Maharaja Ganga Singh University, Bikaner

Learning Outcome-based Curriculum Framework (LOCF)

for

M.Sc.(Cyber Security)

Session 2022-23
Exam 2022 and 2023

Department of Computer Science
Maharaja Ganga Singh University, Bikaner

Table of Contents

Background

Considering the curricular reforms as instrumental for desired learning outcomes, all the academic departments of Maharaja Ganga Singh University Bikaner, made a rigorous attempt to revise the curriculum of postgraduate programs in alignment with National Education Policy-2020 and UGC Quality Mandate for Higher Education Institutions-2021. The process of revising the curriculum could be prompted with the adoption of the "Comprehensive Roadmap for Implementation of NEP-2020". The Roadmap identified the key features of the Policy and elucidated the Action Plan with well-defined responsibilities and an indicative timeline for major academic reforms.

The process of revamping the curriculum started with a series of webinars and discussions conducted by the University to orient the teachers about the key features of the Policy, enabling them to revise the curriculum in sync with the Policy. Proper orientation of the faculty about the vision and provisions of NEP-2020 made it easier for them to appreciate and incorporate the vital aspects of the Policy in the revised curriculum focused on creating holistic thoughtful, creative, and well-rounded individuals equipped with the key 21st-century skills 'for the development of an enlightened, socially conscious, knowledgeable, and skilled nation'.

With NEP-2020 in the background, the revised curricula articulate the spirit of the Policy by emphasising upon - an integrated approach to learning; innovative pedagogies and assessment strategies; multidisciplinary and cross-disciplinary education; creative and critical thinking; ethical and Constitutional values through value-based courses; 21st century capabilities across the range of disciplines through life skills, entrepreneurial and professional skills; community and constructive public engagement; social, moral, and environmental awareness; Organic Living and Global Citizenship Education (GCED); holistic, inquiry-based, discovery-based , discussion-based and analysis-based learning; exposure to Indian knowledge system, cultural traditions and literature through relevant courses offering "Knowledge of India, fine blend of modern pedagogies with indigenous and traditional ways of learning; flexibility in course choices, student-centric participatory learning; imaginative and flexible curricular structures to enable creative combinations of disciplines for study; offering multiple entry and exit points, alignment of Vocational courses with the International Standard Classification of Occupations maintained by the International Labor Organization; breaking the silos of disciplines; integration of extra-curricular and curricular aspects, exploring internships with local industry, businesses and artists and craft persons; closer collaboration between industry and higher education institutions for technical, vocational, and science programs, and formative assessment tools to be aligned with the learning outcomes, capabilities, and dispositions as specified for each course. The university has also developed a consensus on Blended Learning with 10% component of online teaching and 60% face-to-face classes for each program.

The revised curricula of various programs could be devised with concerted efforts of the faculty, Heads of the Departments, and the Deans of Schools of Study. The draft prepared by each department was discussed in a series of discussion sessions conducted at the Department, School, and University levels. The leadership of the University has been a driving force behind the entire exercise of developing the uniform template and structure for the revised curriculum. The Vice-Chancellor of the University conducted series of meetings with Heads and Deans to deliberate upon the vital parameters of the revised curriculum to formulate a uniform template featuring Background, Programme Outcomes, Programme Specific Outcomes, Postgraduate Attributes, Structure of Masters Course, Learning Outcome Index, Semester-wise Courses and Credit Distribution, Course-level Learning Outcomes,

Teaching-Learning Process, Blended Learning, Assessment and Evaluation, Keywords, References, and Appendices. The experts of various Board of Studies and School Boards contributed to a large extent in giving the final shape to the revised curriculum of each program.

To ensure the implementation of curricular reforms envisioned in NEP-2020, the University has decided to implement various provisions in a phased manner. Therefore, the curriculum may be reviewed annually so as to gradually include all relevant provisions of NEP-2020.

Program Outcomes

On completing Masters in the Faculty of Science, the students shall be able to realize the following outcomes:

PO1: Acquired knowledge with facts and figures related to various subjects in pure sciences such as Physics, Chemistry, Botany, Zoology, Mathematics, etc.

PO2: Understood the basic concepts, fundamental principles, and scientific theories related to various scientific phenomena and their relevance in day-to-day life.

PO3: Acquired the skills in handling scientific instruments, planning, and performing laboratory experiments The skills of observations and drawing logical inferences from the scientific experiments.

PO4: Analyzed the given scientific data critically and systematically and the ability to draw objective conclusions.

PO5: Been able to think creatively (divergent and convergent) to propose novel ideas in explaining facts and figures or providing new solutions to problems.

PO6: Realized how developments in any science subject help develop other science subjects and vice-versa and how interdisciplinary approach helps provide better solutions and new ideas for sustainable outcomes.

PO7: Developed scientific outlook concerning science subjects and all aspects related to life.

PO8: Realized that knowledge of subjects in other faculties such as humanities, performing arts, social sciences, etc., can have greatly and effectively influence, which inspires in evolving new scientific theories and inventions.

PO9: Imbibed ethical, moral, and social values in personal and social life, leading to a highly cultured and civilized personality.

PO10: Developed various communication skills such as reading, listening, speaking, etc., which will help express ideas and views clearly and effectively.

PO11: Realized that pursuit of knowledge is a lifelong activity and in combination with untiring efforts and positive attitude and other necessary qualities leads towards a successful life.

Program Specific Outcomes

On completing Masters in the M.Sc. in Computer Science, the students shall be able to realize the following outcomes:

PSO1. Communicate cyber security concepts, designs, and solutions effectively and professionally

PSO2. Apply knowledge of computing to produce effective designs and solutions for specific problems

PSO3. Use software development tools, software systems, and modern computing platforms to solve cyber security related issues

PSO4: To have the knowledge and the ability to develop creative solutions for security solutions

PSO5: To develop skills to learn new technology related to cyber security

PSO6: To develop critical reasoning

PSO7: To apply computer science theory and software development concepts to construct computing-based solutions
PSO8: To acquaint with computer programs/computer-based systems in the area related to algorithms, network security, web security, cloud security, Artificial Intelligence, Mobile and wireless security
PSO9: The ability to understand and use computer programs in the areas related to information security to design solutions of varying complexity
PSO10: The ability to understand the evolutionary changes in the security domain and to understand the real-world problems and meet the challenges of the future
PSO11: The ability to employ modern computer languages, environments, and platforms in creating innovative career paths to be an entrepreneur, lifelong learning and a zest for higher studies and also to act as a good citizen by inculcating in them moral values & ethics

Postgraduate Attributes

- Disciplinary Knowledge
- Creative & Critical Thinking
- Reasoning and Analytical abilities
- Logic/Discrete Mathematics knowledge
- Logical Thinking
- Problem analysis and solving abilities
- Life Skills
- Moral & Ethical Values
- Research Skills

Structure of Masters' Programme

Semester I

	Course Code	Course Title	Exam Hours	Max. Marks		Min. Marks	L	T	P*	Credits
				Int. Marks	Ext. Marks					
Core Courses										
1	FS-COMP-MSC-CY-CC-101	Mathematical Foundations for Cyber Security	3	10	40	13 (25%)	3	1	1	5
2	FS-COMP-MSC-CY-CC-102	Intrusion Detection and Prevention Systems	3	10	40	13 (25%)	3	1	1	5
3	FS-COMP-MSC-CY-CC-103	Computer Networks	3	10	40	13 (25%)	3	1	1	5
4	FS-COMP-MSC-CY-CC-104	C++ and Data Structures	3	10	40	13 (25%)	3	1	1	5
5	FS-COMP-MSC-CY-CP-105	Combined Practical	3	25	75	13 (25%)	*combined practical of above subjects			
Core Foundation Course										
1	FS-COMP-MSC-CY-FC-106	Computer Fundamentals	3	10	40	13 (25%)	4	2	2	5

M.Sc. Computer Sc. (Cyber Security)
Choice Based Credit System

Semester II										
	Course Code	**Course Title**	**Exam Hours**	**Max. Marks**		**Min. Marks**	**L**	**T**	**P***	**Credits**
				Int. Marks	**Ext. Marks**					
Core Courses										
1	FS-COMP-MSC-CY-CC-201	Information Security and Cryptography	3	10	40	13 (25%)	3	1	1	5
2	FS-COMP-MSC-CY-CC-202	Ethical Hacking	3	10	40	13 (25%)	3	1	1	5
3	FS-COMP-MSC-CY-CC-203	DBMS	3	10	40	13 (25%)	3	1	1	5
4	FS-COMP-MSC-CY-CC-204	Operating Systems	3	10	40	13 (25%)	3	1	1	5
5	FS-COMP-MSC-CY-CP-205	Combined Practical	3	25	75	26 (25%)	*combined practical of above subjects			
Core Foundation Course										
1	FS-COMP-MSC-CY-FC-206	Human and National Values	3	10	40	13 (25%)	4	2	2	5

Semester III										
	Course Code	**Course Title**	**Exam Hours**	**Max. Marks**		**Min. Marks**	**L**	**T**	**P***	**Credits**
				Int. Marks	**Ext. Marks**					
Core Courses										
1	FS-COMP-MSC-CY-CC-301	Cyber Forensics, Audit and Investigation	3	10	40	13 (25%)	3	1	1	5
2	FS-COMP-MSC-CY-CC-302	Biometric Security	3	10	40	13 (25%)	3	1	1	5
Core Elective Courses										
3	FS-COMP-MSC-CY-CE-303	a) Python b) Java	3	10	40	13 (25%)	3	1	1	5
4	FS-COMP-MSC-CY-CP-305	Combined Practical	6	25	75	26 (25%)	*combined practical of above subjects			
Open Elective Course										
1	FS-COMP-MSC-CY-EO-306	a) Security Threats b) Cyber Laws and Security Policies	3	10	40	13 (25%)	2	2	1	5

Semester IV

	Course Code	Course Title	Exam Hours	Max. Marks		Min. Marks	L	T	P*	Credits
				Int. Marks	Ext. Marks					
Core Courses										
1	FS-COMP-MSC-CY-CC-401	Malware Analysis	3	10	40	13 (25%)	3	1	1	5
2	FS-COMP-MSC-CY-CC-402	Software Vulnerability Analysis	3	10	40	13 (25%)	3	1	1	5
Core Elective Courses										
3	FS-COMP-MSC-CY-CE-403	a) Wireless LAN & Mobile Computing b) Web Security	3	10	40	13 (25%)	3	1	1	5
4	FS-COMP-MSC-CY-CP-405	Combined Practical/& Project/Dissertation	6	25	75	26 (25%)	*combined practical of above subjects			
Open Elective Course										
1	FS-COMP-MSC-CY-EO-406	a) Intellectual Property Rights b) Research & Publication Ethics	3	10	40	13 (25%)	2	2	1	5

Learning Outcome Index

Learning Outcomes are statements of knowledge, skills, and abilities a student should possess and demonstrate upon completion of learning experiences.

I. Programme Outcomes(PO) and Programme Specific Outcomes (PSO)

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10	PSO11
PO1	x	x	x	x	x	x	x	x		x	x
PO2	x		x		x	x	x	x	x	x	x
PO3	x	x	x		x	x	x	x	x	x	x
PO4	x	x	x	x	x	x		x	x	x	x
PO5	x	x	x	x	x	x	x	x	x	x	x
PO6	x	x	x	x	x	x	x			x	x
PO7				x	x		x		x	x	x
PO8		x		x		x	x	x			x
PO9	x	x		x	x		x	x			x
PO10	x	x	x		x				x		x
PO11	x	x	x		x	x	x	x	x	x	x

II. Programme Specific Outcomes (PSO) and Core Courses (CC)

	MCSEC 101	MCSEC 102	MCSEC 103	MCSEC 104	MCSEC 201	MCSEC 202	MCSEC 203	MCSEC 204	MCSEC 301	MCSEC 302	MCSEC 401	MCSEC 402
PSO1	x	x	x	x	x	x	x	x	x	x	x	x
PSO2	x	x	x	x	x	x	x	x	x	x	x	x
PSO3		x		x	x			x	x	x		x
PSO4	x	x	x	x	x	x	x	x	x	x	x	x
PSO5	x	x	x	x	x	x	x	x	x	x	x	x
PSO6	x		x		x	x	x				x	

PSO7	x	x	x	x	x	x	x	x	x	x	x	x
PSO8		x		x	x			x	x	x		x
PSO9		x	x	x	x			x	x	x	x	x
PSO10	x	x	x	x	x	x	x	x	x	x	x	x
PSO11	x	x	x	x	x	x	x	x	x	x	x	x

III. Programme Specific Outcomes (PSO) and Core Elective Courses (CEC)

	MCS 305a	MCS 305b	MCS 405a	MCS 405b
PSO1	x	x	x	x
PSO2	x	x	x	x
PSO3	x		x	
PSO4	x	x	x	x
PSO5	x	x	x	x
PSO6		x		x
PSO7	x	x	x	x
PSO8	x		x	
PSO9	x	x	x	x
PSO 10	x	x	x	x
PSO 11	x	x	x	x

Objectives, Course-level Learning Outcomes, Contents, and Suggested Readings

Semester I

Duration: 3 Hours | Maximum Marks: 50

Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-101 **Mathematical Foundations for Cyber Security**

Course Objectives:

CO1. To learn to evaluate mathematical arguments revolving around computation
CO2. To understand the basics of Combinations and Permutations
CO3. To acquire the ability to represent relations matrices and digraphs
CO4. To acquire and apply the knowledge on Graphs and Trees to real-world applications
CO5. To have the ability to Demonstrate the working of number theory
CO6. To acquaint with Linear Algebra and Probability theory
CO7. To understand coding Theory

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Comprehend and evaluate mathematical arguments revolving around computation.
LO2. Understand the basics of Combinations and Permutations.
LO3. Represent relations matrices and digraphs.
LO4. Apply the knowledge on Graphs and Trees to real-world applications.
LO5. Demonstrate the working of Grammars and Languages
CO6. Acquaint with Linear Algebra and Probability theory
CO7. Understand coding Theory

Note: Scientific Calculator may be allowed in the examination.

Unit I

Overview of Sets, Basics of counting, Permutations and Combinations, Relations-equivalence and partial orders. Concept of time complexity. **Graph Theory**: Eulerian paths and circuits, Hamiltonian paths and circuits, planar graphs, rooted and binary trees, graph colorings and applications, chromatic number.

Unit II

Analytic Number Theory: Prime numbers, Euclid's lemma, basic properties of congruences, residue classes and complete residue systems, Fermat's little theorem, Chinese remainder theorem. Abstract Algebra: groups, rings, fields, and their properties.

Unit III

Linear Algebra: vector spaces, linear independence, basis and dimensions. **Probability theory**: basics, conditional probability, Bayes theorem, random variables – discrete and continuous, normal probability distribution, stochastic process, Markov chain. **Coding Theory**: Need for coding, Hamming code.

Required Readings

1. Discrete Mathematics and its applications by K. H. Rosen, seventh edition, TMH
2. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.

Suggested Readings

3. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
4. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
5. H. Anton, "Elementary Linear Algebra", John Wiley & Sons, 2010.
6. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
7. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.
8. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.
9. D.S. Malik, J. Mordeson, M.K.Sen, Fundamentals of abstract algebra,TataMcGrawHill

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-102 **Intrusion Detection and Prevention Systems**

Course Objectives:

CO1. To understand the requirement of IDS and IPS
CO2. To know about the concepts of IDS and IPS
CO3. To have knowledge about various state-of-art IPS/IDS system available till the date
CO4. To understand the basic architecture and modeling of IDS/IPS
CO5. To be acquaint with installation and configuration procedure of Snort
CO6. To be acquainted with the functioning of Snort

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the requirement of IDS and IPS
LO2. Know about the concepts of IDS and IPS
LO3. Having the knowledge about various state-of-art IPS/IDS system available till the date

LO4. Understanding of the basic architecture and modeling of IDS/IPS
LO5. Acquaintance with installation and configuration procedure of Snort
LO6. Acquainted with the functioning of Snort

Unit I

Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources. Intrusion Prevention Systems, Network IDs protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion.

Unit II

A model for intrusion analysis , techniques, types of responses mapping, responses to policy Vulnerability analysis, credential analysis, non credential analysis; Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes.

Unit III

Working with Snort Rules, Rule Headers, Rule Options, The SnortConfiguration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL,Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

Required Readings

1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," 1st Edition, Prentice Hall , 2003.
2. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "IntrusionDetection and Correlation Challenges and Solutions", 1st Edition, Springer, 2005.
3. Carl Endorf, Eugene Schultz and Jim Mellander "Intrusion Detection & Prevention", 1st Edition, Tata McGraw-Hill, 2004.

Suggested Readings

4. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", 3rdEdition, New Riders Publishing, 2002.
5. T. Fahringer, R. Prodan, "A Text book on Grid Application Development and Computing Environment". 6th Edition, Khanna Publishers, 2012.
6. Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010
7. Paul E. Proctor, "The Practical Intrusion Detection Handbook ",Prentice Hall , 2001.
8. Ankit Fadia and Mnu Zacharia, "Intrusion Alert", Vikas Publishing house Pvt., Ltd, 2007
9. Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006.

M.Sc. Computer Sc. (Cyber Security)
Choice Based Credit System

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-103 **Computer Networks**

Course Objectives:

After completion of this course the student will be able to-

CO1. To gain ability to create a new protocol and test its efficiency
CO2. To design a new network architecture using protocols and interfaces
CO3. To create a hybrid topology using the existing topologies, and check inefficiency
CO4. To apply different encoding and decoding mechanisms involved in various types of transmission media and measure the transmission impairments
CO5. To design a model internet with various categories of networks and test the transmission rate
CO6. To understand the basics of data communication, networking, the internet, and their importance
CO7. To analyze the services and features of various protocol layers in data networks
CO8. To differentiate wired and wireless computer networks
CO9. To analyze TCP/IP and their protocols
CO10. To recognize the different internet devices and their functions
CO11. To identify the primary security threats of a network

Learning Outcomes:

After completion of this course the student will be able to-

LO1. Create a new protocol and test its efficiency.
LO2. Design a new network architecture using protocols and interfaces.
LO3. Create a hybrid topology using the existing topologies, and check inefficiency.
LO4. Apply different encoding and decoding mechanisms involved in various types of transmission media and measure the transmission impairments.
LO5. Design a model internet with various categories of networks and test the transmission rate.
LO6. Understand the basics of data communication, networking, the internet, and their importance.
LO7. Analyze the services and features of various protocol layers in data networks.
LO8. Differentiate wired and wireless computer networks.
LO9. Analyze TCP/IP and their protocols.
LO10. Recognize the different internet devices and their functions.
LO11. Identify the primary security threats of a network.

Unit I

Introductory Concepts: Goals and Applications of Networks, Network structure and architecture, the OSI reference model, services, networks topology. Physical Layer: The Physical Layer, Theoretical Basis for Data Communication, Guided Transmission Media, Wireless Transmission, Overview of Digital Signal Encoding Formats, Digital Modulation – ASK, FSK, PSK, PSK, Digitization – Sampling Theorem, PCM, DM, Analog Modulation – Introducing AM, FM, PM, The Mobile Telephone System.

Unit II

The Data Link Layer: Data Link Layer Design Issues, Error Detection and Correlation, Flow Control Protocols, Stop-and-wait Flow Control, Sliding – Window Flow Control, Error Control, Stop-and-wait ARQ, Go-back-N; Example of Data Link Protocols-HDLC Medium access sub layer: Channel allocations, ALOHA Protocols, Carrier Sense Multiple Access Protocols, Ethernet, wireless LANs, BlueTooth, Data Link Layer Switching.

Unit III

Network Layer: Point-to-Point network, routing algorithms, congestion control, internetworking, Quality Control, Internetworking, The Network Layer in the Internet, IP packet, IP addresses, IPv6. Transport Layer: Design Issue, connection management, TCP window management, User Datagram Protocol, Transmission Control Protocol, Performance Issues. Application Layer: DNS, E-Mail, WWW, Multimedia, application layer protocols.

Required Readings

1. Forouzan, "Data Communication and Networking", TMH, 4th Edition.
2. A.S. Tanenbaum, "Computer Networks", PHI, 4th Edition.

Suggested Readings

3. W. Stallings, "Data and Computer Communication", Macmillan Press.
4. Comer, "Computer Networks and Internet", PHI. 5.Comer, "Internetworking with TCP/IP", PHI.
5. W. Stallings, "Data and Computer Communication", McMillan.

Duration: 3 Hours Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-104 **C++ and Data Structures**

Course Objectives:

CO1. To declare, initialize and process variables, constants, and arrays
CO2. To read and print values from the keyboard using Scanner and Dialog boxes
CO3. To create statements for decisions and loops
CO4. To define functions and return values
CO5. To create classes, objects, and constructors
CO6. To understand and apply OO design concepts
CO1. To Create and initialize variables, constants, arrays, pointers, structures, and unions.
CO2. To Manipulate values of variables, arrays, pointers, structures, unions, and files.
CO3. To Create a function that can receive variables, arrays, pointers, and structures.
CO4. To define functions that can receive variables, arrays, pointers, and structures.
CO5. To create open, read, manipulate, write and close files.
CO6. To select and use appropriate data structures for the given problems.
CO7. To design efficient algorithms using various algorithm designing strategies
CO8. To analyze the problem and develop the algorithms related to these problems
CO9. To classify the problem and apply the appropriate design strategy to develop an algorithm

CO10. To design algorithm in the context of space and time complexity and apply the asymptotic notation
CO11. To be able to analyze algorithms and algorithm correctness.
CO12. To be able to summarize searching and sorting techniques
CO13. To be able to describe stack, queue, and linked list operations.
CO14. To be able to know. tree and graphs concepts

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Declare, initialize and process variables, constants, and arrays
LO2. Read and print values from the keyboard using Scanner and Dialog boxes
LO3. Create statements for decisions and loops
LO4. Define functions and return values.
LO5. Create classes, objects, and constructors.
LO6. Understand and apply OO design concepts.
LO1. Create and initialize variables, constants, arrays, pointers, structures, and unions.
LO2. Manipulate values of variables, arrays, pointers, structures, unions, and files.
LO3. Create a function that can receive variables, arrays, pointers, and structures.
LO4. Define functions that can receive variables, arrays, pointers, and structures.
LO5. Create open, read, manipulate, write and close files.
LO6. Select and use appropriate data structures for the given problems.
LO7. Design efficient algorithms using various algorithm designing strategies
LO8. Analyze the problem and develop the algorithms related to these problems
LO9. Classify the problem and apply the appropriate design strategy to develop an algorithm
LO10. Design algorithm in the context of space and time complexity and apply the asymptotic notation
LO11. Ability to analyze algorithms and algorithm correctness.
LO12. Ability to summarize searching and sorting techniques
LO13. Ability to describe stack, queue, and linked list operations.
LO14. Ability to know. tree and graphs concepts

Unit I

Basics : Overview of OOPs, if-else statements, loops (for, while). **Functions** : Overview, passing arguments by value and reference, recursive function, pointers. **Arrays**: Overview, array and function, array and pointers. **Class**: Overview, static data members, Inline Function, Constructors and Destructors.

Unit II

Inheritance: usage, types, compile time and run time polymorphism, overloading and overriding, virtual function, friend function, abstract class. String handling, String class, Overview of Templates. **Searching**: Linear Search, Binary Search. **Sorting:** Insertion Sort, Quick sort.

Unit III

Algorithm: Time and Space complexity of Algorithm. **Overview and applications of abstract data types:** Linked List, Stack, Queue. **Trees :** Basic terminologies. **Binary Tree** : Representation as Array, Basic operations, **Tree Traversal** : Inorder, Preorder, Postorder, Application of Binary Tree.

Required Readings

1. Object Oriented Programming With C++ By E. Balagurusamy (Tata Mcgraw Hill)
2. C++ The Complete Reference By Herbert Schildt (Tata Mcgraw Hill)
3. Object Oriented Programming With C++ By Schaum Series (Tata Mcgraw Hill)

Suggested Readings

4. C++11 for Programmers (Deitel Developer) by Paul J. Deitel (Author), Harvey M. Deitel, Prentice Hall; 2nd edition
5. Professional C++ by Marc Gregoire, Nicholas A. Solter and Scott J.Kleper (Goodreads Publications)
6. A Tour of C++ by Bjarne Stroustrup, 2018
7. C++17 in Detail by Bartłomiej Filipek
8. Expert Data Structure with 'C' By R.B Patel (Khana Book Publishing Co.(P))
9. Data structure By Lipschutz (Tata McGraw Hill)
10. Data Structure By Yashvant Kanitkar (BPB)
11. An Introduction to Data Structures with Applications By Jean-Paul Tremblay, Paul G.Sarerson (Tata McGraw Hill)
12. Data Structure Using C and C++ By Yedidyah Langsam, Moshe J.Augenstein, Arora M. Tenenbaum (Prentice- Hall India)

Paper Code:FS-COMP-MSC-CY-FC-106

Paper Name : Computer Fundamentals

Course Objectives:

CO1. To understand the characteristics of computers
CO2. To know about the generations of computers
CO3. To have knowledge about computer languages
CO4. To understand the basics of operating system
CO5. To be acquaint with with word processor, spreadsheet and presentation
CO6. To understand and apply the concept of algorithms and algorithm analysis
CO7. To know about some unsolved problems of computer science

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the characteristics of computers
LO2. Know about the generations of computers
LO3. Having knowledge of computer languages
LO4. Understanding of the basics of operating system
LO5. Acquaintance with with word processor, spreadsheet and presentation
LO6. Understanding and ability to design algorithms
LO7. Know about some unsolved problems of computer science

Unit I

Basics: Block Diagram, characteristics, generations of computers, classification of computers; Binary number system, Limitations of Computers, Primary and secondary memory, Input and output devices; Computer languages: Machine language, assembly language, higher level language, 4GL. Introduction to Compiler, Interpreter, Assembler, System Softwares, Application Softwares.Operating System: Features of Windows, Linux, Macintosh, Android. Open source softwares: concept and examples.

Unit II

Word Processing software: different formats for saving a word document, creating, editing documents and related operations, formatting features and related operations, spelling and grammar checker, headers and footers, creating and managing tables; printing, macros, mail merge, equation editor. Spreadsheet Software: Workbook, worksheets, datatypes, operators, cell formats, freeze panes, editing features, formatting features, creating formulas, using formulas, cell references.

Unit III

Presentation Graphics Software: Templates, views, formatting slide, slides with graphs, animation, using special features, presenting slide shows. Computer Problem Solving: Algorithms, Efficiency and analysis of algorithms, Writing algorithms for simple problems like factorial computation, generation of Fibonacci sequence and checking for prime number; Examples of unsolved problems in Computer Science.

Required Readings

1. P.K Sinha, "Computer Fundamentals", 2004
2. Rajaraman, Fundamentals of Computers, Fourth edition, Prentice Hall India Pvt. Limited, 2006

Suggested Readings

3. Peter Norton, "Introduction to Computers",4th Edition, TMH Ltd, New Delhi, 2017.
4. R.G. Dromey,"How to solve it by Computers", Pearson Publishers, New Delhi, 2007.
5. Dorothy House, "Microsoft Word, Excel, and PowerPoint: Just for Beginners, 2015

Web resources:

1. https://documentation.libreoffice.org/en/english-documentation/getting-started-guide/
2. https://www.coursera.org/learn/creative-problem-solving
3. http://web.mit.edu/rsi/www/pdfs/new-latex.pdf
4. https://www.latex-project.org/help/books/
5. https://support.google.com/docs/?hl=en#topic=1382883
6. https://en.wikipedia.org/wiki/List_of_unsolved_problems_in_computer_science
7. https://www.claymath.org/millennium-problems

Semester II

Duration: 3 Hours — Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-201 **Information Security and Cryptography**

Course Objectives:

CO1. To understand the concept of CNSS 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
CO7. To know about the concept of cryptanalysis

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding the concept of CNSS security model
LO2. Know about the life cycle of security systems
LO3. Having knowledge about basic concepts of cryptography
LO4. Understanding of the basics of symmetric and Asymmetric key cyphers

LO5. Acquaintance with the usage of message authentication and hash functions
LO6. Understanding and ability to apply the concept of MAC algorithms
LO7. Know about the concept of cryptanalysis

Unit I

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

Unit II

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.

Unit III

MAC Algorithms: Secure Hash Algorithm, Digital signatures, Kerberos. Concept and applications of IPSec, SSL, TLS, SET, PGP and S/MIME. Concept of steganography. **Cryptanalysis:** Concept, Linear Cryptanalysis, Differential Cryptanalysis.

Required Readings

1. Principles of Information Security : Michael E. Whitman, Herbert J. Mattord, CENGAGE Learning, 4th Edition.
2. Cryptography and Network Security : William Stallings, Pearson Education, 4th Edition.

Suggested Readings

3. Cryptography and Network Security : Forouzan Mukhopadhyay, McGraw Hill, 2nd Edition.

Duration: 3 Hours Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-202 **Ethical Hacking**

Course Objectives:

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.

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the concept of ethical hacking
LO2. Know about the installation and functioning of kali linux

LO3. Having knowledge of about various malwaress
LO4. Understanding of the basics of metasploit
LO5. Acquaintance with with working and network analysis with Wireshark
LO6. Understanding of the concepts of DDoS attacks
LO7. Know about hardware hacking, hijack sessions, hacking web servers, website Hacking , SQL Injection and SQLMAP
LO8. Have basic knowledge of router attacks, wi-fi attacks, password attacks and phishing attacks.

Unit I

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 II

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 III

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.

Required Readings

1. Basic Security Testing with Kali Linux, by Daniel Dieterle, freely available online.

2. Gray Hat Hacking The Ethical Hacker’s Handbook, Branko Spasojevic, TMH, 2018.\

Suggested Readings

2. Ethical Hacking and Penetration Testing Guide, by Rafay Baloch , Auerbach Publications.

3. Kali Linux Revealed,by Raphaël Hertzog, JimO’Gorman, and Mati Aharoni, offsec press, https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf

5. Kali Linux - An Ethical Hacker's Cookbook, by Himanshu Sharma , Packt Publishing Limited

Web resources:

1. https://nptel.ac.in/courses/106/105/106105217/

M.Sc. Computer Sc. (Cyber Security)
Choice Based Credit System

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-203 **DBMS**

Course Objectives:

CO1: To understand the need for a DB approach and understand the components and roles of DBMS
CO2: To know how to write SQL queries for the given problem statement
CO3: To apply DB system development life cycle to business problems
CO4. To develop ER diagram for representing the conceptual data model
CO5: To convert ER diagram into a set of relations representing the logical data model
CO6: To implement a collection of ties in the chosen DBMS product, such as ORACLE
CO7: To have a broad understanding of database concepts and database management system software
CO8: To have a high-level experience of major DBMS components and their function
CO9: To be able to model an application's data requirements using conceptual modeling tools like ER diagrams and design database schemas based on the conceptual model.
CO10: To be able to write SQL commands to create tables and indexes, insert/update/delete data, and query data in a relational DBMS.
CO11: To understand detailed architecture, define objects, load data, query data, and performance tune SQL databases.
CO12: To be able to handle large volumes of structured, semi-structured, and unstructured data using database technologies.

Learning Outcomes:

After completion of this course the student will be able to-

LO1: Appreciate the need for a DB approach and understand the components and roles of DBMS
LO2: Write SQL queries for the given problem statement
LO3: Apply DB system development life cycle to business problems
LO4. Develop ER diagram for representing the conceptual data model
LO5: Convert ER diagram into a set of relations representing the logical data model
LO6: Implement a collection of ties in the chosen DBMS product, such as ORACLE
LO7: Have a broad understanding of database concepts and database management system software
LO8: have a high-level experience of major DBMS components and their function
LO9: be able to model an application's data requirements using conceptual modeling tools like ER diagrams and design database schemas based on the conceptual model.
LO10: be able to write SQL commands to create tables and indexes, insert/update/delete data, and query data in a relational DBMS.
LO11: To understand detailed architecture, define objects, load data, query data, and performance tune SQL databases.
LO12: Able to handle large volumes of structured, semi-structured, and unstructured data using database technologies.

M.Sc. Computer Sc. (Cyber Security)
Choice Based Credit System

Unit I

Introduction: Characteristics of database approach, Advantages, Database system architecture, Overview of different types of Data Models and data independence, Schemas and instances, Database languages and interfaces; **E-R Model** : Entities, Attributes,keys, Relationships, Roles, Dependencies, E-R Diagram; Normalization: Definition, Functional dependencies and inference rules, 1NF, 2NF, 3NF and BCNF.

Unit II

Introduction to Relational model, Constraints: Domain, Key, Entity integrity, Referential integrity; Keys: Primary, Super, Candidate, Foreign; **Relational algebra**: select, project, union, intersection, minus, cross product, different types of join , division operations; aggregate functions and grouping**; SQL**: Data Types, statements: select, insert, update,delete, create, alter, drop; views, SQL algebraic operations, nested queries; Stored procedures: Advantages, Variables, creating and calling procedures, if and case statements, loops, Cursors, Functions, Triggers.

Unit III

Transactions processing: Definition , desirable properties of transactions, serial and non-serial schedules ,concept of serializability , conflict-serializable schedules; **Concurrency Control:** Two-phase locking techniques, dealing with Deadlock and starvation, deadlock prevention protocols, basic timestamp ordering algorithm; Overview of database recovery techniques; concept of data warehousing.

Required Readings

1. Fundamentals of Database Systems,Ramez A. Elmasri, Shamkant Navathe,5th Ed(Pearson)

2. Database System Concepts By Korth, Silberschatz, Sudarshan (Mcgraw Hill)

Suggested Readings

3. An Introduction to Database Systems By Bipin C. Desai (Galgotia Publication.)

4. SQL, PL/SQL Programming By Ivan Bayross (BPB)

5. Commercial Application Development Using Oracle Developer 2000 By Ivan Bayross (BPB)

Web Resources

1. http://www.mysqltutorial.org/mysql-stored-procedure-tutorial.aspx

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-204 **Operating Systems**

Course Objectives:

CO1. To be able to design and understand the following OS components: System calls, Schedulers, Memory management systems, Virtual Memory, and Paging systems.
CO2. To be able to evaluate, and compare OS components through instrumentation for performance analysis.
CO3. To analyze the various device and resource management techniques for time sharing and distributed systems
CO4. To develop and analyze simple concurrent programs using transactional memory and message passing, and understand the trade-offs and implementation decisions

Learning Outcome:

After completion of this course the student will be able to-

LO1. Allocate Main Memory based on various memory management techniques
LO2. Compare Memory allocation using Best fit, Worst fit, and first hold policies
LO3. Apply page replacement policies for dynamic memory management
LO4. Schedule CPU time using scheduling algorithm for processors
LO5. Compare various device scheduling algorithms. serve

Unit I

Introduction to Operating System, layered Structure, Functions, Types; Process: Concept, Process States, PCB; Threads, System calls; Process Scheduling: types of schedulers, context switch, CPU Scheduling, Pre-Emptive Scheduling, Scheduling Criteria- CPU Utilization, Throughput, Turnaround Time, Waiting Time, Response Time; Scheduling Algorithms- FCFS, SJF, Priority Scheduling, Round Robin Scheduling, MLQ Scheduling, MLQ With Feedback.

Unit II

Synchronization: Critical Section Problem, Requirements for a solution to the critical section problem; Semaphores,simple solution to Readers-Writers Problem. Deadlock: Characterization, Prevention, Avoidance, Banker's Algorithm, Recovery from Deadlock. Memory Management: Physical and virtual address space, Paging, Overview of Segmentation;Virtual Memory Management: Concept,Page Replacement techniques- FIFO, LRU, Optimal

Unit III

Linux:features of Linux, steps of Installation, Shell and kernel, Directory structure, Users and groups,file permissions, commands- ls, cat, cd, pwd, chmod, mkdir, rm, rmdir, mv, cp, man, apt, cal, uname, history etc. ; Installing packages; Shell scripts: writing and executing a shell script,shell variables, read and expr, decision making (if else,case), for and while loops.

Required Readings

1. Operating System Principles By Abraham Silberschatz, Peter Baer Galvin (John Wiley And Sons Inc.)
2. Operating System Concepts And Design By Milan Milen Kovic (Tata Mcgraw Hill)

Suggested Readings

3. Modern Operating System Andrew S. Tanenbaum, Herbert Bos

4. Linux in easy steps, Mike McGrath, in easy steps limited
5. Unix concepts and applications , TMH, Sumitabha Das

Semester III

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-301 **Cyber Forensics, Audit and Investigation**

Course Objectives:

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

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of basic concepts of various file systems and write blockers
LO2. Know about the extracting & recovering partitions
LO3. Having knowledge of NTFS file system architecture
LO4. Understanding of the basics of extended file systems
LO5. Acquaintance with windows forensic analysis
LO6. Understanding of the concepts of mobile forensics
LO7. Know about various audit functions, frameworks, standards and regulations

---

Unit I

Filesystem: 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 II

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 III

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.

Required Readings

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

Suggested Readings

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,Raymond Pompon,Apress 2016
7. Carrier, Brian.File System Forensic Analysis. Addison- Wesley Professional.

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-302 **Biometric Security**

Course Objectives:

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

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the basics of biometrics
LO2. Know about the benefits of biometrics over traditional authentication systems,
LO3. Having knowledge about key biometric terms, processes and applications
LO4. Understanding of various biometric matching methods
LO5. Having knowledge of various physiological biometric technologies
LO6. Understanding of various behavioral biometric technologies

---

Unit I

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.

Required Readings

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

Duration: 3 Hours Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CE-303**a Python**

Course Objectives:

CO1. Apply language features including strings, lists, tuples, dictionaries, regular expressions.
CO2. Create and call functions.
CO3. Create and manipulate files.
CO4. Develop classes using OO features.
CO5. Develop internet applications using packages such as urllib.
CO6. To understand why Python is a proper scripting language for developers.
CO7. To learn how to design and program Python applications.
CO8. To learn how to use lists, tuples, and dictionaries in Python programs.
CO9. To learn how to identify Python object types.
CO10.To learn how to use indexing and slicing to access data in Python programs.
CO11. To define the structure and components of a Python program.
CO12. To learn how to write loops and decision statements in Python.
CO13. To learn how to write functions and pass arguments in Python.
CO14. To learn how to build and package Python modules for reusability.
CO15. To learn how to read and write files in Python.
CO16. To learn how to design object□oriented programs with Python classes.
CO17. To learn how to use class inheritance in Python for reusability.

CO18. To learn how to use exception handling in Python applications for error handling.

Learning Outcomes:

After completing this course, students will be able to:
LO1. Apply language features including strings, lists, tuples, dictionaries, regular expressions. LO2. Create and call functions.
LO3. Create and manipulate files.
LO4. Develop classes using OO features.
LO5. Develop internet applications using packages such as urllib.
LO6. To understand why Python is a proper scripting language for developers.
LO7. To learn how to design and program Python applications.
LO8. To learn how to use lists, tuples, and dictionaries in Python programs.
LO9. To learn how to identify Python object types.
LO10.To learn how to use indexing and slicing to access data in Python programs.
LO11. To define the structure and components of a Python program.
LO12. To learn how to write loops and decision statements in Python.
LO13. To learn how to write functions and pass arguments in Python.
LO14. To learn how to build and package Python modules for reusability.
LO15. To learn how to read and write files in Python.
LO16. To learn how to design object□oriented programs with Python classes.
LO17. To learn how to use class inheritance in Python for reusability.
LO18. To learn how to use exception handling in Python applications for error handling.

Unit I

Basics: Python Interpreter, writing code in Jupyter Notebook, Indentation, comments, importing a module, binary operators, standard scalar data types, type casting, if-else statements, loops(while, for), pass, range, ternary expressions. Data Structures and Sequences: Tuples, Lists and slicing, Built-in Sequence functions, Dictionary, Sets; List, Set, and Dict Comprehensions.

Unit II

Functions: Namespaces, Scope, and Local Functions; Returning Multiple Values, Anonymous (Lambda) Functions, Partial Argument Application, Generators, Errors and Exception handling. Basic File Handling. Objects and Methods in Python. NumPy: creating N-dimensional arrays, arithmetic with NumPy arrays, basic indexing and slicing, Psuedorandom number generation.

Unit III

Pandas: Overview of Series and DataFrames, reading data from csv file, DataFrame operations- working with data using functions like head, tail , info, shape, reshape, columns, isnull, dropna, mean, sum, describe, value_counts, corr, loc, iloc, apply. Matplotlib- plotting basic figures, subplots, line plots, bar plots, histograms, scatter plots. Overview of Scikit-learn, SciPy, networkx. Applications of python.

Required Readings

1. Python for Data Analysis: Data Wrangling with Pandas, NumPy, and Ipython, by Wes McKinney, O'Reilly Media, 2017

2. Python All-in-One for Dummies, by John Shovic and Alan Simpson, John Wiley & Sons, Inc., 2019

Suggested Readings

3. Programming in Python 3: A Complete Introduction to the Python Language, Mark Summerfield, Pearson.

4. Swaroop, C. H. (2003). A Byte of Python. Python Tutorial.

5. Introduction to Computation and Programming Using Python. By John V. Guttag, MIT Press.

6. Learning Python , Mark Lutz, David Ascher, O'Reilly

7. T. Budd, Exploring Python, TMH, 1st Ed, 2011

Web Resources

1. https://www.learnpython.org/
2. https://nptel.ac.in/courses/106/106/106106212/
3. http://greenteapress.com/thinkpython/thinkpython.pdf
4. Python tutorial: https://docs.python.org/3/tutorial/index.html

FS-COMP-MSC-CY-CE-303**b**

Paper Name : Java

Course Objectives:

CO1. To use an integrated development environment to write, compile, run, and test simple object-oriented Java programs.
CO2. To read and make elementary modifications to Java programs that solve real-world problems.
CO3. To validate input in a Java program.
CO4. To identify and fix defects and common security issues in code.
CO5. To document a Java program using Javadoc.
CO6. To use a version control system to track source code in a project.

Learning Outcomes:

After completing this course, students will be able to:
LO1. Use an integrated development environment to write, compile, run, and test simple object-oriented Java programs.
LO2. Read and make elementary modifications to Java programs that solve real-world problems.
LO3. Validate input in a Java program.
LO4. Identify and fix defects and common security issues in code.
LO5. Document a Java program using Javadoc.
LO6. Use a version control system to track source code in a project.

Unit I

Introduction to Java: evolution, features, comparison with C and C++; Java program structure; tokens, keywords, constants, variables, data types, type casting, statements, Operators and Expression; Conditional Statements and Loop Statements. **Class:** syntax, instance variable, class variables, methods, constructors, overloading.

Unit II

Inheritance: types of inheritance, use of super, method overriding, final class, abstract class, wrapper classes.
Arrays, Strings and Vectors, Packages and Interfaces, visibility controls

Unit III

Errors and Exceptions: Types of errors, Exception classes, Exception handling in java, use of try, catch, finally, throw and throws. Taking user input, Command line arguments. **Multithreaded Programming:** Creating Threads, Life cycle of thread, Thread priority, Thread synchronization, Inter-thread communication, Implementing the Runable Interface.

Required Readings

1. The Complete reference Java Ninth Edition By Herbert Schildt (Tata McGraw Hill)
2. Beginning Programming with Java For Dummies by Burd, For Dummies; 3 edition

Suggested Readings

3. Java: A Beginner's Guide, Sixth Edition: A Beginner's Guide by Herbert Schildt, McGraw-Hill Osborne MediaProgramming in JAVA By E. Balagurusamy (TMH)
4. JAVA 2 programming Black Book By Steven Holzner et al. (Dreamtech Press)
5. Programming in JAVA By E. Balagurusamy (TMH)

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CP-305**a Security Threats**

Course Objectives:
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. To be acquaint with various security elements
CO6. To understand various methods of access control

Learning Outcomes:
After completion of this course the student will be able to-
LO1. Understanding of the basic concepts of security threats
LO2. Know about the network security
LO3. Having knowledge of various behavioral biometric technologies
LO4. Understanding of the basics of basics of threat analysis
LO5. Acquaintance with various security elements
LO6. Understanding of various methods of access control

Unit I

Security threats: introduction, sources, motives, target assets and vulnerabilities, consequences of threats, email threats, web threats, intruders and hackers, insider threats. **Network Threats:** active/ passive, interference, interception, impersonation, worms, virus, spams, adware, spyware, Trojans. Covert channels, backdoors, bots, IP spoofing, ARP

spoofing, session hijacking, sabotage-internal threats, environmental threats, threats to server security.

Unit II

Security threat management: risk assessment, forensic analysis, security threat correlation, threat awareness, vulnerability sources and assessment, vulnerability assessment tools, threat identification, **Threat analysis: t**hreat modelling, model for Information Security planning.

Unit III

Security Elements: authorization and authentication, types, policies and techniques, security certification, security monitoring and auditing, security requirements specifications, security polices and procedures, firewalls, IDS, log files, honey pots. **Access control**: trusted computing and multilevel security, security models, trusted systems, software security issues, physical and infrastructure security, security awareness, training, e-mail, and Internet use policies.

Required Readings

1. Joseph M Kizza, "*Computer Network Security*", Springer Verlag, 2005
2. Swiderski, Frank and Syndex, "*Threat Modeling*", Microsoft Press, 2004
3.

Suggested Readings

4. William Stallings and Lawrie Brown, "*Computer Security: Principles and Practice*", Prentice Hall, 2008.
5. Thomas Calabres and Tom Calabrese, "*Information Security Intelligence: Cryptographic Principles & Application*", Thomson Delmar Learning, 2004.

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CP-305**b Cyber Laws and Security Policies**

Course Objectives:

CO1. To understand the concept of computer security
CO2. To know about the secure system planning and administration
CO3. To have knowledge about information security policies and procedures
CO4. To understand the basics of information security
CO5. To be acquaint with organizational and human security

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the concept of computer security
LO2. Know about the secure system planning and administration
LO3. Having knowledge about information security policies and procedures
LO4. Understanding of the basics of information security
LO5. Acquaintance with organizational and human security

Unit I

Introduction to Computer Security: definitions, threats to security, government requirements, information protection and access controls, computer security efforts, standards, computer security mandates and legislation, privacy considerations, international security activity. **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.

Unit II

Information security policies and procedures: corporate policies- tier1, tier2 and tier3 policies, process management, planning and preparation, developing policies, asset classification, policy-developing standards. **Information security:** fundamentals, employee responsibilities, information classification, information handling, tools of information security, information processing, secure program administration.

Unit III

Organizational and Human Security: adoption of information security management standards, human factors in security, role of information security professionals.

Required Readings

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3.

Suggested Readings

4. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
5. Thomas R Peltier, Justin Peltier and John blackley, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996
6. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997
7. James Graham, " Cyber Security Essentials" Averbach Publication T & F Group.

Semester IV

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-401 **Malware Analysis**

Course Objectives:

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 know about various kernels
CO6. To understand and apply various rootkit techniques

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the fundamentals of malware
LO2. Know about the reverse engineering
LO3. Having knowledge of advanced dynamic analysis tools and concepts
LO4. Understanding of the basics of basics of packers
LO5. Have knowledge of various kernels
LO6. Understanding of various rootkit techniques

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;

Unit III

Packers – packing and unpacking, Intro to Kernel – Kernel basics, Windows Kernel API, Windows Drivers, Kernel Debugging, Rootkit Techniques- Hooking, Patching, Kernel Object Manipulation , Rootkit Anti-forensics , Covert analysis.

Suggested Readings

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.

M.Sc. Computer Sc. (Cyber Security)
Choice Based Credit System

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CC-402 **Software Vulnerability Analysis**

Course Objectives:
CO1. To understand the concept of security and authentication
CO2. To know about the application security
CO3. To have knowledge about malicious code
CO4. To understand the basics of penetration testing
CO5. To have the knowledge of access control
CO6. To understand basics of buffer overflow and rootkits
CO7. To know about some aspects of network security & intrusion

Learning Outcomes:
After completion of this course the student will be able to-
LO1. Understanding of the the concept of security and authentication
LO2. Know about the the application security
LO3. Having knowledge about malicious code
LO4. Understanding of the basics of penetration testing
LO5. Having the knowledge of access control
LO6. Understanding of basics of buffer overflow and rootkits
LO7. Know about some aspects of network security & intrusion

Unit I

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, privacy and confidentiality, Multilevel security, Anonimity, Authentication, Integrity, software security pitfalls, Software project goals. **Application Security & Malicious Code:** software risk management for security, role of security personnel, risk assessment, development goes astray, code review (tools) , architectural risk analysis, penetration testing, risk-based security testing, abuse cases and security requirements, security operations

Unit II

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. **Buffer overflow & rootkits**: buffer overflows as security problems, defending against buffer overflow, internal buffer overflows, tools for handling buffer overflows, smashing heaps and stacks, heap overflows, stack overflows, decoding the stack.

Unit III

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, Denial of Service, SYN Flooding, ping of death, teardrop, ping flooding, amplification attacks, Distributed DoS Flooding, TCP/IP hijacking, RST hijacking, continued hijacking, port scanning, stealth SYN Scan, FIN, X-mas, and Null scans, spoofing Decoys, idle scanning, proactive defence (shroud), reach out and hack someone.

Required Readings

1. John Viega & Gary McGraw: *Building Secure Software: How to Avoid Security Problems the Right Way* (Addison-Wesley Professional Computing Series)
2. Gary McGraw: *Software Security: Building Security In* (Addison-Wesley Professional Computing Series)
3.

Suggested Readings

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

Duration: 3 Hours Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CE-403**a Wireless LAN and Mobile Computing**

Course Objectives:
CO1. To understand the architecture of wireless networks
CO2. To know about the wireless LAN and Ad Hoc networks
CO3. To have knowledge of Global System for Mobile Communications(GSM)
CO4. To understand the basics of UMTS and LTE
CO5. To be acquaint with GPRS
CO6. To understand mobile computing
CO7. To know about mobile network later and mobile transport layer

Learning Outcomes:
After completion of this course the student will be able to-
LO1. Understanding of the architecture of wireless networks
LO2. Know about the wireless LAN and Ad Hoc networks
LO3. Having knowledge of Global System for Mobile Communications(GSM)
LO4. Understanding of UMTS and LTE
LO5. Acquaintance with GPRS
LO6. Understanding of mobile computing
LO7. Know about mobile network later and mobile transport layer

---

Unit I

Wireless Networks: Introduction, Architecture, Wireless SwitchingTechnology, Wireless Communication problem, Wireless Network Reference Model, Wireless, Wireless LAN: Infrared vs radio transmission, Infrastructure and Ad-hoc Network, IEEE 802.11:System Architecture,Protocol Architecture, 802.11b, 802.11a, Bluetooth: User Scenarios, Architecture.

Unit II

Global System for Mobile Communications (GSM): Mobile Services, SystemArchitecture, Protocols, Localization & Calling, Handover, Security. GPRS: GPRS System Architecture, UMTS: UMTS System Architecture. LTE: Long Term Evolution. MobileComputing: Mobilecommunication, Mobilecomputing, Mobile Computing Architecture, Mobile Devices, Mobile System Networks, Mobility Management;

Unit III

Mobile Network Layer: Mobile IP: Goals, Assumptions, Entities and Terminology, IP Packet Delivery, Agent Discovery, Registration, Tunneling and Encapsulation, Optimizations, DHCP. Mobile Transport Layer: Traditional TCP, Indirect TCP, Snooping TCP, Mobile TCP, Fast retransmit/fast recovery, Transmission /time-out freezing, Selective retransmission, Transaction oriented TCP, TCP over 2.5G/3G Wireless Networks.

Required Readings

1. Schiller, J. 2008. Mobile Communications. 2nd ed. India: Pearson Education.
2. Kumar,S. and Kakkasageri, M.S. "Wireless and Mobile Networks: Concepts and Protocols", Wiley India.

Suggested Readings

3.Kamal R. 2011. "Mobile Computing", 2ndEd.Oxford University Press.
4. Talukder, A. K., Ahmed, H. andYavagal,R.R. 2010.Mobile Computing: Technology, Applications and Service Creation, 2ndEd. Tata McGraw Hill
5.Gast, M.S. "802.11 Wireless Networks: The Definitive Guide", O'Reilly Media

Duration: 3 Hours Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-CE-403**b Web Security**

Course Objectives:
CO1. To understand the concept of web security
CO2. To know about the web server architecture
CO3. To have knowledge of web hacking
CO4. To understand the basics of digital certificates

CO5. To understand the basics of digital signatures

Learning Outcomes:

After completion of this course the student will be able to-

LO1. Understanding of the concept of web security
LO2. Know about web server architecture
LO3. Having knowledge of web hacking
LO4. Understanding of the basics of digital certificates
LO5. Understanding of the basics of digital signatures

Unit I

Introduction: web security, web languages, web attacks, N-tier web applications, web servers: Apache, IIS, database servers, computer security, cryptography basics, public key cryptography, RSA, shopping, payment gateways

Unit II

Web hacking: basics HTTP & HTTPS URL, web under the cover, overview of java security, reading the HTML source, applet security servlets, symmetric and asymmetric encryptions, network security basics, firewalls & IDS.

Unit III

Digital certificates and digital signatures: digital certificates, hashing, message digest. digital signatures basics, securing databases, secure JDBC, securing large applications, cyber graffiti

---

Required Readings

1. McClure, Stuart, Saumil Shah, and Shreeraj Shah. Web Hacking: attacks and defence. Addison Wesley. 2003.
2. Garms, Jess and Daniel Somerfield. Professional Java Security. Wrox. 2001.

Duration: 3 Hours Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-EO-405**a Intellectual Property Rights**

Course Objectives:

CO1. To understand the concepts of IPR
CO2. To know about the intellectual property law
CO3. To have knowledge about cyber law
CO4. To understand the basics of copyrights
CO5. To understand the laws of patents and copyrights
CO6. To understand what is trade secret and how to apply it
CO7. To know about law and legislation about trade secrets

Learning Outcomes:

After completion of this course the student will be able to-

LO1. Understanding of the concepts of IPR
LO2. Know about intellectual property law
LO3. Having knowledge of cyber law
LO4. Understanding of the basics of copyrights

LO5. Understanding of the laws of patents and copyrights
LO6. Understanding of what is trade secret and how to apply it
LO7. Know about law and legislation about trade secrets

Unit I

Intellectual Property Law: Introduction, evolutionary past, IPR tool kit, paralegal tasks in intellectual property law, ethical obligations in paralegal tasks **Cyber law: i**ntroduction, innovations and inventions trade related intellectual property right

Unit II

Copyrights: principles, rights afforded by copyright law, copyright ownership, transfer and duration, right to prepare derivative works, rights of distribution, rights of perform the work publicity copyright formalities and registrations, limitations, copyright disputes and international copyright law, semiconductor chip protection act

Unit III

Patents: law of patents, patent searches, patent ownership and transfer, patent infringement, international patent law. **Trade secret:** introduction, maintaining trade secret, physical security, employee limitation, employee confidentiality agreement, trade secret law, unfair competition, trade secret litigation, breach of contract, applying state law

---

Require Readings

1. Debirag E.Bouchoux: "Intellectual Property". Cengage learning, New Delhi
2. M.Ashok Kumar and Mohd.Iqbal Ali: "Intellectual Property Right" Serials Pub.

Suggested Readings

3. Cyber Law. Texts & Cases, South-Western's Special Topics Collections
4. Prabhuddha Ganguli: ' Intellectual Property Rights" Tata Mc-Graw –Hill, New Delhi
5. J Martin and C Turner "Intellectual Property" CRC Press
6. Richard Stimm " Intellectual Property" Cengage Learning

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-MSC-CY-EO-405**b Research and Publication Ethics**

Course Objectives:
CO1. To understand the co
CO2. To know about the generations of computers
CO3. To have knowledge about computer languages
CO4. To understand the basics of operating system
CO5. To be acquaint with with word processor, spreadsheet and presentation
CO6. To understand and apply the concept of algorithms and algorithm analysis
CO7. To know about some unsolved problems of computer science

Learning Outcomes:
After completion of this course the student will be able to-
LO1. Understanding of the characteristics of computers
LO2. Know about the generations of computers
LO3. Having knowledge of computer languages

LO4. Understanding of the basics of operating system
LO5. Acquaintance with with word processor, spreadsheet and presentation
LO6. Understanding and ability to design algorithms
LO7. Know about some unsolved problems of computer science

Unit I

PHILOSOPHY AND ETHICS:Introduction to philosophy: definition, nature and scope, concept, branches. Ethics: definition, moral philosophy, nature of moral judgements and reactions. SCIENTIFIC CONDUCT: Ethics with respect to science and research, Intellectual honesty and research integrity. Scientific misconducts: Falsification, Fabrication, and Plagiarism (FFP) 4. Redundant publications: duplicate and overlapping publications, salami slicing. Selective reporting and misrepresentation of data.

Unit II

PUBLICATION ETHICS:Publication ethics: definition, introduction and importance. Best practices / standards setting initiatives and guidelines: COPE, WAME, etc.. Conflicts of interest. PUBLICATION MISCONDUCT: definition, concept, problems that lead to unethical behavior and vice versa, types. Violation of publication ethics, authorship and contributorship. Identification of publication misconduct, complaints and appeals. Predatory publishers and journals. Subject specific ethical issues, FFP, authorship. Conflicts of interest. Complaints and appeals: examples and fraud from India and abroad

Unit III

OPEN ACCESS PUBLISHING:Open access publications and initiatives. SHERPA/RoMEO online resource to check publisher copyright & self-archiving policies . Software tool to identify predatory publications developed by SPPU. Journal finder / journal suggestion tools viz. JANE, Elsevier Journal Finder, Springer Journal Suggester, etc.Use of plagiarism software like Turnitin, Urkund and other open source software tools

---

Required Readings

1.
2.

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-102 Cyber Crime, Cyber Laws and IPR

Course Objectives:
CO1. To understand the concepts of cyber crime and cyber law
CO2. To know about the IT Act 2000
CO3. To have knowledge about various cyber crime issues
CO4. To understand the IT(amendment) Act, 2008
CO5. To know about digital signatures and certificate-legal issues
CO6. To understand intellectual property rights

Learning Outcomes:
After completion of this course the student will be able to-

LO1. Understanding of the cyber crime and cyber law
LO2. Know about the IT Act 2000
LO3. Having knowledge of cyber crime issues
LO4. Understanding of the IT(amendment) Act, 2008
LO5. Acquaintance with with digital signatures and certificate-legal issues
LO6. Understanding of intellectual property rights

Unit I

Introduction to cyber crime and cyber law, cyberspace and information technology, Nature and scope of cyber crime, Jurisdiction of cybercrime. Important definitions under IT Act 2000, Cyber crime issues: unauthorized access, White collar crimes, viruses, malwares, worms, Trojans, logic bomb, Cyberstalking, voyeurism, obscenity in internet, Software piracy

Unit II

IT Act 2000, offences under IT Act and IT(amendment) Act, 2008. CRPC overview, Role Of Intermediaries, Electronic Evidence, Cyberterrorism, espionage, warfare and protection system. Overview of amended laws by the IT Act, 2000: The Indian Penal Code, 1860, The Reserve Bank of India Act 1934, Cyber Theft and the Indian Telegraph Act,1885. Digital Signatures and certificate-legal issues.

Unit III

Intellectual Property rights: Introduction to IP, Copyright, Related Rights, Trademarks, Geographical Indications, Industrial Design, Patents, Licensing and transfer of technology, WIPO Treaties , CopyrightsAct, PatentsAct, Trademark Act.

Required Readings

1. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, Raghu Santanam, M. Sethumadhavan, Information Science Reference.
2. Pfleeger, Charles P.and ShariL. Pfleeger.Security in Computing, 4th Edition. Upper Saddle River, NJ:Prentice Hall,2008.
3.

Suggested Readings

4. Cyber crime:Security and Surveillance in the Information Age,Douglas Thomas; Brian Loader.
5. Computer Crime:A Crime-Fighters Handbook by David Icove.
6. Crime in the Digital Age: Controlling Telecommunications and Cyber space Illegalities,Peter N. Grabosky.
7. Cyber law–The Indian Perspective By Pavan Duggal,Saakshar Law Publications.
8. Jonathan Rosenoer,"Cyber Law:The law of the Internet", Springer-Verlag, 1997.
9. Mark F Grady,Fransesco Parisi,"The Law and Economics of Cyber Security",Cambridge University Press,2006.

Paper Code:MCS-405
Paper Name : Project

After completing this course, students will be able to:
LO1. Identify and define the problem statement
LO2. Define and justify the scope of the proposed problem

LO3. Gather and analyze system requirements
LO4. Propose an optimized solution among the existing solutions
LO5. Practice software analysis and design techniques
LO6. Develop technical report writing and oral presentation skills
LO7. Develop a functional application based on the software design
LO8. Apply to code, debugging, and testing tools to enhance the quality of the software
LO9. Prepare the proper documentation of software projects following the standard guidelines
LO10. Become a master in specialized technology
LO11. Become updated with all the latest changes in the technological world.
LO12. Ability to communicate efficiently.
LO13. Ability to be a multi-skilled engineer with sound technical knowledge, management, leadership, and entrepreneurship skills.
LO14. Capability and enthusiasm for self-improvement through continuous professional development and life-long learning
LO15. Awareness of the social, cultural, global, and environmental responsibility of an engineer.

Practical Training and Project Work:

1. Project Work may be done individually or in groups in case of bigger projects. However if the project is done in a group each student must be given a responsibility for a distinct module and care should be taken to monitor the individual student.
2. Project Work can be carried out in the college or outside with prior permission of college.
3. The Student must submit a synopsis of the project report to the college for approval. The Project Guide can accept the project or suggest modification for resubmission. Only on acceptance of the draft project report the student should make the final copies.
4. **The Project Report should be hand written**

Submission Copy:
The Student should submit a spiral bound copy of the project report.

Format of the Project:

(a) Paper:
The Report shall be typed on White Paper of A4 size.

(b) Final Submission:
The Report to be submitted must be original.

(c) Typing:
Font:- Times New Roman
Heading:- 16 pt., Bold
Subheading:- 14 pt, Bold
Content:- 12 pt.
Line Spacing:- 1.5 line.
Typing Side :-One Side
Font Color:- Black.

(d) Margins:
The typing must be done in the following margin:
Left : 0.75”
Right: 0.75”
Top: 1”

Bottom: 1”
Left Gutter: 0.5”

(e) Binding:
The report shall be Spiral Bound.

(f) Title Cover:
The Title cover should contain the following details:
Top: Project Title in block capitals of 16pt.
Centre: Name of project developer’s and Guide name.
Bottom: Name of the university, Year of submission all in block capitals of 14pt letters on separate lines with proper spacing and centering.

(g) Blank sheets:
At the beginning and end of the report, two white blank papers should be provided, one for the Purpose of Binding and other to be left blank.

(h) Content:

I). Acknowledgement
II). Institute/College/Organization certificate where the project is being developed.
III). Table of contents
IV). A brief overview of project
V). Profiles of problem assigned
VI). Study of Existing System
VII). System Requirement
VIII). Project plan
- o Team Structure
- o Development Schedule
- o Programming language and Development Tools

IX). Requirement Specification
X). Design
- o Detailed DFD and Structure Diagram
- o Data structure, Database and File Specification

XI). Project Legacy
- o Current Status of project
- o Remaining Areas of concern
- o Technical and Managerial Lessons Learnt
- o Future Recommendations

XII). Nomenclature and Abbreviations.
XIII). Bibliography
XIV). Source Code.

Teaching-Learning Process

The teaching learning process may include the following-

- Lectures
- Discussions
- Simulations
- Virtual Labs
- Role Playing
- Participative Learning
- Interactive Sessions
- Seminars

- Research-based Learning/ Dissertation/ Case Study/ Project Work

The Blended Learning mode of teaching and learning is preferable in which offline (face-to-face) and online learning both are used to provide learners the opportunity to enjoy both of the worlds. Teachers can share instructions, lecture notes, and assignments online. On the other hand, students can share information/work/assignments with teachers and other students directly in a collaborative setting. This may have a more enriched learning experience, and collaboration between students can be improved upon if group activities rely on information gathered from online resources or lessons. Students who complete online coursework followed by interactive, face-to-face class activities have richer educational experiences.

Assessment and Evaluation

- A comprehensive and continuous evaluation by mid-semester examinations at regular intervals to find out each course level learning outcome
- Formative assessment on the basis of activities of a learner throughout the program instead of one assessment. for this provision of internal exams, student seminars, and assignments is included
- Open book exam is suggested for internal/ mid-term exams to better facilitate the understanding of the knowledge required
- Group examinations are recommended on problem-solving exercises and in major projects to enhance teamwork capabilities of the learner
- Collaborative/Individual assignments are useful to enhance the capability of learners to gain domain-specific knowledge
- Student Seminars and Quizzes are recommended for the continuous learning and evaluation process

ELIGIBILITY FOR ADMISSION

Graduates possessing 50% marks in any faculty of any statutory university who have studied Computer Science/ Computer Application as a main or vocational subject for three years shall be eligible for admission to the M.Sc. Cyber Security Course (Relaxation to SC/ST etc. as per Prevailing Rules)

PASS CRITERIA

For passing in the examination, a candidate is required to obtain at least a Satisfactory Grade in each paper (Internal + External) and also acquire a Satisfactory Grade in theory and practical separately (in each semester examination).

CLASSIFICATION OF SUCCESSFUL CANDIDATES

As per university norms

INSTRUCTIONS TO PAPER SETTER

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit). **Section-B** will consist of 9 questions (3 questions from each unit). **Section-C** will consist of 6 questions (2 questions from each unit).

The word limit of parts A, B, and C are 50, 200, and 500 respectively

1. **INSTRUCTIONS FOR PRACTICAL EXAMINATION**

Marks Distribution for Practical Exam -

1. Each practical exam is to be conducted by two examiners one External and one Internal. The external examiner should be a senior lecturer from the jurisdiction of other universities. Credit Weightage distribution for external practical of 4 credits is as under

a) Practical Examination exercise of 3 questions 2 credits

b) Viva-Voce 1 credit
c) Laboratory Exercise File 1 credit

2. Marks distribution for External Project report of 40 marks is as under
   a. External Evaluation-
      i. Research Project/ Case Study 2 credits
      ii. Presentation 1 credit
      iii. External Viva Voce 1 credit
   b. Internal Evaluation- Dissertation 1 credit

2. INSTRUCTIONS FOR STUDENTS

- The student has to complete two months of career-oriented summer training from any firm/organization. If the student does not get a chance to go for training, he/she can choose a research topic and can complete the dissertation under the supervision of any of the faculty in his college.
- The student who has to opt for training has to provide a signed certificate from the firm/ organization authority stating that the student has spent two months as a trainee in his organization/firm. The student who has opted for a dissertation has to submit his/her dissertation report with a certificate from his supervisor.
- In both cases, the student has to present his work in front of all the faculty members and fellow students at the starting of the next session.
- In terms of credits, every one-hour session of L amounts to 1 credit per semester and a minimum of two-hour sessions of T or P amounts to 1 credit per semester.

*** An Academic/ Industrial Tour shall be organized by the college/department in every session. A Tour Report shall be prepared and submitted by the students after a study tour to industries/academic institutions of repute.**

Key Features of Revised Curriculum

Following are the key features of the revised curriculum-

- Student Centric Teaching and Learning approach
- Technology oriented approach of teaching
- Hand-on Practical/ Laboratory Sessions
- Problem-oriented teaching and learning
- Problem-analysis oriented assignments and evaluation
- Enhance logical thinking and analytical capabilities

Appendice

List of Open Electives offered by the University -