MAHATMA GANDHI INSTITUTE OF TECHNOLOGY (Autonomous)

B.Tech. Minor in Cyber Security
Scheme of Instruction and Examination
Applicable for the batches admitted from the academic year 2022-23
(MR22 - Regulations)

S.No	Year/Semester	Course Code	Course Title	Instruction Hours Per Week			Credits
				L	T	P	
1	V -Semester	M155AB	Principles of Information Security	3	0	0	3
2	V - Semester	M15502	Principles of Information Security Lab	0	0	3	1.5
3	VI - Semester	M156AB	Foundations of Cyber Security	4	0	0	4
4	VII - Semester	M157AE M157AF	Either Online through MOOCS or off-line Class: Ethical Hacking / Digital Forensics	3	0	0	3
5	VII - Semester	M15705 M15706	The Corresponding lab: Ethical Hacking / Digital Forensics Lab	0	0	3	1.5
6	VIII - Semester	M158AM M158AN M158AP M158AQ M158AR M158AS	Elective: Any **ONE** of the following subjects 1. Security Incident & Response Management 2. Mobile Security 3. IoT Security 4. Blackchain Technologies 5. Authentication Techniques 6. Cloud Security	3	0	0	3
7	VIII - Semester	M15803	Mini Project	0	0	0	2
						Total Credits	**18**

L: Lecture **T**: Tutorial **P**: Practical

B.Tech. Cyber Security (Minor) V SEMESTER

L	T	P	C
3	0	0	3

M155AB: PRINCIPLES OF INFORMATION SECURITY

Prerequisites: A Course on "Mathematics".

Objectives:

1. To understand the fundamentals of Computer Networks.
2. To understand the fundamentals of Cryptography.
3. To understand various Symmetric and Asymmetric encryption algorithms.
4. To understand Mathematics of Cryptograph y, IDS and Firewalls.
5. To apply algorithms used for message Integrity and Authentication.

Outcomes:

1. Demonstrate the knowledge of Compute r Networks, Cryptography, Information security concepts and applications.
2. Ability to apply security principles in system design.

UNIT - I

Introduction to Computer Networks, Network hardware, Network software, OSI and TCP/IP Reference models, Security attacks, Security Services and Mechanisms.

UNIT - II

Integer Arithmetic, Modular Arithmetic, Traditional Symmetric Key Ciphers, Data Encryption Standard (DES), Advanced Encryption Standard (AES).

UNIT - III

Mathematics of Cryptography: Primes, Primality Testing, Factorization, Chinese Remainder Theorem, Asymmetric Cryptography: Introduction, RSA Cryptosystem, Rabin Cryptosystem, Elliptic Curve Cryptosystem,

UNIT - IV

Message Integrity and Message Authentication: Message Authentication Code (MAC), SHA-512 - Digital Signatures.

UNIT - V

Security at the Application Layer: PGP and S/MIME. Security at Transport Layer: SSL and TLS. - Principles of IDS and Firewalls.

TEXT BOOKS:

1. Computer Networks, Andrew S Tanenbaum, David. j. Wetherall, 5th Edition. Pearson Education / PHI.
2. Cryptography & Network Security by Behrouz A. Forouzan. Special Indian Edition, TMH.

REFERENCE BOOK:

1. Network Security Essentials (Applications and Standards), William Stallings Pearson Education.

B.Tech. Cyber Security (Minor) V SEMESTER

L	T	P	C
0	0	3	1.5

M15502: PRINCIPLES OF INFORMATION SECURITY LAB

Prerequisites

A Course on "Mathematics

Objectives

1. To apply algorithms on various Symmetric and Asymmetric encryption algorithms.
2. To demonstrate IDS Tools
3. To apply algorithms used for message Integrity and Authentication

Lab Exercises

1. Write a program to perform encryption and decryption using the following substitution ciphers.
2. Caeser cipher
3. Play fair cipher
4. Hill Cipher
5. Write a program to implement the DES algorithm.
6. Write a program to implement RSA algorithm.
7. Calculate the message digest of a text using the SHA-1 algorithm.
8. Working with sniffers for monitoring network communication (Wireshark).
9. Configuring S/MIME for email communication.
10. Using Snort, perform real time traffic analysis and packet logging.

TEXT BOOKS:

1. "Cryptography and Network Security" by William Stallings 3rd Edition, Pearson Education.
2. "Applied Cryptography" by Bruce Schneier.

REFERENCE BOOK:

1. Cryptography and Network Security by Behrouz A. Forouzan.

B.Tech. Cyber Security (Minor) VI SEMESTER

L	T	P	C
4	0	0	4

M156AB: FOUNDATIONS OF CYBER SECURITY

Prerequisites

1. Knowledge in information security and applied cryptography.
2. Knowledge in Operating Systems.

Course Objectives:

1. To introduce security attacks.
2. To get an exposure to malwares.
3. To gain knowledge on Intrusion detection & prevention systems.

Course Outcomes: Students will learn the fundamental concepts required in the field of cyber security.

UNIT - I

Overview: Computer Security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy.

Access Control: Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control, Example: UNIX File Access Control, Role-Based Access Control, Attribute-Based Access Control, Identity, Credential, and Access Management, Trust Frameworks, Case Study: RBAC System for a Bank.

UNIT - II

Malicious Software: Types of Malicious Software (Malware), Advanced Persistent Threat, Propagation - Infected Content - Viruses, Propagation - Vulnerability Exploit - Worms, Propagation - Social Engineering - Spam E-Mail, Trojans , Payload - System Corruption, Payload - Attack Agent - Zombie, Bots, Payload - Information Theft - Keyloggers, Phishing, Spyware, Payload – Stealthing - Backdoors, Rootkits, Counter measures .

Denial-of-Service Attacks: Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of-Service Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defenses Against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack.

Buffer Overflow: Stack Overflows, Defending Against Buffer Overflows, Other Forms of Overflow Attacks.

UNIT - III

Intrusion Detection: Intruders, Intrusion Detection, Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection, Distributed or Hybrid Intrusion Detection, Intrusion Detection Exchange Format, Honeypots, Example System: Snort.

Firewalls and Intrusion Prevention Systems: The Need for Firewalls, Firewall Characteristics and Access Policy, Types of Firewalls, Firewall Basing, Firewall Location and Configurations, Intrusion Prevention Systems, Example: Unified Threat Management Products.

UNIT - IV

Software Security: Software Security Issues, Handling Program Input, Writing Safe Program Code, Interacting with the Operating System and Other Programs, Handling Program Output.

Physical and Infrastructure Security: Overview, Physical Security Threats, Physical Security Prevention and Mitigation Measures, Recovery from Physical Security Breaches, Example: A Corporate Physical Security Policy, Integration of Physical and Logical Security.

UNIT - V

Human Resources Security: Security Awareness, Training, and Education, Employment Practices and Policies, E-Mail and Internet Use Policies, Computer Security Incident Response Teams.

Legal and Ethical Aspects: Cybercrime and Computer Crime, Intellectual Property, Privacy, Ethical Issues.

TEXT BOOK:

1. William Stallings, “Computer Security: Principles and Practice”, Prentice Hall. Prentice Hall; 2014.

REFERENCE BOOKS:

1. Ankit Fadia, “The ethical hacking guide to corporate security”, McMillan India.
2. G. McGraw, “Software Security: Building Security In”, Addison Wesley, 2006.

B.Tech. Cyber Security (Minor) VII SEMESTER

L	T	P	C
3	0	0	3

M157AE: ETHICAL HACKING

Prerequisites:

1. A course on “Operating Systems”.
2. A course on “Computer Networks”.
3. A course on “Network Security and Cryptography”.

Course Objectives:

1. The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing security.
2. The course includes-Impacts of Hacking; Types of Hackers; Information Security Models;
3. Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

Course Outcomes:

1. Gain the knowledge of the use and availability of tools to support an ethical hack
2. Gain the knowledge of interpreting the results of a controlled attack
3. Understand the role of politics, inherent and imposed limitations and metrics for planning of a test
4. Comprehend the dangers associated with penetration testing

UNIT- I

Introduction: Hacking Impacts, The Hacker Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration

Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture

Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking

UNIT – II

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement

UNIT – III

Preparing for a Hack: Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance

UNIT – IV

Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase
Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern

UNIT – V

Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion

TEXT BOOK:

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press.

REFERENCE BOOKS:

1. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning.
2. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning.

B.Tech. Cyber Security (Minor) VII SEMESTER

L	T	P	C
3	0	0	3

M157AF: DIGITAL FORENSICS

Prerequisites:
Cybercrime and Information Warfare, Computer Networks

Course Objectives:

1. Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
2. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools
4. E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics

Course Outcomes: On completion of the course the student should be able to

1. Understand relevant legislation and codes of ethics.
2. Computer forensics and digital detective and various processes, policies and procedures.
3. E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Email and web forensics and network forensics.

UNIT - I

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.
Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber criminalistics area, holistic approach to cyber-forensics

UNIT - II

Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT - III

Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

UNIT - IV

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics, workstations and software, Conduct an investigation, Complete a case, Critique a case, Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.

UNIT - V

Mobile Forensics: mobile forensics techniques, mobile forensics tools.

Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

TEXT BOOKS:

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

REFERENCE BOOKS

1. William Oettinger, Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt Publishing; 1st edition (30 April 2020), ISBN: 1838648178.
2. Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge.

B.Tech. Cyber Security (Minor) VII SEMESTER

L	T	P	C
0	0	3	1.5

M15705: ETHICAL HACKING LAB

Course Objectives:

1. The aim of the course is to introduce the methodologies framework tools of ethical hacking to get awareness in enhancing the security
2. To get knowledge on various attacks and their detection

Course Outcomes:

1. Gain the knowledge of the use and availability of tools to support an ethical hack
2. Gain the knowledge of interpreting the results of a controlled attack

List of Experiments:

1. Set Up a honey pot and monitor the honey pot on network
2. Write a script or code to demonstrate SQL injection attacks
3. Create a social networking website login page using phishing techniques
4. Write a code to demonstrate DoS attacks
5. Install rootkits and study variety of options
6. Study of Techniques uses for Web Based Password Capturing.
7. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric Crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security And Management
8. Implement Passive scanning, active scanning, session hijacking, cookies extraction using Burp suit tool

B.Tech. Cyber Security (Minor) VII SEMESTER

L	T	P	C
0	0	3	1.5

M15706: DIGITAL FORENSICS LAB

Course Objectives:

1. To provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cybercrime left in digital storage devices, emails, browsers, mobile devices using different Forensics tools.
2. To Understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis.
3. Understand some of the tools of e-discovery.
4. To understand the network analysis, Registry analysis and analyze attacks using different forensics tools.

Course Outcomes:

1. Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing
2. To Learn the file system storage mechanisms and retrieve files in hidden format
3. Learn the use of computer forensics tools used in data analysis.
4. Learn how to find data that may be clear or hidden on a computer disk, find the open ports for the attackers through network analysis, Registry analysis.

List of Experiments:

1. Perform email analysis using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders, Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders
2. Perform Browser history analysis and get the downloaded content, history saved logins, searches, websites visited etc using Foxton Forensics tool, Dumpzilla.
3. Perform mobile analysis in the form of retrieving call logs, SMS log, all contacts list using the forensics tool like SAFT
4. Perform Registry analysis and get boot time logging using process monitor tool
5. Perform Disk imaging and cloning the using the X-way Forensics tools
6. Perform Data Analysis i.e History about open file and folder, and view folder actions using Listview activity tool
7. Perform Network analysis using the Network Miner tool.
8. Perform information for incident response using the crowd Response tool
9. Perform File type detection using Autopsy tool
10. Perform Memory capture and analysis using the Live RAM capture or any forensic tool

TEXT BOOKS:

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerbach Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

REFERENCE BOOKS:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H.Malin, E. Casey and J. M. Aquilina, Syngress, 2012
3. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A. Reyes, Syngress, 2007.

B.Tech. Cyber Security (Minor) VIII SEMESTER

L	T	P	C
3	0	0	3

M158AM: SECURITY INCIDENT AND RESPONSE MANAGEMENT

Prerequisites:

1. Knowledge in information security and applied cryptography.
2. Knowledge in Operating Systems.

Course Objectives:

1. Give an introduction to preparation of inevitable incident and incident detection and characterization.
2. To get an exposure to live data collection, Forensic duplication.
3. To gain knowledge on data analysis including Windows and Mac OS Systems.

Course Outcomes:

1. Learn how to handle the incident response management.
2. Perform live data collection and forensic duplication
3. Identify network evidence
4. Analyze data to carry out investigation

UNIT - I

Introduction: Preparing for the Inevitable incident: Real world incident, IR management incident handbook, Pre-incident preparation, Preparing the Organization for Incident Response, Preparing the IR team, Preparing the Infrastructure for Incident Response. Incident Detection and Characterization: Getting the investigation started on the right foot, collecting initial facts, Maintenance of Case Notes, Understanding Investigative Priorities. Discovering the scope of incident: Examining initial data, Gathering and reviewing preliminary evidence, determining a course of action, Customer data loss scenario, Automated clearing fraud scenario.

UNIT - II

Data Collection: Live Data Collection: When to perform live response, Selecting a live response tool, what to collect, collection best practices, Live data collection on Microsoft Windows Systems, Live Data Collection on Unix-Based Systems. Forensic Duplication: Forensic Image Formats, Traditional duplication, Live system duplication, Duplication of Enterprise Assets.

UNIT - III

Network Evidence: The case for network monitoring, Types for network monitoring, Setting Up a Network Monitoring System, Network Data, Analysis, Collect Logs Generated from Network Events. Enterprise Services: Network Infrastructure Services, Enterprise Management Applications, Web servers, Database Servers

UNIT - IV

Data Analysis: Analysis Methodology: Define Objectives, Know your data, Access your data, Analyse your data, Evaluate Results. Investigating Windows Systems: NTFS and File System analysis, Prefetch, Event logs, Scheduled Tasks, The Windows Registry, Other Artifacts of Interactive Sessions, Memory Forensics, Alternative Persistence Mechanisms.

UNIT - V

Investigating Mac OS X Systems: HFS+ and File System Analysis, Core Operating systems data. Investigating Applications: What is Application Data? Where is application data stored?, General Investigation methods, Web Browser, Email Clients, Instant Message Clients.

TEXT BOOKS:

1. "Incident Response and Computer Forensics", Jason T. Luttgens, Mathew Pepe and Kevin Mandia, 3rd Edition, Tata McGraw-Hill Education.
2. "Cyber Security Incident Response-How to Contain, Eradicate, and Recover from Incidents", Eric. C. Thompson, Apress.

REFERENCE BOOK:

1. "The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk", N.K. McCarthy, Tata McGraw-Hill.

B.Tech. Cyber Security (Minor) VIII SEMESTER

L	T	P	C
3	0	0	3

M158AN: MOBILE SECURITY

Course Objectives: This course provides a thorough understanding of mobile platforms, including attack surfaces, risk landscape & more.

Course Outcomes:

1. Understand common mobile application security vulnerabilities
2. Define the security controls of multiple mobile operating systems
3. Understand and analyze Bluetooth technology
4. understand and analyze overview of SMS security and Enterprise security

UNIT – I:

Top Mobile Issues and Development Strategies: Top Issues Facing Mobile Devices, Physical Security , Secure Data Storage (on Disk), Strong Authentication with Poor Keyboards , Multiple-User Support with Security, Safe Browsing Environment , Secure Operating Systems, Application Isolation, Information Disclosure, Virus, Worms, Trojans, Spyware, and Malware , Difficult Patching/Update Process, Strict Use and Enforcement of SSL, Phishing , Cross-Site Request Forgery (CSRF), Location Privacy/Security, Insecure Device Drivers, Multi Factor Authentication, Tips for Secure Mobile Application Development .

UNIT – II:

WAP and Mobile HTML Security WAP and Mobile HTML Basics, Authentication on WAP/Mobile HTML Sites, Encryption, Application Attacks on Mobile HTML Sites, Cross-Site Scripting, SQL Injection, Cross-Site Request Forgery, HTTP Redirects, Phishing, Session Fixation, Non-SSL Login, WAP and Mobile Browser Weaknesses, Lack of HTTP Only Flag Support, Lack of SECURE Flag Support, Handling Browser Cache, WAP Limitations.

UNIT – III:

Bluetooth Security Overview of the Technology , History and Standards , Common Uses , Alternatives, Future, Bluetooth Technical Architecture , Radio Operation and Frequency, Bluetooth Network Topology , Device Identification , Modes of Operation , Bluetooth Stack ,Bluetooth Profiles, Bluetooth Security Features , Pairing , Traditional Security Services in Bluetooth, Security "Non-Features" , Threats to Bluetooth Devices and Networks, Bluetooth Vulnerabilities, Bluetooth Versions Prior to v1.2, Bluetooth Versions Prior to v2.1. Security for 1g Wi-Fi Applications, Security for 2g Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications

UNIT – IV:

SMS Security Overview of Short Message Service, Overview of Multimedia Messaging Service, Wireless Application Protocol (WAP), Protocol Attacks, Abusing Legitimate Functionality, Attacking Protocol Implementations, Application Attacks, iPhone Safari, Windows Mobile MMS, Motorola RAZR JPG Overflow, Walkthroughs, Sending PDUs, Converting XML to WBXML.

UNIT – V:

Enterprise Security on the Mobile OS Device Security Options, PIN, Remote, Secure Local Storage, Apple iPhone and Keychain, Security Policy Enforcement, Encryption, Full Disk Encryption, E-mail Encryption, File Encryption, Application Sandboxing, Signing, and Permissions, Application Sandboxing, Application Signing, Permissions, Buffer Overflow Protection, Windows Mobile, iPhone, Android, BlackBerry, Security Feature Summary.

TEXT BOOK:

1. Mobile Application Security, Himanshu Dwivedi, Chris Clark, David Thiel, TMH

REFERENCE BOOKS:

1. Mobile and Wireless Network Security and Privacy, Kami S. Makki, et al, Springer.
2. Android Security Attacks Defenses, Abhishek Dubey, CRC Press.

B.Tech. Cyber Security (Minor) VIII SEMESTER

L	T	P	C
3	0	0	3

M158AP: IOT SECURITY

Course Objectives:

1. Understand the fundamentals, various attacks and importance of Security aspects in IoT.
2. Understand the techniques, protocols and some idea on security towards Gaming models.
3. Understand the operations of Bitcoin blockchain, crypto-currency as application of blockchain technology.
4. Understand the essential components of IoT.
5. Understand security and privacy challenges of IoT.

Course Outcomes:

1. Incorporate the best practices learnt to identify the attacks and mitigate the same.
2. Adopt the right security techniques and protocols during the design of IoT products.
3. Assimilate and apply the skills learnt on ciphers and block chains when appropriate.
4. Describe the essential components of IoT.
5. Find appropriate security/privacy solutions for IoT.

UNIT - I

Fundamentals of IoT and Security and its need, Prevent Unauthorized Access to Sensor Data Block ciphers Introduction to Blockchain, Introduction of IoT devices, IoT Security Requirements, M2M Security, Message integrity Modeling faults and adversaries Difference among IoT devices, computers, and embedded devices.

UNIT - II

IoT and cyber-physical systems RFID Security, Authenticated encryption Byzantine Generals problem sensors and actuators in IoT. IoT security (vulnerabilities, attacks, and countermeasures), Cyber Physical Object Security, Hash functions Consensus algorithms and their scalability problems Accelerometer, photoresistor, buttons

UNIT - III

Security Engineering for IoT Development Hardware Security, Merkle trees and Elliptic curves digital signatures, Verifiable Random Functions, Zero-Knowledge Systems Motor, LED, Vibrator. IoT Security Lifecycle Front-end System Privacy Protection, Management, Secure IoT Databases, Public-key crypto (PKI), Blockchain, the Challenges, and Solutions, Analog Signal vs. Digital Signal.

UNIT - IV

Data Privacy Networking Function Security Trees signature algorithms proof of work, Proof of stake, Networking in IoT Device/User Authentication in IoT IoT Networking Protocols, Crypto-currencies, alternatives to Bitcoin consensus, Bitcoin scripting language and their use Real-time communication

UNIT - V

Introduction to Authentication Techniques Secure IoT Lower Layers, Bitcoin P2P network, Ethereum and Smart Contracts, Bandwidth efficiency.

Data Trustworthiness in IoT Secure IoT Higher Layers, Distributed consensus, Smart Contract Languages and verification challenges data analytics in IoT - simple data analyzing methods.

TEXT BOOKS:

1. B. Russell and D. Van Duren, “Practical Internet of Things Security,” Packt Publishing, 2016.
2. FeiHU, “Security and Privacy Internet of Things (IoTs): Models, Algorithms and Implementations”, CRC Press, 2016.
3. Narayanan et al., “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,” Princeton University Press, 2016.

REFERENCE BOOKS:

1. A. Antonopoulos, “Mastering Bitcoin: Unlocking Digital Crypto currencies,” O’Reilly, 2014.
2. T. Alpcan and T. Basar, “Network Security: A Decision and Game-theoretic Approach,” Cambridge University Press, 2011.
3. Security and the IoT ecosystem, KPMG International, 2015.
4. Internet of Things: IoT Governance, Privacy and Security Issues” European Research Cluster.
5. Ollie Whitehouse, “Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond”, NCC Group, 2014.
6. Josh Thompson, ‘Blockchain: The Blockchain for Beginnings, Guide to Blockchain Technology And Blockchain Programming’, Create Space Independent Publishing Platform, 2017.

B.Tech. Cyber Security (Minor) VIII SEMESTER	L	T	P	C
	3	0	0	3

M158AQ: BLOCK CHAIN TECHNOLOGIES

Pre-requisites
1. Knowledge in security and applied cryptography.
2. Knowledge in distributed databases.

Course Objectives:
1. To Introduce block chain technology and Cryptocurrency.

Course Outcomes:
1. Learn about research advances related to one of the most popular technological areas today.
2. Understand Extensibility of Blockchain concepts.
3. Understand and Analyze Blockchain Science.
4. Understand Technical challenges, Business model challenges.

UNIT - I
Introduction: Block chain or distributed trust, Protocol, Currency, Cryptocurrency, How a Cryptocurrency works, Crowdfunding.

UNIT - II
Extensibility of Blockchain concepts, Digital Identity verification, Block chain Neutrality, Digital art, Blockchain Environment.

UNIT - III
Blockchain Science: Gridcoin, Folding coin, Blockchain Genomics, Bitcoin MOOCs.

UNIT - IV
Currency, Token, Tokenizing, Campuscoin, Coindrop as a strategy for Public adoption, Currency Multiplicity, Demurrage currency.

UNIT - V
Technical challenges, Business model challenges, Scandals and Public perception, Government Regulations.

TEXT BOOK:
1. Melanie Swan, Blockchain Blueprint for Economy, O'reilly.

REFERENCE BOOKS:
1. Building Blockchain Apps, Michael Juntao Yuan, Pearson Education.
2. Daniel Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps 1st Edition.
3. Bradley Lakeman, Blockchain Revolution: Understanding the Crypto Economy of the Future. A Non-Technical Guide to the Basics of Cryptocurrency Trading and Investing.

B.Tech. Cyber Security (Minor) VIII SEMESTER

L	T	P	C
3	0	0	3

M158AR: AUTHENTICATION TECHNIQUES

Course Objectives:

Knowledge on concept of authentication types, protocols, physical identification and various authentication algorithms.

Course Outcomes:

1. Understand different types of authentication techniques.
2. Understand text based and voice-based authentication techniques.
3. Understand significance of authentication algorithms and its standards.
4. Apply various authentication protocols in multi-server environment and their Representation.

UNIT - I:

Definition of Authentication, Identification/verification, Stages and steps of authentication, Authentication Entity : User, Device and Application; Authentication attributes: Source, Location, Path, Time duration etc.; Authentication Types : Direct / Indirect, One Way / Mutual, On demand/ Periodic/ Dynamic/Continuous authentication, Assisted/Automatic; 3 Factors of authentication; Passwords, Generation of passwords of varied length and of mixed type, OTP, passwords generation using entity identity credentials; Secure capture, processing, storage, verification and retrieval of passwords.

UNIT - II:

Physical identification using smart cards, remote control device, proximity sensors, surveillance camera, authentication in Card present / Card Not Present transactions as ATM/ PoS Device, mobile phone, wearable device and IoT device-based authentication; single sign- on; Symmetric Key Generation, Key Establishment, Key Agreement Protocols.

UNIT - III:

Biometrics – photo, face, iris, retinal, handwriting, signature, fingerprint, palm print, hand geometry, voice – Text based and text independent voice authentication, style of talking, walking, writing, keystrokes, gait etc. multi-modal biometrics.

UNIT - IV:

Matching algorithms, Patterns analysis, errors, performance measures, ROC Curve; Authentication Standards – International, UIDAI Standard. Kerberos, X.509 Authentication Service, Public Key Infrastructure, Scanners and Software; Web Authentication Methods: Http based, Token Based, OAuth and API.

UNIT - V:

User authentication protocols in multi-server environment, BAN Logic, Representation of authentication protocols using BAN Logic, Random Oracle Model, Scyther Tools, Proverif tool, Chebyshev Chaotic Map, Fuzzy Extractor, Fuzzy Extractor Map, Bloom Filter, LU Decomposition based User Authentication, Blockchain based authentication.

TEXT BOOKS:

1. Protocols for Authentication and Key Establishment, Colin Boyd and Anish Mathuria, springer, 2021
2. Guide to Biometrics, Ruud M. Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Springer 2009.

REFERENCES:

1. Digital Image Processing using MATLAB, Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010.
2. Biometric System and Data Analysis: Design, Evaluation, and data Mining, Ted Dunstone and Neil Yager, Springer.
3. Biometrics Technologies and verification Systems, John Vacca, Elsevier Inc, 2007.
4. Pattern Classification, Richard O. Duda, David G. Stork, Peter E. Hart, Wiley 2007.

B.Tech. Cyber Security (Minor) VIII SEMESTER

L	T	P	C
3	0	0	3

M158AS: CLOUD SECURITY

Pre-requisites: Computer Networks, Cryptography and Network Security, Cloud Computing.

Course Objectives:
1. To understand the fundamentals concepts of cloud computing.
2. To understand the cloud security and privacy issues.
3. To understand the Threat Model and Cloud Attacks
4. To understand the Data Security and Storage
5. To analyze Security Management in the Cloud.

Course Outcome:
1. Ability to acquire the knowledge on fundamentals concepts of cloud computing.
2. Able to distinguish the various cloud security and privacy issues.
3. Able to analyze the various threats and Attack tools
4. Able to understand the Data Security and Storage
5. Able to analyze the Security Management in the Cloud.

UNIT - I

Overview of Cloud Computing: Introduction, Definitions and Characteristics, Cloud Service Models, Cloud Deployment Models, Cloud Service Platforms, Challenges Ahead.
Introduction to Cloud Security: Introduction, Cloud Security Concepts, CSA Cloud Reference Model, NIST Cloud Reference Model, NIST Cloud Reference Model.
Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

UNIT - II

Cloud Security and Privacy Issues: Introduction, Cloud Security Goals/Concepts, Cloud Security Issues, Security Requirements for Privacy, Privacy Issues in Cloud.
Infrastructure Security: The Network Level, the Host Level, the Application Level, SaaS Application Security, PaaS Application Security, IaaS Application Security.
Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

UNIT - III

Threat Model and Cloud Attacks: Introduction, Threat Model- Type of attack entities, Attack surfaces with attack scenarios, A Taxonomy of Attacks, Attack Tools-Network-level attack tools, VM-level attack tools, VMM attack tools, Security Tools, VMM security tools.
Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

UNIT - IV

Information Security Basic Concepts, an Example of a Security Attack, Cloud Software Security Requirements, Rising Security Threats. Data Security and Storage: Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security.
Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

UNIT - V

Evolution of Security Considerations, Security Concerns of Cloud Operating Models, Identity Authentication, Secure Transmissions, Secure Storage and Computation, Security Using Encryption Keys, Challenges of Using Standard Security Algorithms, Variations and Special Cases for Security Issues with Cloud Computing, Side Channel Security Attacks in the Cloud

Security Management in the Cloud- Security Management Standards, Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

TEXT BOOKS:

1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1st Edition published 2022 by CRC press.
2. Cloud Computing with Security Concepts and Practices Second Edition by Naresh Kumar Sehgal Pramod Chandra, P. Bhatt John M. Acken, 2nd Edition Springer nature Switzerland AG2020.
3. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Lati First Edition, September 2019.

REFERENCE BOOKS:

1. Essentials of Cloud Computing by K. Chandrasekaran Special Indian Edition CRC press.
2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley.

B.Tech. Cyber Security (Minor) VIII SEMESTER	**L**	**T**	**P**	**C**
	0	**0**	**0**	**2**

M15803: MINI PROJECT

The Mini Project is in the collaboration with an industry of their specialization. Students will register for this immediately after VI Semester examinations and pursue it during the summer vacation. The Mini Project shall be submitted in a report form and presented before the committee in VIII Semester. It shall be evaluated for 100 external marks. The committee consists of an external examiner, Head of the Department, Supervisor of the Mini project and a senior faculty member of the department. There shall be no internal marks for the Mini Project.