Master of Science (Cyber Security)Two Year

(Four Semesters) Course

The course of study of M.Sc. (Cyber Security)shall extend over a period of **four semesters** spread over two years. On satisfactory completion of the course and after passing the examinations, a candidate will be awarded the Master of Science (Cyber Security)degree.

Every academic year shall be divided into two semesters. First semester starts from July and ends in December. Second semester starts from January and ends in June and so on. There shall be an examinationattheendofeachsemester.Theexaminationsshallconsistoftheorypapers,practical papers. Mediumofinstructionsandexaminationwillbe**English**only.

EligibilityforAdmission:

The admission of the students for M.Sc. (Cyber Security) I and III Semester will be taken for July to December session and II and IV Semester will be from January to June session.

A candidate who has qualified graduate degree with at least 50% marks (48% for SC/ST/OBC/SOBC category) of Rajasthan University or any other university recognized as equivalent shall be admitted to the first year of M.Sc.(Cyber Security) Course.

Semester	CourseDuration	ExaminationTime
I,III	JulytoDecember	December
II,IV	JanuarytoJune	June

Examination Scheme:

Each theory paper shall be of 100 marks (70 marks for written examination of 3 hrs duration and 30 marks for internal assessment).

Each practical paper shall be of 100 marks (60 for practical exam and 40 for internal assessment).

The basis for internal evaluation in theory shall be home assignment, internal test and regularities in the attendance.

The basis for internal assessment in the laboratory courses shall be timely submission of the lab records,performance in the lab, internal tests etc.

Eachtheorypaperexaminationwillbeofthree-hourdurationandshallcarry70marks.Theory paper shall contain three parts.

a) Part-Awillcontain 12veryshort questionsof1markeach(studentwill attemptany 10).
b) PartBwillcontain4shortdescriptivetypesofquestionseachcarrying5marks,allare compulsory.
c) Part Cwill contain 4 long descriptive types of questions each carrying 10 marks, allquestions are compulsory with internal choice.

Each practical examination (Maximum marks 100) will be of four- hour duration on one day and carry 60 marks for exercise(s) assigned in the examination and Viva, and 40 marks for theInternal Assessment.

S.No.	QuestionPattern	Max.Marks (Theory)		Max.Marks (Practical)	
		ESE	CIA	ESE	CIA
1	PartA:12VeryShortQuestions (attempt any 10)	10 X1=10			
2	PartB:4ShortQuestionfromallUnits (Compulsory)	4 X5 =20			
3	PartC:4QuestionsfromeachUnit with Internal Choice	4 X10=40			
	SubTotal	**70**	**30**	**60**	**40**
		100		**100**	

Attendance:
Acandidateshallberequiredtoputinaminimumof75%attendanceatthelecturesand75% attendanceatthepractical'sseparatelyineach paper.

Examination Scheme:

Sr. No.	Paper	ESE	CIA	Total
1	Theory	70%	30%	100
2	Practical	60%	40%	100

NumberofUnitsinSyllabus:

Sr. No.	Stream	No. of Units
1	M.Sc.(Cyber Security)	4

MaximumMarksfortheCourseandNumberofUnitsofEachsubject2Years/4 Semesters:

Sr. No	Stream	Semester	NumberofPapers per semester		Total Marks (Credits)of1 Semester	SubTotal	Grand Total
			Theory (Credits)	Practical (Credits)			
1	M. Sc. (Cyber Security)						
		I ,II,III Sem	5 X100 (5 X4)	3 X100 (3 X4)	500 +300 = 800 (20 + 12 = 32)	800 X3 = 2400 (32 X3 = 96)	2400 (96)
		IVSem, Project	2 X100 (2 X4)	1 X200 (1 X8)	300+300 = 600 (8 +8 =16)	600 X1 =600 (16)	600 (16)
							3000 (112)

ProgrammeOutcomes

PO1: The program equips students with essential domains of computer science and Cyber Security. It empowers them to apply core concepts in the development of domain-specific applications.

PO2: The program fosters critical thinking, cultivates problem-solving skills, encourages evaluative learning of various techniques, and deepens comprehension of problem essence of cyber security.

PO3: The program educates students about the latest industry technologies. The continuous review of syllabi adds value to graduates, preparing them to address dynamic industry demands.

PO4:Theprograminstructsstudentsinapplyingadvancedtoolstoaddressreal-worldchallenges related to cyber security.

PO5: The program trains students to work with Ethical Hacking, Cyber Security, and Forensic Tools.

PO6: Real-world projects expose students to challenging industry environments, making thememployable and industry-ready through hands-on project development training.

PO7: The program hones students to handle cyber security threats, vulnerabilities & ethical hacking in real world application.

SemesterStructure:

M.Sc.(Cyber Security)SemesterI

S.No.	Subject Code	Course Title	Course Category	Credit	Contact Hours Per Week			EoSE Duration (Hrs.)	
					L	T	P	Thy	P
1.	MSCS101	Programming Fundamentals	DSC	4	4			3	
2.	MSCS102	DatabaseManagement System	DSC	4	4			3	
3.	MSCS 103	Data Communication & Networking	DSC	4	4			3	
4.	MSCS104	Computer Architecture	DSC	4	4			3	
5.	MSCS105	OperatingSystem	DSC	4	4			3	
6.	MSCS151	'C'ProgrammingLab	DSCP	4			6		2
7.	MSCS152	DBMSLab	DSCP	4			6		2
8.	MSCS153	Office Management Lab	DSCP	4			6		2

M.Sc.(Cyber Security)SemesterII

S.No.	Subject Code	Course Title	Course Category	Credit	Contact Hours Per Week			EoSE Duration (Hrs.)	
					L	T	P	Thy	P
1.	MSCS201	ObjectOriented Programming Concepts using Java Programming	DSC	4	4			3	
2.	MSCS202	DataStructureand Algorithms	DSC	4	4			3	
3.	MSCS203	WebDesigningand Development	DSC	4	4			3	
4.	MSCS204	Introduction of Cyber Security	DSC	4	4			3	
5.	MSCS205	Information Security & Cryptography	DSC	4	4			3	
6.	MSCS251	JavaProgrammingLab	DSCP	4			6		2
7.	MSCS252	DataStructureLab	DSCP	4			6		2
8.	MSCS253	WebDesigningLab	DSCP	4			6		2

M.Sc.(Cyber Security)SemesterIII

S.No.	Subject Code	Course Title	Course Category	Credit	Contact Hours Per Week			EoSE Duration (Hrs.)	
					L	T	P	Thy	P
1.	MSCS301	Biometric Security,Privacy & Laws	DSC	4	4			3	
2.	MSCS302	PythonProgramming	DSC	4	4			3	
3.	MSCS303	Ethical Hacking	DSC	4	4			3	
4.	MSCS304	Security Threats & Vulnerabilities	DSC	4	4			3	
5.	MSCS305	Cyber Forensic Audit & Investigation	DSC	4	4			3	
6.	MSCS351	Security Lab	DSCP	4			6		2
7.	MSCS352	PythonLab	DSCP	4			6		2
8.	MSCS353	Ethical Hacking Lab	DSCP	4			6		2

M.Sc.(Cyber Security)SemesterIV

S.No.	Subject Code	Course Title	Course Category	Credit	Contact Hours Per Week			EoSE Duration (Hrs.)	
					L	T	P	Thy	P
1.	MSCS401	**Elective Paper-I** a) Cyber Security Management System b) Malware & Software Vulnerability Analysis	DSC	4	4			3	
2.	MSCS402	**Elective Paper-II** a) Software Secure Engineering b) E-Commerce and Digital Payment	DSC	4	4			3	
3.	MSCS451	Project(Project,Report, Viva) (12Weeks)	DSCP	8					2

M.Sc.–(Cyber Security)FirstSemester

MSCS101:ProgrammingFundamentals

Course Outcomes:

CO1:UnderstandtheconceptofAlgorithmsanddifferentsymbolsusedinflowcharts
CO2: Develop conditional and iterative statements to write C programs.
CO3:Utilizeuser-definedfunctionstosolvereal-timeproblems.
CO4: Create C programs that utilize pointers to access arrays, strings, and functions.
CO5:Applyuser-defineddatatypes,includingstructuresandunions,tosolveproblems.
CO6:Demonstratetheconceptoffilehandlingtoshowcaseinputandoutputoperationsin C programs.

Unit-I

ProblemSolvingwithComputers: Algorithms,and Flowcharts.

Basic Structure of C Programs: Creating, Compiling, Linking and Execution of a C program Header Files, C Tokens (Keywords, Identifiers, Constants, and Special symbols), Data types, and Variable declaration, Operators, Expressions, Managing Data Input and Output Operations. Decision-Making and Branching, Looping and Jumping Statements.

Unit-II

Arrays: Declaration, Definition, One- and Two-Dimensional Arrays, Character Arrays andStrings.

Functions: Definition,NeedforFunctions, StandardandUser-DefinedFunctions,FunctionCalls, Category of Functions, Recursion, Storage Class Specifiers

Unit-III

StructuresandUnions: ArrayofStructures,NestingofStructures.

Pointers: Declaration, Definition and Use of Pointers, Difference between Pointers andStructures.

Unit-IV

File Management in C:Creating, Opening and Closing a File, I/O Operations on Files, Command Line Arguments. Dynamic Memory Allocation, Pre-Processor.

RecommendedBooks:

1. Kerighan&Richie theCprogramming language(PHI Publication)
2. ByronGottorfriedSchaum'soutline ofprogrammingwithC
3. E.BalaguruswamyProgramminginAnsi'C'(TataMcGrawHill)
4. Kanetkar"LetUsC", BPBPublications.(TataMcGrawHill)

MSCS102:DatabaseManagementSystem

Course Outcomes:

CO1: Gain a solid understanding of the fundamental concepts of database management systems, including data models, data independence, database architecture, and components.
CO2: Learn the principles and techniques involved in relational database management systems.
CO3: Ability to transform user requirements into efficient and well-structured database schemas.
CO4: Develop proficiency in SQL

Unit-I

Introduction to Database Concepts: Database and Need for DBMS,Characteristics of DBMS, Database Users, 2, 3-tier architecture, Data Models, Views of data- schemes and instances, Independence, Data modeling using the Entity-Relationship approach, Entities, Relationships, Representation of entities, attributes, relationship set, Generalization, Aggregation.

Unit-II

Relational model: Overview of database models, Relational Model, Structure of relational database, different types of keys, Expressing M: N relation, relational algebra, Constraints.
Relational Database Design: Functional dependencies, Normalization Normal forms based on primary keys (1 NF, 2 NF, 3 NF, BCNF, 4 NF, 5 NF) Lossless joins and dependency preserving decomposition.

Unit-III

SQL: Introduction to SQL, SQL Data types and Literals, Types of SQL commands, SQL Operators and their procedures, Tables, Views and Indexes, queries and sub-queries, aggregate function, insert, delete and update operations, Joins, Unions, Intersections, Minus in SQL.
Query Processing: Query Processing Stages, Estimation of Query Processing Cost, Introduction to Transactions, States of Transactions, ACID Properties

Unit-IV

Concurrency Control: Concurrency Control, Lock Based Protocols, Two Phase Locking protocol, Timestamp-based Protocol, multiple granularity, Deadlock Handling, Deadlock Prevention, Deadlock Detection and Recovery.
Recovery: Failure classification, recovery concepts, database backup, recovery concepts based on deferred update and on immediate update. Shadow paging, check points, an overview of Distributed database and client-server Database

RecommendedBooks:

1. FundamentalofDatabaseSystemsbyR.Elmasri,S.Navate; Benjamin Cummings
2. IntroductiontodatabasesystemsbyC.J .Date
3. Databasesystem conceptby Korth
4. PrinciplesofDatabaseManagementbyJamesMartin
5. RelationaldatabasedesignforMicrocomputersApplicationbyPrenticeHall(Jackson)
6. DatabaseManagementSystemsbyBipinDesai

MSCS103:Data Communication & Networking

Course Outcomes:

CO1:Abletounderstandnetworkcommunicationusingthelayeredconcept,OpenSystem Interconnect (OSI) and TCP/IP Model.
CO2:Understandvarioustypesoftransmissionmedia,networkdevices;andparametersof evaluation of performance for each media and device.
CO3:Understandtheconceptofflowcontrol,errorcontrolandLANprotocols
CO4:UnderstandtheworkingprinciplesofLANandtheconceptsbehindphysicalandlogical addressing, sub netting and supernetting.
CO5:UnderstandthefunctionsperformedbyaNetworkManagementSystemandtoanalyze connection establishment and congestion control with respect to TCP Protocol.

Unit-I

Data Communication Concepts: Introduction, Communication System, And Communication mode, Data encoding: Analog and Digital data, digital and analog signal, Communication Channels, Synchronous and asynchronous transmission. Bandwidth concepts, channel capacity.
Introduction to Networking: Computer network, Characteristic & advantages of networking, types of network, LAN, MAN, WAN.

Unit-II

Transmission media & Network Topologies: Guided & Unguided media, Twisted pair, coaxial cable, Fiber optics, Radio. VHF and microwaves, Satellite link. Network topology, bus, star, ring, tree, mesh& hybrid topology. Advantages and disadvantages of different topology. Multiplexing Channels and Concept of multi channeling and modulation, pulse code modulation (PCM) Frequency Division multiplexing, Time Division multiplexing, CODECS.

Unit-III

Digital Data Communication Techniques: Asynchronous and Synchronous Transmission - Types of Errors, Error Detection and Error Correction methodologies.
Network Standards: Introduction, Layered approach, OSI model functions & responsibilities of each layer.

Unit-IV

Internetworking: Principles of internetworking, Connectivity Devices, Switches, Bridges, Routers, Routing with bridges. Internet and e-mail protocols: SMTP, SLIP, POP, PPP, FTP, HTTP, Wi-Fi Network, Bluetooth, Broadband.

RecommendedBooks:

1. IntroductiontoDigitaland DataCommunications,MichalAMiller,JAICOpub.
2. DataandComputerCommunication –WillamStaling,PHI pub.
3. Data Communication& Network – Forouzan(TMH)
4. ComputerNetworks –A.Tanenbaum,(PHI pub.)
5. InternetworkingwithTCP/IPVol-I–Comer(PHIpub.)
6. DataCommunicationsanddistributedNetworks-V.B,Black,(PrenticeHall publication)

MSCS104:Computer Architecture

Course Outcomes:

CO1: Gain a comprehensive understanding of the components of a digital computer system
CO2: Proficient in converting data between different digital number systems (binary, octal, decimal, hexadecimal)
CO3: Design and analyze combinational circuits, such as multiplexers, demultiplexers, encoders, and decoders
CO4: Familiar with the anatomy of a computer system, including components like motherboards, microprocessors (CISC and RISC), different types of memory modules (RAM, Cache), and expansion slots
CO5: Develop a strong grasp of input and output devices, including printers, plotters, and voice output devices.

Unit -I

Introduction to DigitalComputer:Overview ofthe DigitalComputer System(Processor, Memory, Input and Output Devices, Storage Devices, Representation of Data: Digital versus Analog, Digital number system (binary, octal, decimal and hexadecimal numbers,) conversion from one form to another, fractional numbers and signed numbers, 1'S, 2'S Complements, Fixed point and floating point representations, Boolean algebra (addition, subtraction, multiplication and division), Logic Gates(NOT,OR,AND,NAND,NOR,XOR,XNOR)typesCodes(ASCII,EBCDIC,Unicode) Combinational Circuits(Multiplexer, Demultiplexer, coder, Encoder)Sequential Circuits(Flip flops, registers, Counters).

Unit-II

Anatomy of a Computer: Mother Board (Special reference to Intel 810 Chipset motherboard),CISC Micro Processors (Special reference to Pentium, AMD, Cyrix), RISC, types of RAM, Flash, Cache, types of memory modules (SIMM, DIMM), System clock, Bus (Data, Address, Control), Expansion slots (ISA, MCA, EISA, PCI, AGP).

Unit-III

I\O and Storage Devices: Input devices, Output devices, Printers (Dot-Matrix, Line, Label, Ink-Jet, Laser, Color Laser, thermal wax, dye sublimation, fiely, IRIS), Plotters (Pen, Ink-jet, electrostatic), Voice output], Storage devices I Storage types (Magnetic, Optical, Magneto-optical, Solid state), randomversussequentialaccess,formatting,tracksandsectors,speed,storagecapacity,FloppyDisk (5.25 inch, 3.5 inch; 2HD, zip, Superdisk, HiFD) Hard Disk (tracks, cylinders, sectors; Hard Drive Interfaces (IDE, EIDE, Fast SCSI, Fast/wide SCSI, Uitra SCSI; Hard Disk Cartridges, RAID), Optical Disks [pits and lands, CD-ROM, R, RW, DVD-ROM, R, RAM)], Magnetic tape (reels, streamers, DAT,DLT, stripe, Smart card), Modem (Fax/Data/Voice).

Unit-IV

Computer Memory Systems: Architecture of Digital Computer, Processor Design Principles, Control Unit Design: Conventional and Micro programmed, Input- Output System. Memory and I/O Organization: Interfacing with CPU; Main Memory, Auxiliary Memory, Cache Memories, Associative Memory and Virtual Memory. I/O Interfacing with CPU, Addressing Data Transfer Techniques.

Recommended Books:

1. ComputerArchitectureAndOrganization:McgrawHill,2ndEdition,JohnHyaes.
2. ComputerSystemArchitecture:PHI,3rdEdition,M.MorriesMano.
3. ComputerOrganizationAndDesign:PrenticeHallOfIndia,ChaudhariP.P.
4. PerspectiveInComputerArchitecture:PrenticeHallOfIndia,RaoP.V.S.
5. ComputerSystemArchitecture:PrenticeHall,TannenbaumA.
6. ParallelComputerArchitecture:AHardware/SoftwareApproachbyDavid Culler

MSCS105:Operating System

Course Outcomes:

CO1:Analyzevariousschedulingalgorithms.
CO2: Understand deadlock, prevention and avoidance algorithms.
CO3:Compareandcontrastvariousmemorymanagementschemes.
CO4:Understandthefunctionalityoffilesystems.
CO5:UnderstandtheOpensource operating system and basic Linux commands

Unit-I

Introduction to Operating System: Types of software (System/Application), Translators (Assemblers/ Interpreters/ Compilers), Operatingsystem as a resource manager, Operating system need and services, Classification and Evolution of OS, Hierarchical/Layered Organization of OS.

Unit-II

Process Management: Process concept, Process Control Block, Process Life cycle, Type of Scheduler, Scheduling criteria, multiple processor scheduling, scheduling Algorithm, FCFS, SJF, Priority and round robin scheduling, critical section, semaphores. Asynchronous parallel process, multithreading at system/user level, Inter process communication, Process Synchronization & Deadlock, Monitors, Deadlock prevention & avoidance, Deadlock Detection and deadlock Recovery.

Unit-III

Memory Management: Memory Management Techniques; Single partition allocation, multiple partition allocation, Swapping, paging and segmentation, segmented-paged memory management techniques; logical and physical address space; address mapping. Demand paging, Virtual memory, protection and address mapping hardware, page fault, Page replacement and page removal algorithms.

Unit-IV

DeviceManagementandI/OProgramming: Diskstructure,diskscheduling,accessmethodand storage capacity; sharable and non-sharable devices and their management.

Information Management & File System: File organization and access methods, logical and physical file structure; physical file system realized with device management function; file allocation methods, linked and index allocation, logical file implemented on physical file system. File protection and security, Directory structure, single level, two level, tree structure, Free Space Management, Allocation Methods.

RecommendedBooks:

1. JamesL.Peterson&A.Silberschatz:OperatingSystemConcepts;2ndEdn., Addison Wesley, World Student Edition
2. AndrewS.Tenenbaum:ModernOperatingSystems;PrenticeHall,India
3. DietelH.M.:AnIntroductionToOperatingSystems;AddisonWesley,World Student Edition
4. SystemsProgramming&Operating Systems,2ndEdn., TataMcGrawHill

MSCS151:‘C’Programming

Lab Course Outcomes:

CO1: Develop C programs based on a given task or algorithm.
CO2:Read,comprehend,andtracetheexecutionofCprograms.
CO3:ImplementCprogramsusingarrays,pointers,decision-makingstatements,andlooping statements.
CO4:Writeprogramsthatperformoperationsutilizingderiveddatatypes.
CO5:DevelopandimplementmodularapplicationsinCbyeffectivelyutilizingfunctions.
CO6: Develop applications in C that leverage structures and pointers.

Examination: Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper.

MSCS152:DBMSLab

Course Outcomes:

CO1:WritebothsimpleandcomplexSQLqueriestoretrieveinformationfromdatabaseswith many tables to support business decision making.
CO2:WriteSQLDDLtocreate,modifyanddropobjectswithinarelationaldatabase.
CO3:RetrieveandstoreinformationinarelationaldatabaseusingSQLinamulti-user environment.

Examination: Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper.

MSCS153:OfficeManagementLab

Course Outcomes:

CO1: Able to use MS Office (word processor, spreadsheet and power point) professionally.
CO2: Develop understanding about the writing of effective business letters in computer through word processing.
CO3:Abletousespreadsheet programforbusinessdataprocessing.
CO4:Acquireskillsfordevelopmentandpresentationofpowerpointreport**.**

Examination: Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper.

M.Sc.–Cyber SecuritySecondSemester

MSCS201:ObjectOrientedProgrammingConceptsusingJavaProgramming

Course Outcomes:

CO1:Understandtheconceptsof OOPs
CO2:KnowledgeofbasicprogrammingconstructsofJava
CO3:UnderstandandImplementtheconceptsofClassesandObjects
CO4: Implement Polymorphism, Inheritance, and Multithreading
CO5:EnlightentheuseofInterfaces,PackagesandExceptionHandling
CO6: Perform Database Connectivity through JDBC
CO7:UnderstandString&MathClassesandtheirfunctions

Unit-I
Introduction: ObjectOrientedConcepts,IntroductiontoJava,FeaturesofJava,Javavirtual machine.**Programming Fundamentals of Java:** Java Tokens, Operators, Data types, Control Structures, Array

Unit-II
ClassesandObjects: ObjectReferences,MethodOverloading,Constructors,Constructor Overloading, Inheritance. Static, Final, Abstract Keywords
PackagesandInterfaces: AccessSpecifiers,PackageCreation,Useofpackages,Basicsof Interfaces, Use of Interfaces
StringHandling: StringClass,Stringmethods.

Unit-III
Exception handling in Java: Exception classes, Exception raising & handling, use of Try, Catch and finally, Throwing Exceptions, User Defined Exceptions.
Applets: IntroductiontoApplets,Appletlifecycle,CreatingApplets,Applet Viewer
Graphics: GraphicsComponents, Color,Font,Drawing Objects

Unit-IV
ThreadinginJava: ConceptsofMulti-threading,ThreadLifeCycle,Threadclass,Runnable Interface, Thread Management in Java
JDBC:JDBCDrivers,TwoTierandThreeTierclientserverArchitecture,Settingupa connection to database, Creating and executing SQL statements

RecommendedBooks:

1. C.ThomasWu,AnIntroductiontoOOPwithJava,McGrawHill.
2. Deiteland Deitel,Java,Howto Program,Pearson EducationAsia.
3. E.Balaguruswmy,ProgrammingwithJava,TataMcGraw Hill.
4. Zukowski:MasteringJava2,BPBPublications.
5. HerbertScliildt, Java 2,Tata McGrawHill.

MSCS202:DataStructureandAlgorithms

Course Outcomes:

CO1:Analyzetheconceptsofalgorithmevaluationandfindtimeandspacecomplexities for searching and sorting algorithms.
CO2:Implementlineardatastructuresuchasstacks,queues,linkedlistsandtheirapplications.
CO3:Implement basic operations on binary trees
CO4:Demonstratetherepresentationandtraversaltechniquesofgraphsandtheir applications

Unit-I

Introduction, Types of Data Structures, Algorithm, Pseudocode, Characteristics of Algorithms, Algorithm Analysis, Algorithm Complexity – Space Complexity, Time Complexity, AbstractData Types.
StringProcessing–BasicTerminology,StoringStrings,StringOperations,PatternMatching Algorithms.
Arrays: Representation in Memory, Operations - Insertion, Deletion, Searching – Linear Search, Binary Search, Sorting – Bubble Sort, Multidimensional Arrays, Pointers, Pointer Arrays.

Unit-II

Sorting: Internal and External Sorting Techniques, Bubble Sort, Insertion Sort, Selection Sort, Merge Sort, Quick Sort, Radix Sort.
Linked lists: Linked List Vs. Arrays, Representation in Memory, Types of linked List - Singly Linked list, Doubly Linked list, Circular Linked list, Doubly Circular Linked list., Operations on Singly Link List – Insertion, Deletion, Traverse, Searching.

Unit-III

Stacks: Array and Linked List representation of Stacks, Operations – Insertion, Deletion, Traverse, Application of Stack – Recursion, Polish Notation.
Queues: Array and linked list representation in Memory, Type of Queues – Simple Queue, Circular Queue, Priority Queue, Double Ended Queue. Operations on Simple and Circular Queue – Insertion, Deletion, Traverse.Applications of Queues.

Unit-IV

Trees: Basic Tree Concepts, Representation of Binary Tree in memory, Binary Tree Traversals, Binary Search Trees, Heapsort.
Graphs:Representations,sequentialrepresentation,Warshall'sAlgorithm,LinkedRepresentation of graphs, Operations on Graph, Traversing Graph.

RecommendedBooks:

1. S.Lioschutz:DataStructures,McGrawHillInternational Edition.
2. A.V.Aho.,J.E.Hopcroft,andJ.D.Ullman,DataStructuresandAlgorithms,Pearson Education Asia.
3. A.MichaelBerman:DataStructuresviaC++,OxfordUniversity Press.
4. SaraBaaseandAllenVanGelder:ComputerAlgorithms,PearsonEducation Asia.
5. Jean-PaulTremblayandPaulG.Sorenson,AnIntroductiontoDatastructureswith applications, TMH Publishing Co. Ltd.

.

MSCS203:WebDesigningandDevelopment

Course Outcomes:
CO1:UnderstandthefundamentalsofInternet,andtheprinciplesofwebdesign.
CO2: Able to construct websites using HTML and Cascading Style Sheets.
CO3: Able to build dynamic web pages with validation usingJava Script objects
CO4: Implement the event handling mechanisms.

Unit-I
The Internet: History of the World Wide Web, Hardware and Software Trend, Web Server, Web Client.
Creating WebPages: IntroductiontoHTML,Typesof tags,FormattingTags, CommonTags, Hyperlinking, Images, Image Maps, Marquee Tag, Horizontal Rules, Lists.

Unit-II
AdvanceConceptsofHTML:HTMLTables,HTMLForms,Frames
Dynamic HTML: CSS : introduction, inline styles, creating style sheets with the style element, conflicting styles, linking external style sheets, positioning elements, backgrounds, element dimensions, text flow and the box model, user style sheets, Filters and Transitions.

Unit-III
Java Script: Introduction to scripting language, Client side versus Server side scripting , Advantages of Java Script, Features of Java Script, Keywords, Variables, Data Types, Constants, Comments, Java script control structures, Arrays, Array Library Methods, Java script Methods

Unit-IV
DOM:Introduction,Window,History,Navigator,Form,Frames,LocationObjects.
Event Handling in Java Script: Different types of events, key events, mouse events, loading events, Event Handlers,

RecommendedBooks:
1. M.L.Young:CompleteReferenceb:Internet;2ndEdition;TataMcGrawHill,2006.
2. ThomasA.Powel ;WebDesign:C.R.;Second Edition;TMH, 2009.
3. ThomasA.Powel;HTML& XHTML:C.R.;FourthEdition;TMH, 2008.
4. HarelyHahn:TheInternet,TataMcGrawHill.
5. G.Robertson: HandsonHTML,BPBPublications.
6. D.A.Tauber,B.Kienan:MicrosoftFromPage;BPBPublications.
7. PHPTheCompleteReference,StevenHolzer,TataMcGrawHill

MSCS204:Introduction of Cyber Security

Course Outcomes:

CO1: Comprehend the concepts of cybercrime and information security.
CO2: Identify different types of cybercriminals and understand the classification of cybercrimes.
CO3: Examine various tools and methods employed in cybercrime, including phishing and identity theft.
CO4: Analyze the methods and techniques of identity theft, including password cracking, key loggers, spyware, backdoors, steganography, DoS (Denial of Service) attacks, SQL injection, and buffer overflow.
CO5: Explore the security challenges posed by mobile and wireless devices in the context of cybercrime

Unit-I

Cyber Security: definition, cybercrime and information security, cybercriminals, classification of cybercrime, cybercrime Era. Cyber offences: categories of cybercrime, how criminals plan the attack, cyberstalking, cybercafe and cybercrime, botnets and cybercrime, Cloud Computing and cybercrime.

Unit-II

Tools and methods used in cybercrime: phishing and Identity theft; methods of phishing, spear phishing, types of phishing scams, phishing toolkits, and spy phishing, Personally Identifiable Information, types and techniques of ID theft, password cracking, keyloggers and spywares,backdoors, steganography, DoS and DoS attacks, SQL Injection, Buffer Overflow.

Unit-III

Cybercrime on mobile and wireless devices: Security challenges posed by mobile devices, attacks on wireless networks, credit card frauds mobile and wireless era. Authentication security service, attacks on mobile phones; mobile phone theft, mobile virus, mishing, vishing, smishing, hacking Bluetooth.

Unit-IV

Cybercrime and Cyber Terrorism- Intellectual Property in Cyberspace(Copyright, Patent, Trademark, Trade Secret, Trade Name, Domain Name) The Ethical Dimension of Cybercrimes, Sociology of Cybercriminals, Personality Traits of cyber criminals, Information Warfare

RecommendedBooks:

1. Cyber Security by Nina Godbole&SunitBelapure
2. Cryptographic & N/W security: Principles & Practices by Stalling, Prentice Hall.
3. Network Security Essentials: Applications & standards by Stalling, Pearson Education Asia, 2003.

MSCS205:Information Security & Cryptography

Course Outcomes:

CO1: To understand the concept of security model

CO2: To know about the life cycle of security systems

CO3: To have knowledge about basic concepts of cryptography

CO4: To understand the basics of symmetric and Asymmetric key cyphers

CO5: To be acquainted with the usage of message authentication and hash functions

CO6: To understand and apply the concept of MAC algorithms

UNITI

Security threats, Security Services, Security Mechanisms, Network Security Model, Cryptography, Cryptology, Cryptosystem, Cryptoanalysis, Symmetric and Asymmetric Ciphers Schemes, Block Ciphers, Stream Ciphers, Steganography, Attack- Active Attack and Passive Attack

UNITII

Information Security: Introduction, CNSS Security Model, Components of Information System, Approaches to Information Security Implementation, Security Systems Development Life Cycle. Cryptography: Concept, traditional ciphers like Caesar, Substitution, Vigenere, Transposition.

UNIT III

Symmetric key Ciphers: Concept and Types, Structure and analysis of DES, Security of DES, Structure and analysis of AES. Asymmetric key Ciphers: Concept of public key cryptosystems, RSA algorithm, Diffie-Hellman Key exchange. Message Authentication and Hash Functions: Authentication requirements and functions, MAC and Hash Functions, The Birthday Attack.

UNITIV

MAC Algorithms: Secure Hash Algorithm, Digital signatures, Kerberos. Concept and applications of IPSec, SSL, TLS, SET, PGP and S/MIME.Web Security, System Security-Intruders, Malicious Software, Firewalls.

RecommendedBooks:

1. Cryptographic & N/W security: Principles & Practices by Stalling, Prentice Hall.
2. Network Security Essentials: Applications & standards by Stalling, Pearson Education Asia, 2003.
3. Principles of Information Security: Michael E. Whitman, Herbert J. Mattord, CENGAGE Learning, 4th Edition.

MSCS251:JavaProgrammingLab Course Outcomes:

CO1:AbletoimplementthebasicconceptssuchasFunctionOverloading,arrayandstringmanipulation in Java
CO2:Useutilityclassesintherealtimeapplications
CO3: Understand the types of inheritance
CO4:Implementpackages,manipulatethreadsandexceptionhandlingtechniques
CO5: Connect databases with Java programs

Examination:Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper

MSCS252:DataStructureLab Course Outcomes:

CO1:Understandtheconceptofdatastructures,andapplyalgorithmforsolvingproblemslikeSorting, searching, insertion and deletion of data through C language.
CO2:Understandlineardatastructuresforprocessingoforderedorunordereddata.
CO3:ImplementvariousoperationsinCprogramondynamicdatastructureslikesinglelinkedlist, circular linked list and doubly linked list.
CO4:Exploretheconceptofnonlineardatastructuressuchastreesandgraphsthrough Cprogramming.

Examination: Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper

MSCS253:WebDesigningLab Course Outcomes:

CO1:CreatingwebpagesusingbasicHTMLtags
CO2: Styling Webpages using CSS
CO3:CreatingdynamicwebpagesusingJavascript
CO4: Implementation of DOM objects
CO5:Creatingwebpagesimplementingeventhandling,formValidationetc.

Examination: Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper

M.Sc.–Cyber SecurityThirdSemester

MSCS301:Biometric Security &Cyber Laws

Course Outcomes:

CO1: To understand the basics of biometrics
CO2: To know about the benefits of biometrics over traditional authentication systems
CO3: To have knowledge about key biometric terms, processes and applications
CO4: To understand various biometric matching methods
CO5: To have knowledge of various physiological biometric technologies
CO6.:To understand various behavioral biometric technologies

Unit-I

Introduction Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy in biometric systems.

Unit II

Physiological Biometric Technologies: Fingerprints- characteristics, strengths and weaknesses; Facial scan- characteristics, strengths and weaknesses; Iris scan characteristics, strengths and weaknesses; Retina vascular pattern- characteristics, strengths and weaknesses; Hand scan - characteristics, strengths and weaknesses; DNA biometrics.

Unit III

Behavioral Biometric Technologies: Handprint Biometrics, overview of DNA Biometrics. Signature and handwriting technology- description, classification, keyboard/keystroke dynamics; Voice- data acquisition, feature extraction, characteristics, strengths and weaknesses. Multi biometrics and multi factor biometrics.

Unit-IV

Cyber Laws Cyber Law, The Indian IT Act, Digital Signatures and IT Act, Cyber security and organizational implications, Cyber crisis management, Anti-Cybercrime Strategies, Cybercrime and Cyber-terrorism. Cybercrime and Indian ITA 2000.,cyber crime laws

RecommendedBooks:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : “Biometrics -Identity verification in a network”, 1st Edition, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul : “Implementing Biometric Security”, 1st Edition, Wiley Eastern Publication, 2005. Suggested Readings
3. John Berger: “Biometrics for Network Security”, 1st Edition, Prentice Hall, 2004.
4. Paul Reid, Biometrics for network security, Hand book of Pearson, 2004

MSCS302:PythonProgramming

Course Outcomes:

CO1:UnderstandandusePythoncontrolflowstatementswithease,aswellasthelanguage's basic syntax and semantics.
CO2:Abilitytounderstandofhowtohandlestringsandfunctions.
CO3:Learnhowtousedatastructureslikelists,dictionaries,tuples,andsetstodevelopand manipulate Python programs.
CO4: Determine the regular expression and file system operations that are most frequently used.
CO5:UnderstandthePython-specifictermsforObject-OrientedProgramming,suchas encapsulation, inheritance, and polymorphism.

Unit–I

IntroductionandOverview

Introduction,Comments, Keywords and Identifiers, Variables and Assignment statements, Standard Types, Other Built-in Types, Internal Types, Operators, Built-in Functions. Introduction to Numbers, Integers,Floating Point RealNumbers, Complex Numbers, Sequences:Strings,Sequences,Strings,String-only Operators, String Built-in Methods, Special Features of Strings, Conditionals and Loops: if statement, else Statement, elif Statement, while Statement, for Statement, break Statement, continue Statement, pass Statement

Unit–II

ListsandDictionaries

Functions,Lists,ListtypebuiltinMethods,SpecialFeaturesofLists,Tuples,TupleOperatorsandBuilt-in Functions, Special Features of Tuples, Introduction to Dictionaries, Built-in Functions, Built-in Methods, Dictionary Keys, Sets, Comparing Sets, Mathematical set operations, set comprehensions.

Unit–III

RegularExpressionandExceptionHandling

RegularExpression:Introduction,SpecialSymbolsandCharactersforREs,REsandPython,Exceptionsin Python, Detecting and Handling Exceptions, Exceptions as Strings, Raising Exceptions, Assertions, Standard Exceptions

Unit–IV

OOPsinPython

Classes in Python, Principles of Object Orientation, Creating Classes, Instance Methods, Class variables, Inheritance, Polymorphism, Type Identification

RecommendedBooks:

1. Python,TheComplete Reference, MartinCBrown, MacGrawHill
2. CorePythonProgramming,Dr.RNageshwaraRao,DreamtechPressIndiaPvt.Ltd
3. PythonProgramming:UsingProblem SolvingApproach,ReemaThareja
4. Letuspython,Yashvantkanetkar,AdityaKanetkar,BPB Publications

MSCS303:Ethical Hacking

Course Outcomes:

CO1. To understand the concept of ethical hacking
CO2. To have knowledge to installation and functioning of kali linux
CO3. To have knowledge about various malwares
CO4. To understand the basics of metasploit
CO5. To be acquaint with working and network analysis with Wireshark
CO6. To understand the concept of DDoS attacks
CO7. To know about hardware hacking, hijack sessions, hacking web servers, website Hacking SQL Injection and SQLMAP
CO8. To have basic knowledge of router attacks, wi-fi attacks, password attacks and phishing attacks.

UNIT-I

Overview of Ethical Hackers:-Definition and importance, Difference between ethical hackers and malicious hackers, Legal and ethical implications of hacking, **Cyber-security Fundamentals:** Key concepts: Confidentiality, Integrity, and Availability,**Roles and Responsibilities of Ethical Hackers:** Overview of ethical hacker certifications (CEH, OSCP), Legal frameworks and compliance (GDPR, HIPAA)

UNIT II

Introducing Hacking:- Different types of hacking, Phases of hacking, Installation and configuration of Kali Linux, Overview of directory structure, Usage of basic commands; Malwares – Virus , Worms, Trojan; Information gathering using NMAP and ZenMAP.

UNIT III

Metasploit: Exploiting System Software and Privilege, Metasploit Social Engineering Attack. Working and Network analysis with Wireshark , Network and web scanning about target , Packet captures and man-in-the-Middle attacks. Hacking using different social Engineering techniques.

UNIT-IV

DoS and DDoS attacks, Hardware hacking, Hijack sessions, Hacking web servers, Website Hacking , SQL Injection and SQLMAP, Database assessment , Router and Wi-Fi attacks, different types of password attacks, phishing attacks.

RecommendedBooks:

1. Basic Security Testing with Kali Linux, by Daniel Dieterle, freely available online.
2. Gray Hat Hacking The Ethical Hacker’s Handbook, BrankoSpasojevic, TMH, 2018.\
3. Ethical Hacking and Penetration Testing Guide, by RafayBaloch ,Auerbach Publications.
4. Kali Linux Revealed,byRaphaël Hertzog, JimO’Gorman, and MatiAharoni, offsec press, https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf
5. Kali Linux - An Ethical Hacker's Cookbook, by HimanshuSharma ,Packt Publishing Limited

MSCS304:Advanced Security Threats & Vulnerabilities

Course Outcomes:

CO1: To understand the basic concepts of security threats
CO2. To know about network security
CO3. To have knowledge of various behavioral biometric technologies
CO4. To understand the basics of threat analysis
CO5: Recognize and classify different types of vulnerabilities such as software flaws, misconfigurations, and design weaknesses.
CO6 Learn how to identify vulnerabilities in systems, software, and networks using automated tools
CO7:Understand how vulnerabilities are exploited in real-world attacks, and the tools and techniques that attackers use.

Unit-I

Advanced Security Threats:-Advanced Persistent Threats (APT), Characteristics of APTs, Case studies and real-world examples, Insider Threats, Types: Malicious, Negligent, and Unintentional insiders, Mitigation techniques for insider threats, Zero-Day Exploits, zero-day vulnerabilities, exploit zero-day threats and defense mechanisms

Unit-II

Security Measures & Mitigation Techniques, Firewalls and Intrusion Detection Systems (IDS), Functionality of firewalls and IDS, Best practices for configuring and using firewalls, TLS/SSL, VPNs, and end-to-end encryption, Authentication and Access Control, Role-based access control (RBAC), Multi-factor Authentication (MFA), Password management and security, Patch Management and Software Updates, Importance of regular patching, Vulnerability management lifecycle

Unit-III

System and Network Vulnerability:- Metasploit – Penetration testing with framework Metasploit – Scan services to identify vulnerabilities – Scan FTP services – Scan HTTP services – Exploitation – Post Exploitation techniques–Meterpreter–Rootkit–Backdoor–Password Hashes–Privilege Escalation - Nessus – Installation – Configuration – Importing Scanning Module – Scanning Vulnerable Service with Nessus

Unit-IV

Software Vulnerability (OWASP 10)-Fundamentals of OWASP Zed Attack Proxy (ZAP) – Installation – Configuration – Scanning HTTP / HTTPS Packets – Walkthrough of OWASP ZAP Tool – Burp Suite – Maltego – Sn1per – WPScan, Introduction to Human vulnerabilities (e.g., social engineering, weak passwords)

RecommendedBooks:

1. Joseph M Kizza, “Computer Network Security”, Springer Verlag, 2005
2. 2. Swiderski, Frank and Syndex, “Threat Modeling”, Microsoft Press, 2004
   Suggested Readings
3. William Stallings and Lawrie Brown, “Computer Security: Principles and Practice”, Prentice Hall, 2008.
4. Thomas Calabres and Tom Calabrese, “Information Security Intelligence: Cryptographic Principles & Application”, Thomson Delmar Learning, 2004.
5. "Cyber security and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman
6. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice" by Jason Andress
7. "Hacking: The Art of Exploitation" by Jon Erickson

MSCS305: Cyber Forensics, Audit & Investigation

Course Outcomes:

CO1: To understand basic concepts of various file systems and write blockers
CO2: To know about the extracting & recovering partitions
CO3: To have knowledge about NTFS file system architecture
CO4: To understand the basics of extended file systems
CO5: To be acquaint with windows forensic analysis
CO6: To understand the concepts of mobile forensics
CO7: To know about various audit functions, frameworks, standards and regulations

Unit-I

Concepts of Cyber Forensics: Definition and importance of cyber forensics, Role of cyber forensics in criminal investigations, Difference between cyber forensics and traditional forensics, **Fundamentals of Evidence Collection**: Types of digital evidence (e.g., hard drives, logs, emails), Preserving the integrity of digital evidence, Chain of custody in digital forensics, **Digital Forensics Process**: Forensic investigation lifecycle, Identifying, collecting, Analyzing, and reporting evidence, Tools and software used in digital forensics

Unit II

File system: CHS, LBA, HPA, write blockers, Extracting & recovering partitions, MBR, DOS partition table, Extended partition table, RAID; NTFS file system:Architecture, File creation,File deletion, Compression, encryption and indexing; Extended file systems: EXT4, Architecture, File creation, File deletion and Journaling; Other Disk structures; Windows and Linux boot process; File system acquisition and recovery.

Unit III

Windows Forensic Analysis: Window artifacts, Evidence volatility, System time, Logged on user(s), Open files, MRUs, Network information, Process information, Service information, Windows Registry, Startup tasks, Memory dumping; **Document Forensics:** PDF structure, PDF analysis, MS Office Document structure and analysis, Macros, Windows thumbnails.

Unit-IV

Mobile Forensics: SIM Card, Android architecture, Android File System, Android application; Virtual Machines, Network Forensics; **Cyber-crime investigation:** Pre investigation,SOP for Investigation; Case scenarios:social media crime, Email investigation; CDR Analysis. **Auditing:** Internal Audit and IT Audit Function, IT Governance, Frameworks, Standards and Regulations, Identifying information assets, Risk assessment and management.

RecommendedBooks:

1. Computer Evidence-Collection and Preservation. Brown,C.L.T. Course Technology Cengage Learning.
2. Guide to Computer Forensics And Investigations Nelson, Bill; Phillips, Amelia; Enfinger,Frank;Steuat,Christopher Thomson Course Technology.
3. Computer Forensics–Computer Crime Scene Investigation. Vacca, John R. Charles River Media
4. Bunting, Steveand William Wei.EnCase Computer Forensics:The Official EnCE: EnCase Certified

Examiner Study Guide.Sybex, 2006
5. Incident Response: Computer Forensics, Prosise, Chris, Kevin Mandia, and Matt Pepe, McGraw-Hill,2014
6. IT Security Risk Control Management:An Audit Preparation Plan,RaymondPompon,Apress 2016
7. Carrier, Brian.File System Forensic Analysis. Addison- Wesley Professional.
8. Computer Forensics: A Pocket Guide" by Bob Meade
9.A concise and accessible introduction to digital forensics, ideal for beginners.
10."Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet" by Eoghan Casey
11.A comprehensive text on the principles, tools, and methods used in digital forensics.
12."Cyber Crime and Digital Forensics: An Introduction" by Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar

MSIT351:Forensic Lab
Course Outcomes:
CO1:

Examination: Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper.

MSIT352:PythonLab Course Outcomes:
CO1:Understandcoreprogrammingbasicsandprogramdesignusing Pythonlanguage.
Understand the basic concepts of scripting and the contributions of scripting language.
CO2: Write, Test and Debug Python Programs.
CO3:ImplementConditionalsandLoopsforPython Programs.
CO4:UsefunctionsandrepresentCompounddatausingLists,Tuplesand Dictionaries.
CO5:UnderstandarangeofObject-OrientedProgramming,aswellasin-depthdataand information processing techniques.
CO6:Understandthehigh-performanceprogramsdesignedtostrengthenthepractical expertise

Examination: Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper.

MSIT353:Ethical HackingLab
Course Outcomes:
CO1: Comprehend the fundamentals of ethical hacking, including the differences between ethical hacking and malicious hacking.
CO2:
Examination: Practical
Exercisestobeframed soastocover thetopicsandtoolscoveredintheory paper

M. Sc. Cyber Security IV Semester

MSCS401ElectivePaperI (A): Cyber Security Management System

Course Outcomes:

CO1: Explain fundamental concepts of cyber-security, including the CIA Triad (Confidentiality, Integrity, and Availability), threats, vulnerabilities, and risk management.

CO2: Describe the principles of security governance, risk assessment, compliance, and the role of cyber-security management systems in organizational contexts.

CO3: Apply risk management methodologies to identify, assess, and mitigate cybersecurity risks in real-world scenarios.

CO4: Analyze security incidents using cybersecurity tools and techniques for vulnerability assessment, penetration testing, and incident response.

CO5: Implement security policies, controls, and procedures to enhance organizational security posture and ensure compliance with legal and regulatory requirements.

Unit-I

Secure System Planning and administration: introduction to the orange book, security policy requirements, accountability, assurance and documentation requirements, network security, red book and government network evaluations.**: Information Security Management System (ISMS)** Definition, Scope, and Importance of ISMS, Evolution of Information Security and Cyber Threat Landscape, Core Principles of ISMS: **Confidentiality, Integrity, Availability (CIA Triad),** Objectives and Benefits of Implementing ISMS, Key Concepts: Risk, Threats, Vulnerabilities, and Controls

Unit II

Risk Management: Risk Management Concepts:Identification, Assessment, and Mitigation, Definition of risk and risk management, Importance of managing risk in organizations, Overview of risk categories: operational, financial, strategic, cyber security. Risk Assessment Methodologies: Qualitative vs. Quantitative Analysis**. Security Governance**:Roles, Responsibilities, and Leadership in Cyber Security,Information Security Policies, Procedures, and Controls**,** Security Awareness and Training Programs**,** Business Continuity Management (BCM) and Disaster Recovery Planning (DRP)**,** Security Audits and Compliance Management

Unit-III

Cyber Security Incident Management and Business Continuity-Incident Response Lifecycle and Procedures, Digital Forensics and Evidence Handling, Security Audits and Compliance Frameworks (ISO 27001, NIST, GDPR)-National Cyber Security Policy & Strategy, Cyber Security Plan-Cyber Security Policy, Cyber Crisis Management Plan, Types of Security Control & their goals, Business Continuity Planning (BCP) and Disaster Recovery (DR)

Unit-IV

Emerging Trends in Cyber Security- The Impact of Artificial Intelligence and Machine Learning, Cyber Security in IoT, Cloud, and Big Data Environments, The Rise of Zero Trust Architecture, Future Challenges and Opportunities in Cyber Security, Blockchain and Cyber Security

RecommendedBooks:

1. **"Information Security Management Handbook"** by Harold F. Tipton &Micki Krause
2. **"Cybersecurity and Cyberwar: What Everyone Needs to Know"** by P.W. Singer & Allan Friedman

3. **"Principles of Information Security"** by Michael E. Whitman & Herbert J. Mattord
4. **"Information Security Governance: Guidance for Information Security Managers"** by W. KragBrotby.
5. **"Network Security Essentials"** by William Stallings
6. **"NIST Cybersecurity Framework: A Comprehensive Guide"** by Roberta Bragg

MSCS401ElectivePaperI (B): Malware & Software Vulnerability Analysis

CO1: To understand the fundamentals of malware
CO2: To know about the reverse engineering
CO3: To have knowledge of advanced dynamic analysis tools and concepts
CO4: To understand the basics of packers
CO5:To understand the concept of security and authentication
CO6:To know about the application security
CO7: To have knowledge of malicious code and access control
CO8: To understand the basics of penetration testing

Unit I

Introduction to malware, Types of malwares, Basic Static and Dynamic Analysis, Overview of Windows file format, PEView.exe, Patching Binaries , Disassembly(objdump, IDA Pro), Introduction to IDA, Introduction to Reverse Engineering, Extended Reverse Engineering using GDB and IDA;

Unit II

Advanced Dynamic Analysis - debugging tools and concepts, Malware Behavior - malicious activities and techniques, Analyzing Windows programs – WinAPI, Handles ,Networking , COM, Data Encoding, Malware Countermeasures , Covert Launching and Execution, Anti Analysis - Anti Disassembly, VM, Debugging; Packers – packing and unpacking, Intro to Kernel – Kernel basics, Windows Kernel API, Windows Drivers, Kernel Debugging, Covert analysis.

Unit III

Introduction to security & authentication: software security, security failures, bugtraq, CERT Advisories, technical trends affecting software security, penetrate and patch, security goals, prevention, traceability and auditing, monitoring, software security pitfalls, Software project goals. Application Security & Malicious Code: software risk management for security, role of security personnel, risk assessment, architectural risk analysis, penetration testing, risk-based security testing.

Unit IV

Access control & physical protection: Linux access control model, Linux Permissions, modifying file attributes, modifying ownership, the umask, programmatic interface, access control in Windows NT, compartmentalization, fine-grained privileges. Network Security & Intrusion: OSI model, sockets, socket functions, socket addresses, network byte order, internet address conversion, simple server and web clients, Tinyweb server. Peeling back the lower layers, network sniffing, raw socket sniffer, libpcap sniffer, decoding the layers, active sniffing

RecommendedBooks:

1. Michael Sikorski and Andrew Honig, " Practical Malware Analysis", No Starch Press,2012
2. Jamie Butler and Greg Hoglund, "Rootkits: Subverting the Windows Kernel", Addison-Wesley, 2005 Suggested Readings
3. Dang, Gazet and Bachaalany, "Practical Reverse Engineering",Wiley,2014
4. Reverend Bill Blunden, "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition,Jones& Bartlett, 2012.
5. John Viega& Gary McGraw: Building Secure Software: How to Avoid Security Problems the Right Way (Addison-Wesley Professional Computing Series)

6. Gary McGraw: Software Security: Building Security In (Addison-Wesley Professional Computing Series)
7. Michael Howard, David LeBlanc, John Viega: 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Security One-off) (AddisonWesley Professional Computing Series)
8. Jon Erickson: Hacking: The Art of Exploitation, 2nd Edition (No Starch Press, San Fransico)
9. Richard Sinn "Software Security, Theory Programming and Practice" Cengage Learning

MSCS401ElectivePaperI:Secure Software Engineering

Course Outcomes:
CO1: Evaluate secure software engineering problems, including the specification, design, implementation, and testing of software systems.
CO2: Elicit, analyze and specify security requirements through SRS.
CO3: Design and plan software solutions to security problems using various paradigms.
CO4: Model the secure software systems using Unified Modeling Language Sec.
CO5: Develop and apply testing strategies for Secure software applications Course Contents:

Unit I:

Introduction to Data Structures Software assurance and software security, threats to software security, sources of software insecurity, benefits of detecting software security, managing secure software development.

Unit II:

Searching and Sorting Techniques Defining properties of secure software, how to influence the security properties of software, how to assert and specify desired security properties

Unit III:

Stacks Secure software Architecture and Design: Software security practices for architecture and design: Architectural risk analysis, software security knowledge for Architecture and Design: security principles, security guidelines, and attack patterns, secure design through threat modeling.

Unit IV:

Queues Writing secure software code: Secure coding techniques, Secure Programming: Data validation, Secure Programming: Using Cryptography Securely, Creating a Software Security Programs. Programming with Linked Lists Secure Coding and Testing: code analysis- source code review, coding practices, static analysis, software security testing, security testing consideration through SDLC

RecommendedBooks:

1. Ross J Anderson, Security Engineering: A Guide to Building Dependable DistributedSystems, 2nd Edition, Wiley, 2008.
2. Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead, SoftwareSecurity Engineering: A Guide for Project Managers, Addison Wesley, 2008
3. Howard, M. and LeBlanc, D., Writing Secure Code, 2nd Edition, Microsoft Press, 2003

MSCS402ElectivePaperI:E-Commerce Application Development

Course Outcomes:

CO1: Determine the constituent elements of electronic commerce.
CO2: Recognize the advantages of conducting online sales.
CO3: Acquire knowledge on optimizing and ensuring safety during online selling.
CO4: Develop a comprehensive e-commerce strategy tailored to your business.
CO5: Comprehend the risks associated with cyber security in online trading and business transactions.
CO6: Familiarize yourself with methods to safeguard your online business, including securing your accounts and being vigilant about cybercrime.

Unit-I

Introduction to E-Commerce: Definition of e-Commerce, objectives, advantages, disadvantages, scope of e-commerce, Traditional Commerce V/s E-Commerce.

Unit-II

E-Commerce Models: Business to consumer, Business to Business, Consumer to Consumer, Other models-Brokerage Model, Aggregator Model, Info-Mediary Model, Community model, Value chain model, Supply Chain Model. Competitive advantage, Business strategy.

Unit-III

Electronic Data Interchange: Definition of EDI, Types of EDI, EDI standards, EDI Security and Privacy Issues, EDI Implementation, Format of EDI, Electronic-Catalogs, Digital Libraries. EGovernance,E-Buying, E-Selling, E-Banking, E-Retailing. Network Security: Network Security and Firewalls, Client Server Network, Security Threats, Cyber Law, E-mail.

Unit-IV

E-Payment System: Types of E-Payment Systems (EFT, E-Cash, E-Cheque, Credit/Debit Card, Smart Card, Digital Tokens and Electronic Purses/ Wallets) Payment Gateways.

Recommended Books:

1. Davis Whiteley: E-Commerece, TataMcHill, Delhi
2. P. T. Joseph: E-Commerece, Addis Anwesley, Delhi
3. R. Kalakola and A.B. Whiston : Frontiers of Electronic Commerce; AddisionWisley , 1996
4. Greensein, Feinman : Electronic Commerce Security, Risk management and Control; TMH, 2000
5. Saily Chan: Electronic Commerce Managment; John Wisley; 1998.
6. David kosiur ; Understanding E-commerce , The cutting edge of business, Tata-McGraw Hill
7. Kamlesh K. Bajaj &Debjani Nag, E-Commerce, The cutting edge of business, Tata-MCGraw Hill
8. Pete Losuin and A.Murphy, Electronic Commerce, AJaico Book
9. Green Stein "Electronic Commerce", TMH.

MSCS451:Project(Project,Report,Viva)

Course Outcomes:

CO1:Applyacquiredtechnicalskillstoreal-worldITorCSprojects effectively.

CO2: Demonstrate proficiency in project planning, organization, and execution, including setting milestones and managing resources.

CO3:Workcollaborativelywithprofessionalsinanindustrialsetting,showcasingstrong communication and teamwork skills.

CO4: Analyze complex problems, apply critical thinking skills, and develop innovative solutions in the IT or CS field.

CO5:Gainhands-onexperienceinthecompletesoftwaredevelopmentlifecycle,from requirements gathering to deployment, following industry best practices.

Twotypedanddulyboundcopiesofprojectreportshallbesubmittedatleast3weeksbefore commencement of the Theory/Practical examination which ever commences earlier.

GeneralInstructionsaboutPreparationofTrainingReport

1. ThePowerPoint Presentationhasto bepreparedfor theproject report.
2. ThePowerPointPresentationwillbearound10-15mins,andthenquestionanswers.So prepare the number of slides accordingly.
3. Thebindingfor reportswill bespiral binding.
4. Theformatforthereportsshouldbeadheredwithexactly.
5. TheCoding of the Projectshouldnot be included in thereport.
6. ContentsofIndexpageshouldincludethefollowingparts:
    a. ProjectRequirements.
    b. Feasibility Study.
    c. DetailedDesigning:
    d. Listof Figures.
    e. List ofDFD.
    f. Listof ER-Diagram.
    g. List of Tables.
    i. Testing.
    j. Future Scope.

PageFormatofProjectReportshouldbeasfollows.
Paper: A4
Font: Times New Roman, Bookman Old Style
ChapterHeading:16pt,Subheading:14pt.
Running Matter: 12 pt
Alltopicswillbenumberedaccordingly. Paragraph
Gap: 6 Pt Maximum
Line Gap: 1.5
Margins:Left 1.5, Right,Top and Bottom 1inch

PleaseNote: Projectreportofliveprojectinthegivenformathastobepreparedin3sets.These reports should have CD containing the soft copy and Power Point Presentation of Project report.

Formatof Front PageofProject Report.

Project Report

SubmittedtotheS.S.JainSubodhP.G.(Autonomous)College, University of Rajasthan, Jaipur

Logoofcollege **UOR logo**

inPartialfulfillmentoftherequirementforthedegreeof

MASTEROFSCIENCE(INFORMATIONTECHNOLOGY)

Submittedby

(yourname)

Name of Internal Guide

Name of Training Incharge (fromthecompany,whereyou have undergone training)

MSc-IT(AcademicSession)

(monthofdepositionandyear)

Formatof Live TrainingCertificateon company letter head

CERTIFICATE

Thisistocertifythat“**yourname,S/D/O ----------”**is/wasundertrainingfrom……(startdate)to …. (end date) in my supervision for partial fulfillment of the requirement for the award of the Degree of Master of Science (Information Technology).

Duringthisperiodhe/shehasworkedon…….(descriptionoftraining)projectas---------- --. Iwishforhis/hergood future.

Date:

NameofTraining Incharge

Designation