Central University of Rajasthan
School of Engineering & Technology
Department of Computer Science & Engineering
Scheme and Syllabus 2022 – 23 onwards

Master of Technology in Computer Science & Engineering with Specialization in Information Security (M.Tech. (CSE))

Program Outcomes:

PO1.An understanding of the theoretical foundations and the limits of computing.

PO2. An ability to adapt existing models, techniques, algorithms, data structures, etc. for efficiently solving problems.

PO3. An ability to design, develop and evaluate new computer based systems for novel applicationswhich meet the desired needs of industry and society.

PO4. Understanding and ability to use advanced computing techniques and tools.

PO5. An ability to undertake original research at the cutting edge of computer science & its relatedareas.

PO6. An ability to function effectively individually or as a part of a team to accomplish a stated goal.

PO7. An understanding of professional and ethical responsibility.

PO8. An ability to communicate effectively with a wide range of audience.

PO9. An ability to learn independently and engage in life-long learning.

PO10. An understanding of the impact of IT related solutions in an economic, social and environmentcontext.

Program Specific Outcomes:

1. At the end of the program, graduates will be able to get insights into various fields of information security with a deep understanding of theoretical aspects of security and related analysis.
2. Graduates should also get a broader understanding of various security systems, protocols, complexities, standards, practical applicability, and their limitations.
3. During the course, students should enhance their inquisitiveness to ever-evolving domain of information security and apply their knowledge to solve problems.

Scheme

First Year

SEMESTER I						
Sr. No	**Course Code**	**Course Name**	**L**	**T**	**P**	**Credits**
			Hours/week			
1	CSE601	Algorithm and Complexity	3	1	0	4
2	CSE602	Topics in Computer Science	3	0	2	4
3	--	Program Elective -I	3	1	0	4
4	--	Program Elective -II	3	1	0	4
5		Open Elective -I	3	1	0	4
Total Credits						**20**

SEMESTER II						
Sr. No	**Course Code**	**Course Name**	**L**	**T**	**P**	**Credits**
			Hours/week			
1	CSE603	Cryptography and Network Security	3	0	2	4
2	CSE604	Security Engineering	3	0	2	4
3	--	Program Elective –III	3	1	0	4
4		Program Elective – IV	3	1	0	4
5		Open Elective – II	3	1	0	4
Total Credits						**20**

Second Year

SEMESTER III						
Sr. No	**Course Code**	**Course Name**	**L**	**T**	**P**	**Credits**
			Hours/week			
1	CSE701	SSR	0	0	8	4
2	CSE702	Dissertation – I / Project - I	0	0	32	16
Total Credits						**20**

SEMESTER IV						
Sr. No	**Course Code**	**Course Name**	**L**	**T**	**P**	**Credits**
			Hours/week			
1	CSE703	Dissertation – II / Project - II	0	0	40	20
Total Credits						**20**

Note: Course CSE701 shall be of Self-study, where a student is supposed to study a advanced topic in Computer Science/IT and needs to prepare technical report based on their study and the evaluation shall be done through seminar (CIA 1, CIA 2 and ESE).

List of Electives

Following list has to be used for offering Programme Elective/ Open Elective. Additional Elective can be added as and when required after taking departmental approval.

Course Code	Programme / Open Elective (s)
CSE631	Quantum Cryptography
CSE632	Information Security Audit and Assurance
CSE633	Security Analysis of Protocols
CSE634	Cyber Crime, Forensics and Information Warfare
CSE635	Public Key Infrastructure and Trust Management
CSE636	Digital Watermarking and Steganalysis
CSE637	Data Mining and Machine Learning
CSE638	Simulation and Modeling
CSE639	Optimization Techniques
CSE640	Topics in Operating Systems
CSE641	Topics in Computer Architecture
CSE642	Advanced Compiler Design
CSE643	Advanced Topics in Databases
CSE644	Mobile Computing
CSE645	Advance Software Engineering
CSE646	Multimedia System and Security
CSE647	Secure Programming Techniques
CSE648	Network Protocols
CSE649	Cloud Computing
CSE650	Parallel Processing
CSE651	Digital Image Processing
CSE652	Biometrics and Security
CSE653	Number Theory
CSE654	Machine Learning
CSE655	System Design

CSE656	Information Theory and Coding
CSE657	Computer Vision

Syllabus:

First Year

SEMESTER I

CSE601 Algorithm and Complexity		
Teaching Scheme	Examination Scheme	Credits allocated
Theory 3 h/week+ Tutorial 1h/week	End of semester Examination-60 marks	Theory-3, Tutorial-1
Course Prerequisite: Students should have knowledge of data structure concepts		
Course Objective: **1.** To understand the proof of correctness and running time of the algorithms for the classic problems in various domains **2.** To apply algorithmic design paradigms and methods of analysis in common engineering design situations.		
Course Outcomes: On completion this course, students will be able to		
1. Ability to apply the algorithms and design techniques to solve problems. 2. Ability to develop concepts, logics towards solving graph problems so as to useful in IT and research. 3. Understand various concepts of randomized and approximation algorithms in order to perform competitive analysis. 4. Understand theoretical concepts of optimization and decision problems.		
Level	Masters	
Course Content:		
Unit –I	Brief overview of Notations and Recurrence analysis, Amortized analysis, B- Trees, Dictionaries and tries, BinomialHeaps, Fibonacci Heaps, Disjoint Sets, Union by Rank and Path Compression.	10 hrs
Unit-II	Graph Algorithms, Topological sorting, Articulation point, All-PairsShortest Paths, Spanning Tree, Maximum Flow and Bipartite Matching.	10 hrs
Unit-III	Randomized Algorithms, Finger Printing, Pattern Matching, Graph Problems,Primality Testing algorithms, Approximation algorithms, Polynomial Time Approximation Schemes, PTAS, FPTAS, Approximation algorithms for vertex cover, set cover, TSP problem.	10 hrs

Unit-IV	Definitions of P, NP, NP-Hard and NP-Complete Problems, Optimization and Decision Problems, Reducibility, Cook's Theorem, Satisfiability problem, NP completeness reductions examples.	10 hrs

Internal assessment

Part A	CIA-I: Unit I, and II	20 Marks
	CIA-II: Unit III, and IV	20 Marks
Part B	ESE: Term Exam	60 Marks

Text/Reference Books:

1. T. H. Cormen, C. E. Leiserson, R. L. Rivest, Introduction to Algorithms, Prentice Hall.
2. Aho, Hopcraft, Ullman, Design and Analysis of Computer Algorithms, Addison Wesley.
3. R. Motwani and P. Raghavan, Randomized Algorithms, Cambrdige University Press.
4. C. H. Papadimitriou, Computational Complexity, Addison Wesley.
5. S. Basse, Computer Algorithms: Introduction to Design and Analysis, Addison Wesley.

CO/PO mapping

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	2	3	3	2	3				2	2
CO2	2	3	3	2	3				2	2
CO3	2	3	3	2	3				2	2
CO4	2	3	3	2	3				2	2

CSE602 Topics in Computer Science

Teaching Scheme	Examination Scheme	Credits allocated
Theory 3 h/week+ Tutorial 1h/week	End of semester Examination-60 marks	Theory-3, Tutorial-1

Course Prerequisite: Operating Systems, Computer Networks, Programming

Course Objective:

1. To impart advanced knowledge related to different important building blocks of computer science.
2. To enable students to understand the overall solution space and research directions in Computer Science.

Course Outcomes: On completion this course, students will be able to

1. Students should be able to understand various network protocols, their open-source implementations, performance issues, and simulations.
2. Students of this course should be able to understand the need and uses of defensive and secure programming techniques with risks and threats in mind.
3. Students should be able to understand the basic principles of machine learning.
4. Students should be able to understand the important principles of advanced operating systems.

Level	Masters

Course Content:

Unit –I	**Network Performance:** Network Simulation and Modeling, Performance issues in networks, Protocol case studies (e.g. HTTP, HTTPS, SSL, DHCP, DNS, Transport protocols and Routing protocols in wired and wireless networks and their performance).	10 hrs

Unit-II	Secure Design and Coding Principles and Policies.Misuse and Abuse Cases, Risk Assessment, Test Planning, Threat Modeling, Distrustful Decomposition, Defensive Coding, Validation and Sanitization.	10 hrs
Unit-III	Machine Learning: Aspects of developing a learning system: training data, concept representation, function approximation. Linear Regression, ANN	10 hrs
Unit-IV	Advanced Operating Systems: Distributed System principals and case studies.	10 hrs

Internal assessment

Part A	CIA-I: Unit I, and II	20 Marks
	CIA-II: Unit III, and IV	20 Marks
Part B	ESE: Term Exam	60 Marks

Text/Reference Books:

1. Computer Networking: A Top-Down Approach (6th Edition), J Kurose and KW Ross, Pearson, 2012.
2. Bishop, C. (2006) Mitchell, T. M. Machine Learning. McGraw-Hill
3. Pattern Recognition and Machine Learning. Berlin: Springer-Verlag.
4. Richard O. Duda, Peter E. Hart and David G. Stork. Pattern Classi_cation. Wiley-Interscience, second edition,2001.
5. Singhal, Mukesh, and Niranjan G. Shivaratri. *Advanced concepts in operating systems*. McGraw-Hill, Inc., 1994.

CO/PO mapping

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	2	2	2	1	1				2	2
CO2	2	2	2	1	1				2	2
CO3	2	2	2	1	1				2	2
CO4	2	2	3	1	1				2	2

First Year

SEMESTER II

CSE603 Cryptography and Network Security		
Teaching Scheme	Examination Scheme	Credits allocated
Theory 3 h/week+ Tutorial 1h/week	End of semester Examination-60 marks	Theory-3, Tutorial-1

Course Prerequisite:

Course Objective:

1. To enlighten students with advanced concepts of network security.
2. To enable to students to identify research problems in network security and formulate feasible solutions.

Course Outcomes: On completion this course, students will be able to:

1. Understand concepts of network security and cryptographic techniques.
2. Design and analyze cryptographic techniques.
3. Solve network security issues in real time applications.
4. Take up doctoral level research work in security.

5.

Level	Masters

Course Content:		
Unit -I	**Cryptography:** Introduction, steganography, Public versus private key cryptography. **Stream Ciphers**: Conventional Ciphers, playfair, Hill, mono-alphabetic and poly-alphabetic	10 hrs
Unit-II	**Private-key cryptography**: Feistel structure, DES, design of S-boxes, AES, Triple DES, Differential and linear cryptanalysis.	10 hrs
Unit-III	**Public key cryptography:** Key management, Diffie-Hellman,ElGamal, RSA. Random Number Generation, Primality testing, Elliptic Curves and ECC. **Digital Signature:** DSA and its variants, discrete logarithm based digital signatures.	10 hrs
Unit-IV	**Network Security**: Authentication and signature protocols; Kerberos, real-timecommunication security, IPSec: AH, ESP, IKE; SSL/TLS, e-mail security, PEM and S/MIME, PGP, web security, network management security, wireless security. Threats in networks, firewalls, intrusion detection, Honeypots, password management	10 hrs

Internal assessment		
Part A	CIA-I: Unit I, and II	20 Marks
	CIA-II: Unit III, and IV	20 Marks
Part B	ESE: Term Exam	60 Marks

. **Text/Reference Books:**D.R. Stinson, Cryptography - Theory and practice, CRC Press.

. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Applied Cryptography, CRC Press.

3. Stallings, Cryptography and Network Security, Pearson Education.

CO/PO mapping

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	2	2	3	2	1				2	2
CO2	2	3	2	2	1				1	2
CO3	2	2	2	3	1				1	1
CO4	2	2	3	2	1				2	2

CSE604 Security Engineering

Teaching Scheme	Examination Scheme	Credits allocated
Theory 3 h/week+ Lab 2h/week	End of semester Examination-60 marks	Theory-3, Lab-1

Course Prerequisite: Cryptography and Network Security, Programming

Course Objective:

1. To enable students in buildingsecure systems including secure software, hardware and developme and evaluation of such systems.
2. To enable students to find feasible solutions to security requirements of various systems**.**

Course Outcomes: On completion this course, students will be able to

CO1: At the end of this course, students should be able to understand various concepts related engineering secure systems by keeping various threats in mind.

CO2: Understanding of principles related to use of authentication mechanism, their form, security analys overhead, use of security standards related to cryptography and physical security.

CO3: Understanding of building systems using passwords, biometrics, CAPTCHA's, secure programmi techniques, trusted computing, Crypto APIs and physical security.

CO4: Understand a variety of security attacks, their sophistication, and defense mechanisms.

Level	Masters

Course Content:

Unit -I	Introduction to Security Engineering, Passwords and their limitations, attacks on passwords, CAPTCHA, Biometrics. Access Control, ACL, sandboxing, virtualization, trusted computing. Multi-level and Multi-lateral security.	10 hrs
Unit-II	Securing services, Security in Metered Services, pre-payment meters, secure printing and seals. Tamper resistance mechanisms. Secure systems: hardware, software and communication systems – design issues and analysis.	10 hrs
Unit-III	Secure software architecture: models and principles, hardware design related security – smart cards and other security solutions, communication protocols and application systems associated with security.	10 hrs
Unit-IV	Attacks and defenses: Phishing, social networking attacks, Denial of service, API attacks, network attacks and countermeasures, side-channel attack, advanced persistent Threats (APTs), copyright and DRM.	10 hrs

Internal assessment

Part A	CIA-I: Unit I, and II	20 Marks
	CIA-II: Unit III, and IV	20 Marks
Part B	ESE: Term Exam	60 Marks

Text/Reference Books:

1. Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed System. Wiley.
2. Selected papers and online material.

CO/PO mapping

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	2	2	2	1	1				2	2
CO2	2	2	2	1	1				2	2
CO3	2	2	2	1	1				2	2
CO4	2	2	2	1	1				2	2