Analysis and Risk Management", 2nd Edition, CRC Press, Lewish Publishers, 2000.
2	John Bartlet, "Project Risk Analysis and Management Guide", 2nd Edition, ARM Publishing Ltd, 2010
REFERENCE BOOKS	
1	Naagarazan. R.S., "A textbook on Professional Ethics and Human values", New Age International, New Delhi, 2006.
2	Ranganatham and Madhumathi, "Derivatives and Risk Management", Pearson, 2011
3	Rajiv Srivastav, "Derivatives and Risk Management", Oxford University Press, 2010
E-BOOKS	
1	https://the-eye.eu/.../Fundamentals%20of%20Risk%20Analysis%20and%20Risk%20Man.
2	*penka.kroser.com.uy/fundamentals_of_risk_and_insurance.pdf*
MOOC	
1	https://www.mooc-list.com/tags/risk-management
2	https://www.edx.org/learn/risk-management

COURSE TITLE	**PENETRATION TESTING AND VULNERABILITY ASSESSMENT**			**CREDITS**	**3**
COURSE CODE	**ITB3730**	**COURSE CATEGORY**	**PE**	**L-T-P-C**	**3- 0- 0- 3**
CIA	**60%**			**ESE**	**40%**
LEARNING LEVEL	**BTL-3**				

CO	**COURSE OUTCOMES**	**PO**
1	Understand vulnerability and its implications.	3
2	Formulate the techniques of information gathering	1,3
3	Discover the system hacking methods and its advancement	1,2,3
4	Perform a wireless pentesting	1,3

Prerequisites : Nil

MODULE 1 : INTRODUCTION **9**

Penetration Testing phases/Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non Disclosure Agreement Checklist, Phases of hacking, Open-source/proprietary Pentest Methodologies

MODULE 2 : INFORMATION GATHERING AND SCANNING **9**

Information gathering methodologies- Foot printing, Competitive IntelligenceDNS Enumerations- Social Engineering attacks, Port Scanning-Network ScanningVulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration

MODULE 3 : SYSTEM HACKING **9**

Password cracking techniques- Key loggers- Escalating privileges- Hiding Files,Double Encoding, Steganography technologies and its Countermeasures. Active and passive sniffing- ARP Poisoning, MAC Flooding- SQL Injection - Errorbased, Union-based, Time-based, Blind SQL, Out-of-band. Injection Prevention Techniques.

MODULE 4 : ADVANCED SYSTEM HACKING **9**

Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Code, XSS - Stored, Reflected, DOM Based

MODULE 5 : WIRELESS PENTEST **9**

Wi-Fi Authentication Modes, Bypassing WLAN Authentication, Types of Wireless Encryption, WLAN Encryption Flaws, AP Attack, Attacks on the WLAN Infrastructure, DoS-Layer1, Layer2, Layer 3, DDoS Attack, Client Misassociation, Wireless Hacking Methodology, Wireless Traffic Analysis.

REFERENCE BOOKS

1	Kali Linux Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran, Cameron Buchanan, 2015 Packt Publishing
2	SQL Injection Attacks and Defense 1st Edition, by Justin Clarke-Salt, Syngress Publication
3	Mastering Modern Web Penetration Testing By Prakhar Prasad, October 2016 Packt Publishing
4	Kali Linux 2: Windows Penetration Testing, By Wolf Halton, Bo Weaver , June 2016 Packt Publishing