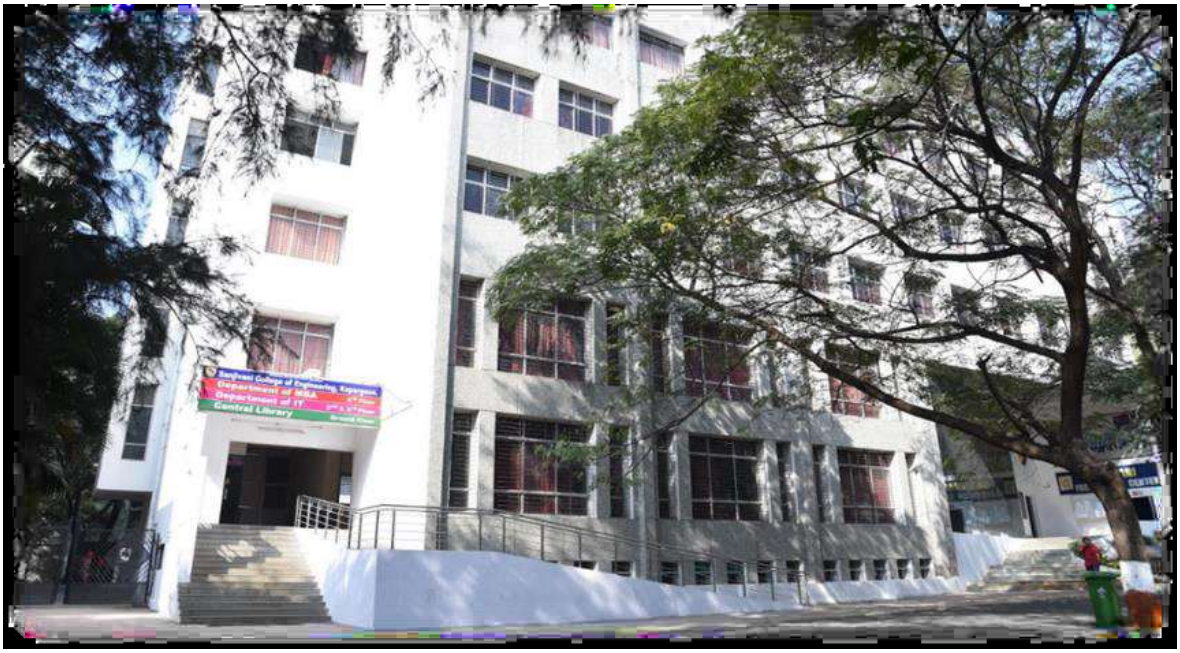
SANJIVANI RURAL EDUCATION SOCIETY'S

SANJIVANI COLLEGE OF ENGINEERING KOPARGAON

(An Autonomous Institute Affiliated to SPPU Pune)



DEPARTMENT OF INFORMATION TECHNOLOGY

COURSE CURRICULUM - 2021 PATTERN

FIRST YEAR M. TECH. CYBER SECURITY

Sanjivani College of Engineering, Kopargaon

(An Autonomous Institute affiliated to SPPU, Pune)

DECLARATION

We, the Board of Studies **INFORMATION TECHNOLOGY**, hereby declare that, We have designed the Curriculum of **F.Y. M.Tech. Cyber Security** of Pattern **2021** w.e.f. A.Y. **2021-2022** as per the guidelines. So, we are pleased to submit and publish this FINAL copy of the curriculum for the information to all the concerned stakeholders.

Submitted by

BoS Chairman

Head
Department of Information Technology
SRES College of Engineering
Kopargaon 3IS-423603

Approved by

Dean Academics

Dean Academics
Sanjivani College of Engineering
Kopargaon-423603

Director

Director
Sanjivani College of Engineering
Kopargaon

SRES College of Engineering, Kopargaon

PROFILE

Sanjivani College of Engineering (An Autonomous Institute), Kopargaon is one among the premier technical institutes in Maharashtra state in the un-aided sector established in 1983. Department of Information Technology is established in the year 2001 with an intake of 60 students. Department is acquainted with 8 well equipped laboratories with latest hardware and Software, 3 class rooms and one tutorial Hall equipped with modern teaching aids and computing facilities. UG Program in IT department is accredited by NBA New Delhi for Second time in Academic Year 2019-2020 for three Years.

There are 15 experienced & well qualified teaching staff members & 6 supporting staff members who carry out the regular academic activities as well as curricular & extracurricular activities as per the plans prepared in advance at the beginning of every semester.

In the academic year 2019-2020 strength of students in department is 275. Apart from regular academic activities students take part in curricular & co curricular activities conducted by department organization ITERA as well as other department's organization & professional bodies in the institute like CSI, ISTE, and IEEE etc. Apart from the central library the department has its own library with a very good collection of reference book, text books and CSI magazines, IEEE magazines.

Along with regular academics Department of IT has started value added courses like SAP Certification Training Programme in collaboration with Primus Techsystems Pvt. Ltd. Pune and REDHAT Academy Centre, MBPS Infotech Pune.

IT Department has started capsule courses to improve technical skill sets of students. Department is having very good placements in various renowned and multi-national companies like TCS, Infosys, Persistent, Cognizant Wipro and many more.

Also to form well balanced Industry Interaction connect and bridge the gap between Industry and institution Department of IT has organized different events like Sanjivani Though Leader, Sanjivani I-connect and Sanjivani My Story Board.

Various personal and professional skill development programs like Communication and Soft Skill programs, Aptitude Training, Technical Skill enhancement programs, Foreign Language Certification Courses, Personal and Spiritual Development Programs, Entrepreneurship Development Activities, and Preparation courses for competitive Examinations (Gate/GRE/CAT etc.) are made available in campus. Students are given opportunities to develop and nurture their leadership qualities through Student Associations, Student Council, Professional Body activities and working as volunteers in various events organized at Department/ College level.

VISION AND MISSION
Vision of Institute
To develop world class professionals through quality education.
Mission of Institute
To create Academic Excellence in the field of Engineering and Management through Education, Training and Research to improve quality of life of people.
Vision of Department
To develop world class IT professionals through quality education.
Mission of Department
To create Academic Excellence in the field of Information Technology through Education, Industry Interaction, Training and Innovation to improve quality of life of people. We are committed to develop industry competent technocrats with life-long learning capabilities and moral values.

PROGRAM EDUCATIONAL OBJECTIVES
PEO 1:
Post Graduates of Cyber Security program should possess knowledge of advanced concepts in application, network & infrastructure security, intrusion detection, digital forensics and data governance as well as skills in the field of Cyber Security for providing solution to complex software security problem of any domain by analyzing, designing and implementing.
PEO 2:
Post Graduates of Cyber Security program should possess better public speaking & presentation, time management, creativity & innovation, strategic planning and teamwork skills leading to responsible and competent research, entrepreneurship and professionals that will be able to address challenges in the field of Cyber Security at global level.
PEO 3:
Post Graduates of Cyber Security program should have commitment to tackle social engineering through advanced technical defenses.

PROGRAM OUTCOMES
PO1:
An ability to independently carry out research /investigation and development work to solve practical problems
PO2:
An ability to write and present a substantial technical report/document.
PO3:
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
PO4:
An ability to demonstrate strategic planning, time management and teamwork skills.
PO5:
An ability to tackle the social engineering attacks.
PO6:
-

PROGRAM SPECIFIC OUTCOMES
PSO1:
An ability to provide security solutions by applying the knowledge of cryptography, blockchain technology and digital forensics.
PSO2:
An ability to create and innovate in the field of cyber security.
PSO3:
-

LIST OF ABBREVIATIONS			
Abbreviation	**Full Form**	**Abbreviation**	**Full Form**
ES	Engineering Science	HSMC	Humanity Science
PC	Professional Core	CA	Continuous Assessment
PE	Professional Elective	OR	End Semester Oral Examination
OE	Open Elective	PR	End Semester Practical Examination
ISE	In-Semester Evaluation	TW	Continuous Term work Evaluation
ESE	End-Semester Evaluation	BSC	Basic Science Course
PRJ	Project	MC	Mandatory Course

COURSE STRUCTURE- 2021 PATTERN
FIRST YEAR M. TECH. CYBER SECURITY

SEMESTER- I

Course		Course Title	Teaching Scheme Hours/ Week			Credits	Evaluation Scheme - Marks						
							Theory			OR	PR	TW	Total
Cat.	Code		L	T	P		ISE	ESE	CA				
PC	CS101	Mathematical Foundations of Cyber Security	3	-	-	3	20	30	50	-	-	-	100
PC	CS102	Cyber Crime and Cyber Law	3	-	-	3	20	30	50	-	-	-	100
PE	CS103	Professional Elective -I	3	-	-	3	20	30	50	-	-	-	100
PE	CS104	Professional Elective -II	3	-	-	3	20	30	50	-	-	-	100
PC	CS105	Lab practice-I	-	-	4	2	-	-	-	50	-	-	50
PE	CS106	Lab practice-II	-	-	4	2	-	-	-	50	-	-	50
MLC	CS107	Research Methodology and IPR	2	-	-	2	-	-	50	-	-	-	50
AC	AC101	**Audit Course - I**	2	-	-	-	-	-	-	-	-	-	-
		Total	16	0	8	18	80	120	250	100	0	0	550

CS103 Professional Elective I	
CS103A	Concept of Ethical Hacking
CS103B	Block-chain and Mathematical Underpinnings
CS103C	Forensic and Social Network Analytics

CS104 Professional Elective II	
CS104A	Ethical Hacking and System Defense
CS104B	Development Platforms and Language Foundations of Block-chain
CS104C	Mobile Digital and Forensics

SEMESTER- II

Course		Course Title	Teaching Scheme Hours/ Week			Credits	Evaluation Scheme – Marks						
							Theory			OR	PR	TW	Total
Cat.	Code		L	T	P		ISE	ESE	CA				
PC	CS108	Wireless Network Security and Privacy	3	-	-	3	20	30	50	-	-	-	100
PC	CS109	Cyber Forensics, Audit and Investigation	3	-	-	3	20	30	50	-	-	-	100
PC	CS110	Professional Elective- III	3	-	-	3	20	30	50	-	-	-	100
PE	CS111	Professional Elective- IV	3	-	-	3	20	30	50	-	-	-	100
PC	CS112	Lab practice-III	-	-	4	2	-	-	-	50	-	-	50
PE	CS113	Lab practice-IV	-	-	4	2	-	-	-	50	-	-	50
PRJ	CS114	Mini-Project with Seminar	-	-	4	2	-	-	-	50	-	-	50
AC	AC102	Audit Course - II	2	-	-	-	-	-	-	-	-	-	-
		Total	16	0	12	18	80	120	200	150	0	0	550

Professional Elective III	
CS110A	Ethical Hacking for Administrators
CS110B	Cryptocurrency Technology and Smart contract
CS110C	Criminology and Analytics

Professional Elective IV	
CS111A	Penetration Testing and Vulnerability Assessment
CS111B	Security in IoT with Blockchain
CS111C	Risk analysis and Management

COURSE STRUCTURE- 2021 PATTERN
SECOND YEAR M. TECH. CYBER SECURITY

SEMESTER - III

Course		Course Title	Teaching Scheme Hours/ Week			Credits	Evaluation Scheme – Marks						
							Theory			OR	PR	TW	Total
Cat.	Code		L	T	P		ISE	ESE	CA				
OE	CS201	Open Elective	3	-	-	3	20	30	50	-	-	-	100
PE	CS202	Professional Elective- V	3	-	-	3	20	30	50	-	-	-	100
PC	CS203	Dissertation Phase -1	-	-	20	10	-	-	-	50	-	-	50
		Total	6	-	16	16	40	60	100	50	-	-	250

Open Elective	
CS201A	Internet of Things Security Framework
CS201B	Cryptography and Network Security
CS201C	Cloud Security
CS201D	Android Security

SEMESTER - IV

Course		Course Title	Teaching Scheme Hours/ Week			Credits	Evaluation Scheme – Marks						
							Theory			OR	PR	TW	Total
Cat.	Code		L	T	P		ISE	ESE	CA				
PC	CS204	Dissertation Phase -II	-	-	32	16	-	-	-	100	-	50	150
		Total	-	-	28	16	-	-	-	150	-	50	150

Total Credits for the programme = 18 + 18 +16 +16 = 68

F.Y.
M. Tech.
Cyber Security
Semester I

CS101: Mathematical Foundations of Cyber Security		
Teaching Scheme	**Examination Scheme**	
Lectures: 3 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 3	**Total:**	**100 Marks**
Prerequisite Course:		

Course Objectives

1. To understand number theory including divisibility, greatest common divisor and prime number.
2. To understand Euclidean algorithm, fermat's theorem and euler theorem.
3. To understand the algebraic structure.
4. To gain knowledge of Bay's theorem.
5. To apply probability for discrete random variables.
6. To understand coding with cryptographic hash function.

Course Outcomes (COs):

After successful completion of the course, student will be able to

Course Outcome (s)		Bloom's Taxonomy	
		Level	**Descriptor**
CO1	**Learn** about Number theory including Divisibility, Greatest common divisor and Prime numbers.	**2**	**Understand**
CO2	**Understand** Euclidean algorithm, Fermat's theorem and Euler's theorem.	**2**	**Understand**
CO3	**Understand** the concept of Algebraic structure including Groups, Rings, Fields and Classifications.	**2**	**Understand**
CO4	**Calculate** probability based on Bay's theorem.	**4**	**Analyse**
CO5	**Calculate** probability for discrete random variables and continuous random variables.	**4**	**Analyse**
CO6	**App**ly the concept of Coding with cryptographic hash function.	**3**	**Apply**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	
CO1	3	2	-	1	1		3	1	
CO2	-	-	-	3	1		2	1	
CO3	1	2	2	2	1		2	1	
CO4	2	-	-	2	-		2	1	
CO5	-	-	-	-	3		1	1	
CO6	1	2	-	2	3		-	-	

Course Contents			
Unit-I	**INTRODUCTION TO NUMBER THEORY**	**No. of Hours**	**COs**
	Introduction-Divisibility - Greatest common divisor – Primes- Prime numbers – Cardinality of Primes, Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers, Fermat's and Euler's Theorem, Testing for Primality, Factorization, The Chinese Reminder Theorem, Quadratic Congruence, Exponentiation and Logarithms, Discrete Logarithms.	6	CO1
Unit-II	**ALGEBRAIC STRUCTURES AND FINITE FIELDS**	**No.of Hours**	**COs**
	Groups – Cyclic groups, Co sets, Modulo groups - Primitive roots – Discrete logarithms The Euclidean Algorithm, Modular Arithmetic, Algebraic Structures-Groups, Rings and Fields, Future Fields of the Form GF(2"), Polynomial Arithmetic, Finite Fields of the Form GF(2n)	6	CO2
Unit-III	**PSEUDORANDOM NUMBER GENERATION AND STREAM CIPHERS**	**No. of Hours**	**COs**
	Principles of Pseudorandom Number Generation, Principles of Pseudorandom Number Generation using a Block Cipher, Stream Ciphers, RC4, True Random Number Generators	6	CO3
Unit-IV	**DISCRETE MATHEMATICS FOR CRYPTOGRAPHY**	**No. of Hours**	**COs**
	Cryptography and Modular Arithmetic, Inverses & GCDs, The RSA Cryptosystems, Mathematical Induction, Recursion, Recurrences and Induction, Recurrences and Selection	6	CO4
Unit-V	**CODING THEORY**	**No. of Hours**	**COs**
	Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes	6	CO5
Unit-VI	**PROBABILITY THEORY&CRYPTOGRAPHIC HASH FUNCTIONS**	**No. of Hours**	**COs**
	Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process- Markov Chain. Application of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Functions (SHA), SHA-512	6	CO6

Text Books:

1. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
2. Joseph A. Gallian, "Contemporary Abstract Algebra", Narosa, 1998.
3. William Stallings, "Cryptography and Network Security", 5th Edition, Pearson Education.

Reference Books:

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, "An introduction to the theory of numbers", John Wiley and Sons 2004.
2. C.L. Liu, "Elements of Discrete mathematics", McGraw Hill, 2008.
3. Behrouz A. Forouzan, "Cryptography and Network Security", TMH Publication.

CS102: Cyber Crime and Cyber Law		
Teaching Scheme	**Examination Scheme**	
Lectures: 3 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 3	**Total:**	**100 Marks**
Prerequisite Course:		

Course Objectives

1. To learn and understand the cyber-crime and cyber-laws.
2. To learn and understand the different cybercrime issues.
3. To explore the knowledge of Cyber Act.
4. To get the information about the amended laws.
5. To learn cyber laws and legislation.
6. To learn the different case studies of cyber crime and cyber law.

Course Outcomes (COs):

After successful completion of the course, student will be able to

Course Outcome (s)		Bloom's Taxonomy	
		Level	**Descriptor**
CO1	**Understand** the cyber-crime and cyber-laws	**2**	**Understand**
CO2	**Understand** the different issues related with cyber-crime.	**2**	**Understand**
CO3	**Explore** the knowledge related with cyber act.	**2**	**Understand**
CO4	**Understand** the IT act for cyber-crime.	**2**	**Understand**
CO5	**Understand** the cyber laws and legislation.	**2**	**Understand**
CO6	**Understand** the different case studies related with cyber-crime and laws	**2**	**Understand**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	
CO1	2	2	2	-	1		1	-	
CO2	3	3	3	-	1		1	-	
CO3	2	2	3	-	3		3	2	
CO4	2	2	2	-	3		3	2	
CO5	2	2	2	-	3		2	3	
CO6	3	3	2	-	3		2	3	

Course Contents			
Unit-I	**INTRODUCTION TO CYBER CRIME**	**No. of Hours**	**COs**
	Introduction to cyber crime and cyber law, cyber space and information technology, Nature and scope of cyber crime, Jurisdiction of cyber crime.	6	CO1
Unit-II	**CYBER CRIME ISSUES**	**No. of Hours**	**COs**
	Important definitions under IT Act 2000, Cyber crime issues: unauthorized access, White collar crimes, viruses, malwares, worms, Trojans, logic bomb, Cyber stalking, voyeurism, obscenity in internet, Software piracy.	6	CO2
Unit-III	**INTRODUCTION TO IT ACT**	**No. of Hours**	**COs**
	IT Act 2000, offences under IT Act and IT (amendment) Act, 2008. CRPC overview, Case studies Role of intermediaries, Electronic evidence, Cyber terrorism, espionage, warfare and protected system.	6	CO3
Unit-IV	**IT ACT FOR CYBER THEFT**	**No. of Hours**	**COs**
	Overview of amended laws by the IT Act, 2000: The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891, The Reserve Bank of India Act, 1934, Cyber Theft and the Indian Telegraph Act, 1885. Relevant Case laws. Digital Signatures and certificate - legal issues.	6	CO4
Unit-V	**CYBER LAW AND RELATED LEGISLATION**	**No. of Hours**	**COs**
	Patent Law, Trademark Law, Copyright, Software – Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book. Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution, Online Dispute Resolution (ODR).	6	CO5
Unit-VI	**CASE STUDY ON CYBER CRIMES**	**No. of Hours**	**COs**
	Harassment Via E-Mails, Email Spoofing (Online A Method Of Sending E-Mail Using A False Name Or E-Mail Address To Make It Appear That The E-Mail Comes From Somebody Other Than The True Sender), Cyber Pornography (Exm.MMS), Cyber-Stalking.	6	CO6

Text Books:

1. K. Kumar, "Cyber Laws: Intellectual property & E Commerce,Security",1st Edition, Dominant Publisher, 2011.
2. Rodney D. Ryder, "Guide to Cyber Laws", 2nd Edition, Wadhwa And Company, New Delhi, 2007.
3. "Information Security Policy & Implementation Issues", NIIT, PHI.

Reference Books:

1. Raghu Santanam, M. Sethumadhavan, "Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives", Information Science Reference

2. Pfleeger, Charles P. and Shari L. Pfleeger, “Security in Computing”, 4th Edition. Upper Saddle River, NJ: Prentice Hall, 2008.
3. Douglas Thomas; Brian Loader, “Cybercrime: Security and Surveillance in the Information Age”, 1st Edition, Routledge, 2013.
4. D. Icove, K. Seger, and W. Von Storch, “Computer Crime: A Crime-Fighter's Handbook”, O'Reilly, 1995.
5. R. Smith, “Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities”, Routledge, 2018.
6. Pavan Duggal, “Cyberlaw – The Indian Perspective”, Saakshar Law Publications.
7. Jonathan Rosenoer, “Cyber Law: The law of the Internet”, Springer-Verlag, 1997.
8. Mark F Grady, Fransesco Parisi, “The Law and Economics of Cyber Security”, Cambridge University Press, 2006.

CS103A: Concepts of Ethical Hacking (Professional Elective – I)		
Teaching Scheme	**Examination Scheme**	
Lectures: 3 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 3	**Total:**	**100 Marks**
Prerequisite Course:		

Course Objectives

1. To introduce the concepts of Ethical Hacking**.**
2. To Give the students the opportunity to learn about different tools and techniques in Ethical hacking and security.
3. To Practically apply Ethical hacking tools to perform various activities
4. To introduce the methodologies framework tools of ethical hacking to get awareness in enhancing the security.
5. To get knowledge on various attacks and their detection.
6. To render all the techniques used for penetration testing for performing security auditing.

Course Outcomes (COs):

After successful completion of the course, student will be able to

	Course Outcome (s)	**Bloom's Taxonomy**	
		Level	**Descriptor**
CO1	**Understand** the core concepts related to vulnerabilities and their causes	**2**	**Understand**
CO2	**Understand** ethics behind hacking and vulnerability disclosure. Appreciate the impact of hacking	**2**	**Understand**
CO3	**Exploit** the vulnerabilities related to computer system and networks using state of the art tools and technologies.	**4**	**Analyze**
CO4	**Gain** the knowledge of the use and availability of tools to support an ethical hack.	**3**	**Apply**
CO5	**Gain** the knowledge of interpreting the results of a controlled attack	**3**	**Apply**
CO6	**Demonstrate** the impact of hacking.	**3**	**Apply**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	
CO1	3	3	3	2	3		3	2	
CO2	3	3	3	2	3		3	2	
CO3	3	3	3	2	3		3	2	
CO4	3	3	3	2	3		3	2	
CO5	3	3	3	2	3		3	2	
CO6	3	3	3	2	3		3	2	

Course Contents			
Unit-I	**INTRODUCTION TO ETHICAL HACKING**	**No. of Hours**	**COs**
	Introduction-Ethical hacking Terminology-types of hacking technologies-phases of ethical hacking Foot printing-Social Engineering-Scanning and enumeration.	6	CO1
Unit-II	**SYSTEM HACKING**	**No. of Hours**	**COs**
	Understanding the password hacking techniques- Rootkits-Trojans-Backdoors-Viruses and worms sniffers-denial of service-Session hijacking.	6	CO2
Unit-III	**WEB SERVER HACKING**	**No. of Hours**	**COs**
	Hacking web servers-web application vulnerabilities –Buffer overflow-Wireless hacking-Physical Security.	6	CO3
Unit-IV	**WIRELESS HACKING**	**No. of Hours**	**COs**
	WEP, WPA Authentication mechanism-wireless sniffers-Physical Security-factors affecting physical security-honeypots-Firewall types.	6	CO4
Unit-V	**PENETRATION TESTING**	**No. of Hours**	**COs**
	Cryptography-overview of MD5, SHA, RC4-penetration testing methodologies- steps-pen test legal framework-penetration testing tools.	6	CO5
Unit-VI	**PORT SCANNING**	**No. of Hours**	**COs**
	Introduction to Port Scanning: Types of Port Scans, Using Port-Scanning Tools: Nmap, Unicornscan, Nessus and OpenVAS Conducting Ping Sweeps: Fping, Hping, Crafting IP Packets, Understanding Scripting: Scripting Basics.	6	CO6

Text Books:

1. Simpson, Michael T., "Hands-on Ethical Hacking and Network Defense: Simpson", Boston, MA: Course Technology, 2013.
2. Steven DeFino, Barry Kaufman, Nick Valenteen, "Official Certified Ethical Hacker Review Guide".

Reference Books:

1. P. Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Waltham, MA, USA: Syngress, 2013.
2. "Hands- On Ethical Hacking and Network Defense", Print Replica, Kindle Edition.

CS103B: Blockchain and Mathematical Underpinnings (Professional Elective-I)		
Teaching Scheme	**Examination Scheme**	
Lectures: 3 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 3	**Total:**	**100 Marks**
Prerequisite Course:		

Course Objectives

1. To describe appropriate cryptocurrencies techniques in the application development.
2. To use appropriate consensus for solving problems and programming.
3. To use Bitcoin basics and use of it in Cryptocurrencies.
4. To apply appropriate constructs of Solidity language, coding standards for application development.
5. To use Ethereum Virtual Machine for solving problems and programming.
6. To select appropriate Zero Knowledge proofs and protocols in Blockchain foundations for problem solving and programming.

Course Outcomes (COs):

After successful completion of the course, student will be able to

	Course Outcome (s)	Bloom's Taxonomy	
		Level	**Descriptor**
CO1	**Describe** appropriate cryptocurrencies techniques in the application development.	**2**	**Understand**
CO2	**Use** appropriate consensus for solving problems and programming.	**3**	**Apply**
CO3	**Use** Cryptographic basics for cryptocurrency concepts in various application developments.	**3**	**Apply**
CO4	**Use** Bitcoin basics and use of it in Cryptocurrencies.	**3**	**Apply**
CO5	**Use** Ethereum Virtual Machine for solving problems and programming.	**4**	**Analyze**
CO6	**Select** appropriate Zero Knowledge proofs and protocols in Blockchain foundations for problem solving and programming.	**4**	**Evaluate**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	
CO1	2	1	2	1	2		3	2	
CO2	2	3	3	2	1		2	2	
CO3	2	1	2	2	2		3	2	
CO4	1	1	2	2	2		2	2	
CO5	2	1	2	2	2		2	2	
CO6	2	2	2	2	2		2	2	

Course Contents			
Unit-I	**COURSE INTRODUCTION**	**No. of Hours**	**COs**
	History of cryptocurrencies, Bitcoin and Ethereum and associated mathematical underpinnings, number theory, integers, primes. The algorithms, one-way and hashing functions, Merkle–Damgård hash functions. Data structures involving data and hash, and blockchains.	06	CO1
Unit-II	**THE CONSENSUS PROBLEM**	**No. of Hours**	**COs**
	The consensus problem - Asynchronous Byzantine Agreement - AAP protocol and its analysis - Nakamoto Consensus on permission-less, nameless, peer-to-peer network - Abstract Models for BLOCKCHAIN - GARAY model - RLA Model - Proof of Work (PoW) as random oracle - formal treatment of consistency, liveness and fairness - Proof of Stake (PoS) based Chains - Hybrid models (PoW + PoS).	06	CO2
Unit-III	**CRYPTOGRAPHIC BASICS FOR CRYPTOCURRENCY**	**No. of Hours**	**COs**
	Cryptographic basics for cryptocurrency - a short overview of Hashing, signature schemes, encryption schemes and elliptic curve cryptography. Totient function, Fermat and Euler theorems, cryptographic algorithms.	06	CO3
Unit-IV	**BITCOIN**	**No. of Hours**	**COs**
	Bitcoin - Wallet - Blocks - Merkley Tree - hardness of mining - transaction verifiability - anonymity - forks - double spending - mathematical analysis of properties of Bitcoin.	06	CO4
Unit-V	**ETHEREUM**	**No. of Hours**	**COs**
	Ethereum - Ethereum Virtual Machine (EVM) - Wallets for Ethereum - Solidity - Smart Contracts - some attacks on smart contracts.	06	CO5
Unit-VI	**PROTOCOLS IN BLOCKCHAIN**	**No. of Hours**	**COs**
	Zero Knowledge proofs and protocols in Blockchain - Succinct non interactive argument for Knowledge (SNARK) - pairing on Elliptic curves - Zcash.	06	CO6

Text Books:

1. Arvind Narayanan, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction” Princeton University Press (July 19, 2016).
2. Don and Alex Tapscott, “Blockchain Revolution”. Portfolio Penguin 2016.
3. William Mougayar, “Business Blockchain Promise, Practice and Application of the Next Internet Technology, John Wiley & Sons 2016.

Reference Books:

1. Imran Bashir, “Mastering Blockchain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained”, Second Edition, Packt Publishing, 2018.
2. Andreas Antonopoulos, Satoshi Nakamoto, “Mastering Bitcoin”, O”Reilly, 2014.
3. Roger Wattenhofer, “The Science of the Blockchain” CreateSpace Independent Publishing, 2016.
4. Joseph Bonneau et al, SoK: Research perspectives and challenges for Bitcoin and cryptocurrency, IEEE Symposium on security and Privacy, 2015 (article available for free download) { curtain raiser kind of generic article, written by seasoned experts and pioneers}.

5. J.A.Garay et al, “The Bitcoin Backbone Protocol - Analysis and Applications”, EUROCRYPT 2015 LNCS VOl 9057, (VOLII), pp 281-310. (Also available at eprint.iacr.org/2016/1048) . (serious beginning of discussions related to formal models for bitcoin protocols).
6. R.Pass et al, “Analysis of Blockchain protocol in Asynchronous Networks” , EUROCRYPT 2017, (eprint.iacr.org/2016/454) . A significant progress and consolidation of several principles).
7. R.Pass et al, “Fruitchain, a Fair Blockchain”, PODC 2017 (eprint.iacr.org/2016/916).

CS103C: Forensic and Social Network Analytics (Professional Elective - I)		
Teaching Scheme	**Examination Scheme**	
Lectures: 3 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 3	**Total:**	**100 Marks**
Prerequisite Course:		

Course Objectives

1. To understand Network forensics.
2. To understand Disk forensics.
3. To develop semantic web related applications.
4. To discover mobile social networks and communities from Social Networks.
5. To decentralize Online Social Networks and predict human behavior for social communities.
6. To explore different applications of Social Networks.

Course Outcomes (COs):

After successful completion of the course, student will be able to

Course Outcome (s)		Bloom's Taxonomy	
		Level	**Descriptor**
CO1	**Understand** Network forensics.	**2**	**Understand**
CO2	**Understand** Disk forensics.	**2**	**Understand**
CO3	**Develop** semantic web related applications.	**3**	**Apply**
CO4	**Discover** mobile social networks and communities from Social Networks.	**2**	**Understand**
CO5	**Decentralize** Online Social Networks and predict human behavior for social communities.	**4**	**Analyze**
CO6	**Explore** different applications of Social Networks.	**2**	**Understand**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	
CO1	1	--	2	1	--		--	3	
CO2	1	--	2	1	2		--	3	
CO3	2	--	3	--	2		--	3	
CO4	--	2	--	--	--		--	3	
CO5	--	1	--	--	--		--	3	
CO6	1	--	--	--	1		--	3	

Course Contents			
Unit-I	**NETWORK FORENSICS**	**No. of Hours**	**COs**
	Network components – nodes, edges, adjacency matrix, Port Scans, SYN flood, Key Loggers, Email Forensics, Email spoofing, Phishing, Mail header analysis, Network protocols, Protocols Susceptible to Sniffing - Active and Passive Sniffing, Wireshark - Capture and Display Filters, pcap analysis, Problems - Trojans and Backdoors, Overt and Covert Channels, Types of Trojans, Botnets, Types of botnet, Structure of bots, Crime bots, Spamming bots, Honey Pots, Forensic evidences.	06	CO1
Unit-II	**DISK FORENSICS**	**No. of Hours**	**COs**
	Digital data, Digital device, Hard disk, Types, Disk characteristics, SSD, File systems – NTFS, MFT Structure - fragmentation, MFT fragmentation, Files and attributes, File hashing, Slack space, Disk Forensics tools, Win Hex, Disk imaging, write blockers, Types of blockers, Data Carving, techniques, Scalpel, Registry Forensics, Registry, Registry data types, RegEdit, Concept of timeline, Anti forensics.	06	CO2
Unit-III	**INTRODUCTION TO SEMANTIC WEB**	**No. of Hours**	**COs**
	Limitations of Current Web, The Semantic Solution, Development of Semantic Web, Emergence of the Social Web, Social Network analysis, Development of Social Network Analysis – Key concepts and measures in network analysis, Electronic sources for network analysis.	06	CO3
Unit-IV	**SOCIAL MEDIA MINING AND SEARCH**	**No. of Hours**	**COs**
	Discovering Mobile social Networks by semantic Technologies, Online Identities in Social Networking, Detecting Communities in Social Networking, Discovering Communities from Social Networks, Methodologies and Applications.	06	CO4
Unit-V	**SOCIAL NETWORK INFRASTRUCTURES AND COMMUNITIES**	**No. of Hours**	**COs**
	Discovering Mobile Social Networks by Semantic Technologies, Online Identities in Social Networking, Detecting Communities in social Networking, Discovering Communities from Social Networks, Methodologies and Applications.	06	CO5
Unit-VI	**VISUALISATION AND APPLICATIONS OF SOCIAL NETWORKS**	**No. of Hours**	**COs**
	Visualization and Applications of Social Networks, Novel Visualizations and Interactions for Social Networks Exploration, Applications of Social Network Analysis, Online Advertising in Social Networks.	06	CO6

Text Books:

1. Dejey, "Cyber forensics", Oxford, 2018.
2. Marjie T. Britz, "Computer Forensics and Cyber Crime - An Introduction", 3rd Edition.
3. Peter Mika, "Social Networks and the Semantic Web", 1st Edition, Springer 2007.
4. Charles Kadushin, "Understanding Social Networks: Theories, Concepts and Findings", 1st Edition. Oxford University Press, 2012.

Reference Books:

1. Gerard Johanses, "Digital Forensics and Incident Response", 2017.
2. GuandongXu,Yanchun Zhang and Lin Li, "Web Mining and Social Networking – Techniques and applications", 1st Edition, Springer, 2011.
3. Borko Furht, "Handbook of Social Network Technologies and Applications", 1st Edition, Springer, 2010.
4. Max Chevalier, Christine Julien and Chantal Soulé-Dupuy, "Collaborative and Social Information Retrieval and Access: Techniques for Improved user Modelling", IGI Global Snippet, 2009.

CS104A: Ethical Hacking and System Defense (Professional Elective – II)		
Teaching Scheme	**Examination Scheme**	
Lectures: 3 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 3	**Total:**	**100 Marks**
Prerequisite Course:		

Course Objectives

1. To understand concepts of Ethical Hacking.
2. To understand Wireless Hacking.
3. To understand concepts of Vulnerability.
4. To learn tools and techniques in Ethical hacking.
5. To learn Mobile platform security.
6. To learn Network defence.

Course Outcomes (COs):

After successful completion of the course, student will be able to

Course Outcome (s)		Bloom's Taxonomy	
		Level	**Descriptor**
CO1	**State** the fundamental concepts of wireless technologies and security.	**1**	**Remember**
CO2	**Explain** the confidentiality, integrity and availability in mobile phones.	**2**	**Understand**
CO3	**Understand** the basic concepts of mobile phone forensics.	**2**	**Understand**
CO4	**Understand** the evidential potential of digital devices and its handling.	**2**	**Understand**
CO5	**Remember** the methods of investigation using digital forensic techniques.	**1**	**Remember**
CO6	**Apply** digital forensic knowledge to use computer forensic tools.	**3**	**Apply**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	
CO1	1	1	2	1	3		3	1	
CO2	1	1	2	1	3		3	1	
CO3	1	1	2	1	3		3	1	
CO4	1	1	2	1	3		3	1	
CO5	1	1	2	1	3		3	1	
CO6	1	1	2	1	3		3	1	

Course Contents			
Unit-I	**TCP/IP OVERVIEW CONCEPTS**	**No. of Hours**	**COs**
	Overview of TCP/IP-IP addressing-numbering systems-Denial of service attacks-distributed denial of service attacks.	06	CO1
Unit-II	**PORT SCANNING**	**No. of Hours**	**COs**
	Introduction to port scanning-types of port scan-port scanning tools-ping sweeps Understanding scripting-Enumeration-Net BIOS basics-Enumeration tools	06	CO2
Unit-III	**PROGRAMMING FOR SECURITY PROFESSIONALS**	**No. of Hours**	**COs**
	Introduction to programming fundamentals-Basics of C-Basics of HTML-Understanding perl Understanding oops concepts.	06	CO3
Unit-IV	**DESKTOP AND SERVER OS VULNERABILITIES**	**No. of Hours**	**COs**
	Windows OS vulnerabilities-tools for identifying vulnerabilities in windows-Linux OS vulnerabilities -vulnerabilities of embedded OS.	06	CO4
Unit-V	**NETWORK PROTECTION SYSTEMS**	**No. of Hours**	**COs**
	Understanding routers-understanding firewalls-risk analysis tools for firewalls-understanding intrusion and detection and prevention systems-honeypots.	06	CO5
Unit-VI	**PROGRAMMING FOR CYBER SECURITY**	**No. of Hours**	**COs**
	Introduction to programming fundamentals-Basics of C++-Basics of PHP-Understanding Python Understanding oops concepts.	06	CO6

Text Books:

1. Baloch, R., "Ethical Hacking and Penetration Testing Guide", CRC Press, 2015.
2. Beaver, K., "Hacking for Dummies", 3rd Edition, John Wiley & Sons., 2013.
3. Council, Ec. , "Computer Forensics: Investigating Network Intrusions and Cybercrime", Cengage Learning, 2nd Edition, 2010.
4. McClure S., Scambray J., and Kurtz G, "Hacking Exposed", Tata McGraw-Hill Education, 6th Edition, 2009.

Reference Books:

1. William Stallings, "Network Security Essentials: Applications and Standards", Prentice Hall, 4th edition, 2010.
2. James S. Tiller, "The Ethical Hack: A Framework for Business Value Penetration Testing", Auerbach Publications, 2004.
3. "International Council of E-Commerce Consultants by Learning, Penetration Testing Network and Perimeter Testing Ec-Council/ Certified Security Analyst", Vol. 3 of Penetration Testing, Cenage Learning, 2010.
4. Davidoff, S. and Ham, J., "Network Forensics Tracking Hackers through Cyberspace", Prentice Hall, 2012.
5. Michael G. Solomon, K Rudolph, Ed Tittel, Broom N., and Barrett, D.,Computer, "Forensics Jump Start", Willey Publishing, Inc, 2011.

CS104B: Development Platforms and Language Foundations of Block-Chain (Professional Elective – II)		
Teaching Scheme	**Examination Scheme**	
Lectures: 3 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 3	**Total:**	**100 Marks**
Prerequisite Course:		

Course Objectives

1. To use of programming language for Cryptocurrencies with Blockchain.
2. To use Javascript in the decentralized application.
3. To use of Hyperledger Platform for Blockchain development.
4. To apply Blockchain in Financial, Manufacturing and Retails.
5. To use of smart contract in Ethereum Blockchain.
6. To use of programming language for Cryptocurrencies with Ethereum.

Course Outcomes (COs):

After successful completion of the course, student will be able to

	Course Outcome (s)	Bloom's Taxonomy	
		Level	**Descriptor**
CO1	**Use** of programming language for Cryptocurrencies with Blockchain.	**3**	**Apply**
CO2	**Use** of Javascript in the decentralized application.	**3**	**Apply**
CO3	**Use** of Hyperledger Platform for Blockchain development.	**3**	**Apply**
CO4	**Apply** Blockchain in Financial, Manufacturing &Retails.	**3**	**Apply**
CO5	**Use** of smart contract in Ethereum Blockchain.	**3**	**Apply**
CO6	**Use** of programming language for Cryptocurrencies with Ethereum.	**3**	**Apply**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	
CO1	2	1	3	2	2		3	2	
CO2	2	1	3	3	2		3	2	
CO3	2	1	3	3	2		3	2	
CO4	2	1	3	2	3		3	2	
CO5	2	1	3	1	2		3	2	
CO6	2	1	3	1	2		3	2	

Course Contents			
Unit-I		**No. of Hours**	**COs**
	Programming languages used in cryptocurrencies and blockchain technologies.	06	CO1
Unit-II		**No. of Hours**	**COs**
	Programming in the Ethereum platform (decentralized applications): Role of Javascript, Solidity and Serpent in Ethereum contract programming.	06	CO2
Unit-III		**No. of Hours**	**COs**
	Programming languages in Hyperledger development (Go Lang, Node and Javascript). IBM Hyperledger platform (composer, blockchain fabric, operator).	06	CO3
Unit-IV		**No. of Hours**	**COs**
	Programming assignments to include business use cases in the financial services, manufacturing, and retail industries.	06	CO4
Unit-V		**No. of Hours**	**COs**
	Programming in the Solidity platform (decentralized applications): Role of script, Solidity and Serpent in Ethereum contract programming.	06	CO5
Unit-VI		**No. of Hours**	**COs**
	Programming languages used in cryptocurrencies and Ethereum technologies.	06	CO6
Text Books:			
1. Melanie Swan, "Blockcahin-Blueprint for new economy", O'Reilly Publication, ISBN: 978-1-491-92049-7. 2. Tiana Laurence "Blockcahin for dummies" Wiley Publication, ISBN: 978-1-119-36559-4.			
Reference Books:			
1. Dr.Gavin Wood "Mastering Ethereum: Building Smart Contracts And DApps", O'Reilly Publication, ISBN-9789352137961.			

CS104C: Mobile Digital and Forensics (Professional Elective – II)		
Teaching Scheme	**Examination Scheme**	
Lectures: 3 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 3	**Total:**	**100 Marks**
Prerequisite Course: Computer Networks, Cryptography and Security		

Course Objectives

1. To learn the basics of wireless technologies and security.
2. To understand the confidentiality, integrity and availability in mobile phones.
3. To introduce the fundamental concepts of mobile phone forensics.
4. To study evidential potential of digital devices and its handling.
5. To learn the methods of investigation using digital forensic techniques.
6. To learn computer forensic tools and task performed by computer forensic tools.

Course Outcomes (COs):

After successful completion of the course, student will be able to

Course Outcome (s)		Bloom's Taxonomy	
		Level	**Descriptor**
CO1	**State** the fundamental concepts of wireless technologies and security.	1	Remember
CO2	**Explain** the confidentiality, integrity and availability in mobile phones.	2	Understand
CO3	**Understand** the basic concepts of mobile phone forensics.	2	Understand
CO4	**Understand** the evidential potential of digital devices and its handling.	2	Understand
CO5	**Remember** the methods of investigation using digital forensic techniques.	1	Remember
CO6	**Apply** digital forensic knowledge to use computer forensic tools.	3	Apply

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	
CO1	2	1	3	1	1		3	1	
CO2	2	1	3	1	1		3	2	
CO3	3	1	3	1	3		3	3	
CO4	3	1	3	1	3		3	3	
CO5	3	1	3	1	2		3	2	
CO6	3	1	3	1	2		3	2	

Course Contents			
Unit-I	**OVERVIEW OF WIRELESS TECHNOLOGIES AND SECURITY**	**No. of Hours**	**COs**
	Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-Fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.	06	CO1
Unit-II	**CIA TRIAD IN MOBILE PHONES**	**No. of Hours**	**COs**
	Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Net monitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues	06	CO2
Unit-III	**MOBILE PHONE FORENSICS**	**No. of Hours**	**COs**
	Crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques.	06	CO3
Unit-IV	**DIGITAL FORENSICS**	**No. of Hours**	**COs**
	Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contamination.	06	CO4
Unit-V	**DIGITAL FORENSICS EXAMINATION PRINCIPLES**	**No. of Hours**	**COs**
	Previewing, imaging, continuity, hashing and evidence locations- Seven element security model developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context.	06	CO5
Unit-VI	**COMPUTER FORENSICS TOOLS**	**No. of Hours**	**COs**
	Need and types of computer forensic tools, task performed by computer forensic tools. Study of open source Tools like SFIT, Autopsy etc. to acquire, search, analyze and store digital evidence.	06	CO6

Text Books:

1. Iosif I. Androulidakis, "Mobile phone security and forensics: A Practical Approach", Springer publications.
2. Angus M. Marshall, "Digital Forensics: Digital Evidence in Criminal Investigation", John – Wiley and Sons.

Reference Books:

1. Gregory Kipper, "Wireless Crime and Forensic Investigation", Auerbach Publications.
2. Andrew Hoog, "Android Forensics: Investigation, Analysis and Mobile Security for Google Android", Elsevier Publications.
3. Cory Altheide, Harlan Carvey "Digital Forensics with Open Source Tools" Syngress Publishing, Inc.
4. Nilakshi Jain, Dhananjay Kalbande, "Digital Forensic : The Fascinating World of Digital Evidences" Wiley India Pvt Ltd.

CS105: Lab Practice - I		
Teaching Scheme	**Examination Scheme**	
Lectures: 4 Hrs./Week	**Term Work:**	**NA**
	Oral:	**50 Marks**
	Practical:	**NA**
Credits: 2	**Total:**	**50 Marks**
Prerequisite Course:		

Guidelines
Faculty incharge will also suggest suitable licensed/open source tools to perform the assignments. Term work shall consist of preparation of a journal containing all assignments performed with objective, methodology, observations, results and conclusion.
Assignments
Faculty incharge shall suitably frame 12 Assignments based on the course Mathematical Foundation for Cyber Security.

CS106: Lab Practice - II		
Teaching Scheme	**Examination Scheme**	
Lectures: 4 Hrs./Week	**Term Work:**	**NA**
	Oral:	**50 Marks**
	Practical:	**NA**
Credits: 2	**Total:**	**50 Marks**
Prerequisite Course:		

Guidelines
Faculty incharge will also suggest suitable licensed/open source tools to perform the assignments. Term work shall consist of preparation of a journal containing all assignments performed with objective, methodology, observations, results and conclusion.
Assignments
Faculty incharge shall suitably frame 12 Assignments based on the Professional Elective – I and II courses.

CS107: Research Methodology		
Teaching Scheme	**Examination Scheme**	
Lectures: 2 Hrs./Week	**Continuous Assessment:**	**50 Marks**
	In-Sem Exam:	**NA**
	End-Sem Exam:	**NA**
Credits: 2	**Total:**	**50 Marks**
Prerequisite Course:		

Course Objectives

1. To learn basic concepts of research and its methodologies.
2. To learn the methodology to conduct the Literature Survey, ethics in research, academic integrity and plagiarism.
3. To acquaint with the tools, techniques, and processes of doing research.
4. To learn techniques to find outcome of Research.
5. To acquire skill of writing the research paper, Report and thesis.
6. To know methods of presenting research work over various platform.

Course Outcomes (COs):

After successful completion of the course, student will be able to

Course Outcome (s)		Bloom's Taxonomy	
		Level	Descriptor
CO1	**Understand** research problem formulation.	**2**	**Understand**
CO2	**Analyze** research related information.	**4**	**Analyze**
CO3	**Follow** research ethics.	**3**	**Apply**
CO4	**Understand** that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.	**2**	**Understand**
CO5	**Understand** that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.	**2**	**Understand**
CO6	**Understand** that research presentation skill and IPR protection in R & D Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.	**2**	**Understand**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5		PSO1	PSO2	PSO3
CO1	3	2	1	2	-		-	3	
CO2	3	2	1	2	-		-	3	
CO3	3	2	1	2	-		-	3	
CO4	3	2	1	2	-		-	3	
CO5	3	2	1	2	-		-	3	
CO6	3	2	1	2	-		-	3	

Course Contents			
Unit-I	**RESEARCH PROBLEM**	**No. of Hours**	**COs**
	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.	02	CO1
Unit-II	**EFFECTIVE LITERATURE STUDIES**	**No. of Hours**	**COs**
	Effective literature studies approaches, analysis Plagiarism, Research ethics.	02	CO2
Unit-III	**EFFECTIVE TECHNICAL WRITING**	**No. of Hours**	**COs**
	Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee.	02	CO3
Unit-IV	**NATURE OF INTELLECTUAL PROPERTY**	**No. of Hours**	**COs**
	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.	02	CO4
Unit-V	**PATENT RIGHTS**	**No. of Hours**	**COs**
	Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications.	02	CO5
Unit-VI	**NEW DEVELOPMENTS IN IPR**	**No. of Hours**	**COs**
	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.	02	CO6

Text Books:

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students".
2. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction".
3. Ranjit Kumar, "Research Methodology: A Step by Step Guide for beginners", 2nd Edition.
4. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd , 2007.
5. Mayall, "Industrial Design", McGraw Hill, 1992.
6. Niebel , "Product Design", McGraw Hill, 1974.
7. Asimov, "Introduction to Design", Prentice Hall, 1962.
8. Robert P. Merges, Peter S. Menell, Mark A. Lemley, "Intellectual Property in New Technological Age", 2016.
9. T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008.