NEW HORIZON COLLEGE OF ENGINEERING

Autonomous College Permanently Affiliated to VTU, Approved by AICTE & UGC
Accredited by NAAC with 'A' Grade, Accredited by NBA

The Trust is a Recipient of Prestigious Rajyotsava State Award 2012 Conferred by the Government of Karnataka
Awarded Outstanding Technical Education Institute in Karnataka-2016
Ring Road, Bellandur Post, Near Marathalli, Bangalore -560 103, INDIA

Academic Year 2021-22

ISE – Information Science & Engineering

M.Tech in Cyber Forensics and Information Security

I and II Semesters

Scheme and Syllabus

CONTENTS

1. Vision, Mission and Program Educational Objectives (PEO) 1
2. Program Outcomes (PO) with Graduate Attributes 2
3. Mapping of POs with PEOs 3

SCHEME

4. Scheme of First Semester M. Tech 4
5. Scheme of Second Semester M. Tech 5
6. Scheme of Third Semester M. Tech 6
7. Scheme of Fourth Semester M. Tech 7

SYLLABUS

8. Syllabus of First Semester M.Tech: 8
   a) Ethical Hacking 9
   b) Number Theory and Cryptology 11
   c) Information Security and Computer Networking 14
   d) Cyber Crime and Cyber Forensics 16
   e)Research Methodology 18
   f)Access control and Identity Management System 21
   g) Cloud Security 23
   h) Advanced Cryptography 25
   i) Application and Web Security 27
   j) Ethical Hacking lab 30
   k) Number Theory and Cryptology lab 32
   l) Mini Project 34

9. Syllabus of Second Semester M.Tech: 35
   a) Preserving and Recovering Digital Evidence 36
   b) Operating System Security 38
   c) Secured Programming 40
   d) Cyber Laws and Ethics 42
   e) Biometric Security 45
   f) Trust Management in E-Commerce 47
   g) Information Security Policies in Industry 49
   h) Database Security 51
   i) Seminar 54
   j)Mini Project 54

Appendix A Outcome Based Education 55
Appendix B Graduate Parameters as defined by National Board of Accreditation 56
Appendix C Bloom's Taxonomy 57

VISION

To evolve as a centre of academic excellence and advanced research in information science and engineering discipline and to endeavour the computational competence of students for their dream career achievement and enhancing the managerial and technical skills.

MISSION

To inculcate students with profound understanding of fundamentals related to discipline, attitudes, skills and their application in solving real world problems, with an inclination towards societal issues and research.

Program Education objectives (PEOs)

PEO1	To excel in their professional career with expertise in providing solutions to Information Technology problems.
PEO2	To pursue higher studies with profound knowledge enriched with academia and industrial skill sets.
PEO3	To exhibit adaptive and agile skills in the core area of Information Science & Engineering to meet the technical and managerial challenges.
PEO4	To demonstrate interpersonal skills, professional ethics to work in a team to make a positive impact on society.

PEO to Mission Statement Mapping

Mission Statements	PEO1	PEO2	PEO3	PEO4
To prepare the students with academic and industry exposure by empowering and equipping them with necessary domain knowledge.	3	2	2	2
To prepare the students for global career in information technology with relevant technical and soft skills.	3	2	2	2
To encourage students to participate in co-curricular and extracurricular activities leading to the enhancement of their social and professional skills.	2	2	3	3

Correlation: 3- High, 2-Medium, 1-Low

Program Specific Outcomes (PSO's)

PSO1: The ability to understand, analyze and develop computer programs in the areas related to algorithms, system software, multimedia, web design, big data analytics and networking or efficient design of computer based systems of varying complexity.

PSO2: The ability to apply standard practices and strategies in software project development using innovative ideas and open ended programming environment with skills in teams and professional ethics to deliver a quality product for business success.

Program Outcomes (PO) with Graduate Attributes

	Graduate Attributes	Program Outcomes (POs)
1	Engineering Knowledge	PO1: The basic knowledge of Mathematics, Science and Engineering.
2	Problem analysis	PO2: An Ability to analyse, formulate and solve engineering problems.
3	Design and Development of Solutions	PO3: An Ability to design system, component or product and develop interfaces among subsystems of computing.
4	Investigation of Problem	PO4: An Ability to identify, formulate and analyze complex engineering problem and research literature through core subjects of Computer Science.
5	Modern Tool usage	PO5: An Ability to use modern engineering tools and equipments for computing practice.
6	Engineer and society	PO6: An Ability to assess societal, health, cultural, safety and legal issues in context of professional practice in Computer Science & Engineering.
7	Environment and sustainability	PO7: The broad education to understand the impact of engineering solution in a global, economic, environmental and societal context.
8	Ethics	PO8: An understanding of professional and ethical responsibility.
9	Individual & team work	PO9: An Ability to work both as individual and team player in achieving a common goal.
10	Communication	PO10: To communicate effectively both in written and oral formats with wide range of audiences.
11	Lifelong learning	PO11: Knowledge of contemporary issues, Management and Finance.
12	Project management and finance	PO12: An Ability to recognize the need and thereby to engage in independent and life-long learning for continued professional and career advancement.

Mapping of POs with PEOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
PEO1	3	3	3	2	3	-	-	2	3	1	3	1
PEO2	3	3	3	2	3	-	-	2	3	1	3	1
PEO3	3	3	3	2	3	-	-	2	3	1	3	1
PEO4	3	3	3	2	3	-	-	2	3	1	3	1

Correlation: 3- High, 2-Medium, 1-Low

New Horizon College of Engineering
Department of Information Science and Engineering
First Semester M. Tech Program–Scheme AY: 2019-20

Sl. No	Course Code	Course	BOS	Credit Distribution			Overall Credits	Contact Hours	Marks		
				L	T	P			CIE	SEE	TOTAL
1	19SFC11	Ethical Hacking	ISE	3	0	0	3	3	50	50	100
2	19SFC12	Number Theory and Cryptology	ISE	3	0	0	3	3	50	50	100
3	19SFC13	Information Security and Computer Networking	ISE	3	0	0	3	3	50	50	100
4	19SFC14	Cyber Crime and Cyber Forensics	ISE	3	0	0	3	3	50	50	100
5	19SFC15	Research Methodology	ISE	2	0	0	2	2	25	25	50
6	19SFC16X	Professional Elective-1	ISE	4	0	0	4	4	50	50	100
7	19SFCL17	Ethical Hacking lab	ISE	0	0	2	2	4	25	25	50
8	19SFCL18	Number Theory and Cryptology lab	ISE	0	0	2	2	4	25	25	50
9	19SFC19	Mini Project	ISE	-	-	-	3	0	50	50	100
	TOTAL						**25**	**26**	**375**	**375**	**750**

Professional Elective – 1	
Course Code	**Course Name**
19SFC161	Access control and Identity Management System
19SFC162	Cloud Security
19SFC163	Advanced Cryptography
19SFC164	Application and Web Security

New Horizon College of Engineering
Department of Information Science and Engineering
Second Semester M. Tech Program-Scheme AY: 2019-20

Sl.No	Course Code	Course	BOS	Credit Distribution			Overall Credits	Contact Hours	Marks		
				L	T	P			CIE	SEE	TOTAL
1	19SFC21	Preserving and Recovering Digital Evidence	ISE	4	0	0	4	4	50	50	100
2	19SFC22	Operating System Security	ISE	4	0	0	4	4	50	50	100
3	19SFC23	Secured Programming	ISE	4	0	0	4	4	50	50	100
4	19SFC24	Cyber Laws and Ethics	ISE	4	0	0	4	4	50	50	100
5	19SFC25X	Professional Elective-2	ISE	4	0	0	4	4	50	50	100
6	19SFC26	Technical Seminar	ISE	-	-	-	2	0	25	25	50
6	19SFC27	Mini Project	ISE	-	-	-	3	0	50	50	100
TOTAL							**25**	**20**	**325**	**325**	**650**

Professional Elective – 2	
Course Code	**Course Name**
19SFC251	Biometric Security
19SFC252	Trust Management in E-Commerce
19SFC253	Information Security Policies in Industry
19SFC254	Database Security

FIRST SEMESTER

(SYLLABUS)

ETHICAL HACKING

Course Code :19SFC11 **Credits : 03**
L:T:P :3:0:0 **CIE Marks : 50**
Exam Hours : 03 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to do the following:

CO1	Learn aspects of security, importance of data gathering, foot printing and system hacking.
CO2	Summarize tools and techniques to carry out a penetration testing.
CO3	Interpretation of intruders escalating privileges.
CO4	Describe Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
CO5	Compare different types of hacking tools.
CO6	Apply the techniques for real world problems in the domain

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	2	2	3	-	3	1	1	2	2
CO2	3	3	3	2	2	3	-	3	1	1	2	2
CO3	3	3	3	2	2	3	-	3	1	1	2	2
CO4	3	3	3	2	2	3	-	3	1	1	2	2
CO5	3	3	3	2	2	3	-	3	1	1	2	2
CO6	3	3	3	2	2	3		3	1	1	2	2

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Casing the Establishment: What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating	9	CO1

	Common Network services. Case study: Network Security Monitoring.		
2	Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access, After hacking root.	9	CO2
3	Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, Brute-Force Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media.	9	CO3
4	Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of Dos Attackers, Types of DoS attacks, Generic Dos Attacks, UNIX and Windows DoS.	9	CO4
5	Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.	9	CO5, CO6

TEXT BOOKS:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata McGraw Hill Publishers, 2010.

2. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall of India, 2010.

REFERENCE BOOKS:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, 5th Edition, Tata McGraw Hill Publishers, 2010.

2. RafayBaloch, “A Beginners Guide to Ethical Hacking”.

3. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, “Gray Hat Hacking The Ethical Hackers Handbook”, 3rd Edition, McGraw-Hill Osborne Media paperback(January 27, 2011)

Assessment Pattern:

CIE- Continuous Internal Evaluation (50 Marks).

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	5	-	-
Understand	5	5	-
Apply	5	5	10
Analyze	5	5	-
Evaluate	5	-	-
Create	-	-	-

SEE- Semester End Examination (50Marks).

Bloom's Category	Questions (50 Marks)
Remember	10
Understand	10
Apply	10
Analyze	10
Evaluate	10
Create	-

NUMBER THEORY AND CRYPTOLOGY

Course Code :19SFC12 **Credits : 03**
L:T:P:3:0:0 **CIE Marks :50**
Exam Hours : 3 **SEE marks :50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Understand the significance of cryptography to the modern world and the internet.
CO2	Understand the rationale behind block cipher design.
CO3	Perform the cryptanalysis of a simple block cipher.
CO4	Integrate cryptographic algorithms into software projects.
CO5	Solve elementary problems in number theory relating to cryptography.
CO6	Build on number theoretic basics to further their knowledge of advanced methods of cryptography

Mapping of Course Outcomes to Program Outcomes

CO/ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	2	-	1	2	1	3	2	1	2
CO2	3	3	3	2	-	1	2	1	3	2	1	2
CO3	3	3	3	2	-	1	2	1	3	2	1	2
CO4	3	3	3	2	-	1	2	1	3	2	1	2
CO5	3	3	3	2	-	1	2	1	3	2	1	2
CO6	3	3	3	2	-	1	2	1	3	2	1	2

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

CO/ PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	2
CO6	3	2

Module No	Module Contents	Hours	CO's
1	Methods Elementary Number Theory: Finite fields, Modular arithmetic, Efficient algorithms for modular arithmetic, Fermat's little theorem, Euler's criteria, Euler's totient function	9	CO1
2	Advanced Number Theory:Primality testing, prime factorization, The Chinese remainder theorem, Quadratic residues and calculating modular square roots and cube roots, The Jacobi symbol	9	CO2
3	Basic Cryptography Concepts- Basic Cryptography Concepts: Symmetric Encryption Algorithms, Purpose of Cryptography, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES). Classical methods: Caesar cipher, Vigenere cipher, The one-time pad, Mechanical rotor systems	9	CO3
4	Modern ciphers: Block ciphers and their applications, Structure of a block cipher, The Fiestel structure, Key and block size length, The Data Encryption Standard (DES), The Advanced Encryption Standard (AES)	9	CO4

5	Hash Functions: One-way hash functions and their applications, SHA-1 and its successors. Cryptanalysis: Linear cryptanalysis, Differential cryptanalysis, Meet-in-the-middle attacks. Key Distribution: The key distribution problem, The Diffie-Hellman method, RSA and relatedmethods	9	CO5, CO6

TEXT BOOKS:

1. A Course in Number Theory and Cryptography, Â Neal Koblitz, (Springer 2006)
2. An Introduction to Mathematical Cryptography, Jill Pipher, Jeffrey Hoffstein, Joseph H. Silverman (Springer, 2008)
3. An Introduction to theory of numbers, Niven, Zuckerman and Montgomery, (Wiley 2006)
4. Elliptic curves: number theory and cryptography, Lawrence C. Washington, (Chapman & Hall/CRC 2003)

REFERENCE BOOKS:

1. An Introduction to Cryptography, R.A. Mollin (Chapman & Hall, 2001)
2. Rational Points on Elliptic Curves, Silverman and Tate (Springer 2005)
3. Guide to elliptic curve cryptography Hankerson, Menezes, Vanstone (Springer, 2004)
4. Elementary Number Theory, Jones and Jones (Springer, 1998)

CIE- Continuous Internal Evaluation: Theory (50 Marks)

Bloom's Category (Marks out of 50)	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (15 Marks)
Remember	5	-	-
Understand	5	-	-
Apply	10	10	5
Analyze	5	5	5
Evaluate	5	-	-
Create	-	-	-

SEE- Semester End Examination: Theory (50Marks)

Bloom's Category Marks (out of 50)	Marks
Remember	10
Understand	10
Apply	20
Analyze	5
Evaluate	5
Create	-

INFORMATION SECURITY AND COMPUTER NETWORKING

Course Code : 19SFC13 **Credits : 03**
L:T:P : 3:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Understand the fundamentals of Cryptography.
CO2	Acquire knowledge on cryptographic tools used to provide confidentiality, integrity and authenticity.
CO3	Differentiate the various user authentication methods, access control schemes and authentication applications.
CO4	Acquire the knowledge on IP Security tools.
CO5	Acquire the knowledge about malicious software.
CO6	Apply Information security to real world cases

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	2	1	2	1	2	2	1	2	2
CO2	3	3	3	2	1	2	1	2	2	1	2	2
CO3	3	3	3	2	1	2	1	2	2	1	2	2
CO4	3	3	3	2	1	2	1	2	2	1	2	2
CO5	3	3	3	2	1	2	1	2	2	1	2	2
CO6	3	3	3	2	1	2	1	2	2	1	2	2

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Overview: Computer Security Concepts, Requirements, Architecture, Trends, Strategy Perimeter Security: Firewalls, Intrusion Detection, Intrusion Prevention systems, Honeypots Case Study: Readings, Intrusion and intrusion detection by John McHugh.	9	CO1
2	User Authentication: Password, Password-based, token based, Biometric, Remote User authentication. Access Control: Principles, Access Rights, Discretionary Access Control, Unix File Access Control, Role Based Access Control Internet Authentication Applications: Kerberos, X.509, PKI, Federated Identity Management.	9	CO2, CO3
3	Cryptographic Tools: Confidentiality with symmetric encryption, Message Authentication & Hash Functions, Digital Signatures, Random Numbers. Symmetric Encryption and Message Confidentiality: DES, AES, Stream Ciphers, Cipher Block Modes of Operation, Key Distribution.	9	CO3, CO4
4	Internet Security Protocols: SSL, TLS, IPSEC, S/ MIME. Public Key Cryptography and Message Authentication: Secure Hash Functions, HMAC, RSA, Diffie Hellman Algorithms Case Study: Readings, Programming Satan's Computer Ross Anderson and Roger Needham.	9	CO5
5	Malicious Software: Types of Malware, Viruses & Counter Measures, Worms, Bots, Rootkits Software Security: Buffer Overflows, Stack overflows, Defense, Other overflow attacks Case Study.	9	CO6

TEXT BOOKS:

1. Computer Security: Principles and Practice, William Stalling &Lawrie Brown, 2008, Indian Edition 2010, Pearson.

REFERENCE BOOKS:

1. Readings: Smashing The Stack For Fun And Profit, Aleph One
http:// www.phrack.com/issues.html ? issue = 49&id=14#article

2. Chuck Easttom, " Computer Security Fundamentals" Pearson, 2012.

CIE - Continuous Internal Evaluation (50 Marks)

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	-	-	-
Understand	5	5	5
Apply	5	5	5
Analyze	5	-	-
Evaluate	5	5	-
Create	5	-	-

SEE – Semester End Examination (50 Marks)

Bloom's Taxonomy	Marks
Remember	10
Understand	10
Apply	10
Analyze	10
Evaluate	5
Create	5

CYBER CRIME AND CYBER FORENSICS

Course Code : 19SFC14 **Credits : 03**
L: T: P : 3:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Understand the fundamentals of Cyber Crime
CO2	Analyze the nature and effect of cybercrime in society.
CO3	Demonstrate Accounting Forensics.
CO4	Analyze Computer Crime and Criminals and Liturgical Procedures.
CO5	Apply the laws and regulations to the applications
CO6	Analyze the email tracking cyber applications

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	-	1	2	-	-	-	-	-	-	1
CO2	3	1	2	1	-	-	-	-	-	-	-	2
CO3	2	3	2	2	1	1	-	-	-	-	1	3
CO4	3	3	3	1	1	-	-	-	-	-	-	3
CO5	3	1	2	1	2	-	1	-	-	-	-	3
CO6	3	3	2	3	1	-	-	1	-	-	2	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime, Social Engineering, Categories of Cyber Crime, Property Cyber Crime.	9	CO1, CO2
2	Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.	9	CO6
3	Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.	9	CO4
4	Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies, Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.	9	CO2, CO3
5	Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.	9	CO5

TEXT BOOKS:

1. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004. "Understanding Forensics in IT ", NIIT Ltd, 2005.
2. Nelson Phillips and EnfingerSteuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.

REFERENCE BOOKS:

1. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics ",Tata McGraw -Hill, New Delhi, 2006.
2. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.

CIE- Continuous Internal Evaluation (50 Marks)

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	5	-	-
Understand	10	-	5
Apply	10	10	5
Analyze	-	5	-
Evaluate	-	--	-
Create	-	-	-

SEE- Semester End Examination (50 Marks)

Bloom's Category	Tests
Remember	10
Understand	20
Apply	20
Analyze	-
Evaluate	-
Create	-

RESEARCH METHODOLOGY

Course Code: 19SFC15 **Credits: 02**
L: T: P: 2:0:0 **CIE Marks: 25**
Exam Hours: 03 **SEE Marks: 25**

COURSE OUTCOMES: at the end of the course, the students will be able to:

CO1	Understand the significance and suitability of research for various engineering applications.
CO2	Analyze the various processing techniques of research.
CO3	Understand the research in the development of engineering materials/process.
CO4	Analyze the properties/process of research through various techniques. Understanding that when IPR would take such important place in growth of
CO5	Evaluate the influence of design, analysis and testing of research.
CO6	Knowledge of Report writing

Mapping of Course outcomes to Program outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	1	1	1	1	1	1	1	2
CO2	3	2	2	2	1	1	1	1	1	1	1	2
CO3	2	2	2	2	3	1	1	1	1	1	1	2
CO4	2	2	2	2	3	1	1	1	1	1	1	2
CO5	2	2	3	2	1	3	1	1	1	1	1	2
CO6	3	3	2	2	2	1	1	1	1	1	1	1

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	1
CO4	3	2
CO5	3	1
CO6	3	2

Ratings: 3 for high, 2 for substantial, 1 for low.

Module No	Contents of Module	Hrs	Cos
1	**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	**7**	**CO1,CO2**
2	**Research Design**: Concept and Importance in Research – Features of a good research design, Exploratory Research Design, concept, types and uses, Descriptive Research Designs, concept, types and uses. Experimental Design: Concept of Independent & Dependent variables. **Qualitative and Quantitative Research**: Qualitative research, Quantitative research, Concept of measurement, causality, generalization, and replication. Merging the two approaches.	**7**	**CO2**
3	**Measurement**: Concept of measurement, Problems in measurement in research, Validity and Reliability. Levels of measurement – Nominal, Ordinal, Interval, Ratio.	**7**	**CO3**

	Sampling: Concepts of Statistical Population, Sample, Sampling Frame, Sampling Error, Sample Size, Non Response. Characteristics of a good sample. Probability Sample – Simple Random Sample, Systematic Sample, Stratified Random Sample & Multi-stage sampling. Determining size of the sample – Practical considerations in sampling and sample size.		
4	**Interpretation of Data and Paper Writing** – Layout of a Research Paper, Journals in Computer Science, Impact factor of Journals, When and where to publish ? Ethical issues related to publishing, Plagiarism and Self-Plagiarism. **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.	**7**	**CO4**
5	**References**: Encyclopedias, Research Guides, Handbook etc., Academic Databases for Computer Science Discipline. **Use of tools / techniques for Research**: methods to search required information effectively, Reference Management Software like Zotero/Mendeley, Software for paper formatting like LaTeX/MS Office, Software for detection of Plagiarism	**7**	**CO5,CO6**

Textbooks:

1. Garg, B.L., Karadia, R., Agarwal, F. and Agarwal, U.K., 2002. An introduction to Research Methodology, RBSA Publishers.
2. Kothari, C.R., 1990. Research Methodology: Methods and Techniques. 2016, w Age International.Fourth edition, ISBN-13: 978-9386649225

Reference Books:

1. Garg, B.L., Karadia, R., Agarwal, F. and Agarwal, U.K., 2002. An introduction to Research Methodology, RBSA Publishers.
2. Kothari, C.R., 1990. Research Methodology: Methods and Techniques. 2016, w Age International.Fourth edition, ISBN-13: 978-9386649225
3. Anderson, T. W., An Introduction to Multivariate Statistical Analysis, 2009, Wiley Eastern Pvt., Ltd., New Delhi, Wiley; Third edition, BN-13: 978-8126524488

4 Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction", Juta Academic; 2nd ed edition, 2001, ISBN-13: 978-0702156601
5 Robert P. Merges, Peter S. Menell, Mark A. Lemley, 2016, " Intellectual Property in New Technological Age", Clause 8 Publishing , ISBN-13: 978-1945555015

ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM

Course Code : 19SFC161 **Credits : 04**
L: T: P : 4:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Analyze to compute tasks with security contexts.
CO2	Categorize the identity management system into different classes.
CO3	Measure the different elements of Trust paradigms for various models.
CO4	Compare and contrast between Discretionary access model and Access Matrix Model.
CO5	Categorize all the active entities of a protection system.
CO6	Classify all the active entities of a protection system.

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	2	2	1	-	-	-	-	-	-	1
CO2	3	3	2	2	-	-	-	-	-	-	-	2
CO3	2	2	2	2	1	1	-	-	-	-	1	3
CO4	3	3	3	3	1	-	-	-	-	-	-	3
CO5	3	3	2	2	2	-	1	-	-	-	-	3
CO6	3	3	2	2	1	-	-	1	-	-	2	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	2	1
CO3	2	2
CO4	3	1
CO5	2	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Access control: Introduction, Attenuation of privileges, Trust and Assurance, Confinement problem, Security design principles, Identity Management models, local, Network, federal , global web identity, XNS approach for global Web identity, Centralized enterprise level Identity Management.	9	CO1, CO2
2	Elements of trust paradigms in computing, Third party	9	CO6

	approach to identity trust, Kerberos, Explicit third party authentication paradigm, PKI approach to trust establishment, Attribute certificates, Generalized web of trust models, Examples.		
3	Mandatory access control, comparing information flow in BLP and BIBA models, Combining the BLP and BIBA models, Chinese wall problem.	9	CO4
4	Discretionary access control and Access matrix model, definitions, Safety problem, The take grant protection model, Schematic protection model, SPM rules and operations, Attenuating, Applications	9	CO2, CO3
5	Role based access control, Hierarchical Access Control, Mapping of a mandatory policy to RABC, Mapping discretionary control to RBAC, RBAC flow analysis, Separation of Duty in RBAC, RBAC consistency properties, The privileges perspective of separation of duties, Functional specification for RBAC.	9	CO5

TEXT BOOKS:

1. Messoud Benantar, "Access Control Systems: Security, Identity
2. Management and Trust Models", Springer, 2009.

REFERENCE BOOKS:

1. Elena Ferrari and M. Tamer A-zsu , "Access Control In Data Management
2. Systems", Morgan & Claypool Publishers, 2010.

CIE- Continuous Internal Evaluation (50 Marks)

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	5	-	-
Understand	5	-	5
Apply	10	10	5
Analyze	5	5	-
Evaluate	-	--	-
Create	-	-	-

SEE- Semester End Examination (50 Marks)

Bloom's Category	Tests
Remember	10
Understand	10
Apply	20
Analyze	10
Evaluate	-
Create	-

CLOUD SECURITY

Course Code : 19SFC162 | **Credits : 04**
L: T: P : 4:0:0 | **CIE Marks : 50**
Exam Hours : 3 | **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Demonstrate the growth of Cloud computing, architecture and different modules of implementation.
CO2	Evaluate the different types of cloud solutions among IaaS, PaaS, SaaS.
CO3	Access the security implementation flow, actions and responsibilities of stake holders.
CO4	Generalize the Data Centre operations, encryption methods and deployment details.
CO5	Provide recommendations for using and managing the customer's identity and choose the type of virtualization to be used.
CO6	Summarize the need of cloud compliance and existing cloud solutions.

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	2	2	2	2	1	1	1	1
CO2	3	2	2	2	2	2	2	2	1	1	1	2
CO3	2	2	2	2	2	2	2	2	1	1	1	3
CO4	3	2	2	2	2	2	2	2	1	1	1	3
CO5	3	2	2	2	2	2	2	2	1	1	1	3
CO6	3	2	2	2	2	2	2	2	1	1	1	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	3
CO2	2	1
CO3	2	1
CO4	3	1
CO5	2	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing,Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference	9	CO1

	Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.		
2	Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.	9	CO2
3	Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).	9	CO3
4	Data Center Operations: Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations.	9	CO4, CO5
5	Identity and Access Management: Identity and Access Management in the cloud, 8 Hours Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS , IDaaS Security Recommendations. Virtualization: Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.	9	CO6

TEXT BOOKS:

1.Tim Mather, Subra Kumaraswamy, Shahed Latif, “Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance”, Oreilly Media 2009.

REFERENCE BOOKS:

1.Vic (J.R.) Winkler, “Securing the Cloud, Cloud Computer Security Techniques and Tactics”, Syngress, April 2011.

CIE- Continuous Internal Evaluation (50 Marks)

Bloom’s Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)

Remember	5	-	-
Understand	5	-	5
Apply	10	10	5
Analyze	5	5	-
Evaluate	-	--	-
Create	-	-	-

SEE- Semester End Examination (50 Marks)

Bloom's Category	Tests
Remember	10
Understand	10
Apply	20
Analyze	10
Evaluate	-
Create	-

ADVANCED CRYPTOGRAPHY

Course Code : 19SFC163 **Credits : 04**
L: T: P : 4:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Describe the concepts of principles and practice of cryptography and network security.
CO2	Demonstrate Feistel cipher, Distribution of Public Keys, digital signatures and Authentication protocols.
CO3	Analyze the security of multiple encryption schemes and Triples DES.
CO4	Build secure authentication systems by use of message authentication techniques.
CO5	Summarize the concepts of principles and practice of visual cryptography.
CO6	Analyze the security of multiple encryption schemes and Triples DES.

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	3	3	1	1	2	1	1	1	1
CO2	3	3	3	3	3	1	1	2	1	1	1	2
CO3	3	3	3	3	3	1	1	2	1	1	1	3
CO4	3	3	3	3	3	1	1	2	1	1	1	3
CO5	3	3	3	3	3	1	1	2	1	1	1	3
CO6	3	3	3	3	3	1	1	2	1	1	1	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	3

CO2	2	1
CO3	2	2
CO4	3	2
CO5	2	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	OSI security architecture: Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality.	9	CO1
2	Key management: Diffie Hellman key exchange, Elliptic curve architecture and cryptography, Introduction to number theory, Confidentiality using symmetric encryption, Public key cryptography and RSA.	9	CO2
3	Authentication requirements: Authentication functions, Message authentication codes,Hash functions, Security of hash functions and MACS, MD5 Message Digest algorithm,Secure hash algorithm, Ripend, HMAC digital signatures, Authentication protocols.	9	CO3, CO4
4	Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle,polarization states of photons, quantum cryptography using polarized photons, local vs.non local interactions, entanglements, EPR paradox, Bell's theorem, Bell basis,teleportation of a single qubit theory and experiments.	9	CO5
5	Future trends: Review of recent experimental achievements, study on technological feasibility of a quantum computer candidate physical systems and limitations imposed by noise.	9	CO6

TEXT BOOKS:

1. William Stallings, "Cryptography and Network Security -Principles and Practices", 3rd Edition, Prentice Hall of India, 2003.
2. Atul Kahate, "Cryptography and Network Security", Tata McGraw -Hill, 2003.
3. William Stallings, "Network Security Essentials: Applications and Standards", Pearson Education Asia, 2000.

REFERENCE BOOKS:

1. R. P. Feynman, "Feynman lectures on computation", Penguin Books, 1996.
2. Gennady P. Berman, Gary D. Doolen, Ronnie Mainiri & Valdmis Itri Frinovich, "Introduction to quantum computers", World Scientific, Singapore, 1998.
3. Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography" Principles And Protocols",CRC Press.

CIE- Continuous Internal Evaluation (50 Marks)

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	5	-	-
Understand	5	-	5
Apply	10	10	5
Analyze	5	5	-
Evaluate	-	-	-
Create	-	-	-

SEE- Semester End Examination (50 Marks)

Bloom's Category	Tests
Remember	10
Understand	10
Apply	20
Analyze	10
Evaluate	-
Create	-

APPLICATION AND WEB SECURITY

Course Code : 19SFC164 **Credits : 04**
L: T: P : 4:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Achieve Knowledge of web application's vulnerability and malicious attacks.
CO2	Understand the basic web technologies used for web application development
CO3	Understands the basic concepts of Mapping the application.
CO4	Able to illustrate different attacking illustrations
CO5	Illustrate different attacking illustrations.
CO6	Analyze Basic concepts of Attacking Data Stores.

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	2	2	1	1	2	2	1	1	2	2
CO2	3	3	2	2	1	1	2	2	1	1	2	2
CO3	3	3	2	2	1	1	2	2	1	1	2	3
CO4	3	3	2	2	1	1	2	2	1	1	2	3
CO5	3	3	2	2	1	1	2	2	1	1	2	3
CO6	3	3	2	2	1	1	2	2	1	1	2	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	3

CO2	3	1
CO3	3	1
CO4	3	1
CO5	2	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Web Application (In) security: The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications , Web Application Security. Core Defense Mechanisms: Handling User Access Authentication, Session Management, Access Control, Handling User Input, Varieties of Input Approaches to Input Handling, Boundary Validation. Multistep Validation and Canonicalization: Handling Attackers, Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks.	9	C1
2	Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, Client-Side Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks.	9	CO2
3	Mapping the Application: Enumerating Content and Functionality, Web Spidering, User-Directed Spidering, Discovering Hidden Content, Application Pages Versus Functional Paths, Discovering Hidden Parameters, Analyzing the Application, Identifying Entry Points for User Input, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface.	9	CO3
4	Attacking Authentication: Authentication Technologies, Design Flaws in AuthenticationMechanisms, Bad Passwords, Brute-Forcible Login, Verbose Failure Messages, Vulnerable Transmission of Credentials, Password Change, Functionality, Forgotten Password Functionality, "Remember Me" Functionality, User Impersonation, Functionality Incomplete, Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords, Insecure Distribution of Credentials. Attacking Access Controls: Common Vulnerabilities, Completely Unprotected, Functionality Identifier-Based Functions, Multistage Functions, Static Files, Platform Misconfiguration, Insecure Access Control Methods.	9	CO4, CO5
5	Attacking Data Stores: Injecting into Interpreted Contexts,	9	CO6

	Bypassing a Login, Injecting into SQL, Exploiting a Basic Vulnerability Injecting into Different Statement Types,Finding SQL Injection Bugs, Fingerprinting the Database, The UNION Operator, Extracting Useful Data, Extracting Data with UNION, Bypassing Filters, Second-Order SQL Injection, Advanced Exploitation Beyond SQL Injection: Escalating the Database Attack, Using SQL Exploitation Tools, SQL Syntax and Error Reference, Preventing SQL Injection.		

TEXT BOOKS:

1. The Web Application Hacker's Handbook: Finding And Exploiting Security
2. Defydd Stuttard, Marcus Pinto Wiley Publishing, Second Edition.

REFERENCE BOOKS:

1. Professional Pen Testing for Web application, Andres Andreu, Wrox Press.
2. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, “Web Application Security” Springer; 1st Edition
3. Joel Scambray, Vincent Liu, Caleb Sima ,“Hacking exposed”, McGraw-Hill; 3rd Edition, (October, 2010).
4. OReilly Web Security Privacy and Commerce 2nd Edition 2011.
5. Software Security Theory Programming and Practice, Richard sinn, Cengage Learning.
6. Database Security and Auditing, Hassan, Cengage Learning.

CIE- Continuous Internal Evaluation (50 Marks)

Bloom’s Category	**Tests (25 Marks)**	**Assignments (15 Marks)**	**Quizzes (10 Marks)**
Remember	5	-	-
Understand	5	-	5
Apply	10	10	5
Analyze	5	5	-
Evaluate	-	--	-
Create	-	-	-

SEE- Semester End Examination (50 Marks)

Bloom’s Category	**Tests**
Remember	5
Understand	20
Apply	10

Analyze	5
Evaluate	10
Create	-

ETHICAL HACKING LABORATORY

Course Code :19SFCL17 **Credits : 02**
L:T:P :0:0:2 **CIE Marks : 25**
Exam Hours :03 **SEE Marks : 25**

Course Outcomes: At the end of the Course, the Student will be able to do the following:

CO1	Learn aspects of security, importance of data gathering, foot printing and system hacking.
CO2	Learn tools and techniques to carry out a penetration testing.
CO3	How intruders escalate privileges?
CO4	Explain Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
CO5	Compare different types of hacking tools.
CO6	Apply the techniques for real world problems in the domain

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	2	2	-	-	-	1	1	-	2
CO2	3	3	3	2	2	-	-	-	1	1	-	2
CO3	3	3	3	2	2	-	-	-	1	1	-	2
CO4	3	3	3	2	2	-	-	-	1	1	-	2
CO5	3	3	3	2	2	-	-	-	1	1	-	2
CO6	3	3	3	2	2				1	1		2

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	2
CO6	3	2

Experiment No.	Experiment
1	Wireshark: Experiment to monitor live network capturing packets and

	analyzing over the live network.
2	LOIC: DoS attack using LOIC.
3	FTK: Bit level forensic analysis of evidential image and reporting the same.
4	Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network. 4.
5	HTTrack: Website mirroring using Httrack and hosting on a local network.
6	XSS: Inject a client side script to a web application
7	Emailtrackerpro: Email analysis involving header check, tracing the route. Also perform a check on a spam mail and non-spam mail.

Note:
For SEE Examination:

- Student should demonstrate the one experiment from list mentioned above.
- Examination will be conducted for 50 marks and scaled down to 25 marks
- Marks Distribution : Procedure write-up – 20%
  Conduction – 60%
  Viva – Voce – 20%
- Change of the experiment is allowed only once and procedure write-up marks will be considered as '0'

TEXT BOOKS:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata McGraw Hill Publishers, 2010.
2. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall of India, 2010.

REFERENCE BOOKS:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, "Hacking Exposed Network Security Secrets & Solutions", 5th Edition, Tata McGraw Hill Publishers, 2010.
2. RafayBaloch, "A Beginners Guide to Ethical Hacking".
3. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, "Gray Hat Hacking The Ethical Hackers Handbook", 3rd Edition, McGraw-Hill Osborne Media Paperback (January 27, 2011)

Assessment Pattern:

CIE- Continuous Internal Evaluation (25 Marks).

Bloom's Category	**Tests (25 Marks)**
Remember	-
Understand	5
Apply	15

Analyze	5
Evaluate	-
Create	-

SEE- Semester End Examination (25 Marks).

Bloom's Category	Questions (25 Marks)
Remember	-
Understand	5
Apply	15
Analyze	5
Evaluate	-
Create	-

NUMBER THEORY AND CRYPTOLOGY LAB

Course Code :19SFCL18 **Credits : 02**
L:T:P :0:0:2 **CIE Marks : 25**
Exam Hours : 03 **SEE Marks : 25**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Understand the significance of cryptography to the modern world and the internet.
CO2	Understand the rationale behind block cipher design.
CO3	Perform the cryptanalysis of a simple block cipher.
CO4	Integrate cryptographic algorithms into software projects.
CO5	Solve elementary problems in number theory relating to cryptography.
CO6	Build on number theoretic basics to further their knowledge of advanced methods of cryptography

Mapping of Course Outcomes to Program Outcomes

CO/ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	2	-	1	2	1	3	2	1	2
CO2	3	3	3	2	-	1	2	1	3	2	1	2
CO3	3	3	3	2	-	1	2	1	3	2	1	2
CO4	3	3	3	2	-	1	2	1	3	2	1	2
CO5	3	3	3	2	-	1	2	1	3	2	1	2

CO6	3	3	3	2	-	1	2	1	3	2	1	2

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

CO/ PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	2
CO6	3	2

Experiment No.	Experiment
1	Implement the Chinese Remainder Theorem in Java
2	Implement Fermat Primality Test Algorithm in Java.
3	Write a Java program to perform encryption and decryption using the following algorithms: a) Ceaser Cipher b) Substitution Cipher c) Hill Cipher
4	Write a Java program to implement the DES algorithm logic
5	Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).
6	Write a Java program to implement RSA Algoithm
7	Calculate the message digest of a text using the SHA-1 algorithm in JAVA.

Note:

For SEE Examination:

- Student should demonstrate the one experiment from list mentioned above.
- Examination will be conducted for 50 marks and scaled down to 25 marks
- Marks Distribution : Procedure write-up – 20%
  Conduction – 60%
  Viva – Voce – 20%
- Change of the experiment is allowed only once and procedure write-up marks will be considered as ‘0’

TEXT BOOKS:

1. A Course in Number Theory and Cryptography, Â Neal Koblitz, (Springer 2006)
2. An Introduction to Mathematical Cryptography, Jill Pipher, Jeffrey Hoffstein, Joseph H. Silverman (Springer, 2008)
3. An Introduction to theory of numbers, Niven, Zuckerman and Montgomery, (Wiley 2006)

4. Elliptic curves: number theory and cryptography, Lawrence C. Washington, (Chapman & Hall/CRC 2003)

REFERENCE BOOKS:

1. An Introduction to Cryptography, R.A. Mollin (Chapman & Hall, 2001)
2. Rational Points on Elliptic Curves, Silverman and Tate (Springer 2005)
3. Guide to elliptic curve cryptography Hankerson, Menezes, Vanstone (Springer, 2004)
4. Elementary Number Theory, Jones and Jones (Springer, 1998)

Assessment Pattern:

CIE- Continuous Internal Evaluation (25 Marks).

Bloom's Category	Tests (25 Marks)
Remember	-
Understand	5
Apply	10
Analyze	5
Evaluate	5
Create	-

SEE- Semester End Examination (25 Marks).

Bloom's Category	Questions (25 Marks)
Remember	-
Understand	5
Apply	15
Analyze	5
Evaluate	-
Create	-

MINI PROJECT

Course Code :19SFC19 **Credits : 03**
L:T:P :0:0:3 **CIE Marks : 50**
Exam Hours : 03 **SEE Marks : 50**

The student will carry out a mini project relevant to the course. The project must be development of an application (Hardware/Software). It is preferable if the project is based on mobile application development.

Conduction of Practical Examination:

The student shall prepare the report by including:

1. Define project (Problem Definition)
2. Prepare requirements document
3. Statement of work

4. Functional requirements
5. Software / Hardware requirements
6. Develop use cases
7. Research, analyze and evaluate existing learning materials on the application
8. Develop user interface and implement code
9. Prepare for final demo

SECOND SEMESTER

(SYLLABUS)

PRESERVING AND RECOVERING DIGITAL EVIDENCE

Course Code: 19SFC21 **Credits: 04**
L: T: P: 4:0:0 **CIE Marks: 50**
Exam Hours : 03 **SEE Marks: 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Summarize Digital evidence and computer crime and Laws
CO2	Illustrate the Computer basics for digital investigators w.r.t Unix and Macintosh systems
CO3	Illustrate the Networks basics for digital investigators
CO4	Investigate computer intrusions and cyber stalking
CO5	Interpret the basic concepts how to Handling the digital crime scene, digital evidence examination guidelines
CO6	Analyze the Digital evidence in real time applications

Mapping of Course Outcomes to Program Outcomes:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	2	3	1	2	1	2	1	3	2	2
CO2	3	3	2	3	1	2	1	2	1	3	2	2
CO3	3	3	2	3	1	2	1	2	1	3	2	2
CO4	3	3	2	3	1	2	1	2	1	3	2	2
CO5	3	3	2	3	1	2	1	2	1	3	2	2
CO6	3	3	2	3	1	2	1	2	1	3	2	2

Course Syllabus

Module No.	Contents of the Module	Hours	COs
1	Digital evidence and computer crime: history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room.	9	CO1
2	Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems, forensic xamination of Unix systems, forensic examination of Macintosh systems, and forensic examination of handheld devices.	9	CO2
3	Networks basics for digital investigators: applying forensic science to networks, digital evidence on physical and datalink layers, digital idence on network and transport layers, digital evidence on the internet .	9	CO3, CO4
4	Investigating computer intrusions, investigating cyber stalking, digital evidence as alibi.	9	CO5
5	Handling the digital crime scene, digital evidence examination guidelines.	9	CO6

TEXT BOOKS:

1. Digital Evidence and Computer Crime Forensic science, Computers and Internet - Eoghan Case Elsevier Academic Press, Second Edition.

REFERENCE BOOKS:

1. A Electronic Discovery and Digital Evidence in a Nut Shell-Shira A scheindlin, Daniel J Capra The Sedona Conference, Academic Press, Third Edition (No where available).
2. Digital Forensic for Network, Internet, and Cloud Computing A forensic evidence guide for moving Targets and Data' – Terrence V.Lillard, Glint P.Garrison, Craig A..Schiller, James SteeSyngress.
3. The Best Damn Cybercrime and Digital Forensics Book Period' [Paperback] Jack Wiles , Anthony Reyes , Jesse Varsalone, Syngress Edition, 2007.

Assessment Pattern:

CIE- Continuous Internal Evaluation (50 Marks).

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	5	-	-
Understand	5	5	-
Apply	5	5	10
Analyze	5	5	-
Evaluate	5	-	-
Create	-	-	-

SEE- Semester End Examination (50Marks).

Bloom's Category	Questions (50 Marks)
Remember	10
Understand	10
Apply	10
Analyze	10
Evaluate	10
Create	-

OPERATING SYSTEM SECURITY

Course Code : 19SFC22 **Credits: 04**
L: T: P : 4:0:0 **CIE Marks: 50**
Exam Hours : 3 **SEE Marks: 50**

Course Outcomes: At the end of the course the student will be able to:

CO1	Define fundamental concepts and mechanisms for enforcing security in OS.
CO2	Build a secure OS by exploring the early work in OS.
CO3	Illustrate formal security goals and variety of security models proposed for development of secure operating systems.
CO4	Describe architecture of various secure OS and retrofitting security feature on existing commercial OS's.
CO5	Analyze variety of approaches applied to the development & extension services for securing operating systems.
CO6	Develop the security systems for real time applications

Mapping of Course Outcomes with Program Outcomes

CO/ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	3	2	2	1	1	2	1	1	1	1
CO2	3	2	3	2	2	1	1	2	1	1	1	1
CO3	3	2	3	2	2	1	1	2	1	1	1	1
CO4	3	2	3	2	2	1	1	2	1	1	1	1
CO5	3	2	3	2	2	1	1	2	1	1	1	1
CO6	3	2	3	2	2	1	1	2	1	1	1	1

Mapping of Course Outcomes with Program Specific Outcomes

CO/ PSO	PSO1	PSO2
CO1	2	1
CO2	2	1
CO3	2	1
CO4	2	1
CO5	2	1
CO6	2	1

Module No.	Module Contents	Hours	CO's
1	Introduction: Secure OS, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system.	9	CO1
2	Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.	9	CO2

3	Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.	9	CO3
4	Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement.	9	CO4
5	Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration. Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.	9	CO5, CO6

TEXT BOOKS:

1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008

REFERENCES:

1. Michael Palmer, Guide to Operating system Security Thomson
2. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition
3. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont.

CIE - Continuous Internal Evaluation (50 Marks)

Bloom's Taxonomy	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	-	-	-
Understand	10	5	5
Apply	10	5	5
Analyze	5	5	-
Evaluate	-	-	-
Create	-	-	-

SEE – Semester End Examination (50 marks)

Bloom's Taxonomy	Tests
Remember	5
Understand	20
Apply	25
Analyze	-
Evaluate	-
Create	-

SECURED PROGRAMMING

Course Code :19SFC23 **Credits : 04**
L:P:T : 4:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	How to respond to security alerts which identifies software issues
CO2	Identify possible security programming errors
CO3	Define methodology for security testing and use appropriate tools in its implementation
CO4	Apply new security-enhanced programming models and tools
CO5	Analyze the security issues in applications using programming techniques
CO6	Identify the attacks on the applications and analyze the root cause

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	3	1	3	2	2	2	-	-	-	3
CO2	3	3	3	2	3	2	2	2	-	-	-	3
CO3	2	2	3	3	2	2	2	2	-	-	-	3
CO4	2	2	3	3	2	2	2	2	-	-	1	3
CO5	3	1	3	3	3	2	2	2	1	1	1	3
CO6	2	2	3	2	2	2	2	2	3	1	2	3

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

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	1
CO3	3	2
CO4	3	2
CO5	3	2
CO6	3	2

Module No.	Module Contents	Hours	COs
1	Validating all input & Designing secure programs: Command line and environment variables, File descriptors, names and contents, Web based application inputs, Locale selection and character encoding, Filtering represent able URIs, preventing cross site malicious input content, Forbidding HTTP Input to perform non-queries. Good	9	CO1

	security design principles: Securing the interface, separation of data and control. Minimize privileges: Granted, time, modules, resources etc, Using chroot, careful use of setuid/setgid, Safe default value and load initializations. Avoid race conditions		
2	Declarations and Initializations and Expressions: Declare objects with appropriate storage durations, Identifier declaration with conflict linkage classifications, Using correct syntax for declaring flexible array member, Avoiding information leakage in structure padding, Incompatible declarations of same function or object. Dependence on evaluation order for side effects: Reading uninitialized memory and dereferencing null pointers, Modifying objects with temporary lifetime, Accessing variable through (pointer) incompatible type, Modifying constant objects and comparing padding data.	9	CO2
3	Integers and Floating Points: Wrapping of unsigned integers, Integer conversions and misrepresented data, Integer overflow and divide by zero errors, Shifting of negative numbers, Using correct integer precisions, Pointer conversion to integer and vice versa. Floating point values for counters: Domain and range errors in math functions, Floating point conversions and preserving precision.	9	CO3
4	Arrays , Strings and Memory Management: Out of bounds subscripts and valid length arrays, Comparing array pointers, Pointer arithmetic for non-array object, scaled integer, Modifying string literals, Space allocation for strings (Null terminator), Casting large integers as unsigned chars, Narrow and wide character strings and functions. Accessing freed memory: Freeing dynamically allocated memory, Computing memory allocation for an object.	9	CO4
5	I/O, Signals and Error Handing: User input and format strings, Opening an pre-opened file, Performing device operations appropriate for files, Dealing with EOF, WEOF,Copying FILE object, Careful use of fgets, fgetws, getc, putc, putwc. Use of fsetops and fgetops, Accessing closed files.	9	CO5 , CO6

TEXT BOOKS

1. Robert C. Seacord, “The CERT ® C Coding Standard: 9 8 Rules for Developing Safe, Reliable, and Secure Systems, Second Edition”, Addi son Wesley Professional, April 2014

2. David Wheeler, “Secure Programming for Linux and Un ix HowTo”, Linux Documentation project, Aug 2004

REFERENCES:

1. JohnViega, Matt Messier, “Secure Programming Cookbo ok for C and C++”, O'Reilly Media, 1st Edition, July 2003.

CIE- Continuous Internal Evaluation (50Marks)

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	-	-	-
Understand	5	-	-
Apply	5	-	2.5
Analyze	5	-	2.5
Evaluate	5	5	-
Create	5	5	-

SEE- Semester End Examination (50 Marks)

Blooms Category	Tests
Remember	5
Understand	15
Apply	20
Analyze	5
Evaluate	5
Create	-

CYBER LAWS AND ETHICS

Course Code : 19SFC24 **Credits: 04**
L:P:T : 4:0:0 **CIE Marks: 50**
Exam Hours : 3 **SEE Marks: 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Describe the Indian legal system, ITA 2000/2008, cyber security and related legal issues.
CO2	Classify the Types of contract law, Digital signature , related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues, the types of cyber crimes and related legal issues
CO3	Interpret the cyber crime investigation and prosecution in depth
CO4	Apply the Cyber laws and to follow the ethics in the product development
CO5	Identify the Intellectual Property Rights for the concept developed
CO6	Analyze the cyber crime rate and effective measures to minimize it.

Mapping of Course Outcomes to Program Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	-	1	1	1	1	2	1	1

CO2	3	2	2	2	-	1	1	1	1	2	1	1
CO3	3	2	2	2	-	1	1	1	1	2	1	1
CO4	3	2	2	2	-	1	1	1	1	2	1	1
CO5	3	2	2	2	-	1	1	1	1	2	1	1
CO6	3	2	2	2	-	1	1	1	1	2	1	1

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

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	2
CO6	3	2

Module No	Module Contents	Hours	COs
1	Introduction to Cyber Law and Cyber Ethics: Introduction to Cyber Crimes and Ethical Issues in IT, Basic concepts of Law and Information Security, overview Of Information Security obligations under ITA 2008, Privacy and data protection concepts.	9	CO1
2	Law of Contracts applicable for Cyber Space transactions: introduction to Contract law, legal recognition of Electronic Documents, Authentication of Electronic Documents, Cyber space contracts, Resolution of Contractual disputes, stamping of Contractual document.	9	CO2
3	Intellectual Property Law for Cyber Space: Concept of Virtual assests, nature of Intellectual property, Trademarks and domain names, copyright law, law of patents.	9	CO3
4	Classification – civil, criminal cases. Essential elements of criminal law. Constitution and hierarchy of criminal courts. Criminal Procedure Code. Cognizable and non-cognizable offences. Bailable and non-bailable offences. Sentences which the court of Chief Judicial Magistrate may pass. Indian Evidence Act – Evidence and rules of relevancy in brief. Expert witness. Cross examination and re-examination of witnesses. Sections 32, 45, 46, 47, 57, 58, 60, 73, 135, 136, 137, 138, 141. Section 293 in the code of criminal procedure.	9	CO4

5	Miscellaneous Issues in Cyber Crimes and Cyber Security: Cyber Crime Investigation and Prosecution, Digital evidence and Cyber forensics, Jurisdiction issues, Information Security Management in corporate Sector.	9	CO5 CO6

TEXT BOOKS:

1. Cyber Laws for Engineers, Naavi, Ujvala Consultants Pvt Ltd, 2010.

REFERENCES:

1. Deborah G Johnson, Computer Ethics, Pearson Education Pub., ISBN : 81-7758-593-2.
2. Earnest A. Kallman, J.P Grillo, Ethical Decision making and Information Technology: An Introduction with Cases, McGraw Hill Pub.
3. John W. Rittinghouse, William M. Hancock, Cyber security Operations Handbook, Elsevier Pub.
4. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 2nd Edition, Cengage Learning Pub.
5. Randy Weaver, Dawn Weaver, Network Infrastructure Security, Cengage Learning Pub

CIE - Continuous Internal Evaluation (50 Marks)

Bloom's Taxonomy	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	5	-	-
Understand	5	-	-
Apply	10	10	10
Analyze	5	-	-
Evaluate	-	-	-
Create	-	5	-

SEE – Semester End Examination (50 marks)

Bloom's Taxonomy	Tests
Remember	5
Understand	10
Apply	15
Analyze	5
Evaluate	5
Create	10

BIOMETRIC SECURITY

Course Code : 19SFC251 **Credits : 04**
L: T: P : 4:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Illustrate the capability to select a suitable algorithm / system for a given application context
CO2	Illustrate of data privacy principles and the impact on the design and configuration of biometric systems.
CO3	Visualize traditional and biometric systems.
CO4	Analyze different algorithms of biometric systems.
CO5	Compare strengths and weaknesses of different biometric systems.
CO6	Design multimodal biometric systems.

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	2	2	2	1	1	-	-	-	1	1
CO2	3	3	2	2	2	1	1	-	-	-	1	2
CO3	3	2	2	2	2	1	1	-	-	-	2	3
CO4	3	3	2	3	2	1	1	-	-	-	1	3
CO5	3	3	2	2	2	1	1	-	-	-	1	1
CO6	3	3	2	2	2	1	1	1	-	-	2	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	3
CO2	2	1
CO3	2	1
CO4	2	1
CO5	1	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy in biometric systems.	9	CO1
2	Physiological Biometric Technologies: Fingerprints:	9	CO2,

	Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, weaknesses, deployment. Iris scan: Technical description, characteristics, strengths, weaknesses, deployment. Retina vascular pattern: Technical description, characteristics, strengths, weaknesses, deployment. Hand scan: Technical description, characteristics, strengths, weaknesses, deployment , DNA biometrics.		CO3
3	Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke Dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment.	9	CO4
4	Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.	9	CO5
5	Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.	9	CO6

TEXT BOOKS:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Biometrics –Identity verification in a networked World, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Eastern Publications, 2005.

REFERENCE BOOKS:

1. John Berger, Biometrics for Network Security, Prentice Hall, 2004.

CIE- Continuous Internal Evaluation (50 Marks)

Bloom's Category	**Tests (25 Marks)**	**Assignments (15 Marks)**	**Quizzes (10 Marks)**
Remember	5	-	-
Understand	5	-	5
Apply	10	10	5
Analyze	5	5	-
Evaluate	-	--	-
Create	-	-	-

SEE- Semester End Examination (50 Marks)

Bloom's Category	**Tests**
Remember	10

Understand	10
Apply	20
Analyze	10
Evaluate	-
Create	-

TRUST MANAGEMENT IN E-COMMERCE

Course Code : 19SF252 **Credits : 04**
L: T: P : 4:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Illustrate technologies & tools for E-Commerce with emphasis on Security
CO2	Identify best techniques & practices for different types of legacy & partner requirements
CO3	Analysis and explain the issues, risks and challenges in inter-organizational trust in E-Commerce
CO4	Describe the Trusted platforms for organizations and individuals
CO5	Illustrate the Key components and Trust mechanisms of trusted computing platform.
CO6	Describe the Trusted platforms for organizations and individuals

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	1	-	-	3	-	-	1	1
CO2	3	2	2	2	1	-	-	3	-	-	1	2
CO3	2	2	2	2	1	-	-	3	-	-	1	3
CO4	3	3	3	3	1	-	-	3	-	-	1	3
CO5	3	2	2	2	2	-	-	3	-	-	1	3
CO6	3	2	2	2	1	-	-	3	-	-	1	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	3
CO2	2	1
CO3	2	1
CO4	3	1
CO5	2	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Introduction to E-Commerce: Network and E-Commerce, Types of E-Commerce. Ecommerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models. Ecommerce	9	CO

	Payment systems: Types of payment system, Credit card E-Commerce transactions, B2C E-Commerce Digital payment systems, B2B payment system.		
2	Security and Encryption: E-Commerce Security Environment, Security threats in Ecommerce environment, Policies, Procedures and Laws.	9	CO2
3	Inter-organizational trust in E-Commerce: Need, Trading partner trust, Perceived benefits and risks of E-Commerce, Technology trust mechanism in E-Commerce, Perspectives of organizational, economic and political theories of inter-organizational trust, Conceptual model of inter-organizational trust in E-Commerce participation.	9	CO3
4	Introduction to trusted computing platform: Overview, Usage Scenarios, Key components of trusted platform, Trust mechanisms in a trusted platform.	9	CO4, CO5
5	Trusted platforms for organizations and individuals: Trust models and the E-Commerce domain.	9	CO6

TEXT BOOKS:

1. Kenneth C. Laudon and Carol Guercio Trave, Study Guide to E-Commerce Business Technology Society, Pearson Education, 2005.
2. Pauline Ratnasingam, Inter-Organizational Trust for Business-to-Business E-Commerce,IRM Press, 2005.

REFERENCE BOOKS:

1. Siani Pearson, et al, Trusted Computing Platforms: TCPA Technology in Context, Prentice Hall PTR, 2002.

CIE- Continuous Internal Evaluation (50 Marks)

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	5	-	-
Understand	5	-	5
Apply	10	10	5
Analyze	5	5	-
Evaluate	-	--	-
Create	-	-	-

SEE- Semester End Examination (50 Marks)

Bloom's Category	Tests
Remember	10

Understand	10
Apply	20
Analyze	10
Evaluate	-
Create	-

INFORMATION SECURITY POLICIES IN INDUSTRY

Course Code : 19SFC253 **Credits : 04**
L: T: P : 4:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Illustrate the differences between the organization's general information security policy and the needs and objectives of the various issue-specific and system-specific policies the organization will create.
CO2	Interpret organization institutionalizes its policies, standards, and practices using education, training and awareness programs.
CO3	Illustrate the threats to the stored data or data in transit and able to write policy document
CO4	Able to write policy document for securing network connection and interfaces.
CO5	Describe the content, need, and responsibilities of information security policies.
CO6	Become familiar with what viable information security architecture is, what it includes, and how it is used

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	1	-	-	2	-	-	1	1
CO2	3	2	2	2	1	-	-	2	-	-	1	2
CO3	2	2	2	2	1	1	-	2	-	-	1	3
CO4	3	3	3	3	1	-	-	2	-	-	1	3
CO5	3	2	2	2	2	-	1	2	-	-	1	3
CO6	3	2	2	2	1	-	-	2	-	-	1	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	3
CO2	2	1
CO3	2	1
CO4	3	1
CO5	2	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.	9	CO
2	Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goal Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in Organization, Business Objectives, Standards: International Standards.	9	CO2
3	Writing The Security Policies: Computer location and Facility construction,Contingency Planning, Periodic System and Network Configuration Audits,Authentication and Network Security, Addressing and Architecture, Access Control,Login Security, Passwords, User Interface, Telecommuting and Remote Access,Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies.	9	CO3
4	Establishing Type of Viruses Protection: Rules for handling Third Party Software,User Involvement with Viruses, Legal Issues, Managing Encryption and Encrypted data, Key Generation considerations and Management, Software Development policies, Processes Testing and Documentation, Revision control and Configuration management, Third Party Development, Intellectual Property Issues.	9	CO4, CO5
5	Maintaining the Policies: Writing the AUP, User Login Responsibilities,Organization's responsibilities and Disclosures, Compliance and Enforcement,Testing and Effectiveness of Policies, Publishing and Notification Requirements of the Policies, Monitoring, Controls and Remedies, Administrator Responsibility, Login Considerations,	9	CO6

	Reporting of security Problems, Policy Review Process, The Review Committee, Sample Corporate Policies, Sample Security Policies.		

TEXT BOOKS:

1. Scott Barman, Writing Information Security Policies, Sams Publishing, 2002.
2. Thomas.R.Peltier, Information Policies, Procedures and Standards, CRC Press, 2004.

REFERENCE BOOKS:

1. Thomas R Peltier, Justin Peltier, John Backley, " I nformation Security Fundamentals", Auerbach publications, CRC Press, 2005.
2. Harold F. Tipton and Micki Krause "Information Secu rity Management Handbook", Auerbach publications, 5th Edition, 2005.

CIE- Continuous Internal Evaluation (50 Marks)

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	-	-	-
Understand	5	-	5
Apply	10	10	5
Analyze	5	5	-
Evaluate	5	--	-
Create	-	-	-

SEE- Semester End Examination (50 Marks)

Bloom's Category	Tests
Remember	-
Understand	10
Apply	20
Analyze	10
Evaluate	10
Create	-

DATABASE SECURITY

Course Code : 19SFC254 **Credits : 04**
L: T: P : 4:0:0 **CIE Marks : 50**
Exam Hours : 3 **SEE Marks : 50**

Course Outcomes: At the end of the Course, the Student will be able to:

CO1	Fundamental security concepts and architectures that serve as building blocks to database security

CO2	Operational components necessary to maximize database security using various security models
CO3	Carry out a risk analysis for a large database
CO4	Implement identification and authentication procedures, fine-grained access control and data encryption techniques
CO5	Implement identification and authentication procedures, fine-grained access control and data encryption techniques
CO6	Set up accounts with privileges and roles

Mapping of Course Outcomes to Program Outcomes:

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	1	-	-	-	-	-	1	1
CO2	3	2	2	2	-	-	-	-	-	-	1	2
CO3	2	2	2	2	1	1	-	-	-	-	1	3
CO4	3	3	3	3	1	-	-	-	-	-	1	3
CO5	3	2	2	2	2	-	1	-	-	-	1	3
CO6	3	2	2	2	1	-	-	1	-	-	1	3

Mapping of Course Outcomes to Program Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	3
CO2	2	1
CO3	2	1
CO4	3	1
CO5	2	2
CO6	3	2

Module No.	Module Contents	Hours	CO's
1	Introduction: Introduction to Databases, Security Problems in Databases Security Controls Conclusions. Security Models 1: Introduction, Access Matrix Model, Take- Grant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases.	9	CO
2	Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion. Security Mechanisms: Introduction, User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation, Security Functionalities in Some Operating Systems, Trusted	9	CO2

	Computer System, Evaluation Criteria.		
3	Security Software Design: Introduction, A Methodological Approach to Security,Software Design, Secure Operating System Design, Secure DBMS Design, SecurityPackages, Database Security Design.	9	CO3
4	Statistical Database Protection & Intrusion Detection Systems: Introduction, Statistics,Concepts and Definitions, Types of Attacks, Inference Controls, evaluation Criteria forControl Comparison, Introduction IDES System, RETISS System, ASES System Discovery.	9	CO4, CO5
5	Models For The Protection Of New Generation Database Systems 1: Introduction, A Model for the Protection of Frame Based Systems, A Model for the Protection of Object-Oriented Systems, SORION Model for the Protection of Object-Oriented Databases. Models For The Protection Of New Generation Database Systems 2: A Model for the Protection of New Generation Database Systems, the Orion Model, Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions.	9	CO6

TEXT BOOKS:

1. Database Security and Auditing, Hassan A. Afyoun i, India Edition, CENGAGE Learning, 2009.
2. Database Security, Castano, Second edition, Pearson Education.

REFERENCE BOOKS:

1. Database security by Alfred Basta, Melissa Zgola , CENGAGE learning..

CIE- Continuous Internal Evaluation (50 Marks)

Bloom's Category	Tests (25 Marks)	Assignments (15 Marks)	Quizzes (10 Marks)
Remember	5	-	-
Understand	5	-	5
Apply	5	5	5
Analyze	5	5	-
Evaluate	5	-	-
Create	-	5	-

SEE- Semester End Examination (50 Marks)

Bloom's Category	Tests
Remember	10
Understand	10
Apply	10
Analyze	10
Evaluate	10

Create	-

SEMINAR

Course Code :19SFC26 **Credits : 02**
L:T:P :0:0:2 **CIE Marks : 25**
Exam Hours : 03 **SEE Marks : 25**

1.Identifying recent IEEE base paper and formulating the framework for future enhancement and it should be approved by PG committee.
2.Minimum 3 reviews to be conducted by the PG committee.
3. Report on work carried out for the seminar.
4. CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a senior faculty of the department. Participation in the seminar by all postgraduate students of the same and other semesters of the programme shall be mandatory.
5. The CIE marks awarded for Technical Seminar, shall be based on the evaluation of Seminar Report, Presentation skill and Question and Answer session in the ratio 50:25:25.

MINI PROJECT

Course Code :19SFC27 **Credits : 03**
L:T:P :0:0:3 **CIE Marks : 50**
Exam Hours : 03 **SEE Marks : 50**

The student will carry out a mini project relevant to the course. The project must be development of an application (Hardware/Software).

Conduction of Practical Examination:
The student shall prepare the report by including:

1. Define project (Problem Definition)
2. Prepare requirements document
3. Statement of work
4. Functional requirements
5. Software / Hardware requirements
6. Develop use cases
7. Research, analyze and evaluate existing learning materials on the application
8. Develop user interface and implement code
9. Prepare for final demo

APPENDIX A

Outcome Based Education

Outcome-based education (OBE) is an educational theory that bases each part of aneducational system around goals (outcomes). By the end of the educational experience each student should have achieved the goal. There is no specified style of teaching or assessment in OBE; instead classes, opportunities, and assessments should all help students achieve the specified outcomes.

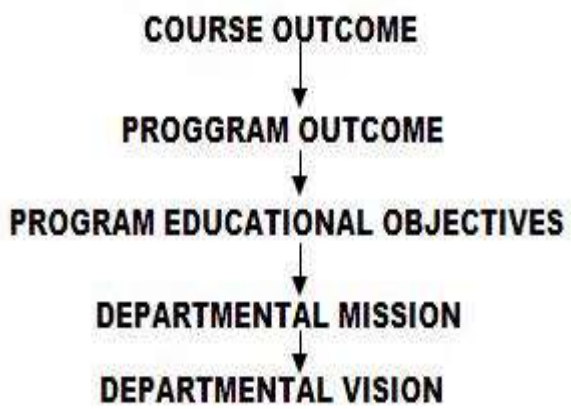
There are three educational Outcomes as defined by the National Board of Accredition:

Program Educational Objectives: The Educational objectives of an engineering degreeprogram are the statements that describe the expected achievements of graduate in their career and also in particular what the graduates are expected to perform and achieve during the first few years after graduation. [nbaindia.org]

Program Outcomes: What the student would demonstrate upon graduation. Graduateattributes are separately listed in Appendix C

Course Outcome: The specific outcome/s of each course/subject that is a part of theprogram curriculum. Each subject/course is expected to have a set of Course Outcomes

Mapping of Outcomes



APPENDIX B

The Graduate Attributes of NBA

Engineering knowledge: Apply the knowledge of mathematics, science, engineeringfundamentals, and an engineering specialisation to the solution of complex engineering problems.

Problem analysis: Identify, formulate, research literature, and analyse complex engineeringproblems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

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.

Conduct investigations of complex problems: The problems that cannot be solved by straight forward application of knowledge, theories and techniques applicable to the engineering discipline that may not have a unique solution. For example, a design problem can be solved in many ways and lead to multiple possible solutions that require consideration of appropriate constraints/requirements not explicitly given in the problem statement (like: cost, power requirement, durability, product life, etc.) which need to be defined (modeled) within appropriate mathematical framework that often require use of modern computational concepts and tools.

Modern tool usage: Create, select, and apply appropriate techniques, resources, andmodern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

The engineer and society: Apply reasoning informed by the contextual knowledge to assesssocietal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

Environment and sustainability: Understand the impact of the professional engineeringsolutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

Ethics: Apply ethical principles and commit to professional ethics and responsibilities andnorms of the engineering practice.

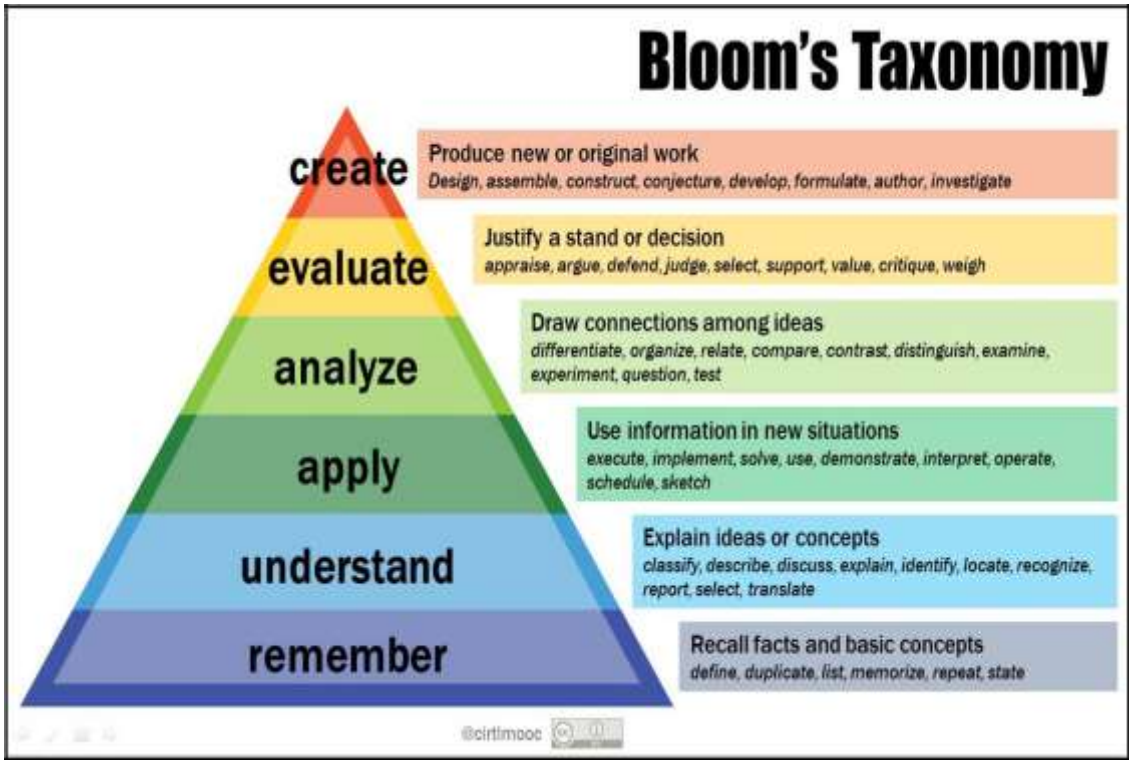
Individual and team work: Function effectively as an individual, and as a member or leaderin diverse teams, and in multidisciplinary settings.

Communication: Communicate effectively on complex engineering activities with theengineering 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.

Project management and finance: Demonstrate knowledge and understanding of theengineering 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.

Life-long learning: Recognise the need for, and have the preparation and ability to engage inindependent and life-long learning in the broadest context of technological change.

APPENDIX C

BLOOM'S TAXONOMY

Bloom's taxonomy is a classification system used to define and distinguish different levels of human cognition—i.e., thinking, learning, and understanding. Educators have typically used Bloom's taxonomy to inform or guide the development of assessments (tests and other evaluations of student learning), curriculum (units, lessons, projects, and other learning activities), and instructional methods such as questioning strategies.