M.Sc. in Computer Science with Specialization in Cyber Security (Ay 2022)

Semester 1				
Course Code	**Title of the Course**	**Credits**	**Credit Split Lecture/Lab/ Seminar/Project**	**Level**
	Digital Experience Laboratory	4	1-3-0-0	300
	Design Thinking and Innovation	3	3-0-0-0	300
M2020101	Mathematics for Computer Science	4	3-0-1-0	200
M3022102	Cyber Security and Digital Forensics	3	3-0-0-0	300
	Computer Networks and Security	3	3-0-0-0	200
M2020104	Computer Architecture	3	3-0-0-0	200
M1020105	Python Programming	4	3-1-0-0	100
M3022106	Cyber Security and Forensics Lab	1	0-1-0-0	300
Total Credits		25		

Semester 2				
Course Code	**Title of the Course**	**Credits**	**Credit Split Lecture/Lab/ Seminar/Project**	**Level**
	Digital Access for Community Empowerment	3	0-0-0-3	300
M3022201	Modern Cryptography	4	3-1-0-0	300
M3022202	Cyber Analytics	3	3-0-0-0	300
M2020203	Operating Systems	3	3-0-0-0	200
	Data Structures and Algorithms	4	3-1-0-0	200
	Elective 1	4		300
M2022206	Security Auditing Lab	1	0-1-0-0	200
M3022207	Cyber Analytics Lab	1	0-1-0-0	300
Total Credits		23		

Electives for Semester 2				
Course Code	**Title of the Course**	**Credits**	**Credit Split Lecture/Lab/ Seminar/Project**	**Level**
M3020205	Augmented and Virtual Reality	4	3-1-0-0	300
M3020215	Biometrics	4	3-1-0-0	300
M3020225	Information Retrieval	4	3-0-0-1	300
M3020235	Malware Analysis and Reverse Engineering	4	3-1-0-0	300
M3020245	Cloud and Edge Computing	4	3-0-0-1	300
M3020255	Hardware Security	4	3-1-0-0	300
Total Credits		4		

Semester 2 Internship				
Course Code	**Title of the Course**	**Credits**	**Credit Split Lecture/Lab/**	**Level**

			Seminar/Project	
M3020265	M.Sc. Summer Internship/Team Project	2	0-0-0-2	300
Total Credits		2		

Semester 3				
Course Code	**Title of the Course**	**Credits**	**Credit Split Lecture/Lab/ Seminar/Project**	**Level**
M3022301	Database Security	4	3-0-0-1	300
M3022302	Ethical Hacking and Defensive Techniques	3	3-0-0-0	300
	Elective 2	4		300
	Elective 3	4		300
	Elective 4	4		300
M3022306	Ethical Hacking and Penetration Testing Lab	1	0-1-0-0	300
M3020307	IoT Experience Lab	2	0-2-0-0	300
M3020308	M.Sc. Mini Project	4	0-0-0-3	300
Total Credits		26		

Electives for Semester 3				
Course Code	**Title of the Course**	**Credits**	**Credit Split Lecture/Lab/ Seminar/Project**	**Level**
M3020303	Applied Cryptography	4	3-0-1-0	300
M3020313	Blockchain Technology	4	3-1-0-0	300
M3020323	Cognitive Computing	4	3-0-0-1	300
M3020333	Artificial Intelligence for Cyber Security	4	3-0-0-1	300
M3020343	Mobile Application Security	4	3-0-0-1	300
M3020353	Embedded Systems	4	3-0-0-1	300
M3020363	Secure Software Engineering	4	3-0-0-1	300
M3020373	Natural Language Processing	4	3-0-0-1	300
M3020383	Quantum Computing & Cryptography	4	3-0-1-0	300
M3020393	Object-Oriented Analysis and Design	4	3-0-0-1	300
M3020304	Security in Digital Transformation	4	3-0-0-1	300
M3020314	Soft Computing	4	3-0-0-1	300
M3020324	Web Technology	4	3-0-0-1	300

Semester 4				
Course Code	**Title of the Course**	**Credits**	**Credit Split Lecture/Lab/ Seminar/Project**	**Level**
M4020401	M.Sc. Internship/Project	24	0-0-0-24	400
Total Credits		24		

M2020101 MATHEMATICS FOR COMPUTER SCIENCE

Course Code	Course Name	Credit Split Lecture/Lab/Seminar/Project	Year of Introduction
M2020101	**Mathematics for Computer Science**	**3-0-1-0**	**2021**

Prerequisites: Nil

Course Objectives:

1. To provide students with a good understanding of the essential concepts of number theory, algebra, linear algebra, probability, random variables, optimization techniques, graph theory.
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to various topics in computer science, cyber security and machine learning.

Course Outcomes: After completion of this course, the students would be able to:

CO1: Understand the mathematical foundations of computer science and cyber security.
CO2: Analyze and evaluate critically the appropriate mathematical techniques required for solving various computer sciences and cyber security problems.
CO3: Apply various mathematical techniques in computer science, cyber security, and machine learning problems.

Program Learning Outcomes:

PLO 1 Develop strong fundamental disciplinary knowledge
PLO 2 Demonstrate research skills that are of experimental, computational, or theoretical nature
PLO 3 Apply scholarship to conduct independent and innovative research
PLO 4 Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
PLO 5 Practice ethical standards of professional conduct and research;
PLO 6 Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

Mapping of course outcomes with program learning outcomes:

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CO1	3	2	2	2		
CO2	1	3	3	2		
CO3	1	3	3	2		

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

Syllabus:

Module	Content

1	Basic Properties of the integers, Divisibility and primality, Congruence, Residue classes, Euler's phi function, Fermat's little theorem Groups, Subgroups, Group homomorphisms and isomorphisms, Cyclic groups, Lagrange's theorem, Field, Galois fields
2	Matrices, Systems of Linear Equations, Solving Systems of Linear Equations, Eigenvalues and Eigenvectors, Cholesky Decomposition Eigen decomposition and Diagonalization, Singular Value Decomposition Vector Spaces, Basis, Linear Mappings, Inner Products, Orthogonality, Orthonormal Basis, Orthogonal Projections, Cauchy Shwartz inequality, Gram Schmidt Orthogonalization, Norms
3	Probability, sample space, events, axioms of probability, conditional probability, independent events, Bayes Theorem, Random Variables, Expectation and variance, Distribution Function, Discrete Random Variables, Continuous Random Variables, Mean and Variance, probability distributions: uniform, Bernoulli, binomial, Poisson, Exponential, and Gaussian, MAP, MLE
4	Graph terminology and special types of graphs, representation of graphs, Graph Isomorphism, Connected Graphs, Eulerian and Hamiltonian graphs, Convex sets, convex functions, Linear Optimization, Farkas' lemma, Duality theory, The Simplex method, Convex Optimization, Gradient descent, Non linearoptimization, Karush-Kuhn-Tucker conditions, Lagrangian duality.

References

1. I. N. Herstein, *Topics in Algebra*, Second Edition, Wiley India, 2006.
2. N. Koblitz, *A Course in Number Theory and Cryptography*, Second Edition, Springer Verlag (low price edition), 1994.
3. K. Hoffman and R. Kunze, *Linear Algebra*, Prentice-Hall of India Pvt.Ltd, 1972.
4. H. P. Hsu, *Theory and problems of probability, random variables, and random processes*, New York: McGraw-Hill, May 2014.
5. M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag, 1992.
6. S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.
7. S. Sra *et al.*, *Optimization for Machine Learning,* The MIT Press, 2011.
8. D. Bertsimas and J. Tsitsiklis, *Introduction to linear optimization*, Athena Scientific, 1997.
9. E. Chong and S. Zak, *An Introduction to Optimization*, Wiley, 2004.
10. T. Hastie *et al.*, *The Elements of Statistical Learning*, Springer New York, NY, USA, 2001.
11. D. F. Stanat and D. F. McAllister, *Discrete mathematics in Computer Science,* Prentice Hall Professional Technical Reference, 1977.
12. T. Koshy, *Elementary number theory with Applications*, Elsevier, 2002.
13. G**.** Chartrand and P**.** Zhang**,** *Introduction to Graph Theory*, McGraw-Hill Companies, 2006.
14. D. B. West, *Introduction to Graph Theory*, Prentice Hall of India, 2001.

M3022102 CYBER SECURITY AND DIGITAL FORENSICS

Course Code	Course Name	Credit Split Lecture/Lab/Seminar/Project	Year of Introduction
M3022102	Cyber Security and Digital Forensics	3-0-0-0	2021

Prerequisites: Nil

Course Objectives:

1. Familiarize with cyber crimes and cyber security
2. Understand various techniques of cyber attacks and defences
3. Perform digital forensic investigations

Course Outcomes: After completion of this course, the students would be able to:

CO1 Understand various cyber attacks/crimes and cyber security mechanisms.

CO2: Perform digital forensics analysis on OS, memory, networks and network devices etc.

CO3: Utilize various cyber security and forensic tools to understand cyber attacks and collect digital evidence.

Program Learning Outcomes:

PLO 1 Develop strong fundamental disciplinary knowledge

PLO 2 Demonstrate research skills that are of experimental, computational, or theoretical nature

PLO 3 Apply scholarship to conduct independent and innovative research

PLO 4 Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

PLO 5 Practice ethical standards of professional conduct and research;

PLO 6 Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

Mapping of course outcomes with program learning outcomes:

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CO1	3	3	2			
CO2	3	3	3		3	
CO3	3	3	3		3	

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

Syllabus:

Module	Content
1	Cybercrimes and Information Security, Tools and Techniques used to commit Cyber Crimes, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Phishing Attack, Spam, Social Engineering, Cyberstalking, Credit Card Frauds, Financial crimes, Security mechanisms against these attacks and crimes .

2	Darknet, Crypto Currencies and Crimes, Crimes in Social Media and Online Financial Transactions, Attacks on Wireless Networks, Security issues in mobile platforms and applications, Security issues in cloud, Security issues in IoT networks, Security mechanisms against various attacks in these networks
3	Digital Evidence, Source and Nature of Digital Evidence, Collection of Digital Evidence, Physical Drives Imaging, Network Drives Imaging and Logical File Collection, Chain of Custody, Gathering Information from External Agencies / Companies, OS Forensics: Registry Analysis, Timestamp Analysis, Event Viewer Analysis. Memory Forensics: Volatile Data Collection, Memory Dump, Volatility Framework and Plugins, Bulk Extractor and YARA tools.
4	Network Forensics, Understanding Network Protocols with Wireshark, Packet Capturing using Wireshark, Packet Filtering, Extracting of Data from PCAP file, Analysis of Logs, Email Investigation. Virtual Machine Forensics: Importance of Virtual Machines in Forensic Analysis, Imaging of a Virtual Machine, Identification and extraction of supporting VM files in the host system.

Text Books:

1. B. Nelson *et al*., *Guide to Computer Forensics and Investigations*, Sixth Edition, 2020.
2. K. Satyanarayana, *Step by Step in Cyber Crimes Investigation, Challenges and Solutions*, Asia Law House; 1st Edition, 2020.
3. N. Godbole and S. Belapure, *Cyber Security: Understanding Cyber Crimes, Computer Fore nsics and Legal Perspectives*, Wiley, 2011,
4. J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Fore nsics*, Elsevier, 2014.
5. P. W. Singer and A. Friedman, *Cyber security and Cyber war: What Everyone Needs to Know*, Oxford University Press, 2014,
6. A. M. Marshall, *Digital Forensics: Digital Evidence in Criminal Investigation*, John – Wiley and Sons, 2008.
7. R. Krishnamurthy, *Introduction to Forensic Science in Criminal Investigation*, Selective & Scientific Books, 2015.
8. N. Reddy, *Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations*, New York, Apress, 1st Edition, 2019.

References:

1. T. J. Holt *et al*., *Cybercrime and Digital Forensics: An Introduction*, Routledge, 2nd Edition, 2017.
2. EC-Council, *Computer Forensics: Investigating Network Intrusions and Cyber Crime*, EC Council Press Series: Computer Forensics, 2016.
3. J. Bayuk, *Cyber Forensics: Understanding Information Security Investigations*, Springer's Forensic Laboratory Science Series, 2010.

COMPUTER NETWORKS AND SECURITY

Course Code	Course Name	Credit Split Lecture/Lab/Seminar/Project	Year of Introduction
	Computer Networks and Security	**3-0-1-0**	**2021**

Prerequisites: Nil

Course Objectives:

- To introduce the fundamental aspects of computer networks
- To enable the students to understand various cyber attacks targeted on computer networks
- To enable the students to develop various security mechanism for computer networks
- To enable the students to simulate various network attacks

Course Outcomes: After completion of this course, the students would be able to:

CO1: Summarize principles of Networks
CO2: Describe the layered protocol model.
CO3: Discriminate between various protocols
CO4: Appraise security threats and resolve effectively
CO5: Analyse the challenges in different network architectures

Program Learning Outcomes:

PLO 1 Develop strong fundamental disciplinary knowledge
PLO 2 Demonstrate research skills that are of experimental, computational, or theoretical nature
PLO 3 Apply scholarship to conduct independent and innovative research
PLO 4 Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
PLO 5 Practice ethical standards of professional conduct and research;
PLO 6 Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

Mapping of course outcomes with program learning outcomes:

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CO1	3	2	3	2		
CO2	3	3	3	2		
CO3	2	3	3	2		

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

Syllabus:

Module	Content

1	Network Basics: The Network Edge, The Network Core, Access Networks, Delay, Loss and Throughput, Protocol Layers and Their Service Models, Application Layer: RPC, P2P, HTTP, FTP, DNS, DHCP, Electronic Mail, WLAN, Socket, Programming with TCP & UDP
2	Transport Layer: Services, TCP, UDP, Network Layer: Functions, design issues, Internet Protocol (IP), IPV4 & IPv6, Routers, Routing algorithms, Congestion Control Algorithms
3	Data Link Layer: Design issues, framing methods, Error Detection and Correction, PPP, Sliding Window Protocols, Multiple Access Protocols, Address Resolution, Protocol (ARP), Ethernet, Link Layer Switches, Spanning Tree Protocol, VLAN
4	Security Attacks, Security Services, Security Mechanisms, Key Management and Distribution, User Authentication Protocols, SSL, TLS, Wireless Network Security, Electronic Mail Security, Vulnerability Analysis, Attacks in sensor and IoT networks, Endpoint Security, familiarization of Network simulators - NS2/NS3 or Cooja/Contiki and simulation of attacks and analyze network performance .

Text Books:

1. J. Kurose and K. Ross, Computer Networking: A Top-Down Approach, 7th Edition, Pearson, 2016.
2. A. S. Tanenbaum, Computer Networks, 5th Edition, Pearson, 2013.
3. W. Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall, 1998.
4. V. Tsiatsis *et al*., *Internet of Things: Technologies and Applications for a New Age of Intelligence*, Elsevier Academic press, 2018.
5. Z. Mahmood, *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for IoV*, Springer, 2020.
6. I. F. Akyildiz and M. Can Vuran, Wireless Sensor Networks. Wiley, 2010.

References:

1. L. L. Peterson and B. S. Davie, *Computer Networks, A systems approach*, Morgan Kaufmann, 2011.
2. S. Keshav, *An Engineering Approach to Computer Networking*, Pearson Education, 2000.
3. S. S. Shinde, *Computer Network*, New Age International, 2009.
4. P. Raj and A. C. Raman, *The Internet of Things: Enabling Technologies, Platforms, and Use Cases*, 1st Edition, Auerbach Publications, 2017.
5. A. McEwen, *Designing the Internet of Things*, Wiley, 2013.

M2020104 COMPUTER ARCHITECTURE

Course Code	Course Name	Credit Split Lecture/Lab/Seminar/Project	Year of Introduction
M2020104	Computer Architecture	3-0-0-0	2021

Prerequisites: Nil

Course Objectives:

1. To help students understand the fundamentals behind a computer and its architecture.
2. To explore the working principles of all the important building blocks of a computer.
3. To understand how these building blocks are put together to design a so-called computer.
4. To explore a few advanced topics in computer architecture.

Course Outcomes: After completion of this course, the students would be able to:

CO1: Know how different components of a computer system are working.

CO2: Apply the knowledge of computer architecture while modelling systems for security analysis.

CO3: Compare various types of computer architectures and can analyze the design principles.

CO4: Use a computer more confidently with the acquired knowledge of its constituent components.

Program Learning Outcomes:

PLO 1 Develop strong fundamental disciplinary knowledge

PLO 2 Demonstrate research skills that are of experimental, computational, or theoretical nature

PLO 3 Apply scholarship to conduct independent and innovative research

PLO 4 Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

PLO 5 Practice ethical standards of professional conduct and research;

PLO 6 Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

Mapping of course outcomes with program learning outcomes:

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CO1	3		2			
CO2		3	3	2	3	3
CO3	2	3	2	1	2	1
C04	2	2	3	2	3	2

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

Syllabus:

Module	Content
1	Computer Fundamentals: Computer types, functional units, Basic concepts. Von Neumann Architecture Instruction Sets: Machine instructions, Memory operations, addressing modes, Instructions sets, Stacks, Subroutines, RISC & CISC architectures.
2	Processing Unit: Components (Registers, ALU, Datapath), Instruction execution, Control signals, Operations of control unit: Hardwired controlled unit, Microprogrammed control unit) - horizontal and vertical micro-programming, Computer Arithmetic: Basic operations on signed numbers, Floating point operations.
3	Memory Management: Memory Hierarchy, Semiconductor based memory (Internal Organization, SRAM, DRAM), Read only memory, Cache memories – mapping techniques, Performance, Virtual memory (Address translation), Memory management, Secondary storage, RAID introduction Input/output: Accessing I/O devices, Bus Operations, I/O Modules, I/O Control mechanisms – Programmed I/O, Interrupt controlled, Direct Memory Access, I/O Interface (Serial, Parallel), I/O interconnection Standards.
4	Pipelining: Pipeline concept, Speedup, Throughput, Hazards in pipeline – structural hazard, data hazard, control hazard: Branch hazard; Dealing with hazards - Register Renaming, Branch Prediction. Advanced Computer Architecture: Parallel Processing - Flynn's classification, Amdahl's law, Characteristics of Multiprocessors, Interconnection Structures, Interprocessor Arbitration, Interprocessor Communication and Synchronization, Cache Coherence, Vector/Array Processing.

Text Books:

1. C. Hamacher *et al*., *Computer Organization*, 6th Edition, McGraw-HillHigher Education, 2011.
2. D. A. Patterson and J. L. Hennessy, *Computer Organization and Design – The Hardware/Software Interface*, 6th Edition, Morgan Kaufmann, 2020.
3. W. Stallings, *Computer Organization & Architecture designing for performance*, 8th Ed., Pearson, 2009,
4. P. Pal Chaudhuri, *Computer Organization and Design*, 3rd Edition, PHI, 2008.
5. A. S. Tanenbaum, *Structured Computer Organization*, 6th Edition, Pearson, 2012.

References:

1. J. P. Hayes, *Computer Architecture and Organization*, 3rd Ed., Mcgraw-Hill Education, 1998.
2. M. M. Mano, *Computer Systems Architecture*, 3rd Ed., Pearson/PHI, 1992.

M1020105 PYTHON PROGRAMMING

Course Code	Course Name	Lecture/Lab/Seminar/Project Credits	Year of Introduction
M1020105	**Python for Data Science**	**3-1-0-0**	**2021**

Prerequisites: Nil

Course Objectives:

- To help students learn the problem-solving techniques.
- To help students understand the fundamental concepts of programming using the Python programming language and introduce the basic concepts of Object-Oriented programming in Python.
- To introduce students to the database concepts and simple data science tools.
- To help students build practical skills for solving problems computationally.

Course Outcomes: After completion of this course, the students would be able to:

CO1: Explain the basic concepts of computational problem solving, and procedural and object-oriented programming paradigms and database programming.

CO2: Use algorithms and flowcharts to layout the procedure to solve a problem**.**

CO3: Explain the basics of Python such as variables, datatypes, control structures, functions and files and apply the knowledge of python to solve computational problems.

CO4: Explain coding and analyzing data with Python using tools like Pandas, NumPy, and Matplotlib and understand the basics of cybersecurity data analytics.

Program Learning Outcomes:

PLO 1 Develop strong fundamental disciplinary knowledge

PLO 2 Demonstrate research skills that are of experimental, computational, or theoretical nature

PLO 3 Apply scholarship to conduct independent and innovative research

PLO 4 Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

PLO 5 Practice ethical standards of professional conduct and research;

PLO 6 Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

Mapping of course outcomes with program learning outcomes:

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CO1	3					
CO2	3					1
CO3	3					
CO4	3			2		1

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

Syllabus:

Module	Content

1	Computational Problem Solving. Algorithms and Flowcharts, Introduction to Computer Programming. Programming Paradigms and Programming Languages. Introduction to Object Oriented Programming. Introduction to Database Programming and Scripting. Software Development Process. Programming Code of Ethics. Introduction to Python. Real-world Applications of Python. Features of Python Programming Language. Implementations of Python. Python Career Opportunities.
2	Python Data Types, Variables, Basic Input-Output Operations, Basic Operators. Boolean Values, Conditional Execution, Loops, Lists and List Processing, Logical and Bitwise Operations. Functions, Tuples, Dictionaries, and Data Processing. Modules, Packages, String and List Methods, and Exceptions.
3	The Object-Oriented Approach: Classes, Methods, Objects, and Exception Handling. A brief introduction to OO Design. File Handling in Python. Introduction to Data Science. Tools for Data Science (GitHub, Jupyter Notebooks). Database Concepts and SQL. SQL using Python.
4	Data Handling using NumPy and Pandas. Data Visualization in Python. Simple projects. Case studies.

Lab Exercises:

Module 1:

1. Problems on number systems and data encoding.
2. Writing simple algorithms and flowcharts.
3. Writing advanced algorithms and flowcharts, installing and running Python.
4. Writing simple programs (e.g. Drake equation) to familiarize with variables, keywords, operators, expressions, data types and operator precedence. The print() function, type conversion, formatting numbers and strings.

Module 2:

5. Conditional statements, writing simple scripts, using comments for program readability.
6. Loops, nested loops, break and continue statements (e.g. Prime number, Fibonacci series, Factorial, Armstrong number, Palindrome)
7. Built-in data structures and their applications - Lists, Tuples, Sets and Dictionaries, Range function, Functions such as zip() and enumerate().
8. More coding exercises using lists (e.g. Merging sorted lists), tuples, sets, dictionaries.

Module 3:

9. Defining and calling functions: Passing arguments and returning values (e.g. Pascal's triangle.), scope, local functions, Lambda functions, function redefinition, standard library modules.
10. File and exception handling.
11. Coding exercises to practice Object Oriented Programming.

Module 4:

12. Data Handling using NumPy and Pandas.
13. Python and SQL
14. Data Visualization in Python

Text Books:

1. C. Dierbach, *Introduction to Computer Science Using Python: A Computational Problem-Solving Focus*, Wiley, 2017.
2. A, N. Kamthane and A. A. Kamthane, *Programming and Problem Solving with*

Python, McGraw-Hill Education, 2018.
3. S. F. Lott, *Object Oriented Python*, Packt Publishing, 2014.
4. W. McKinney, *Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython*, O'Reilly Media, 2012.

References:

1. R. Thareja, Python Programming using Problem Solving Approach, Oxford Higher Education, 2017.
2. B. N. Miller and David L. Ranum, Problem Solving with Algorithms and Data Structures Using Python, Franklin, Beedle & Associates, 2011.
3. D. D. Riley and K. A. Hunt, Computational Thinking for the Modern Problem Solver, CRC Press, 2014.
4. J. VanderPlas, Python Data Science Handbook, Github.
5. F. Nelli, Python Data Analytics: With Pandas, NumPy, and Matplotlib, Second Edition, Kindle Edition.

M3022106 CYBER SECURITY AND FORENSICS LAB

Course Code	Course Name	Credit Split Lecture/Lab/Seminar/Project	Year of Introduction
M3022106	**Cyber Security and Forensics Lab**	**0-1-0-0**	**2021**

Prerequisites:
Nil

Course Objectives:

1. Perform various cyber security attacks
2. Test tools to detect and prevent cyber attacks
3. Perform digital forensic investigations using various tools

Course Outcomes: After completion of this course, the students would be able to:

CO1 Simulate cyber attacks/crimes and cyber security mechanisms.
CO2: Perform digital forensics analysis on OS, memory, networks and network devices etc.
CO3: Utilize various cyber security and forensic tools to understand cyber attacks and collect digital evidence.

Program Learning Outcomes:

PLO 1: Develop strong fundamental disciplinary knowledge
PLO 2: Demonstrate research skills that are of experimental, computational, or theoretical nature
PLO 3: Apply scholarship to conduct independent and innovative research
PLO 4: Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

PLO 5: Practice ethical standards of professional conduct and research;
PLO 6: Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

Mapping of course outcomes with program learning outcomes:

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CO1	3	3	2			
CO2	3	3	3		3	
CO3	3	3	3		3	

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

Syllabus:

Module	Content
1	Testing strengths of passwords using password cracking tools, Monitoring using key loggers, Familiarization with malwares: creating test malwares and detecting them, Using steganographic tools for hiding data, Launching SQL injection attacks and prevention, Studying XSS and XSRF attacks, Studying phishing attacks, Implementing buffer over flows and analyzing the vulnerabilities, Familiarization with major open source cyber security tools, Investigating on latest trends in the cyber attacks.
2	Familiarize with Android application .apk files. By performing static and dynamic analysis on the app find the vulnerable application and document the inferences, perform mobile device forensics, Investigate crimes in Darknet, crimes involving crypto currencies, crimes in social media and crimes in online financial transactions Perform social media forensics, Perform email forensics
3	File carving for digital forensics, Familiarization of various tools used in disk forensics, OS Forensics, Perform Registry Analysis, Timestamp Analysis, Event Viewer Analysis. Familiarization of various tools used in Memory Forensics, Perform Volatile Data Collection, Memory Dump Familiarize with volatility Framework and Plugins, Bulk Extractor and YARA tools.
4	Familiarization of various tools used Network forensics, Familiarization of various tools used for Image, audio and video forensics, Familiarization of various anti forensics tools.

Text Books:

1. M. Gregg, *Build Your Own Security Lab: A Field Guide for Network Testing*, 1st Edition, Wiley, 2008.
2. M. Gregg, The *Network Security Test Lab: A Step-by-Step Guide*, 1st Edition, Wiley, 2015.
3. B. Nelson *et al., Guide to Computer Forensics and Investigations*, Sixth Edition, 2020.
4. K. Satyanarayana, *Step by Step in Cyber Crimes Investigation, Challenges and Solutions*, Asia Law House, 1st Edition, 2020.
5. N. Godbole and S. Belapure, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, 2011.
6. J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, Elsevier, 2014.
7. P. W. Singer and A. Friedman, Cyber *security and Cyber war: What Everyone Needs to Know,* Oxford University Press, 2014.
8. A. M. Marshall, *Digital Forensics: Digital Evidence in Criminal Investigation*, John – Wiley and Sons, 2008.
9. R. Krishnamurthy, *Introduction to Forensic Science in Criminal Investigation*, Selective & Scientific Books, 2015.
10. N. Reddy, *Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations,* Apress, 1st Edition, 2019.

References:

1. T. J. Holt *et al.*, *Cybercrime and Digital Forensics: An Introduction*, Routledge, 2nd Edition 2017.
2. EC Council, *Computer Forensics: Investigating Network Intrusions and Cyber Crime,* EC Council Press Series: Computer Forensics, 2016.
3. J. Bayuk*, Cyber Forensics: Understanding Information Security Investigations,* Springer's Forensic Laboratory Science Series, 2010.