SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

Minor - CYBER SECURITY - Offered by CSE Department

S.No	Course Code	CourseTitle	Scheme of Instructions HoursperWeek				Scheme ofExaminationMaximumMarks		
			L	T	P	C	I	E	Total
1	23MRCSY1	Introduction to Cyber Security	3	-	-	3	30	70	100
2	23MRCSY2	Cyber Crimes & Digital Forensics	3	-	-	3	30	70	100
3	23MRCSY3	Cryptography & Network Security (Pre-requisite: Computer Networks)	3	-	-	3	30	70	100
4	23MRCSY4	Cyber Laws and Security Policies	3	-	-	3	30	70	100
5	23MRCSY5	Blockchain Technology	3	-	-	3	30	70	100
6	23MRCSY6	Cyber Security Lab	-	-	3	1.5	30	70	100
7	23MRCSY7	Cryptography & Network Security Lab	-	-	3	1.5	30	70	100

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

COMPUTER SCIENCE Department

Minor- CYBER SECURITY

	INTRODUCTION TO CYBER SECURITY	L	T	P	C
		3	0	0	3

PRE-REQUISITES:

COURSE EDUCATIONAL OBJECTIVES:

- Develop a foundational comprehension of cybersecurity concepts, encompassing threats, vulnerabilities, and protective strategies.
- Identify and categorize common cyber threats, understand their propagation, and implement effective countermeasures.
- Explore techniques for ensuring data integrity, authentication, and data availability, while comprehending cryptographic controls.
- Develop skills to respond to cybersecurity incidents, execute disaster recovery plans, and enhance system availability.
- Analyse the ethical dimensions of cybersecurity, understand professional responsibilities, and uphold ethical standards in the field.

UNIT –1: **(9)**

Cyber security Essentials and Cube : The Cyber security World, Cyber Criminals versus Cyber security Specialists, Common Threats, Spreading Cyber security Threats, The Three Dimensions of the Cyber security Cube, CIA Triad, States of Data, Cyber security Countermeasures, IT Security Management Framework.

UNIT –2: **(9)**

Cyber security Threats, Vulnerabilities, Attacks and Protecting Secrets: Introduction, Governance, Managing Cloud Security Risk, Compliance, Legal Issues in Cloud, Audit, CSA Tools.

UNIT –3: **(9)**

Data Integrity: Types of Data Integrity Controls, Digital Signatures, Certificates, Database Integrity Enforcement.

UNIT –4: **(9)**

Data Availability and Recovery: High Availability, Measures to Improve Availability, Incident Response, Disaster Recovery.

UNIT –5: **(9)**

Protecting a Cyber security Domain : Defending Systems and Devices, Server Hardening, Network Hardening, Physical and Environmental Security, Cyber security Domains, Ethics of Working in Cyber security.

.

Total Hours: 45

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

COURSE OUTCOMES:

On successful completion of the course, students will be able to		**Pos**
CO1	Demonstrate various cyber threats and vulnerabilities, understanding their potential impact on digital assets.	
CO2	Implement proactive measures to mitigate cyber threats and protect against common attack vectors.	
CO3	Apply cryptographic techniques to ensure data integrity, authenticity, and confidentiality.	
CO4	Develop incident response plans and disaster recovery strategies to minimize the impact of cyber security incidents.	
CO5	Understand to ethical principles and professional responsibilities while making informed decisions in the realm of cyber security	

TEXT BOOKS:

1. CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, Mike Chapple, James Michael Stewart and Darril Gibson, 9th Edition
2. Cybersecurity: The Beginner's Guide, Dr.ErdalOzkaya, Packt Publishing Limited, 2019.

REFERENCE BOOKS:

1. Cybersecurity Essentials, Charles J. Brooks, Christopher Grow, Philip Craig and Donald Short, 1st edition, Sybex.
2. Network Security Essentials, William Stallings, 6th edition, Pearson Education, 2018

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

	CYBER CRIMES & DIGITAL FORENSICS	L	T	P	C
		3	0	0	3

PRE-REQUISITES:

COURSE EDUCATIONAL OBJECTIVES:

- To analyze how to conduct a digital forensics investigation and validate forensics data.
- Understand the impact of cyber crime in real time applications
- Discover the various methods to find the cyber crime
- Apply the forensics technology
- Develop the laws to control cyber crime

UNIT –1: **(9)**

Introduction: 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.

UNIT –2: **(9)**

Cyber Crime Issues: 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.

UNIT –3: **(9)**

Investigation: 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.

UNIT –4: **(9)**

Digital Forensics: 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.

UNIT –5: **(9)**

Laws and Acts: Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC, Electronic Communication Privacy ACT, Legal Policies

Total Hours: 45

COURSE OUTCOMES:

On successful completion of the course, students will be able to		**Pos**
CO1	Understand the fundamentals of cybercrime.	
CO2	Understand the various cybercrime issues.	
CO3	Understand different investigation tools for cybercrime.	
CO4	Understand basics of Forensic Technology and Practices.	
CO5	Analyze different laws, ethics and evidence handling procedures.	

TEXT BOOKS:

1. Nelson Phillips and EnfingerSteuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics ", Tata McGraw -Hill, New Delhi, 2006.

REFERENCE BOOKS:

1. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.
2. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004.
3. "Understanding Forensics in IT ", NIIT Ltd, 2005.

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

	CRYPTOGRAPHY & NETWORK SECURITY	L	T	P	C
		3	0	0	3

PRE-REQUISITES:

COURSE EDUCATIONAL OBJECTIVES:

- The concepts of classical encryption techniques and concepts of finite fields and number theory
- Working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes, and message digests, and public key algorithms
- Design issues and working principles of various authentication protocols, PKI standards
- Various secure communication standards including Kerberos, IP sec, TLS and email
- Concepts of cryptographic utilities and authentication mechanisms to design secure applications

UNIT –1: **(9)**

Computer and Network Security Concepts: Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security,

Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography,

Block Ciphers: Traditional Block Cipher Structure, The Data Encryption Standard, **Advanced Encryption Standard:** AES Structure, AES Transformation Functions

UNIT –2: (9)

Number Theory: The Euclidean Algorithm, Modular Arithmetic, Fermat's and Euler's Theorems, The Chinese Remainder Theorem, Discrete Logarithms,

Finite Fields: Finite Fields of the FormGF(p), Finite Fields of the FormGF(2^n).

Public Key Cryptography: Principles, Public Key Cryptography Algorithms, RSA Algorithm, DiffieHellman Key Exchange, Elliptic Curve Cryptography

UNIT –3: **(9)**

Cryptographic Hash Functions: Application of Cryptographic Hash Functions, Requirements & Security, Secure Hash Algorithm, Message Authentication Functions, Requirements & Security, HMAC & CMAC. Digital Signatures: NIST Digital Signature Algorithm, Distribution of Public Keys, X.509 Certificates, Public-Key Infrastructure

UNIT –4: **(9)**

User Authentication: Remote User Authentication Principles, Kerberos.

Electronic Mail Security: Pretty Good Privacy (PGP) And S/MIME.

IP Security: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange

UNIT –5: **(9)**

Transport Level Security: Web Security Requirements, Transport Layer Security (TLS), HTTPS, Secure Shell (SSH)

Firewalls: Firewall Characteristics and Access Policy, Types of Firewalls, Firewall Location and Configurations.

Total Hours: 45

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

COURSE OUTCOMES:

On successful completion of the course, students will be able to		**Pos**
	After completion of the course,students will be able to	
	Identify information security goals, classical encryption techniques and acquire fundamental knowledge on the concepts off inite fields and number theory	
	Compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication	
	Apply the knowledge of cryptographic check sums and evaluate the performance of different message digest algorithms for verifying the integrity of varying messagesizes.	
	Apply different digital signature algorithms to achieve authentication and create secure applications	
	Apply network security basics, analyse different attacks on networks and evaluate the performance of firewalls and security protocols like TLS, IPSec, and PGP	
	Apply the knowledge of cryptographic utilities and authentication mechanisms to design secure applications	

TEXT BOOKS:

1. Cryptography and Network Security – William Stallings, Pearson Education, 7th Edition.
2. Cryptography, Network Security and Cyber Laws –Bernard Menezes, Cengage Learning, 2010 edition.

REFERENCE BOOKS:

1. Cryptography and Network Security – Behrouz A Forouzan ,Debdeep Mukhopadhyaya, Mc-GrawHill, 3rdEdition, 2015.
2. Network Security Illustrated, Jason Albaneseand Wes Sonnenreich, MGH Publishers, 2003.

REFERENCE WEBSITE:

1. https://nptel.ac.in/courses/113105100https://nptel.ac.in/courses/106/105/106105031/lecture
2. https://nptel.ac.in/courses/106/105/106105162/lecture
3. https://www.mitel.com/articles/web-communication-cryptography-and-network-

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

23MR3DP4	CYBER LAWS AND SECURITY POLICIES	L	T	P	C
		3	0	0	3

PRE-REQUISITES:

COURSE EDUCATIONAL OBJECTIVES:

- Gain an understanding of the evolution and jurisprudence of cyber law in India, including the IT Act 2000.
- Learn about digital signatures, e-governance, and their legal implications under the IT Act.
- Understand the legal framework for electronic contracts, their formation, and international perspectives.
- Explore taxation issues in cyberspace, cybercrimes, electronic evidence, and their adjudication under the IT Act.

UNIT –1: **(9)**

Introduction: History of Internet and World Wide Web, Need for cyber law, Cybercrime on the rise, Important terms related to cyber law.
Cyber law in India: Need for cyber law in India, History of cyber law in India.
Information Technology Act, 2000: Overview of other laws amended by the IT Act, 2000, National Policy on Information Technology 2012.

UNIT –2: **(9)**

Overview of the Information Technology Act, 2000: Applicability of the Act, Important provisions of the Act: Digital signature and Electronic signature, Digital Signature under the IT Act, 2000, E-Governance Attribution, Acknowledgement and Dispatch of Electronic Records, Certifying Authorities, Electronic Signature Certificates, Duties of Subscribers, Penalties and Offences, Intermediaries.

UNIT –3: **(9)**

Overview of rules issued under The IT Act, 2000, Electronic Commerce, Electronic Contracts, Cyber Crimes, Cyber Frauds.

UNIT –4: **(9)**

Regulatory Authorities: Department of Electronics and Information Technology, Controller of Certifying Authorities (CCA), Cyber Appellate Tribunal, Indian Computer Emergency Response Team (ICERT), Cloud Computing, Case Laws.

UNIT –5: **(9)**

Introduction to Cybercrime and procedure to report Cyber crime:procedure to report cybercrime, some basic rules for safe operations of the computer and internet, the criminal law (amendment) act, 2013: legislative remedies for online harassment and cyberstalking in India.

Total Hours: 45

COURSE OUTCOMES:

On successful completion of the course, students will be able to		**Pos**
	Learn evolution and key aspects of Indian cyber law, including recent amendments.	
	Gain knowledge about the legalities of digital signatures and the role of e-governance in the IT Act.	
	Develop an understanding of the legalities involved in electronic contracts and international conventions.	
	Adapt in understanding and analyzing cybercrime, electronic evidence, and intellectual property rights in the context of IT.	

TEXT BOOKS:

1. Text book on "Cyber Law", **2 Ed Rp 2023**, PavanDuggal, Universal Law Publishing.
2. Text book on "Indian Cyber law on Cybercrimes", PavanDuggal,

REFERENCE BOOKS:

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
4. Thomas R Peltier, Justin Peltier and John Blackley," Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996.

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

	BLOCK CHAIN TECHNOLOGY	L	T	P	C
		3	0	0	3

PRE-REQUISITES:

COURSE EDUCATIONAL OBJECTIVES:

- Understand how block chain systems (mainly Bit coin and Ethereum) work and to securely interact with them.
- Design, build, and deploy smart contracts and distributed applications.
- Integrate ideas from block chain technology into their own projects.

UNIT –1: **(9)**

Introduction: Introduction, Scenarios, Challenges Articulated, Block chain, Block chain Characteristics, Opportunities Using Block chain, History of Block chain. Evolution of Block chain: Evolution of Computer Applications, Centralized Applications, Decentralized Applications, Stages in Block chain Evolution, Consortia, Forks, Public Block chain Environments, Type of Players in Block chain Ecosystem, Players in Market.

UNIT –2: **(9)**

Blockchain Concepts: Introduction, Changing of Blocks, Hashing, Merkle-Tree, Consensus, Mining and Finalizing Blocks, Currency aka tokens, security on blockchain, data storage on blockchain, wallets, coding on blockchain: smart contracts, peer-to-peer network, types of blockchain nodes, risk associated with blockchain solutions, life cycle of blockchain transaction.

UNIT –3: **(9)**

Architecting Blockchain solutions: Introduction, Obstacles for Use of Blockchain, Blockchain Relevance Evaluation Framework, Blockchain Solutions Reference Architecture, Types of Blockchain Applications. Cryptographic Tokens, Typical Solution Architecture for Enterprise Use Cases, Types of Blockchain Solutions, Architecture Considerations, Architecture with Blockchain Platforms, Approach for Designing Blockchain Applications.

UNIT –4: **(9)**

Ethereum Block chain Implementation: Introduction, Tuna Fish Tracking Use Case, Ethereum Ecosystem, Ethereum Development, Ethereum Tool Stack, Ethereum Virtual Machine, Smart Contract Programming, Integrated Development Environment, Truffle Framework, Ganache, Unit Testing, Ethereum Accounts, My Ether Wallet, Ethereum Networks/Environments, Infura, Ether scan, Ethereum Clients, Decentralized Application, Metamask, Tuna Fish Use Case Implementation, Open Zeppel in Contracts

UNIT –5: **(9)**

Hyper ledger Block chain Implementation: Introduction, Use Case – Car Ownership Tracking, Hyper ledger Fabric, Hyper ledger Fabric Transaction Flow, FabCar Use Case Implementation, Invoking Chain code Functions Using Client Application.

Advanced Concepts in Blockchain: Introduction, Inter Planetary File System (IPFS), Zero Knowledge Proofs, Oracles, Self-Sovereign Identity, Blockchain with IoT and AI/ML Quantum Computing and Blockchain, Initial Coin Offering, Blockchain Cloud Offerings, Blockchain and its Future Potential.

Total Hours: 45

COURSE OUTCOMES:

On successful completion of the course, students will be able to		**Pos**
	Demonstrate the foundation of the Block chain technology and understand the processes in payment and funding. Identify the risks involved in building Block chain applications.	
	Review of legal implications using smart contracts.	
	Choose the present landscape of Blockchain implementations and Understand Crypto currency markets	
	Examine how to profit from trading crypto currencies.	

TEXT BOOKS:

1. Ambadas, ArshadSarfarzAriff, Sham "Blockchain for Enterprise Application Developers", Wiley, 2020
2. Andreas M. Antonopoulos, "Mastering Bitcoin: Programming the Open Blockchain", O'Reilly, 2017

REFERENCE BOOKS:

1. Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions, Joseph Bambara, Paul R. Allen, McGraw Hill.
2. Blockchain: Blueprint for a New Economy, Melanie Swan, O'Reilly

REFERENCE WEBSITE:

https://github.com/blockchainedindia/resources

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

	CYBER SECURITY LAB	L	T	P	C
		-	-	3	1.5

PRE-REQUISITES: Nil.

COURSE EDUCATIONAL OBJECTIVES:

To get practical exposure of Cyber security threats and Forensics tools.

List of Experiments

1. Perform an Experiment for port scanning with n map
2. Set Up a honey pot and monitor the honey pot on the network
3. Install Jscript/Cryptool tool (or any other equivalent) and demonstrate Asymmetric, symmetric crypto algorithm, Hash and Digital/PKI signatures.
4. Generate minimum 10 passwords of length 12 characters using open SSL command
5. Perform practical approach to implement Foot printing-Gathering target information using Dmitry-Dmagic, UAtester
6. Working with sniffers for monitoring network communication (Wire shark).
7. Using Snort, perform real time traffic analysis and packet logging.
8. Perform email analysis using the Autopsy tool.
9. Perform Registry analysis and get boot time logging using process monitor tool
10. Perform File type detection using Autopsy tool
11. Perform Memory capture and analysis using FTK imager tool
12. Perform Network analysis using the Network Miner tool

TEXT BOOKS:

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

REFERENCE BOOKS:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010.
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012.
3. The Best Damn Cybercrime and Digital Forensics Book

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

	CRYPTOGRAPHY AND NETWORK SECURITY LAB	L	T	P	C
		-	-	3	1.5

PRE-REQUISITES: Nil.

COURSE EDUCATIONAL OBJECTIVES:

To provide hands-on experience in implementing cryptographic algorithms and security techniques using programming tools.

List of Experiments:

1. Write a C program that contains a string (char pointer) with a value 'Hello world'. The program should XOR each character in this string with 0 and displays the result.
2. Write a C program that contains a string (char pointer) with a value 'Hello world'. The program should AND or and XOR each character in this string with 127 and display the result.
3. Write a Java program to perform encryption and decryption using the following algorithms
   a. Ceasercipher b. Substitution cipher c. Hill Cipher
4. Write a C/JAVA program to implement the DES algorithm logic.
5. Write a C/JAVA program to implement the Blowfish algorithm logic.
6. Write a C/JAVA program to implement the Rijndael algorithm logic.
7. Write the RC4 logic in Java Using Java cryptography; encrypt the text "Hello world" using Blowfish. Create your own key using Java key tool.
8. Write a Java program to implement RSA algorithm.
9. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript.
10. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.
11. Calculate the message digest of a text using the MD5 algorithm in JAVA.

TEXT BOOKS:

1) Cryptography and Network Security –William Stallings, Pearson Education, 7thEdition.
2) Cryptography, Network Security and Cyber Laws –Bernard Menezes, CengageLearning, 2010 edition.

REFERENCE BOOKS:

1) Cryptography and Network Security-BehrouzA Forouzan, Debdeep Mukhopadhyaya, Mc-GrawHill, 3rdEdition,2015.
2) Network Security Illustrated ,Jason Albanese and Wes Sonnenreich, MGH Publishers,2003.

SREENIVASAINSTITUTEOFTECHNOLOGYANDMANAGEMENTSTUDIES
(Autonomous)

COURSE OUTCOMES:

On successful completion of the course, students will be able to		**POs**
CO1	Implement basic encryption techniques such as XOR, AND, Caesar, and substitution ciphers.	
CO2	Apply symmetric key algorithms (DES, AES, Blowfish, RC4) for secure data encryption and decryption.	
CO3	Demonstrate the use of asymmetric key algorithms (RSA, Diffie-Hellman) in secure communication.	
CO4	Analyze and implement cryptographic hash functions such as SHA-1 and MD5.	
CO5	Utilize programming tools like Java Cryptography Architecture and key management tools for practical security implementation.	