



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited A++ Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF COMPUTING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

1.1.3 Courses having focus on employability/ entrepreneurship/ skill development

B.E Computer Science and Engineering With Specialization In Cyber Security			
Employability			
S.No	Course Code	Course Name	Page No
	SCSA1519	Ethical Hacking	2
	SCSA1520	Blockchain and Cryptocurrency	3
	SCSA1616	Linux Programming	4
	SCSA1617	AI Enhanced Cyberthreats	5
	SCSB1271	Introduction to Cyber Security	7
	SCSB1262	Block chain and Crypto Currency	9
Skill Development			
	SCSA2510	Ethical Hacking- Lab	11
	SCSA2511	Database Security Lab	12
	SCSA2612	Linux Lab	14
Entrepreneurship			
	S614AIPROJ	Interdisciplinary Project	

SCSA1519	ETHICAL HACKING	L	T	P	Credits	Total Mark
		3	0	0	3	100

COURSE OBJECTIVES:

- To introduce the basic concepts of Ethical Hacking and Penetration Testing
- To acquire knowledge about gathering information about the victim
- To demonstrate Enumeration and Port Scanning
- To learn about vulnerability scanning
- To demonstrate Network sniffing

UNIT 1 INTRODUCTION TO ETHICAL HACKING

12 Hrs. Important Terminologies Categories of Penetration Test Writing Reports Structure of PT report Vulnerability-Assessment Summary Risk Assessment - Methodology - Detailed Findings Reports

UNIT 2 INFORMATION GATHERING

12 Hrs. Active and Passive Information Gathering Sources - Copying Website locally yougetsignal.com NeoTrace Intercepting a Response - Acunetix Vulnerability Scanner NetCraft Google Hacking Interacting with DNS Servers DNS Cache Snooping

UNIT 3 ENUMERATION AND PORT SCANNING

12 Hrs. Host Discovery Scanning for Open Ports and Services Types of Port Scanning TCP Three-way handshake TCP Flags Port Status Types TCP SYN Scan TCP Connect Scan NULL, FIN and XMAS SCA NULL Scan FIN Scan XMAS Scan TCP ACK Scan Responses - UDP Port Scan Scanning a vulnerable host Performing an IDLE scan with NMAP Service Version Detection OS Fingerprinting

UNIT 4 VULNERABILITY SCANNING

12 Hrs. Working with Vulnerability Scanners Nmap Testing SCADA Environments - Nessus Vulnerability Scanner Installing Nessus Adding a user - Creating a new policy Safe Checks Silent Dependencies Port Range Preferences

UNIT 5 NETWORK SNIFFING

12 Hrs. Introduction Types of Sniffing Hubs vs. Switches - Promiscuous Mode vs. Non-Promiscuous Mode MITM Attacks ARP Protocol Basics -How ARP works ARP attacks DoS Attacks -Sniffing with Wireshark DNS Spoofing DHCP Spoofing
Max. 60 Hrs.

COURSE OUTCOMES:

On the completion of the course, the students will be able to

- C01: Understand the basic concepts of Ethical Hacking and Penetration Testing and will be able to prepare penetration testing reports. C02: Demonstrate information gathering about the victim using various tools such acunetix, netcraft and google hacking
- C03: Enumerate and perform different types of scanning and demonstrate nmap.
- C04: Explore the vulnerability scanners: nmap and Nessus.
- C05: Understand and demonstrate sniffing, MITM attacks, ARP attacks and DoS attacks.
- C06: Explore the crucial areas of Ethical Hacking and Penetration Testing with Case Studies.

TEXT/ REFERENCE BOOKS

1. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, CRC Press Taylor & Francis Group, 2015.
2. Jon Erickson, Hacking The Art of Exploitation, No Starch Press, San Francisco ,2nd Edition,2008.
3. Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray"Hat Hacking: The Ethical
4. Hackers Handbook, TMH ,3rd Edition, 2011.

SCSA2510	ETHICAL HACKING - LAB	L	T	P	Credits	Total Marks
		0	0	4	2	100

COURSE OBJECTIVES

- To gather and learn more information about the victim
- To collect tools and techniques used by the target
- To find the vulnerabilities on the network
- To find the vulnerabilities on the web application
- To analysis and explore the packets on the network

SUGGESTED LIST OF EXPERIMENTS

1. Copying Websites Locally for Website Spoofing
2. Tracing and Fingerprinting Network
3. Information Gathering Tools
4. Exploring Webservers with Netcraft
5. Finding Information using Google Hacking
6. Working with Acunetix Vulnerability Scanner
7. Demonstrating different types of port scanning
8. Fingerprinting with NMAP
9. Working with Nessus Vulnerability Scanner
10. Packet Sniffing using Wireshark

COURSE OUTCOMES

On the completion of the course, the students will be able to

CO1: To apply the skills and duplicate a website for web spoofing

CO2: To identify the weakness of the target by finding the tools and techniques used CO3:

To examine and trace the blueprint of the network

CO4: To examine and find out the vulnerabilities of the web application

CO5: To explore and sniff the packets moving across the network

CO6: To perform vulnerability assessment in an efficient manner

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100

Evaluation of Regular Lab class

Model practical exam

End Semester Practical Exam

Exam Duration:3 Hrs. CAE:

15 Marks

10 Marks

25 Marks ESE:

25 Marks

SCSA2511	DATABASE SECURITY LAB	L	T	P	Credits	Total Marks
		0	0	4	2	100

COURSE OBJECTIVES

- Introduce the database security issues.
- Cover in details the various state-of-art database security methods and techniques.
- Cover in details the security features in databases
- Make students aware and experiment with database security analysis tools.

SUGGESTED LIST OF EXPERIMENTS

1. Introduction to database security issues
2. The role of databases in information systems.
3. Access control management features.
4. Cryptographic data protection.
5. SQL language features.
6. Statistical databases.
7. Database security methods and techniques
8. Access control to database objects: tables, attributes, records.
9. Triggers, views, data masking
10. Cryptographic methods of protection.
11. Escaping queries to a database.
12. Change Tracking.
13. Data integrity in the databases.
14. Database backups.
15. Security features in databases
16. SQL statements for access control.
17. Integrity (domain, attributes, tables, referential).
18. Database monitoring tools.
19. Database security analysis tools
20. An overview of the main methods for analysing database security.
21. SQL injections.
22. Database security scanners.
23. Writing your own security analysis tools.

COURSE OUTCOMES

On completion of the course students are expected to be able to:

- CO1: Understand and characterize modern techniques of database information security threats and techniques for database security assessment. CO2: Analyze information in a database to identify information security incidents. Understand and use the main tools for database management systems monitoring.
- CO3: Use build-in database functions to enable database integrity support. Understand and identify database information security threats, critically evaluate and apply the potential countermeasures.
- CO4: Create a plan for vulnerabilities detection and identification in databases. Use and analyze the results obtained by the database vulnerability scanners.
- CO5: Apply new methods of a database protection and use tools for database security assessment.
- CO6: Understand the various security analysis tools

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100

CAE: Evaluation of Regular Lab class

Exam Duration:3 Hrs.

15 Marks

SCSA1520	BLOCKCHAIN AND CRYPTOCURRENCY	L	T	P	Credits	Total Marks
		3	0	0	3	100

COURSE OBJECTIVES

- To Impart strong technical understanding of Blockchain technologies.
- To introduce the concept and the basics of Ethereum that helps developers publish distributed applications.
- To learn various aspects of working and use of BitCoin.
- To give the knowledge to transfer of money for medium of exchange
- to provide knowledge on SECURITY AND PRIVACY of Blockchain technologies
- To applied the various applications of blockchain technologies.

UNIT 1 INTRODUCTION OF BLOCKCHAIN

9 Hrs.

Peer-to-Peer(P2P) Networking, Blockchain Architecture, Design and Integration, key Participants in the block chaining, Blocks in Blockchain, Types of Block chain, the Logical Components of Blockchain, Core Components of Blockchain Architecture, Smart contracts and their applications.

UNIT 2 ETHEREUM BASICS

9 Hrs.

Ethereum and Smart Contracts, The Turing Completeness of Smart Contract Languages and verification challenges, using smart contracts to enforce legal contracts, comparing Bitcoin scripting vs. Ethereum Smart Contracts, writing smart contracts using Solidity & JavaScript

UNIT 3 INTRODUCTION OF BITCOIN

9 Hrs.

Bitcoin features, Blockchain and Bitcoin, Bitcoin Security, Bitcoin Transaction, Transaction Lifecycle, Consensus Protocol, Role of Bitcoin Crimes, Dark Side of Bitcoin Crimes, Open Challenges to Bitcoin Crimes.

UNIT 4 FUNDAMENTALS OF CRYPTOCURRENCIES

9Hrs.

Nodes, P2P, Ledger, Gossip Protocol, Consensus Methods, Messages, Account Balance, Genesis Block and New Coins, how a Crypto currency Works, crypto currency Exchange, Smart Contracts, E- Governance

UNIT 5 SECURITY AND PRIVACY ISSUES OF BLOCKCHAIN TECHNOLOGY

9 Hrs.

Introduction, Blockchain Aspects for Consideration, Security of block chain, Privacy of blockchains, Security Issues of Blockchain Technology, Privacy Issues of Blockchain Technology, Types of Attack, Security Enhancement to Blockchain Systems, Applications of Blockchain in Health care, Finance.

Max. 45 Hrs.

COURSE OUTCOME

On the completion of the course, the students will be able to

- CO1: Understand the concepts of Blockchain technologies.
- CO2: Implement Ethereum block chain contract.
- CO3: Illustrate the concepts of Bitcoin and their usage.
- CO4: Understand basic principles of Cryptocurrencies.
- CO5: Apply security features in blockchain technologies.
- CO6: Use smart contract in real world applications.

TEXT/ REFERENCE BOOKS

11. Tapscott, Don, Tapscott, Alex," Blockchain Revolution How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World".
12. Merunas Grincalaitis, "Mastering Ethereum: Implement Advanced Blockchain Applications using Ethereum-supported Tools, Services, and Protocols", Packt Publishing.
13. Raj, Pethuru Saini, Kavita Surianarayanan, Chellammal," Blockchain Technology and Applications".
14. Melanie Swan," Blockchain Blueprint for a New Economy".
15. Shiho Kim, Ganesh Chandra Deka," Advanced Applications of Blockchain Technology".
16. Rajneesh Gupta," Hands-On Cybersecurity with Blockchain Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain".
17. Martin Quest," Cryptocurrency Master Everything You Need to Know About Cryptocurrency and Bitcoin Trading, Mining, Investing, Ethereum, ICOs, and the Blockchain".

18. Narayanan, Bonneau, Felten, Miller and Goldfeder, "Bitcoin and Cryptocurrency Technologies A Comprehensive Introduction", Princeton University Press.
9. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.
10. Imran Bashir, "Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained", Packt Publishing.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100

Hrs. PART A: 10 Questions carrying 2 marks each – No choice

PART B: 2 Questions from each unit of internal choice, each carrying 16 marks

Exam Duration: 3

20 Marks

80 Marks

SCSA1616	LINUX PROGRAMMING	L	T	P	Credits	Total Marks
		3	0	0	3	100

COURSE OBJECTIVES

- To understand and make effective use of Linux utilities and shell scripting language to solve problems
- To develop skillsets that are required for systems programming including file system programming, process and signal management and inter process communication
- To develop the basic skills required to write network programs using sockets

UNIT 1 INTRODUCTION AND FILE UTILITIES

9 Hrs.

Introduction to Linux - Linux Utilities - File handling utilities, Security by file permissions, Process utilities, Disk utilities, Networking commands, Filters, Text processing utilities and Backup utilities - grep commands - sed commands - System commands in awk

UNIT 2 SHELL PROGRAMMING

9 Hrs.

Introduction to Shell programming – Working with Bourne again shell (Bash): Shell commands, Shell variables, Command substitution, Shell responsibilities, Pipes and Redirection, Aliases, Shell environment, Quoting, Test command, Control structures, Arithmetic in shell, Shell script examples, Interrupt processing, Functions, Debugging shell scripts

UNIT 3 FILE AND DIRECTORIES

9 Hrs.

Files and Directories: File Concept, File types, File System Structure, Inodes, File Attributes, File types, Standard I/O operations, Kernel support for files, System calls, File descriptors, File and directory management – Directories: creating, removing, and changing directories – Directory API functions.

UNIT 4 PROCESS AND SIGNALS

9 Hrs. Process and

Signals: Process concepts, process identifiers, process structure: process table, viewing processes, system processes, process scheduling, starting new processes: waiting for a process, zombie processes, orphan process, fork, vfork, exit, wait, waitpid, exec – Signal generation and handling, Signals functions, Reliable and unreliable signals, Interrupted system calls, kill, raise, alarm, pause, abort, system, sleep functions

UNIT 5 IPC AND SOCKETS

9 Hrs.

Inter Process Communication: Introduction – Pipes, Process pipes, the pipe call, parent and child processes, and named pipes: FIFOs, Semaphores, File locking with Semaphores, Message queues, Shared memory – Introduction to Sockets: Socket connections - Socket attributes, Socket addresses, Socket, connect, bind, listen, accept, socket communications.

Max. 45 Hrs.

COURSE OUTCOMES

On the completion of the course, the students will be able to

- CO1: Understand the basic commands of Linux operating system and can write shell scripts.
- CO2: Create and operate file systems and directories.
- CO3: Create processes background and foreground etc. by fork () system calls.
- CO4: Create shared memory segments, pipes, message queues and can exercise inter process communication. CO5: Understand Socket connections and attributes and write network scripts.
- CO6: Learn the concepts of Inter process Communication.

TEXT / REFERENCE BOOKS

19. Sumitabha Das, "Unix Concepts and Applications", Tata McGraw-Hill, 4th Edition, New Delhi, India.
20. W. Richard. Stevens, "Advanced Programming in the UNIX Environment", Pearson Education, 3rd edition, New Delhi, India.
21. Beginning Linux Programming, 4th Edition, N. Matthew, R. Stones Wrox, Wiley India Edition.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100

Exam Duration: 3 Hrs.

PART A: 10 Questions carrying 2 marks each – No choice

20 Marks PART B:

2 Questions from each unit of internal choice, each carrying 16 marks

80 Marks

SCSA1617	AI ENHANCED CYBER THREATS	L	T	P	Credits	Total Marks
		3	0	0	3	100

COURSE OBJECTIVES

- To understand the knowledge in solving AI problems
- To study the fundamentals of Cyber security
- To learn and analyse the impact of AI on cyber security
- To secure the web with AI and develop the Web Application Security
- To study the cyber threats

UNIT 1 INTRODUCTION AND PROBLEM SOLVING

9 Hrs.

Introduction – Understanding AI Basics – History of AI – Intelligent agent – Types of agents - Structure – Problem solving agents – Uninformed search strategies - Searching with partial Information. Fundamentals of AI for Security- deep learning fundamentals from a security perspective - cyber security space problem solution

UNIT 2 FUNDAMENTALS OF CYBER SECURITY

9 Hrs.

Identity, authentication, confidentiality, privacy, anonymity, availability and integrity-Exploring cryptographic algorithms together with major attacks- Exploring high-level security protocols- biometric authentication - Compliance and security assessment – introduction to penetration testing - Active Directory Security Assessment (ASDA) and cyber insurance risk assessment.

UNIT 3 IMPACT OF AI ON CYBER SECURITY

9 Hrs.

Threat hunting in memory, file system and network data - introductory analysis of malicious programs - cyber threat hunting and digital investigation -- detailed analysis of real-world case studies - unusual and non-virulent types of malwares: KNN (K - Nearest Neighbours) for threat visualizers, Isolation Forest for anomaly detection, LSTM for multi-vector correlation, DBSCAN for risk ware detection and fraud, LSTM (Autoencoder) for endpoint protection

UNIT 4 SECURE WEB AND APPLICATION

9 Hrs.

Securing web with AI - making websites secure using AI techniques for injection - using regular expressions and identifying patterns and matching with existing scores – Applications using statistical patterns and Bayesian statistics -Web Application Security, Injection, Broken authentication, Sensitive data exposure, XML External Entities (XXE), Broken access control, Security misconfiguration, Cross-Site Scripting (XSS), Insecure deserialization, Using components with known vulnerabilities and Insufficient logging and monitoring.

UNIT 5 CYBER THREATS

9 Hrs.

Future of AI in Advancing Security and Promoting, Artificial Intelligence vs. Data Analytics, Applying AI to cybersecurity, some early AI adopters, AI Use by Adversaries, Using Artificial Intelligence Tools to Enhance Security, Deep learning applications, Cyber Security Threats and Development of Secure Software, Securing IOT Infrastructure, Secure AI Development, Large scale deployment of AI algorithms on production, End-to-end case study for a secure IoT application in a develops ecosystem

Max. 45 Hrs.

COURSE OUTCOMES

On the completion of the course, the students will be able to CO1:

Understand the knowledge in solving AI problems.

CO2: Study the fundamentals of Cyber security.

CO3: Learn and analyze the impact of AI on cyber security.

CO4: Secure the web with AI and develop the Web Application Security.

CO5: Study the cyber threats.

CO6: Learn the case study for secure IOT application.

TEXT/ REFERENCE BOOKS

1. Jerzy Peja and rzej Piegat, "Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems", Springer, Technical University of Szczecin, Poland.
2. <https://www.coursera.org/learn/ibm-cyber-threat-intelligence#instructors>
3. <https://www.captechu.edu/search?keywords=syllabus>
4. http://polisci.rutgers.edu/images/syllabi/Cyber_Security_and_AI_790_574_90_Course_Syllabus_V1_19493.pdf

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100

Exam Duration: 3 Hrs.

PART A: 10 Questions carrying 2 marks each – No choice

20 Marks

PART B: 2 Questions from each unit of internal choice, each carrying 16 marks

80 Marks

SCSA2612	LINUX LAB	L	T	P	Credits	Total Marks
		0	0	4	2	100

COURSE OBJECTIVES

- To familiarize basic commands of kernel and shell programming
- To demonstrate use of system calls
- To demonstrate Inter Process Communication

SUGGESTED LIST OF EXPERIMENTS

1. Study and Practice on various commands like man, passwd, tty, script, clear, date, cal, cp, mv, ln, rm, unlink, mkdir, rmdir, du, df, mount, umount, find, unmask, ulimit, ps, who, w.
2. Study and Practice on various commands like cat, tail, head, sort, nl, uniq, grep, egrep, fgrep, cut, paste, join, tee, pg, comm, cmp, diff, tr, awk, tar, cpio.
3. a) Write a Shell Program to print all .txt files and .c files.
b) Write a Shell program to move a set of files to a specified directory.
4. a) Write a Shell program to display all the users who are currently logged in after a specified time.
b) Write a Shell Program to wish the user based on the login time.
5. a) Simulate cat command.
b) Simulate cp command.
6. a) Simulate head command.
b) Simulate tail command.
7. a) Simulate mv command.
b) Simulate nl command.
8. Write a program to handle the signals like SIGINT, SIGQUIT, SIGFPE.
9. Write a program to create a Zombie process
10. Write a program to create a child process and allow the parent to display "parent" and the child to display "child" on the screen.
11. Implement the following IPC forms
a) FIFO b) PIPE
12. Implement message queue form of IPC.
13. Implement shared memory form of IPC.
14. Write a Socket program to print system date and time (Using TCP/IP).

COURSE OUTCOMES

On the completion of the course, the students will be able to

- CO1: Understand the basic commands of kernel system and can write BASH scripts.
- CO2: Create and operate file systems and directories operations and handle text documents using BASH.
- CO3: Create Inter Process Communication viz., Parent – Child process, FIFO & PIPE, Zombies and Socket program.
- CO4: Create a logging process using shell programs
- CO5: Analyze the concepts of inter process communication
- CO6: Understand the socket programming.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100

Exam Duration: 3 Hrs.

CAE: Evaluation of Regular Lab class

15 Marks

Model practical exam

10 Marks

25 Marks

ESE: End Semester Practical Exam

25 Marks

SCSB1271	INTRODUCTION TO CYBER SECURITY	L	T	P	EL	Credits	Total Marks
		3	0	0	0	3	100

COURSE OBJECTIVES

- Understand the key concepts and principles of cybersecurity.
- To Identify common threats, attacks, and vulnerabilities in computer systems.
- Understand basics of cryptographic algorithms.
- Demonstrate knowledge of cryptographic techniques and their applications.
- Understand legal and ethical issues related to cybersecurity.

UNIT 1 INTRODUCTION TO CYBERSECURITY

9 Hrs.

Definition and scope of cybersecurity, Cybersecurity goals and objectives, Security principles: confidentiality, integrity, availability, Threats, Attacks, and Vulnerabilities-Overview of common cybersecurity threats and attack vectors, Malware, phishing, and other attack techniques, Identifying and assessing vulnerabilities in systems and networks

UNIT 2 NETWORK SECURITY

9 Hrs.

Network security concepts and protocols - Firewall -Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-TCP/IP-Virtual Private Network (VPN)- Internet Protocol Security (IPsec)- -Secure Sockets Layer/Transport Layer Security (SSL/TLS)- Internet Protocol Security (IPsec)

UNIT 3 CRYPTOGRAPHY AND DATA PROTECTION

9 Hrs.

Basics of cryptography: encryption, decryption, hashing, Symmetric and asymmetric encryption algorithms- Advanced Encryption Standard (AES)- Data Encryption Standard (DES)- Blowfish, RSA (Rivest-Shamir-Adleman)- Diffie-Hellman (DH)- Digital Signature Algorithm (DSA)- PGP (Pretty GoodPrivacy), ElGamal.

UNIT 4 WEB SECURITY

9 Hrs.

Common web security vulnerabilities (e.g., Cross-Site Scripting, SQL injection), Web application security best practices, Securing web servers and web applications. Access Control and Authentication- Principles of access Control- Authentication methods (e.g., passwords, biometrics).

UNIT 5 ETHICAL AND LEGAL ISSUES IN CYBERSECURITY

9 Hrs.

Ethical principles and professional codes of conduct, Laws, regulations, and privacy issues in cybersecurity, Cybersecurity ethics in the workplace.

Max. 45 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

- CO1** - Understands the importance fundamentals of cyber threat intelligence and its importance in cybersecurity.
CO2 - Understands to develop skills to collect, analyze, and interpret threat intelligence data.
CO3 - Understands basics of cryptographic algorithms.
CO4 - Understands various types of malware and their characteristics.
CO5 - Explain the fundamentals of cryptography and its role in securing data
CO6 - Understand legal and ethical issues related to cybersecurity.

TEXT / REFERENCE BOOKS

1. Raef Meeuwisse." Cybersecurity For Beginners"Lulu,2015
2. Mayank Bhusan/Rajkumar Singh Rathore/Aatif Jamshed, "Fundamentals of Cyber Security", BPB, 2020

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100

Exam Duration: 3 Hrs.

PART A: 10 questions of 2 marks each – No choice

20 Marks

PART B: 2 questions from each unit of internal choice; each carrying 16 marks

80 Marks

SCSB1262	BLOCKCHAIN AND CRYPTOCURRENCY	L	T	P	EL	Credits	Total Marks
		3	0	0	0	3	100

COURSE OBJECTIVES

- To Impart strong technical understanding of Blockchain technologies.
- To introduce the concept and the basics of Ethereum that helps developers publish distributed applications.
- To learn various aspects of working and use of BitCoin.
- To give the knowledge to transfer of money for medium of exchange .
- To provide knowledge on SECURITY AND PRIVACY of Block chain technologies.
- To applied the various applications of block chain technologies.

UNIT 1 INTRODUCTION OF BLOCKCHAIN

9 Hrs.

Peer-to-Peer(P2P) Networking, Blockchain Architecture, Design and Integration, key Participants in the block chaining, Blocks in Blockchain, Types of Block chain, the Logical Components of Blockchain, Core Components of Blockchain Architecture, Smart contracts and their applications.

UNIT 2 ETHEREUM BASICS

9 Hrs.

Ethereum and Smart Contracts, The Turing Completeness of Smart Contract Languages and verification challenges, using smart contracts to enforce legal contracts, comparing Bitcoin scripting vs. Ethereum Smart Contracts, writing smart contracts using Solidity & JavaScript

UNIT 3 INTRODUCTION OF BITCOIN

9 Hrs.

Bitcoin features, Blockchain and Bitcoin, Bitcoin Security, Bitcoin Transaction, Transaction Lifecycle, Consensus Protocol, Role of Bitcoin Crimes, Dark Side of Bitcoin Crimes, Open Challenges to Bitcoin Crimes.

UNIT 4 FUNDAMENTALS OF CRYPTOCURRENCIES

9 Hrs.

Nodes, P2P, Ledger, Gossip Protocol, Consensus Methods, Messages, Account Balance, Genesis Block and New Coins, how a Crypto currency Works, crypto currency Exchange, Smart Contracts, E- Governance.

UNIT 5 SECURITY AND PRIVACY ISSUES OF BLOCKCHAIN TECHNOLOGY

9 Hrs.

Introduction, Blockchain Aspects for Consideration, Security of block chain, Privacy of blockchains, Security Issues of Blockchain Technology, Privacy Issues of Blockchain Technology, Types of Attack, Security Enhancement to Blockchain Systems, Applications of Blockchain in Health care, Finance.

Max. 45 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 - Understand the concepts of Blockchain technologies.

CO2 - Implement Ethereum block chain contract.

CO3 - Illustrate the concepts of Bitcoin and their usage. **CO4** -

Understand basic principles of Cryptocurrencies. **CO5** - Apply security

features in blockchain technologies. **CO6** - Use smart contract in real world applications.

TEXT / REFERENCE BOOKS

1. Tapscott, Don, Tapscott, Alex, "Blockchain Revolution How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World".
2. Merunas Grincalaitis, "Mastering Ethereum: Implement Advanced Blockchain Applications using Ethereum-supported Tools, Services, and Protocols", Packt Publishing.
3. Raj, Pethuru Saini, Kavita Surianarayanan, Chellammal, "Blockchain Technology and Applications".
4. Melanie Swan, "Blockchain Blueprint for a New Economy".
5. Shiho Kim, Ganesh Chandra Deka, "Advanced Applications of Blockchain Technology".
6. Rajneesh Gupta, "Hands-On Cybersecurity with Blockchain Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain".
7. Martin Quest, "Cryptocurrency Master Everything You Need to Know About Cryptocurrency and Bitcoin Trading, Mining, Investing, Ethereum, ICOs, and the Blockchain".
8. Narayanan, Bonneau, Felten, Miller and Goldfeder, "Bitcoin and Cryptocurrency Technologies A Comprehensive Introduction", Princeton University Press.
9. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100

Exam Duration: 3 Hrs.

PART A: 10 questions of 2 marks each – No choice

20 Marks

PART B: 2 questions from each unit of internal choice; each carrying 16 marks

80 Marks