



SRI VENKATESWARA COLLEGE OF ENGINEERING,
(An Autonomous Institution, Affiliated to Anna University, Chennai – 600025)

M.Tech CYBERFORENSICS AND INFORMATION SECURITY

CURRICULUM AND SYLLABUS REGULATION – 2022 CHOICE BASED CREDIT SYSTEM

Curriculum Revision No:	00	Board of Studies recommendation date :	16.09.2022	Academic Council Approved date:	
Salient Points of the revision	01.				
	02.				
	03.				
	04.				
	05.				

Note: Times new Roman font and size 12 should be used throughout the document if specific size is not mentioned.

SRI VENKATESWARA COLLEGE OF ENGINEERING,
(An Autonomous Institution, Affiliated to Anna University, Chennai – 600025)

REGULATIONS 2022

M.Tech CYBERFORENSICS AND INFORMATION SECURITY

CHOICE BASED CREDIT SYSTEM

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

- I. Evolve as globally competent cyber security professionals, researchers and entrepreneurs possessing 21st century skills, to define the architecture, design, and management of the security of an organization
- II. Possess in-depth knowledge and skill sets in Cyber Security to monitor, prepare, predict, detect respond and prevent cyber-attacks and ensure enterprise security.

PROGRAM OUTCOMES (POs)

PO GRADUATE ATTRIBUTES

1. An ability to independently carry out research /investigation and development work to solve practical problems.
2. An ability to write and present a substantial technical report/document.
3. Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PEO's-PO's&PSO's MAPPING: (Example)

POs	PEOs	
	I	II
1.	✓	✓
2.	✓	✓
3.	✓	✓

**SRI VENKATESWARA COLLEGE OF ENGINEERING,
(An Autonomous Institution, Affiliated to Anna University, Chennai – 600025)**

**REGULATION 2022
CHOICE BASED CREDIT SYSTEM**

M.Tech CYBERFORENSICS AND INFORMATION SECURITY

CURRICULUM

SEMESTER I

Sl. No.	Course Code	Course Title	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1	MA22182	Mathematical Foundations For Information Security	FC	3	1	0	4	4	-	F
2	CF22101	Foundations of Cyber Security	PC	3	1	0	4	4	-	F
3	CF22102	Advanced Operating Systems	PC	3	0	0	3	3	-	F
4	CF22103	Network Principles and Security	PC	3	0	0	3	3	-	F
5	CF22104	Computer Forensics and Digital Evidence	PC	3	0	0	3	3	-	F
6	GR22251	Introduction to Research Methodology & IPR (Common to all branches)	MC	3	0	0	3	3	-	F
Practical Subjects										
7	CF22111	Network Design and Security Laboratory	PC	0	0	4	2	4	-	F
8	CF22112	Ethical Hacking Essentials Laboratory	PC	0	0	4	2	4	-	F
Total				18	2	6	24	28		

SEMESTER II

Sl. No.	Course Code	Course Title	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1	CF22201	Fundamentals to Security in Biometrics	PC	3	0	0	3	3	Foundations of Cyber Security	M
2	CF22202	Digital Forensics and Digital Investigations	PC	3	1	0	4	4	-	M
3	CF22203	Blockchain for Security	PC	3	0	0	3	3	-	F
4	CF22204	Internet of Things and Security	PC	3	1	0	4	4	-	F
5		Professional Elective I	PE	3	0	0	3	3	-	F
Practical Subjects										
6	CF22211	IoT and Blockchain Laboratory	PC	0	0	3	2	3	-	F
7	CF22212	Digital Forensics Laboratory	PC	0	0	3	2	3	-	F
8	CF22213	Case Study I – Forensic Investigations	EEC	0	0	2	1	2	-	F
Total				15	2	8	22	25		

Semester III

Sl. No.	Course Code	Course Title	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1		Professional Elective III	PE	3	0	0	3	3	-	M
2		Professional Elective IV	PE	3	0	0	3	3	-	M
3		Professional Elective V	PE	3	0	0	3	3	-	M
Practical Subjects										
6	CF22311	Project Phase I	EEC	0	0	12	6	12	-	F
Total				9	0	12	15	21		

Semester IV

Sl. No.	Course Code	Course Title	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
Practical Subjects										
6	CF22411	Project Phase II	EEC	0	0	24	12	24	-	F
Total				0	0	24	12	24		

Total Credit : 73

PROFESSIONAL ELECTIVE

Sl. No.	Course Code	Course Title	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1	CF22002	Penetration and Application Testing	PE	3	0	0	3	3	-	M
2	CF22004	Applied Cryptography	PE	3	0	0	3	3	-	M
3	CF22006	Data Mining Techniques	PE	3	0	0	3	3	-	M
4	CF22008	Network Virtualisation	PE	3	0	0	3	3	-	M
5	CF22010	Cloud Computing Technologies	PE	3	0	0	3	3	-	M
6	CF22001	Energy Aware Computing	PE	3	0	0	3	3	-	M
7	CF22003	Advanced Infrastructure Management	PE	3	0	0	3	3	-	M
8	CF22005	Machine Learning Techniques	PE	3	0	0	3	3	-	M
9	CF22007	Intrusion Detection and Prevention Systems	PE	3	0	0	3	3	-	M
10	CP22008	Social Network Analysis	PE	3	0	0	3	3	-	M
11	CF22011	Principles of Secure Coding	PE	3	0	0	3	3	-	M
12	CF22013	Trust Management in E – Commerce	PE	3	0	0	3	3	-	M
13	CF22015	Biometric Image Processing	PE	3	0	0	3	3	-	M
14	CF22017	Cyber Security Management and Cyber Laws	PE	3	0	0	3	3	-	M
15	CF22019	Malware Analysis and Reverse Engineering	PE	3	0	0	3	3	-	M
16	CF22021	Data Analytics and Business Intelligence	PE	3	0	0	3	3	-	M
17	CF22023	Wireless Security	PE	3	0	0	3	3	-	M

L	T	P	C
3	1	0	4

COURSE OBJECTIVES:

1. To understand the concepts of number theory which play an important role in computer science and cryptography.
2. To understand basic concepts of various algebraic structures used in computer science.
3. To understand the concepts of advanced algebraic structures used in computer science
4. To understand the basic mathematical principles and functions that form the foundation for coding theory
5. To understand basics of elliptic curves and pseudo random numbers and its usage

UNIT I NUMBER THEORY 12

Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theorem. Congruences - Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

UNIT II ALGEBRAIC STRUCTURES I 12

Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Rings – Sub rings, ideals and quotient rings.

UNIT III ALGEBRAIC STRUCTURES II 12

Integral domains, Fields – Finite fields - Classification - Structure of finite fields.

UNIT IV CODING THEORY 12

Introduction - Basic concepts - Codes, minimum distance, equivalence of codes, Linear codes -Generator matrices and parity - Check matrices - Hamming codes.

UNIT V ELLIPTIC CURVES AND PSEUDORANDOM NUMBER GENERATION 12

Discrete Logarithm - Elliptic curves - Introduction to Pseudo random numbers.

TOTAL: 60 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	CO statements	RBT level
CO1	Grasp the concepts of number theory and their applications to	AP

	cryptography.	
CO2	Prove statements and construct examples of some classes of groups and rings.	AP
CO3	Explain integral domain field and finite field and perform an in-depth analysis of various algebraic structures used in computer science.	AN
CO4	Identify the mathematical principles and functions and apply them to the concept of coding theory	AP
CO5	Gain knowledge on discrete logarithms, elliptic curves and pseudo random numbers.	U

TEXT BOOKS:

1. Kenneth H Rossen, Discrete Mathematics and its Applications, Seventh Edition, McGrawHill, 2012.
2. Rudolf Lidl, Gunter Pilz, Applied Abstract Algebra, Second Edition, Springer, 1998.
3. D.S. Malik, J. Mordeson, M.K. Sen, Fundamentals of abstract algebra, McGraw Hill, 1997.
4. Joseph A. Gallian, Contemporary Abstract Algebra, Narosa, 1998.
5. L. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman & Hall/CRC, 2003.

REFERENCES:

1. Niven, H.S. Zuckerman, H. L. Montgomery, An introduction to the theory of numbers, John Wiley and Sons, 2001.
2. Fraleigh J.B., A first course in abstract algebra, Pearson Education, 2005.
3. Douglas R Stinson, Cryptography: Theory and Practice, CRC Press, 2015.

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	1		3
2.	1		3
3.	1		3
4.	1		3
5.	1		3

L	T	P	C
3	1	0	4

COURSE OBJECTIVES:

1. Understand various block cipher and stream cipher models
2. Describe the principles of public key cryptosystems, hash functions and digital signature
3. To get a firm knowledge on Cyber Security Essentials

UNIT I INTRODUCTION TO SECURITY 12

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm

UNIT II PUBLIC KEY CRYPTOGRAPHY AND HASH ALGORITHMS 12

Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange- Hash functions-Hash Algorithms (MD5, Secure Hash Algorithm)

UNIT III FUNDAMENTALS OF CYBER SECURITY 12

How Hackers Cover Their Tracks- Fraud Techniques- Threat Infrastructure- Techniques to Gain a Foothold (Shellcode, SQL Injection, Malicious PDF Files)- Misdirection, Reconnaissance, and Disruption Methods

UNIT IV PLANNING FOR CYBER SECURITY 12

Privacy Concepts -Privacy Principles and Policies -Authentication and Privacy - Data Mining - Privacy on the Web - Email Security - Privacy Impacts of Emerging Technologies

UNIT V CYBER SECURITY MANAGEMENT 12

Security Planning - Business Continuity Planning - Handling Incidents - Risk Analysis - Dealing with Disaster – Legal Issues – Protecting programs and Data – Information and the law – Rights of Employees and Employers - Emerging Technologies - The Internet of Things - Cyber Warfare

TOTAL: 60 PERIOD**OUTCOMES:**

Upon successful completion of the course, students should be able to:

CO	CO statements	RBT level
CO1	Implement basic security algorithms required by any computing system	AP
CO2	Analyze the vulnerabilities in any computing system and hence be able to design a security solution	AN

CO3	Analyze the possible security attacks in complex real time systems and their effective countermeasures	AN
CO4	Enumerate various governing bodies of cyber laws	AP
CO5	Impart various privacy policies for an organization	AP

REFERENCES:

1. William Stallings, "Cryptography and Network Security", Pearson Education, 6th Edition, 2013.
2. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, Security in Computing, 5th Edition, Pearson Education, 2015.
3. Graham, J. Howard, R., Olson, R., Cyber Security Essentials, CRC Press, 2011.
4. George K. Kostopoulos, Cyber Space and Cyber Security, CRC Press, 2013.

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	3	1	3
2.	3	1	3
3.	3	1	3
4.	3	1	3
5.	3	1	3

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

1. Have a detailed knowledge on Operating system concepts
2. Understand the need for operating system security
3. Administer an open source Operating System

UNIT I	OPERATING SYSTEMS: OVERVIEW	9
	Operating System structure and operations - Process Management- Memory Management – Storage Management - Protection and Security– Process Scheduling – Inter process communication- Multi threading models- Semaphores – Monitors - Deadlocks- Mutexes- Critical Section problem	
UNIT II	MEMORY MANAGEMENT IN OPERATING SYSTEM	9
	Swapping – Contiguous Memory Allocation – Segmentation – Paging – Virtual Memory: Demand Paging – Page Replacement – Allocation of Frames – Thrashing – Allocating Kernel Memories	
UNIT III	LINUX SYSTEM ADMINISTRATION	9
	Requirements for a Linux Administrator – Server Requirements – Logging in Remotely – Network configuration – Providing DNS – Adding Relational DB – Configuring mail securely – Adding FTP services – Synchronizing the system clock – Installing perl modules	
UNIT IV	OPERATING SYSTEMS: TRUST MODEL	9
	Security Goals – Trust and Threat Model – Protection System – Reference Monitor – Secure Operating System – Assessment Criteria – Mutics History – Multics System and Security	
UNIT V	OPERATING SYSTEMS SECURITY	9
	System History – Unix and Windows History – Unix Security – Windows Security – Verifiable Security Goals – Security Kernels – Securing Commercial Operating Systems	

TOTAL: 45 PERIODS**OUTCOMES:**

Upon successful completion of the course, students should be able to:

CO	CO statements	RBT level
CO1	Enumerate the basic functionalities of operating system	AP
CO2	Demonstrate Linux system administration	AP
CO3	Formulate Security features for an operating system	AP

CO4	Perform memory management in OS	AP
CO5	Implement Trust model for Multics system	AP

REFERENCES:

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, “Operating System Concepts”, John Wiley & Sons ,Inc., 9th Edition, 2012.
2. Trent Jaeger, “Operating Systems Security”, Morgan & Claypool Publishers, 2008.
3. Tom Adelstein and Bill Lubanovic, “Linux System Administration”, O'Reilly Media, Inc., 1st Edition, 2007.
4. William Stallings, “Operating System: Internals and Design Principles”, Prentice Hall, 7th Edition, 2012.

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	3	1	3
2.	3	1	3
3.	3	1	3
4.	3	1	3
5.	3	1	3

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

1. Identify the basic networking principles
2. Understand the need for network security
3. Expose themselves to security at various network layers

UNIT I FUNDAMENTALS OF NETWORKS 9

Networking Technology – Connecting Devices - The OSI Model - TCP/IP Model - Threats to Network communications - Wireless Network Security – Denial of Service – Distributed Denial of Service

UNIT II CRYPTOGRAPHY IN NETWORK SECURITY 9

Malicious vs Non Malicious code – Counter Measures – Authentication – Access Control – Network and Browser Encryption – Firewalls – IDS – Network Management

UNIT III NETWORK AND TRANSPORT LAYER SECURITY 9

Network Layer: IPSec Protocol – IP Authentication Header – IP ESP – VPN - Key Management Protocol for IPSec – Transport Layer: SSL Protocol – TLS Protocol

UNIT IV E – MAIL AND WEB SECURITY 9

Pretty Good Privacy – MIME – S/MIME - Enhanced Security Services for S/MIME - SET for E-commerce Transactions

UNIT V CLOUD AND WIRELESS NETWORK SECURITY 9

Cloud Computing – Cloud Security Risks and Counter Measures – Cloud Security as a Service – Wireless Network Security: Wireless Security – Mobile Device Security – WLAN Security

TOTAL: 45 PERIODS**OUTCOMES:**

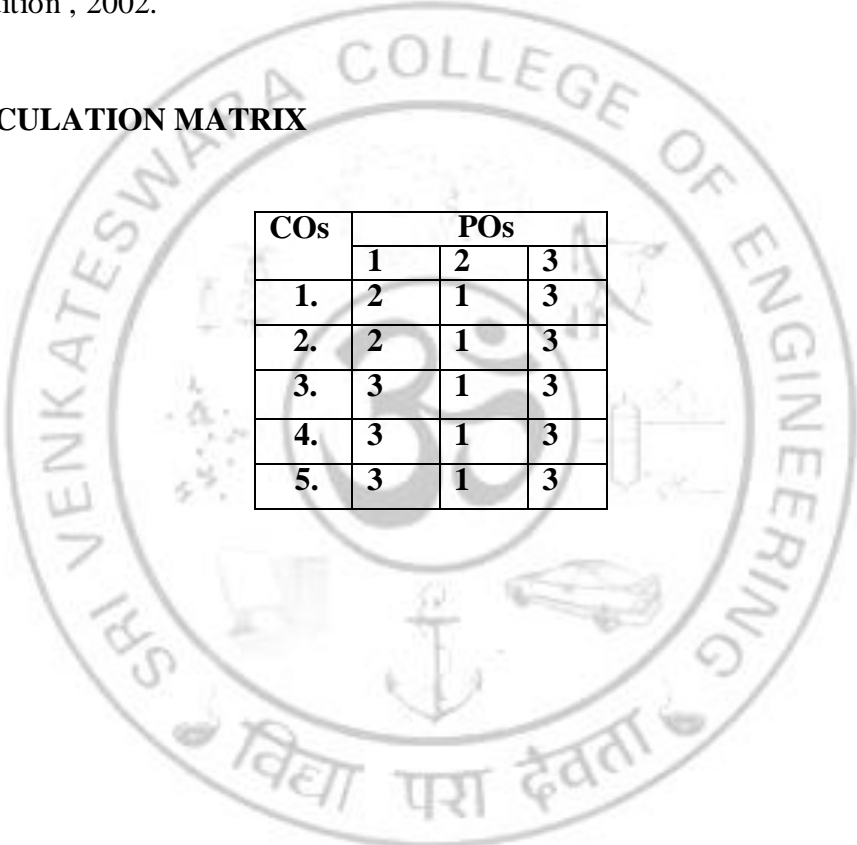
Upon successful completion of the course, students should be able to:

CO	CO statements	RBT level
CO1	Classify and secure various layers of networks	AN
CO2	Understand the concept of Network Layer Security	U
CO3	Develop protocols for Web and Mail security	AP
CO4	Apply various password management techniques for system security	AP
CO5	Develop measures for cloud and wireless network security	AP

REFERENCES:

1. Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", Wiley Publications, 2003.
2. Charles Pfleeger, "Security in Computing", Prentice Hall, 4th Edition, 2006.
3. William Stallings, "Cryptography and Network Security", Pearson Education, 6th Edition, 2013.
4. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security", Prentice Hall, 2nd edition, 2002.

COURSE ARTICULATION MATRIX



COs	POs		
	1	2	3
1.	2	1	3
2.	2	1	3
3.	3	1	3
4.	3	1	3
5.	3	1	3

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

1. Study the procedure for forensic investigation
2. Audit and analyze the computer systems for data extraction
3. Understand the process of cloud and mobile device forensics

UNIT I COMPUTER FORENSICS FUNDAMENTALS 9

Introduction to Computer Forensics – Computer Forensics Services – Benefits of Professional Forensics Methodology – Steps taken by Computer Forensics Specialists – Types of Computer Forensics System: IDS, Firewall – PKI – Wireless Network Security – Identity Management Security System – Identity Theft.

UNIT II COMPUTER FORENSICS TECHNOLOGY 9

Types of Military, Business and Law Enforcement Computer Forensic Technology – Specialized Forensics Techniques – Hidden Data and How to Find it – Spyware and Adware – Encryption Methods – Internet Tracing Methods – Avoiding Pitfalls with Firewall – Biometric Security Systems.

UNIT III DATA ACQUISITION AND PROCESSING CRIME SCENES 12

Understanding Storage Formats for Digital Evidence - Determining the Best Acquisition Method - Using Acquisition Tools - Validating Data Acquisitions - Performing RAID Data Acquisitions - Identifying Digital Evidence - Collecting Evidence in Private-Sector Incident Scenes - Processing Law Enforcement Crime Scenes - Preparing for a Search - Securing a Computer Incident or Crime Scene - Seizing Digital Evidence at the Scene - Obtaining a Digital Hash.

UNIT IV NETWORK AND E – MAIL FORENSICS 9

Performing Live Acquisitions - Network Forensics Overview - Exploring the Role of E-mail in Investigations - Exploring the Roles of the Client and Server in E-mail - Investigating E-mail Crimes and Violations - Understanding E-mail Servers - Using Specialized E-mail Forensics Tools.

UNIT V CLOUD AND MOBILE DEVICE FORENSICS 6

An Overview of Cloud Computing - Legal Challenges in Cloud Forensics - Technical Challenges in Cloud Forensics - Acquisitions in the Cloud - Tools for Cloud Forensics - Understanding Mobile Device Forensics - Understanding Acquisition Procedures for Mobile Devices.

TOTAL: 45 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	CO statements	RBT level
CO1	Plan and prepare for all stages of an investigation	AP
CO2	Explore web server attacks, DNS and router attacks	AN
CO3	Identify various evidences of cyber crime	AP
CO4	Examine network traffic and identify illicit servers	E
CO5	Acquire data from mobile devices and crime scenes securely	AP

REFERENCES:

1. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations: Processing Digital Evidence", 5th edition, Cengage Learning, 2015.
2. John R.Vacca, "Computer Forensics", Cengage Learning, 2005.
3. Nelson, Phillips, Enfinger, Steuart, "Computer Forensics and Investigations", Cengage Learning, India Edition, 2008.
4. Marjie T.Britz, "Computer Forensics and Cyber Crime: An Introduction", 3rd Edition, Prentice Hall, 2013.

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	2	3
2.	2	2	3
3.	2	2	3
4.	2	2	3
5.	2	2	3

GR22251 Introduction to Research Methodology and IPR

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

To impart knowledge on formulation of research problem, research methodology, ethics involved in doing research and importance of IPR protection.

UNIT I RESEARCH METHODOLOGY

6

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations. Effective literature studies approaches, analysis Plagiarism, Research ethics

UNIT II RESULTS AND ANALYSIS

6

Importance and scientific methodology in recording results, importance of negative results, different ways of recording, industrial requirement, artifacts versus true results, types of analysis (analytical, objective, subjective) and cross verification, correlation with published results, discussion, outcome as new idea, hypothesis, concept, theory, model etc.

UNIT III TECHNICAL WRITING

6

Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

UNIT IV INTELLECTUAL PROPERTY RIGHTS

6

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.

UNIT V PATENT RIGHTS AND NEW DEVELOPMENTS IN IPR

6

Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications. New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

TOTAL: 30 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	CO statements	RBT level
CO1	Critically evaluate any research article based upon research	E

	methodology.	
CO2	Correlate the results of any research and develop hypothesis, concept, theory and model.	AN
CO3	Developing a research proposal, research presentation and review article in the field of engineering.	AP
CO4	Enumerate the importance of intellectual property right in research.	AP
CO5	Develop proposal for patent rights and identify the new developments in IPR	AP

TEXT BOOKS:

1. Ranjit Kumar, Research Methodology- A step by step guide for beginners, Pearson Education, Australia, fourth edition, 2014
2. Ann M. Korner, Guide to Publishing a Scientific paper, Bioscript Press 2008
3. T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008

REFERENCES:

1. Kothari, C. R. Research Methodology - Methods and Techniques, New Age International publishers, New Delhi, fourth edition, 2019
2. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students", Juta & Company, 1996.
3. Robert P. Merges, Peter S. Menell and Mark A. Lemley, "Intellectual Property in New Technological Age", Aspen Publishers, 2016.

At the end of the course add the Course articulation matrix as per the following format:

COURSE ARTICULATION MATRIX

COs	PO													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	3	3	3	2	3	2	2	3	-	2	1	2	3	3
2.	3	3	3	3	3	1	1	2	2	2	2	2	3	3
3.	3	3	3	3	3	-	2	3	2	2	3	2	3	3
4.	2	2	3	2	2	1	-	3	1	2	2	1	2	3
5.	3	3	3	2	3	2	2	3	2	2	2	2	3	3

L	T	P	C
0	0	3	2

COURSE OBJECTIVES:

1. Understand the basics of Networking
2. Learn network programming in Linux using C/Python

List of Exercises**I Network Design using CISCO Packet Tracer**

1. Configure a LAN with a switch/hub with minimum 3 PCs
2. Configure a internetwork with 2 routers and two or more LANs using static routes
3. Establish a dynamic routing based internetwork with 2 routers and two or more LANs using RIP/OSPF
4. Analyze the performance of various TCP variants using an FTP application for the given network

II Network Programming using C/Python

5. Develop a program for demonstrating inter process communication
6. Creation of TCP client/server application
7. Creation of UDP client/server application
8. Develop an Iterative UDP server with 2 or 3 clients
9. Develop a concurrent TCP server with 2 or 3 clients
10. Implement Digital Signature
11. Implement ARP and RARP
12. Create a Socket based application in Python
13. Intrusion Detection using Snort tool
14. Create an application that interacts with e-mail servers in python
15. Develop applications that work with remote servers using SSH, FTP etc in Python
16. Simulate PING and TRACEROUTE commands

Total Hours:45 Periods

Course Outcomes:

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

CO	CO statements	RBT level
CO1	Design and Configure LAN's	AP
CO2	Create simple network applications using C/Python	AP
CO3	Demonstrate Interprocess communication	AP
CO4	Simulate IDPS	AP
CO5	Develop applications that work with remote servers	AP

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS**SOFTWARE:**

Windows/Ubuntu/ Kali Linux with C/C++/Java/Python Cisco Packet Tracer, Snort IDS, Eclipse or equivalent IDE

HARDWARE:

Standalone desktops - 18

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	1	3
2.	2	1	3
3.	3	1	3
4.	3	1	3
5.	3	1	3

L	T	P	C
0	0	3	2

COURSE OBJECTIVES:

1. Understand the basics of Ethical Hacking
2. Learn various Hacking tools

List of Exercise

1. Basic Linux Commands
2. Advanced Linux commands
3. Information Gathering
4. Vulnerability Analysis
5. Web Application Analysis
6. Database Assessment
7. Password Attacks
8. Wireless Attacks
9. Reverse Engineering
10. Exploitation tools
11. Sniffing & spoofing
12. VM-WARE

Total Hours:45 Periods**Course Outcomes:**

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

CO	CO statements	RBT level
CO1	Gather the information from various sources	AP
CO2	Assess the vulnerabilities in Database	AN
CO3	Analyse the vulnerabilities in Web application	AN
CO4	Enumerate various attacks and its counter measures	AP
CO5	Use different Exploitation tools	AP

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS:

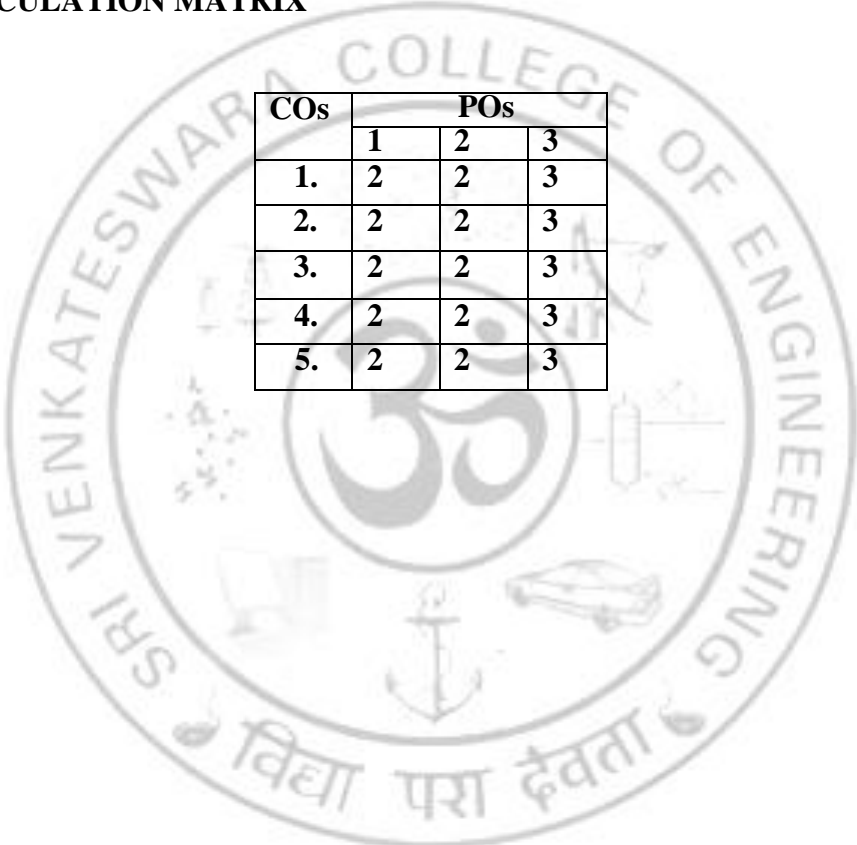
SOFTWARE:

Kali Linux and its Tools

HARDWARE:

Standalone desktops - 18

COURSE ARTICULATION MATRIX



COs	POs		
	1	2	3
1.	2	2	3
2.	2	2	3
3.	2	2	3
4.	2	2	3
5.	2	2	3

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

The students will be able to

1. Understand the functionalities of biometrics
2. Discover the need of biometrics for an organization
3. Learn to develop biometric based applications
4. Emphasize the need of biometric security

UNIT I FUNDAMENTALS OF BIOMETRICS 9

Biometric System – Enrollment and recognition – Sensor modules – Feature extraction module - Database module – Matching module – Biometric functionalities – Biometric system errors – Design cycle of Biometrics – Security and Privacy issues.

UNIT II FINGERPRINT RECOGNITION 9

Friction ridge pattern: Features and formation – Fingerprint Acquisition – Feature extraction – Matching – Fingerprint indexing – Fingerprint synthesis: Level 1 and Level 2 – Palmprint.

UNIT III FACE AND IRIS RECOGNITION 9

Psychology of face recognition – Facial features – Design – Image acquisition – Face detection - Feature extraction and matching – Face modelling – Iris Recognition: Design and Image acquisition – Image segmentation – Image normalization, Encoding and matching – Iris quality-Performance Evaluation.

UNIT IV SIGNATURE AND KEYSTROKE RECOGNITION 9

Behavioural biometrics – Features and Classification – Signature Recognition: History of Handwriting Analysis - Automated Systems for Signature Recognition - Offline and Online Signatures - Types of Forgeries - Databases for Signature System Evaluation - Commercial Software – Signature Recognizers – Keystroke Dynamics: Keystroke Analysis - Authentication and Identification - Characteristics of Keystroke Dynamics - Approaches to Keystroke Dynamics.

UNIT V SECURITY IN BIOMETRICS 9

Adversary Attacks – Insider and Infrastructure attack - Attacks at the User Interface – Impersonation – obfuscation – spoofing - Countermeasure: spoof detection - Attacks on Biometric Processing – System modules and interconnections - Attacks on the Template Database - Biometric template security.

TOTAL: 45 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	CO statements	RBT level
CO1	Identify various biometric techniques	
CO2	Design biometric recognition systems	
CO3	Develop simple biometric based application	
CO4	Elucidate the need for biometric security	
CO5	Analyse the various attacks possible in Biometric system	

References

1. James wayman, Anil k. Jain, Arun A. Ross, Karthik Nandakumar, "Introduction to Biometrics", Springer, 2011.
2. Khalid saeed with Marcin Adamski, "New Directions in Behavioral Biometrics", CRC Press 2017
3. Paul Reid "Biometrics For Network Security", Person Education 2004.

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	2	3
2.	3	2	3
3.	3	2	3
4.	2	2	3
5.	2	2	3

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

The students will be able

1. To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.
2. To understand how to examine digital evidences such as the data acquisition, identification analysis.

UNIT I DIGITAL FORENSICS 9

Foundations of Digital Forensics - Digital Evidence - Increasing Awareness of Digital Evidence - Digital Forensics: Past, Present, and Future - Principles and Challenges of Digital Forensics - Digital Forensics Research - Language of Computer Crime Investigation.

UNIT II DIGITAL INVESTIGATIONS 9

Conducting Digital Investigations - Digital Investigation Process Models - Scaffolding for Digital Investigations - Applying the Scientific Method in Digital Investigations - Fundamental Principles - Preparing to Handle Digital Crime Scenes – Surveying and Preserving the Digital Crime Scene -Equivocal Forensic Analysis – Victimology - Crime Scene Characteristics.

UNIT III DIGITAL EVIDENCE 9

Violent Crime and Digital Evidence - Digital Evidence as Alibi - Investigating an Alibi – Time and Location as Alibi - Investigating Computer Intrusions - Forensic Preservation of Volatile Data - Investigation of Malicious Computer Programs – Cyberstalking.

UNIT IV COMPUTER BASICS FOR DIGITAL INVESTIGATORS 9

Basic Operation of Computers - Representation of Data - File Systems and Location of Data - Dealing with Password Protection and Encryption - Applying Forensic Science to Computers - Digital Evidence on Windows Systems - Digital Evidence on UNIX Systems.

UNIT V FORENSIC SCIENCE ON NETWORKS 9

Digital Evidence on the Internet - Online Anonymity and Self-Protection - E-mail Forgery and Tracking - Usenet Forgery and Tracking - Digital Evidence on Physical and Data-Link Layers - Digital Evidence at the Network and Transport Layers.

TOTAL: 45 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	CO statements	RBT level
CO1	Relate the fundamentals of computer forensics, laws, report writing and tools in digital investigations.	
CO2	Assess the investigative smart practices and applicability of concerned laws & investigative tools	
CO3	Inspect the acquired data, recover the deleted data and manage a case .	
CO4	Select the correct method to handle the digital evidence and acquire appropriate certification to build the career in digital forensics.	
CO5	Create a method for gathering, assessing and applying new and existing legislation specific to the practice of digital forensics.	

References

1. Eoghan Casey, “Digital Evidence and Computer Crime Forensic Science, Computers and the Internet”, Third Edition, Elsevier, 2011
2. Kevin Mandia, Chris Prosise, Matt Pepe, —Incident Response and Computer Forensics —, TataMcGraw -Hill, New Delhi, 2006.
3. Nelson Phillips and Enfinger Steuart, —Computer Forensics and Investigationsl, CengageLearning, New Delhi, 2009.
4. Cory Altheide and Harlan Carvey, —Digital Forensics with Open Source Toolsl Elsevierpublication, April 2011

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	2	3
2.	2	2	3
3.	2	2	3
4.	2	2	3
5.	2	2	3

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

The students will be able to

1. Understand the cryptography basics of a blockchain
2. Recognize the requirement of a simple blockchain application
3. Study about the tools used for blockchain development

UNIT I	CRYPTO FUNDAMENTALS FOR BLOCKCHAIN	12
Hash Functions – Digital Hash – Pre-image resistance – Second pre-image resistance – MessageDigest – Secure Hash Algorithms – Distributed Hash Tables – Digital Signatures – Signcryption – Blind Signatures.		
UNIT II	FEATURES OF BLOCKCHAIN	9
History of Blockchain – Decentralization – Generic Elements of Blockchain – Addresses – Transaction – Block – Contents of a Block – Block Header - State Machine – Nodes– Types of Blockchain.		
UNIT III	CONSENSUS IN BLOCKCHAIN	9
Fault tolerance – Paxos – Consensus – Byzantine Agreement – Proof of Work – Proof of Stake – Proof of Elapsed Time – Proof of Importance – Practical Byzantine Fault Tolerance – CAPTheorem - Mining – How blockchain accumulates block.		
UNIT IV	HYPERLEDGER FOR BLOCKCHAIN	9
Hyperledger as a protocol – Fabric – Sawtooth lake – Reference Architecture – Privacy and Confidentiality – Fabric Architecture – Components of the fabric – Blockchain services – API's and CLI's.		
UNIT V	APPLICATIONS OF BLOCKCHAIN	9
Bitcoin – Cryptocurrency – Smart Contracts – Financial Applications – IoT BlockchainApplications – Government Applications – Blockchain Security.		

TOTAL: 45 PERIODS

OUTCOMES:

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

CO	CO statements	RBT level
CO1	Elucidate the requirements of a blockchain	
CO2	Design a simple blockchain based application	
CO3	Implement Consensus mechanism in blockchain	
CO4	Deploy sample applications over Hyperledger	
CO5	Explain the requirement of mining in blockchain	

References

1. Imran Bashir, "Mastering Blockchain", Packt Publishing 2017.
2. Melanie Swan, "Blockchain - Blueprint for a New Economy", O'Reilly Media, 2015
3. Roger Wattenhofer, "The science of the blockchain", Inverted Forest Publishing, 2016
4. www.blockchain.io
5. www.blockchain.org

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	1	3
2.	2	1	3
3.	3	1	3
4.	3	1	3
5.	3	1	3

L	T	P	C
3	1	0	4

COURSE OBJECTIVES:

The students will be able to

1. Understand the fundamentals of Internet of Things
2. Fabricate a low cost embedded system using Raspberry Pi or Arduino
3. Apply IoT in Real world scenario

UNIT I FUNDAMENTALS OF IOT 12

The flavour of the Internet – Technology of IoT – Enchanted objects – Design principles for connected device – Privacy – Webthinking – Affordance.

UNIT II INTERNET PRINCIPLES 12

Internet Communications – IP, TCP – Protocol suite – UDP – IP Addresses – TCP and UDP ports – MAC Address – Application Layer Protocols.

UNIT III PROTOTYPING EMBEDDED DEVICES 12

Prototypes and production - Open source versus closed source - Tapping into the community – Electronics - Embedded computing basics – Arduino - Raspberry pi - electric imp – plug computing.

UNIT IV PROTOTYPING PHYSICAL AND ONLINE COMPONENTS 12

Preparation, sketch, iterate and explore - Non digital methods - Laser cutting - 3D printing – Getting started with API – Writing a new API – Real time reactions – Memory Management.

UNIT V PROTOTYPE TO BUSINESS MODELS 12

Business model canvas – Models - Funding an internet of things startup – Scaling up Software – Ethics: Privacy – Control – Environment – Solutions

TOTAL: 60 PERIODS

OUTCOMES:

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

CO	CO statements	RBT level
CO1	Analyze various protocols of IoT	
CO2	Design a portable IoT application using Raspberry Pi or Arduino	
CO3	Deploy an IoT application to the cloud.	
CO4	Analyze applications of IoT in real time scenario	
CO5	Design Prototype for physical and online components	

References

1. Adrian McEwen, Hakim Cassimally, Designing the Internet of Things, 1/e, Wileypublication, 2013
2. Charalampos Doukas , Building Internet of Things with the Arduino, Create space, 2002.
3. Dieter Uckelmann (et.al), Architecting the Internet of Things, Springer, 2011.

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	1	3
2.	3	1	3
3.	2	1	3
4.	2	1	3
5.	3	1	3

Course Objectives:

The students will be able to

1. Understand the basics of Arduino/ Raspberry Pi programming
2. Learn to develop simple blockchain applications.

Arduino and Raspberry Pi

1. Arduino programming to make the LED Blink with and without delay
2. Serial Communication in Arduino with Wireless Module and Programming
3. Bluetooth (HC-05) and ZigBee (TI -CC2500)
4. Programming the Raspberry Pi to make the LED Blink using Python
5. Integration of sensors/components with Raspberry Pi and Programming
6. Serial Communication Between Arduino and Raspberry Pi using Universal SerialBus(USB)

Security in Arduino and Raspberry Pi

7. Implementation of MD5, SHA1, SHA256 in Arduino/Raspberry Pi using Hash Functions.
8. Implementation of DES and AES Algorithms in Arduino/Raspberry Pi using ArduinoCryptographic Library.

Blockchain Implementation

9. Implementation of basic Hash algorithms required for Blockchain
10. Developing simple applications using Hyperledger framework
11. Developing simple applications using Ethereum framework
12. Simulation of mining in Blockchain
13. Implementation of ethereum smart contracts

Course Outcomes:

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

1. Develop simple applications using Arduino/ Raspberry Pi
2. Implement various security protocols
3. Create simple applications using blockchain tools
4. Simulate mining in blockchain

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS:

SOFTWARE:

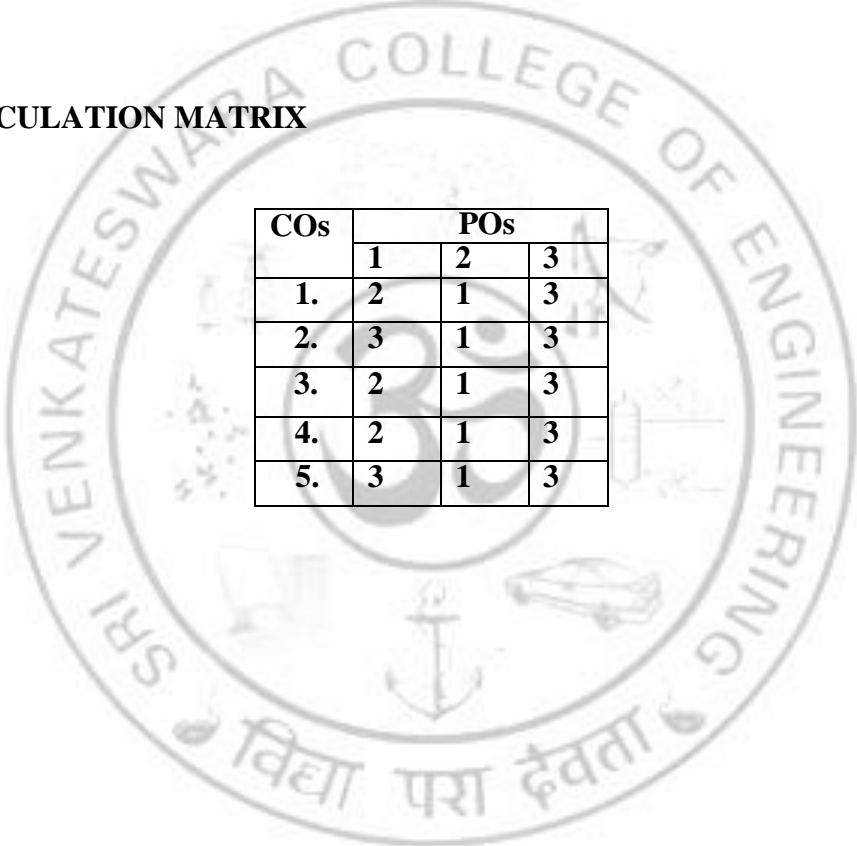
Windows/Ubuntu/ Kali Linux with C/C++/Java/Python Cisco Packet Tracer, Snort IDS, Eclipse or equivalent IDE

HARDWARE:

Standalone desktops – 18 IoT kit -18

Total Hours:45 Periods

COURSE ARTICULATION MATRIX



COs	POs		
	1	2	3
1.	2	1	3
2.	3	1	3
3.	2	1	3
4.	2	1	3
5.	3	1	3

Course Objectives:

The students will be able to
Perform basic digital forensics.
Demonstrate the use of simple digital forensics tools.
Conduct a digital forensics exercise.

List of Exercises**Disk Imaging and Cloning**

1. Use VMWare and modify device configuration in a VMWare system

Analyzing disk structure and file systems

2. The Sleuth Kit Tools

Search Word Filtering from Unallocated, Slack and Swap**SpaceUnix File Recovery – Data Unit Level**

3. Review of unallocated space and extracting with dls

FILE RECOVERY: META DATA LAYER

4. Find meta data information for evidence found in a search list

Keyword Searches, Timelines, Hidden Data**Data Mining for Digital Forensics**

5. Encryption and Password Recovery
6. Steganography Detection
7. File Extension Renaming and Signaturing
8. Application Analysis
9. Client and Web Analysis
10. Network Analysis

Course Outcomes:

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

4. Practice and gain basic knowledge about VMware and various file system
5. Analyse disk structure and file system
6. Perform file recovery
7. Perform mining for digital forensics
8. Apply steganography in digital forensics

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS:

SOFTWARE:

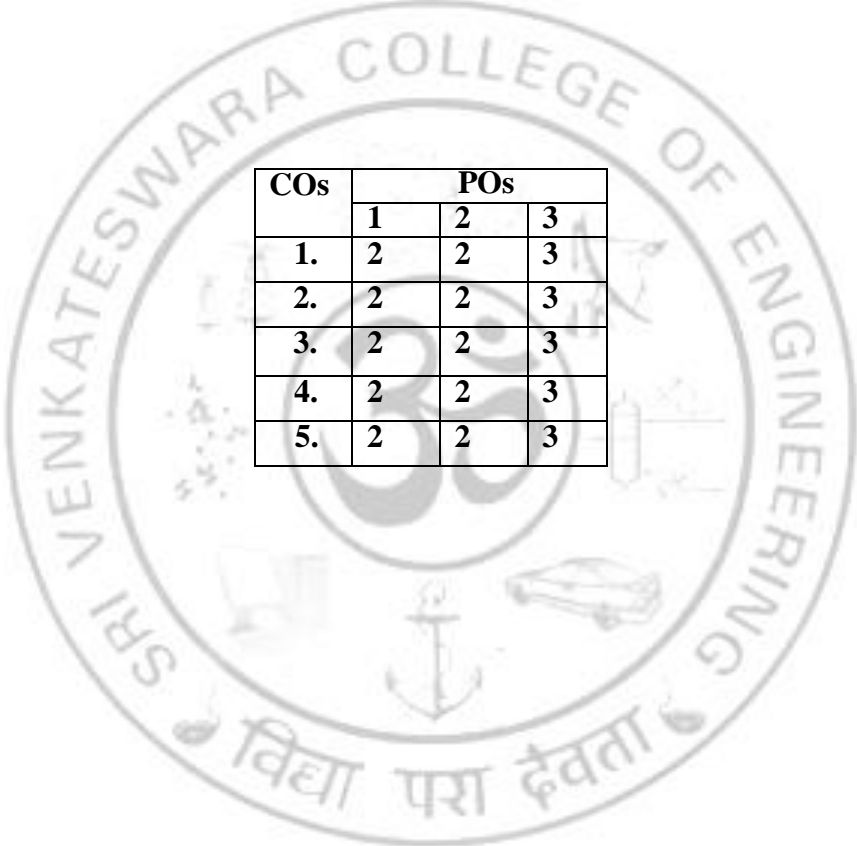
Ubuntu/ Kali Linux with C/C++/Java/Python Sleuth Kit,
Wireshark, VMWare, OWASP, DVWA

HARDWARE:

Standalone desktops - 18

Total Hours:45

COURSE ARTICULATION MATRIX



COs	POs		
	1	2	3
1.	2	2	3
2.	2	2	3
3.	2	2	3
4.	2	2	3
5.	2	2	3

