INDIAN INSTITUTE OF INFORMATION TECHNOLOGY KOTTAYAM

Curriculum and Syllabus for the PG Course e-MTech Programme in Cyber Security and Digital Forensics

Contents

e-MTech in Cyber Security and Digital Forensics
General Course Structure

Semester- I					
Course Code	Course Name	**L**	**T**	**P**	**C**
CBM511	Mathematical Foundations for Cyber Security	2	0	0	2
CBM513	Computer Networks and Security	2	0	2	3
CBM524	AI, Machine Learning and Security	2	0	2	3
DSC523	Data Mining	3	0	0	3
CBM613	Operating System Security	3	0	0	3
Semester- II					
CBM521	Secure Software Engineering	3	0	0	3
CBM522	Information Security and Applied Cryptography	2	0	2	3
CBM616	Network,Wireless ~~, IoT & Mobile~~ & IoT Security	2	0	2	3
CBMXXX	Digital Forensic s	2	0	2	3
Semester- III					
CBMXXX	Malware and Penetration Testing	2	0	2	3
CBM615	Blockchain Architecture and Applications	2	0	0	2
CBMXXX	Legal and Ethical Issues in Computing	1	0	0	1
CBE711	Project(Phase I)				14
Semester- IV					
CBE721	Project(Phase II)				14
Total Credits					60

L	T	P	C
2	0	0	2

SEMESTER I

CBM511 Mathematical Foundations for Cyber Security

Pre-requisites

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

Course Objectives

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

Course Outcomes

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

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

Syllabus

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.

Learning Resources

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

L	T	P	C
2	0	2	3

DSC512 Programming and Data Structures

Course 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.

Course 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.

Syllabus

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.

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

L	T	P	C
2	0	2	3

CBM513 Computer Networks and Security

Course Objectives

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

Course Outcomes

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

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

Syllabus

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.

Learning Resources

1. Michael Goodrich, Roberto Tamassia, Introduction to Computer Security: Pearson publications, 2nd edition, 2021, ISBN-13: 978-0133575477. 2
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.

L	T	P	C
2	0	2	3

CBM524 AI, Machine Learning and Security

Course Objectives

-
- An overview of different AI and Machine Learning models in Cyber Security
- Using Machine Learning for effective security
- Various attack on ML models
- Machine Learning and Privacy

Course Outcomes

- Understand the concepts in Machine Learning
- Learn various AI and Machine learning models for cyber security
- Ability to apply AI and machine learning models in cyber security issues

Syllabus

Introduction: Role of AI in Cyber Security and Security Framework: Artificial Intelligence in Cyber Security, Challenges and Promises, Security Threats of Artificial Intelligence, Use-Cases: Artificial Intelligence Email Observing, Programming in Python,Basics of manipulation of Data.

Machine Learning in Security: Introduction to Machine Learning, Applications of Machine Learning in Cyber Security Domain, Machine Learning: tasks and Approaches, Anomaly Detection, Privacy Preserving Nearest Neighbour Search, Machine Learning Applied to Intrusion Detection, Online Learning Methods for Detecting Malicious Executables.

Deep Learning in Security: Introduction to deep learning, Cyber Security Mechanisms Using Deep Learning Algorithms, Applying deep learning in various use cases, Network Cyber threat Detection.

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

Learning Resources

1. Tom Mitchell. Machine Learning. McGraw Hill, 1997.
2. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.

3. Artificial Intelligence and Data Mining Approaches in Security Frameworks, Editor(s):Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.

4. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy, and reliability. Springer Science & Business Media, 2009.

5. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press. 6. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.

L	T	P	C
3	0	0	3

CBM613 Operating System Security

Course Objectives

- Learn security of operating systems.
- Learn relevant tools to secure operating systems.
- Learn how to enforce mandatory access control.
- General information security.

Course Outcomes

Students who successfully complete this course will be able to

- Identify and define key terms related to operating systems.
- Learn, and understand the main concepts of advanced operating systems design.
- Develop ability to protect operating systems.
- Improve the security of operating systems from malicious software.

Syllabus

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.

Learning Resources:

1. Andrew S. Tanenbaum, Modern Operating Systems, Third Edition, Prentice Hall, 2007.
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, Operating System Concepts with Java", Eighth Edition, Wiley, 2008.

3. Trent Jaeger, Operating System Security, Synthesis Lectures on Information Security, Privacy and Trust, Morgan and Claypool, 2008.

4. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, Prentice Hall Professional, 2003.

5. W. Mauerer, Professional Linux Kernel Architecture, Wiley, 2008.

6. D. P. Bovet and M.Cesati, Understanding the Linux Kernel, Third Edition, O'Reilly Media, Inc., 2005.

L	T	P	C
3	0	0	3

SEMESTER II

CBM 521 Secure Software Engineering

Course Objectives

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

Course Outcomes

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

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

Syllabus

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.

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

Learning Resources

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.

L	T	P	C
2	0	2	3

CBM522 Information Security and Applied Cryptography

Pre-requisites

Mathematical Foundations for Cyber Security (CBM 511)

Course Objectives

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

Course Outcomes

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

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

Syllabus

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.

Learning Resources

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.

L	T	P	C
2	0	2	3

CBM616 Network,Wireless ~~, IoT & Mobile~~ & IoT Security

Pre-requisites

- Computer Networks and Security
- Programming and Data Structure

Course Objectives

- ~~Introduce the concept and the basics of Wireless, IoT and Cloud technologies.~~
- Introduce the concepts and basics of Wireless and IoT technologies.
- Analyze various secured Wireless Communication Protocols for IoT Infrastructure.
- Provide knowledge on various applications of IoT based technologies and their associated circuits.
- Enable awareness on the different IoT Vulnerabilities, Attacks, and security methods

Course Outcomes

Students who successfully complete this course will be able to:

- ~~Learn the basics of communication in wireless sensor network, Cloud Computing.~~
- Learn the basics of communication in wireless sensor network and IoT.
- Compare various secured Wireless Communication Protocols for IoT Infrastructure.
- Understand the various applications of IoT
- Design IoT based applications using Arduino or Raspberry PI boards.
- Understand the various attacks and different security measures in IoT infrastructure.

Syllabus

Introduction: Basics of networking - wired, wireless, MANET, PAN, Wireless Sensor Networks, M2M Communication. Secured Wireless Communication Protocols for IoT Infrastructure-IPv6 -LowPAN, LoRa, Transport-Bluetooth- LPWAN, Data -MQTT –CoAP

IoT architectures and programming- basic architectures, Sensor basics, sensing and actuation, sensor communications, connectivity challenges Data processing mechanisms, scalability issues, visualization issues, analytics basics, the utility of cloud computing, fog computing, and edge computing, advanced IoT architectures Raspberry Pi and Arduino programming.

IoT security: Vulnerabilities, Attacks, and countermeasures - security engineering for IoT development - IoT security lifecycle.

Privacy preservation models in IoT -Trust and Authentication models in IoT - Wireless Communication for Industrial IoT - Security in Industrial IoT, and Best Practices.

Learning Resources

1. Pethuru Raj and Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases, CRC Press, First edition, 2017.
2. B. Rusell and D. Van Duren, "Practical Internet of Things Security," Packt Publishing, 2016.
3. Fei HU, "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations", CRC Press, 2016.
4. Honbu Zhou, The Internet of Things in the Cloud: A Middleware Perspective, CRC press, First edition, 2012.
5. Arshdeep Bahga and Vijay Madisetti, Internet of Things: A Hands-on Approach, Universities Press, First edition, 2014.
6. Mung Chiang, Bharath Balasubramanian, Flavio Bonomi, Fog for 5G and IoT (Information and Communication Technology Series, Wiley series, First edition, 2017.
7. Alan A. A. Donovan, Brian W. Kernighan, The Go Programming Language, Addison Wesley Professional Computing Series, First edition, 2015.

L	T	P	C
2	0	2	3

CBMXXX Digital Forensics

Course Objectives

- Understand the principles and stages of digital forensic investigation.
- Understand how to acquire digital data forensically following best practices
- Perform analysis over evidence extracted from computers and mobile devices
- Prepare reports by analysing digital forensic evidence
- Understand the android architecture, file system and apk reverse engineering.

Course Outcomes

At the end of this course, students will be able to:

- Acquire data forensically from memory and hard disk utilizing forensic tools
- Analyse memory to detect presence of malicious executables utilizing Volatility
- Analyse artifacts from RAM, Hard disk and mobile phones utilizing forensic software's
- Prepare forensic reports utilizing forensic tools
- Analyse a mobile apk using reverse Engineering.

Syllabus

Introduction: Computer Forensics Investigation Process, Challenging Aspects of Digital Evidence, Features of forensic tools, Anti forensics techniques and mitigation.

Data Acquisition and Memory Analysis: Data Acquisition of memory and disk using Forensic Tools, Analysis of Artifacts in RAM, Memory Forensics to detect malicious executables, Volatility Framework and Plugins to conduct memory forensics.

Artifact Analysis and Reporting: Understanding Hard disks and File systems, Analysis of artifacts from Registry, Operating System, Web, Email, Media and Cloud. Tagging and Reporting of artifacts.

Mobile Application Forensics and Reverse Engineering: Mobile Forensic Investigation process, Android Architecture, File hierarchy, Mobile artifact analysis, Reverse Engineering an APK

Tools Used: FTK Imager, Dumpit, Volatility Framework, Autopsy, Magnet Axiom, Registry Explorer, Android Debug Bridge, Apk tool, Jadx.

Learning Resources

1. Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, 6th edition, Publisher Cengage Learning.

2. Magnet Forensics AXIOM Academic Curriculum Manual (Provided by Instructor)

3. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory Published by John Wiley & Sons, Inc.

4. Tamma, Rohit, and Donnie Tindall. Learning android forensics. Packt Publishing Ltd, 2015.

L	T	P	C
2	0	2	3

SEMESTER III

CBMXXX Malware and Penetration Testing

Course Objectives

- Introduce penetration testing fundamentals, methodologies, and reporting.
- Develop skills in reconnaissance, social engineering, and OSINT.
- Perform network, wireless, and web application exploitation.
- Understand post-exploitation techniques and security countermeasures.

Course Outcomes

Students who complete this course will be able to:

- Apply penetration testing techniques to assess security risks.
- Conduct reconnaissance and social engineering attacks.
- Exploit vulnerabilities in networks, wireless systems, and web apps.
- Implement post-exploitation tactics and recommend mitigations.

Syllabus

Introduction: Important Terminologies - Categories of Penetration Testing - Writing Reports - Fundamentals of Linux - Risk Assessments

Social Engineering and Information Gathering: Fundamentals of social engineering - Types of Social Engineering - Phishing - Creating Infectious Media, Passive Reconnaissance - Profiling Target Organization IT Infrastructure - Gathering Employee's Data, Active Reconnaissance - DNS Reconnaissance - Enumerating Common Network Services, OSINT Strategies - Social Media Reconnaissance

Network Penetration Testing: Profiling Target Systems - Password Based Attacks - Identifying and Exploiting Vulnerable Services - Post Exploitation - Data Encoding and Exfiltration - MITM and Packet Sniffing Attacks

Wireless Penetration Testing: Introduction to Wireless Networking - Performing Wireless Reconnaissance - Compromising WPA & WPA2 Networks - Wi-Fi Honeypots - WPA3 Attack

Web application pen testing: Overview of Web and Related Technologies - Static and Dynamic Web Applications, HTTP Methods and Response Codes - OWASP top 10 vulnerabilities

- Client-Side Attacks - Server-Side Attacks

Learning Resources

Text Books:

1. The Ultimate Kali linux Book, Glen D. Singh, Second Edition, 2022, packt Publishing.
2. Ethical Hacking and Penetration Testing Guide, Rafay Baloch, 2025, CRC Press Taylor & Francis Group

Reference Books:

1. Metasploit The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, and Aharoni, 2011, William pollock.
2. Social Engineering The science of Human Hacking, Christopher Hadnagy, 2018, John Wiley & Sons.
3. Kali Linux Network Scanning Cookbook, Michael Hixon, Justin Hutchens, Second Edition, 2017, Packt Publishing.
4. Ethical Hacker's Penetration Testing Guide, Samir Kumar Rakshit, First Edition, 2022, BPB Publications

L	T	P	C
2	0	0	2

CBM615 Blockchain Architecture and Applications

Pre-requisites

- Computer Networks and Security
- Information Security and Applied Cryptography

Course Objectives

- Introduce the concept and the basics of blockchain technologies
- Enable awareness on the different generations of blockchains
- Provide knowledge on various applications of blockchain technologies

Course Outcomes

Students who successfully complete this course will be able to:

- Understand the basics of blockchain Technologies and its various applications
- Capable of identifying problems on which blockchains could be applied.

Syllabus

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.

Ethereum- Introduction to Ethereum, Consensus Mechanisms, Smart Contracts

Applications – Blockchain applications, e-governance, smart cities, smart industries, Finance, Medical Record Management System, use cases, trends on Blockchains.

Learning Resources

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.

L	T	P	C
1	0	0	1

CBMXXX Legal and Ethical Issues in Computing

Pre-requisites

None.

Course Objectives

- Cover various aspects of Cyber law as per Indian/IT act and E-Commerce Ethics.
- Determining the impact of Privacy Laws on Information Security.

Course Outcomes

Students who successfully complete this course will be able to:

- Demonstrate an understanding of the Cyber law with respect to Indian IT/Act and E-Commerce Ethics.
- Understand the importance and significance of Data Privacy Law.

Syllabus

Introduction and Challenges associated with Cyber Crimes, Purpose of Law, Legal Rights, Evolution of the IT Act, IT Act, 2000, Components of Cyber law, Penalties & Offences, amendments.

Case Laws on Cyber Space Jurisdiction and Jurisdiction issues under IT Act, Electronic Signature in Indian Laws, E-Commerce Ethics and Case Studies. Online payment and Security issues, Consumer Protection Act and E-commerce.

Learning Resources

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.