ಮಂಗಳೂರು ವಿಶ್ವವಿದ್ಯಾನಿಲಯ

MANGALORE UNIVERSITY

(Accredited by NAAC with 'A' Grade)

ಕ್ರಮಾಂಕ/ No. : MU/ACC/CR.24/2022-23/A2

ಕುಲಸಚಿವರ ಕಛೇರಿ
ಮಂಗಳಗಂಗೋತ್ರಿ – 574 199
Office of the Registrar
Mangalagangothri – 574 199
ದಿನಾಂಕ/Date:10.10.2022

NOTIFICATION

Sub: Revised syllabus of M.Sc. Cyber Security programme.
Ref: Academic Council approval vide agenda
No.: ಎಸಿಸಿ:ಶೈ.ಸಾ.ಸ.2:25(2022–23) dtd 27.09.2022

*****

The revised syllabus of M.Sc. Cyber Security programme which is approved by the Academic Council at its meeting held on 27.09.2022 is hereby notified for implementation with effect from the academic year 2022-23.

Copy of the Syllabus should be downloaded from the University Website (www.mangaloreuniversity.ac.in)

REGISTRAR

To,

1. The Chairman, P.G. BOS in Electronics, Mangalore University, Mangalagangothri.
2. The Co-ordinator, Cyber Security Programme, Dept. of Electronics, Mangalore University, Mangalagangothri.
3. The Registrar (Evaluation), Mangalore University, Mangalagangothri.
4. The Principals of the College Concerned.
4. The Superintendent (ACC), O/o the Registrar, Mangalore University.
5. The Asst. Registrar (ACC), O/o the Registrar, Mangalore University.
6. The Director, DUIMS, Mangalore University – with a request to publish in the website.
7. Guard File.

SEMESTER I			
SL. NO	**COURSE NAME**		**CREDITS**
HARD CORE			
1	CSCH 401	INTRODUCTION TO CYBER SECURITY	4
2	CSCH 402	FOUNDATIONS OF CRYPTOGRAPHY	4
3	CSCH 403	DATA STRUCTURES	4
SOFT CORE			
4	CSCS 404	MATHEMATICAL FOUNDATIONS	3
5	CSCS 405	PROBLEM SOLVING USING PYTHON	3
6	CSCS 406	E-COMMERCE AND E-GOVERNANCE	3
7	CSCS 407	COMPUTER NETWORKS	3
8	CSCS 408	UNIX AND SHELL PROGRAMMING	3
PRACTICALS			
9	CSCP 409	DATA STRUCTURES LABORATORY	2
10	CSCP 410	UNIX AND SHELL PROGRAMMING LABORATORY	2
		Total	**22**

SEMESTER II			
SL. NO	**COURSE NAME**		**CREDITS**
HARD CORE			
1	CSCH 451	DESIGN AND ANALYSIS OF ALGORITHMS	4
2	CSCH 452	NETWORK SECURITY	4
3	CSCH 453	DATA COMMUNICATIONS	4
SOFT CORE			
4	CSCS 454	DESIGN OF CRYPTOGRAPHIC ALGORITHMS	3
5	CSCS 455	CYBER THREAT INTELLIGENCE	3

6	CSCS 456	CLOUD COMPUTING AND SECURITY	3
7	CSCS 458	INTERNET OF THINGS	3
PRACTICALS			
8	CSCP 459	NETWORK SECURITY LABORATORY	2
9	CSCP 460/A	DESIGN AND ANALYSIS OF ALGORITHMS LABORATORY	2
		SEMINAR	
10	CSCS 461	SEMINAR ON LATEST TRENDS AND TECHNIQUES IN CYBERSECURITY	1
		OPEN CHOICE	
11	CSCO 462	INTRODUCTION TO CYBER SECURITY	3
		TOTAL	**26**

SEMESTER III			
SL. NO	**COURSE NAME**		**CREDITS**
HARD CORE			
1	CSCH 501	DIGITAL FORENSICS	4
2	CSCH 502	ETHICAL HACKING	4
3	CSCH 503	INTRODUCTION TO BLOCKCHAIN	4
SOFT CORE			
4	CSCS 505	INTRUSION DETECTION SYSTEM	3
5	CSCS 506	CYBER LAWS	3
6	CSCS 507	APPLICATION SECURITY	3
7	CSCS 508	BIG DATA ANALYTICS	3
PRACTICALS			

8	CSCP 509	ETHICAL HACKING LABORATORY	2
9	CSCP 510	BLOCKCHAIN TECHNOLOGY LABORATORY	2
		SEMINAR	
10	CSCS 511	SEMINAR ON LATEST TRENDS AND TECHNIQUES IN CYBERSECURITY	1
		OPEN CHOICE	
11	CSCO 512	CYBER LAWS	3
12	CSCO 513	ETHICAL HACKING AND DIGITAL FORENSICS	3
		TOTAL	**26**

SEMESTER IV			
SL. NO	**COURSE NAME**		**CREDITS**
1	CSCH 551	INDUSTRY INTERNSHIP / PROJECT WORK	18

SEMESTER	**MAIN COURSE CREDITS**	**OPEN CHOICE CREDITS**
I	22	0
II	23	03
II	23	03
IV	18	0
TOTAL	**GRAND TOTAL**	**92**

Scheme of Examination for M.Sc. in Cyber Security

Semester I

Course Code	Title of the Course	Credits	Hours per week	Duration of the Exam	Marks		
					IA	EXAM	Total
Hard Core (All are Compulsory)							
CSCH 401	Introduction to Cyber Security	04	04	3 hours	30	70	100
CSCH 402	Foundations of Cryptography	04	04	3 hours	30	70	100
CSCH 403	Data Structures	04	04	3 hours	30	70	100
Softcore (two to be chosen by the student)							
CSCS 404	Mathematical Foundations	03	03	3 hours	30	70	100
CSCS 405	Problem solving using Python	03	03	3 hours	30	70	100
CSCS 406	E-Commerce and E-Governance	03	03	3 hours	30	70	100
CSCS 407	Computer Networks	03	03	3 hours	30	70	100
CSCS 408	Unix and Shell Programming	03	03	3 hours	30	70	100
Practicals							
CSCP 409	Data Structures Laboratory	02	04	03hours	30	70	100
CSCP 410	Unix and Shell Programmin g Laboratory	02	04	03 hours	30	70	100
Total					**210**	**490**	**700**

Semester II **Hard Core (All are Compulsory)**							
CSCH 451	Design and Analysis of Algorithms	04	04	3 hours	30	70	100
CSCH 452	Network Security	04	04	3 hours	30	70	100
CSCH 453	Data Communications	04	04	3 hours	30	70	100
Softcore (two to be chosen by the student)							
CSCS 454	Design of Cryptographic Algorithms	03	03	3 hours	30	70	100
CSCS 455	Cyber Threat Intelligence	03	03	3 hours	30	70	100
CSCS 456	Cloud Computing and Security	03	03	3 hours	30	70	100
CSCS 458	Internet of Things	03	03	3 hours	30	70	100
Practicals							
CSCP 459	Network Security Laboratory	02	04	03 hours	30	70	100
CSCP 460/A	Design and Analysis of Algorithms Laboratory	02	04	03 hours	30	70	100
Seminar							
CSCS 461	Seminar on latest trends and techniques in Cyber security	01	01	-	15	35	50
Open Choice							
CSCO 462	Introduction to Cyber Security	03	03	3 hours	30	70	100
Total					**255**	**595**	**850**

Semester III **Hard Core (All are Compulsory)**							
CSCH 501	Digital Forensics	04	04	3 hours	30	70	100
CSCH 502	Ethical Hacking	04	04	3 hours	30	70	100
CSCH 503	Introduction to Block Chain	04	04	3 hours	30	70	100
Softcore (two to be chosen by the student)							
CSCS 505	Intrusion Detection System	03	03	3 hours	30	70	100
CSCS 506	Cyber Laws	03	03	3 hours	30	70	100
CSCS 507	Application Security	03	03	3 hours	30	70	100
CSCS 508	Big Data Analytics	03	03	3 hours	30	70	100
Practicals							
CSCP 509	Ethical Hacking Laboratory	02	04	03 hours	30	70	100
CSCP 510	BlockChain Technology Laboratory	02	04	03 hours	30	70	100
Seminar							
CSCS 461	Seminar on latest trends and techniques in Cyber security	01	01	-	15	35	50
Open Choice							
CSCO 512	Cyber Laws	03	03	3 hours	30	70	100
CSCO 513	Ethical hacking and digital forensics	03	03	3 Hours	30	70	100
Total					**255**	**595**	**850**

Semester IV

Course Code	Title of the course	Credits	Marks		
			IA	Dissertation / Viva	Total
CSCH 551	Project Work / Industry internship Dissertation	12	100	300	400
	Literature Review	03	100	---	100
	Project Demonstration / Presentation	03	--	100	100
Total		**18**	**200**	**400**	**600**

Marks Distribution Semester Wise

Semester	Credits	Marks
I	22	700
II	26	850
III	26	850
IV	18	600
Total	**92**	**3000**

SEMESTER - I

CSCH 401 : INTRODUCTION TO CYBER SECURITY

Course Objectives :

1. To provide an introduction to the cybercrimes and cyber assets
2. To enlighten about the need for comprehensive treatment to the cybersecurity risks and controls

Course Outcomes :

1. Student gets the ability to decipher the complex field of cybersecurity
2. Student realises that the cybersecurity challenge is not merely a technology one, but more of a managerial one in nature.

UNIT I

Information Security Overview : The Importance of Information Protection, The Evolution of Information Security, Justifying Security Investment : Business Agility, Cost Reduction, Portability, Security Methodology, How to Build a Security Program : Authority, Framework, Assessment, Planning, Action, Maintenance, The Impossible Job, The Weakest Link, Strategy and Tactics, Business Processes vs. Technical Controls Risk Analysis : Threat Definition : Threat Vectors, Threat Sources and Targets, Types of Attacks : Malicious Mobile Code, Advanced Persistent Threats (APTs), Manual Attacks, Risk Analysis, Compliance with Standards, Regulations, and Laws : Information Security Standards : COBIT, ISO 27000 Series, NIST

(16 Hours)

UNIT II

Regulations Affecting Information Security Professionals : The Duty of Care, Gramm-Leach-Bliley Act (GLBA). Sarbanes-Oxley Act , HIPAA Privacy and Security Rules, NERC CIP, PCI DSS: Payment Card Industry Data Security Standard, Laws Affecting Information Security Professionals : Hacking Laws, Electronic Communication Laws, Other Substantive Laws, Secure Design Principles : The CIA Triad and Other Models : Confidentiality, Integrity, Availability, Additional Concepts, Defence Models : The Lollipop Model, The Onion Model, Zones of Trust, Best Practices for Network Defence, Secure the Physical Environment, Harden the Operating System, Keep Patches Updated, Use an Antivirus Scanner (with Real-Time Scanning), Use Firewall Software, Secure Network Share Permissions, Use Encryption, Secure Applications, Secure Applications, Backup the System, Implement ARP Poisoning Defences, Create a Computer Security Defence Plan, Security Policies, Standards, Procedures, and Guidelines : Security Policies, Security Policy Development, Security Policy Contributors, Security Policy Audience, Policy Categories, Frameworks, Security Awareness, Importance of Security Awareness, Objectives of an Awareness Program, Increasing Effectiveness, Implementing the Awareness Program, Enforcement

(16 Hours)

UNIT III

Policy Enforcement for Vendors, Policy Enforcement for Employees, Software-Based Enforcement, Example Security Policy Topics, Acceptable Use Policies, Computer Policies, Network Policies, Data Privacy Policies, Data Integrity Policies, Personnel Management Policies, Security Management Policies, Physical Security Policies, Security Standards, Security Standard Example, Security Procedures, Security Procedure Example, Security Guidelines, Security Guideline Example, Ongoing Maintenance, Security Organisation : Roles and Responsibilities, Security Positions, Security Incident Response Team, Managed Security Services, Services Performed by MSSPs, Services That Can Be Monitored by MSSPs, Security Council, Steering Committee, or Board of Directors, Interaction with Human Resources, Authentication and Authorization : Authentication, Usernames and Passwords, Certificate-Based Authentication, Extensible Authentication Protocol (EAP), Biometrics, Additional Uses for Authentication, Authorization, User Rights, Role-Based Authorization (RBAC) , Access Control Lists (ACLs), Rule-Based Authorization, Compliance with Standards, NIST, ISO 27002, COBIT

(16 Hours)

Textbooks :

1. “Information Security, the Complete Reference”, Second Edition, Mark Rhodes-Ousley, McGraw-Hill, 2013
2. “The Complete Guide to Cybersecurity Risks and Controls”, Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016
3. ”Securing an IT Organisation through Governance, Risk Management, and Audit”, Ken Sigler, Dr. James L. Rainey, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016
4. “A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)”, Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016
5. “Cybercrimes: A Multidisciplinary Analysis”, Sumit Ghosh, Elliot Turrini, Springer, 2010

CSCH 402 : FOUNDATIONS OF CRYPTOGRAPHY

Course Objectives :

1. To make the student understand the foundation of information security in cyberspace
2. To make the student understand how cryptography provides CIA triad of cybersecurity

Course Outcomes :

1. Student will be able to design the required cryptographic scheme for different needs of information security
2. Student will be able to make the right choice of algorithms for different situations of information security

UNIT I

Fundamentals : Sets, Relations and Functions, Combinatorics, Computational Complexity, Discrete Probability, Random Numbers Encryption Schemes and Definitions of Security : Encryption Schemes, Perfect Secrecy, Computational Security, Indistinguishable Encryptions, Eavesdropping Attacks, Chosen Plaintext Attacks, Chosen Ciphertext Attacks, Pseudorandom Generators, Pseudorandom Functions, Block Ciphers and Operation Modes, Elementary Number Theory : Integers, Congruences, Modular Exponentiation, Algebraic structures : Groups, Rings and Fields, Finite Fields, Linear and Affine Maps

(16 Hours)

UNIT II

Block Ciphers : Constructions of Block Ciphers, Advanced Encryption Standard, Stream Ciphers : Definition of Stream Ciphers, Linear Feedback Shift Registers, RC4128, Salsa20, ChaCha20, Hash Functions, Definitions and Security Requirements, Applications of Hash Functions, Merkle-Damgård Construction, SHA-1, SHA-2, SHA-3, Message Authentication Codes : Definitions and Security Requirements, CBC MAC, HMAC, Authenticated Encryption

(16 Hours)

UNIT III

Public-Key Encryption and the RSA Cryptosystem : Public-Key Cryptosystems, Plain RSA, RSA Security, Generation of Primes, Efficiency of RSA, Padded RSA, Integer Factoring, Key Establishment : Key Distribution, Key Exchange Protocols, Diffie-Hellman Key Exchange, Diffie-Hellman using Subgroups of $\mathbb{Z}p^{*}$, Discrete Logarithm, Key Encapsulation, Hybrid Encryption, Digital Signatures : Definitions and Security Requirements, Plain RSA Signature, Probabilistic Signature Scheme, Qualitative Introduction to Elliptic Curve Cryptography

(16 Hours)

Textbooks :

1. “A Course in Cryptography”, Heiko Knospe, American Mathematical Society, 2019
2. “Introduction to Modern Cryptography”, Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008
3. “Foundations of Cryptography - Basic Tools”, Oded Goldreich, Cambridge University Press, 2004
4. “Foundations of Cryptography - Basic Applications”, Oded Goldreich, Cambridge University Press, 2009

CSCH 403 : DATA STRUCTURES

Course Objectives :

1. To provide the basic foundation in computer programming to supplement the algorithms while implementing cybersecurity components
2. To get the knowledge about the ways how different kinds of data can be organised and saved in different ways in computer memory

Course Outcomes :

1. Student gets the ability to make decisions about the choice of the required data structures while programming
2. Gets the knowledge about the cost of a data structure in terms of time and space complexities

UNIT I

Introduction: Data Structures, Classifications (Primitive & Non Primitive), Data structure Operations, Review of Arrays, Structures, Self-Referential Structures, and Unions. Pointers and Dynamic Memory Allocation Functions. Representation of Linear Arrays in Memory, Dynamically allocated arrays. Array Operations: Traversing, inserting, deleting, searching, and sorting. Multidimensional Arrays, Polynomials and Sparse Matrices. Strings: Basic Terminology, Storing, Operations and Pattern Matching algorithms. Programming Examples.

(16 Hours)

UNIT II

Stacks: Definition, Stack Operations, Array Representation of Stacks, Stacks using Dynamic Arrays, Stack Applications: Polish notation, Infix to postfix conversion, evaluation of postfix expression. Recursion - Factorial, GCD, Fibonacci Sequence, Tower of Hanoi, Ackerman's function. Queues: Definition, Array Representation, Queue Operations, Circular Queues, Circular queues using Dynamic arrays, Dequeues, Priority Queues, A Mazing Problem. Multiple Stacks and Queues. Programming Examples. Linked Lists: Definition, Representation of linked lists in Memory, Memory allocation; Garbage Collection. Linked list operations: Traversing, Searching, Insertion, and Deletion. Doubly Linked lists, Circular linked lists, and header linked lists. Linked Stacks and Queues. Applications of Linked lists – Polynomials, Sparse matrix representation. Programming Examples.

(16 Hours)

UNIT III

Terminology, Binary Trees, Properties of Binary trees, Array and linked Representation of Binary Trees, Binary Tree Traversals - Inorder, postorder, preorder; Additional Binary tree operations. Threaded binary trees, Binary Search Trees – Definition, Insertion, Deletion, Traversal, Searching, Application of Trees-Evaluation of Expression, Programming Examples. Graphs: Definitions, Terminologies, Matrix and Adjacency List Representation Of

Graphs, Elementary Graph operations, Traversal methods: Breadth First Search and Depth First Search.

(16 Hours)

Textbooks :

1. Ellis Horowitz and Sartaj Sahni, Fundamentals of Data Structures in C, 2nd Ed, Universities Press, 2014.
2. Seymour Lipschutz, Data Structures Schaum's Outlines, Revised 1st Ed, McGraw Hill, 2014.

CSCS 404 : MATHEMATICAL FOUNDATIONS

Course Objectives :

1. To make the student aware of the tool kit of mathematics required for cryptography
2. To make the student aware of the relationship between mathematical objects and the algorithms

Course Outcomes :

1. Student gets required awareness stated in the Objectives, to build cryptographic algorithms
2. Student gets required awareness stated in the Objectives, to build cryptographic protocols which are build against attacks by hackers

UNIT I

Algebra and Number Theory : Modular Arithmetic, Groups, Rings, and Fields, Greatest Common Divisors and Multiplicative Inverse, Subgroups, Subrings, and Extensions, Groups, Rings, and Field Isomorphisms, Polynomials and Fields.

(12 Hours)

UNIT II

Construction of Galois Field, Extensions of Fields, Cyclic Groups of Group Elements, Efficient Galois Fields, Mapping between Binary and Composite Fields. Block Ciphers: Inner Structures of a Block Cipher, The Advanced Encryption Standard(AES), The AES Round Transformations.

(12 Hours)

UNIT III

Rijndael in Composite Field, Elliptic Curves, Scalar Multiplications: LSB First and MSB First Approaches, Montgomery's Algorithm for Scalar Multiplication.

(12 Hours)

Textbooks :

1. "Hardware Security Design, Threats, and Safeguards", Debdeep Mukhopadhyay Rajat Subhra Chakraborty, CRC Press, 2015
2. "Hardware IP Security and Trust", Prabhat Mishra, Swarup Bhunia, Mark Tehranipoor, Springer, 2017
3. "Fault Tolerant Architectures for Cryptography and Hardware Security", Sikhar Patranabis Debdeep Mukhopadhyay, Springer, 2018
4. "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

CSCS 405 : PROBLEM SOLVING USING PYTHON

Course Objectives :

1. To empower the student with the most versatile computer language available for wide variety of tasks in cybersecurity
2. To make the student aware of the different language components which serve different purposes in programming

Course Outcomes :

1. Student gets the knowledge about the right choice of data structures for a task
2. Student gets the feel for applying a programming language for different scenarios in cybersecurity.

UNIT I

A Gentle Introduction to Python: A proper introduction, Enter the Python, About Python, What are the drawbacks, Who is using Python today?, Setting up the environment, Installing Python, How you can run a Python program, How is Python code organised? Python's execution model, Guidelines on how to write good code, Built-in Data Types: Mutable or immutable? That is the question Numbers, Immutable sequences, Mutable sequences, Set types, Mapping types – dictionaries, The collections module, Enums, Final considerations.

(12 Hours)

UNIT II

Iterating and Making Decisions Conditional programming: Looping, Putting all this together, A quick peek at the itertools module, Functions, the Building Blocks of Code: Why use functions?, Scopes and name resolution, Input parameters, Return values, A few useful tips, Recursive functions, Anonymous functions, Function attributes, Built-in functions, One final example, Documenting your code, Importing objects, Saving Time and Memory: The map, zip, and filter functions, Comprehensions, Generators, OOP, Decorators, and Iterators: Decorators, A decorator factory, Object-oriented programming (OOP).

(12 Hours)

UNIT III

Files and Data Persistence: Working with files and directories, Data interchange formats, IO, streams, and requests, Persisting data on disk, Data Science: IPython and Jupyter Notebook, Dealing with data, Web Development: What is the web? How does the web work?, The Django web framework, A regex website, The future of web development.

(12 Hours)

Textbooks :

1. “Learn Python Programming The no-nonsense, beginner's guide to programming, data science, and web development with Python 3.7”, Fabrizio Romano, Second Edition, 2018.
2. “Python for Everybody: Exploring Data Using Python 3”, Charles R.Severance, 1st Edition, CreateSpace Independent Publishing Platform, 2016.
3. “Learning Python for Forensics - Leverage the power of Python in forensic investigations”, Preston Miller, Chapin Bryce, Packt Publishing, Second Edition, 2019

CSCS 406 : E-COMMERCE AND E-GOVERNANCE

Course Objectives :

To make the student aware of the ways in which the business has been shifted online

1. To make the student aware of the different technologies used in e-Business

Course Outcomes :

1. Student gets the skills to understand the components of the e-Business
2. Student gets the difference between different ways doing business online

UNIT I

eBusiness Framework: Defining Electronic Business, Case Studies : Electronic Shop (B2C), Electronic Health Market (B2B), Electronic Voting and Elections (A2C), Knowledge Exchange via Electronic Books (C2C), eProducts and eServices: Components of a Business Model, Anatomy of an Electronic Marketplace, Classification of Business Webs According to Tapscott, Comparison and Valuation of Networks, The Price Formation Process, eProcurement: Strategic and Operational Procurement, Information Support for Procurement, Basic Types of eProcurement Solutions, Catalog Management.

(12 Hours)

UNIT II

eMarketing : The Path to Individual Marketing, Comparison of the Communications Media, The Development Model for Online Customers, Online Promotion, eContracting: The Electronic Negotiation Process, Generic Services for the Negotiation Process, The Digital Signature, XML and Electronic Contracts, Legal Rights of the Information Society, eDistribution: Components of a Distribution System, Types of Distribution Logistics, Supply Chain Management, Electronic Software Distribution (ESD), Protection Through Digital Watermarks, ePayment : Credit Card-Based Procedures, Asset-Based Procedures, Innovative ePayment Solutions, Comparison of ePayment Solutions.

(12 Hours)

UNIT III

eCustomer Relationship Management: The Customer Equity Model by Blattberg et al, Analytical Customer Relationship Management, Operational Customer Relationship Management, Use of CRM Systems, mBusiness : Mobile Devices, Mobile Communications, Mobile Applications, eSociety: Virtual Organisations, Work Organization in eTeams, The Knowledge Worker in a Knowledge Society, Measuring the Success of Intellectual Capital, Ethical Maxims for eTeams.

(12 Hours)

Textbooks :

1. “eBusiness & eCommerce- Managing the digital Value Chain”, Andreas Meier, Henrik Stormer, Springer, 2009
2. “Digital Economy: Impacts, Influences and Challenges”, Harbhajan S. Kehal, Varinder P. Singh, Idea group publishing, 2005
3. “The Digital Economy Fact Book”, ninth edition, Daniel B. Britton Stephen McGonegal, The Progress & Freedom Foundation, 2007

CSCS 407 : COMPUTER NETWORKS

Course Objectives :

1. To give the foundational knowledge of how internet is build
2. To give the foundation about the protocols which make the internet work

Course Outcomes :

1. Student gets the knowledge of necessity to design networks which protect CIA of the information
2. Student gets the knowledge of TCP/IP protocol suite, which is the lingua franca of the networked machines

UNIT I

A TCP/IP World : The Internet, TCP/IP Suite, Internet Protocol Stack, Some Application Layer Protocols, Information Retrieval, File Transfer, Mail Transfer, Using Another Computer, Resolving Names and Numbers, User Datagram Protocol, UDP Attributes, UDP Header, Checksum, Transmission Control Protocol (TCP), Sequencing, Segmentation, TCP Header, TCP Ports, Checksum, Urgent Data, Cumulative Acknowledgments, Selective Acknowledgments, Flow Control, Retransmission Time-Out, Creating a Connection, OPEN Function Calls, Flags, Connection Denied, Connection Termination, Internet Protocol, IP Version 4, IP Version 6, Other Internet Layer Protocols, Network Interface Layer, TCP/IP Protocol Stack, Data Communication : Communication Equipment, Making a Data Call, Open Systems Interconnection Model, OSI Model, Layer Tasks, Internet Model, Application Layer, Transport Layer, Internet Layer, Network Interface Layer, Local Area Networks : Ethernet, Classic Ethernet, IEEE 802.3 (Ethernet) LAN, New Configurations, IEEE 802.5 Token-Ring LAN, What Is a Token, Token Ring Frame, Fibre Distributed Data Interface, Bit Ordering

(12 Hours)

UNIT II

Wide Area Networks : Point-to-Point Links, High-Level Data Link Control Protocol, PPP and SLIP, Non Broadcast Multiple Access Links, Packet-Switched Networks, Cell Relay, Frame Relay, Quality of Service, Differentiated Services, T-1 Performance Measures, ATM Performance Measures, Frame Relay Performance Measures,QoS, Connecting Networks Together : More Than One Network, Repeaters, Bridges, Routers, and Gateways, Layer 2 and Layer 3 Switches, Bridging, Bridging Identical LANs, Bridging Dissimilar LANs, Routing, Routing over Broadcast Links, Routing over Point-to-Point Links, Routing over Non Broadcast Multiple Access Links, Router, Static Routing, Dynamic Routing, Border Gateway Routing, Intermediate System-to-Intermediate System, Virtual LANs, Tags, Edge and Core Switches, Multiprotocol Label Switching, Label Distribution, Label Location, MPLS Operation

(12 Hours)

UNIT III

Protecting Enterprise Catenets : Operating Environment, Enterprise Catenet, Interconnections, Combating Loss of Privacy, Network Address Translation, Proxies, Tunnels, Encryption, Decryption, and Authentication, IP Security, Other Tunnelling Protocols, Firewalls, Functions Performed in Firewall, Virtual Private Networks, Types of VPNs, Basic Connections, Transmission Facilities : Twisted Pairs, Cable Pair Impairments, Circuit Noise, Crosstalk, Transport Based on Twisted Pairs, Transmission System 1 (T-1), ISDN, Optical Fibres, Single-Mode Fibre, Optical Properties, Wavelength Division Multiplexing, Optical Amplifiers, Short-Distance Facilities,Transport Based on Optical Fibres, Synchronous Optical Network, Synchronous Digital Hierarchy, Radio, Frequencies and Modulation, IEEE 802.11 Standard, The Convergence of Voice and Data : The Last Mile, The Local Loop, Modems and Digital Subscriber Lines, Cable Television, Voice over IP (VoIP), Packet Voice, Telephone Signalling, Real-Time Transport Protocols, Major Signalling Protocols

(12 Hours)

Textbooks :

1. "A Professional's Guide to Data Communication in a TCP/IP World", E. Bryan Carne, Artech house, 2004
2. James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth edition, Pearson,2017
3. Nader F Mir, Computer and Communication Networks, 2nd Edition, Pearson, 2014

CSCS 408 – UNIX AND SHELL PROGRAMMING

Course Objectives :

1. To provide the student with the "swiss knife" of cybersecurity, namely Unix commands
2. To make the student automate the cybersecurity tasks

Course Outcomes :

1. Student gets the ability to manage computer systems and networks with the Unix and Shell commands
2. Student gets the most important skill required in the whole of cybersecurity

UNIT I

The Linux Command Line : Starting with Linux Shells, Looking into the Linux kernel, Linux Distributions, Getting to the Shell, Terminal Emulation, The Linux Console, The GNOME Terminal, Starting the Shell, Basic bash Shell Commands, Filesystem Navigation, File Handling, More bash Shell Commands, Monitoring Programs, Monitoring Disk Space, Working with Data Files, Using Linux Environment Variables, Setting Environment Variables, Setting the PATH Environment Variable, Understanding Linux File Permissions, Linux Security,Changing Security Settings, Working with Editors-vim, emacs, KDE Family, GNOME.

(12 Hours)

UNIT II

Shell Scripting Basics : Basic Script Building, Creating a Script File, Using Variables, Exiting the Script, Using Structured Commands, The if-then-else Statement, Compound Condition Testing, Advanced if-then Features, The case Command, More Structured Commands, The for, while & until Commands, Looping on File Data, Command Line & Special Parameters, Handling User Input, Presenting Data, Script Control, Handling Signals, Running Scripts in Background Mode, Job Control, Being Nice, Creating Functions, Basic Script Functions, Function Recursion, Creating a Library, Introducing sed and gawk, Regular Expressions, Shell Scripts for Administrators, Monitoring System Statistics, Performing Backups.

(12 Hours)

UNIT III

Linux Administration : Where to Start, Linux's relationship to UNIX, Notation and typographical conventions, Where to go for information, Booting and Shutting Down, Bootstrapping, Using boot loaders: LILO and GRUB, Working with startup scripts, Rebooting and shutting down, Rootly Powers, The superuser, Becoming root, Other pseudo-users, Controlling Processes, Components of a process, The life cycle of a process, The Filesystem, File types, Adding New Users, Adding a Disk, Periodic Processes, Backups, Syslog and Log Files, Software and Configuration Management.

(12 Hours)

Textbooks :

1. "Linux Command Line and Shell Scripting Bible", Richard Blum, Wiley Publishing, Inc, 2008.
2. "Linux Administration Handbook", Evi Nemeth, Garth Snyder & Trent R. Hein, Second Edition, Prentice Hall, 2006.

Semester - II

CSCH 451 – DESIGN AND ANALYSIS OF ALGORITHMS

Course Objectives :

1. To make the student aware of the need to analyse the time and space complexities of algorithms
2. To make the student aware of the foundational role played by algorithms in providing the security for modern cryptography.

Course Outcomes :

1. Gets to know the ultimate limits of security and how security is physically built into cyberspace, through algorithms.
2. Gets the knowledge that the condition P ≠ NP is very important for security, without which there will be pandemonium in cyberspace.

UNIT I

Introduction to algorithms : Big-O notation, Algorithms with numbers: Basic arithmetic, Modular arithmetic, Primality testing, Cryptography, Universal hashing, Randomised algorithms, Introduction to Different Strategies in algorithm design : Divide and Conquer, Greedy approach, dynamic programming, linear programming

(16 Hours)

UNIT II

NP-complete problems: Search problems, Class NP, NP-hard problem, Reduction, NP-complete problems, Coping with NP-completeness: Intelligent exhaustive search, Approximation algorithms, Local search heuristics, SAT solvers, Implications on Information security : P vs NP Problem, Reasons for P ≠NP (the foundation and the assumption of modern cryptography), Implications of P = NP on Information security

(16 Hours)

UNIT III

Complexity Analysis of algorithms used in Modern Cryptography namely, Integer Factorization Problem, Discrete log problem, primality testing, Modular exponentiation, Hashing Algorithms, Qualitative Introduction to Quantum Computing Algorithms : Peter Shor's quantum algorithm for factoring and Grover's Searching algorithm and their Implications on Information security

(16 Hours)

Textbooks :

1. Algorithms - Sanjoy Dasgupta, Christos Papadimitriou and Umesh Vazirani, TMH-2008
2. Introduction to Algorithms – Thomas H.Cormen, Charles E. Leiserson, Ronald L Rivest, Clifford Stein, third edition, The MIT Press, 2009
3. Combinatorial Optimization : Algorithms and Complexity, Christos H. Papadimitriou, Kenneth Steiglitz
4. "A Course in Cryptography", Heiko Knospe, American Mathematical Society, 2019
5. "Introduction to Modern Cryptography", Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008
6. "Foundations of Cryptography - Basic Tools", Oded Goldreich, Cambridge University Press, 2004
7. "Foundations of Cryptography - Basic Applications", Oded Goldreich, Cambridge University Press, 2009

CSCH 452 - NETWORK SECURITY

Course Objectives :

1. To make the student aware of the security needs of the computer network which works on protocols and how the weakness in these protocols be exploited
2. To make the student aware of the wrong practices of the employees which lead to cyber attacks

Course Outcomes :

1. Student gets the knowledge of the security loopholes in the existing network topologies and the ways to safeguard them
2. Student gets the knowledge to patch the networks with security patches whenever they are available from vendors

UNIT I

Secure Network Design : Introduction to Secure Network Design: Acceptable Risk, Designing Security into a Network, Designing an Appropriate Network, The Cost of Security, Performance, Availability, Security: Wireless Impact on the Perimeter, Remote Access Considerations, Internal Security Practices, Intranets, Extranets, and DMZs, Outbound Filtering, Compliance with Standards: NIST, ISO 27002, COBIT, Network Device Security : Switch and Router Basics: MAC Addresses, IP Addresses, and ARP, TCP/IP, Hubs, Switches, Routers, Network Hardening: Patching, Switch Security Practices, Access Control Lists, Disabling Unused Services, Administrative Practices, Internet Control Message Protocol (ICMP), Anti-Spoofing and Source Routing, Logging

(16 Hours)

UNIT II

Firewalls: Overview: The Evolution of Firewalls, Application Control, Must have Firewall features, Core Firewall Functions, Network Address Translation (NAT), Auditing and Logging, Additional Firewall Capabilities: Application and Website Malware Execution Blocking, Antivirus, Intrusion Detection and Intrusion Prevention, Web Content (URL) Filtering and Caching, E-Mail (Spam) Filtering, Enhance Network Performance, Firewall Design: Firewall Strengths and Weaknesses, Firewall Placement, Firewall Configuration, Virtual Private Networks: How a VPN Works, VPN Protocols: IPSec, PPTP, L2TP over IPSec, SSL VPNs, Remote Access VPN Security: Authentication Process, Client Configuration, Client Networking Environment, Offline Client Activity, Site-to-Site VPN Security, Wireless Network Security: Radio Frequency Security Basics: Security Benefits of RF Knowledge, Layer One Security Solutions, Data-Link Layer Wireless Security Features, Flaws, and Threats: 802.11 and 802. 15 Data-Link Layer in a Nutshell, 802.11 and 802.15 Data-Link Layer Vulnerabilities and Threats, Closed-System SSIDs, MAC Filtering, and Protocol Filtering, Built-in Bluetooth Network Data-Link Security and Threats, Wireless Vulnerabilities and Mitigations: Wired Side Leakage, Rogue Access Points, Misconfigured Access Points, Wireless Phishing, Client Isolation, Wireless Network Hardening Practices and Recommendations: Wireless Security Standards, Temporal Key Integrity Protocol and Counter Mode with CBC-MAC Protocol, 802.1x-Based Authentication and EAP Methods, Wireless Intrusion Detection and Prevention: Wireless IPS and IDS, Bluetooth IPS, Wireless Network Positioning and Secure Gateways

(16 Hours)

UNIT III

Intrusion Detection and Prevention Systems: IDS Concepts, Threat Types, First-Generation IDS, Second-Generation IDS, IDS Types and Detection Models: Host-Based IDS, Network-Based IDS (NIDS), Anomaly-Detection (AD) Model, Signature-Detection Model, the type of IDS to Use, IDS Features: IDS End-User Interfaces, Intrusion-Prevention Systems (IPS), IDS Management, IDS Logging and Alerting, IDS Deployment Considerations: IDS Fine-Tuning, IPS Deployment Plan, Security Information and Event Management (SIEM): Data Aggregation, Analysis, Operational Interface, Additional SIEM Features, Voice over IP (VoIP) and PBX Security: Background, VoIP Components, Call Control, Voice and Media Gateways and Gatekeepers, MCUs, Hardware Endpoints, Software Endpoints, Call and Contact Center Components, Voicemail Systems, VoIP Vulnerabilities and Countermeasures: Old Dogs, Old Tricks: The Original Hacks, Vulnerabilities and Exploits, The Protocols, Security Posture: System Integrators and Hosted VolP, PBX: Hacking a PBX, Securing a PBX, TEM: Telecom Expense Management

(16 Hours)

Textbooks :

1. "Information Security - The Complete Reference", Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg McGraw Hill Education; Second Edition
2. Network Security For Dummies – a book by Chey Cobb, CISSP, Publisher-John Wiley & Sons, 2011
3. Network Security: A Practical Approach- a book by Jan L. Harrington Morgan Kaufmann publications
4. Convery, Sean. Network Security Architectures. Cisco Press, 2004.
5. Ghosh, Sumit, and H. Lawson. Principles of Secure Network Systems Design. Springer, 2001.
6. Northcutt, Stephen, et al. Inside Network Perimeter Security. New Riders Publishing, 2005.
7. Strassberg, Keith, Richard Gondek, and Gary Rollie. Firewalls: The Complete Reference. McGraw-Hill/Osborne, 2002.
8. Zwicky, Elizabeth, Simon Cooper, and D. Brent Chapman. Building Internet Firewalls. 2nd ed. O'Reilly & Associates, Inc., 2000.
9. Akin, Thomas. Hardening Cisco Routers. O'Reilly, 2002.
10. Davis, Peter. Securing and Controlling Cisco Routers. Auerbach, 2002.
11. Hogg, Scott, and Eric Vyncke. IPv6 Security. Cisco Press, 2008.

CSCH 453 : DATA COMMUNICATIONS

Course Objectives :

1. To make the student aware of the different protocols and devices used in computer network for data communication
2. To make the student aware of the new technologies which are emerging in the market

with new features and facilities

Course Outcomes :

1. Student gets the wide spectrum of devices and protocols which connect together to create the IT infrastructure
2. Student gets the knowledge of the working and the interoperability between the data communication devices

UNIT I

Computer Networking Devices : Router, switch, hub, Internet cables in the sea, DNS service, Certifying Authority(CA), Ethernet, Wireless routers and switches, Network Interface Card, IMEI in mobile phones, Network Protocols: FTP, SMTP, POP3, IMAP, HTTP, HTTPS, ARP, DHCP

(16 Hours)

UNIT II

Wifi, Lifi, Wimax, Bluetooth, ZigBee, hotspots, Credit card, debit card, card readers, QR code, bar code, Biometric devices, EM spectrum, Infrared communication, Satellite communications, RADAR, SONAR

(**16 Hours**)

UNIT III

The Onion Router (TOR), darkweb, ATM network, Data flow in Banking Infrastructure, GSM, CDMA, Mobile networks 2G/3G/4G/5G, Point of sale (POS) machine, Data flow in in credit card, debit card, RFID, NFC, GPS, Geofencing, data modulation techniques, Wireless Sensor Network (WSN), data communication in drone

(16 Hours)

Textbooks :

1. D. Roddy, “Satellite Communication”, (4/e), McGraw- Hill, 2009.
2. Shuang-Hua Yang, “Wireless Sensor Networks: Principles, Design and Applications”,Springer-Verlag London, 2014.
3. “A Professional’s Guide to Data Communication in a TCP/IP World”, E. Bryan Carne, Artech house, 2004
4. James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth edition, Pearson,2017
5. Nader F Mir, Computer and Communication Networks, 2nd Edition, Pearson, 2014

CSCS 454 - DESIGN OF CRYPTOGRAPHIC ALGORITHMS

Course Objectives :

1. To make the student aware of the need to design tamper proof protocols using the cryptographic algorithms
2. To make the student aware of the higher level protocols which can withstand the attack from the hackers

Course Outcomes :

1. Student gets the ability to design and test one's own protocol and test their security strengths
2. Student gets the ability to read the laborious protocols written by others and the ability to meticulous work with them

UNIT I

Cryptographic Protocols : Introduction to protocols, communications using symmetric cryptography, one-way functions, one-way hash functions, communications using public-key cryptography, digital signatures, digital signatures with encryption, random and pseudo-random-sequence generation Basic protocols : authentication, key exchange, authentication and key exchange, formal analysis of authentication and key-exchange protocols, multiple-key public-key cryptography, secret splitting, secret sharing, cryptographic protection of databases

(12 Hours)

UNIT II

Intermediate protocols : Timestamping services, subliminal channel, undeniable digital signatures, designated confirmer signatures, proxy signatures, group signatures, fail-stop digital signatures, computing with encrypted data, bit commitment, fair coin flips, mental poker, one-way accumulators, all-or-nothing disclosure of secrets, key escrow

(12 Hours)

UNIT III

Advanced protocols : zero-knowledge proofs, zero-knowledge proofs of identity, blind signatures, identity-based public-key cryptography, oblivious signatures, oblivious transfer, simultaneous contract signing, digital certified mail, simultaneous exchange of secrets, Esoteric protocols : secure elections, secure multiparty computation, anonymous message broadcast, digital cash

(12 Hours)

Textbooks :

1. "Applied Cryptography, protocols, algorithms, and source code in C ", second edition, Bruce Schneier, Wiley, 1996

2. “A Course in Cryptography”, Heiko Knospe, American Mathematical Society, 2019
3. “Introduction to Modern Cryptography”, Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008
4. “Foundations of Cryptography - Basic Tools”, Oded Goldreich, Cambridge University Press, 2004
5. “Foundations of Cryptography - Basic Applications”, Oded Goldreich, Cambridge University Press, 2009

CSCS 455 - CYBER THREAT INTELLIGENCE

Course Objectives :

1. To make the student aware of the different threats existing from the dark web and to study their behaviour and strategies
2. To employ Machine learning and AI for the same purposes of learning their behaviour

Course Outcomes :

1. Student gets the ability to choose between different AI and ML strategies for gathering threat intelligence
2. Student gets the right skills required for defending the modern day industry infrastructure from attackers

UNIT I

Moving to Proactive Cyber Threat Intelligence: Proactive Intelligence beyond the Deepweb and Dark Web, Understanding Darkweb Malicious Hacker Forums: Forum Structure and Community Social Organization.

(12 Hours)

UNIT II

Basics of Machine Learning in Cybersecurity : What is machine learning, Different types of machine learning algorithm, Algorithms in machine learning, Knocking Down CAPTCHAs: Characteristics of CAPTCHAs, Using artificial intelligence to crack CAPTCHAs, Using Data Science to Catch Email Fraud and Spam

(12 Hours)

UNIT III

Automatic Mining of Cyber Intelligence from the Darkweb, Analysing Products and Vendors in Malicious Hacking Markets: Marketplace Data Characteristics, Users Having Presence in Markets/Forums, Discovery of Zero-Day Exploits, Exploits Targeting Known Vulnerabilities.

(12 Hours)

Textbooks :

1. “Darkweb Cyber Threat Intelligence Mining”, John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath, Jana Shakarian, Paulo Shakarian, Cambridge University Press, 2017
2. “Cybercrimes: A Multidisciplinary Analysis”, Sumit Ghosh, Elliot Turrini, Springer, 2010
3. “Big Data Analytics in Cybersecurity”, Onur Savas, Julia Deng, CRC Press, 2017
4. “Data Analytics and Decision Support for Cybersecurity”, Iván Palomares Carrascosa, Harsha Kumara Kalutarage, Yan Huang, Springer, 2017
5. “Data Analysis for Network Cyber-Security”, Niall Adams, Nicholas Heard, Imperial College Press, 2014

CSCS 456 : CLOUD COMPUTING AND SECURITY

Course Objectives :

1. To make the student aware of the trend in the industry to put every service and data on cloud
2. To make student aware of the vocabulary of this new technology and to alert about the security challenges

Course Outcomes :

1. Student gets the skill required to work with various cloud platforms and their pros and cons
2. Student gets the knowledge about the security needs of the cloud technologies

UNIT I

Introduction : Introducing Cloud Computing, Grasping the Fundamentals, Discovering the Value of the Cloud for Business, Getting Inside the Cloud, Developing Your Cloud Strategy.

(12 Hours)

UNIT II

Understanding the Nature of the Cloud : Seeing the Advantages of the Highly Scaled Data Centre, Exploring the Technical Foundation for Scaling Computer Systems, Checking the Cloud’s Workload Strategy, Managing Data, Discovering Private and Hybrid Clouds

(12 Hours)

UNIT III

Cloud Elements & its Security : Seeing Infrastructure as a Service, Exploring Platform as a Service, Using Software as a Service, Understanding Massively Scaled Applications and Business Processes, Setting Some Standards. Web Services Delivered from the Cloud, Building Cloud Networks, Federation, Presence, Identity, and Privacy in the Cloud, Security in the Cloud.

(12 Hours)

Textbooks :

1. "Cloud Computing for Dummies", Judith Hurwitz, Robin Bloor, Marcia Kaufman and Dr. Fern Halper, Wiley Publishing, Inc., 2010.
2. "Cloud Computing: A Practical Approach", Anthony T. Velte, Toby J. Velte, Robert Elsenpeter, McGraw-Hill, 2010.
3. "Cloud Computing - Implementation, Management, and Security", John Rittinghouse, James Ransome, CRC Press, 2009.

CSCS 458 : INTERNET OF THINGS

Course Objectives :

1. To make the student aware of the new wave of connectivity, of the every "thing" using internet technologies
2. To make the student aware of the security challenges of the new technological trend

Course Outcomes :

1. Student gets the difference between the security needs of an ordinary node and an IoT node
2. Student gets the knowledge of the tradeoffs required in implementing security on an IoT device

UNIT I

Defining the IoT, Cybersecurity versus IoT security and cyber-physical systems, IoT uses today, The IoT in the enterprise, The IoT of the future and the need to secure. Vulnerabilities, Attacks, and Countermeasures: Primer on threats, vulnerability, and risks (TVR), Primer on attacks and countermeasures, Today's IoT attacks, Lessons learned and systematic approaches. Security Engineering for IoT Development: Building security into design and development, Safety and security design, Processes and agreements, Technology selection – security products and services.

(12 Hours)

UNIT II

The IoT Security Lifecycle: The secure IoT system implementation lifecycle, Operations and maintenance, Dispose. Cryptographic Fundamentals for IoT Security Engineering: Cryptography and its role in securing the IoT, Cryptographic module principles, Cryptographic key management fundamentals, Examining cryptographic controls for IoT protocols, Future directions of the IoT and cryptography. Identity and Access Management Solutions for the IoT: An introduction to identity and access management for the IoT, Authentication credentials, IoT IAM infrastructure, Authorization and access control.

(12 Hours)

UNIT III

Mitigating IoT Privacy Concerns: Privacy challenges introduced by the IoT, Guide to performing an IoT PIA, PbD principles, Privacy engineering recommendations. Setting Up a Compliance Monitoring Program for the IoT: IoT compliance, A complex compliance environment. Cloud Security for the IoT: Cloud services and the IoT, Exploring cloud service provider IoT offerings, Cloud IoT security controls, Tailoring an enterprise IoT cloud security architecture, New directions in cloud-enabled IOT computing. IoT Incident Response: Threats both to safety and security, Planning and executing an IoT incident response

(12 Hours)

Textbooks :

1. Brian Russell and Drew Duren, “Practical Internet of Things Security”, Packt Publishing, 2016
2. Giancarlo Fortino and Carlos E. Palau “Interoperability, Safety and Security in IoT” Springer Publications 2017.
3. Zaigham Mahmood, Shijiazhuang, “Security, Privacy and Trust in the IoT Environment” Springer Publications, 2019.

CSCO 462 : INTRODUCTION TO CYBER SECURITY

Course Objectives :

1. To provide an introduction to the cybercrimes and cyber assets
2. To enlighten about the need for comprehensive treatment to the cybersecurity risks and controls

Course Outcomes :

1. Student gets the ability to decipher the complex field of cybersecurity
2. Student realises that the cybersecurity challenge is not merely a technology one, but more of a managerial one in nature.

UNIT I

INTRODUCTION TO CYBERCRIME : Cybercrime - Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cyber Crimes, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens, Cyber Offences: How Criminals Plan Them, How Criminals Plan the Attacks, Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing. Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices

(12 Hours)

UNIT II

Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organisations, Organisational Measures for Handling Mobile, Organisational Security Policies and Measures in Mobile Computing Era, Laptops. TOOLS AND METHODS USED IN CYBERCRIME : Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan-horses and Backdoors, Steganography, DoS and DDoS At-tacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction to Phishing, Identity Theft (ID Theft).

(12 Hours)

UNIT III

UNDERSTANDING COMPUTER FORENSICS : Introduction, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics. Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Anti Forensics.

(12 Hours)

Textbooks :

1. Sunit Belapure and Nina Godbole, “Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives”, Wiley India Pvt Ltd, ISBN: 978-81-265-21791, Publish Date 2013.
2. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, KLSI. “Introduction to information security and cyber laws”. Dreamtech Press. ISBN: 9789351194736, 2015.
3. Thomas J. Mowbray, “Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions”, Copyright © 2014 by John Wiley & Sons, Inc

Semester - III

CSCH 501: DIGITAL FORENSICS

Course Objectives :

1. To make the student aware of the need to perform forensic of the computer and digital devices from the point of forensic investigation.
2. To make the student aware of the procedures required to keep the digital trail of

crimes, in the modern world

Course Outcomes :

1. Student gets the skills required to preserve the digital trail of crimes, both computer crimes and conventional crimes
2. Student gets the skill required to perform the forensic investigation in line with the legal framework of the nation

UNIT I

Introduction To Digital Forensics : Introduction, Evolution Of Computer Forensics, Stages Of Computer Forensics Process, Benefits Of Computer Forensics, Uses Of Computer Forensics, Objectives Of Computer Forensics, Role Of Forensics Investigator, Forensics Readiness, Computer Forensics Investigation Process : Introduction To Computer Crime Investigation, Assess The Situation, Acquire The Data, Analyse The Data, Report The Investigation, Digital Evidence And First Responder Procedure, Digital Evidence, First Responder Toolkit, Issues Facing Computer Forensics, Types Of Investigation, Techniques Of Digital Forensics

(16 Hours)

UNIT II

Understanding Storage Media And File System : Hard Disk Drive, Details Of Internal Structure Of Hdd, The Booting Process, File System, Windows Forensics : Introduction, Recovering Deleted Files And Partitions, More About Recovering Lost Files/Data, Logs & Event Analysis And Password Cracking : Introduction, Windows Registry, Windows Event Log File, Windows Password Storage, Application Passwords Crackers, Network Forensics : Introduction, Network Components And Their Forensics Importance, Osi, Forensics Information From Network, Log Analysis, Forensics Tools, Wireless Attacks : Introduction, 4.3wireless Fidelity (Wi-fi)(802.11), Wireless Security, Wireless Attacks Detection Techniques, Wireless Intrusion Detection Systems

(16 Hours)

UNIT III

Investigating Web Attacks : Introduction, Types Of Web Attacks, Web Attack Forensics, Web Application Forensics Tools, Investigating Email Attacks : Introduction, Email Attacks And Crimes, Privacy In Emails, Email Forensics, Email Forensic Tools, Mobile Device Forensics : Introduction, Challenges In Mobile Forensics, Mobile Communication, Evidences In A Mobile Device, Mobile Forensic Process, Forensic Acquisition Tools, Investigative Reports, Expert Witness And Cyber Regulations : Introduction, Report Preparation, Legal Aspects Of Computing

(16 Hours)

Textbooks :

1. “Digital Forensics”, Dr.Jeetendra Pande, Dr. Ajay Prasad, Uttarakhand Open

University, Haldwani - 2016

2. “Computer Forensics and Cyber Crime An Introduction”- Marjie T. Britz, Pearson, Third Edition, 2013
3. “Learning Python for Forensics - Leverage the power of Python in forensic investigations”, Preston Miller, Chapin Bryce, Packt Publishing, Second Edition, 2019
4. “A Practical Guide to Computer Forensics Investigations”, Dr. Darren R. Hayes, Pearson Education, 2015

CSCH 502 : ETHICAL HACKING

Course Objectives :

1. To make the student aware of the need to hack one’s own systems and networks, ethically.
2. To understand the availability of tools available for ethical hacking

Course Outcomes :

1. Student gets the most sought after skill in cybersecurity and IT audits
2. Student gets the knowledge of how delicate is the situation of security of our cyber assets and therefore the need to implement security

UNIT I

Introduction to Ethical Hacking, Footprinting & Reconnaissance, Scanning Networks, Enumeration, Vulnerability Analysis.

(16 Hours)

UNIT II

System Hacking, Malware Threats, Sniffing, Social Engineering, Denial-of-Services, Session Hijacking, Evading IDS, Firewall & Honeypots.

(16 Hours)

UNIT III

Hacking Web Servers, Hacking Web Applications, SQL Injection, Hacking Wireless Networks, Hacking Mobile Platforms, IoT Hacking, Cloud Computing.

(16 Hours)

Textbooks :

1. “CEH V10 EC-Council Certified Ethical Hacker”, Nouman Ahmed Khan, Abubakar Saeed, Muhammad Yousuf
2. “CEH v10 TM Certified Ethical Hacker Study Guide”, Ric Messier, Sybex, 2019
3. “Hack proofing your network “, Ryan Russell, Syngress, 2002

4. “Network and System Security”, John R. Vacca, Syngress, 2010

CSCH 503 : INTRODUCTION TO BLOCKCHAIN

Course Objectives :

1. To make the student aware of the distributed ledger system which has the ability disrupt all walks of modern economy
2. To make the student aware of different blockchains existing and the differences between them

Course Outcomes :

1. Student gets the knowledge of choosing the right blockchain infrastructure for the business problem in hand
2. Student gets the knowledge of legal acceptance of the cryptocurrencies and pitfalls of the wrong use of them

UNIT I

Introducing Blockchain and Ethereum : Introduction to blockchain, Internet versus blockchain, How blockchain works, The building blocks of blockchain, Ethereum, Private vs Public Blockchain, Business adaptation. Introduction to Solidity Programming

(16 Hours)

UNIT II

Hyperledger, the Blockchain for Businesses : Technical requirements, Hyperledger overview, Blockchain-as-a-service (BaaS), Architecture and core components, Hyperledger Fabric model, Bitcoin versus Ethereum versus Hyperledger, Hyperledger Fabric capabilities, Blockchain on the CIA Security Triad : Understanding blockchain on confidentiality, Blockchain on integrity, Understanding blockchain on availability, Deploying PKI-Based Identity with Blockchain : PKI, Challenges of the existing PKI model, How blockchain can help, Two-Factor Authentication with Blockchain: Introduction to 2FA, Blockchain for 2FA

(16 Hours)

UNIT III

Blockchain-Based DNS Security Platform : Understanding DNS components, DNS structure and hierarchy, DNS topology for large enterprises, Challenges with current DNS, Blockchain-based DNS solution, Deploying Blockchain-Based DDoS Protection : DDoS attacks, Types of DDoS attacks, Challenges with current DDoS solutions, How blockchain can transform DDoS protection, Facts about Blockchain and Cyber Security: Decision path for blockchain, Leader's checklist, Challenges with blockchain, The future of cybersecurity with blockchain

(16 Hours)

Textbooks :

1. “Hands-On Cybersecurity with Blockchain”, Rajneesh Gupta, Packt Publishing, 2018
2. “Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions”, Joseph J. Bambara Paul R. Allen, McGraw-Hill Education, 2018
3. “Blockchain Enabled Applications”, Vikram Dhillon, David Metcalf, Max Hooper, Apress, 2017
4. “Blockchain Blueprint for a New Economy”, Melanie Swan, O’Reilly Media, 2015
5. “Blockchain Basics: A Non-Technical Introduction in 25 Steps”, Daniel Drescher, Apress, 2017

CSCS 505 : INTRUSION DETECTION SYSTEM

Course Objectives :

1. To make the student aware of the latest IDS systems available in the market
2. To make the student aware of the tradeoffs while designing and implementing an IDS

Course Outcomes :

1. Student gets the skills required to work with latest IDS systems
2. Student gets the knowledge of tradeoffs required to work with latest IDS systems

UNIT I

History of Intrusion detection, Audit, Concept - definition, Internal and external threats to data, attacks, need and types of IDS, Information sources, Host based information sources, Network based information sources. Intrusion Prevention Systems, Network IDs protocol-based IDs, Hybrid IDs, Analysis schemes, thinking about intrusion, A model for intrusion analysis, techniques.

(12 Hours)

UNIT II

Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options, Step-By-Step Procedure to Compile and Install Snort, Location of Snort Files, Snort Modes, Snort Alert Modes. Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL Using ACID and SnortSnarf with Snort.

(12 Hours)

UNIT III

Securing database-to-database communications : Monitor and limit outbound communications, Secure database links and watch for link-based elevated privileges, Protect link usernames and passwords, Monitor usage of database links, Secure replication mechanisms, Map and secure all data sources and sinks, Trojans : The four types of database Trojans, Baseline calls to stored procedures and take action on Divergence, Control creation of and changes to procedures and triggers, Watch for changes to run-as privileges, Closely monitor developer activity on production environments, Monitor creation of traces and event monitors, Monitor and audit job creation and scheduling, Be wary of SQL attachments in emails.

(12 Hours)

Textbooks :

1. Rebecca Gurley Base "Intrusion Detection" MacMillan Technology Series (MTP Series)
2. Rafeeq Rehman "Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID", Prentice Hall PTR, 2003.
3. RonBen Natan, Implementing Database Security and Auditing, Elsevier, Indian reprint,.

CSCS 506 : CYBER LAWS

Course Objectives :

1. To make the student aware about the legal aspects of our actions in cyberspace.
2. To make the student aware about the punishments for cyber offences

Course Outcomes :

1. Students get the required frame of mind to work in an IT powered workplace and all walks of life.
2. Student gets the knowledge of the need to protect the data privacy of the clients

UNIT I

The Information Technology Act (IT Act), 2000 : Preliminary, Digital Signature And Electronic Signature, Electronic Governance, Attribution, Acknowledgement And Despatch Of Electronic Records, Secure Electronic Records And Secure Electronic Signature, Regulation Of Certifying Authorities, Electronic Signature Certificates, Duties Of Subscribers, Penalties, Compensation And Adjudication, The Appellate Tribunal, Offences, Intermediaries Not To Be Liable In Certain Cases, Examiner Of Electronic Evidence, Miscellaneous, Amendments As Introduced By The IT Amendment Act, 2008, Amendments to Indian Penal Code, Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 due IT Act 2000

(12 Hours)

UNIT II

Personal Data Protection Bill (PDPB), 2019: Preliminary, Obligations Of Data Fiduciary, Grounds For Processing Of Personal Data Without Consent, Personal Data And Sensitive Personal Data Of Children, Rights Of Data Principal, Transparency And Accountability Measures, Restriction On Transfer Of Personal Data Outside India, Exemptions, Data Protection Authority Of India, Penalties And Compensation, Appellate Tribunal, Finance, Accounts And Audit, Offences, Miscellaneous

(12 Hours)

UNIT III

General Data Protection Regulation (GDPR), 2018 of European Union : General provisions, Principles, Rights of the data subject, Controller and processor, Transfers of personal data to third countries or international organisations, Independent supervisory authorities, Cooperation and consistency, Remedies, liability and penalties, Provisions relating to specific processing situations, Delegated acts and implementing acts, Final provisions.

(12 Hours)

Textbooks :

1. "The Information Technology Act", 2000
2. "The Personal Data Protection Bill", 2019
3. "General Data Protection Regulation(GDPR)"- Official Journal of the European Union, 2016, https://gdpr-info.eu/
4. "The Information Technology ACT", 2008
5. "A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians"- Expert Committee Report under the Chairmanship of Justice B.N. Srikrishna, 2018
6. "Computer Forensics and Cyber Crime An Introduction"- Marjie T. Britz, Pearson, Third Edition, 2013

CSCS 507 : APPLICATION SECURITY

Course Objectives :

1. To make the student aware of the ned to create secured applications
2. To make the student aware of the need to enforce security concerns while developing and testing applications

Course Outcomes :

1. Student gets the security architectures needed while developing the softwares
2. Student gets the knowledge of different attack vectors which are to be taken care of while designing applications

UNIT I

Secure Application Design: Secure Development Lifecycle, Application Security Practices, Web Application Security, Client Application Security, Remote Administration Security. Writing Secure Software: Security Vulnerabilities: Causes and Prevention, Buffer Overflows, Integer Overflows, Cross-Site Scripting, SQL Injection, Whitelisting vs. Blacklisting. J2EE Security: Java and J2EE Overview, The J2EE Architecture, Servlets, Authentication and Authorization, Protocols

(12 Hours)

UNIT II

Windows .NET Security: Core Security Features of .NET, Application-Level Security in .NET. Controlling Application Behaviour: Controlling Applications on the Network, Restricting Applications Running on Computers. Security Operations: Communication and Reporting, Change Management, Acceptable Use Enforcement, Administrative Security, Management Practices, Accountability Controls, Keeping Up with Current Events, Incident Response

(12 Hours)

UNIT III

Disaster Recovery, Business Continuity, Backups, and High Availability: Disaster Recovery, Business Continuity Planning, Backups, High Availability, Compliance with Standards. Incident Response and Forensic Analysis: Incident Response, Forensics, Compliance with Laws During Incident Response.

(12 Hours)

Textbooks :

1. Information Security: The Complete Reference by Mark Rhodes-Ousley
2. Web Application Security: Exploitation and Countermeasures for Modern Web Applications 1st Edition by Andrew Hoffman
3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition by Dafydd Stuttard

CSCS 508 : BIG DATA ANALYTICS

Course Objectives :

1. To make the student aware of the need to analyse the huge volumes of data connected to cyberspace.
2. To make the student aware of the value of the varieties of data in all walks modern life

Course Outcomes :

1. Student gets the right skills required to handle complex data
2. Student gets the knowledge to make right choice of algorithms and technologies for big data analytics

UNIT I

Applying Big data into different Cyber Security aspects: The Power of Big Data in Cybersecurity, Big Data for Network Forensics, Dynamic Analytics-Driven Assessment of Vulnerabilities and Exploitation, Root Cause Analysis for Cybersecurity, Data Visualisation for Cybersecurity, Cybersecurity Training.

(12 Hours)

UNIT II

Machine Unlearning: Repairing Learning Models in Adversarial Environments, Big data in emerging cybersecurity domains : Big Data Analytics for Mobile App Security, Security, Privacy, and Trust in Cloud Computing, Cybersecurity in Internet of Things (IoT), Big Data Analytics for Security in Fog Computing

(12 Hours)

UNIT III

Analysing Deviant Socio-Technical Behaviours Using Social Network Analysis and Cyber Forensics-Based Methodologies, Tools and Datasets for Cybersecurity : Security Tools, Data and Research Initiatives for Cybersecurity Analysis.

(12 Hours)

Textbooks :

1. "Big Data Analytics in Cybersecurity", Onur Savas, Julia Deng, CRC Press, 2017
2. "Data Analytics and Decision Support for Cybersecurity", Iván Palomares Carrascosa, Harsha Kumara Kalutarage, Yan Huang, Springer, 2017
3. "Darkweb Cyber Threat Intelligence Mining", John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath, Jana Shakarian, Paulo Shakarian, Cambridge University Press, 2017
4. "Data Analysis for Network Cyber-Security", Niall Adams, Nicholas Heard, Imperial College Press, 2014

CSCO 512 : CYBER LAWS

Course Objectives :

1. To make the student aware about the legal aspects of our actions in cyberspace.
2. To make the student aware about the punishments for cyber offences

Course Outcomes :

1. Student gets the required frame of mind to work in a IT powered workplace and all walks of life.
2. Student gets the knowledge of the need to protect the data privacy of the clients

UNIT I

The Information Technology Act (IT Act), 2000 : Preliminary, Digital Signature And Electronic Signature, Electronic Governance, Attribution, Acknowledgement And Despatch Of Electronic Records, Secure Electronic Records And Secure Electronic Signature, Regulation Of Certifying Authorities, Electronic Signature Certificates, Duties Of Subscribers, Penalties, Compensation And Adjudication, The Appellate Tribunal, Offences, Intermediaries Not To Be Liable In Certain Cases, Examiner Of Electronic Evidence, Miscellaneous, Amendments As Introduced By The IT Amendment Act, 2008, Amendments to Indian Penal Code, Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 due IT Act 2000.

(12 Hours)

UNIT II

Personal Data Protection Bill (PDPB), 2019: Preliminary, Obligations Of Data Fiduciary, Grounds For Processing Of Personal Data Without Consent, Personal Data And Sensitive Personal Data Of Children, Rights Of Data Principal, Transparency And Accountability Measures, Restriction On Transfer Of Personal Data Outside India, Exemptions, Data Protection Authority Of India, Penalties And Compensation, Appellate Tribunal, Finance, Accounts And Audit, Offences, Miscellaneous

(12 Hours)

UNIT III

General Data Protection Regulation (GDPR), 2018 of European Union : General provisions, Principles, Rights of the data subject, Controller and processor, Transfers of personal data to third countries or international organisations, Independent supervisory authorities, Cooperation and consistency, Remedies, liability and penalties, Provisions relating to specific processing situations, Delegated acts and implementing acts, Final provisions.

(12 Hours)

Textbooks :

1. “The Information Technology Act”, 2000
2. “The Personal Data Protection Bill”, 2019

3. "General Data Protection Regulation(GDPR)"- Official Journal of the European Union, 2016, https://gdpr-info.eu/
4. "The Information Technology ACT", 2008
5. "A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians"- Expert Committee Report under the Chairmanship of Justice B.N. Srikrishna, 2018
6. "Computer Forensics and Cyber Crime An Introduction"- Marjie T. Britz, Pearson, Third Edition, 2013

CSCO 513 : Ethical Hacking and Digital Forensics

Course Objectives :

1. To make the student aware of the need to ethically hack one's own systems and network to know the loopholes.
2. To make the student aware of the forensics which need to performed to produce digital trails of crimes in the modern world

Course Outcomes :

1. Student gets the skills and the knowledge of the tools required for performing ethical hacking and the digital forensics
2. Student gets the legal architecture of the nation which needs to be observed while performing ethical hacking and digital forensic

UNIT I

HACKING WINDOWS : Network Hacking, Web Hacking, Common Network Hacking Techniques, Password hacking, Cracking Passwords, Input Validation Attacks, SQL Injection Attacks, Buffer overflow attacks, Privacy Attacks, **TCP / IP AND FIREWALLS** : TCP/IP-Checksum, TCP / IP and Firewalls, IP Spoofing, Services Vulnerable to IP Spoofing, Port Scanning, DNS Spoofing, DNS ID Spoofing, DOS Attack, Application Level Attacks, Distributed Denial-of-Service Attacks (DDoS), DDoS Tools, UDP Flooding, Firewalls, Packet Filtering Firewall, Filtering on IP Header Criteria, Application Proxy Firewalls, Firewall's security policy, Batch File Programming

(12 Hours)

UNIT II

COMPUTER FRAUD: Insider Threat Concepts, Insider Threat Study, Methodology for the Optimization of Resources in the Detection of Computer Fraud, Managing the Insider Threat, The Insider Threat Strategic Planning Process, Cyber-Security Risk Governance Processes for Web-Based Application Protection (Understanding the External Risks and Internal Information Security Risks), The Risk Management Process, The Tailored Risk Integrated Process (TRIP), Security Controls in Application Systems Controls (ISO 27001, The Strategic Planning Process for Reducing the Insider Threat, The Threat Assessment Matrix, Application and Code Review, Strategic, Legal/Regulatory, and Operational Risk Ratings, The Information Security Scorecard, Develop Security Patterns for Applications/ Systems Software Engineering (Process and Product Improvements), Implemented Software Engineering InfoSec Process and Product Improvements

(12 Hours)

UNIT III

ARCHITECTURE STRATEGIES: Architecture strategies for computer fraud prevention, Architectural Strategies to Prevent and Detect ICF, Intrusion Detection Systems, NIDS-Network Intrusion Detection Systems, Host-Based Intrusion Detection Systems (HIDS), The Penetration Testing Process, Web Services-Reducing Transaction risks, Extensible Mark-up Language (XML), XML and Security, Simple Object Access Protocol (SOAP), Problems with Web Services Security, **FRAUD SELECTION & DETECTION**: Key Fraud Indicator selection process, Macro Computer Fraud Taxonomy, Key fraud signature selection process, Accounting Forensics, Computer Forensics, Journaling and its requirements, The National Industrial Security Program Operating Manual (NISPOM), Journaling Risk/Controls Matrix, Standardised Logging Criteria for Forensic Photo Frames, Neural networks – Misuse detection and Novelty detection

(12 Hours)

Textbooks :

1. Kenneth C.Brancik, Insider Computer Fraud, Auerbach Publications Taylor & Francis, Group 2008.
2. Ankit Fadia, Ethical Hacking, Second Edition Macmillan India Ltd, 2006.
3. https://healholistic.files.wordpress.com/2013/08/batch-file-programming-ankit-fadia.pdf. 4. https://www.princeton.edu/~rblee/ELE572F02presentations/DDoS.pp
4. Permission to reproduce extracts from BS ISO/IEC/2700: 2005 is granted by BSI.British Standards can be obtained in PDF format from the BSI Online Shop: http://www.BS l-Global.com/en/shop
5. GTAG (Global Technology Audit Guide), Application Based Controls. The Institute of Internal Auditors, 2005.
6. The FFIEC Information Security Booklet, 2006.
7. Komanosky, Sasha. Enterprise Security Patterns, June 2004. The original source for the security pattern was the 3/03I SSA Password/Journal Enterprise Security Patterns
8. Caudill, Maureen and Butler, Charles, Naturally Intelligent Systems, MIT Press, Cambridge, MA, 1992. 9. Hawkins, Jeff, On Intelligence, Times Books, Henry Holt, New York, 2004.
9. Saffron Technologies, Technical White Paper, Morrisville, NC, 2004 (www.saffrontech.com). 11. Nigrini, Mark, Fraud Detection—I've Got Your Number. Journal of Accountancy, May, 79–83, 1999.