AICTE Mandatory Disclosures

Information of Infrastructure and Other Resources Available

- Number of Class Rooms and size of each : 1 (80 Sqm)
- Number of Tutorial rooms and size of each : 1(83 Sqm)
- Number of Laboratories and size of each : 1(83 Sqm)
- Number of Drawing Halls with capacity of each : 1(136) Sqm
- Number of Computer Centres with capacity of each : 1(83 Sqm)
- Barrier Free Built Environment for disabled and elderly persons : Available(Certified by competent authority)
- Occupancy Certificate : Available(Certified by competent authority)
- Fire and Safety Certificate : Available(Certified by competent authority)

Library

- Number of Library books/ Titles/ Journals available (program-wise) : 2209
- List of online National/ International Journals subscribed : 15
- E- Library facilities : Available

Computing Facilities

- Internet Bandwidth : 1Gbps
- Number and configuration of System : 30
- Total number of system connected by LAN : 30
- Total number of system connected by WAN: 30
- Major software packages available : MsOffice, Matlab, R, Python, Wireshark

List of facilities available

- Games and Sports Facilities
    - Table Tennis
    - Carroms
    - Chess

- Extra-Curricular Activities
- Soft Skill Development Facilities : Yes

M.Tech Information Security:

- Title of the Course : M.Tech.Information Security (With specialization in Cyber Security)
- Curricula and Syllabi : Given Below
- Laboratory facilities exclusive to the Post Graduate Course : 1 Lab(20PCs)+2 Research Labs

Enrollment of students in the last 3 years

M.Tech(Information Security)				
Year	2018-19	2019-20	2020-21	2021-22
No. of Students Enrolled	13	14	16	8

Teaching Learning Process

- **Curricula and syllabus for each of the Programmes as approved by the University**

UNIVERSITY OF HYDERABAD (UoH)

School of Computer and Information Sciences (SCIS)

Jointly with

CR RAO ADVANCED INSTITUTE OF MATHEMATICS, STATISTICS

AND COMPUTER SCIENCE (AIMSCS)

M.Tech.

Information Security

(With specialization in Cyber Security)

2 Years Full Time Programme

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Vision Statement:
To disseminate advances made in the Disciplines of Mathematics, Statistics and Computer Science.
To conduct, Promote, Carry out research and advanced study in Mathematics, Statistics and Computer Science

Mission Statements:
To work in the cutting edge areas of Mathematics, Statistics and Computer Science and vigorously purse their application in making out lives better.

MS-1: To conduct Courses, Conferences, Seminars, Colloquia, Workshops and undertake related activities in the disciplines of Mathematics, Statistics and Computer Science for Human Resource Development.

MS-2: To conduct, promote and carry out research and advanced study in Mathematics, Statistics and Computer Science and to disseminate the advances made in these trinity of areas.

MS-3: To encourage talented students both rural and urban to pursue professional and research careers in Mathematics, Statistics and Computer Science

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security)

Program Educational Objectives (PEOs)

PEO-1: To provide students with strong foundational concepts in Computer Science and Mathematics to understand the advances in Cyber space.

PEO-2: To enable students for innovative products and solutions.

PEO-3: To inculcate student a constant learning practice pace with changing landscape of technologies.

PEO-4: To nurture talent for designing and developing cyber security applications

PEO-5: To impart critical analysis thought in information security domain.

Mapping Program Educational Objectives (PEOs) with Mission Statements (MS)

	MS-1	MS-2	MS-3
PEO-1	3	3	3
PEO-2	3	3	2
PEO-3	2	3	2
PEO-4	3	2	3
PEO-5	1	1	1

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security)

Program Outcomes (POs)

PO-1: To enable students with latest technology trends in cyber world

PO-2: To provide wider understanding of information technology

PO-3: In-depth understanding of core system technologies in the security point of view

PO-4: To provide students with solid foundation in various cyberattack methods

PO-5: To prepare students to excel in analyze the information security threats and the network traffic

PO-6: To prepare students for bringing out new solutions in cyber security

Program Specific Outcomes (PSOs)

PSO-1: In-depth understanding of cryptography and security tools implementation

PSO-2: To inculcate students with ability to analyze new security requirements and development of new tools

PSO-3: To train students with good in cybersecurity so as to comprehend, analyze, design and create secure computing solutions for the real life problems.

Mapping of Program Outcomes (POs) and Program Specific Outcomes (PSOs) with Program Educational Objectives (PEOs)

	PEO-1	PEO-2	PEO-3	PEO-4	PEO-5
PO-1	3	1	3	3	2
PO-2	2	3	2	1	1
PO-3	3	2	2	2	3
PO-4	3	1	1	3	2
PO-5	3	1	1	3	3
PO-6	1	2	3	2	3
PSO-1	2	2	1	2	3
PSO-2	2	3	2	3	3
PSO-3	2	3	2	3	3

Mapping of Program Specific Outcomes (PSOs) where applicable.

Write '3' in the box for 'high-level' mapping, 2 for 'Medium-level' mapping, 1 for 'Low-level' mapping.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

M.Tech (Information Security) Scheme

Semester I

Course Code	Course Name	Credits
IS401	Mathematical Foundation for Information Security	4-0-0
IS402	Secure Operating System and Computer Organization	3-1-0
IS403	Laboratory: Reverse Engineering and Malware Analysis	1-0-2
CS425	Cryptography	4-0-0
	Elective – 1.1	3/4
	Elective – 1.2	3/4
Credits	**Min:22/Max:24**	**22/24**

Semester II

Course Code	Course Name	Credits
CS476	Advanced Computer Networks	4-0-0
IS451	Security Tools and Technologies	3-1-0
IS452	Ethical Hacking & Computer Forensics	3-1-0
IS453	Laboratory: Cyber Security	1-0-2
	Elective - 2.1	3/4
	Elective - 2.2	3/4
Credits	**Min:22/Max:24**	**22/24**

Semester III-IV

	Course Name	Credits
	DISSERTATION	18
Credits	**Min, Max:18**	**18**

Grand Total Credits = 62(Min) / 64 (Max

Electives	Semester I	Semester II
General Information Security	CS426 BlockChain Technology	AI473 Machine Learning
	IS423 Coding Theory and Information Theory	IS472 Statistics and Probability
Cyber Security Specialization	IS421 Current trends in Web Security	CS472 Cloud Computing
	IS422 Big Data Security	IS471 Information System Control and Audit

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (M.Tech-1)

Course Code: IS401 Title of the Course: Mathematical Foundation for Information Security
L-T-P : 4-0-0 Credits 4

Prerequisite Course / Knowledge (If any): Permutations and combinations, number system

Course Outcomes (COs)

After completion of this course successfully, the students will be able to:

- CO-1: Develop problem Solving techniques needed to calculate probabilities and number theory (Evaluate).
- CO-2: Apply Euler's Phi Function and concept of Prime Numbers to information security algorithms (Apply).
- CO-3: Apply concepts of power modulo in the real time application of security (Apply).
- CO-4: Explain the concept of Quadratic Reciprocity (Understand).
- CO-5: Apply the concepts of Elliptic Curves in secure communication (Apply).

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	1	1	2	3	3	2	1	2	2
CO2	1	1	2	3	2	2	1	1	2
CO3	1	1	1	3	2	2	1	2	2
CO4	1	1	1	3	3	2	2	2	3
CO5	1	2	3	3	3	3	2	3	3
CO6	1	1	2	3	3	2	1	2	2

Detailed Syllabus:

UNIT-I - Probability and Basics of Number Theory
Basic asymptotic complexity and order notation (big-O), random number generation, Elementary discrete probability. Introduction to Number Theory, Pythagorean Triples and the UNIT Circle, Sums of Higher Powers and Fermat's Last Theorem, Divisibility and the Greatest Common Divisor, Linear Equations and the Greatest Common Divisor,

UNIT-II - More on Number Theory
Factorization and the Fundamental Theorem of Arithmetic, Congruence: Powers, and Fermat's Little Theorem, Powers, and Euler's Formula, Euler's Phi Function, Prime Numbers: Counting Primes, Mersenne Primes and Perfect Numbers,

UNIT-III - Power modulo
Powers Modulo m and Successive Squaring, Computing k'th Roots Modulo m, Powers, Roots, and "Unbreakable" Codes, Euler's Phi Function and Sums of Divisors, Powers Modulo p and Primitive Roots, Primitive Roots and Indices,

UNIT-IV - Quadratic Reciprocity
Squares Modulo p, Quadratic Reciprocity, Which Primes Are Sums of Two Squares? Which Numbers Are Sums of Two Squares? The Equation X^4+Y^4=Z^4, Pell's Equation, Diophantine Approximation and Pell's Equation,

UNIT-V - Elliptic Curves
Cubic Curves and Elliptic Curves, Elliptic Curves with Few Rational Points, Points on Elliptic Curves modulo p, Defect Bounds and Modularity Patterns, Elliptic Curves and Fermat's Last Theorem

Reference Books

1. Kenneth H. Rosen (2011), Discrete Mathematics and Its Applications, 7th Edition, McGraw-Hill ,1072 pages.
2. J. Silverman (1996), A Friendly Introduction to Number Theory, Prentice Hall,432 pages.
3. Kenneth Ireland, Michael Rosen(1998), A Classical Introduction to Modern Number Theory,Springer, 394 pages.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech((Information Security) (M.Tech-I)

Course Code: IS402 Title of the Course: Secure Operating System and Computer Organization
L-T-P: 3-0-1 Credits 4

Prerequisite Course / Knowledge (If any): components of Computers and Operating Systems

Course Outcomes (COs)

After completion of this course successfully, the students will be able to:

- CO-1: Explain the computer organization and I/O operations of computer. (Understand)
- CO-2: Demonstrate the representation of data at the machine level. (Apply)
- CO-3: Categorize the security requirements of Operating System. (Analyze)
- CO-4: Assess the OS protection principles. (Evaluate)
- CO-5: Appraise the Trusted Operating System concepts (Evaluate)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	2	3	2	1	1	1	2	1	1
CO2	2	3	2	1	1	1	1	1	2
CO3	3	2	3	1	2	2	3	2	2
CO4	3	2	3	2	3	3	3	3	2
CO5	3	2	3	3	3	3	3	3	2

Detailed Syllabus

UNIT – I: Definition of Computer Organization, Computer Design and Computer Architecture. Basic Computer Organization and Design: Instruction codes, Computer Registers, Computer instructions, Timing and Control, Instruction cycle, Memory Reference Instructions, Input – Output and Interrupt, Complete Computer Description.

UNIT – II: Memory Organization: Memory Hierarchy, Main Memory, Auxiliary Memory, Associate Memory, Cache Memory. Pipeline and Vector Processing: Parallel Processing, Pipelining, Arithmetic Pipeline, Instruction Pipeline, RISC Pipeline, Vector Processing, Array Processors.

UNIT – III: Software assurance and software security, threats to software security, sources of software insecurity, benefits of detecting software security, managing secure software development Defining properties of secure software. Security Goals, Trust Model, Threat Model.

UNIT – IV : Secure software Architecture and Design, Security practices for architecture and design: Architectural risk analysis, security guidelines, and attack patterns, secure design through threat modeling. Access Control Fundamentals: Protection System, Reference Monitor, Secure Operating System Definition, Assessment Criteria.

UNIT – V : Verifiable Security Goals: Information Flow, Information Flow Secrecy Models, Denning's Lattice Model, Bell-LaPadula Model, Information Flow Integrity Models, Biba Integrity Model. Security in Virtual Machine Systems.

References Books:

1. William Stallings, (2016), Computer Organization and Architecture, 10th Edition, Pearson Education India. 864 pages.
2. David A. Patterson, John L. Hennessy, (2009), Computer Organization and Design – The Hardware / Software Interface, 4th Edition, Morgan Kaufmann, 741 pages.
3. Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead, (2008), Software Security Engineering: A Guide for Project Managers, Addison Wesley, 368 pages.
4. Ross J Anderson, (2008), Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, Wiley, 595 pages.
5. Trent Jaeger, (2008), Operating System Security, Morgan & Claypool, 220 pages.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (MTECH-I)

Course Code: IS421 Title of the Course: Current trends in Web Security

L-T-P: 3-0-0 Credits 3

Prerequisite Course / Knowledge (If any): Basics of Operating System and Web Technology.

Course Outcomes (COs)

After completion of this course successfully, the students will be able to

- CO-1: Evaluate various cyber security threats of the internet (Evaluate)
- CO-2: Compare and Contrast appropriate Intrusion Detection Mechanism (Analyze)
- CO-3: Appraise about the various cryptographic techniques used in Internet (Analyze)
- CO-4 : Compare and Contrast different attacks in the web –Trojans, worms and virus(Analyze)
- CO-5 : Design and develop of Firewalls for enhanced web security (Create)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	3	1	2	2	2	1	1	1	3
CO2	2	1	2	2	2	2	2	2	3
CO3	2	1	1	2	2	1	3	2	2
CO4	3	1	1	3	3	2	1	1	2
CO5	3	1	2	2	3	3	2	3	3

Detailed Syllabus:

UNIT I

Introduction to Security, Computer Security and Cyber Security. Security Terminologies and Principle, Security Threats, Types of attacks. Introduction Intrusion Detection System (IDS), Types of Intrusion Detection Systems, System Integrity Verifiers (SIVS).

UNIT II

Indication of Intrusion: System Indications, File System Indications Network Indications. Intrusion Detection Tools ,Post attack IDS Measures & Evading IDS Systems. Penetration Testing, Categories of security assessments, Vulnerability Assessment, Types of Penetration Testing.

UNIT III

Theory of Cryptography, Simple ciphers, Symmetric cryptography, stream ciphers, Block ciphers, Public key cryptography, Ciphers with public key ,Cryptographic Hash functions, Different hash algorithms, Digital signatures.

UNIT IV

Trojans and Backdoors, Viruses and Worms:. Sniffers, Phishing, Web Application Security- Secured authentication mechanism, secured session management, Cross-site Scripting, SQL Injection and other vulnerabilities Denial-of Service Attacks, Session Hijacking, Spoofing v Hijacking, TCP/IP hijacking, CAPTCHA Protection

UNIT V

IP Security, Web Security, Firewalls: Types, Operation, Design Principles, Trusted Systems. Computer Forensics,Forensic Investigation in Tracking Cyber Criminals, Incident Handling.Overview of System Hacking Cycle.Hacking, Classes of Hacker (Black hats, grey hats, white hats, suicide hackers), Footprinting, Scanning (Types-Port, Network, Vulnerability).

REFERENCE BOOKS:

1. William Stallings (2017), *Cryptography And Network Security: Principles and Practices*, Seventh Edition, Pearson Publication, 768 pages.
2. William Stallings, Lawrie Brown(2016), *Computer Security: Principles and Practices,* Second Edition, Pearson Publication, 792 pages.
3. Chwan-Hwa Wu, J. David Irwin(2017), *Introduction To Computer Networks And Cyber Security*, Third Edition, CRC Press, 1336 pages.
4. Hanqing Wu, Liz Zhao(2015), *Web Security: A Whitehat Perspective*, First Edition, Auerbach Publications, CRCPress, 596 pages.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (MTECH-I)

Course Code: IS403 Title of the Course: Reverse Engineering and Malware Analysis Lab
L-T-P : 1-0-2 Credits 3

Prerequisite Course / Knowledge (If any): Basics of Operating System and Web Technology.

Course Outcomes (COs)

After completion of this course successfully, the students will be able to

CO-1: Categorize and Identify appropriate Open Source tools for reverse engineering (Analyze).CO-2: Analyze the commonly used file formats using reverse engineering tools (Analyze)

CO-3: Explain how the malware works, identified, detected and eliminated for the computer. (Understand)

CO-4: Evaluate & assess various malware threats. (Evaluate).

CO-5: Appraise about the various malware attacking techniques (Analyze)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	3	2	3	3	2	2	3	3	2
CO2	2	3	3	3	2	2	1	2	2
CO3	3	1	2	3	3	3	2	1	3
CO4	2	1	3	3	3	2	2	1	3
CO5	3	3	3	3	3	2	2	2	2

Detailed Syllabus:

Week -1	**Task :** introduction to reverse engineering ,tools(gdb) to extract assembly code **Objective: u**nderstanding the essence of the reverse engineering, tools required.
Week -2	**Task :** recognizing main function' s stack frame, variables, memory allocation, branching (if-else) **Objective:** understanding the memory dump of runnable programs.
Week -3	**Task :** recognizing loops(while, for, do while) ,dynamic/static initialization of variables **Objective:** understanding how different loop constructs work in assembly level
Week -4	**Task :** recognizing function calls, nested function calls(inbuilt/user defined),recursion **Objective:** understanding of memory dump during function calls)
Week -5	**Task :** introduction to malware analysis, virtual box set up (windows_xp, remnux) **Objective: u**nderstanding the essence of malware analysis, tools required.
Week -6	**Task :** exploring the different tools available in the v-box set up **Objective:** understanding the usability of tools.
Week -7	**Task :** dynamic analysis of malwares(srvcp.exe) making use of different tools (wireshark,etc) **Objective:** detecting the malware by making use of tools.
Week -8	**Task :**introduction to buffer over flow attack, understanding memory dump with the help of tools **Objective:** understanding concept of buffer, buffer overflow vulnerability
Week -9	**Task :**demo of buffer over flow exploit **Objective:** understanding how we can access the sudo power by making use of buffer overflow vulnerability
Week-10	**Task:** demo of pdf analysis_ tools **Objective:** understanding the header metadata of pdf, injecting malware (keylogger) into pdf, detecting embedded scripts in the pdf.

Suggested reading:

1. Michael Sikorski and Andrew Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", No Starch Press,2012.
2. Jamie Butler and Greg Hoglund, "Rootkits: Subverting the Windows Kernel", Addison-Wesley, 2005.
3. Dang, Gazet, Bachaalany, "Practical Reverse Engineering", Wiley, 2014.
4. Reverend Bill Blunden, "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition, Jones & Bartlett, 2012.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (MTECH-I)

Course Code**:** IS422 Title of the Course**:** Big Data SecurityL-T-P : 4-0-0 Credits 4

Prerequisite Course / Knowledge (If any): Basic understanding of distributed computing, networking.

Course Outcome (COs)

After completion of this course successfully, the students will be able to…

- CO-1: Describe the challenges of securing distributed systems (Understanding)
- CO-2: Discuss cryptographic protocols required for secure big data communication process. (Understanding)
- CO-3: Examine the complexity and security measures for Cryptographically enforcedsystems (Analyze)
- CO-4: Design a secure Hadoop and Spark Cluster using the best practices. (Create)
- CO-5: Practice network security and operating systems security principles in real world domains. (Apply)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	1	1	2	2	3	2	1	2	2
CO2	1	1	2	2	1	3	3	2	2
CO3	1	2	3	3	2	3	2	2	1
CO4	3	2	3	2	3	2	2	2	3
CO5	3	2	2	1	2	2	2	2	3

Detailed Syllabus:

UNIT – I

Definitions of Big data, Sources of Big data, Types of data, Big data Challenges, Big Data applications - Detecting Fraud, Anti-Money Laundering, Terrorism.

UNIT – II

Securing Distributed Systems, Network Security- Network Segmentation, Firewalls, Intrusion Detection and prevention, Operating systems security

UNIT – III

Cryptographically enforced secure access control mechanisms, Cryptographic protocols required for secure big data communication process, complexity and security measures

UNIT – IV

Secure Computational Platforms for Big data analytics, Hadoop overview, Hadoop ecosystem, Architecture, HDFS Storage, Map-Reduce distributed Processing, example data sets, Spark Overview, Hadoop vs Spark, ,Introduction to HPC, HPC cluster components

UNIT – V

Data Protection, Encryption Algorithms, Encrypting Data at Rest, Encryption and Key Management, HDFS Data-at-Rest Encryption, MapReduce Intermediate Data Encryption, Filesystem Encryption

References Books:

1. Spivey, B., & Echeverria, J. (2015). *Hadoop Security: Protecting your big data platform*. " O'Reilly Media, Inc.".
2. Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (2015). *Application of big data for national security: a practitioner's guide to emerging technologies*. Butterworth-Heinemann.
3. Bunnik, A., Cawley, A., Mulqueen, M., & Zwitter, A. (Eds.). (2016). *Big data challenges: society, security, innovation and ethics*. Springer
4. Dunning, T., & Friedman, E. (2015). *Sharing Big Data Safely: Managing Data Security*. " O'Reilly Media, Inc.".
5. White, T. (2012). *Hadoop: The definitive guide*. " O'Reilly Media, Inc.".
6. Karau, H., & Warren, R. (2017). *High performance Spark: best practices for scaling and optimizing Apache Spark*. " O'Reilly Media, Inc.".

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: **M.Tech (Information Security) (MTECH-I)**

Course Code**:** IS423 Title of the Course**:** Coding Theory and Information TheoryL-

T-P: 4-0-0 Credits 4

Pre-requisite Course: Basic understanding of coding

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Analyze the robustness of coding techniques. (Analyze)
- CO-2: Describe the error correcting codes (Understanding)
- CO-3: Apply error correcting codes. (Apply)
- CO-4: Discuss various convolution encoding techniques. (Understanding)
- CO-5: Apply randomized network coding application of network coding. (Apply)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	2	2	3	2	2	2	1	13	2
CO2	2	3	2	3	22	3	1	2	1
CO3	1	2	2	2	3	3	2	3	3
CO4	2	1	3	3	3	2	3	1	2
CO5	1	3	3	3	2	2	2	2	3

Detailed Syllabus:

UNIT – I
Information Theory: Entropy, its characterization and related properties, Huffman codes, Shannon-Fano coding, robustness of coding techniques, Information measure-noiseless coding, discrete memoryless channel – channel capacity, fundamental theorem of information theory.

UNIT – II
Coding Theory: Error correcting codes, minimum distance principles, Hamming bound, general binary code, group code, and linear group code.

UNIT – III
Convolution encoding: algebraic structure, Gilbert bound. Threshold decoding: threshold decoding for block codes. Cyclic binary codes: BCH codes, generalized BCH code and decoding, optimum codes, concepts of non-cyclic codes.

UNIT – IV
Combinatorial Designs: Definitions of BIBD, Hadamard Designs, Latin Squares, Mutually Orthogonal Latin Squares, Orthogonal Arrays. Constructions of codes using designs: Example: Hadamard codes.

UNIT – V
Network Coding: Fundamentals of Network Coding: Butterfly networks, graphs and networks, The max-flow min-cut theorem, the multi-source multicast problem, deterministic code design for network coding, randomized network coding application of network coding.

Suggested Reading:

1. J. H. van Lint: Introduction to Coding Theory, Third Edition, Springer, 1998.
2. F. J. MacWilliams and N.J. Sloane: Theory of Error Correcting Codes, Parts I and II, North-Holland, Amsterdam, 1977.
3. J. A. Thomas and T. M. Cover: Elements of information theory, Wiley, 2006.
4. D. Stinson: Combinatorial Designs: Constructions and Analysis, Springer, 2003
5. P. J. Cameron and J. H. van Lint: Designs, Graphs, Codes and their Links, Cambridge University Press, 2010.
6. C. Fragouli and E. Soljanin: Network Coding Fundamentals, Now Publisher, 2007.

M.Tech (Information Security)

II-Semester

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: **M.Tech (Information Security) (MTECH-II)**

Course Code**:** IS451 Title of the Course**:** Security Tool and Technologies

L-T-P: 4-0-0 Credits 4

Pre-requisite Course: Basic understanding of coding

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Design of Access Control and Authentication mechanisms for security (Create)
- CO-2: Appraise the perimeter security fundamentals (Evaluate)
- CO-3: Assemble the router security to set it up as a security device (Create)
- CO-4: Describe PKI security protocols and Digital Certificate (Understand)
- CO-5: Assess host hardening for various attacks. (Evaluate)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	2	2	3	2	2	2	1	13	2
CO2	2	3	2	3	2	3	1	2	1
CO3	1	2	2	2	3	3	2	3	3
CO4	2	1	3	3	3	2	3	1	2
CO5	1	3	3	3	2	2	2	2	3

Detailed Syllabus:

UNIT I

Securing Information Using Authentication and Access Control: introduction to Access Control, Implementing an Authentication Strategy, Implementing an Access Control Strategy, Cryptography, PKI: Introduction to Certificates, Introduction to Public Key Infrastructure, Deploying and Managing Certificates

UNIT II

Perimeter Security Fundamentals, Packet Filtering: How packet filtering works, Problems with packet filters, Dynamic packet, Stateful firewalls: How stateful firewall works, The concept of a state, Stateful inspection and stateful filtering

UNIT III

Proxy firewalls: Proxy or application gateway firewalls, Protocol issues for proxies, Security policy, Router as a security device, Router hardening

UNIT IV

Network Intrusion Detection: The roles of network IDS in a perimeter defence, IDS sensor placement, Virtual Private Networks: Advantages and Disadvantages of VPNs, IPSec basics, Other VPN, protocols PPTP & L2TP

UNIT V

Security protocols & Implementations: SSL/TLS, SSH, PGP, SHTTP, IPSec, Open SSL, Host hardening: Against local attacks, against network attacks, against application attacks, Antivirus solutions and deployment, Software updates and patches.

Reference books:

1. William Stallings(2017), *Cryptography And Network Security: Principles and Practices*, Seventh Edition, Pearson Publication.

2. William Stallings, Lawrie Brown(2016), *Computer Security: Principles and Practices*, Second Edition, Pearson Publication.

3. Ashutosh Saxena (2004), *PKI: Concept, Design and Deployment*, Tata McGrawHill Publication.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (MTECH-II)

Course Code**:** IS452 Title of the Course**:** Ethical Hacking & Computer Forensics

L-T-P: 3-0-0 Credits 3

Pre-requisite Course: Programming Methodology, Operating Systems, DBMS, Computer Networks, Information Security

Course Outcome (COs)

After completion of this course successfully, the students will be able to:

CO-1: Explain the concepts of Ethical Hacking (Understand)
CO-2: Explain the types of Hackers and their roles in IT industry (Understand)
CO-3: Write Batch programming for hacking (Create)
CO-4: Set up hacking environment using virtualization platform by creating virtual machine to simulate hacking (Create)
CO-5: Describe password cracking techniques and various tools (Understand)
CO-6: Explain the concepts of Packet sniffing, Email spoofing, DNS cache poisoning, Proxies/VPN, google dorks, Steganography, DDoS attacks, etc. (Understand)
CO-7: Describe the phases in computer forensics (Understand)
CO-8: Discuss the file system concepts used in Windows and Linux (Understand)
CO-9: Review various digital forensic tools for Seizure, Acquire and Analysis (Understand) CO-10: Design and develop given tasks on Ethical Hacking / Computer forensics (Create)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	2	2	3	2	2	2	1	3	2
CO2	2	3	2	3	2	3	1	2	1
CO3	1	2	2	2	3	3	2	3	3
CO4	2	1	3	3	3	2	3	1	2
CO5	1	3	3	3	2	2	2	2	3
CO6	2	2	3	2	2	2	1	3	2
CO7	1	3	3	3	2	2	2	2	3
CO8	2	2	3	2	2	2	1	3	2
CO9	3	3	2	2	1	2	2	1	3
CO10	3	1	2	1	2	3	3	2	3

Detailed Syllabus:

Detailed Syllabus:

UNIT-I: Introduction: Aims and Objectives, Technology involved and current issues in the IT industry, glimpse of information security, Ethical Hacking and Computer forensics.

UNIT-II: Batch programming for Hacking. Penetration testing using NMAP, Metasploitable linux: OS for penetration testing, Metasploit framework: Framework for exploiting.

UNIT-III: Introduction to password cracking techniques. Exploring various password cracking tools: Cain & Abel, mimkatz, John the Ripper, RainbowCrack, etc. Various DoS attack techniques, DDoS attack and RDDoS attack.

UNIT-IV: Introduction to Packet sniffing (WireShark, TCPDump, NetworkMiner, etc.), Keyloggers (keyghost/kidlogger, form grabbing), Email spoofing, DNS cache poisoning, Proxies/VPN (cyber ghost VPN), google dorks, Steganography (Invisible secrets, S tools), etc.

UNIT-V: Introduction to computer forensics, cyber-crime, recent cyber-crimes within and outside the country. Phases of digital forensics to analyze cyber-crimes. Roles of law-enforcement and cyber-crime investigator in combatting cyber-crimes.

UNIT-VI: Introduction to file systems. File structural details of how files get created and deleted at system level (for file systems: FAT, NTFS, Ext2/Ext3). Exploring computer forensic tools: TrueBack, CyberCheck, FTKImager, DFF (digital forensic framework), TSK (The sleuth Kit), Volatility framework, etc.

Text Books:

1. James S. Tiller, "The Ethical Hack: A Framework for Business Value Penetration Testing", Auerbach Publications, CRC Press, 2004.
2. JOHN R. VACCA, Computer Forensics : Computer Crime Scene Investigation, Firewall Media.

Reference Books:

3. Kenneth C.Brancik "Insider Computer Fraud" Auerbach Publications Taylor & Francis Group -2008.
4. Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, 4e, Cengage Learning.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: **M.Tech (Information Security) (MTECH-II)**

Course Code**:** IS453 Title of the Course**:** Cyber Security Lab

L-T-P: 1-0-2 Credits 3

Pre-requisite Course: Basics of Operating Systems and Web Technology

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Evaluate and assess the various cyber security threats (Evaluate)
- CO-2: Categorize and identify appropriate Open Source tools for CS (Analyze)
- CO-3: Appraise about the various attacking techniques used in the Internet (Analyze)
- CO-4: Compare and Contrast different attacks in the web (Analyze)
- CO-5: Evaluate the web site vulnerabilities using scanning tools (Evaluate)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	3	2	3	3	2	2	3	3	2
CO2	2	3	3	3	2	2	1	2	2
CO3	3	1	2	3	3	3	2	1	3
CO4	2	1	3	3	3	2	2	1	3
CO5	3	3	3	3	3	2	2	2	2

Detailed Syllabus:

Week	Name of the Experiment
Lab-1	Install 2 VMs with different OSs and establish communication between two hosts and remote access of either host **Objective:** To understand the installation and remote access procedure of the VM
Lab-2	Using Burp Suite tool to scan local website and make a report of all vulnerabilities. **Objective:** To understand the functioning of the scanning tool and site vulnerabilities thereof.
Lab-3	TCP scanning using NMAP **Objective**: To understand the functioning of network ports.
Lab-4	TCP / UDP connectivity using Netcat **Objective**: To understand the connectivity in the network.
Lab-5	Network vulnerability using OpenVAS **Objective**: To Understand the network related.
Lab-6	Web application testing using DVWA **Objective**: To Understand the processes of securing web applications
Lab-7	Manual SQL injection using DVWA **Objective**: To understand and execute malicious SQL statements that control a web application's database server.
Lab-8	XSS using DVWA **Objective**: To understand XSS statements and their effect on web application.

Suggested Readings

1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
2. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison Wesley, 2011.
3. Wu and Liz Zhao, WEB SECURITY A WhiteHat PerspectiveHanqing, CRC Press, 2015.
4. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, 1st Edition, No-Starch Press, 2014.
5. Justin Seitz, Black Hat Python: Python Programming for Hackers and Pentesters 1st Edition, No-Starch Press, 2014.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech((Information Security) (M.Tech-II)

Course Code**:** IS471 Title of the Course**:** Information System Control and Audit

L-T-P: 3-1-0 Credits 4

Pre-requisite Course: Information Systems

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Describe the Control and Audit process.(Understand)
- CO-2: Demonstrate the Information Systems Audit. (Apply)
- CO-3: Evaluate the planning and leading function of IS Audit (Evaluate)
- CO-4: Assess the Application Control Framework.(Evaluate)
- CO-5: Evaluate asset Safeguarding and Data Integrity.(Evaluate)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PSO1**	**PSO2**	**PSO3**
CO1	2	3	2	1	1	1	2	1	1
CO2	2	3	2	1	1	1	1	1	2
CO3	3	2	3	1	2	2	3	2	2
CO4	3	2	3	2	3	3	3	3	2
CO5	3	2	3	3	3	3	3	3	2

Detailed Syllabus

UNIT- I

Overview of Information System Auditing, Effect of Computers on Internal Controls, Effects of Computers on Auditing, Foundations of information Systems Auditing, Conducting an Information Systems Audit.

UNIT- II

The management Control Framework: Introduction, Evaluating the planning Function, Evaluating the Leading Function, Evaluating the Controlling Function, Systems Development Management Controls, Approaches to Auditing Systems Development, Normative Models of the Systems Development Process, Evaluating the Major phases in the Systems Development Process, Programming Management Controls, Data Resource Management Controls.

UNIT-III

The Application Control Framework-I: Boundary Controls, Input Controls, Communication Controls. The Application Control Framework-II: Processing Controls, Database Controls, output Controls.

UNIT- IV

Evidence Collection: Audit Software, Code Review, Test Data, and Code Comparison, Concurrent Auditing techniques, Interviews, Questionnaires, and Control Flowcharts. Performance Management tools.

UNIT -V

Evidence Evaluation: Evaluating Asset Safeguarding and Data Integrity, Evaluating System Effectiveness, Evaluating System Efficiency.

References Books.:

1. Ron Weber, Information Systems Control and Audit, Pearson Education, 2002.
2. M.Revathy Sriram, Systems Audit, TMH, New Delhi, 2001.
3. Jalote : Software Project Mangement in Practice, Pearson Education
4. Royce : Software Project Management, Pearson Education.

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (MTECH-II)

Course Code**:** IS472 Title of the Course**:** Statistics & Probability

L-T-P: 3-0-0 Credits 3

Pre-requisite Course: Prior knowledge of the counting aspects of discrete mathematics is desirable including permutations and combinations

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Describe the process of data collection and its analysis (Understanding)
- CO-2 : Evaluate moments, kurtosis and skewness (Evaluate)
- CO-3 : Apply correlation and regression to data analysis (Apply)
- CO-4 : Apply the results of distributions and sampling distribution to the given data
- CO-5 : Test a given hypothesis (Analyze)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	1	1	2	3	3	2	1	2	2
CO2	1	1	2	3	2	2	1	1	2
CO3	1	1	1	3	2	2	1	2	2
CO4	1	1	1	3	3	2	2	2	3
CO5	1	2	3	3	3	3	2	3	3

Detailed Syllabus:

Unit I:

Data analysis and its Phases: Stating and refining the question, Exploring the data, Building formal statistical models, interpreting the results, communicating the results. Dimensionality reduction and itsimportance in data analysis.

Unit II:

Measures of Central Tendency: Arithmetic mean, Median, Quartiles, Deciles, Percentiles, the mode, geometric mean. Measures of dispersion: the range, quartile deviation, mean deviation, coefficient of meandeviation, standard deviation, variance, coefficient of variation. Moments, moments about the mean, Skewness, Kurtosis.

Unit III:

Correlation and Regression: correlation, degree of correlation, causation of correlation, simple and multiplelinear regression, Karl-Pearson's coefficient of correlation, multiple correlation analysis.

Unit IV:

Probability, A priori probability, conditional probabilities, Baye's theorem, random variables, expectations,probability distributions: binomial, normal, Poisson distribution, random sampling, sampling distributions

Unit V:

Estimation and Testing of Hypothesis: estimation and confidence level, standard error estimation,statistical inferences and testing of hypothesis.

Reference Books

1. Douglas C Montgomery and George C Runger (2010), *Applied Statistics and Probability for Engineers, 5thEdition*, John Wiley & Sons, 784 pages.
2. Walter A Rosenkrantz (2008), *Introduction to Probability and Statistics for Science, Engineering, and Finance,1st Edition,* Chapman and Hall / CRC, 680 pages.
3. William Feller (1968), *An Introduction to Probability Theory and its Applications, 3rd Edition,* Wiley, 528pages.
4. Robert V Hogg, Joeseph McKean, Allen T Craig (2012), *Introduction to Mathematical Statistics, 7th Edition*, Pearson Education, 704 pages.

Academic Time Table with the name of the Faculty members handling the Course

M.Tech Information Security (Sem-1)

Tentative Time Table (Nov-2021)

	9 -10 **(1)**	***10 -11*** **(2)**	***11-12*** **(3)**	***12-1*** **(4)**	***1-2***	***2-3*** **(5)**	***3-4*** **(6)**	***4-5*** **(7)**
Monday		MFIS	BCT	BCT	**L U N C H**		CTWS	CTWS
Tuesday		MFIS	Crypto	Crypto			CTWS	CTWS
Wednesday		RE Lab	RE Lab	RE Lab		MFIS	MFIS	
Thursday		SOS	SOS			BCT	Crypto	
Friday		SOS	SOS					
Saturday								

Course Code	**Course Name**	**Faculty**
Core Courses		
IS401	Mathematical Foundation for Information Security(MFIS)	Dr.G.Padmavathi(C R RaoAIMSCS)
IS402	Secure Operating System and Computer Organization(SOS)	Dr. Sirisha V(C R RaoAIMSCS)
CS425	Cryptography	Dr.Y.V. Subba Rao(SCIS)
IS453	Laboratory: Reverse Engineering and Malware Analysis (RE)	Dr. Appala Naidu/Dr. Barnali Gupta(C R RaoAIMSCS)
Electives		
CS426	BlockChain Technology (BCT)	Dr. N. Rukma Rekha (SCIS)
IS421	Current trends in Web Security(CTWS)	Dr. Pradeepthi K.V. (C R RaoAIMSCS)

- Internal Continuous Evaluation System in place : Yes
- Student's assessment of Faculty, System in place : Yes