ಮಂಗಳೂರು ವಿಶ್ವವಿದ್ಯಾನಿಲಯ

MANGALORE UNIVERSITY

(Accredited by NAAC)

ಕ್ರಮಾಂಕ/ No. : MU/ACC/CR 17/2021-22/A2

ಕುಲಸಚಿವರ ಕಛೇರಿ
ಮಂಗಳಗಂಗೋತ್ರಿ – 574 199
Office of the Registrar
Mangalagangothri – 574 199
ದಿನಾಂಕ/Date:13.12.2021

NOTIFICATION

Sub: Revised syllabus of M.Sc. Cyber Security programme.
Ref: Academic Council approval vide agenda
No.: ಎಸಿಸಿ:ಶೈ.ಸಾ.ಸ.2: 10(2021–22) dtd 27.10.2021.

*****

The Revised syllabus of M.Sc. Cyber Security programme which is approved by the Academic Council at its meeting held on 27.10.2021 is hereby notified for implementation with effect from the academic year 2021-22.

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

REGISTRAR

To,

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

M.Sc. in Cyber Security Programme Structure

Semester I		
Sl. No	**Course Name**	**Credits**
Hard Core		
1	CSCH 401 : Introduction to Cybersecurity	4
2	CSCH 402 :Unix and Shell Programming	4
3	CSCH 403 : Data Structure	4
Soft Core		
4	CSCS 404 : Mathematical Foundations	3
5	CSCS 405 : Problem Solving using Python	
6	CSCS 406 : E-Commerce and E-Governance	
7	CSCS 407 : Computer Networks	
8	CSCS 408 : Foundation of Cryptography	
Practicals		
9	CSCP 409 : Data Structures Laboratory	2
10	CSCP 410 : Unix & 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 Communication	4
Soft Core		
4	CSCS 454 : Design of Cryptographic Algorithms	3
5	CSCS 455 : Cyber Threat Intelligence	
6	CSCS 456 : Cloud Computing and Security	
7	CSCS 458 : Internet of Things	
Practicals		
8	CSCP 459 : Network Security Laboratory	2
9	CSCP 460 : Data 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 Cybersecurity	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	
5	CSCS 506 : Cyber Laws	
6	CSCS 507 : Application Security	3
7	CSCS 508 : Big Data Analytics	
Practicals		
8	CSCP 509 : Ethical Hacking Laboratory	2
9	CSCP 510 : Block Chain Technology Laboratory	2
Seminar		
10	CSCS 511: Seminar on latest trends and techniques in Cybersecurity	1
Open Choice		
11	CSCO 512 : Cyber Laws	3
	Total	**26**

Semester IV		
Sl No	**Course Name**	**Credits**
1	CSCH 551 : Industry Internship / Project Work	18

Credit Distribution

Semester	Main Course Credits	Open Choice Credits
I	22	0
II	23	03
III	23	03
IV	18	0
Total	86	06
-	**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	Unix and Shell Programming	04	04	3 hours	30	70	100
CSCH 403	Data Structures	04	04	3 hours	30	70	100
Soft Core (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 andE-Governance	03	03	3 hours	30	70	100
CSCS 407	Computer Networks	03	03	3 hours	30	70	100
CSCS 408	Foundations of Cryptography	03	03	3 hours	30	70	100
Practicals							
CSCP 409	Data Structures Laboratory	02	04	03 hours	30	70	100
CSCP 410	Unix and Shell Programming Laboratory	02	04	03 hours	30	70	100
Total		**-**	**-**	**-**	**210**	**490**	**700**

Semester II

Course Code	Title of the Course	Credits	Hours per week	Duration of the Exam	Marks		
					IA	Exam	Total
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
Soft Core							
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	Design and Analysis of Algorithms Laboratory	02	04	03 hours	30	70	100
Seminar							
CSCS 461	Seminar on latest trends and techniques in Cybersecurity	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

Course Code	Title of the Course	Credits	Hours per week	Duration of the Exam	Marks		
					IA	Exam	Total
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
Soft core (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	Block Chain Technology Laboratory	02	04	03 hours	30	70	100
Seminar							
CSCS 511	Seminar on latest trends and techniques in Cybersecurity	01	01	-	15	35	50
Open Choice							
CSCO 512	Cyber Laws	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 Objective:

The objective of the courses to

1) To understand the authentication controls and security operations
2) To understand the fundamental functioning of security patterns.

UNIT I

The Importance of Cybersecurity Management: The Growing Pains of an Emerging Discipline, Understanding the Costs and Benefits of cybersecurity management to an Organization, Two Absolute Rules for Cybersecurity Work, Implementing a Strategic Response, **Control-Based Information Governance:** The Value of Formal Control, Organizing Things into a Rational Process, Information Audit and Control, Control Principles, **A Survey of Control Frameworks:** COSO Framework, IT Infrastructure Library Framework, ISO 27001, COBIT 5, IT Security Controls**,** General Structure and Applications. **(16 hours)**

UNIT II

The Importance of Controls: Goal-Based Security Controls, Implementation-Based Security Controls, The Security Control Formulation and Development Process, Control Implementation through Security Architecture Design, **Implementing a Multitiered Governance and Control Framework in a Business :** Constructing Practical Systems of Controls, Building the Security Control System, Initial Setup and Tradeoffs, **Risk Management and Prioritization Using a Control Perspective:** Five Elements of the Risk Management Process, Risk Management Plan, Implementing a Managed Risk Control Process, Planning for Effective Risk Management, Writing the Risk Management Plan, Risk Management Controls, Evaluating the Overall Policy Guidance **(16 hours)**

UNIT III

Control Formulation and Implementation Process: The Control Formulation Process**,** Creating and Documenting Control Objectives, Creating a Management-Level Control Process, Measurement-Based Assurance of Controls, **Security Control Validation and Verification:** Security Control Assessment Fundamentals, NIST Security Control Assessment Process, Common Types of Operational and Technical Security Tests**,** Common Operational and Technical Security Examination Techniques**, Control Framework Sustainment and Security of Operations:** Operational Assurance, Response Management, Operational Oversight and Infrastructure Assurance of Control Set Integrity **(16 hours)**

Course Outcome:

At the end of the course student will be able to

1) Understand the basics of security patterns.
2) Understanding the enterprise security, risk management and control frameworks.

TextBooks

(1). "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

(2)."Securing an IT Organization through Governance, Risk Management, and

Audit", Ken Sigler, Dr. James L. Rainey, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016
(3). "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
(4). "Cybercrimes: A Multidisciplinary Analysis", SumitGhosh, Elliot Turrini, Springer, 2010

CSCH 402 – UNIX AND SHELL PROGRAMMING

Course Objective:
The objective of the courses to
1) Understand the fundamentals of Linux and Linux administration.
2) To learn Linux/Unix library, functions and system calls.

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. **(16hours)**

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. **(16hours)**

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.

(16hours)

Course Outcome:
At the end of the course student will be able to
1) Understand the Basics set of command and utilities in Linux/Unix.
2) Conceptualize the components involved in Linux security.

Text Books:

(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.

CSCH 403: DATA STRUCTURES

Course Objective:

The objective of the courses to

1) To understand the fundamentals of data structure.
2) Explore the knowledge on stacks, Linked list and queues.

UNIT 1

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 2

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 3

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**

Course Outcome:

At the end of the course student will be able to

1) Ability to analyze the algorithm and its correctness.

2) Ability to describe stack, queue and linked list operations.

Text Books:

1. Ellis Horowitz and SartajSahni, 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 Objective:

The objective of the courses to

1) Enable to understand and create mathematical argument and solving them with logical skills.
2) Understanding number theory, ciphers which are applied data security.

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)

Course Outcome:

At the end of the course student will be able to

1) Ability to apply logical and mathematical model in practical application.
2) Ability to employ theory concepts in designing efficient algorithms.

TextBooks:

(1). "Hardware Security Design, Threats, and Safeguards", DebdeepMukhopadhyayRajatSubhraChakraborty, CRC Press, 2015

(2). " Hardware IP Security and Trust", Prabhat Mishra, SwarupBhunia, Mark Tehranipoor,Springer, 2017

(3). "Fault Tolerant Architectures for Cryptography and Hardware Security", SikharPatranabisDebdeepMukhopadhyay, Springer, 2018

(4). "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

(5). "Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications", Basel Halak, Springer, 2018

(6). "Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography", Roger Dube, Wiley, 2008

CSCS 405 : PROBLEM SOLVING USING PYTHON

Course Objective:

The objective of the courses to

1) To understand basics of python from scratch
2) To strengthen the fundaments skills in Python.

UNIT I

Foundation: Computer hardware architecture, Understanding programming, The Way of the Program, The building blocks of programs, Writing a program, Variables, Variable names and keywords, Expressions and Statements, Operators and operands, String operations, Functions, Built-in functions, Type conversion functions, Conditionals and Recursion, Chained conditionals, Catching exceptions using try and except, Iteration, break & continue, Loop patterns. **(12 hours)**

UNIT II

Data Processing : Strings, String slices, String len functions, Looping and counting with strings, string methods, Format operator, Lists, List operations, Lists and functions, Lists and strings, Dictionaries, Dictionaries and files, Looping and dictionaries, Tuples, Tuple assignment, Using tuples as keys in dictionaries, Files, Text files and lines, Using try, except, and open. **(12 hours)**

UNIT III

Object Orientation : Managing Larger Programs, Classes as Types, Object Lifecycle, Our First Python Object, Fruitful Functions & void functions, Classes and Functions, Subdividing a Problem-Encapsulation, Many Instances, Classes and Methods, Inheritance, Debugging, Syntax errors, Runtime errors, Semantic errors.

(12 hours)

Course Outcome:

At the end of the course student will be able to

1) Understand the environmental setup and program basics.
2) Understand the data structure and data types in python.

Text Books:

(1). "Think Python: How to Think Like a Computer Scientist", Allen B. Downey, Second Edition, Green Tea Press, 2015.

(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 Objective:

The objective of the courses to

1) Understanding E-Commerce and E-Business framework
2) Have knowledge in different types of marketing and E-management.

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 Organizations, Work Organization in eTeams, The Knowledge Worker in a Knowledge Society, Measuring the Success of Intellectual Capital, Ethical Maxims for eTeams**.** **(12 hours)**

Course Outcome:

At the end of the course student will be able to

1) Understand the basic concepts and technology used in E-Commerce and E-Governance
2) Be aware of ethical, social and security issues.

TextBooks :

(1). "eBusiness&eCommerce- Managing the digital Value Chain", Andreas Meier, HenrikStormer, 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 Objective:

The objective of the courses to

1) Understand basics of computer network and reference models.
2) To understand types of protocol and its uses.

UNIT 1

Application Layer: Principles of Network Applications: Network Application Architectures, Processes Communicating, Transport Services Available to Applications, Transport Services Provided by the Internet, Application-Layer Protocols. The Web and HTTP: Overview of

HTTP, Non-persistent and Persistent Connections, HTTP Message Format, User-Server Interaction: Cookies, Web Caching, The Conditional GET, File Transfer: FTP Commands & Replies, Electronic Mail in the Internet: SMTP, Comparison with HTTP, Mail Message Format, Mail Access Protocols, DNS; The Internet's Directory Service: Services Provided by DNS, Overview of How DNS Works, DNS Records and Messages, Peer-to-Peer Applications: P2P File Distribution, Distributed Hash Tables, Socket Programming: creating Network Applications: Socket Programming with UDP, Socket Programming with TCP.

12 Hours

UNIT 2

Transport Layer : Introduction and Transport-Layer Services: Relationship Between Transport and Network Layers, Overview of the Transport Layer in the Internet, Multiplexing and Demultiplexing: Connectionless Transport: UDP,UDP Segment Structure, UDP Checksum, Principles of Reliable Data Transfer: Building a Reliable Data Transfer Protocol, Pipelined Reliable Data Transfer Protocols, Go-Back-N, Selective repeat, Connection-Oriented Transport TCP: The TCP Connection, TCP Segment Structure, Round-Trip Time Estimation and Timeout, Reliable Data Transfer, Flow Control, TCP Connection Management, Principles of Congestion Control: The Causes and the Costs of Congestion, Approaches to Congestion Control, Network-assisted congestion-control example, ATM ABR Congestion control, TCP Congestion Control: Fairness. **12 Hours**

UNIT 3

The Network layer: What's Inside a Router?: Input Processing, Switching, Output Processing, Where Does Queuing Occur? Routing control plane, IPv6,A Brief foray into IP Security, Routing Algorithms: The Link-State (LS) Routing Algorithm, The Distance-Vector (DV) Routing Algorithm, Hierarchical Routing, Routing in the Internet, Intra-AS Routing in the Internet: RIP, Intra-AS Routing in the Internet: OSPF, Inter/AS Routing: BGP, Broadcast Routing Algorithms and Multicast. **12 Hours**

Course Outcome:

At the end of the course student will be able to

1) Learns basic of Computer Networks
2) Understands reference model (OSI & TCP/IP models)

Textbooks:

1. James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth edition, Pearson,2017 .
2. Nader F Mir, Computer and Communication Networks, 2nd Edition, Pearson, 2014.

CSCS 408: FOUNDATIONS OF CRYPTOGRAPHY

Course Objective:

The objective of the courses to

1) Understanding the fundaments of cryptography and its applications.
2) Understanding security techniques used in cryptography.

UNIT I

Introduction and Classical Cryptography: Cryptography and Modern Cryptography, The Setting of Private-Key Encryption, Historical Ciphers and Their Cryptanalysis, The Basic Principles of Modern Cryptography, Perfectly-Secret Encryption : Definitions and Basic Properties, The One-Time Pad (Vernam's Cipher), Limitations of Perfect Secrecy Private-Key Cryptography: Private Key Encryption and Pseudo randomness, A Computational Approach to Cryptography, Defining Computationally-Secure Encryption, Pseudo

randomness, Constructing Secure Encryption Schemes. **(12 hours)**

UNIT II

Message Authentication Codes and Collision-Resistant Hash Functions: Secure Communication and Message Integrity, Encryption vs. Message Authentication, Constructing Secure Message Authentication Codes, Collision-Resistant Hash Functions, Practical Constructions of Pseudorandom Permutations (Block Ciphers): Substitution-Permutation Networks, Feistel Networks, DES – The Data Encryption Standard, AES – The Advanced Encryption Standard. **(12 hours)**

UNIT III

Public-Key (Asymmetric) Cryptography: Number Theory and Cryptographic Hardness Assumptions, Preliminaries and Basic Group Theory,Primes, Factoring, and RSA: Assumptions in Cyclic Groups, Cryptographic Applications of Number-Theoretic Assumptions, Private-Key Management and the Public-Key Revolution: Limitations of Private-Key Cryptography, A Partial Solution – Key Distribution Centers, The Public-Key Revolution, Diffie-Hellman Key Exchange, Public-Key Encryption, Hybrid Encryption, RSA Encryption, Digital Signature Schemes: RSA Signatures, The "Hash-and-Sign" Paradigm, Lamport's One-Time Signature Scheme, Public-Key Cryptosystems in the Random Oracle Model. **(12 hours)**

Course Outcome:

At the end of the course student will be able to

1) Learns basics and advanced techniques in cryptography.
2) Able to deal with symmetric and asymmetric cryptography management.

Text Books:

(1). "Introduction to Modern Cryptography", Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008

(2). "Foundations of Cryptography - Basic Tools", OdedGoldreich, Cambridge University Press, 2004

(3). "Foundations of Cryptography - Basic Applications", OdedGoldreich, Cambridge University Press, 2009

SEMESTER – 2

CSCH 451 – DESIGN AND ANALYSIS OF ALGORITHMS

Course Objective:

The objective of the courses to

1) Describes fundamentals of design and analysis of Algorithms.
2) Derive, solve and describes performance of different algorithmic approach.

UNIT I

Introduction to algorithms: Books and algorithms, Fibonacci numbers, Big-O notation, **Algorithms with numbers:** Basic arithmetic, Modular arithmetic, Primality testing, Cryptography, Universal hashing, Randomized algorithms**, Divide-and-conquer algorithms:** Multiplication, Recurrence relations, Mergesort, Medians, Matrix multiplication, Fast Fourier transform,**Decompositions of graphs:** The need of graphs, Depth-first search in undirected graphs, Depth-first search in directed graphs. **(16 hours)**

UNIT II

Paths in graphs: Distances, Breadth-first search, Lengths on edges, Dijkstra's algorithm, Priority queue implementations, Shortest paths in the presence of negative edges,Shortest paths in dags,**Greedy algorithms:** Minimum spanning trees, Huffman encoding **Dynamic programming:** Longest increasing subsequences, Knapsack, Chain matrix multiplication, Shortest paths, Independent sets in trees. **(16 hours)**

UNIT III

Linear programming and reductions: An introduction to linear programming, Flows in networks, Bipartite matching, Duality, Zero-sum games, The simplex algorithm, **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, P vs NP Problem, SAT solvers.

(16 hours)

Course Outcome:

At the end of the course student will be able to

1) Explain major algorithms and analysis
2) Explain greedy paradigm and explain when an algorithms call for it.

Textbooks:

(1) Algorithms - SanjoyDasgupta, Christos Papadimitriou and UmeshVazirani, TMH-2008
(2)Introduction to Algorithms – Thomas H.Cormen, Charles E. Leiserson, Ronald L Rivest,Clifford Stein, 3rd edition, The MIT Press, 2009
(3) Combinatorial Optimization : Algorithms and Complexity, Christos H. Papadimitriou, Kenneth Steiglitz

CSCH 452 - NETWORK SECURITY

Course Objective:

The objective of the courses to

1) Understanding the basics of networks and attacks on computer networks.
2) Exploration of commercial security tools.

UNIT 1

How To Hack Computer Network: Understanding the Current Legal Climate, The

Laws of Security: Client-Side Security Doesn't Work : Hacking Firewalls, Evading IDS Can, Insecurity Secret Cryptographic Algorithms, password to protect password in client side, **Classes of Attack:** Denial of Service, Information Leakage, Symbolic Link Attacks, Attacks against Special Files, Attacks against Databases, Identifying Methods of Testing for Vulnerabilities, Methodology, Diffing, Cryptography, Unexpected Input, Buffer Overflow, Format Strings. **(16 hours)**

UNIT II

Sniffing: Obtaining Authentication Information, Popular Sniffing Software, Advanced Sniffing Techniques, Exploring Operating System APIs, Taking Protective Measures, Employing Detection Techniques **Session Hijacking:** Understanding Session Hijacking, Examining the Available Tools, Playing MITM for Encrypted Communications, **Spoofing:** Attacks on Trusted Identity, The Evolution of Trust, Establishing Identity within Computer, Capability Challenges, Desktop Spoofs, Impacts of Spoofs, **Tunneling:** Strategic Constraints of Tunnel Design, Designing End-to-End Tunneling Systems, Port Forwarding: Accessing Resources on Remote Networks, Hardware Hacking, Viruses, Trojan Horses, and Worms. **(16 hours)**

UNIT III

IDS Evasion: Using Packet Level Evasion, Using Application Protocol Level Evasion, **Automated Security Review and Attack Tools** : Exploration of the Commercial automated security Tools, Reporting Security Problems. **(16 hours)**

Course Outcome:

At the end of the course student will be able to

1) Understanding the basic knowledge on network security and risk management.
2) Understanding different attack and tools.

Text Books

(1). "Hack proofing your network ", Ryan Russell, Syngress, 2002
(2). "Network and System Security", John R. Vacca, Syngress, 2010
(3). "COMPUTER NETWORKS, A Systems Approach", Larry L. Peterson & Bruce S. Davie, Third Edition, Morgan Kaufmann Publishers, 2003
(4). "Computer Networks" , Andrew S. Tanenbaum David J. Wetherall, Fifth Edition, Pearson Education Limited 2014

CSCH 453 : DATA COMMUNICATIONS

Course Objective:

The objective of the courses to

1) Understanding how communication works in data networks.
2) Understands role of protocols in communication.

UNIT I

Foundation: Building a Network, Requirements: Connectivity, Cost-Effective Resource Sharing, Support for Common Services, Network Architecture: Layering and Protocols, OSI Architecture, Internet Architecture, Implementing Network Software: Application Programming Interface (Sockets), Example Application, Protocol Implementation Issues, Performance: Bandwidth and Latency, Delay × Bandwidth Product, High-Speed Networks, Application Performance Needs. **(16 hours)**

UNIT II

Direct Link Networks : Hardware Building Blocks: Nodes, Links, Encoding (NRZ, NRZI, Manchester, 4B/5B), Framing : Byte-Oriented Protocols (BISYNC, PPP, DDCMP), Bit-Oriented Protocols (HDLC), Clock-Based Framing (SONET), Error Detection:Two-Dimensional Parity, Internet Checksum Algorithm, Cyclic Redundancy Check, Reliable Transmission : Stop-and-Wait, Sliding Window, Concurrent Logical Channels, , Ethernet (802.3): Physical Properties, Access Protocol, Experience with Ethernet, Token Rings (802.5, FDDI): Physical Properties, Token Ring Media Access Control, Token Ring Maintenance, Frame Format, Wireless (802.11):Physical Properties, Collision Avoidance, Distribution System, Frame Format, Network Adaptors. **(16 hours)**

UNIT III

Packet Switching : Switching and Forwarding : Datagrams, Virtual Circuit Switching, Source Routing, Bridges and LAN Switches: Learning Bridges, Spanning Tree Algorithm, Broadcast and Multicast, Limitations of Bridges, Cell Switching (ATM): Cells, Segmentation and Reassembly, Virtual Paths, Physical Layers for ATM, ATM in the LAN, Implementation and Performance. **(16 hours)**

Course Outcome:

At the end of the course student will be able to

1) Recognize different networking devices and its functions.
2) Designing network requirements for data communication.

TextBooks:

(1). "Computer Networks, A Systems Approach", Larry L. Peterson & Bruce S. Davie, Third Edition, Morgan Kaufmann Publishers, 2003

(2). "Computer Networks" , Andrew S. Tanenbaum David J. Wetherall, Fifth Edition, Pearson Education Limited 2014

(3). "A Professional's Guide to Data Communication in a TCP/IP World", E. Bryan Carne, Artech House Inc, 2004

CSCS 454 - DESIGN OF CRYPTOGRAPHIC ALGORITHMS

Course Objective:

The objective of the courses to

1) To understand the fundamentals of Cryptography.
2) To understand the security techniques used in cryptography.

UNIT I

Primes, Factoring, and RSA, Assumptions in Cyclic Groups, Cryptographic Applications of Number-Theoretic Assumptions, **Private-Key Management and the Public-Key Revolution:** Limitations of Private-Key Cryptography, A Partial Solution – Key Distribution Centers, The Public-Key Revolution, Diffie-Hellman Key Exchange, Public-Key Encryption, Hybrid Encryption, RSA Encryption. **(12 hours)**

UNIT II

Digital Signature Schemes: RSA Signatures, The "Hash-and-Sign" Paradigm, Lamport's One-Time Signature Scheme, Public-Key Cryptosystems in the Random Oracle Model. **(12 hours)**

UNIT III

Hardware Design of the Advanced Encryption Standard (AES) : Algorithmic and

Architectural Optimizations for AES Design, Circuit for the AES S-Box, Implementation of the MixColumns Transformation, Reconfigurable Design for the Rijndael Cryptosystem, Single Chip Encryptor/Decryptor.

(12 hours)

Course Outcome:

At the end of the course student will be able to

1) Learns the fundamentals and development of cryptographic algorithms.
2) Understand hardware design of the advanced Encryption Standards.

TextBooks:

(1). "Hardware Security Design, Threats, and Safeguards", DebdeepMukhopadhyayRajatSubhraChakraborty, CRC Press, 2015

(2). "Hardware IP Security and Trust " ,Prabhat Mishra, SwarupBhunia, Mark Tehranipoor,Springer, 2017

(3). "Fault Tolerant Architectures for Cryptography and Hardware Security", SikharPatranabisDebdeepMukhopadhyay, Springer, 2018

(4). "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

(5). "Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications", Basel Halak, Springer, 2018

(6). "Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography", Roger Dube, Wiley, 2008

CSCS 455 - CYBER THREAT INTELLIGENCE

Course Objective:

The objective of the courses to

1) Understand the Fundamentals of Cyber threats
2) Understand the threats and prevention methods.

UNIT I

Moving to Proactive Cyber Threat Intelligence: Proactive Intelligence beyond the Deepweb and Darkweb, **Understanding Darkweb Malicious Hacker Forums:** Forum Structure and Community Social Organization. **(12 hours)**

UNIT II

Automatic Mining of Cyber Intelligence from the Darkweb, Analyzing 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. **(12hours)**

UNIT III

Using Game Theory for Threat Intelligence: Security Game Framework, Computational Complexity, Algorithms, **Application:** Protecting Industrial Control Systems, **Challenges and Environmental Characteristics.**

(12 hours)

Course Outcome:

At the end of the course student will be able to

1) Analysis and evaluate efficient methods, applications and challenges in threat intelligence.
2) Ability to evaluate effective detection and prevention methods.

TextBooks:

(1). "Darkweb Cyber Threat Intelligence Mining", John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, VivinPaliath, Jana Shakarian, Paulo Shakarian, Cambridge University Press, 2017
(2). "Cybercrimes: A Multidisciplinary Analysis", SumitGhosh, Elliot Turrini, Springer, 2010
(3). "Big Data Analytics in Cybersecurity", OnurSavas, Julia Deng, CRC Press, 2017
(4). "Data Analytics and Decision Support for Cybersecurity", IvánPalomaresCarrascosa, 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 Objective:

The objective of the courses to

1) Understand the basic concepts of cloud computing and its security.
2) To learn the fundamentals of cloud and its elements.

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 Center, 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)**

Course Outcome:

At the end of the course student will be able to

1) Understand basics and capabilities of cloud computing
2) Understand fundamentals of developing current and the future cloud computing security.

Text Books:

(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 Objective:

The objective of the courses to

1) Fundamentals of IoT and its security.
2) Learn how to manage IoT threat and its countermeasures.

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)**

Course Outcome:

At the end of the course student will be able to

1) Understand the concepts of IoT and its security.
2) Understand the IoT attacks, countermeasures and security life cycle.

Text Books:

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. ZaighamMahmood, Shijiazhuang, “Security, Privacy and Trust in the IoT Environment” Springer Publications, 2019.

CSCO 462 – INTRODUCTION TO CYBER SECURITY

Course Objective:

The objective of the courses to

1) Understand the fundamental s of cyber security and cyber crimes.
2) Understand the tools and methods in cybercrimes and understanding computer forensics.

UNIT - I

INTRODUCTION TO CYBERCRIME [1st TEXTBOOK]

Cybercrime- Definition and Origins of the WordCybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. (1.2-1.5,1.9,1.10)

Cyberoffenses: How Criminals Plan Them:How Criminals Plan the Attacks, Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing. (2.2-2.8)

CYBERCRIME:

Mobile and Wireless Devices:Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops. (3.13.12) **12 Hours**

UNIT - II

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. (4.1-4.12)

Phishing and Identity Theft: Introduction to Phishing, Identity Theft (ID Theft). (5.2,5.3)

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. (7.1,7.3-7.13) **12 Hours**

UNIT - III

Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Antiforensics. (7.14-7.19)

INTRODUCTION TO SECURITY POLICIES AND CYBER LAWS [2nd Textbook]

Need for An Information Security Policy, Information Security Standards – ISO, Introducing Various Security Policies and Their Review Process, Introduction to Indian Cyber Law, Objective and Scope of the IT Act, 2000, Intellectual Property Issues, Overview of Intellectual Property Related Legislation in India, Patent, Copyright, Law Related to Semiconductor Layout and Design, Software License. (4.1-4.11)

12 Hours

Course Outcome:

At the end of the course student will be able to

1) Understand the basic concepts of cyber security and cyber crimes.
2) Understand the security policies and cyber laws.

TEXTBOOKS:

1. SunitBelapure 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 PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla, KLSI. "Introduction to information security and cyber laws". Dreamtech Press. ISBN: 9789351194736, 2015.

REFERENCE BOOKS:

1. Thomas J. Mowbray, "Cybersecurity: Managing Systems, Conducting Testing, and
2. Investigating Intrusions", Copyright © 2014 by John Wiley & Sons, Inc, ISBN: 978 - 1-118 -84965 -1.
3. James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", CRC Press, 15-Dec 2010.
4. Anti- Hacker Tool Kit (Indian Edition) by Mike Shema, McGraw-Hill Publication.

SEMESTER III

CSCH 501: DIGITAL FORENSICS

Course Objective:

The objective of the courses to

1) Understanding the concepts of Digital forensics and mobile device forensics.
2) Getting in depth knowledge of volume analysis and file systems.

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, Analyze 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)

Course Outcome:

At the end of the course student will be able to

1) Knowledge on various web attacks and cybercrimes.
2) Investigating attacks and cybercrimes for collecting data.

Text Books:

(1). "Digital Forensics"- Dr.JeetendraPande, 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 Objective:

The objective of the courses to

1) Basic introduction to ethical hacking.
2) Exploreattacks and attack management.

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)**

Course Outcome:

At the end of the course student will be able to

1) Comprehensive knowledge in ethical hacking
2) Understand, analysis and evaluation of threats and tools.

TextBooks:

(1). "CEH V10 EC-Council Certified Ethical Hacker", Nouman Ahmed Khan, AbubakarSaeed,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 BLOCK CHAIN

Course Objective:

The objective of the courses to

1) Understanding and exploring the working of Block chain technology.
2) Understand and analyze the working of Hyperledger and PIC I based identity.

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)**

Course Outcome:

At the end of the course student will be able to

1) Ability to understand the fundamentals of block chain and solidity programming.
2) Ability to apply the learning of solidity and decentralized apps in ethereum

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", VikramDhillon, 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 Objective:

The objective of the courses to

1) Basic concepts of intrusion detection system
2) Understanding and application of threat detection and prevention.

UNIT - I

Chapter 2: History of Intrusion detection, Audit, Concept and 2.1- definition, Internal and external threats to data, attacks, 2.3 - need and types of IDS, 2.3.7 - Information sources, 2.3.7.2 - Host based information sources, 2.3.7.1- 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

[1st Reference book]

Chapter 1: Introduction to Snort, Chapter 2: 2.1 - Snort Installation Scenarios, 2.2- Installing Snort, 2.3 - Running Snort on Multiple Network Interfaces, 2.4 - Snort Command Line Options, 2.5- Step-By-Step Procedure to Compile and Install Snort, 2.6 - Location of Snort Files, 2.7 - Snort Modes, 2.8 - Snort Alert Modes.
Chapter 3: Working with Snort Rules, 3.5 - Rule Headers, 3.6 - Rule Options, 3.7 - The Snort Configuration File etc. Chapter 4: Plugins, Preprocessors and Output Modules, Chapter 5: Using Snort with MySQL Chapter 6: Using ACID and SnortSnarf with Snort. **12 Hours**

UNIT - III

[2nd Reference book]

Chapter 8 : Securing database-to-database communications : 8.1 - Monitor and limit outbound communications , 8.2 - Secure database links and watch for link-based elevated privileges, 8.3 - Protect link usernames and passwords, 8.4 - Monitor usage of database links, 8.5 - Secure replication mechanisms, 8.6 - Map and secure all data sources and sinks, Chapter 9: Trojans : 9.1 - The four types of database Trojans, 9.2 - Baseline calls to stored procedures and take action on Divergence, 9.3 - Control creation of and changes to procedures and triggers, 9.4 - Watch for changes to run-as privileges, 9.5 - Closely monitor developer activity on production environments, 9.6 - Monitor creation of traces and event monitors, 9.7 - Monitor and audit job creation and scheduling, 9.8 - Be wary of SQL attachments in e-mails.
12 Hours

Course Outcome:

At the end of the course student will be able to

1) Obtain comprehensive knowledge in the subject of Intrusion Detection System.
2) Gets random exposure to principles and techniques used in Intrusion Detection System.

TEXTBOOK:

1. Rebecca Gurley Base “Intrusion Detection” MacMillan Technology Series (MTP Series) ISBN 1578701856, 9781578701858

REFERENCE BOOKS:

1. RafeeqRehman “Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID”, Prentice Hall PTR, 2003 ISBN 0-13-140733-3.
2. RonBenNatan, Implementing Database Security and Auditing, Elsevier, Indian reprint, ISBN: 9781555583347.

CSCS 506 : CYBER LAWS

Course Objective:

The objective of the courses to

1) Understand the basic cyber laws
2) Understating Information Technology Act 2000 and Cyber Security policies

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 **(12 hours)**

UNIT III

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)**

Course Outcome:

At the end of the course student will be able to

1) Get awareness about cyber laws and policies
2) Understand the international laws in Cyber Security.

Text Books:

(1). “The Information TechnologyAct”, 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 Objective:

The objective of the courses to

1) To understand basic concepts of Cyber security.
2) To Understand the fundamental concepts of OWASP.

UNIT I

Secure Web Site Design: Choosing a Web Server, The Basics of Secure Site Design, Guidelines for Java, JavaScript, and Active X**,** Designing and Implementing Security Policies. **Introduction to OWASP** **(12 hours)**

UNIT II

Implementing a Secure E-Commerce Web Site: Implementing Security Zones, Understanding Firewalls, Implementing Intrusion Detection, Managing and Monitoring the Systems, Pros and Cons of Outsourcing Your Site, **Securing Financial Transactions:** Understanding Internet-Based Payment Card Systems, Options in Commercial Payment Solutions, Examining E-Commerce Cryptography. **(12 hours)**

UNIT III

Handling Large Volumes of Network Traffic : Determining the Load on Your Site, Managing Bandwidth Needs, Introduction to Load Balancing. **(12 hours)**

Course Outcome:

At the end of the course student will be able to

1) Learn fundamentals of OWASP and E-commerce website security.
2) Learns basic on handling large volume network traffic.

TextBooks:

(1). “Hack Proofing your E-commerce Site”, Ryan Russell, Mark S. Merkow, Robin Walshaw,Teri Bidwell, Michael Cross, Oliver Steudler, Kevin Ziese, L. Brent Huston, Syngress, 2001
(2). “The Secure Online Business”, Adam Jolly, Kogan Page, 2003
(3). “The Secure Online Business handbook e-commerce, IT functionality & business continuity”, third edition, jonathanreuvid, Kogan Page, 2003
(4). ”Security Fundamentals for E-Commerce”, VesnaHassler, Artech House, 2001

CSCS 508 : BIG DATA ANALYTICS

Course Objective:

The objective of the courses to

1) Introduction to big data and exploring the big data analytics and techniques.
2) Exploring tool and databases for cyber security.

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 Visualization for Cybersecurity, Cybersecurity Training. **(12 hours)**

UNIT II

Machine Unlearning: Repairing Learning Models in Adversarial Environments, B**ig data in emerging cybersecuritydomains :**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

Analyzing Deviant Socio-Technical Behaviors 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)

Course Outcome:

At the end of the course student will be able to

1)Able to explore big data applications.

2) Understating fundamentals of big data analytics techniques for security application.

TextBooks:

(1). "Big Data Analytics in Cybersecurity", OnurSavas, Julia Deng, CRC Press, 2017

(2). "Data Analytics and Decision Support for Cybersecurity", IvánPalomaresCarrascosa,Harsha Kumara Kalutarage, Yan Huang, Springer, 2017

(3). "Darkweb Cyber Threat Intelligence Mining", John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, VivinPaliath, 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 Objective:

The objective of the courses to

1) Understand the basic cyber laws
2) Understating Information Technology Act 2000 and Cyber Security policies

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 **(12 hours)**

UNIT III

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)**

Course Outcome:

At the end of the course student will be able to

1) Get awareness about cyber laws and policies
2) Understand the international laws in Cyber Security.

Text Books:

(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