SCHEME & SYLLABUS

OF

VII & VIII SEMESTER B.E.

INFORMATION SCIENCE & ENGINEERING

2023-24

Vision of the College:
To develop thoughtful and creative young minds in a learning environment of high academic ambience by synergising spiritual values and technological competence.

Mission of the College:
1. To continuously strive for the total development of students by educating them in state-of-the-art-technologies and managerial competencies providing best in class learning experience with emphasis on skills, values and learning outcomes and helping them imbibe professional ethics and societal commitment.
2. To create research ambience that promotes interdisciplinary research catering to the needs of industry and society.
3. To collaborate with premier academic and research institutions and industries to strengthen multidisciplinary education, applied research, innovation, entrepreneurship and consulting ecosystems.

Vision of the Department:
To be a centre for quality education and research in Information Science and Engineering to create high quality professionals for catering to the need of the society.

Mission of the Department:
1) To enable students to acquire strong fundamental concepts related to the Information Science and Engineering through experiential learning.
2) To educate students towards state-of-the-art-technologies and multidisciplinary practices for a successful career by creating learning-teaching-learning ambience.
3) To inculcate life-long learning through innovation and research attitudes among students related to Information Science and Engineering.

Program Educational Objectives (PEOs):

The objectives of Information Science and Engineering degree program are to prepare students to meet the academic excellence, professionalism, and ability to solve a broad range of problems in rapidly changing technological, economic and social environment.

Graduates of the program will:

1. Pursue career as software engineer, project manager, data scientist, entrepreneur and pursue higher studies and research in Information Science and Engineering domains.

2. Apply mathematical, scientific and Information Science and Engineering knowledge with multidisciplinary approaches to solve real world problems.
3. Possess professionalism, ethical and societal responsibilities and engage in life-long learning through pursuit of skill development and certification courses in Information Science and Engineering.

Programme Outcomes (POs):

To achieve the above objectives, Information Science and Engineering degree programme strives to obtain the following outcomes which should be achieved by all graduates at the time of their graduation.

Engineering Graduates will be able to:

1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Programme Specific Outcomes (PSOs):

1) **Computing System:** Demonstrate the knowledge of evolving hardware and/or software to develop solutions to real life computational problems with a focus on performance optimization.

2) **Communication and Security:** Design and develop solutions for providing efficient transmission, storage, security and privacy of data in diverse computing environment.

3) **Information management:** Apply tools and techniques for management of information system, data analysis and knowledge discovery in the process of decision making.

SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMKUR
DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING
B.E VII Semester academic year 2023-24

Sl. No	Sub. Code	Title	Teaching Dept.	Teaching Hours/ Week			Examination				Credits
				L	T	P	Duration (Hrs.)	C.I.E. Marks	End Exam Marks.	Total Marks	
1	7RIS01	Cryptography and Blockchain Technology	ISE	4	1	-	3	50	50	100	4.5
2	7RIS02	Cyber Crime and Digital Forensics	ISE	4	-	-	3	50	50	100	4.0
3	RISEX	Professional Elective – III	ISE	3	-	-	3	50	50	100	3.0
4	OEX	Open Elective – III	OD	3	-	-	3	50	50	100	3.0
5	7RISL1	Cyber Crime and Digital Forensics Laboratory	ISE	-	-	3	3	50	50	100	1.5
6	7RISP1	Major Project Phase – I	ISE	-	-	4	-	100	-	100	2.0
7	7RISIT	Internship / Industrial Training	--	-	-	-	-	100	-	100	2.0
8	7RISTS	Technical Seminar	ISE	-	-	3	-	100	-	100	1.0
9	AICTEAP	AICTE Activity Points	ISE	Minimum 50 hrs./semester							-
		Total		**14**	**1**	**10**	**15**	**550**	**250**	**800**	**21.0**

SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMKUR
DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING
B.E VIII Semester academic year 2023-24

Sl. No	Sub. Code	Title	Teaching Dept.	Teaching Hours/ Week			Examination			
				L	T	P	Duration (Hrs.)	C.I.E. Marks	End Exam Marks.	Total Marks
1	RISEX	Professional Elective - IV	ISE	3	-	-	3	50	50	100
2	RISEX	Professional Elective - V	ISE	3	-	-	3	50	50	100
3	RISEX	Professional Elective - VI	ISE	3	-	-	3	50	50	100
4	8RISP2	Project Work Phase – 2	ISE	-	2	16	3	50	50	100
5	AICTEAP	AICTE Activity Points	ISE	(Min. 50 hrs./semester) 400 hrs. for the entire program			--	100	--	100
		Total		**9**	**2**	**16**	**12**	**300**	**200**	**500**

Professional Electives for Academic Year 2023-2024
Fifth Semester - Eighth Semester

Sl. No.	Code	Elective Name
1	RISE01	Advanced DBMS
2	RISE02	System Software
3	RISE03	Computer Vision
4	RISE04	Advanced Data Structures and Algorithms
5	RISE05	Cloud Computing
6	RISE06	Language Processor
7	RISE07	Object Oriented Modeling and Design
8	RISE08	Mobile Application Development
9	RISE09	Wireless Sensor Networks
10	RISE10	Data warehouse and Data Mining
11	RISE11	Digital Image Processing
12	RISE12	Business Intelligence
13	RISE13	Enterprise Content Management
14	RISE14	Wireless and Mobile Networks
15	RISE15	Storage Technology
16	RISE16	System simulation and Modeling

Sl. No.	Code	Elective Name
17	RISE17	High Performance Computing
18	RISE18	Information Retrieval
19	RISE19	Fuzzy Logic with Engg. Applications
20	RISE20	Artificial Neural Networks and Deep Learning
21	RISE21	Distributed Operating System
22	RISE22	Big Data Analytics
23	RISE23	Advanced Computer Architecture
24	RISE24	Bioinformatics
25	RISE25	Intelligent Agent Systems
26	RISE26	Human Computer Interaction
27	RISE27	NLP with Python
28	RISE28	Sensors and Internet of Things
29	RISE29	Agile Software Technology
30	RISE30	Web Technology
31	RISE31	JAVA and J2EE
32	RISE32	AWS

Cryptography and Blockchain Technology

Contact Hours/ Week	: 4L+1T	Credits :	4.5
Total Lecture Hours	: 52+13	CIE Marks :	50
Sub. Code	: 7RIS01	SEE Marks :	50

Course Objectives:

This course will enable students to:

1. Understand the significance of number theory in cryptographic algorithms
2. Describe the working of different block ciphers
3. Discuss the structure of SHA 512 as an example for cryptographic hash function
4. Differentiate symmetric and asymmetric cryptographic algorithms and their applications
5. Understand the basics of blockchain technology

UNIT I

Introduction to Number Theory

Divisibility and the Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality.

Computer Security concepts, The OSI Security Architecture, Security Services, Mechanisms and Attacks, A Model of Network Security.

SYMMETRIC CIPHERS: Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Rotor machine, Steganography.

10 Hrs.

UNIT II

Block Ciphers and the Data Encryption Standard

Traditional Block Cipher Structure, The Data Encryption Standard, A DES Example, The Strength of DES, Block Cipher Design Principles,

Block Cipher Operation

Multiple Encryption and Triple DES, Electronic Codebook, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode

10 Hrs.

UNIT III

Random Bit Generation and Stream Ciphers

Principles of Pseudorandom Number Generation, Pseudorandom Number Generators, Pseudorandom Number Generation Using a Block Cipher, Stream Ciphers, RC4

Public-Key Cryptography and RSA

Principles of Public-Key Cryptosystems, The RSA Algorithm

10 Hrs.

UNIT IV

Other Public-Key Cryptosystems

Diffie-Hellman Key Exchange, Elgamal Cryptographic System, Elliptic Curve Arithmetic, Elliptic Curve Cryptography

Cryptographic Hash Functions

Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA)

11 Hrs.

UNIT V

Blockchain

Distributed systems, The history of blockchain

Electronic cash

Introduction to blockchain

Various technical definitions of blockchains, Generic elements of a blockchain

Features of a blockchain, Applications of blockchain technology, Tiers of blockchain technology

Types of blockchain

Public blockchains, Private blockchains, Semi-private blockchains, Sidechains, Permissioned ledger, Distributed ledger, Shared ledger, Fully private and proprietary blockchains

Tokenized blockchains, Tokenless blockchains, Consensus in blockchain

CAP theorem and blockchain

Benefits and limitations of blockchain

Decentralization, Transparency and trust, Immutability, High availability, Highly secure, Simplification of current paradigms, Faster dealings, Cost saving, Challenges and limitations of blockchain technology

11 Hrs.

TEXT BOOKS

1	William Stallings	Cryptography and Network Security -Principles and Practices. 7th Edition, Prentice Hall of India. 2011.
2	Imran Bashir	Mastering Blockchain, Published by Packt Publishing Ltd. Birmingham B3 2PB, UK. ISBN 978-1-78712-544-5

REFERENCE BOOK

1	R. P. Feynman	Feynman lectures on computation. Penguin Books. 1996.
2	Jonathan Katz, Yehuda Lindell	Introduction to Modern Cryptography. Principles and Protocols, CRC Press.
3	Lesley Anne MacPherson	Grey Level Visual Cryptography for General Access Structures, A thesis from University of Waterloo

Course Outcomes:

Upon completion of this course the student will be able to:

CO1: **Apply** the concepts of number theory to **build** security mechanisms.

CO2: **Present** an overview of block cipher structure and analyze different block cipher operations.

CO3: **Illustrate** distribution of public keys and analyze security of multilevel encryption schemes.

CO4: **Paraphrase** authentication system by using various Message Authentication techniques.

CO5: **Identify** the elements, different types, benefits and limitations of blockchains.

Cyber Crime & Digital Forensics

Contact Hours/ Week:	4L+0T	Credits:	4.0
Total Lecture Hours:	52	CIE Marks:	50
Sub. Code:	7RIS02	SEE Marks:	50

Course objectives:

This course will enable students to:

1. Provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cyber-crime left in digital storage devices.
2. Understand topics of forensic data examination of computers and digital storage media.
3. Investigate computers used for wrong-doing.
4. 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.
5. Compare working of some Forensic tools.

UNIT I

Introduction to Cybercrime: Cybercrime: Definition and Origins of the Word, Cybercrime and information security, Who are Cybercriminals? Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. Cyberoffenses: How Criminals Plan Them: How Criminals Plan the Attacks. Social Engineering, Cyberstalking, Cybercafé and Cybercrimes. Botnets: The Fuel for Cybercrime, Attack Vector, cloud Computing.

11 Hrs.

UNIT II

Cybercrime: Mobile and Wireless Devices: introduction, Proliferation of Mobile and Wireless Devices. Trends in Mobility, Credit Card frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

11Hrs.

UNIT III

Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, virus and Worms. Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks Phishing and Identity Theft: Introduction, Phishing, identity Theft (ID Theft)

10Hrs.

UNIT IV

Understanding Computer Forensic: Introduction, History of Cyberforensics, Digital Forensics Science. The Need for Computer Forensics, Cyberforensics and Digital Evidence, Forensics, Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics. Approaching a Computer Forensics Investigation,

10Hrs.

UNIT V

Setting up a Computer Forensics Laboratory: Understanding the Requirements Computer Forensics. Forensics and Social Networking sites. The Security/Privacy Threats, Computer Forensics from Compliance. Perspective, Challenges in computer Forensics, special tools and Techniques, Forensics, Forensics Auditing, Anti Forensics.

10Hrs.

TEXT BOOKS		
1	Sunit Belapure and Nina Godbole.	Cyber Security: Understanding Cyber Crime, Computer Forensic And Legal Perspectives, Wiley India Pvt Ltd, ISBN: 978-81-265-2179, 2013.

REFERENCE BOOKS		
1	Bil Nelson, Amelia Philips and Christopher Steuart	Guide to Computer Forensics and Investigation, 4th Edition, Cengage Learning 2015.
2	Thomas J Mowbray	Cyber security Managing Systems, Conducting Testing, and Investigating Intrusions, by John Wiley & sons, ISBN: 978-1-118-84965, 2014.

Course Outcomes:

Upon completion of this course the student will be able to:

CO1: **Describe** fundamental concepts of cybercrime and Forensics.

CO2: **Analyze** motive and causes for cybercrime, detection and handling.

CO3: **Investigate** areas affected by cybercrime and investigation.

CO4: **Analyze** the need for Computer Forensics and digital evidence.

CO5: **Investigate** real world cases in the field of forensics.

Cyber Crime and Digital Forensics Lab

Lab Hours/ Week	: 3	Credits :	1.5
Sub. Code	: 7RISL1	CIE Marks :	50
		SEE Marks :	50

Course objectives:

This course will enable students to:

1. Acquire knowledge about different types of cyber-attacks.
2. Able to use different open source tools to detect vulnerabilities.
3. Perform analysis on files and folders using FTK Imager.

Lab Experiments

1. Identifying web vulnerabilities and Target Scanning using Nmap,
2. Identifying web vulnerabilities and Target Scanning using Zenmap
3. Generate malicious payload, distribute the payload to target system using Metasploit tool.
4. Attack on Target System (Based on Weaknesses identified during target scanning) using Metasploit tool.
5. To perform DNS Pharming attack using any method on computers in a LAN Environment.
6. Sniffing Website Credentials using Social Engineering Toolkit
7. Create virus and implement attack and analyse the effect of various viruses.
8. Program to perform DOS attack.
9. Program to perform DDOS attack.
10. Create a file on a USB drive and calculate its hash value like FTK Imager. Change the file and calculate the hash value again to compare the files.
11. Perform Escalation Attack and SQL Injection attack on web application.

Course Outcomes-COs

Upon successful completion of this course the student should be able to

1. **Identify** web vulnerabilities and target scanning on victim's machine.
2. **Implement** DNS Pharming attack, DOS and DDOS attack using appropriate tools.
3. **Analyse** the effect of sniffing and viruses on web applications using appropriate toolkits.

FOR

PROFESSIONAL ELECTIVE

SUBJECTS

REFER ELECTIVE SCRIPTLET