INDIAN INSTITUTE OF INFORMATION TECHNOLOGY KOTTAYAM

Curriculum and Syllabus for the PG Course

MTech Programme

In Cyber Security

For Working Professionals

Contents

Detailed Course Structure

Subject		L-T-P	Credits
Semester I			
CBM 511	Mathematical Foundations for Cyber Security	2-0-0	2
DSC 512	Programming and Data Structures	2-0-3	3
CBM 513	Computer Networks and Security	2-0-3	3
Semester II			
CBM 521	Secure Software Engineering / Digital Forensics	2-0-0	2
CBM 522	Information Security and Applied Cryptography	2-0-3	3
CBM 523	Decision Support and Artificial Intelligence/ Distributed System Security / AI, Machine Learning and Security	2-0-3	3
Semester III			
CBM 611	Operating System Security / Cloud Computing and Security	2-0-3	3
CBM 612	Advanced Database Security /Secure Hardware Design	2-0-3	3
CBM 614	Blockchain Architecture and Applications / Network, Wireless, IOT, Mobile & Security	2-0-3	3
Semester IV			
CBM 621	Forensics, Malware, and Penetration Testing / Intrusion Detection Systems and Firewall	3-0-3	4
CBM 622	Legal Aspects of Computing / Information Security Policies, Security Standards, Audits, Cyber Ethics, Privacy and Legal Issues	2-0-0	2
CBM 623	Criminal Psychology and Behaviour Intelligence	1-0-0	1
Semester V			
CBE 711	Project (Stage 1)		14
Semester VI			
CBE 761	Project (Stage 2)		14
Total Credits			**60**

CURRICULUM

SEMESTER I

CBM 511 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY [2-0-0-2]

Prerequisite for the Course

Students are expected to have knowledge in basic linear algebra, probability theory, set theory and logic.

Course Objectives

1. To provide mathematical background required for cyber security.
2. To familiarise the basic building blocks of important cyber security applications
3. To discuss the theoretical aspects of number theory
4. To introduce vital concepts of graph and probability theory which will be useful for data compression, information hiding.

Expected Outcome

Students who successfully complete this course will be able to: -

1. Visualize abstract concepts, quantitative relationships, and spatial connections.
2. Understand, communicate and model using symbols and numbers.
3. Illustrate the use of algebraic structures in cryptography.
4. Apply probability theory in key generation in encrypted system.

Discrete Mathematics: Mathematical reasoning, Mathematical induction, Modular Arithmetic, Graph Theory: Isomorphism, Planar graphs, graph colouring, Hamilton circuits and Euler cycles. Algebraic Structures: Groups - Modulo groups - Primitive roots - Discrete logarithms. Rings, Fields - Finite fields - GF (p^n), GF(2^n)

Number Theory: Fundamental theorem of arithmetic, Division algorithm, Prime and relatively prime, Mersenne primes, Euclidean algorithm, Fermat's theorem, Euler totient function, Euler's Theorem, Congruences and Residue Classes, Chinese Remainder Theorem, Tests for primality – Solovay-Stressen test, Miller-Rabin test.

Probability and Statistics: Family of random variables – types, densities and distributions, Application of probability in encryption, Statistical inference – Testing of hypothesis.

Reference Books

1. Papoulis A, Pillai SU. *Probability, Random Variables, and Stochastic Processes*. Tata McGraw-Hill Education, 2002.

2. Niven I, Zuckerman HS, Montgomery HL. *An introduction to the theory of numbers*. John Wiley & Sons, 1991.
3. Lewis, Harry, and Rachel Zax. *Essential discrete mathematics for computer science*. Princeton University Press, 2019.
4. Stinson, Douglas Robert, and Maura Paterson. *Cryptography: theory and practice*. CRC press, 2018.
5. Vince, John. *Foundation Mathematics for Computer Science*. Springer International Publishing, Switzerland, 2015.
6. Montgomery, Douglas C., and George C. Runger. *Applied statistics and probability for engineers*. Seventh Edition, John Wiley & Sons, 2018.
7. Gross, Jonathan L., and Jay Yellen. *Graph theory and its applications*. CRC press, 2005.

Research Papers

1. Taylor, Ian. "Alan M. Turing: The Applications of Probability to Cryptography." *arXiv preprint arXiv:1505.04714* (2015).
2. Priyadarsini, P. L. K. "A survey on some applications of graph theory in cryptography." *Journal of Discrete Mathematical Sciences and Cryptography* 18, no. 3 (2015): 209-217. https://doi.org/10.1080/09720529.2013.878819

DSC 512 PROGRAMMING AND DATA STRUCTURE [2-0-3-3]

Objectives

The course is intended to provide the foundations of the practical implementation and usage of Algorithms and Data Structures. One objective is to ensure that the student evolves into a competent programmer capable of designing and analysing implementations of algorithms and data structures for different kinds of problems. The second objective is to expose the student to the algorithm analysis techniques, to the theory of reductions, and to the classification of problems into complexity classes like NP.

Outcomes

- Design and analyse programming problem statements.
- Choose appropriate data structures and algorithms, understand the ADT/libraries, and use it to design algorithms for a specific problem.
- Understand the necessary mathematical abstraction to solve problems.
- Come up with analysis of efficiency and proofs of correctness
- Comprehend and select algorithm design approaches in a problem specific manner.

Introduction: Introduction to Data Structures and Algorithms, Review of Basic Concepts, Asymptotic Analysis of Recurrences. Randomized Algorithms. Randomized Quicksort, Analysis of Hashing algorithms.

Algorithm Analysis Techniques - Amortized Analysis. Application to Splay Trees. External Memory ADT - B-Trees. Priority Queues and Their Extensions: Binomial heaps, Fibonacci heaps, applications to Shortest Path Algorithms. Partition ADT: Weighted union, path compression, Applications to MST. Algorithm Analysis and Design Techniques.

Dynamic Programming, Greedy Algorithms-Bellman-Ford. Network Flows-Max flow, min-cut theorem, Ford-Fulkerson, Edmonds-Karp algorithm, Bipartite Matching.

Intractable Problems: Polynomial Time, class P, Polynomial Time Verifiable Algorithms, class NP, NP completeness and reducibility, NP Hard Problems, NP completeness proofs, Approximation Algorithms.

Learning Resources

1. Introduction to Algorithms, by T. H. Cormen, C. E. Lieserson, R. L. Rivest, and C. Stein, Third Edition, MIT Press.
2. Fundamentals of Data Structures in C by Horowitz, Sahni, and Anderson-Freed, Universities Press
3. Algorithms, by S. Dasgupta, C. Papadimitrou, U Vazirani, Mc Graw Hill.
4. Algorithm Design, by J. Klienberg and E. Tardos, Pearson Education Limited.

CBM 513 COMPUTER NETWORKS AND SECURITY [2-0-3-3]

Prerequisite for the Course

No prerequisite courses. However, please consult the instructor if you are not sure about the programming requirement.

Course Objectives

1. Study of architecture and protocols of computer networks.
2. Study the ISO and Internet models; medium access control and retransmission protocols; protocol analysis and verification; data-communication principles.
3. Comprehend the necessity of network security along with the basic concept of Network security.
4. Investigate various network vulnerabilities like virus, worm, malware, rootkit and devise strategies to mitigate them.
5. Analyse privacy threatening behaviour over the internet and formulate defensive techniques to preserve privacy.

Expected Outcome

Students who successfully complete this course will be able to:-

1. List all layers and their functionality of the ISO and Internet network architectures.
2. Describe the concepts underlying the design and implementation of the major protocols at various network layers.
3. Understand the need for network security and have through grasp of the fundamentals of network security.
4. Recognise network vulnerabilities and develop Network defensive strategies by utilizing Intrusion Detection Systems, Honeypot etc.
5. Identify and defend against various privacy threatening tools and techniques over the internet.

Introduction. Overview and motivation: Telephone Network and the Internet Network, Circuit Switching vs. Packet Switching, History of the Internet.
Architecture-OSI, TCP/IP models, Physical and Data link layer protocols: Encoding, Framing, Error detection, HDLC, PPP, sliding window protocols. Network Layer protocols: Internet addressing, IP, ARP, ICMP, CIDR, Routing algorithms. Transport Layer protocols: UDP, TCP, flow control, congestion control. Application Layer protocols: DNS, Web, HTTP, email, authentication, encryption.
Introduction to Network Security, Need for Network Security, Network Security Fundamentals, Principles of Security, Working of internet and DNS Vulnerabilities, Secure Network Communication.
Malware, Insider Attack and Defence, Computer Virus Types and Defence, Computer Worms, Rootkits, Botnet, Denial of Service Attack.
Need For Physical Security, User Authentication Technologies, Environmental Attacks and Accidents, Firewall, Intrusion Detection System, Honeypot, Tunnelling, Virtual Private Network, Privacy Preserving Communication, Anonymity, Onion Routing.

Reference Books

1. Michael Goodrich, Roberto Tamassia, *Introduction to Computer Security*: Pearson publications, 2nd edition, 2021, ISBN-13: 978-0133575477.
2. L. L. Peterson and B. S. Davie, *Computer Networks: A Systems Approach*, 6th edition, Elsevier publications, 2021, Paperback ISBN: 9780128182000.
3. A. S.Tanenbaum and D.J. Wetherall, *Computer Networks*, Pearson publications, 5th Edition, 2013, ISBN-13: 978-8131770221.
4. J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th Edition, Pearson publications, 2017, ISBN-13: 9780134296159.
5. Kun Peng, *Anonymous Communication Networks: Protecting Privacy on the Web*, Auerbach publications, 2019, ISBN: 9780367378738.

6. Sagar Rahalkar, *Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit*, 1st Edition, Apress publications, 2019, Softcover ISBN: 978-1-4842-4269-8.
7. Christopher Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd Edition, Wiley Publisher, 2018, ISBN-13: 978-1119433385.

SEMESTER II

CBM 521 SECURE SOFTWARE ENGINEERING [3-0-0-3]

Prerequisite for the Course

Fundamentals of Software Engineering, UML

Course Objectives

1. Design and implementation of secure software
2. Introduce the role of security in the development lifecycle
3. To design secure software
4. To learn methodological approaches to improving software security during different phases of software development lifecycle
5. To know best security programming practices

Expected Outcome

Students who successfully complete this course will be able to:-

1. Explain terms used in secured software development and life cycle process
2. Incorporate requirements into secured software development process and test software for security vulnerability
3. Identify vulnerable code in implemented software and describe attack consequences
4. Apply mitigation and implementation practices to construct attack resistant software
5. Apply secure design principles for developing attack resistant software

Introduction & Motivation: Hacker vs. Cracker, Historical Background, Mode of Ethical Hacking, Hacker Motive, Gathering Information, Secure Software, Compliance Requirements, C-Level Language, Assets, Threats and Risks, Security Requirements, Confidentiality, Integrity, Availability

Secure Software Development Methodologies: Secure Software Development Lifecycle (SSDLC), Guidelines for Secure Software, SD-3 Principles, Security Practices, Secure coding standards, OWASP, ISO15408, Common Criteria (CC), build-insecurity

Requirements Engineering: Availability, Authenticity, Confidentiality, Efficiency, Integrity, Maintainability, Portability, Reliability, Requirements Engineering, Trustworthiness, Threat Analysis and Risk Management

Secure Architectural Design: Threat Modelling, Asset, Threat, Attack, Dataflow Diagram (DFD), Threat Tree (Attack Tree), STRIDE, DREAD. Security Architecture, Software Attack Surface, Secure, Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-based Access Control (RBAC), Access Matrix

Secure Coding and Security Testing: Introduction to Vulnerabilities, Vulnerability Patterns,

Secure Coding Practices, Code Checking, Tools, Cross Site Scripting, Injection Flaws, Cross Site Request Forgery, Denial of Service, Test Cases, Security Test Plan, White Box Test, Black Box Test, Penetration Testing, Code Review, Test Report

Secure Deployment: Secure Default Configuration, Product Life Cycle, Automated Deployment Process, Secure Target Environment, Secure Delivery of Code, Trusted Origin, Code Signing, Least Privilege Permissions, ITIL Release and Deployment Management

Security Response: Security Response, Security Bulletins, Vulnerabilities, Security Patches, Disclosure, Responsible Disclosure, Patch Tuesday, Security Response Policy, Security Response Process, Common Vulnerability Scoring System, CVSS

Code & Resource Protection: Introduction to Back Door, Time Bomb, Four-Eyes Principle, Confidentiality Classification, Background Screening, Security Clearance, Offline and Online Licensing, Mechanisms, Code Obfuscation

Reference Books

1. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw and Nancy Mead Software Security Engineering: A Guide for Project Managers by. Addison-Wesley, (2004)
2. Gary McGraw ,Software Security: Building Security, Addison-Wesley (2006)
3. Threat Modelling: Designing for Security by Adam Shostack, John Wiley and Sons Inc,
4. Mano Paul ,7 Qualities of Highly secure Software Taylor and Francis, CRC Press (2012)
5. Mark Merkow and Lakshmikanth Raghavan, Secure and Resilient Software, CRC Press, ISBN 9781439826973.

CBM 522 INFORMATION SECURITY AND APPLIED CRYPTOGRAPHY [3-0-0-3]

Prerequisite for the Course

Student should have a passing Grade in Number Theory, Discrete Mathematics.

Course Objectives

1. To lay a foundation on Security in Networks, Classical Cryptosystem and Block Cipher Modes of Operation.
2. To analyse various Private and Public key Cryptosystem for encryption, key exchange and hashing, Authentication Protocols.
3. To acquire the fundamental knowledge on applications of cryptography.

Expected Outcome

Students who successfully complete this course will be able to:-

1. Understand the fundamental concepts of Classical and modern Cryptosystem.
2. Compare various private and public key Cryptosystem for encryption, key exchange and authentication algorithms.
3. Understand the different applications of cryptography.

INTRODUCTION – Cryptography, cryptanalysis, cryptology, classical cryptosystem- shift cipher, affine cipher, Vignere cipher, substitution, transposition techniques,
BLOCK CIPHERS AND MODES OF OPERATIONS- DES - Data Encryption Standard-Block cipher principles-block cipher modes of operationAES-TripleDES-Blowfish-RC5
PUBLIC KEY CRYPTOGRAPHY- Public Key Cryptosystem, Key distribution, Diffie Hellman Key Exchange-MITM Attack - RSA, Random Number Generation-ECC-Key Management
HASH FUNCTIONS AND DIGITAL SIGNATURES- Authentication requirement– Authentication function – MAC – Hash function – SHA - HMAC - Digital signature and authentication protocols.
APPLICATIONS- Authentication – Kerberos, IP Security – IPSec, Web Security - SSL, TLS, Blockchain, IoT Security.

Reference Books

1. William Stallings, Cryptography and Network Security –6th Edition, Pearson Education.
2. Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 5nd Edition, Mc Graw Hill Education.
3. Rich Helton, Johennie Helton, Mastering Java Security: Cryptography Algorithms and Practices, John Wiley Publishers.
4. Charles P. Pleeger, “Security in Computing”, Pearson Education Asia, 5th Edition.
5. William Stallings, “Network Security Essentials: Applications and standards”, Person Education Asia.
6. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security: Private Communication in a public world”, Prentice Hall India, 6th Edition.

CBM 523 DECISION SUPPORT AND ARTIFICIAL INTELLIGENCE [2-0-0-3]

Course Objectives

- An overview of different Decision support system and Machine Learning models
- Using Machine Learning for effective security
- Various attack on ML models
- Machine Learning and Privacy

Expected Outcome

- Understand the concepts in Machine Learning
- Learn how to use machine learning for solving cyber security issues

Introduction: data science, data analytics, machine learning, and Artificial Intelligence. Programming in Python, Basics of manipulation of Data. Introduction to modern data analysis (Data visualization; probability; histograms; multinomial distributions),

Machine Learning Overview: Types of learning, Supervised, Unsupervised, Application in Security

Deep Learning Overview: Applying Deep Learning in various use cases, anomaly detection

Artificial Intelligence in Cyber Security: Model Stealing & Watermarking, Network Traffic Analysis, Network Traffic Analysis

Reference Books

1. Tom Mitchell. Machine Learning. McGraw Hill, 1997.
2. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.
3. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.
4. Deep Learning by Ian Goodfellow, Yoshua Bengio, and Aaron Courville
5. Cathy O'Neil and Rachel Schutt. Doing Data Science, Straight Talk from The Frontline. O'Reilly. 2014.

SEMESTER III

CBM 611 OPERATING SYSTEM SECURITY [3-0-0-3]

Prerequisite for the Course

Fundamentals of Operating Systems, Basic programming.

Course Objectives

1. Learn security of operating systems.
2. Learn relevant tools to secure operating systems.
3. Learn how to enforcing mandatory access control.
4. General information security.

Expected Outcome

1. Students who successfully complete this course will be able to:-
2. Identify and define key terms related to operating systems.
3. Learn, and understand the main concepts of advanced operating systems design.
4. Develop ability to protect operating systems.
5. Improve the security of operating systems from malicious software.
6. Learn OS issues related to the Internet, intranets, pervasive computing, embedded systems, mobile systems and wireless networks.
7. Learn to design a secure operating system

Fundamentals- OS Processes, Synchronization, Memory Management, File Systems Trusted Operating Systems, Assurance in Trusted Operating Systems, Virtualization Techniques.
Secure operating systems- Security goals, Trust model, Threat model
Access Control Fundamentals – Protection system – Lampson's Access Matrix, Mandatory protection systems, Reference monitor.
Multics – Multics system, Multics security, Multics vulnerability analysis
Security in Ordinary OS – Unix, Windows,
Verifiable security goals – Information flow, Denning's Lattice model, Bell-Lapadula model, Biba integrity model, Covert channels.
Security Kernels – Secure Communications processor, Securing Commercial OS
Secure Capability Systems – Fundamentals, Security, Challenges
Secure Virtual Machine Systems
Case study - Linux kernel, Android, DVL, Solaris Trusted Extensions

Reference Books

1. Andrew S. Tanenbaum, *Modern Operating Systems*, Third Edition, Prentice Hall, 2007.
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, *Operating System Concepts*
3. *with Java*", Eighth Edition, Wiley, 2008.
4. Trent Jaeger, *Operating System Security, Synthesis Lectures on Information Security*,
5. *Privacy and Trust*, Morgan and Claypool, 2008.
6. C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, Prentice Hall Professional, 2003.
7. W. Mauerer, *Professional Linux Kernel Architecture*, Wiley, 2008.
8. D. P. Bovet and M.Cesati, *Understanding the Linux Kernel*, Third Edition, O'Reilly Media, Inc., 2005.

CBM 612 ADVANCED DATABASE SECURITY [3-0-0-3]

Prerequisite for the Course

Database Management System.

Course Objectives

1. Introduce the database and its security issues.
2. Compare in details the various state-of-art database security methods and techniques.
3. Learn in detail the security features in databases.
4. Understand the database security analysis tools.

Expected Outcome

Students who successfully complete this course will be able to:-

1. Understand and characterize modern techniques of database information security threats and techniques for database security assessment.
2. Analyze information in a database to identify information security incidents
3. Understand and use the main tools for database management systems monitoring.
4. Apply build-in database functions to enable database integrity support.
5. Create a plan for vulnerabilities detection and identification in databases.

Introduction-Database System Applications, Purpose of Database Systems, View of Data - Data Abstraction, Instances and Schemas, ER diagrams, Introduction to the Relational Model - Querying relational data, Form of Basic SQL Query - Examples of Basic SQL Queries.
Introduction to database security issues- The role of databases in information systems. Access control management features. Cryptographic data protection. SQL language features, Statistical databases.

Database security methods and techniques- Access control to database objects: tables, attributes, records. Triggers, views, data masking. Cryptographic methods of protection. Escaping queries to a database. Change Tracking. Data integrity in the databases. Database backups.
Security features in databases- SQL statements for access control. Integrity (domain, attributes, tables, referential). Database monitoring tools.
Database security analysis tools- An overview of the main methods for analyzing database security. SQL injections. Database security scanners. Writing your own security analysis tools.

References Books

1. Basta A., Zgola M, "Database Security" 3nd Edition, Cengage Learning, US, 2011
2. Ron Ben Natan, "Implementing database security and auditing", Digital Press, 2005.
3. Bhavani Thuraisingham, Database and Applications Security, Auerbach Publications, 2005.
4. Rose Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001.
5. Michael Gertz, Sushil Jajodia, Handbook of Database Security Applications and Trends, Springer, 2008.
6. Silvana Castano, Database Security, ACM Press. Alfred Basta, Melissa Zgola, Database Security, Cengage Learning.

CBM 613 SECURE HARDWARE DESIGN [3-0-0-3]

Prerequisite for the Course

Digital System Design, Cryptography

Course Objectives

1. To address the different security threats on modern hardware design
2. To introduce and implement cryptographic algorithms on hardware
3. To understand and implement various hardware security measurements

Expected Outcome

Students who successfully complete this course will be able to:-

1. Demonstrate proficiencies in hardware implementations of a popular crypto primitive.
2. Demonstrate proficiencies in understanding hardware security issues.
3. Demonstrate proficiencies in understanding hardware security primitives.
4. Demonstrate proficiencies in applying cryptography and security primitives to address hardware security issues.
5. Demonstrate critical thinking and analytical skills through a summary and evaluation of an open hardware security problem.

Introduction - Hardware Security & Trust, Security & Protection Objectives, Why choose hardware? - Performance, Protection Environment, Scalability

Security by design- Physical or implementation attacks- Side-channel attacks- Hardware reverse engineering attacks- Hardware Trojans.

FPGAs - FPGA Versus Software Programming: Why, When, and How?, High-Level Synthesis, High-Level Synthesis Solutions for FPGAs.

The role of cryptography- Modern Cryptography: PKE, RSA, AES, SIMON, Working together

Useful Hardware Security Primitives: Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA, Physically Unclonable Functions (PUFs), PUF Implementations.

Side-channel Attacks on Cryptographic Hardware: Basic Idea, Current-measurement based Side-channel Attacks (Case Study: Kocher's Attack on DES), Design Techniques to Prevent Side-channel Attacks, Cache Attacks.

Hardware Trojans: Hardware Trojan Nomenclature and Operating Modes, Countermeasures Such as Design and Manufacturing Techniques to Prevent/Detect Hardware Trojans, Logic Testing and Side-channel Analysis based Techniques for Trojan Detection, Impact of Hardware Security Compromise on Public Infrastructure, Defense Techniques.

Reference Books

1. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press
2. Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer.
3. M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2012.
4. Koch, D., Hannig, F., & Ziener, D. (Eds.). (2016). FPGAs for software programmers. Berlin, Germany: Springer.
5. Ted Huffmire et al: Handbook of FPGA Design Security, Springer.
6. Stefan Mangard, Elisabeth Oswald, Thomas Popp: Power analysis attacks - revealing the secrets of smart cards. Springer 2007.
7. Doug Stinson, Cryptography Theory and Practice, CRC Press.
8. Wagner, M. (2016). The hard truth about hardware in cyber-security: it's more important. Network Security, 2016(12), 16-19.

CBM 614 BLOCKCHAIN ARCHITECTURE AND APPLICATIONS [3-0-0-3]

Prerequisite for the Course

Computer Networks, Cryptography, Linux Commands

Course Objectives

1. Introduce the concept and the basics of blockchain technologies,
2. Enable awareness on the different generations of blockchains.
3. Provide knowledge on various applications of blockchain technologies

Expected Outcome

Students who successfully complete this course will be able to:-

1. Understand the basics of blockchain Technologies and its various applications.
2. Implement blockchain ledgers.
3. Capable to identifying problems on which blockchains could be applied.

Introduction – Blockchain history, basics, architectures, Types of blockchain, Base technologies – Dockers, Hash function, Digital Signature - ECDSA, Zero Knowledge Proof.
Bitcoins – Fundamentals, aspects of bitcoins, properties of bitcoins, bitcoin transactions, bitcoin P2P networks, block generation at bitcoins, consensus algorithms- Proof of Work, Proof of Stake, Proof of Burn.
Blockchain hyperledger – Fabric architecture, implementation, networking, fabric transactions, demonstration, smart contracts.
Applications – Blockchain applications, e-governance, smart cities, smart industries, anomaly detections, use cases, trends on Blockchains, serverless blocks, scalability issues, blockchain on clouds.

Reference Books

1. Baxv Kevin Werbach, The Blockchain and the new architecture of Trust, MIT Press, 2018
2. Joseph J. Bambara and Paul R. Allen, Blockchain – A practical guide to developing business, law, and technology solutions, McGraw Hill, 2018.
3. Joseph J. Bambara and Paul R. Allen, Blockchain, IoT, and AI: Using the power of three to develop business, technical, and legal solutions, Barnes & Noble publishers, 2018.
4. Melanie Swan, Blockchain – Blueprint for a new economy, OReilly publishers, 2018.
5. Jai Singh Arun, Jerry Cuomo, Nitin Gaur, Blockchain for Business, Pearson publishers, 2019.
6. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

SEMESTER IV

CBM 621 FORENSICS, MALWARE, AND PENETRATION TESTING [3-0-3-4]

Prerequisite for the Course

Student should have a passing Grade in CBM 513 (Computer Networks and Security) and CBM 522 (Information Security and Applied Cryptography) or the instructor's approval.

Course Objectives

1. Introduces the concepts of Penetration testing.
2. Gives the students the opportunity to learn about different tools and techniques for penetration testing and security.
3. Practically apply penetration testing tools to perform various activities.

Expected Outcome

Students who successfully complete this course will be able to:-

1. Understand the core concepts related to vulnerabilities and their causes.
2. Understand ethics behind hacking and vulnerability disclosure.
3. Comprehend the impact of Hacking.
4. Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies.

Introduction and Information Security Overview, Hacking and Ethical hacking concepts, Hacker behaviour & mindset, Hacking Methodology.
Footprinting Concepts and Methodology, Footprinting Tools and Countermeasures, Active and Passive Sniffing, Network Scanning Concepts and Tools, Preparation of Ethical Hacking and Penetration Test Reports and Documents.
Social Engineering attacks and countermeasures, Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing.
DoS attacks. Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client-side browser exploits, privilege escalation.
Metasploit framework, Metasploit Console, Payloads, Metrpreter, Introduction to Armitage, Introduction to penetration testing tools in Kali Linux.

Reference Books

1. Baloch, R., *Ethical Hacking and Penetration Testing Guide*, Auerbach Publications, CRC Press, 2015.
2. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, *Metasploit: The Penetration Tester's Guide*, No Starch Press, 2011, ISBN: 159327288X,9781593272883.
3. Sagar Rahalkar, *Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit*, 1st Edition, Apress publications, 2019, Softcover ISBN: 978-1-4842-4269-8.
4. Christopher Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd Edition, Wiley Publisher, 2018, ISBN-13: 978-1119433385.
5. Glen D. Singh, *Learn Kali Linux 2019: Perform Powerful Penetration Testing Using Kali Linux, Metasploit, Nessus, Nmap, And Wireshark*, Packt Publishing, 2019, ISBN: 1789611806.
6. Michael Hixon, Justin Hutchens, Kali Linux. Network Scanning Cookbook, Packt Publishing, 2017, ISBN: 139781787287907

CBM 622 LEGAL ASPECTS OF COMPUTING [2-0-0-2]

Prerequisite for the Course

None.

Course Objectives

The course deals with all the aspects of Cyber law as per Indian/IT act. It also covers overview of Intellectual Property Right and Trademark Related laws with respect to Cyber Space.

Expected Outcome

Students who successfully complete this course will be able to demonstrate a critical understanding of the Cyber law with respect to Indian IT/Act and Intellectual Property Rights.

Cyber Crimes Categories and kinds, Evolution of the IT Act, IT Act, 2000, various authorities under IT Act and their powers. Penalties & Offences, amendments.
Case Laws on Cyber Space Jurisdiction and Jurisdiction issues under IT Act, E –commerce and Laws in India, Digital / Electronic Signature in Indian Laws.
Intellectual Property Rights, Domain Names and Trademark Disputes, Copyright in Computer Programmes, Concept of Patent Right, Sensitive Personal Data or Information in Cyber Law, Cyber Law an International Perspective.

Reference Books

1. Sushma Arora, Raman Arora, *Cyber Crimes & Laws*, 4th Edition 2021, Publisher: Taxmann, ISBN-10: 9390712491
2. N S Nappinai, *Technology Laws Decoded*, 1st Edition, Publisher: Lexis Nexis, ISBN: 9789350359723
3. Suresh T. Vishwanathan, The *Indian Cyber Law*, Bharat Law House New Delhi
4. P.M. Bukshi and R.K. Suri, *Guide to Cyber and E –Commerce Laws*, Bharat Law House, New Delhi
5. Rodney D. Ryder, *Guide to Cyber Laws*; Wadhwa and Company, Nagpur
6. The Information Technology Act, 2000; Bare Act –Professional Book Publishers, New Delhi

CBM 623 CRIMINAL PSYCHOLOGY AND BEHAVIOUR INTELLIGENCE [1-0-0-1]

Prerequisite for the Course

None.

Course Objectives

1. To makes the students familiar with the field of Criminal Psychology.
2. To make the students understand the origins of Criminal Behaviour.

Expected Outcome

Students who successfully complete this course should have a comprehensive understanding of Criminal Behaviour and Psychological aspects of various crimes.

Nature and History of Criminal and Forensic Psychology, Social context of Crime: Extent of Criminality, Changing nature of Crime: Conservative and Radical interpretations in complexity of victimization.

Types of Offenders, Violent Offenders: Media influences and Research Statistics, Theories of Homicide: Psychological disposition, Socio-Biological theory and Multi-Factorial Approach.

Mental Illness and Crime: Problem of evidence; Mental illness and Crime in general.

Eyewitness Testimony: Accuracy of witness evidence in Court, Witness confidence and improving the validity of line-up, Clinical approaches in Risk and danger assessment.

Reference Books

1. Dennis Howitt, *Introduction to Forensic and Criminal Psychology*, 6th Edition, Publisher: Pearson, 2018
2. Wayne Petherick Brent Turvey Claire Ferguson, *Forensic Criminology*, 1st Edition, Publisher: Elseiver, ISBN: 9780123750716
3. Bruce Arrigo Stacey Shipley, *Introduction to Forensic Psychology*, 2nd Edition, Publisher: Academic press, ISBN: 9780080468532