CC 1- Fundamentals of Computing - using C Language

Course Objective: The course is designed to provide a working knowledge and skills of programming with C Language. Students will be able to develop logics which will help them to create programs. Also by learning the basic programming constructs they can easily be able to grasp any other new computer languages in future.

Sl	Course Outcome (CO)
1	Remember & Understand the Computer Fundamentals
2	Remember & Understand the Program methods using C
3	Understand general problem solving using C
4	Understand& Apply control flow, function of PS, Arrays & Pointers using C
5	Analyse the Structure and Input & Output using C
6	Application& Analysis using guided competitive programming laboratory work

THEORY- CYS (T) 101

CO	Blooms Level (if applicable)	Modules	%age of questions
CO1	1,2	M1, M2	20
CO2	1,2	M2, M3	20
CO3	1,2	M2, M3	20
CO4	2,3	M3, M4	20
CO5	2,3,4	M3, M4, M5	20
CO6	1,2,3,4	M2, M3, M6	
			100

PRACTICAL- CYS 191

CO	Blooms Level (if applicable)	Modules	%age of questions
CO1	1,2		
CO2	1,2	M2, M3	15
CO3	1,2	M2, M3	40
CO4	2,3	M3, M4	35
CO5	2,3,4	M3, M4, M5	10
CO6	1,2,3,4		
			100

Credits- 4T +2P

Module 1-Computer fundamentals: Computing systems: hardware & software, Architecture & organization history: von Neumann Architecture: memory, processor, I/O; Data vs Information: Bit, byte number system: binary, octal, hexadecimal, 1's, 2's complement arithmetic, digital logic: AND, OR etc. BIOS, Booting, Application software, system software, Introduction of Operating systems, program, process; introduction of programming languages: brief overview of Pascal, FORTRAN, and BASIC**. (Total Hours-8)**

Module 2- Programming Method: Debugging, macro, User defined Header, User defined Library Function, make file **(Total Hours-5)**

Module 3- General problem solving concepts: Algorithm and Flowchart for problem solving with Sequential Logic Structure, Decisions and Loops, time & space complexity; Imperative languages: Introduction to imperative language; syntax and constructs of a specific language (ANSI C*).*
Variable Names, Data Type and Sizes (Little Endian Big Endian), Constants, Declarations, Arithmetic Operators, Relational Operators, Logical Operators, Type Conversion, Increment Decrement Operators, Bitwise Operators, Assignment Operators and Expressions, Precedence and Order of Evaluation, proper variable naming and Hungarian Notation **(Total Hours-6**)

Module 4- Control Flow, Function of PS, Arrays& Pointers: Statements and Blocks, If-Else-If, Switch, Loops – while, do, for, break and continue, Goto Labels, structured and un- structured programming. Basics of functions, parameter passing and returning type, C main return as integer, External, Auto, Local, Static, Register Variables, Scope Rules, Block structure, Initialisation, Recursion, Preprocessor, Standard Library Functions and return types.Arrays, Pointers and address, Pointers and Function Arguments, Pointers, Address Arithmetic, character Pointers and Functions, Pointer Arrays, Pointer to Pointer, Multi-dimensional array and Row/column major formats, Initialization of Pointer Arrays, Command line arguments, Pointer to functions, complicated declarations and how they are evaluated. (Total Hours-16)

Module 5- Structures Input & Output: Basic Structures, Structures and Functions, Array of structures, Pointer of structures, Self-referral Structures, Table look up, Typedef, Unions, Bit-fields.
Standard I/O, Formatted Output – printf, Formated Input – scanf, Variable length argument list, file access including FILE structure, fopen, stdin, sdtout and stderr,Error Handling including exit, perroranderror.h,LineI/O,relatedmiscellaneous functions, scope of advance C, a brief introduction of VDU basics, Mouse programming, C- assembly**. (Total Hours-9)**

Module 6- Competitive Programming Laboratory

1. Algorithm and flowcharts of small problems likeGCD
2. Structured code writingwith:

a. Small but trickycodes
b. Proper parameterpassing
c. Command lineArguments
d. Variableparameter
e. Pointer tofunctions
f. User definedheader
g. Make fileutility
h. Multi file program and user definedlibraries
i. Interesting substring matching / searchingprograms
j. Relatedassignments

(Total Hours-12)

Text Books:

1. Herbert Schildt, “C: The Complete Reference”, Fourth Edition, McGrawHill.
2. B. Gottfried, “Programming in C”, Second Edition, Schaum OutlineSeries.
3. R.S. Salaria, “Problem Solving and Programming in C”, Khanna PublishingHouse

Reference Books:

1. B. W. Kernighan and D. M. Ritchi, The ‘C Programming Language”, Second Edition,PHI.
2. YashavantKanetkar, “Let Us C”, BPBPublications.
3. R.S. Salaria, “Computer Concepts and Programming in C”, Khanna PublishingHouse

CC 2- Mathematics and Statistics (including Lab)

Course Objective: The course is designed to provide a basic understanding and knowledge of Mathematics, Probability and Statistics for Computing. Students will be able to apply Mathematics and Statistics to solve problems related to Cyber Security.

Sl	Course Outcome (CO)
1	Learn& Understand the Mathematics for Computation
2	Apply the Mathematics to Computational Problems
3	Learn and Understand Probability Theory and Basic Statistics
4	Apply Combinatorics to Build Statistical Distribution
5	Apply Probability Theory to Cyber Security Problems
6	Analyse Data to Build Statistical Models

THEORY- CYS(T) 102

CO	Blooms Level (if applicable)	Modules	%age of questions
CO1	1,2,3	M1, M2	15%
CO2	1,2,3	M1, M2	25%
CO3	1,2,3	M3, M4	15%
CO4	1,2,3,4	M3, M4, M5	25%
CO5	1,2,3,4	M3, M4, M5	20%
CO6	3,4		
			100

PRACTICAL- CYS 192

CO	Blooms Level (if applicable)	Modules	%age of questions
CO1	1,2,3		
CO2	1,2,3	M1, M2	40%
CO3	1,2,3		
CO4	1,2,3,4	M3, M4, M5	20%
CO5	1,2,3,4	M3, M4, M5	20%
CO6	3,4	M5, M6	20%
			100

Credits-4T+2P

Module 1: Discrete Mathematics

Sets, Relation and Function: Operations and Lawsof Sets, Cartesian Products, Binary Relation, PartialOrdering Relation, Equivalence Relation, Image of aSet, Sum and Product of Functions, Bijectivefunctions, Inverse and Composite Function, Size ofa Set, Finite and infinite Sets, Countable anduncountable Sets, Cantor's diagonal argument andThe Power Set theorem, Schroeder-Bernsteintheorem.

Principles of Mathematical Induction: The WellOrdering Principle, Recursive definition, TheDivision algorithm: Prime Numbers, The GreatestCommon Divisor: Euclidean Algorithm, TheFundamental Theorem of Arithmetic.

(Total Hours-8)

Module 2: Algebraic Structures and Morphism

AlgebraicStructures with one Binary Operation, Semi-Groups, Monoids, Groups, Congruence Relation andQuotient Structures, Free and Cyclic Monoids and Groups, Permutation Groups, Substructures,Normal Subgroups, Algebraic Structures with twoBinary Operation, Rings, Integral Domain andFields. Boolean Algebra and Boolean Ring,

Identities of Boolean Algebra, Duality,Representation of Boolean Function, Disjunctiveand Conjunctive Normal Form

(Total Hours-8)

Module 3: Combinatorics and Probability

Set Theory, Basic Probability and Venn diagram, Compound Probability of independent events, Dependantevents, Permutations and Combinations, Probability using Combinatorics, pigeon-hole principle

(Total Hours-6)

Module 4: Frequency Distribution

Data presentation- Frequency table, histogram, Barchart and frequency polygons, stem and leaf plots, measure of location and spread, box andwhisker plots

(Total Hours-10)

Module 5: Introduction to Statistics

Definition and scope of Statistics, concepts of statistical population and sample.

Data: quantitative and qualitative, attributes, variables, scales of measurement - nominal, ordinal,interval and ratio. Presentation: tabular and graphic, including histogram and ogives.

Measures of Central Tendency: mathematical and positional. Measures of Dispersion: range,quartile deviation, mean deviation, standard deviation, coefficient of variation, moments,skewness and kurtosis.
(Total Hours-14)

Module 6: Bivariate Statistics
Definition, scatter diagram, simple, partial and multiple correlation (3 variablesonly), rank correlation. Simple linear regression, principle of least squares and fitting of polynomials and exponential curves.
Theory of attributes, consistency of data, independence and association of attributes,measures of association and contingency.
(Total Hours-10)

Text Books:

1. Russell Merris, Combinatorics, Wiley-Interscience series in Discrete Mathematics andOptimisation
2. N. Chandrasekaran and M. Umaparvathi, Discrete Mathematics, PHI
3. Goon A.M., Gupta M.K. and Dasgupta B. (2002): Fundamentals of Statistics, Vol. I & II, 8th Edn. The World Press, Kolkata.

Paper: English Communication
Code: CYS-164

Course Objective: The course is designedto develop the student's communicative competence in English by giving adequate exposure in the four communication skills - LSRW - listening, speaking, reading and writing and the related sub-skills, thereby, enabling the student to apply the acquired communicative proficiency in social and professional contexts.

Sl	Course Outcome	Mapped modules
1	Students will be able to Remember & Understand the basic concepts of the usage of English grammar & vocabulary in communication.	M1
2	Students will be able to Comprehend facts and ideas by organizing, comparing, translating, interpreting, giving descriptions, and stating the main ideas given in written texts.	M1,M2
3	Students will be able to Synthesise and Apply acquired linguistic knowledge in producing various types of written texts	M1, M3
4	Students will be able to Comprehend facts and ideas from aural inputs and Synthesise and Apply acquired linguistic knowledge in giving spoken response	M1, M4

Module Number	Content	Total Hours	%age of questions	Blooms Level (if applicable)	Remarks (If any)
M 1	Functional grammar & Vocabulary	2	10	1,2	
M 2	Reading Skills	2	20	1,2	
M 3	Writing Skills	8	40	2,3,4,	
M 4	Listening & Speaking Skills	8	30	2,3,4	
		20	**100**		

Paper: English Communication
Code: CYS 164
Contact Hours / Week: 2L
Credits: 2

Module 1 : Functional Grammar & Vocabulary : Tense: Formation and application; Affirmative / Negative / Interrogative formation; Modals and their usage; Conditional sentences; Direct and indirect speech; Active and passive voice; usage of common phrasal verbs, synonyms & antonyms.
1L + 1T

Module 2 : Reading Skills: Comprehension passages; reading and understanding articles from technical writing. Interpreting texts: analytic texts, descriptive texts, discursive texts; SQ3R reading strategy. 1L + 1T

Module 3 : Writing Skills: Writing business letters - enquiries, complaints, sales, adjustment, collection letters, replies to complaint & enquiry letters; Job applications, Résumé, Memo, Notice, Agenda, Reports – types & format, E-mail etiquette, advertisements 4L + 4T

Module 4 : Listening & Speaking
Listening: Listening process, Types of listening; Barriers in effective listening, strategies of effective listening
Speaking: Presentations, Extempore, Role-plays, GD, Interview 4L + 4T

Suggested readings:

1. Bhatnagar, M &Bhatnagar, N (2010) Communicative English for Engineers and Professionals. New Delhi: Pearson Education.
2. Raman, M & Sharma, S (2017) Technical Communication. New Delhi: OUP.
3. Kaul, Asha (2005) The Effective Presentation: Talk your way to success. New Delhi: SAGE Publication.
4. Sethi, J &Dhamija, P.V. (2001), A Course in Phonetics and Spoken English. New Delhi:PHI.
5. Murphy, Raymond (2015), English Grammar in Use. Cambridge: Cambridge University Press

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

2nd Semester

Subject Type	Course Name	Course Code	Credit Distribution			Credit Points	Mode of Delivery			Proposed Moocs
			Theory	Practical	Tutorial		Offline	Online	Blended	
CC 3	Computer Architecture & Object Oriented Concepts	CYS (T) 201	4	0	0	6	✓			As per MAKAUT Notification
		CYS 291	0	2	0					
CC 4	Data Structures & Algorithms	CYS (T) 202	4	0	0	6	✓			
		CYS 292	0	2	0					
GE 2	Students will have to choose from the GE Basket					6			✓	
AECC 2	Environmental Science	CYS 265	2	0	0	2	✓			
Semester Credits						**20**				

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

Course: Computer Architecture & Object-Oriented Concepts

Credits- 4T+2P

Course Objective: The course is designed to provide an elaborate idea about the different memory systems and buses and introduce processor architecture to students. Also give them a knowledge about object oriented programming concepts to enable them to develop efficient codes.

Sl	Course Outcome	Mapped modules
1	Remember & Understand the structure, function and characteristics of computer systems	M1, M2
2	Remember & Understand the design of the various functional units and components of computers	M2 ,M3
3	Understand and identify the elements of modern instructions sets and their impact on processor design.	M1, M4
4	Understand & Apply the function of each element of a memory hierarchy	M1, M3,M4
5	Analyse the Structure and Input & Output using C++	M5, M6
6	Application & Analysis using guided competitive programming laboratory work	M5 ,M6

Theory- CYS(T) 201

Module Number	Content	Total Hours	%age of questions	Blooms Level (if applicable)	Remarks (If any)
M 1	Computer Organization & Memory System	10	20	1,2	
M 2	Computer Arithmetic	5	25	1,2	
M 3	Input and Output System	10	30	2	
M 4	Instruction Set and addressing modes	10	25	2,3	
		35	**100**		

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

Practical- CYS 291

Module Number	Content	Total Hours	%age of questions	Blooms Level (if applicable)	Remarks (If any)
M 5	Concepts of OOP & Basics of C++	10	40	4	
M 6	Objects and Classes	10	60	3,4	
		20	**100**		

Detailed Syllabus

Module I: Computer Organization & Memory System (10L)
Computer types, Structure with basic computer components, Function in brief with instruction fetch and execute, Interrupts and I/O communication, Interconnection structure, bus interconnection, Multiple Bus hierarchies, Elements of bus design Performance metrics and measurement.
Memory hierarchy, Main memory definition, types of main memory, types of RAM, ROM, difference between SRAM & DRAM. Cache memory, Cache memory mapping – Direct, Associative, Set Associative, Virtual memory, mapping using pages, page fault, mapping using segments, TLB

Module II : Computer Arithmetic (5L)
Addition and Subtraction algorithm of sign magnitude number. Addition and subtraction algorithm for signed 2's complement data. Multiplication algorithm, Booth's algorithm and division algorithm.

Module III : Input and Output System (10L)
Peripheral devices, Input – output interface, Isolated I/O, Memory mapped I/O, Asynchronous data transfer: strobe & handshaking, Programmed I/O, Interrupt initiated I/O, Basic idea of DMA

Module IV : Instruction Set and addressing modes (10L)
Instruction codes, Direct address, Indirect address & Effective address, List of basic computer registers, Computer instructions: memory reference, register reference & input – output instructions, Block diagram & brief idea of control unit of basic computer, Instruction cycle

Module V: Concepts of OOP & Basics of C++ (10L)
Introduction to OOP, Procedural vs OOP, Program structure, namespace, identifiers, variable, constants, enum, operators, typecasting, control structure. Simple functions, call and return by reference, inline function, overloading of functions, friend functions

Module VI : Objects and Classes (10L)
Basic of objects and classes in C++, Private and public, static data and function member, constructor and their types, destructor, Inheritance, Polymorphism

Text Books:

1. Computer System Architecture, M. Morris Mano, PEARSON
2. Computer Organization & Architecture – Designing For Performance, William Stallings, PEARSON
3. Computer Architecture & Organisation, J.P. Hayes, TATA MCGRAW HILL
4. Computer Organization and Architecture, T. K. Ghosh, TATA MCGRAW-HILL 5. Computer Architecture, Behrooz Parhami, OXFORD UNIVERSITY PRESS
5. Object Oriented Programming With C++, E Balagurusamy, TMH
6. Mastering Object Oriented Programming in C++, R.S. Salaria, Khanna

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

Course: Data Structures and Algorithms
Credits- 4T+2P

Course Objective: The course is designed to introduce the fundamental concept of data structures and to emphasize the importance of data structures in developing and implementing efficient algorithms. In addition, another objective of the course is to develop effective software engineering practice, emphasizing such principles as decomposition, procedural abstraction, and software reuse.

Sl	Course Outcome	Mapped modules
1	Remember & Understand how the choice of data structures and algorithm design methods impacts the performance of programs.	M1
2	Remember & Understand how to solve problems using data structures such as linear lists, stacks, queues, hash tables, binary trees	M4, M5
3	Understand and identify the ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs	M1, M2, M3, M4, M5, M6
4	Understand & Apply the appropriate data structure and algorithm design method for a specified application	M2 M3,M4, M5, M6
5	Analyse the ability to apply design and development principles in the construction of software systems of varying complexity	M2, M5, M6
6	Application & Analysis using guided competitive programming laboratory work	M4, M5 ,M6

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

Theory- CYS(T) 202

Module Number	Content	Total Hours	%age of questions	Blooms Level (if applicable)	Remarks (If any)
M 1	Concepts of Abstract data type	4	10	1,2	
M 2	Data Structure using Array	4	20	1,2	
M 3	Searching and Sorting	6	20	2	
M 4	Linked List	5	20	2,3	
M5	Trees	6	10	2,3	
M6	Graphs & Hashing	10	20	2,3	
		35	**100**		

Practical- CYS 292

Module Number	Content	Total Hours	%age of questions	Blooms Level (if applicable)	Remarks (If any)
M 2	Data Structure using Array	2	20	1,2	
M 3	Searching and Sorting	4	20	2	
M 4	Linked List	4	20	2,3	
M5	Trees	5	20	2,3	
M6	Graphs & Hashing	5	20	2,3	
		20	**100**		

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

Detailed Syllabus-

Module I: Concepts of Abstract data type(4L)
Concept of abstract data types, Structure, union, enum, pointer to structure, Self-referential structure, Pointer to pointer

Module II: Data Structure using Array(4L+2L)
stack, queue, circular queue, priority queue, dequeue and their operations and applications.

Module III: Searching and Sorting(6L+4L)
Searching: linear search, Binary search, their comparison, Sorting: insertion sort, Selection sort. Quick sort, Bubble sort Heap sort, Comparison of sorting methods , Analysis of algorithm, complexity using big 'O' notation

Module IV: Linked List(5L+4L)
Linear link lists, doubly linked lists, stack using linked list, queue using linked list, circular linked list and their operations and applications.

Module V: Trees (6L+5L)
Binary trees, binary search trees, representations and operations, thread representations, sequential representations, B tree B+ tree,

Module VI: Graphs & Hashing (10L+5L)
Introduction to graphs, Definition, Terminology, Directed, Undirected & Weighted graph, Representation of graphs, Graph Traversal: Depth first search and Breadth first search. Spanning Trees, minimum spanning Tree, Shortest path algorithm. Definition of hashing, Hashing functions, Load factor and collision, open addressing (linear probing) and chaining method to avoid collision.

Text Books

1.Data structure using c and c++ - Tanenbaum
2.Fundamentals of Data structure in c++ - E.Horwitz,Sahni,D.Mehta

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

AECC 2- Environmental Science

Semester Credits- 2T

Course Objective: The course is designed to provide a working knowledge of environment, ecology and physical sciences for problem solving. The learner will be able to remember, understand and apply the taught concepts and methods involving social and environmental processes for betterment of environmental health and safety.

COURSE OUTCOMES (CO):

Sl	Course Outcome	Mapped modules
1	Be able to remember the basic concepts related to environment & ecology	M1,M2
2	Be able to remember & understand the scientific problem related to air, water, noise & land pollution	M1, M2
3	Be able to understand environmental laws , regulations , guidelines and n applying those for maintaining quality of environmental health and safety .	M1, M2,M3

Module Number	Content	Total Hours	%age of questions	Covered CO	Blooms Level
Module 1	Environmental Concepts	7	30%	1,2	L1
Module 2	Resources & Pollution	6	30%	2,3	L1, L2

Module 3	Environment Management	7	40%	1,2,3	L2,L3

SYLLABUS

Module 1: Environmental Concepts – Definition & basic concept of Environment & Ecology, man, society & environment, their interrelationship, Elements of ecology elements of ecology - species, population, community, definition of ecosystem- Structure & function of ecosystem (Bio geo chemical cycles, food chain, energy flow, ecological pyramid), Biodiversity & its threats and remedies. [7]

Module 2: Resources & Pollution – renewable & non-renewable resources, Bio-degradable and non-biodegradable pollutants, Sources & Effects of Pollution, Methods of Control (Air, Water. Land, & Noise)

Module 3: Environment Management - Concept & scope of environment Management, National environmental policy & Environmental Legislations in India, Environment Management System – ISO 14000, Environmental Audit, Eco mark, green Industry, Cases on Environment Impact Assessment.

REFERENCES

Suggested Readings
1. N.K. Oberoi: Environmental Management, Excel Books
2. G.N. Pandey: Environmental Management, Vikas
3. K.M. Agrawal & P.K. Sikdar: Text Book of Environment, MacMillan
4. L.W. Canter: Environmental Impact Assessment, McGraw Hill
5. M.P. Poonia & S.C. Sharma, Environmental Studies, Khanna Publishing House (AICTE Recommended Textbook – 2018)
6. Masters, G. M., “Introduction to Environmental Engineering and Science”, Prentice-Hall of India Pvt. Ltd.,1991.
7. De, A. K., “Environmental Chemistry”, New Age International
8. Fundamentals of Ecology -Odum, E.P.

9. Instant notes on Ecology -Mackenzie, A., Ball, A.S. and Virdee, S.R. (1999) Viva Books
10. G. Dasmahapatra – Basic Environmental Engineering & Elementary Biology, Vikas Publication
11. Environmental Science, Cunningham, TMH
12. Environmental Pollution Control Engineering, C.S.Rao,New Age International
13. Environmental Science, Wright & Nebel, PHI
14.Environmental Pollution Analysis, S.M.Khopkar, New Age International

3rd Semester

 # Only in case offline classes are not possible due to reasons like COVID Pandemic the classes will be in synchronous online mode

Subject Type	Course Name	Course Code	Credit Distribution			Credit Points	Mode of Delivery			Proposed Moocs
			Theory	Practical	Tutorial		Offline#	Online	Blended	
CC 5	Ethical Hacking and Systems Defence	CYS (T) 301	4	0	0	6	✓			As per MAKAUT Notification
		CYS 391	0	2	0					
CC 6	Cyber Systems & Cyber Threat and Modelling	CYS (T) 302	4	0	0	6	✓			
		CYS 392	0	2	0					
CC 7	Vulnerability Analysis, Penetration Testing, and Incident Handling	CYS (T) 303	4	0	0	6	✓			
		CYS 393	0	2	0					
GE 3	Students will have to choose from the GE Basket					6			✓	
SEC 1	Operating System and Linux	CYS 354	0	2	0	2	✓			
Semester Credits						**26**				

CYS 301- Ethical Hacking and Systems Defence

Credits- 4L+2P

Course Objective: The course is designed to provide an elaborate idea about the different system hacking techniques with proper ethics and applying system defence techniques.

Sl	Course Outcome	Mapped modules
1	Understand and experiment with ethical hacking.	M1
2	Understand and experiment with system hacking.	M2
3	Make use of TCP/IP overview concepts and port scanning.	M3
4	Analyse desktop and server operating systems(OS) vulnerabilities.	M4
5	Assess details of system and network security.	M5
6	Inspect vulnerabilities in OS.	M6

Theory – CYS(T) 301

Mapped Modules	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Introduction to Ethical Hacking	10	25	1,2,3	
M2	System Hacking	14	25	1,2,3	
M3	TCP/IP Overview Concepts and Port Scanning	14	30	2,3	
M4	Desktop and Server OS Vulnerabilities	10	20	3,4	
		48	**100**		

Practical- CYS 391

Mapped Modules	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M5	System and Network Security	14	60	3,4,5	
M6	Identifying vulnerabilities in OS	14	40	3,4,5	
		28	**100**		

Ethical Hacking and Systems Defence

MODULE 1: INTRODUCTION TO ETHICAL HACKING:
Introduction: Hacking/ Ethical hacking, Types of Hacking/Hackers, Cybercrime, Types of cybercrime, Hacker Mind set, Threats, Concept of ethical hacking, Phases involved in ethical hacking, Role of Ethical Hacking, Common Hacking Methodologies, Profiles of Hackers, Benefits of Ethical Hacking, Limitations of Ethical Hacking, Foot printing-Social Engineering-Scanning and enumeration

MODULE 2: SYSTEM HACKING:
System hacking, Types of System hacking, ha4cking tools, Computer Hole, Hacking Process, Various methods of password cracking, Remote Password Guessing, Role of eavesdropping, Keystroke Loggers, Types of Keystroke Loggers, Detection, Prevention and Removal, Rootkits-Trojans-Backdoors-Viruses and worms, sniffers-denial of service-Session hijacking.

MODULE 3: TCP/IP OVERVIEW CONCEPTS AND PORT SCANNING:
Review of TCP/IP Internetworking, Networking and Security Overview, Attack Methods, Access Control and Site Security, Host Security, Security issues in Internet protocols: TCP, DNS, and routing, Overview of TCP/IP-IP addressing-numbering systems- Introduction to port scanning-types of port scan port scanning tools-ping sweeps- Understanding scripting-Enumeration.

MODULE 4: DESKTOP AND SERVER OS VULNERABILITIES: OS Security Vulnerabilities, Programming Bugs and Malicious code, Windows OS vulnerabilities-tools for identifying vulnerabilities in windows-Linux OS vulnerabilities, vulnerabilities of embedded OS.

MODULE 5: System and Network Security: Desktop Security, Operating System Security: Designing Secure Operating Systems, Understanding routers-understanding firewalls-risk analysis tools for firewalls- understanding intrusion and detection and prevention systems-honeypots, Disaster recovery, Digital Signature, International Standards maintained for Cyber Security, Security Audit, and Investigation by Investing Agency.

Module 6: Practical: Identifying vulnerabilities in OS, Computer Forensics, Practical: hacking the server (through virtual machine), Micro Project.

Suggested Readings

1 Michael T. Simpson, Kent Backman, James Corley ―Hands-On Ethical Hacking and Network Defense‖,2016
2 Steven DeFino, Barry Kaufman, Nick Valenteen ―Official Certified Ethical Hacker Review Guide‖,2015
REFERENCE BOOKS 1 The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series)
E BOOKS: https://www.nationalcyberwatch.org/resource/ethical-hacking-systems-defense-nationalcyberwatch-center-edition/

CYS 302- Cyber Systems & Cyber Threat and Modelling

Credits- 4L+ 2P

Course Objective: The course is designed to provide competencies about the different cyber systems issues and different threat modelling systems.

Sl. No.	Course Outcome	Mapped Module/s(if applicable)
1.	Understand threat models by discussing strategies and structured approaches to threat modelling.	M1
2.	Apply different processes(such as finding, spoofing, tampering etc.) to the threats.	M2
3.	Make use of different techniques for managing and addressing the threats.	M3
4.	Explain and Identify different threat modelling tools.	M4
5.	Evaluate different threats to cryptosystems.	M5
6.	Appraise different intrusion and detection techniques.	M6

Theory- CYS(T) 302

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Dive In and Threat Model	12	25	1,2	
M2	Finding Threats	12	30	2,3	
M3	Managing and Addressing Threats	12	30	2,3	
M4	Threat Modelling Tools	12	15	2,3	
		48	**100**		

Practical- CYS 392

Module No	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M5	Threats to Cryptosystems	14	60	3,4,5	
M6	Intrusion and detection techniques	14	40	3,4,5	
		28	**100**		

Cyber Systems & Cyber Threat and Modelling

Module-1: Dive in and Threat Model, learning to Threat Model. Strategies for Threat Modelling, Brainstorming Your Threats, Structured Approaches to Threat Modelling, Models of Software,

Module-2: Finding Threats, STRIDE, Spoofing Threats, Tampering Threats, Repudiation Threats, Information Disclosure Threats, Denial-of-Service Threats. Attack Trees, Working with Attack Trees, Representing a Tree, Real Attack Trees. Attack Libraries, Properties of Attack Libraries.

Module-3 Managing and Addressing Threats, Processing and Managing Threats, Starting the Threat Modelling Project, Digging Deeper into Mitigations, Tracking with Tables and Lists, Scenario-Specific Elements of Threat Modelling. Defensive Tactics and Technologies, Tactics and Technologies for Mitigating Threats, Addressing Threats with Patterns, Mitigating Privacy Threats.

Module-4 Threat Modelling Tools, Generally Useful Tools, Open-Source Tools, Commercial Tools. Web and Cloud Threats, Web Threats, Cloud Tenant Threats, Cloud Provider Threats, Mobile Threats.

Module-5 Threats to Cryptosystems, Cryptographic Primitives, Classic Threat Actors, Attacks against Cryptosystems, building with Crypto, Things to Remember about Crypto Experimental Approaches, looking in the Seams, Operational Threat Models, Threats to Threat Modelling Approaches, How to Experiment.

Module 6: Intrusion and detection techniques, Programming Bugs and Malicious code, E-commerce Security, web browser security, Mini Project.

Suggested Readings:

1. Adam Shostack, “Threat Modelling: Designing for Security Designing for Security” Wiley publication, Edition, 2008.
2. Frank Swiderski, Window Snyder “Threat Modelling (Microsoft Professional)” Microsoft Press, Edition, 2008.

CYS 303- Vulnerability Analysis, Penetration Testing, and Incident Handling

Credits- 4L+2P

Course Objective: The course is designed to provide competencies about the different cyber systems issues and different threat modelling systems.

Sl. No.	Course Outcome	Mapped Module/s(if applicable)
1.	Demonstrate details of vulnerability.	M1
2.	Make use of and penetration testing overview.	M2
3.	Examine the details of cyber security incident management.	M3
4.	Test for ethical hacking.	M4
5.	Test for and evaluate vulnerability assessment tool.	M5
6.	Determine and design different hacking techniques.	M6

Theory- CYS (T) 303

Module No	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Vulnerability	12	25	1,2	
M2	Introduction to Penetration Testing, Penetration Testing Overview	12	25	2,3	
M3	Cyber Security Incident Management	12	25	2,3,4	
M4	Ethical Hacking	12	25	2,3,4	
		48	**100**		

Practical- CYS 393

Module No	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M5	Working of Vulnerability Assessment Tool	14	50	3,4,5	
M6	Hacking Techniques	14	50	3,4,5,6	
		28	**100**		

Vulnerability Analysis, Penetration Testing, and Incident Handling

Module 1: Vulnerability - Introduction, Overview of Security threats and Vulnerability, Benefits, Methodology, Vulnerability and Threats, Malware: Viruses, Worms, Trojan horses, Security Vulnerabilities Types of attacks on Confidentiality, Integrity and Availability, Vulnerability Assessment, Reasons for Vulnerability Existence, Steps for Vulnerability Analysis, Web Application vulnerability, Security Counter Measures, Intrusion Detection, Antivirus Software Intrusion Detection, Antivirus Software, vulnerability to security risks, Failure to Restrict URL, Remote Code Execution, tools use for vulnerability checking.

Module 2: Introduction to Penetration Testing, Penetration Testing Overview: What is Penetration Testing? When to Perform Penetration Testing? How is Penetration Testing Beneficial? Penetration Testing Method: Steps of Penetration Testing Method, Planning & Preparation, Reconnaissance, Discovery, Analysing Information and Risks, Active Intrusion Attempts, Final Analysis, Report Preparation. Penetration Testing Vs. Vulnerability Assessment, Penetration Testing, Vulnerability Assessment, and Which Option is Ideal to Practice? Types of Penetration Testing: Types of Pen Testing, Black Box Penetration Testing. White Box Penetration Testing, Grey Box Penetration Testing, Areas of Penetration Testing. Penetration Testing Tools, Limitations of Penetration Testing, Conclusion.

Module 3: Cyber security Incident Management: The Cyber security Incident Chain, Stakeholders, Cyber security Incident Checklist, Five Phases of Cyber security Incident Management: Plan and Prepare, Detect and Report, Assess and Decide, Respond and Post-Incident Activity, Handling an Incident: Preparation: Preparing to Handle Incidents, Preventing Incidents. Detection and Analysis: Attack Vectors, Signs of an Incident, Sources of Precursors and Indicators, Incident Analysis, Incident Documentation, Incident Prioritization & Incident Notification, Post-Incident Activity: Lessons Learned, Using Collected Incident Data, Evidence Retention.

Module 4: Ethical Hacking, Penetration Testing, Vulnerability Assessment and Penetration Testing, SQL-Injection, Blind Injection Detection, Cross-Site Scripting, Broken Authentication & Session Management, Security Counter Measures, Overview of digital forensics,

Module 5: Working of Vulnerability Assessment Tool, Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration, – vulnerability analysis, Planning and Discovery Knowledge Check, Attack and Reporting.

Module 6: Hacking Techniques, Penetration Testing Tools, Tools use in Incident Response, Incident Response Knowledge.

Suggested Readings:

1. Mastering Modern Web Penetration Testing by Prakhar Prasad, October 2016 Packt Publishing.
2. Kali Linux Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran, Cameron Buchanan,2015 Packt Publishing.

CYS 354- Operating System and Linux
Credits- 2P

Course Objective: The course is designed in order to provide an elaborate idea about different functional components of the Linux Operating System and their various utilities. At the end of the course, the students are expected to know about various functional components of an operating system, their utilities, significance and applications through Linux OS, in order to solve real life problems.

Sl	Course Outcome	Mapped modules
1	Understand the structure, function and applications of basic Linux utilities	M1, M2
2	Understand and apply various file handling utilities and filters in Linux OS	M2, M3
3	Explain the basic structure and implications of advanced file attributes in Linux OS	M3, M4
4	Model the basic structure and utility of the shell interface in Linux OS	M4, M5
5	Develop programming skills in order to work with Linux Shell & Shell Scripting	M4, M5
6	Examine and explain the various OS related functions being implemented by the Linux OS	M5, M6

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Basic LINUX Utilities	4	10%	1,2	
M2	Directory and Ordinary File Handling	4	10%	1,2	
M3	Basic Filters	4	20%	2,3	
M4	File attributes	4	20%	2,3	
M4	Shell and Shell Scripting	6	30%	4,5,6	
M5	Process and Memory management in Linux	4	10%	4,5	
		26	**100**		

Module 1: Basic LINUX Utilities (4 hrs)
Calendar (*cal*), Display system date (*date*), Message display (*echo*), Calculator (*bc*), Password changing (*passwd*), knowing who are logged in (*who*, *w*), Knowing System information (*uname*).

Module 2: Directory and Ordinary File Handling (4 hrs)
Displaying pathname of the current directory (*pwd*), Changing the current directory (*cd*), Make directory (*mkdir*), Remove directories (*rmdir*), Listing contents of directory (*ls* and its options), Absolute pathname, Relative pathname, Referring directories with dot (.) and dot dot (..) identifiers Displaying and creating files (*cat*), Copying a file (*cp*), Deleting a file (*rm*), Renaming/ moving a file (*mv*), Paging output (*less, more*), Knowing file type (*file*), Line, Word & Character counting (*wc*), Comparing files (*cmp*), Finding common between two files (*comm*), Displaying file differences (*diff*)

Module 3: Basic Filters (4 hrs)
Prepare file for printing (*pr*), Horizontal division of file (*head* and *tail)*, Vertical division of file (*cut*), Paste files (*paste*), Sort file (*sort*), Finding repetition and non- repetition (*unique*), Manipulating characters (*tr*), Searching patterns in files (*grep*).

Module 4: File attributes (4 hrs)
File and directory attributes listing, File ownership, File permissions, changing file permissions – relative permission & absolute permission, changing file ownership, changing group ownership, File system and Inodes, Hard link, Soft link, setting Default permissions of file and directory using *umask*, listing of modification and access time, Time stamp changing, File locating.

Module 5: Shell and Shell Scripting (6 hrs)
Types of shell, Pattern matching, Escaping, Quoting, Redirection, Pipe, Tee, Command substitution, Shell variables. Introduction to shell scripting: Simple shell scripts, Interactive shell scripts, using command line arguments, Logical operators (&&, ||), Condition checking (*if-then-fi, if-then-else-fi, if-then—elif-else-fi, case*), Expression evaluation (*test, []),* Computation (*expr*), Using *expr* for strings, Looping (*while*, *for*, *until*, *break*, *continue*), Use of positional parameters. Simple implementation of basic LINUX commands, utilities, filters etc. using shell scripts.

Module 6: Process and Memory management in Linux (4 hrs)
Display process attributes (*top*), Display System processes (*ps*), Changing process priority (*nice*), Listing jobs (*jobs*), Sending jobs to background (bg) and foreground (fg), Killing or terminating processes (*kill*), Inter Process Communication management (*ipcs*), Memory management commands and utilities – *free, df, top, htop, vmstat, dmidecode,* etc.

4th Semester

Subject Type	Course Name	Course Code	Credit Distribution			Credit Points	Mode of Delivery			Proposed Moocs
			Theory	Practical	Tutorial		Offline#	Online	Blended	
CC 8	Cryptography and Information Security	CYS (T) 401	4	0	0	6	✓			As per MAKAUT Notification
		CYS 491	0	2	0					
CC 9	Software Engineering & Software Design with UML	CYS (T) 402	4	0	0	6	✓			
		CYS 492	0	2	0					
CC 10	Advanced Computer Network & Security	CYS (T) 403	4	0	0	6	✓			
		CYS 493	0	2	0					
GE 4	Students will have to choose from the GE Basket					6			✓	
SEC 2	Database Management	CYS 455	0	2	0	2	✓			
Semester Credits						**26**				

 # Only in case offline classes are not possible due to reasons like COVID Pandemic the classes will be in synchronous online mode

CC 8: Cryptography & Information Security
Code: CYS 401
Credits- 4L +2P

Course Objective: The course is designed to provide an elaborate idea about the different cryptography techniques, development of key generation algorithms for information protection.

Sl. No.	Course Outcome	Mapped Modules
1.	Understand the concept of cryptography, number system etc.	M1
2.	Understand One time pad and stream ciphers.	M2
3.	Define Block ciphers	M3
4.	Understand message integrity	M4
5.	Define public key cryptography.	M5
6.	Make use of digital signature and protocols.	M6

Theory: CYS (T) 401

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Overview of cryptography, number system	10	20	1,2	
M2	One time pad and stream ciphers	10	20	1,2	
M3	Block ciphers, message integrity	14	30	2,3	
M4	Public key cryptography, digital signature	14	30	2,3	
		48	100		

Practical: CYS 491

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M5	Arithmetic modulo, programming	12	40	3,4	
M6	Cryptography algorithm design and programming	16	60	3,4	
		28	100		

MODULE 1: Overview of cryptography, number system:
Arithmetic modulo operations, Abstract algebra, modular inverse, mathematics of Secure Communications; Classical Cryptosystems etc.

MODULE 2: Classical cryptosystem, one time pad and stream ciphers:
Classical Cryptosystems, Substitution Cipher, Play Fair Cipher, Vignere cipher, Introduction to stream cipher, RC4, ARC4 algorithms.

MODULE 3: Block ciphers, message integrity:
Symmetric key encryption, block cipher mode of operations, Fiestel Cipher, DES, AES, 3-DES, use of block cipher,

MODULE 4: Public key cryptography, digital signature:
Public key Cryptosystems Diffie-Hellman key exchange, semantically secure El-Gamal encryption, RSA and other Cryptosystems, Key Exchange Protocols, Hash Functions, Digital signature.

MODULE 5: Arithmetic modulo, programming:
Euclidean Algorithm, Extended Euclidean Algorithm, random number generation and programming.

MODULE 6: Cryptography algorithm design and programming:
Polynomial arithmetic, implementation of symmetric and asymmetric key algorithms, design of cryptography algorithms.

TEXT BOOKS

1. William Stallings: Cryptography and Network security, Pearson Education

2. V.K. Jain: Cryptography and Network security, Khanna Publishing House

3. Alfred Menezes: Handbook of Applied Cryptography.

CC 9: Software Engineering & Software Design with UML
Code: CYS 402
Credits- 4L+2P

Course Objective: This course is an introduction to the application of software design principles to the design of applications. This course approaches software design from three perspectives: the software engineering principles that enable development of quality software, modelling of software elements using the Unified Modelling Language (UML), and the application of design patterns as a means of reusing design models that are accepted best practices.

Sl	Course Outcome	Mapped modules
1	Remember & Understand the Software engineering and its different aspects	M1
2	Remember & Understand the design of the various SDLC models	M2
3	Understand and identify the elements of modern Software Engineering tools	M3
4	Understand & apply the planning and managing requirements of a S/W development	M4
5	Understanding the Software design and Analysis and UML modelling	M5, M6
6	Application & Analysis using Software quality and security and risk management	M7,M8,M9

Theory- CYS (T) 402

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M 1	SOFTWARE ENGINEERING FUNDAMENTALS	5	10	1,2	
M 2	SOFTWARE DEVELOPMENT LIFE CYCLES (SDLCs)	5	15	1,2	
M 3	SOFTWARE ENGINEERING TOOLS	5	10	2	
M 4	PLANNING AND MANAGING REQUIREMENTS	5	10	2,3	
M 5	INTRODUCTION TO SOFTWARE ANALYSIS AND DESIGN	5	10	1,2	
M 6	OBJECT MODELING USING UML	10	15	2,3	
M 7	SOFTWARE VERIFICATION AND VALIDATION	3	10	4,6	
M 8	SOFTWARE QUALITY AND SECURITY	5	10	4,6	
M 9	RISK MANAGEMENT IN SOFTWARE ENGINEERING PROJECTS	5	10	2,4	
		48	**100**		

Practical- CYS 492

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M 3	SOFTWARE ENGINEERING TOOLS	14	40	3,4	
M 6	OBJECT MODELING USING UML USING VARIOUS OPEN SOURCE TOOLS	14	60	3,4	
		28	**100**		

Module I: SOFTWARE ENGINEERING FUNDAMENTALS (5T)
Introduction – Software Engineering, Software Development Challenges, Software Scope, Software Engineering Discipline, Software Methodologies and Related Process Models, The Human Side of Software Development, Introduction to Agile Software Engineering

Module II: SOFTWARE DEVELOPMENT LIFE CYCLES - SDLCs (5T)
Process Models and Solution Life Cycle Phases. Traditional Life Cycle Models: Waterfall, V, Phased, Evolutionary, Spiral, CBSE. Alternative Techniques – UP, RAD, JAD, PSP/TSP, Prototyping
Agile Software Engineering Process Models: Extreme Programming, Agile Software Development, DevOps, Site Reliability Engineering (SRE). Roles and Types of Standards, ISO 12207: Life Cycle Standard, IEEE Standards for Software Engineering Processes and Specifications

Module III: SOFTWARE ENGINEERING TOOLS (5T + 10L)
Requirements Management Tools (e.g., IBM Rational Doors)
Design Tools (e.g., Sparx Enterprise Architect)
Development Tools - IDEs (e.g., Xcode, Eclipse, IntelliJ IDEA, NetBeans, Microsoft Visual Studio, Atom), Source Control Management (e.g.,GitHub) , Release Orchestration (e.g., OpenMake) , Collaboration (e.g., Jira, Trello, Slack)
Operations Management Tools - Database Automation (e.g., Datical), Deployment (e.g, ElasticBox), Configuration Management (e.g., Ansible, Chef, Puppet), Continuous Integration (e.g, Jenkins), Container Management (e.g., Docker, Kubernetes).
Testing Tools and Frameworks - Testing Tools (e.g., Junit, Selenium), PaaS (e.g., PythonAnywhere, AWS Code9, Heroku)
Management and Monitoring Frameworks - AIOps (e.g, Splunk, Logstash), Analytics (e.g., Dynatrace, ElasticSearch), Monitoring (e.g., Nagios)
Security Frameworks (e.g., Snort, BlackDuck)
Cloud Platforms (e.g., AWS, Azure, GCP, IBM Cloud)
Project Management (e.g., Scoro, Basecamp, Microsoft Project)

Module IV: PLANNING AND MANAGING REQUIREMENTS (2T)
Requirements Development Methodology - Specifying Requirements - Eliciting Accurate Requirements - Documenting Business Requirements - Defining User Requirements - Validating Requirements - Achieving Requirements Traceability - Managing Changing Requirements - Reviews, Walkthroughs, and Inspections - Requirements Modeling - Agile Requirements Engineering

Module V: INTRODUCTION TO SOFTWARE ANALYSIS AND DESIGN (3T)
Roles of Analysis and Design - Traditional Data and Process Modeling Approaches - Performing Requirements Analysis - Object-Oriented Modeling - User Experience Design - Design for Mobility - Selecting and Combining Approaches - Creating a Data Model

Module VI: OBJECT MODELING USING UML (10T + 10L)
Building an Object Model using UML - Architectural and Pattern-Based Design - Model Driven Architectures – Class Diagram - Sequence Diagram- Use case diagrams –Sate machine diagrams – Activity Diagrams- Using Open Source, free, paid, and Enterprise software

Module VII: SOFTWARE VERIFICATION AND VALIDATION (2T)
Unit Testing - Integration and System Testing - Static Confirmation - Dynamic Testing - Traceability Matrices - Automated Testing - Other Specialized Testing

Module VIII: SOFTWARE QUALITY AND SECURITY (3T)
Software Quality Concepts - Software Configuration Management (CM) - Software Quality Assurance (SQA) - Software Quality and Agile Methods: Automated and Manual Functional Testing, Acceptance testing, Mock objects, User interface testing (HTTPUnit, Canoo), Performance testing - Software Metrics and Analytics - Quality and Process Standards and Guidelines: ISO 9000, SWEBOK, ISO 15504, SEI's Capability Maturity Model (CMM), CMM Integration (CMMI) - Software Security Engineering

Module IX: RISK MANAGEMENT IN SOFTWARE ENGINEERING PROJECTS (5T)
Project Management Concepts - Project Planning and Estimation - Cooperative roles of software engineering and project management - Developing risk response strategies - Risk Management in Agile Processes - Agile Project Planning - Project Management Metrics - Software Support Strategies

Text Books:1. Software Engineering - Architecture-driven Software Development By Richard F Schmidt · 2013, Elsevier Science
2. FUNDAMENTALS OF SOFTWARE ENGINEERING, FIFTH EDITION By Rajib Mall · 2018, PHI Learning Private Limited
3. UML Distilled - A Brief Guide to the Standard Object Modelling Language By Martin Fowler · 2018 , Pearson Education

CC 10: Advanced Computer Network & Security
Code: CYS 403
Credits- 4L +2P

Course Objective: The course is designed to provide an elaborate idea about the Computer networking in advance level and threats identification and prevention modelling of operating systems.

Sl. No.	Course Outcome	Mapped Modules
1.	Understand Computer Network Fundamental	M1
2.	Demonstrate Network devices, IEEE protocols	M2
3.	Relate different techniques encoding, switching, and congestion control.	M3
4.	Demonstrate advance communication protocols.	M4
5.	Understand introduction and Security Threats	M5
6.	Demonstrate network security.	M6

Theory: CYS (T) 403

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Computer Network Fundamental	10	20	1,2	
M2	Network devices, IEEE protocols	14	30	2	
M3	Encoding, switching, congestion control	14	30	2,3	
M4	Advance communication protocols	10	20	2,3	
		48	100		

Practical: CYS 493

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M5	Introduction and Security Threats	14	40	2,3	
M6	Network security	14	60	2,3	
		28	100		

Module-1: Computer Network Fundamental
Data Communication, Analog-Digital Signals. TCP/IP and OSI Model, Client, Server and Peers, Client/Server architecture, Wired & Wireless transmission, Guided-Unguided Media, Bus, Star, Ring, Mesh, Hybrid, LAN, MAN, WAN, Simplex, Half duplex and Full duplex, Asynchronous and Synchronous Transmission, Parallel and Serial Transmission, Base band and Broadband transmission.

Module-2: Network devices, IEEE protocols
Different networking devices, IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11, FDDI, DQDEB, ATM, Physical Addressing, Logical Addressing, Port Addresses, IPV4, IPV6, Classfull-Classless Addressing, Subnetting and Masking, NAT, DHCP, BOOTP, ARP, RARP, ICMP

Module-3: Encoding, switching, congestion control
Different Encoding Techniques, FDM, TDM, Circuit Switching, Packet Switching, Message Switching. Routing, Routing Protocols: Distance Vector, Link State, Congestion Control: Leaky Bucket and Token Bucket Algorithm, ISDN

Module-4: Advance communication protocols
TCP, UDP, Firewalls, Proxy Router, DNS, FTP, TFTP, SMTP, TELNET, NFS, WWW, E-mail, HTTPS, Cable Network, Telephone Network

Module-5: Introduction and Security Threats

Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare, Confidentiality, Integrity, Availability, Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection. Malware: Viruses, Logic bombs.

Module 6: Network security
Centralized or decentralized infrastructure, private key protection, Trust Models: Hierarchical, peer to peer, hybrid, Firewalls: working, design principles, trusted systems, Kerberos, Security topologies, IP security: overview, architecture, IPSec configurations, IPSec security, Email security : security of email transmission, malicious code, spam, mail encryption.

References/Text Books:
1. B. Fourauzan, "Data Communications and Networking", 4th Edition, Tata McGraw-Hill
2. Tanenbaum, Computer Networks, 3rd Edition, PHI, New Delhi
3. D. Comer, "Computer Networks and Internet", 2nd Edition, Pearson Education
4. Data and Communication by W. Stallings
5. An integrated approach to Computer Networks by Bhavneet Sidhu, Khanna Publishing H

SEC 2: Database Management
Code: CYS 455
Credits- 2P

Course Objective: The course is designed to introduce the concepts of Database Programming and to understand, develop and implement the queries with the database programming. In this course, you will learn to create relational databases, write SQL statements to extract information in order to satisfy the required requests. As you develop these skills, you will use either Oracle or MySQL to execute SQL statements

Sl. No	Course Outcome	Mapped modules
1	Remember & understand the concepts of Database Programming which aims to implement real-world entities for creating relational databases.	M1, M2
2	Understand and identify the ability to design, implement, and evaluate a query using the concepts of Relational Model	M2, M3
3	Understand & apply the appropriate SQL statements to extract information in order to satisfy the required requests.	M2,M3, M4
4	Understand & apply more features of SQL commands to get into depth of SQL queries.	M2,M3,M4

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M 1	Introduction to DBMS	6	20	1,2	
M 2	Features of Relational Model	6	20	2	
M 3	Introduction to SQL	8	30	2,3	
M 4	More features of SQL	8	30	2,3	
		28	**100**		

Module I: Introduction to DBMS(4L)

Concept & Overview of DBMS, Components of Database System, Basics of Database Management System, File-based System and Database Management System, Advantages of using Database over File based system, Data Models, Database Languages, Database Administrator, Database Users.

Module II: Features of Relational Model (4L)
Concept of Relational Model, Relational Model – Introduction, Advantages and Disadvantages, Keys, Entity integrity Rule, Functional Dependency, Relational Set Operators, Relational Algebra.

Module III: Introduction to SQL (6L)
Introduction, Features of SQL, Database Languages - Data definition and Data manipulation languages, Data Definition Commands, Data Manipulation Commands, (SELECT Statement and different Clauses, SQL Functions - Date and Time Functions, String Functions,
Null Values, Domain Constraints, Referential Integrity Constraints.

Module IV: More features of SQL (6L)
Describing Oracle tables, Using the set commands, Joining Oracle tables -Equi-join, Outer join Hiding joins by creating views, Using IN, NOT IN, EXISTS and NOTEXISTS, Subqueries, Exercise – write a subquery, Correlated subquery, Non-correlated subqueries, Advanced SQL operators - Between operator, IN and NOT IN operators, Sub-queries-EXISTS clause, Using wildcards in queries (LIKE operator), Aggregation in SQL -Count (*), Sum, Avg, Min and max. Using the group by clause, SQL access methods.

Study and lab Resources:

1. Korth, Silberschatz, Sudarshan – Database System Concepts; Tata Mc. Graw Hill
2. Ramez Elmasri, Shamkant B Navathe - Fundamentals of Database Systems; Pearson
3. Walter Shields -SQL QuickStart Guide: The Simplified Beginner's Guide to Managing, Analyzing, and Manipulating Data With SQL
4. Ben Forta- SQL in 10 Minutes a Day, Sams Teach Yourself
5. https://www.w3schools.com/sql/
6. https://www.tutorialspoint.com/sql/index.htm

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus for B.Sc.in Cyber Security (Industry Induced) Programme
(Effective for Students Admitted in Academic Session 2019-2020)

Semester 5:

Cyber Forensics

Unit 1: Cyber Forensics Science: Forensics science, computer forensics, and digital forensics. **Computer Crime:** Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics -- 7L

Unit 2: Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation. -- 6L

Unit 3: Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause. -- 7L

Unit 4: Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case, **Network Forensics:** open-source security tools for network forensic analysis, requirements for preservation of network data. --- 8L

Unit 5: Mobile Forensics: mobile forensics techniques, mobile forensics tools. **Legal Aspects of Cyber Forensics:** IT Act 2000, amendment of IT Act 2008.---- 5L

Unit 6: Recent trends in mobile forensic technique and methods to search and seizure electronic evidence ---- 3L

References:

1. John Sammons, The Basics of Digital Forensics, Elsevier Model Curriculum of Engineering & Technology PG Courses [Volume-I]

2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

Cyber law and Ethics

Unit – 1: Introduction of Cybercrime: [4L]
What is cybercrime?, Forgery, Hacking, Software Piracy, Computer Network intrusion

Unit – 2: Category of Cybercrime: **[4L]**
how criminals plan attacks, passive attack, Active attacks, cybers talking.

Unit – 3: Cybercrime Mobile & Wireless devices: [8L]
Security challenges posted by mobile devices, cryptographic security for mobile devices, Attacks on mobile/cellphones, Theft, Virus, Hacking. Bluetooth; Different viruses on laptop.

Unit -4: Tools and Methods used in Cyber crime: [8L]
Proxy servers, panword checking, Random checking, Trojan Horses and Backdoors; DOS & DDOS attacks; SQL injection: buffer over flow.

Unit– 5: Phishing & Identity Theft: [4L]
Phising methods, ID Theft; Online identity method.

Unit --6: Cybercrime & Cybersecurity: [4L]
Legal aspects, indian laws, IT act, Public key certificate

Unit—7: Ethics [4L]: Legal Developments, Cyber security in Society, Security in cyber laws case studies, General lawand Cyber Law-a Swift Analysis.

Text: 1. Cyber security by Nina Gobole & Sunit Belapune; Pub: Wiley India.

2. Mark F Grady, Fransesco Parisi, "The Law and Economics of Cyber Security", Cambridge University Press, 2006

Malware Analysis and Reverse Engineering

Unit 1: Fundamentals of Malware Analysis (MA): Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAVSignatures, Creating Custom ClamAV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser'sREMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks, Introduction to Python ,Introduction to x86 Intel assembly language, Scanners: Virus Total, Jotti, and NoVirus Thanks, Analyzers: Threat Expert, CWSandbox, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools: Virtual Box, VM Ware, Python , Other Analysis Tools --- 11 L

Unit 2: Malware Forensics: Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates. ---6L

Unit 3: Malware and Kernel Debugging: Opening and Attaching to Processes, Configuration of JIT Debugger for Shell code Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands**,** DLL Export Enumeration, Execution, and Debugging**,** Debugging a VMware Workstation Guest (on Windows)**,** Debugging a Parallels Guest (on Mac OS X). Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts**,**
Kernel Debugging with IDA Pro. ---8L

Unit 4:Memory Forensics and Volatility: Memory Dumping with MoonSols Windows Memory Toolkit**,** Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps**,** Code Injection and Extraction**,** Detecting and Capturing Suspicious Loaded DLLs**,** Finding Artifacts in Process Memory**,** Identifying Injected Code with Malfind and YARA. ---6L

Unit 5: Researching and Mapping Source Domains/IPs: Using WHOIS to Research Domains**,** DNS Hostname Resolution**,** Querying Passive DNS**,** Checking DNS Records**,** Reverse IP Search New Course Form**,** Creating Static Maps**,** Creating Interactive Maps.---6L

Unit 6: Case Study: Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA --3L

Book:

1. Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher Williampollo

Intrusion Detection and Prevention Systems-(Elective-1)

Unit1: History of Intrusion detection, Audit, 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. The state of threats against computers, and networked systems, Overview of computer security solutions and failure causes, Vulnerability assessment, firewalls—6L

Unit2: Overview of Intrusion Detection and Intrusion Prevention, Network and Host-based IDS, Evaluation of IDS, Cost sensitive IDS, Anomaly Detection Systems and Algorithms, Network Behavior Based Anomaly Detectors (rate based), Host-based Anomaly Detectors—6L

Unit3: Intrusion Prevention Systems, Network IDs protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis, techniques, Classes of attacks, Network layer attack (scans, denial of service, penetration), Application layer attack(software exploits, code injection), Human layer attack (identity theft, root access), Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis, Automated: Drones, Worms, Viruses—8L

Unit4: A General IDS model and taxonomy, Signature-based Solutions, Introduction to Snort, Snort rules, 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, State transition, Immunology, Payload Anomaly Detection, Attack trees and Correlation of alerts, Autopsy of Worms and Botnets, Malware detection—8L

Unit5: Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL, Email/IM security issues, Viruses/Spam, From signatures to thumbprints to zero-day detection, Insider Threat issues , Masquerade and Impersonation, Traitors, Decoys and Deception Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs—8L

Books:

1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," Prentice Hall
2. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "Intrusion Detection and Correlation Challenges and Solutions",
3. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention", Tata McGraw-Hill
4. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", New Riders Publishing
5. T. Fahringer, R. Prodan, "A Text book on Grid Application Development and Computing Environment". Khanna Publihsers

Biometric Security (Elective-2)

Unit 1: Introduction and Definitions of bio-metrics, Traditional authenticated methods and technologies.-- 5L

Unit 2: Bio-metric technologies: Fingerprint, Face, Iris, Hand Geometry, Gait Recognition, Ear, Voice, Palm print, On-Line Signature Verification, 3D Face Recognition, Dental Identification and DNA.---8L

Unit 3: The Law and the use of multi bio-metrics systems. ---4L

Unit 4: Statistical measurement of Bio-metric. Bio-metrics in Government Sector and Commercial Sector. –8L

Unit 5: Case Studies of bio-metric system, Bio-metric Transaction. Bio-metric System Vulnerabilities.---7L

Unit 6:
Recent trends in Bio-metric technologies and applications in various domains. Case study of 3D face recognition and DNA matching.---4L

Books:

1. Paul Reid, Biometrics for network security, Hand book of Pearson, 2004.
2. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, 2003
3. A. K. Jain, R. Bolle, S. Pankanti (Eds.), BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.
4. J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2004.
5. Anil Jain, Arun A. Ross, Karthik Nanda kumar, Introduction to biometric, Springer, 2011.
6. Biometric Systems: Technology, Design and Performance Evaluation, J. Wayman, A.K. Jain, D. Maltoni, and D. Maio
7. Gonzalez, R.C. and Woods, R.E., Digital Image Processing. 2nd ed. India: Person Education, 2009

Cyber Forensics Lab

1. Data acquisition using tools like FTK Imager, DumpIt etc.
2. Volatile Memory Analysis using Hex Editor and Volatility.
3. Defeating Anti Forensic Technique using tools like EaseUS Data recovery, Recuva, Steller Data recovery, Passware password recovery tools, Stegspy, Open Stego and crypt analysis etc.
4. Metadata extraction Using Exif tools
5. Network Forensic Using Wireshark.
6. Operating System Forensic using OSForensic, Autopsy.
7. Malware Analysys using tools like **ProcessMonitor, ProcessExplorer, RegShot / TotalCommander, PeStudio, Resource Hacker etc.**
8. Mobile Forensic using tools Mobileedit, Oxygen etc.
9. Cloud Forensic Lab

Malware Analysis Lab

1. Windows PE Format Analysis
2. Application Cracking
3. Basic Static Malware Analysis

4. Basic Dynamic Malware Analysis
5. Advanced Malware Analysis
6. Tool Used: Ollydbg, Immunity Debugger, Hex Editor, etc.

Semester 6:

Artificial Intelligence In Cyber security & Industry use cases

Unit-1: Introduction: Looking at the Various Aspects of Cyber security, Social engineering and phishing, Introducing ransomware, Malware intrusion, Non-malware intrusion, Detect, Respond, and Mitigate, Responding to and Recovering from Cyber attacks and Security Events, Challenges of Cybersecurity –[6L]

Unit-2: Fathoming Artificial Intelligence: Teaching Machines to be Smarter, Learning Algorithms, Supervised learning, Unsupervised learning, Being Smarter, Interacting with Humans, Natural Language Processing –[5L]

Unit-3: Applying Machine Learning and Deep Learning to Cybersecurity: Deep Learning and Deeply Layered Neural Networks, Deep Blue plays chess, introducing cognitive computing, Structured and Unstructured Data, Predictive Analytics, Introducing cognitive computing, Investigate Security Incidents taking Intelligent Action, Understand, Reason, and Learn, Winning with Threat Intelligence—[10L]

Unit-4: Trends in Cybersecurity: Responding to Ransomware, Combining Application development and Cybersecurity, Using Deep Learning to Detect DGA-Generated Domains Detecting Non-Malware Threats. Adaptive Honeypots and Honeytokens, Gaining a Better Understanding of How Neural Networks Work, Employing, Capsule Networks, Deep Reinforcement Learning. Protecting the IoT, Predicting the Future—[12L]

Unit-5: Industry Use Cases: Cognitive security with Watson, Tenable's ICS security capabilities, Cybersecurity Solutions - Real-time Insights **—[7L]**

Books:

1. Leslie F. Sikos, "AI in Cybersecurity", Springer, 2018
2. Ted Coombs, "Artificial Intelligence & Cybersecurity", IBM Limited Edition
3. Alessandro Parisi, "Hands-On Artificial Intelligence for Cybersecurity"

Block Chain & Cryptocurrency: (Elective-3)

Unit 1: Introduction: Introduction: Overview of Block chain, Public Ledgers, Bitcoin, Smart Contracts, Block in a Block chain, Transactions, Distributed Consensus, Public vs Private Block chain, Understanding Cryptocurrency to Block chain, Permissioned Model of Block chain, Overview of Security aspects of Block chain Basic Crypto Primitives: Cryptographic Hash Function, Properties of a hash function, Hash pointer and Merkle tree, Digital Signature, Public Key Cryptography --12L

Unit 2: Understanding Block chain for Enterprises: Permissioned Block chain: Permissioned model and use cases, Design issues for Permissioned block chains, Execute contracts, State machine replication, Overview of Consensus models for permissioned block chain- Distributed consensus in closed environment, Paxos, RAFT Consensus, Byzantine general problem, Byzantine fault tolerant system, Lamport-Shostak-Pease BFT Algorithm, BFT over Asynchronous systems. Enterprise application of Block chain: Cross border payments, Know Your Customer (KYC), Food Security, Mortgage over Block chain, Block chain enabled Trade, We Trade – Trade Finance Network, Supply Chain Financing, Identity on Block chain—12L

Unit 3: Block chain application development: Hyperledger Fabric- Architecture, Identities and Policies, Membership and Access Control, Channels, Transaction Validation, Writing smart contract using Hyperledger Fabric, Writing smart contract using Ethereum, Overview of Ripple and Corda ---8L

Unit 4: Crypto currency: A basic cryptocurrency. Bitcoin and Block chain: Creation of coins, Payments and double spending, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Block propagation and block relay. Working with Consensus in Bitcoin**:** Distributed consensus in open environments, Consensus in a Bitcoin network, Proof of Work (PoW) – basic introduction, Hashcash PoW, Bitcoin PoW, Attacks on PoW and the monopoly problem, Proof of Stake, Proof of Burn and Proof of Elapsed Time, The life of a Bitcoin Miner, Mining Difficulty, Mining Pool. --- 8L

BOOKS:

1. Melanie Swan, "Block Chain: Blueprint for a New Economy", O'Reilly, 2015
2. Josh Thompsons, "Block Chain: The Block Chain for Beginners- Guide to Block chain Technology and Leveraging Block Chain Programming"
3. Daniel Drescher, "Block Chain Basics", Apress; 1stedition, 2017
4. Anshul Kaushik, "Block Chain and Crypto Currencies", Khanna Publishing House, Delhi.
5. Imran Bashir, "Mastering Block Chain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained", Packt Publishing
6. Ritesh Modi, "Solidity Programming Essentials: A Beginner's Guide to Build Smart Contracts for Ethereum and Block Chain", Packt Publishing
7. Salman Baset, Luc Desrosiers, Nitin Gaur, Petr Novotny, Anthony O'Dowd, Venkatraman Ramakrishna, "Hands-On Block Chain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer", Import, 2018

Artificial Intelligence in Cyber security & Industry use cases:

Module 1: OWL Ontologies in Cybersecurity: Modeling of Cyber-Knowledge. [2]

Module 2: Knowledge Representation of Network Semantics for Reasoning-Powered Cyber-Situational Awareness. [4]

Module 3: The Security of Machine Learning Systems, Threat Model, Data Poisoning, Attacks at Test Time. [4]

Module 4: Patch Before Exploited: Approach to Identify Targeted Software Vulnerabilities, Supervised Learning Approaches, and Challenges of Exploit Prediction, Exploit Prediction Model, and Vulnerability and Exploit Analysis, [6]

Module 5: Applying Artificial Intelligence Methods to Network Attack Detection, Binary Classifiers, Training the Binary Classifier for Detecting Network Attacks, Schemes for Combining the Binary Classifiers, [8]

Module 6: Application of AI in Cyber Security and Use cases: Detect email threats such as spamming and phishing using AI, Polymorphic malware samples, Overcome antivirus limits in threat detection, Predict network intrusions and detect anomalies with machine learning, Verify the strength of biometric authentication procedures with deep learning. [10]

Text Books:

1. Hands-On Artificial Intelligence for Cybersecurity, Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies by Alessandro Parisi.
2. AI in Cybersecurity by Leslie F. Sikos, Springer, Cham.