NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL

RULES AND REGULATIONS

SCHEME OF INSTRUCTION AND SYLLABI

M.Tech. (Computer Science and Information Security)

Effective from 2021-22

Department of Computer Science and Engineering

NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL

VISION

Towards a Global Knowledge Hub, striving continuously in pursuit of excellence in Education, Research, Entrepreneurship and Technological services to the society

MISSION

- Imparting total quality education to develop innovative, entrepreneurial and ethical future professionals fit for globally competitive environment.
- Allowing stake holders to share our reservoir of experience in education and knowledge for mutual enrichment in the field of technical education.
- Fostering product-oriented research for establishing a self-sustaining and wealth creating centre to serve the societal needs.

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

VISION

Attaining global recognition in Computer Science & Engineering education, research and training to meet the growing needs of the industry and society

MISSION

- Imparting quality education through well-designed curriculum in tune with the challenging software needs of the industry.
- Providing state-of-art research facilities to generate knowledge and develop technologies in the thrust areas of computer science and engineering.
- Developing linkages with world class organizations to strengthen industry-academia relationships for mutual benefit.

Department of Computer Science and Engineering:

Brief about the Department:

The Department of Computer Science and Engineering was established in the year 1991. The department offers high quality undergraduate, postgraduate and doctoral programs. The B. Tech. (Computer Science and Engineering) program was started in the year 1983 with an intake of 20 students. The intake was subsequently increased to 120 in 2008. M. Tech (Computer Science and Engineering) program was started in 1987 with an intake of 18 and subsequently increased to 20 in 2008. M. Tech (Information Security) was introduced in the year 2008 Under ISEAP sanctioned by Ministry of Communication and Information Technology (MCIT), DOE, GOI, New Delhi with intake of 20. Later, it was renamed as Computer Science and Information Security. The Master of Computer Applications (MCA) program was started in 1986 with an intake of 30 and increased to 46 from 2008. B. Tech, M. Tech. (CSE) and M. Tech. (CSIS) programs were accredited in 2014 by NBA as per Washington Accord.

List of Programs offered by the Department:

Program	Title of the Program
B.Tech.	Computer Science and Engineering
M. Tech.	Computer Science and Engineering
	Computer Science and Information Security
MCA	Master in Computer Applications
Ph. D.	Computer Science and Engineering

Note: Refer to the Rules and Regulations for M. Tech. program (weblink) given on the institute website.

M.TECH IN COMPUTER SCIENCE AND INFORMATION SECURITY

PROGRAM EDUCATIONAL OBJECTIVES

PEO1	Apply knowledge of computer science to provide information security.
PEO2	Design and develop secure software systems using models as per user requirements.
PEO3	Work in teams using common security tools and environment to achieve project objectives
PEO4	Communicate effectively, demonstrate leadership qualities and exhibit professional ethics.
PEO5	Engage in lifelong learning to adapt to changing professional and societal needs for career advancement.

MAPPING OF DEPARTMENT MISSION STATEMENTS WITH PROGRAM EDUCATIONAL OBJECTIVES

Mission Statement	**PEO1**	**PEO2**	**PEO3**	**PEO4**	**PEO5**
Imparting quality education through well-designed curriculum in tune with the challenging software needs of the industry	2	3	2	2	2
Providing state-of-art research facilities to generate knowledge and develop technologies in the thrust areas of computer science and engineering	1	1	3	2	1
Developing linkages with world class organizations to strengthen industry-academia relationships for mutual benefit.	2	3	2	1	1

PROGRAM OUTCOMES: At the end of the program the student will be able to:

PO1	Engage in critical thinking and pursue investigations / research and development to solve practical problems.
PO2	Communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.
PO3	Demonstrate higher level of professional skills to tackle multidisciplinary and complex problems related to information security.
PO4	Specify secure protocols for safe handling the digital assets and for exchange of information among entities in the real world.
PO5	Design algorithms for secure multi-party computations and analyze their complexities.
PO6	Evaluate alternative designs of secure systems focusing on efficiency, scalability and cost parameters with compliance to legal, privacy and ethical issues of the operational field.

MAPPING OF PROGRAM OUTCOMES WITH PROGRAM EDUCATIONAL OBJECTIVES

PO	PEO1	PEO2	PEO3	PEO4	PEO5
1	2	3	1		1
2			1	2	1
3		2	2		1
4	3	3	2		2
5	3	1			2
6	2	3	3	2	2

CURRICULAR COMPONENTS

Degree Requirements for M. Tech. in Computer Science and Information Security

Category of Courses	Credits
Program Core Courses (PCC)	32
Professional Elective Courses (PEC)	12
Seminar I and II (SEM)	2
Comprehensive Viva-voce (CVV)	2
Dissertation Work (DW)	32
Total	**80**

SCHEME OF INSTRUCTION

M.Tech (Computer Science and Information Security) Course Structure

M. Tech. I - Year I - Semester

S. No.	Course No.	Course Name	L	T	P	Credits	Cat. Code
1	CS5101	Advanced Algorithms	3	0	0	3	PCC
2	CS5201	Web and Database Security	3	0	0	3	PCC
3	CS5202	Foundations of Cryptography	3	0	0	3	PCC
4	CS5203	Data Mining	3	0	0	3	PCC
5	CS5204	Computational Mathematics Practice	1	1	2	3	PCC
6		Elective – 1	3	0	0	3	PEC
7	CS5205	Cryptography Lab	0	1	2	2	PCC
8	CS5206	Web and Database Security Lab	0	1	2	2	PCC
9	CS5248	Seminar – I	0	0	2	1	SEM
		Total	**18**	**2**	**6**	**23**	

M. Tech. I - Year II - Semester

S. No.	Course No.	Course Name	L	T	P	Credits	Cat. Code
1	CS5251	Network Security	3	0	0	3	PCC
2	CS5252	Data Privacy	3	0	0	3	PCC
3	CS5152	Deep Learning	3	0	0	3	PCC
4		Elective – 2	3	0	0	3	PEC
5		Elective – 3	3	0	0	3	PEC
6		Elective – 4	3	0	0	3	PEC
6	CS5253	Network Security Lab	0	0	2	1	PCC
7	CS5254	Data Privacy Lab	0	0	2	1	PCC
8	CS5154	Deep Learning Lab	0	1	2	2	PCC
10	CS5298	Seminar- II	0	0	2	1	SEM
		Total	**18**	**1**	**8**	**23**	

M. Tech II - Year I - Semester

S. No.	Course No.	Course Name	L	T	P	Credits	Cat. Code
1	CS6247	Comprehensive Viva-voce	0	0	0	2	CVV
2	CS6249	Dissertation Work – Part A	0	0	0	12	DW
		Total				**14**	

M. Tech II - Year II - Semester

S. No.	Course No.	Course Name	L	T	P	Credits	Cat. Code
1	CS6299	Dissertation Work – Part B	0	0	0	20	DW
		Total				**20**	
		Total Credits				**80**	

Credit Distribution Table – Semester-wise and Category-wise

Cat code	I year		II year		Total
	Sem I	Sem II	Sem I	Sem II	
PCC	19	13			32
PEC	3	9			12
SEM	1	1			2
CVV			2		2
DW			12	20	32
Total	23	23	14	20	**80**

Professional Elective Courses

M. Tech. I - Year I - Semester

Semester	Elective Number	Course Code	Course Title
1	1	CS5211	Computational Number Theory
1	1	CS5212	Mathematical models for Internet
1	1	CS5213	Cryptanalysis
1	1	CS5214	Computability and Complexity
1	1	CS5215	Information Systems Control and Auditing
1	1	CS5216	Probabilistic Algorithms
1	1	CS5217	Biometric Security
1	1	CS5218	Unix Internals
1	1	CS5219	Secure Software Engineering
1	1	CS5220	Secure Cloud Computing
1	1	CS5221	Algorithmic Game Theory
1	1	CS5222	Digital Video Processing
1	1	CS5223	Information Security and Secure Coding
1	1	CS5224	Scripting languages for information security
1	1	CS5225	Wireless and Mobile Networks
[M.Tech. CSE courses]			
1	1	CS5103	Advanced Operating Systems
1	1	CS5104	Data Science Fundamentals
1	1	CS5105	Advanced Software Engineering
1	1	CS5112	Advanced Databases
1	1	CS5113	Computer Vision & Image Processing
1	1	CS5116	Distributed Computing
1	1	CS5117	Quantum Computing
1	1	CS5119	Advanced Artificial Intelligence
1	1	CS5120	Big Data
1	1	CS5121	Bio-Informatics
1	1	CS5122	Advanced Data Structure
1	1	CS5123	Advanced Compiler Design

M. Tech. I - Year II - Semester

2	2/3/4	CS5261	Foundations of Block Chain Technology
2	2/3/4	CS5262	Secure Operating Systems
2	2/3/4	CS5263	Design of Secure Protocols
2	2/3/4	CS5264	Secure Multiparty Computation
2	2/3/4	CS5265	Secure Protocols for Electronic Commerce
2	2/3/4	CS5266	Research study on Information Security
2	2/3/4	CS5267	Network Coding
2	2/3/4	CS5268	Public Key Infrastructure and Trust Management
2	2/3/4	CS5269	Cyber laws and Intellectual Property Rights
2	2/3/4	CS5270	Algorithmic Coding Theory
2	2/3/4	CS5271	Digital Forensics

2	2/3/4	CS5272	Secure Dependable and Distributed Computing
2	2/3/4	CS5273	Data Hiding
2	2/3/4	CS5274	Identity Based Cryptography
2	2/3/4	CS5275	Information Security Risk Management
2	2/3/4	CS5276	Privacy Enhancing Technologies
2	2/3/4	CS5277	Security of E-Based Systems
2	2/3/4	CS5278	Secure Group Communication
2	2/3/4	CS5279	Cyber crime and Information Warfare
2	2/3/4	CS5280	Cryptography and Game Theory
2	2/3/4	CS5281	Malware Analysis
2	2/3/4	CS5282	Cyber Security
2	2/3/4	CS5283	Elliptic Curve Cryptosystems
2	2/3/4	CS5284	Secure Systems Engineering
2	2/3/4	CS5285	Privacy and Security for online social networks
2	2/3/4	CS5161	Service Oriented Architecture and Micro-Services
[M.Tech. CSE courses]			
2	2/3/4	CS5151	Advanced Computer Networks
2	2/3/4	CS5163	Software Reliability and Quality Management
2	2/3/4	CS5165	Formal Methods in Program Design
2	2/3/4	CS5167	Cognitive Radio Networks
2	2/3/4	CS5168	Model Driven Frameworks
2	2/3/4	CS5169	Exploratory and Interactive Data Analysis
2	2/3/4	CS5170	Internet of Things
2	2/3/4	CS5171	Real Time Systems
2	2/3/4	CS5172	Optimization in Computer Science
2	2/3/4	CS5173	High Performance Computing
2	2/3/4	CS5175	Human Computer Interaction
2	2/3/4	CS5176	Social Media Analytics
2	2/3/4	CS5179	Software Defined Networks
2	2/3/4	CS5180	Natural Language Processing
2	2/3/4	CS5181	Information Retrieval
2	2/3/4	CS5182	Soft Computing Techniques
2	2/3/4	CS5183	Advanced Data Mining
2	2/3/4	CS5184	Fault Tolerant Systems
2	2/3/4	CS5185	Fog and Edge Computing
2	2/3/4	CS5187	Reinforcement Learning

Note: A student is allowed to register a maximum of one elective from other departments and a maximum of two electives from other M.Tech. programmes offered by the Department of CSE.

DETAILED SYLLABUS

Course Code: CS5101	ADVANCED ALGORITHMS	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analyze worst-case running times of algorithms using asymptotic analysis.
CO2	Classify problems into different complexity classes corresponding to deterministic, approximation and parameterized algorithms.
CO3	Analyze the complexity of graph problems for different graph classes.
CO4	Analyze approximation algorithms and determine approximation factor.
CO5	Design and analyze efficient randomized algorithms.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	3	-	3	3	-	-
CO2	3	-	3	3	-	-
CO3	3	-	3	3	-	-
CO4	3	-	3	3	-	-
CO5	3	-	3	3	-	-

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Average case analysis of algorithms, Correctness of Master Theorem, Selection in Worst Case Linear Time, Large integer multiplications using FFT, Dynamic Programming - Matrix Chain Multiplication Problem, Optimal Binary Search Tree, Linear Algorithm for Domination in Trees, Maximum Cardinality Search and Chordal Graphs, Greedy Algorithm for Optimal Coloring of Chordal Graphs, NP-completeness, Efficient Reduction Proofs via Examples, Domination in Subclasses of Bipartite Graphs and Chordal Graphs, Exact Exponential Algorithm for Domination Problems, Treewidth, Parameterized Complexity Classes, APX-hardness and APX-completeness, Approximation Algorithm for Connected Dominating Set Problem, The Stable Marriage Problem, The Coupon Collector`s Problem.

Text Books/Reference Books/Online Resources:

1. *Introduction to Algorithms*, Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, PHI, 2009, Third Edition.

2. *Fundamentals of Computer Algorithms*, Ellis Horowitz, Sartaj Sahni and Sanguthevar Rajasekaran, Universities Press, 2011, Second Edition.
3. *Algorithmic Graph Theory and Perfect Graphs*, Martin Charles Golumbic, 2004, Elsevier, Second Edition.
4. *Treewidth: Computations and Approximations*, Ton Kloks, Springer-Verlag, 1994.
5. *Graph Classes A Survey* : Andreas Brandstädt, Van Bang Le and Jeremy P.Spinard, SIAM, 1987.
6. *Algorithms and Complexity*, Herbert S. Wilf, AK Peters/CRC Press, 2002, Second Edition.
7. *Parameterized Complexity*, Rodney G. Downey and M. R. Fellows, Springer, 2012.
8. *Approximation Algorithms*, Vijay V. Vajirani, Springer, 2001.
9. *Randomized Algorithms*, Rajeev Motwani and Prabhakar Raghavan, Cambridge University Press, 1995.
10. *Computers and Intractability: A Guide to the theory of NP-Incompleteness*, Michael R. Garey and David S. Johnson, W.H. Freeman & Co., 1979, First Edition.
11. *Topics in Domination in Graphs*, Teresa W. Haynes, Stephen T. Hedetniemi and Michael A.Henning, Springer, 2020.

Course Code: CS5201	Web and Database Security	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Identify access control methods for secure web & database application development
CO2	Analyse vulnerabilities in the Web and Database applications.
CO3	Design & Evaluate methods for web & database intrusion detection
CO4	Apply security audit methods
CO5	Design Secure Database schema

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	1	1	1	1
CO2		1	1	1	1	1
CO3		1	2	2	1	2
CO4						2
CO5	1		2	2		1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Database Basics: Overview of Relational Model, SQL, Building of database, Manipulation of data; Goals of Database Security, access points of database security, database security levels, and menaces to databases. Database security methods and methodologies, Security controls: flow control, inference control and access control, Database Application Security models – Types of users, access matrix model, access modes model, commonly used application types. Classes of access control: Discretionary access control (DAC), Mandatory access control (MAC) and Role based Access control (RBAC); Discretionary Access Control (DAC) mechanisms such as capabilities, profiles, access control lists, passwords, and permission bits. RBAC based security models features like User role assignment, Support for role relationships and Constraints , Assignable privileges. MAC based security models. Implementing Fine Grained access controls with views , Virtual Private databases: need for VPDs, Implementing VPD using views, The Database Security Design includes the controls that will be implemented to restrict users from accessing information, based on how the information is classified and the security model. HTML Injection and Cross- Site Scripting, Cross-Site Request, Forgery, SQL Injection and Data Store Manipulation, Breaking Authentication Schemes, Abusing Design Deficiencies, Leveraging Platform Weaknesses, Statistical database security; Database privacy – Hippocratic databases

Text Books/Reference Books/Online Resources:

1. SilvanoCastano, Fugini, Martella, Samarati, *Database Security*, Addison Wesley, 1994.
2. M. Gertz, S. Jajodia, *Handbook of Database Security*, Springer, 2008
3. Ben-Natan, R. B., *Implementing Database Security and Auditing: Includes Examples for Oracle, SQL Server, Db2 Udb, Sybase*, Digital Press, 2005
4. Mike Shema, *Hacking Web Apps Detecting and Preventing Web Application Security Problems*, Syngress publications- Elsevier, 2012

Course Code : CS5202	Foundations of Cryptography	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand Number Theory and Algebra for design of cryptographic algorithms
CO2	Construct finite fields and apply number theoretic concepts in cryptographic algorithm
CO3	Analyse and compare symmetric-key encryption public-key encryption schemes based on different security models
CO4	Prove the security of cryptographic algorithms against attack models
CO5	Investigate and apply homomorphic encryption

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		1	2	2	
CO2	1				1	
CO3	2		1	2	2	3
CO4	2	1	2	3	3	3
CO5	3	2	2	3	2	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Number Theory – Divisibility, Congruences, Quadratic residues and residuacity, Abstract Algebra – Groups, rings, fields, construction of finite fields, vector space, Galoise field cryptography- Notion and need for security proofs, Attack models, Perfect secrecy, Computational secrecy, One-time Pad (OTP), Pseudo-random generator (PRG), Pseudo-random function (PRF), design principles of stream and block ciphers, stream and block ciphers (DES, AES), Attacks on stream and block ciphers, Semantic security, Block cipher modes, Message Integrity – MAC and cryptographic hash function, NMAC, HMAC, Authenticated encryption.

One way function, Cryptographic hardness assumptions, Key exchange algorithms, Public key encryption algorithms (RSA, ElGamal, Rabin, ECC), Attacks on text book encryption algorithms, Semantically secure encryption algorithms, Security against chosen plain text and chosen cipher text attacks, Zero knowledge proofs, homomorphic encryption, Post quantum Cryptography.

Text Books/Reference Books/Online Resources:

1. N. Koblitz, *Number Theory and Cryptography*, Springer, 2001
2. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Third edition CRC press, 2020.
3. Wenbo Mao, *Modern Cryptography: Theory and Practice*, first edition, Pearson Education, 2004.
4. Menezes, et.al, *Handbook of Applied Cryptography*, CRC Press, 2004.
5. Golreich O, *Foundations of Cryptography*, Vol.1.2, Cambridge University Press, 2004.

Course Code: CS5203	Data Mining	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analyze and evaluate performance of algorithms for Association Rules
CO2	Analyze Classification and Clustering algorithms
CO3	Analyze Algorithms for sequential patterns.
CO4	Extract patterns from time series data.
CO5	Develop algorithms for Temporal Patterns.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	2	1	3	2	3
CO2	1	1	1	3	3	3
CO3	2	1	1	3	3	2
CO4	1		1	3	2	3
CO5	1	1	2	2	2	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Data Mining Techniques: Basic concepts of Association Rule Mining, Frequent Item set mining, Mining various kinds of association rules, Classification by decision tree induction, Bayesian Classification, Rule- based Classification, Classification Back-propagation, Associative Classification, Lazy Learners, Rough set approach, Clustering methods, Data Objects and Attribute Types, Basic Statistical Descriptions of Data, Measuring Data Similarity and Dissimilarity Partition based Clustering, Hierarchical based clustering, Density based clustering.

Sequential Pattern Mining concepts, primitives, scalable methods; Transactional Patterns and other temporal based frequent patterns, Mining Time series Data, Periodicity Analysis for time related sequence data, Trend analysis, Similarity search in Time-series analysis;

Text Books/Reference Books/Online Resources:

1. Jiawei Han and M Kamber, *Data Mining Concepts and Techniques*, Second Edition, Elsevier, 2011.
2. Vipin Kumar, Pang-Ning Tan, Michael Steinbach, *Introduction to Data Mining,* Addison Wesley, 2006.
3. G Dong and J Pei, *Sequence Data Mining*, Springer, 2007.

Course Code: CS5204	Computational Mathematics Practice	Credits 1-1-2: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Apply the concepts of Linear Algebra.
CO2	Use the Mathematical concepts to solve the given problem.
CO3	Apply the concepts of Probability and Distribution for a given problem.
CO4	Use the concepts of Discrete Mathematics for solving the given problem.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		2		1	1
CO2	2		1		1	1
CO3	2		1		1	1
CO4	2		2		1	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Mathematical Foundations: Introduction and Motivation.

Linear Algebra: System of linear equations, Matrices, Solving Systems of Linear Equations, Vector Spaces, Linear Independence, Basis and Rank, Linear Mappings.

Analytic Geometry: Norms, Inner Product, Lengths and Distances, Angles and Orthogonality, Orthonormal Basis, Orthogonal Complement, Fourier Transform.

Matrix Decomposition: Determinant and Trace, Eigen values and Eigen vectors, Eigen decomposition and Diagonalization, Single Value Decomposition, Matrix Approximation.

Vector Calculus: Differentiation of univariate functions, Partial Differentiation and Gradients, Gradients of vector-values functions, Gradients of Matrices.

Probability and Distribution: Construction of a Probability Space, Discrete and Continuous Probabilities, Sum Rule, Product Rule, Bayes Theorem, Summary Statistics and Independence.

Discrete Mathematics: Sets and Relations, Mathematical Logic and Induction, Elementary Combinatorics, Recurrence Relations, Lattices as Partially Ordered Sets, Graphs, Trees. Groups, Rings and Fields.

Laboratory:

Lab programs to understand and demonstrated the topics in

1. Problems related to Array, Stack, Queue, Linked Lists, Trees and Graphs.
2. Linear Algebra
3. Analytic Geometry
4. Matrix Decomposition
5. Vector Calculus
6. Probability and Distribution
7. Discrete Mathematics

Text Books/Reference Books/Online Resources:

1. Marc Peter Deisenroth, A. Aldo Faisal and Cheng Soon Ong, *Mathematics for Machine Learning*, Cambridge University Press, 2020. (for topics other than Discrete Mathematics)
2. Joe L. Mott, Abraham Kandel, Theodore P. Baker, *Discrete Mathematics for Computer Scientists and Mathematicians*, Second Edition, PHI, 2001.
3. J. P. Tremblay and R. Manohar, *Discrete Mathematical Structures with Applications to Computer Science*, MGH, 1997.
4. Kenneth H. Rosen, *Discrete Mathematics and its Applications with Combinatorics and Graph Theory*, Seventh Edition, MGH, 2011.

Course Code: CS5211	Computational Number Theory	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analyse large integer computations in Z_n
CO2	Analyse primality testing and integer factorization algorithms
CO3	Develop algorithms for computations in groups, rings and fields
CO4	Develop algorithms for computations in polynomial rings
CO5	Develop algorithms for computations in finite fields

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1			1	1	1
CO2	1			1	2	1
CO3	1		2	2	1	2
CO4	1		2	2	1	2
CO5	1		2	2	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Basic properties of the integers :Congruences, Computing with large integers, Computing in Zn, Euclid's algorithm. The distribution of primes, Finite and discrete probability distributions, Hash functions, Probabilistic algorithms. Abelian groups, Polynomial rings, Ideals and quotient rings, homomorphisms and isomorphisms, Probabilistic primality testing, Finding generators and discrete logarithms in Z_p , Finding a generator for Z_p, Quadratic residues and quadratic reciprocity, Computational problems related to quadratic residues. Modules and vector spaces; Matrices; Sub exponential-time discrete logarithms and factoring, Algebras, Unique factorization of polynomials, General properties of extension fields, Formal power series and Laurent series, Unique factorization domains, Polynomial arithmetic and applications, Linearly generated sequences and applications. Finite fields - Algorithms for finite fields, Testing and constructing irreducible polynomials, Computing minimal polynomials in F[X]/(f), Factoring polynomials: the Cantor–Zassenhaus algorithm, Factoring polynomials: Berlekamp's algorithm, Deterministic factorization algorithms, Faster square-free decomposition. Deterministic primality testing.

Text Books/Reference Books/Online Resources:

1. Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 2008
2. Henri Cohen, A*Course in Computation Algebraic Number Theory*, Springer-Verlag, 2000

Course Code: CS5212	Mathematical Models for Internet	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Illustrate TCP/IP protocol stack including IPv4 and IPv6
CO2	Analysis of network (Internet) Traffic using queuing disciplines
CO3	Analysis of congestion control algorithms by considering network throughput and delay
CO4	Design of routing algorithms for the Internet

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1			1		
CO2	1			1	1	1
CO3	1			1	1	2
CO4	2			1	2	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction to Internet and TCP/IP protocol stack, IPv4 and IPv6, Stochastic Processes (The Poisson process and Markov chains), Analysis of network (Internet) Traffic using queuing disciplines (M/M/1, M/M/1/C and M/M/C/C), Randomized algorithms and File sharing in the Internet, Networks and Graphs (including the internet graph and web graph), Analysis of Algorithms for Congestion Control, Performance Analysis of TCP Reno, TCP Tahoe and TCP Vegas, Linear Analysis with Delay: The single link case, Linear Analysis with Delay: The network case, Routing protocols for next generation Internet traffic, Mathematical models for Internet of Things.

Text Books/Reference Books/Online Resources:

1. FabrizioLuccio, Linda Pagli and Graham Steel, *Mathematical and Algorithm Foundations of the Internet*, Chaman and Hall, 2011
2. D. Bertsekas and R. Gallagar, *Data Networks*, PHI, 2nd Edition, 1992
3. RayadurgamSrikant, *The Mathematics of Internet congestion control (systems and control: foundations and applications)*, 1st Edition, Birkhauser, 2003.
4. S. M. Ross, *Stochastic Processes*, Wiley, 2nd Edition, 1996

Course Code: CS5213	Cryptanalysis	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analysis of vulnerabilities in an elliptic curve cryptography
CO2	Identify security vulnerabilities of different types of cryptosystems.
CO3	Analyze methods of attacking symmetric key cryptography
CO4	Analyze methods of public key cryptography
CO5	Development of secure cryptosystem.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		1	2		1
CO2	1		1	2		2
CO3	1		1	2		1
CO4	1		1	2		1
CO5	2		2	3	2	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Modern Cryptography Preliminaries - Defining security in cryptography, Number theory concepts Linear Algebra, Sieving methods, Tutorial, Introduction to symmetric key cryptography, Symmetric ciphers- triple DES, Modes of operation, Stream ciphers –RC4, Stream ciphers – Attacks, Linear analysis. Differential analysis, Tutorials, Introduction to public key cryptography, Public key cryptography and RSA. Key management and Distribution, Other public Key Cryptosystems, Attacks on RSA, Attacks on Diffie-Hellman Attacks on ElGamal. Introduction to Discrete Logarithm Problem. Shanks baby step and Gaint step algorithm, Pollard Rho, Pollard Kangaroo, Pohlig-Hellman. Introduction to index calculus method, Number Field Sieve method, Introduction to Elliptic Curve Cryptography, Generic algorithms to solve ECDLP, Anomalous attack, MOV attack.

Text Books/Reference Books/Online Resources:

1. Antoine Joux, *Algorithmic Cryptanalysis*, CRC Press, 2009
2. Gregory V. Bard, *Algebraic Cryptanalysis*, Springer, 2009.

Course Code: CS5214	Computability and Complexity	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand the limits of models of computation under the Church-Turing hypothesis.
CO2	Classify problems into appropriate complexity classes.
CO3	Identify the possibility of intractability for a given problem.
CO4	Apply the concept of interactive proofs in the analysis of optimization problems.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1			1		
CO2	1					1
CO3				1		1
CO4	1		1	2		1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Computability: Models of computation, The Church–Turing Thesis, Turing model of computation, Variants of Turing machines, Decidable, semi-decidable and undecidable problems, Post correspondence problem, Mapping reducibility, The recursion theorem, The Rice's theorem, Decidability of logical theories and Turing reducibility.
Complexity: Introduction to complexity theory, Nondeterminism and NP-completeness, Diagonalization, Relations between the standard complexity classes, The Cook–Levin theorem, Space complexity, Savitch's theorem, PSPACE, PSPACE-completeness ,Circuits, Randomized computation and complexity, Interactive proof systems, Complexity of counting, Parallel computation and complexity, Probabilistic complexity classes, Decision trees, Communication complexity , Circuit complexity, Probabilistically checkable proofs, Quantum computation and Logic in complexity theory.

Text Books/Reference Books/Online Resources:

1. Christos H. Papadimitriou, *Computational Complexity*, Addison-Wesley, 1994.
2. Michael Sipser, *Introduction to Theory of Computation*, Third edition, PWS Publishing Company, 2012.
3. Sanjeev Arora and Boaz Barak ,*Computational Complexity: A Modern Approach*, Cambridge University Press, 2010.

Course Code: CS5215	Information Systems Control and Auditing	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Ability to recognize the propensity of errors and remedies in processes involving Information Technology
CO2	A consummate knowledge of risks and controls in IT operations in Industry
CO3	An ability to provide protective IT security guidelines for various types of Industries
CO4	The necessary wherewithal to become an IS Auditor and/or Security specialist eventually
CO5	Evaluate asset safeguarding and data integrity, system effectiveness and system efficiency

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		2			2
CO2	1	1	1	1	1	1
CO3			1			1
CO4			2			
CO5			2			1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction: Overview of Information Systems Auditing. Conducting an Information Systems Audit. Management and the application Control Framework: Top Management Controls, Security Management Controls. Operations Management Controls. Quality Assurance Management Controls. Boundary Controls. Communication Controls.

Evidence Collection and Evidence evaluation: Audit Software. Concurrent Auditing Techniques. Interviews, Questionnaires, and Control Flowcharts. Evaluating Asset Safeguarding and Data Integrity. Evaluating System Effectiveness and System Efficiency. Managing the Information Systems Audit Function.

Practice study: CISA examination questions.

Text Books/Reference Books/Online Resources:

1. Ron Weber, *Information Systems Control and Audit*, Pearson Education, 1999
2. John B. Kramerk, *The CISA Prep Guide*, Wiley Publications, 2003
3. *Information Systems Control and Audit*, BOS, Institute of Chartered Accountants of India, New Delhi, 2013

Course Code: CS5216	Probabilistic Algorithms	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Design and analyze efficient randomized algorithms
CO2	Apply tail inequalities to bound error-probability
CO3	Analyze randomized algorithms with respect to probability of error and expected running time.
CO4	Apply probabilistic method to demonstrate existence of combinatorial objects
CO5	Apply to graph problems

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	1	1	2	1	2
CO2				1		
CO3	1			1	2	2
CO4	1	1	1	1	1	1
CO5	1	1	1		1	

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Las Vegas and Monte Carlo Algorithms, Computational Model and Complexity Classes, Game Tree Evaluation, The Markov and Chebyshev Inequalities, The Stable Marriage Problem, The Coupon Collectors Problem, The Chernoff Bound, Routing in a Parallel Computer, The Probabilistic Method: Overview, probabilistic analysis, use of indicator random variables, Randomly permuting arrays, Birthday paradox, analysis using indicator random variables, Balls and bins, Streaks, Online hiring problem, Maximum Satisfiability, Expanding Graphs, The Lovasz Local Lemma, Markov Chains, Random Walks on Graphs, Graph Connectivity, Expanders and Rapidly Mixing Random Walks, Pattern Matching, Random Traps, Skip Lists, Hash Tables, Linear Programming, The Min-Cut Problem, Minimum Spanning Trees, The DNF Counting Problem, The Online approximations paging Problem, Adversary Models and Paging against an Oblivious Adversary, Randomized number theoretic and algebraic algorithms

Text Books/Reference Books/Online Resources:

1. Rajeev Motwani, PrabhakarRaghavan, *Randomized Algorithms*, Cambridge University Press, 1995.
2. J. Hromkovic, *Design and Analysis of Randomized Algorithms*, Springer 2005.

Course Code: CS5217	Biometric Security	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes**:** At the end of the course the student will be able to:

CO1	Analyze biometric systems
CO2	Design basic biometric system applications.
CO3	Identify the acceptance issues associated with the design and implementation of biometric systems.
CO4	Identify various Biometric security issues.
CO5	Design biometric system to solve security issues.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1					3
CO2		1				2
CO3	1		1		2	
CO4	1			1		
CO5					1	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Biometric Fundamentals And Standards : Biometrics versus traditional techniques, bio metric in identification system biometric processes: Biometric matching methods, Performance measures in biometric systems, Assessing the privacy risks of biometrics - Designing privacy sympathetic biometric systems, Different biometric standards. Physiological Biometrics: Facial scan, finger print, Ear scan, Retina vascular pattern-

Behavioral Biometrics: Hand print biometrics-DNA biometrics- Signature scan, Keystroke scan, Voice scan, Gait recognition, Gesture recognition, User Interfaces: Biometric interfaces: Human machine interface - BHMI structure, Human side interface: Iris image interface -Hand geometry and fingerprint sensor, Machine side interface: Parallel port - Serial port - Network topologies, Case study: Palm Scanner interface. Biometric Applications: Categorizing biometric applications, application areas - E-commerce and retail/ATM, Issues

in deployment, Biometrics in medicine. Biometric Privacy- Assessing the privacy risks of biometrics - Designing privacy sympathetic biometric systems,

Text Books/Reference Books/Online Resources:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, *Biometrics -Identity verification in a network*, 1stEdition, Wiley Eastern, 2002.
2. John Chirillo, Scott Blaul, *Implementing Biometric Security*, 1st Edition, Wiley Eastern Publication, 2005.
3. Anil K Jain, Patrick Flynn and Arun A Ross, *Handbook of Biometrics*, Springer,USA,2010.
4. John R Vacca, *Biometric Technologies and Verification Systems*, Elsevier, USA, 2007.
5. Samir Nanavati, Michael Thieme and Raj Nanavati, *Biometrics – Identity Verification in a Networked World*, John wiley& Sons, New Delhi, 2003.
6. Paul Reid, *Biometrics for Network Security*, Pearson Education, New Delhi, 2004.
7. David D Zhang, *Automated Biometrics: Technologies and Systems*, Kluwer Academic Publishers, New Delhi, 2000.

Course Code: CS5218	Unix Internals	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Design and implement Unix kernel data structures and algorithms
CO2	Analyze synchronization problems in uniprocessor and multiprocessor systems
CO3	Evaluate the scheduling requirements of different types of processes and find their solutions
CO4	Implement user level thread library and mimic the behavior of Unix kernel for scheduling, synchronization and signals.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		1	1	3	
CO2				2	3	1
CO3				2	3	1
CO4	1		2	2	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction to UNIX, The process and the kernel, Mode, space and context, Process abstraction, executing in kernel mode, synchronization by blocking interrupts, process scheduling. Introduction to Threads: Fundamental abstractions, Lightweight process design, issues to consider, User level thread libraries, scheduler activations, Multi-threading on Solaris, Pthreads library, Thread library implementation Using ucontext_t structures. Signals: Signal generation and handling, Unreliable signals, Reliable signals, Signals in SVR4, Signals implementation, Exceptions, Process Groups. Process Scheduling: Clock interrupt handling, Scheduler Goals, Traditional UNIX scheduling, Scheduling case studies. Synchronization and Multiprocessing: Introduction, Synchronization in Traditional UNIX Kernels, Multiprocessor Systems, Multiprocessor synchronization issues, Semaphores, spin locks, condition variables Read-write locks for multiprocessor systems, Reference counts and other considerations. Kernel Memory Allocators: Resource map allocator, Simple power-of-two allocator, McCusick-Karels Allocator, Buddy system, SVR4 Lazy Buddy allocator, OSF/1 Zone Allocator, Hierarchical Allocator, Solaris Slab Allocator. File system interface

and framework: The user interface to files, File systems, Special files, File system framework, The Vnode/Vfs architecture, Implementation Overview, File System dependent objects, Mounting a file system, Operations on files. File System Implementations : System V file system (s5fs) implementation, Berkeley FFS, FFS functionality enhancements and analysis, Temporary file systems, Buffer cache and other special-purpose file systems.

Text Books/Reference Books/Online Resources:

1. UreshVahalia, *UNIX Internals*, Pearson Education, 2005.
2. Richard Stevens, Stephen Rago, *Advanced Programming in the UNIX Environment*, Pearson Education, 2/e, 2005

Course Code: CS5219	Secure Software Engineering	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Evaluate secure software engineering problems, including the specification, design, implementation, and testing of software systems.
CO2	Elicit, analyze and specify security requirements through SRS
CO3	Design and Plan software solutions to security problems using various paradigms
CO4	Model the secure software systems using Unified Modeling Language Sec(UMLSec)
CO5	Develop and apply testing strategies for Secure software applications

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		2	1		2
CO2	2	2	1	1		2
CO3	2		2	1		2
CO4	1	1	1	1		1
CO5	2		2	1		2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

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, how to influence the security properties of software, how to assert and specify desired security properties, Secure software Architecture and Design: Software security practices for architecture and design: Architectural risk analysis, software security knowledge for Architecture and Design: security principles, security guidelines, and attack patterns, secure design through threat modeling, Writing secure software code: Secure coding techniques, Secure Programming: Data validation, Secure Programming: Using Cryptography Securely, Creating a Software Security Programs. Secure Coding and Testing: code analysis- source code review, coding practices, static analysis, software security testing, security testing consideration through SDLC

Text Books/Reference Books/Online Resources:

1. Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead, *Software Security Engineering: A Guide for Project Managers*, Addison Wesley, 2008
2. Ross J Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition, Wiley, 2008.
3. Howard, M. and LeBlanc, D., *Writing Secure Code*, 2nd Edition, Microsoft Press, 2003.

Course Code: CS5220	Secure Cloud Computing	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analyze the security and privacy issues in the cloud computing.
CO2	Understand the auditing and compliance process.
CO3	Build security as a cloud service for secure cloud computing.
CO4	Implement various case studies.
CO1	Analyze the security and privacy issues in the cloud computing.

Course Articulation Matrix:

Course Outcomes	PO 1	PO2	PO3	PO4	PO5	PO6
CO1	1		1	2	2	1
CO2	1			1	2	2
CO3			1	2	2	2
CO4				2	1	2
CO5			1	1	1	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Cloud Computing Defined, SPI Framework, Traditional Software Model, Cloud Services Delivery Model, Cloud Deployment Models, Key Drives to Adopting the Cloud, Impact of Cloud Computing on Users, Governance in the Cloud, Barriers to Cloud Computing Adoption in the Enterprise, Infrastructure Security: The Network Level, The Host Level, The Application Level, Data Security and Storage, Identity and Access Management, Security Management on the Cloud, Privacy, Audit and Compliance, Cloud Service Providers, Security as a Cloud Service, Impact of Cloud Computing on the Role of Corporate IT, The Future of the Cloud, Case Studies.

Text Books/Reference Books/Online Resources:

1. Tim Mather, Subra Kumaraswamy and Shahed Latif, *Cloud Security and Privacy*, First Edition, O'Reilly, 2009.
2. Simon Gallagher and Aidan Dalgleish, VMware Private Cloud Computing with vCloud Director, SYBEX, A Wiley Brand, 2013.

Course Code: CS5221	Algorithmic Game Theory	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analyze games based on complete and incomplete information about the players
CO2	Analyze games where players cooperate
CO3	Compute Nash equilibrium
CO4	Apply game theory to model network traffic
CO5	Analyze auctions using game theory

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		2	1	1	1
CO2	1		2	1	1	1
CO3	1			1		1
CO4	1		2	2	1	2
CO5	1		1	1	1	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Noncooperative Game Theory: Games in Normal Form - Preferences and utility, examples of normal-form, Analyzing games: Pareto optimality, Nash equilibrium, Maxmin and minmax strategies, dominated strategies, Rationalizability, Correlated equilibrium; Computing Solution Concepts of Normal-Form Games: Computing Nash equilibria of two-player, zero-sum games, Computing Nash equilibria of two-player, general-sum games, Complexity of computing Nash equilibrium, Lemke–Howson algorithm, Searching the space of supports, Computing Nash equilibria of n-player, general-sum games, Computing maxmin and minmax strategies for two-player, general-sum games, Computing correlated equilibria; Games with the Extensive Form: Perfect-information extensive-form games, Subgame-perfect equilibrium, Computing equilibria, Imperfect-information extensive-form games, Sequential equilibrium; Other Representations: Repeated games: Finitely repeated games, Infinitely repeated games, automata, Stochastic games. Bayesian games: Computing equilibria; Coalitional Game Theory: Transferable Utility, Analyzing Coalitional Games, The Shapley Value, The Core; Mechanism Design: strategic voting, unrestricted preferences,

Implementation, quasilinear setting, Efficient mechanisms, Computational applications of mechanism design, Task scheduling, Bandwidth allocation in computer networks; Auctions: Single-good auctions, Canonical auction families, Bayesian mechanisms, Multiunit auctions, Combinatorial auctions.

Text Books/Reference Books/Online Resources:

1. Noam Nisan, Tim Roughgarden, Eva Tardos, Vijay V. Vazirani, *Algorithmic Game Theory*, Cambridge University Press, 2007.
2. Ronald Cohn Jesse Russell, *Algorithmic Game Theory*, VSD Publishers, 2012.

Course Code: CS5222	Digital Video Processing	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Use the suitable image/video acquisition approach, representation and quality assessment for a given scenario.
CO2	Apply image/video processing operations for enhancement and restoration.
CO3	Understand image/video compression standards
CO4	Solve a video indexing, summarization, browsing and retrieval problem
CO5	Implement an approach to solve a video analytics problem

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	2	1			
CO2	2	2				
CO3	-	2	1			
CO4	3	2	1			1
CO5	3	2	1		1	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction – Introduction to digital image and video processing.

Image/Video processing – Intensity transformations, Applications of linear filtering and non-linear filtering. Morphological operations. Colour image processing. Features for Image and Video processing. Geometric transforms and Image registrations, Image segmentation and analysis. Spatiotemporal noise filtering, coding artifact reduction, Blotch detection and removal, video stabilization, and recent image/video operations and features in contemporary literature.

Image Compression – lossless coding, block transform coding, fundamentals of vector quantization, wavelet image compression, JPEG image compression.

Video Compression – basic concepts and techniques of video coding and the H.261 Standard, spatiotemporal subband/Wavelet Video Compression, Object-based video coding, introduction to video coding standards and formats: H.261, MPEG-2/DVB, MPEG-4, H.264/AVC, H.265/HEVC, H.266/VVC.

Image and Video Acquisition – Image scanning, sampling and interpolation, video sampling and interpolation. Recent standards and practices in image and video acquisition.
Video Quality Assessment – Introduction, HVS Modelling based methods, feature based methods, motion modelling-based methods, and approaches based on contemporary research.
Indexing, Summarization, Browsing and Retrieval – Introduction, Image and Video features, Video analysis, video representation, video browsing and video retrieval. Video features in contemporary research.
Video Analytics – Review of video analytics algorithms for: motion and change detection, object detection, object tracking, behaviour analysis, face recognition, Image and Video classification and recent visual analytics approaches in contemporary research.

Text Books/Reference Books/Online Resources:

1. Alan C Bovik, *Handbook of Image and Video Processing*, 2nd Edition, Academic Press, 2005.
2. Alan C. Bovik, *The Essential Guide to Video Processing,* 1st Edition, Academic Press, 2009.
3. Rafael C. Gonzalez, Richard E. Woods, *Digital Image Processing*, 4th Edition, Pearson, 2018.
4. Recent articles in Research and Industry.

Course Code: CS5223	Information Security and Secure Coding	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course, the student will be able to:

CO1	Analyse and understand secure design
CO2	Analyse and apply authentication and authorization principles
CO3	Design secure application
CO4	Writing secure software

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	2	2	3	3	3
CO2	1	1	3	2	2	2
CO3	3	2	2	3	3	3
CO4	1	3	1	1	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Information Security Basics: Introduction to Information Security – Risk Analysis – Legal Issues – Secure Design – Policy, Standards, Procedures and Guidelines – Security Organization structure.

Information Security Policy and Compliance: Authentication and Authorization principles - Securing unstructured data – Information Rights Management – Storage security – Data base security.

Secure Application: Secure application design – Writing Secure Software – J2EE vulnerabilities

Secure Infrastructure Management: Security Operations Management – Disaster Recovery and Backups – Physical Security.

Text Books/Reference Books/Online Resources:

1. Information Security – The complete reference; Chapters: 1-9, 11-12, 26-28, 31, 32, and 34 Author: Mark Rhodes – Ousley; McGraw Hill, 2013;ISBN Number: 978-0-07-178436-8

Course Code: CS5224	Scripting languages for information security	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course, the student will be able to

CO1	Understand, analyze and build dynamic, interactive and secure web sites
CO2	Understand current and evolving Web languages for integrating media and user interaction in both front end and back end elements of a Web site
CO3	Analysis and reporting of web data and minimizing cyber risks
CO4	Applying different testing and debugging techniques and analyzing the web site effectiveness.
CO5	Applying different cyber security tools and scripting languages to mitigate frequent cyber attacks.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	-	-	2	1	2	1
CO2	1	1	-	-	2	-
CO3	2	-	2	1	3	1
CO4	1	3	-	1	2	3
CO5	2	1	1	-	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

HTML: Introduction to HTML, What is HTML, HTML Documents, Basic structure of an HTML document, Creating an HTML document, Mark up Tags, Heading-Paragraphs, Line Breaks, HTML Tags. Elements of HTML: Introduction to elements of HTML, Working with Text, Working with Lists, Tables and Frames, Working with Hyperlinks, Images and Multimedia, Working with Forms and controls.

Java Script: Introduction to JavaScript, Basic Syntax, Control Structures, Writing Functions, Working with Arrays, The Document Object Model, Events Handling, Client-side Validation, Form Validation & RegExps, ASP, Perl CGI, & Form Methods, SSI & Cookies, Frames & Windows, mimeTypes, plugins, & Java

PHP: PHP installation and Introduction, Loops String Functions in PHP, PHP Email Function, PHP Basics, Variables Arrays in PHP with Attributes Date & Time, Image, Uploading File handling in PHP Functions in PHP, Errors handling in PHP.

Python: Introduction to Python, Python basics, Data Types and variables Operators, Looping & Control Structure List, Modules Dictionaries, String Regular Expressions, Functions and Functional Programming, Object Oriented Linux Scripting Environment – Classes, Objects and OOPS concepts, File and Directory Access, Permissions and Controls Socket, Libraries and Functionality Programming, Servers and Clients Web Servers and Client scripting, Exploit Development techniques, Writing plugins in Python, Exploit analysis, Automation Process, Debugging basics, Task Automation with Python

Perl & NodeJS: Introduction to Perl – Overview of Perl Features, Getting and Installing Perl, Accessing Documentation via perldoc, HTML-Format Reference Documentation, Perl Strengths and Limitations, Security Issues in Perl Scripts. Introduction to Node.js; Events; Streams; Modules; Express; Socket.io; Persisting Data

Text Books/Reference Books/Online Resources:

1. Deitel, Deitel and Nieto, Internet and Worldwide Web - How to Program, 5th Edition, PHI, 2011.
2. Bai and Ekedhi, The Web Warrior Guide to Web Programming, 3rd Edition, Thomson, 2008.
3. Computer Programming And Cyber Security for Beginners: Zack Codings (Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking)

Course Code: CS5225	Wireless and Mobile Networks	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Identify issues related to environment, communication, protocols in wireless and mobile networks
CO2	Understand the functionalities of cellular networks and analyze the methods to improve capacity and coverage.
CO3	Analyze the performance of MAC protocols for wireless and mobile networks.
CO4	Evaluate the performance of different routing protocols
CO5	Analyze QoS and energy efficiency issues in resource constrained wireless and mobile environment.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		2	2	2	
CO2	2		3	2	2	
CO3	2		3	2		
CO4	2		3	2	2	
CO5	2		2	2	2	

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction to Mobile Networks, Wireless Communication Fundamentals, Multi-hop Communication, Impact of mobility.

Cellular networks: Introduction, Frequency Reuse, Channel Assignment Straggles, Handoff Strategy, Inference and system capacity, Improving coverage and capacity.

Medium Access Control: MACA, MACAW, Wireless LAN.

Wireless Sensor Networks (WSN) MAC Protocols: Issues in designing MAC protocols for adhoc wireless networks, design goals, classification of MAC protocols, MAC protocols for sensor network, location discovery, S-MAC, IEEE 802.15.4.

Routing in Mobile Ad hoc Networks (MANET): Ad-hoc On-Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing (DSR), Secure routing protocols in MANET.

WSN Routing Protocols: Issues in designing a routing protocol, classification of routing protocols, table-driven, on-demand, hybrid, flooding, hierarchical, and power aware routing protocols, WSN Localization methods, Sensor Deployment Strategies, QoS and Energy Management, Underwater sensor networks communication .

5G Architecture: Software Defined Networking – Network Function Virtualization – Basics about RAN Architecture –High-Level Requirements for 5G Architecture – Functional Architecture and 5G Flexibility

Text Books/Reference Books/Online Resources:

1. Jochen Schiller, "Mobile Communications", Pearson Education, 2nd Edition, 2003.
2. Ian F.Akyildiz and Mehmet Can Vuran, "Wireless sensor networks ", Wiley Publication.
3. Jonathan Rodriquez, “Fundamentals of 5G Mobile Networks”, Wiley, 2015
4. Feng Zhao and Leonides Guibas, "Wireless sensor networks ", Elsevier publication - 2004.
5. C. Siva Ram Murthy, and B. S. Manoj, "AdHoc Wireless networks ", Pearson Education - 2008.
6. Asif Oseiran, Jose F.Monserrat and Patrick Marsch, “5G Mobile and Wireless Communications Technology”, Cambridge University Press, 2016.

Course Code: CS5205	Cryptography Laboratory	Credits 0-1-2: 2

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Implement and analyze the number theoretic algorithms.
CO2	Assess attacks including brute force attacks on symmetric key encryption protocols
CO3	Implement number theoretic algorithms using multi-precision integer package.
CO4	Implement Public Key Cryptosystems and analyze their security.
CO5	Implementation of Elliptic Curve Cryptosystem

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		1			
CO2	3		2	1	1	1
CO3	1		1			
CO4	2		2	3	3	2
CO5	2		1	3	2	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Programming Assignment Set 1:

a. Euclidean and Extended Euclidean algorithm for finding the Greatest Common Divisor of two large integers. Computing the Multiplicative inverses in Z_n.
b. Repeated square and multiply algorithm for modular exponentiation in Z_n.
c. Determining the order of a group element. Finding a generator of a cyclic group.
d. Chinese remainder theorem.
e. Computation of Legendre symbol and Jacobi symbol
f. Modular polynomial arithmetic
g. RSA public key algorithm
h. ElGamal Cryptosystem
i. Rabin cryptosystem
j. Diffie-Hellman Key exchange protocol.

Programming Assignment Set II:

a. Pollard's rho algorithm for factoring integers.
b. Pollard's p-1 algorithm for factoring integers.
c. Fermat's factorization method
d. Congruence of squares. Finding a congruence of squares modulo n to factor n.
e. Construction of Finite Field of characteristic 2.
f. Computations in elliptic curve over a finite field.

Programming Assignment Set III:

a. Sieve of Eratosthenes
b. Fermat primality test
c. Solovay-Strassen probabilistic primality test
d. Miller-Rabin probabilistic primality test
e. Lucas-Lehmer primality test

Instructions:

1. C/C++ Programming Language under Linux Operating System
2. gmp-man-6.1.2.pdf (Refer GMP library manual)
3. Code should be well modularised and documented
4. Use the standard coding style

Text Books/Reference Books/Online Resources:

1. Menezes, P.C. van Oorschot, S.A. Vanstone: *Handbook of Applied Cryptography*: CRC Press, 1996.
2. Abhijit Das and C.E.VeniMadhavan, *Public-key Cryptography: Theory and Practice*, Pearson, 2009.
3. Darrel Hankerson, Alfred Menezes, Scott Vanstone,*Guide to Elliptic Curve Cryptography*, Springer- Verlag, 2004.

Course Code: CS5206	Web & Database Security Laboratory	Credits 0-1-2: 2

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Design of access control methods for secure web & database application development
CO2	Analyse and Classify the vulnerabilities in the Web and Database applications.
CO3	Design & implementation various methods for web & database intrusion detection
CO4	Design and Implementation security audit methods

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	1	1	2		1
CO2	1	1	2	1		1
CO3	1	1	1		1	1
CO4	1	1		1		2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

1. Creation and manipulation of database using SQL scripts and graphical interfaces.
2. Implementing DAC: Implementation of database security policies using DAC in oracle 10g/SQL server
3. Implementing of MAC to ensure confidentiality and control information flow using either Oracle 10g or SQL server. This provides exposure to understand the concepts of MAC and Trojan hose
4. Implementation of Virtual Private Database using View using Oracle 10g or SQL server
5. Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers.
6. Determine HTML injection bugs and possible measures to prevent HTML injection exploits.
7. Implement Secure coding for buffer flow heap attacks.
8. Implementation of Design methods to break authentication schemes
9. Implementation of methods for abusing Design Deficiencies against web sites

Text Books/Reference Books/Online Resources:

1. Mike Shema, *Hacking Web Apps Detecting and Preventing Web Application Security Problems*, Syngress publications- Elsevier, 2012
2. M. Gertz, S. Jajodia, *Handbook of Database Security*, Springer, 2008
3. Ben-Natan, R. B, *Implementing Database Security and Auditing: Includes Examples for Oracle, SQL Server,Db2Udb, Sybase*, Digital Press, 2005.

Course Code: CS5248	SEMINAR-I	Credits 0-0-2: 1

Pre-Requisites: None

Course Outcomes:

At the end of the course, the student will be able to

CO1	Analyze the selected topic, organize the content and communication to audience in an effective manner
CO2	Practice the learning by self study

Course Articulation Matrix:

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
CO1	2	3	1	1		
CO2	2	3	1	1		

1 - Slightly; 2 - Moderately; 3 – Substantially

Course Code: CS5251	Network Security	Credits 3-0-0: 3

Pre-requisites: Foundations of Cryptography

Course Outcomes: At the end of the course the student will be able to:

CO1	Design adversary models and protocols
CO2	Design of secure communication protocols in Internet applications.
CO3	Analyze cryptographic algorithms
CO4	Identify security threats in Mobile Applications.
CO5	Design of secure protocols for wireless ad-hoc and sensor networks.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1			1	2		2
CO2			2	3		
CO3				2		3
CO4	2			2		2
CO5				3		2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Cryptographic algorithms, Pseudorandom Generators, Hash functions, Block ciphers, Stream Ciphers, Access Control Methods, Message Authentication and Digital Signatures, Design of secure Internet protocols, Key distributions, Design of Access control methods, Network Anomaly Detection methods, Mobile IPv6, https protocol, Design of Firewalls and Intrusion Detection Systems, Malware detection methods, Mobile application security models, Mobile threats and malware, Trust based protocols, Mobile app security, Vulnerabilities and Security Challenges in Wireless networks, Trust Assumptions, Adversary models and Protocols, Attacks against naming and addressing in the Internet, Security protocols for address resolution and address auto configuration, IP Security (IP Sec) protocol, Key Establishment and Revocation Protocols, Secure Neighbor Discovery, Secure routing protocols in multi-hop wireless networks, Provable Security for Ad-hoc Network routing protocols, Privacy preserving routing in Ad-hoc Networks, Location privacy in vehicular Ad-hoc networks.

Text Books/Reference Books/Online Resources:

1. John R. Vacca, *Computer and Information Security Handbook, Elsevier, 2009*
2. L. Buttyan, J. P. Hubaux, *Security and Cooperation in Wireless Networks,* Cambridge University Press*, 2008.*
3. *W. Trappe,* L. C. Washington, *Introduction to Cryptography with Coding Theory,* Prentice-Hall 2005
4. NoureddineBoudriga, *Security of Mobile Communications,* Auerbach Publications, Taylor and Francis Group, 2010.

Course Code: CS5252	Data Privacy	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Define differential privacy
CO2	Design techniques to achieve differential privacy for linear queries.
CO3	Design mechanisms for query release problem using online learning algorithms.
CO4	Analyze computational complexity of differentially private mechanisms

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	2	2	2	2	2
CO2	1	3	3	3	3	3
CO3	1	2	3	3	3	3
CO4	1	3	3	3	3	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

The Promise of Differential Privacy: Privacy-preserving data analysis; Basic Terms: The model of computation, Towards defining private data analysis, Formalizing differential privacy; Basic Techniques and Composition Theorems: Useful probabilistic tools, Randomized response, The laplace mechanism, The exponential mechanism, Composition theorems, The sparse vector technique; Releasing Linear Queries with Correlated Error: An offline algorithm: SmallDB, An online mechanism: private multiplicative weights; Generalizations: Mechanisms via α-nets, The iterative construction mechanism, Connections; Boosting for Queries: The boosting for queries algorithm, Base synopsis generators; When Worst-Case Sensitivity is Atypical: Subsample and aggregate, Propose-test-Release, Stability and privacy; Lower Bounds and Separation Results: Reconstruction attacks, Lower bounds for differential privacy; Differential Privacy and Computational Complexity: Polynomial time curators, Some hard-to-Syntheticize distributions, Polynomial time adversaries; Differential Privacy and Mechanism Design: Differential privacy as a solution concept, Differential privacy as a tool in mechanism design, Mechanism design for privacy aware agents; Differential Privacy and Machine Learning: The sample complexity of

differentially private machine learning, Differentially private online learning, Empirical risk minimization; Additional Models: The local model, Pan-private streaming model, Continual observation, Average case error for query release.

Text Books/Reference Books/Online Resources:

1. C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*, now Publishers, 2014.
2. Charu C. Aggarwal, *Privacy-Preserving Data Mining: Models and Algorithms*, 1st Edition, Springer, 2008.
3. Relevant Research Papers

Course Code: CS5152	Deep Learning	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Identify Convolutional Neural Networks models to solve Supervised Learning Problems
CO2	Design Autoencoders to solve Unsupervised Learning problems
CO3	Use BiLSTM Networks for time series analysis classification problems.
CO4	Apply Classical Supervised Tasks for Image Denoising, Segmentation and Object detection problems.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	3	2	1	2	1	2
CO2	2	1	2	2	3	1
CO3	2	1	2	2	3	3
CO4	1	2	3	2	3	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction to Biological Neurons, Artificial Neural Networks, McCulloch Pitts Neuron, Learning processes, Perceptron, Perceptron convergence theorem, XOR problem, Multilayer perceptron, Back Propagation Learning, Activation functions, loss functions, Radial Basis Functions. Introduction to Self Organizing Maps; Optimizers: Gradient Descent (GD), Batch Optimization, Momentum Based GD, Stochastic GD, AdaGrad, RMSProp, Adam; Sequence to sequence models, LSTM, BiLSTM, BERT, SciBERT, BioBERT for NLP Applications; Convolutional Neural Network, Building blocks of CNN, Transfer Learning; Regularization: Bias Variance Tradeoff, L2 regularization, Early stopping, Dataset augmentation, Parameter sharing and tying, Dropout; Autoencoders : Unsupervised Learning with Deep Network, Autoencoders, Stacked, Sparse, Denoising Autoencoders, Variational Autoencoders; Recent Trends in Deep Learning Architectures, Residual Network, Skip Connection Network, DensenNet, InceptionNets, SqueezNet, MobileNet, NasNet, HRnet Models; Classical Supervised Tasks with Deep Learning, Segmentation: ResUnet, SegNet, Mask RCNN models, Object Localization: FastRCNN, Faster RCNN, SSD with Applications; Attention Mechanism, Attention Models in Vision; Image Captioning, Visual QA, Visual Dialog, Transformer, Generative Adversarial Network on Image, CycleGANs, Progressive GANs, StackGANs, Unet GAN, vision and NLP Applications.

Text Books/Reference Books/Online Resources:

1. Deep Learning- Ian Goodfelllow, Yoshua Benjio, Aaron Courville, The MIT Press.
2. Christopher Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.
3. Simon Haykin, “Neural Networks, A Comprehensive Foundation”, 2nd Edition, Addison Wesley Longman, 2001.

Course Code: CS5261	Foundations of Block Chain Technology	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand how blockchain work, including private and public platforms
CO2	Understand the technical underpinnings of blockchain technology at sufficient depth to perform analysis.
CO3	Apply various blockchain concepts to analyse examples, proposals, case studies, and preliminary blockchain system design discussions.
CO4	Know and be able to apply the concepts, tools, and frameworks for building blockchain decentralized applications.
CO5	Design secure smart contract applications on blockchain.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	2	2	2	2	2
CO2	1	3	3	3	3	3
CO3	1	2	3	3	3	3
CO4	1	3	3	3	3	2
CO5	3	2	3	3	3	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Blockchain technology Introduction, Concepts of Blockchain Systems, Key Problem Challenges and Solutions, Bitcoin Concept- Merkle Tree - hardness of mining - transaction verifiability - anonymity, Attacks on Bitcoin- Double-spend attacks, Selfish mining, Security of Transactions in Bitcoin, Privacy in Bitcoin, Cryptographic Primitives in Blockchain- Cryptosystems in practice, Cryptographic Hash Functions, Digital Signatures-Aggregate Signature, Threshold Signature Blockchain Platforms - Blockchain-Ethereum, Smart Contracts - Attacks on smart contracts, Permissioned Blockchain – Hyperledger, Blockchain Applications & Use Cases, Consensus Protocols- The consensus problem- Byzantine Generals problem, Asynchronous Byzantine Agreement, Consensus mechanisms used in Bitcoin Blockchain, Ethereum Blockchain and Hyperledger Blockchain, Blockchain (BoT)-

Advantages of integrating Blockchain to IoT, Trust Building, Cost Reduction, Accelerate Data Exchanges, Scaled Security for IoT,

Text Books/Reference Books/Online Resources:

1. Arvind Narayanan, “Bitcoin and Cryptocurrency Technologies- A Comprehensive Introduction”, Princeton University Press, 2016.
2. William Magnuson, “Blockchain Democracy- Technology, Law and the Rule of the Crowd”, Cambridge University Press, 2020.
3. Pethuru Raj, Kavita Saini, Chellammal Surianarayanan, “Blockchain Technology and Applications”, CRC Press, 2021.
4. Chandramouli Subramanian, “Blockchain Technology”, Universities Press, 2020.
5. Relevant Research Paper and While Papers.

Course Code: CS5262	Secure Operating Systems	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analyze for the vulnerabilities in a given system.
CO2	Evaluate Information flow secrecy models, integrity models and trust models
CO3	Identify the system level security features incorporated in Multics, SELinux, Solaris etc.
CO4	Assess the security parameters of secure capability systems and secure virtual machines

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	3	1	3	1	3	1
CO2	1	1	1	1	2	3
CO3	1	1	1	3	1	1
CO4	1	1	1	2	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction: Security Goals, Trust Model, Threat Model; Access Control Fundamentals: Protection System, Reference Monitor, Secure Operating System Definition, Assessment Criteria; Multics: Multics History, Multics Security Fundamentals, Multics Protection System Models, Multics Security, Multics Vulnerability Analysis; Security in Ordinary Operating Systems: UNIX Security, UNIX Protection System, UNIX Authorization, UNIX Security Analysis, UNIX Vulnerabilities, Windows Security, Windows Protection System, Windows Authorization, Windows Security Analysis, Windows Vulnerabilities; Verifiable Security Goals: Information Flow, Information Flow Secrecy Models, Denning's Lattice Model, Bell-LaPadula Model, Information Flow Integrity Models, Biba Integrity Model, Low-Water Mark Integrity, Clark-Wilson Integrity, The Challenge of Trusted Processes, Covert Channels, Channel Types, Noninterference; Building a Secure Operating System for Linux: Linux Security Modules, LSM History, LSM Implementation, Security-Enhanced Linux, SELinux Reference Monitor, SELinux Protection State, ELinux Labeling State, SELinux Transition State, SELinux Administration, SELinux Trusted Programs, SELinux Security Evaluation;

Secure Capability Systems: Capability System Fundamentals, Capability Security, Challenges in Secure Capability Systems, Building Secure Capability Systems; Secure Virtual Machine Systems: Separation Kernels, VAX VMM Security Kernel, Security in Other Virtual Machine Systems

Text Books/Reference Books/Online Resources:

1. Trent Jaeger, *Operating System Security*, Morgan & Claypool, 2008
2. P.G Neumann (PI), *A Provably Secure Operating System*, Final Report published by Stanford Research Institute, California, US., 1975
3. Morrie Gasser, *Building A Secure Computer System*, Van Nostrand Reinhold, 1988
4. Michael Palmer, *Operating Systems Security*, Thomaon Course Technology, 2004

Course Code: CS5263	Design of Secure Protocols	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Design adversary models and protocols
CO2	Analyze Secure protocols for global IP mobility
CO3	Develop cryptographic algorithms
CO4	Identify security threats in Advanced Wireless networks.
CO5	Design secure routing protocols in wireless ad-hoc networks.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		2	2		2
CO2		1	1	1		2
CO3	1		1	2	2	3
CO4	1		2	2	1	2
CO5	2	1	2	2	2	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

One-Way Functions, Pseudorandom Generators, Hash functions, Block ciphers, Stream Ciphers, Access Control Methods, Message Authentication and Digital Signatures, Vulnerabilities and Security Challenges of Wireless networks, Trust Assumptions, Adversary models and Protocols, Attacks against naming and addressing in the Internet, Security protocols for address resolution and address auto configuration, Security for global IP mobility, IP Security (IP Sec) protocol, Key Establishment and Revocation Protocols in Sensor Networks, Secure Neighbor Discovery, Secure routing protocols in multi-hop wireless networks, Provable Security for Ad-hoc Network routing protocols, Privacy preserving routing in Ad-hoc Networks, Location privacy in vehicular Ad-hoc networks, Secure protocols for behavior enforcement Game theoretic model of packet forwarding

Text Books/Reference Books/Online Resources:

1. L. Buttyan, J. P. Hubaux, “Security and Cooperation in Wireless Networks”, Cambridge University Press, 2008.
2. O. Goldrich, “Foundation of Cryptography-Vol. 1 and Vol. 2”, Cambridge University Press, 2001.
3. James Kempf, —Wireless Internet Security: Architecture and Protocols‖, Cambridge University Press, 2008.

Course Code: CS5264	Secure Multiparty Computation	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analyze models of secure computation
CO2	Analyse secure computation with semi-honest security
CO3	Analyse secure computation with Active security
CO4	Construct Broadcast&Byzantine Agreement Protocols
CO5	Apply to Secure Set Intersection, Privacy Preserving Biometrics & Genomics, Secure Cloud Computing

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		1	1	2	2
CO2	1		1	1	2	2
CO3	1		1	1	2	2
CO4	2	1	2	3	2	2
CO5	1	1	2	2	3	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Models of Secure Computation, Defining Secure Computation: Computational/statistical Indistinguishability, Real-Ideal World or Simulation-based Security notions. Secure computation with semi-honest security: Honest-majority Setting: Secret Sharing, BenOr-Goldwasser-Wigderson (BGW) Construction, Optimizations (MPC in preprocessing mode and circuit randomization), Cramer-Damgaard-Neilsen (CDN) Construction. Dishonest majority Setting: Oblivious Transfers (OT), two-party Goldreich-Micali-Wigderson (GMW) construction, Optimizations of GMW (Random input OT and OT extension), Yao construction, BMR construction and multi-party GMW construction. Secure computation with Active security: Honest Majority Setting. Verifiable Secret Sharing, BGW Construction with active security, Hyper-invertible Matrices and Beerliova-Hirt (BH) Construction, Information Checking Protocol. Dishonest majority Setting: Commitment Schemes, Zero-knowledge, GMW Compiler for active corruption, Cut-and-Choose OT and Lindell-Pinkas Construction.

Broadcast & Byzantine Agreement (BA): Impossibility results. Dolev-Strong (DS) Broadcast, Exponential Information Gathering (EIG) construction for BA, Berman-Garay-Perry (BGP) construction for BA. Multi-valued Broadcast and BA. Secure Set Intersection, Privacy Preserving Biometrics & Genomics, Secure Cloud Computing

Text Books/Reference Books/Online Resources:

1. CarmitHazay and Yehuda Lindell ,*Efficient Two-party Protocols- Techniques and Constructions* , Springer, 2010
2. Ronald Cramer, Ivan Damgaard and JesperBuusNielsen ,*Secure Multiparty Computation and Secret Sharing*, Cambridge Press, 2015

Course Code: CS5265	Secure Protocols for Electronic Commerce	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Identify algorithms and architecture for security
CO2	Classify security for Business-to-Business electronic commerce
CO3	Apply the SET Protocol
CO4	Evaluate the Secure Payments systems

Mapping of Course Outcomes with program outcomes Course Outcomes:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	1	2	1	1
CO2		1	1	2	1	2
CO3			2	3		1
CO4		1	1	2	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Overview of Electronic Commerce - Electronic Commerce and Mobile Commerce, Effects of the Internet and Mobile Networks, Network Access, Barcodes, Smart Cards, Parties in Electronic Commerce, Security; Money and Payment Systems - Mechanisms of Classical Money, Payment Instruments, Types of Dematerialized Monies, Purses, Holders, and Wallets; Transactional Properties of Dematerialized Currencies, Overall Comparison of the Means of Payment, Practice of Dematerialized Money, Clearance and Settlement in Payment Systems, Drivers of Innovation in Banking and Payment Systems; Algorithms and Architectures for Security - Security of Open Financial Networks, OSI Model for Cryptographic Security, Security Services at the Link Layer, Security Services at the Network Layer, Security Services at the Application Layer, Message Confidentiality, Data Integrity, Identification of the Participants, Biometric Identification, Authentication of the Participants, Access Control, Denial of Service, Nonrepudiation, Secure Management of Cryptographic Keys, Exchange of Secret Keys: Kerberos; Public Key Kerberos, Exchange of Public Keys, Certificate Management, Authentication, Security Cracks; Business-to-Business Commerce-Drivers for Business-to-Business Electronic Commerce, Four Stages of Systems

Integration, Overview of Business-to-Business Commerce, Short History of Business-to-Business Electronic Commerce, Examples of Business-to-Business Electronic Commerce, Evolution of Business-to-Business Electronic Commerce, Implementation of Business-to-Business Electronic Commerce, X12 and EDIFACT, EDI Messaging, Security of EDI, Integration of XML and Traditional EDI, New Architectures for Business-to-Business Electronic Commerce, Electronic Business (Using) Extensible Markup Language, Web Services, Relation of EDI with Electronic Funds Transfer; Transport Layer Security and Secure Sockets Layer - Architecture of SSL/TLS, SSL/TLS Security Services, SSL/TLS Subprotocols, Performance of SSL/TLS, Implementation Pitfalls; Wireless Transport Layer Security - Architecture, From TLS to WTLS, Operational Constraints, WAP and TLS Extensions, WAP Browsers; The SET Protocol -SET Architecture, Security Services of SET, Certification, Purchasing Transaction, Optional Procedures, Efforts to Promote SETs, SET versus TLS/SSL; Payments with Magnetic Stripe Cards - Point-of-Sale Transactions, Communication Standards for Card Transactions, Security of Point-of-Sale Transactions, Internet Transactions, 3D Secure, Migration to EMV; Secure Payments with Integrated Circuit Cards - Description of Integrated Circuit Cards, Integration of Smart Cards with Computer Systems, Standards for Integrated Circuit Cards, Multi application Smart Cards, Security of Smart Cards, Payment Applications of Integrated Circuit Cards, EMV® Card, General Consideration on the Security of Smart Cards; Mobile Payments - Reference Model for Mobile Commerce, Secure Element in Mobile Phones; Barcodes, Bluetooth, Near-Field Communication, Text Messages, Bank- Centric Offers, Mobile Operator–Centric Offers, Third-Party Service Offers, Collaborative Offers, Payments from Mobile Terminals; Micropayments - Characteristics of Micropayment Systems, Standardization Efforts, Electronic Purses, Online Micropayments, Market Response to Micropayment Systems; Case Study of PayPal - Evolution of PayPal, Personal Accounts, Business Accounts; Digital Money -Privacy with Cash and Digital Money, DigiCash (eCash), Anonymity and Untraceability in DigiCash, Evaluation of DigiCash; Bitcoin and Cryptocurrencies - Bitcoin Protocol, Operation, Risk Evaluation; Electronic Commerce in Society - Harmonization of Communication Interfaces, Governance of Electronic Money, Protection of Intellectual Property, Electronic Surveillance and Privacy, Content Filtering and Censorship, Taxation of Electronic Commerce, Trust Promotion, Archives Dematerialization

Text Books/Reference Books/Online Resources:

1. Mostafa Hashem Sherif, *Protocols for Secure Electronic Commerce*, Third Edition, CRC Press, Taylor and Francis group, 2016
2. Ghosh, Anup K. (Ed.), *E-Commerce Security and Privacy*, Springer Publishing, 2001

Course Code: CS5266	Research study on Information Security	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Comprehend popular techniques in the chosen area of research.
CO2	Relate some technological problems to the research areas.
CO3	Justify the approaches to the problems.
CO4	Write survey paper.
CO5	Revise some method in the concerned domain for better solution.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	3	1			1
CO2	1	2	1			1
CO3	1	1	1			1
CO4		2	1			1
CO5		2	1			3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Research Monographs, Articles, Papers as prescribed by the faculty.

Course Code: CS5267	Network Coding	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand the Network Coding Theorem, Finite Fields and Polynomials
CO2	Develop Network Codes to handle noise and attacks
CO3	Analyze the network codes for robustness
CO4	Apply Network Coding to storage systems

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1					
CO2	1		1	2	2	2
CO3	1			2	2	2
CO4	1			1	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Single-Source Multicast Problem, Main Network Coding Theorem, Finite Fields and Polynomials, Algebraic Network Coding, Random Network Coding, non-Multicast Scenarios, Practical NC, NC in P2P, Practical NC Avalanche, RNC in P2P, Analysis of NC and P2P, Avalanche analysis, Index Coding, ANC, WNC, LP framework , Intersession Coding, Multiple Unicasts, Alignment , Intro to Pollution Attacks, Homomorphic tags (Anh), Null Keys, Subspace properties, NC Storage

Text Books/Reference Books/Online Resources:

1. C. Fragouli and E.Soljanin, *Network Coding Applications*, Now Publishers, Available online, http://www.nowpublishers.com/article/Details/NET-013, 2007
2. M.Medard and A. Sprintson, *Network Coding: Fundamentals and Applications*, Academic Press, 2012.
3. T. Ho and D. S. Lun, *Network Coding: An Introduction*, Cambridge University Press, Cambridge, U.K., April 2008.

Course Code: CS5268	Public Key Infrastructure and Trust Management	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Analyze Core PKI services: Authentication, Integrity, and confidentiality
CO2	Design Certificates using Trust Models , PKI Considerations and Electronic Legislation
CO3	Identify PKIX standardization Requirements
CO4	Distinguish Public key certificate management models
CO5	Apply Cryptographic Applications

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1	1	1	1	1
CO2	2		2	2	2	2
CO3	1		1	1		1
CO4	1	1	1	1	1	1
CO5		1	1	2	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction – services offered by PKI- components of a fully functional PKI : Certification authority, Certificate repository, Certificate revocation, Key backup and recovery, Automatic key update, Key history management, Cross-certification, Support for non-repudiation, Time stamping, Client software

PKI architectures – Single CA, Hierarchial PKI, Mesh PKI, Trust Lists, Bridge CAs

PKI standards : X.509: Components of X.509: Tamper evident envelope, Basic certificate contents, certificate extensions.; PGP: Web of Trust; Simple PKI (SPKI) / Simple Distributed Security Infrastructure (SDSI): Representing certificates in terms of S-Expressions- Certificate

Chain Discovery - Distinct Advantages of SPKI/SDSI over X.509. PKI application : Smart card integration with PKI's

Access Control Mechanisms: Discretionary Access Control (DAC) – Mandatory Access Control (MAC) – Role Based Access Control (RBAC).Issues : Revocation- Anonymity-Privacy issues

Trust Management: Policy based Trust Management System- Social network based Trust Management System- Reputation based Trust Management System (DMRep, EigenRep, P2Prep)- Framework for Trust Establishment. Risks Impact on E-Commerce and E-Business: Information Risk – Technology Business Risk

Text Books/Reference Books/Online Resources:

1. Desmedt, Yvo G. (Ed.), *Secure Public Key Infrastructure Standards, PGP and Beyond*, Springer, 2012.
2. J. Camenisch and C. Lambrinoudakis, *Public Key Infrastructures, Services and Applications*, EuroPKI 2010.

Course Code: CS5269	Cyber Laws and Intellectual Property Rights	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand cyberspace, issues there in and need for a cyber law
CO2	Understand facets of India IT act n addressing e-trade and e-governance
CO3	Understanding of issues and problems arising out of online transactions
CO4	Understanding crimes with case law
CO5	Understand of intellectual property issues and development of the law in this regard

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1		2	1	1		2
CO2		2	1			2
CO3		2	1	1		2
CO4		2	2			2
CO5		2	1	1		2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Cyber Space- Fundamental definitions -Interface of Technology and Law – Jurisprudence and-Jurisdiction in Cyber Space - Indian Context of Jurisdiction -Enforcement agencies – Need for IT act - UNCITRAL – E- Commerce basics; Information Technology Act, 2000 - Aims and Objects — Overview of the Act – Jurisdiction -Electronic; Governance – Legal Recognition of Electronic Records and Electronic Evidence - Digital Signature Certificates - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators under the Act -The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability– Powers of Police under the Act – Impact of the Act on other Laws; Cyber Crimes -Meaning of Cyber Crimes –Different Kinds of Cyber crimes – Cyber crimes under IPC; Cr.P.C and Indian Evidence Law - Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber

Terrorism- Violation of Privacy on Internet - Data Protection and Privacy – Indian Court cases; Intellectual Property Rights – Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases, Patents - Understanding Patents - European Position on Computer related Patents, Legal position on Computer related Patents - Indian Position on Patents – Case Law, Domain names -registration - Domain Name Disputes-Cyber Squatting-IPR cases

Text Books/Reference Books/Online Resources:

1. Justice Yatindra Singh, *Cyber Laws*, Universal Law Publishing Co., New Delhi, 2010
2. Farooq Ahmed, *Cyber Law in India,* New Era publications, New Delhi, 2005
3. S.R.Myneni, *Information Technology Law(Cyber Laws),* Asia Law House, Hyderabad, 2014
4. Chris Reed, *Internet Law-Text and Materials*, Cambridge University Press, 2004
5. Pavan Duggal, *Cyber Law- the Indian perspective,* Universal Law Publishing Co., New Delhi, 2004

Course Code: CS5270	Algorithmic Coding Theory	Credits 3-0-0: 3

Pre-requisites: Advanced Algorithms and Foundations of Cryptography

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand Shannon's noisy coding theorem, Shannon capacity and entropy
CO2	Design of error correcting codes and decoding algorithms
CO3	Design and Analysis of light weight and code-based cryptosystems
CO4	Design of network coding algorithms for communication networks

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		2			
CO2	3		2	2	2	3
CO3	2		2	3	2	3
CO4	3		2	3	2	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Shannon Theorem, Shannon capacity, Hamming's Theory, Error correcting codes, Linear codes, Impossibility results for codes, Mac Williams Identities, Linear programming bound, The asymptotic perspective, Encoding, Decoding from erasures, Decoding RS codes, List decoding, linear time decoding, LDPC codes, Sipser-Spielman codes, Linear time encoding and decoding, Linear time and near optimal error decoding, Expander based constructions of efficiently, decodable codes, Some NP hard coding theoretic problems, Applications in complexity theory, Cryptography with error correcting codes, Lossless Multicast Network Coding, Network coding in Lossy Networks, Security against adversarial errors, Error correction bounds for centralized network coding.

Text Books/Reference Books/Online Resources:

1. Tom Richardson, RudigerUrbanke, *Modern Coding Theory,* Cambridge University Press, 2008

2. John b. Anderson and Seshadri Mohan, *Source and Channel Coding: An Algorithm Approach*, Springer, 1991.
3. G. Kabatiansky, E. Krouk and S. Semenov, *Error Correcting Coding and Security for Data Networks,*
   John Wiley & Sons Ltd., 2005.
4. Jiri Adamek, *Foundations of Coding, Wiley Interscience Publication,* John Wiley & Sons, 1991

Course Code: CS5271	Digital Forensics	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand the need for digital forensics
CO2	Identify different technologies for digital forensics
CO3	Understand different investigation methodologies
CO4	Apply the digital forensics for different fields.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1				1	1	1
CO2	1			2	1	1
CO3				2	2	1
CO4	2		1	2	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Information formats, PC hardware, Disc geometry, File system, Electronic organizers. Forensic analysis – Investigative Methodology: Forensic Analysis, Electronic Discovery, Intrusion Investigation. Technology: Windows Forensic Analysis, UNIX Forensic Analysis, Embedded Systems Analysis, Mobile Network Investigations. Intrusion Investigation, Analysis tools, Financial forensics.

Text Books/Reference Books/Online Resources:

1. Sammes T, B. Jenkinson, *Forensic Computing*, Springer, 2007.
2. Eoghan Casey. Ed., *Handbook of Digital Forensics and Investigation*, Academic Press, 2010.

Course Code: CS5272	Secure Dependable and Distributed Computing	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand secure development processes in distributed systems
CO2	Modeling threats and vulnerabilities for host, network, resident code, storage, grid and applications in distributed computing
CO3	Designing architectures for security services in distributed computing
CO4	Applying security models for distributed systems

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1				1	2	1
CO2	2		2	2	2	2
CO3	1		1	2	2	2
CO4	1		1	2	2	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Distributed Systems Security, Secure Development Lifecycle Processes - A Typical Security Engineering Process - Security; Engineering Guidelines and Resources. Common Security Issues and Technologies: Security, Issues, Common Security Techniques; Host-level Threats and Vulnerabilities: Transient code Vulnerabilities - Resident Code; Vulnerabilities - Malware: Trojan Horse – Spyware - Worms/Viruses – Eavesdropping - Job; Faults. Infrastructure-Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities - Grid Computing Threats and Vulnerabilities – Storage Threats and Vulnerabilities – Overview of Infrastructure Threats and Vulnerabilities; Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities -Injection, Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues; Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-

Level Attacks - Services Threat Profile; Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code -Memory Firewall – Antimalware. Infrastructure-Level Solutions: Network-Level Solutions - Grid-Level Solutions - Storage-Level Solutions; Application-Level Solutions: Application-Level Security Solutions; Service-Level Solutions: Services Security Policy - SOA Security Standards Stack – Standards, Deployment Architectures for SOA Security - Managing Service-Level Threats; Future Directions - Cloud Computing Security – Security Appliances, Dependability concepts - Faults and Failures – Redundancy – Reliability – Availability – Safety – Security – Timeliness - Fault-classification - Fault-detection and location - Fault containment, Byzantine failures - Fault injection - Fault-tolerant techniques - Performability metrics, Fault-tolerance in real-time systems - Space- time tradeoff - Fault-tolerant techniques (N-version programming - Recovery block - Imprecise computation; (m,k)- deadline model) - Adaptive fault-tolerance - Fault detection and location in real-time systems. Security Engineering – Protocols - Hardware protection - Cryptography – Introduction – The Random Oracle model –Symmetric Crypto- primitives – modes of operations – Hash functions – Asymmetric crypto primitives; Distributed systems - Concurrency - fault tolerance and failure recovery – Naming. Multilevel Security – Security policy model – The Bell Lapadula security policy model – Examples of Multilevel secure system – Broader implementation of multilevel security system. Multilateral security – Introduction – Comparison of Chinese wall and the BMA model – Inference Control – The residual problem; Nuclear Command and control – Introduction – The kennedy memorandum – unconditionally secure authentication codes – shared control security – tamper resistance and PAL – Treaty verification. Security printing and seals – Introduction – History – Security printing – packaging and seals – systemic vulnerability – evaluation methodology.

Text Books/Reference Books/Online Resources:

1. Ross J Anderson, Ross Anderson, *Security Engineering: A guide to building dependable distributed systems*, Wiley, 2001.
2. David Powell, *A generic fault-Tolerant architecture for Real-Time Dependable Systems*, Springer, 2001.
3. Hassan B Diab and Albert Y. Zomaya, *Dependable computing systems: Paradigm, Performance issues and Applications*, Wiley series on Parallel and Distributed Computing, 2000
4. Abhijit Belapurakar, AnirbanChakrabarti and et al., *Distributed Systems Security: Issues. Processes and Solutions*, Wiley, Ltd., Publication, 2009.
5. Abhijit Belapurkar, AnirbanChakrabarti, HarigopalPonnapalli, NiranjanVaradarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, *Distributed Systems Security: Issues, Processes and Solutions*, Wiley publications, 2009.
6. RachidGuerraoui and Franck Petit, *Stabilization, Safety, and Security of Distributed Systems*, Springer, 2010.

Course Code: CS5273	Data Hiding	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Identify techniques for data hiding
CO2	Analyse models of watermarking
CO3	Identify different types of attacks
CO4	Apply data hiding techniques into different domains
CO5	Apply the data hiding techniques in digital rights management

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1	1		2		2
CO2	1			2		2
CO3	1	1		2		1
CO4		1	2	1		1
CO5		2	2	2		1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction: data hiding models, security and privacy aspects, techniques for hiding data- Digital audio, video, images and text. Steganography: Introduction, how it is different from cryptography, Classification of steganography algorithms: Transform-based, spatial domain, statistical, other, Applications of steganography: Covert channels, audio data, military, e-commerce. Watermarking: Introduction, how it is different from steganography and cryptography, watermarking algorithms, watermarking applications, limitations in watermarking. Digital rights management issues: e-commerce, copyright protection, intellectual property. Issues, digital signatures, authentication, case studies, business models. Multimedia security and information assurance, visual cryptography, key management;

Attacks and benchmarks for data hiding systems; Applications of data hiding technology in medicine, law enforcement, remote sensing, and e- commerce, Software for digital data hiding

Text Books/Reference Books/Online Resources:

1. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, 2nd Edition, Morgan Kaufmann, 2007.
2. Michael T. Raggo and Chet Hosmer, *Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols*, 1st Edition, Syngress, 2012

Course Code: CS5274	Identity Based Cryptography	Credits 3-0-0: 3

Pre-requisites: Foundations of Cryptography, Advanced Algorithms

Course Outcomes: At the end of the course the student will be able to:

CO1	Analysesecurity models for IBE and HIBE
CO2	Design CCA- secure IBE and HIBE
CO3	Develop algorithms for IBE without Pairing
CO4	Develop algorithms for Signature Schemes, Key agreement, Broadcast Encryption
CO5	Develop algorithms for Certificate and certificate less encryption

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		1	1		1
CO2	2		1	2		2
CO3	2	1	1	2		2
CO4	2	1	2	2		2
CO5	2	1	2	2		2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Public key encryption, Security Models for IBE – CCA, CPA, Selective-ID Model, Anonymous (H)IBE, Random Oracles, Finite fields, Elliptic Curves and Pairing, Hardness Assumptions , Boneh-Franklin IBE – Hierarchical IBE, CPA security, Selective identity model, Canetti-Halevi-Katz Transformation, The Boyen- Mei-Waters Transformation, Constant size HIBE, Security analysis against Adaptive chosen cipher text attacks, Adaptive Identity Model without Random Oracle - Boneh-Boyen IBE, Generalisation of Waters IBE, Converting to a CCA-Secure HIBE, Dual System Encryption, IBE without Pairing - IBE Based on Number Theory, IBE From Lattices, Applications – Signature Schemes, Key agreement, Broadcast Encryption; Certificate and certificate less encryption, Avoiding Key Escrow.

Text Books/Reference Books/Online Resources:

1. Sanjit Chatterjee, Palash Sarkar, *Identity-Based Encryption*, Springer, 2011.
2. Marc Joye and G. Neven, *Identity Based Cryptography*, IOS Press, 2009.

Course Code: CS5275	Information Security Risk Management	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand risk-planning and risk management of computer and information systems.
CO2	Apply vulnerability assessment for natural disaster
CO3	Analyzing the implications of emergency response
CO4	Design methods for risk mitigation for infrastructure

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		1	1	1	1
CO2	2		1	2		2
CO3	1			1		1
CO4	2		2	2	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Development of concepts required for risk-based planning and risk management of computer and information systems (Risk analysis, risk perception, Communicating risk, risk mitigation); Objectives and methods for vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures;

Text Books/Reference Books/Online Resources:

1. Alan Calder, Steve G. Watkins, Information Security Risk Management for ISO27001/ISO27002, IT Governance, 2010.
2. Susan Snedaker, Chris Rima, Business Continuity and Disaster Recovery Planning for IT Professionals, Elsevier ScienceDirect, second edition, 2014
3. Harold F. Tipton, Micki Krause Nozaki, Information Security Management Handbook, Volume 6, Sixth Edition, Auerbach Publications, 2016

Course Code: CS5276	Privacy Enhancing Technologies	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1				1		1
CO2	2		2	3	1	2
CO3	2	2	2	3	1	2
CO4	2		2	3	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Major issues in computer security related to protecting privacy, threats to the privacy of computer users; Private communications, anonymous communications, censorship circumvention and traffic analysis; Private authentication, selective disclosure credentials for identify management, and zero-knowledge proof techniques; Private statistics and computations through homomorphic encryption and secure multi-party computation and differential privacy; Privacy threats such as pervasive surveillance, profiling, location analysis, and traffic analysis, as well as the technical mitigation techniques relying on modern cryptography and differential privacy; Standard threats to on-line privacy such as profiling, and location analysis; Methods to mitigate abuses arising from anonymous communication, while preserving privacy, through the use of private authentication, and selective disclosure credentials that can be used to build digital cash systems; Zero-knowledge proofs and their use as building blocks of privacy enhancing technologies; Problem of computing on private data using simple homomorphic encryption schemes as well as modern secure multi-party computation techniques; Statistical disclosure control, ad-hoc techniques for analysis and techniques based on differential privacy.

Text Books/Reference Books/Online Resources:

1. Benjamin C.M. Fung, Ke Wang, Ada Wai-Chee Fu and Philip S. Yu, Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques, 1st Edition, Chapman & Hall/CRC, 2010.
2. Charu C. Aggarwal, Privacy-Preserving Data Mining: Models and Algorithms, 1st Edition, Springer, 2008.
3. Note: Selected research papers are also be given time to time.

Course Code: CS5277	Security of E-Based Systems	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Propose protocols for e-based systems
CO2	Test the protocols using tools
CO3	Analyze the e-based systems and identify the issues
CO4	Understand fundamentals of authentication protocols

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		1	2	1	2
CO2				2		2
CO3	1		1	2		2
CO4	1			1		1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction to e-security, Security services, Security attacks, Threats and vulnerabilities, Basics of protection, Security management, Security policies, Protections of users and networks, Protection of employees of networks, Security planning, Risk analysis, Security plans, Legal issues in system security. Symmetric encryption, Public key cryptosystems, Trapdoor function model, Conventional public key encryption, Public key management, Attacks against public key cryptosystems, The PKIX architecture model, PKIX management functions, Public key certificates, Trust hierarchical models, Bridge certification authority architecture, Deploying the enterprise's PKI, Weak and Strong authentication schemes, Attacks on authentication, Digital signature frameworks, Authentication applications, X.509 Authentication service, Kerberos service, IP authentication header protocol, Authentication in wireless networks. Trust management in communication networks, Delegation of trust, Digital credentials, Authorization and access control systems. Basic technologies for e-services, E-services security, E-government: concepts and practices, Egovernment assets, Challenges, limits, and obstacles to e-government, Authentication in e- government, Privacy in e-government, Monitoring e-government security.

Text Books/Reference Books/Online Resources:

1. Mohammad Obaidat, *Security of e-Systems and Computer Networks,* Monmouth University, New Jersey, 2007 (ISBN-13: 9780521837644)
2. AshutoshSaxena, *PKI: Concepts, Design and Deployment*, Tata McGraw Hill Ltd, 2003
3. SeifedineKadry, Abdelkhalak El Hami, *E-Systems for the 21st Century: Concept, Developments, and Applications - Two Volume Set,* Apple Academic Press, 2016 ISBN 9781771882552

Course Code: CS5278	Secure Group Communications	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Identify challenges and factors enabling secure group communication
CO2	Analyse group key managements schemes
CO3	Analyse centralized group key distribution schemes
CO4	Analyse dynamic conference schemes and hierarchical Access Control
CO5	Apply group key management techniques to mobile networks

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1			1	1	1
CO2	2		1	2	3	2
CO3	2		1	2	3	2
CO4	2		1	2	3	2
CO5	2		2	3	3	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction - Overview of Secure group communications, Preliminaries, Enabling Technologies, Group Dynamics and Security; Group Key Management Schemes – Classification of Typical Group Key Management Schemes, Public Key Based Secure Group Communication Schemes – RPS and STB, Secrete Key Based Secure Group Communication Schemes – CBT, Iolus, and DEP, Group Key Management Based on Hierarchical Clusters, N-Party Diffie Hellman Key Exchange suites – ING,BD and GDH protocols; Tree Based Key Management Schemes – Centralized Key Distribution based on Tree Structure – Key Tree, Bursty behavior and its implementation, d-ary key tree, OFT, OFC, Collusion attacks on OFT and its improvement, Distributed Key Agreement based on Tree structure – TGDH,BF-TGDH, DISEC; Dynamic Conferencing Schemes (DCS) – Introduction and a Naïve solution, Public-Key based DCS (PKDCS), Chinese Remainder Theorem based DCS, Symmetric Polynomial

based DCS, Tree based DCS, BF-TGDH based DCS; Secure Group Communications with Hierarchical Access Control – Classification, Unconditionally Secure Keying Schemes for HAC, One Way function Schemes for HAC, Index based Schemes for SGC with HAC, CRT based Schemes for SGC with HAC; SGC Challenges – Factors enabling SGC functionality, admission control and membership management, message/packet source authentication, Coordination, Broadcast authentication; SGC for Wireless and mobile Networks – Topology matching key management, Key management for TMKM, Admission scoped key management, SGC over adhoc networks.

Text Books/Reference Books/Online Resources:

1. Zou, Xukai, Ramamurthy, Byrav, Magliveras, Spyros S, *Secure Group Communications over Data Networks,* Springer, 2005.
2. Jeremy Moskowitz, *Group Policy: Fundamentals, Security, and the Managed Desktop*, 1st Edition, Cybex, 2010.

Course Code: CS5279	Cyber Crime and Information Warfare	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand principles of cyber crime and cyber forensics.
CO2	Verify cryptography techniques using Cryptool
CO3	Apply appropriate countermeasures to defend threats
CO4	Apply suitable forensic tools for forensic analysis
CO5	Understand social and web intelligence in era of information age.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1					
CO2				1		1
CO3	1		1	2	1	2
CO4	1		1	2	1	2
CO5	2		2	2		2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Cyber Crime: Industrial espionage and cyber-terrorism, principles of criminal law, computer forensic investigation, elements of personnel security and investigations, principles of risk and security management, conspiracy in computer crime, and computer fraud investigation. **Introduction to Cyber Forensics:** Computer Forensics and the law, Private & Public sector workplace practices, Cyber Crime examples: Defacements, DoS, Credit Card theft, Silent intrusion, internal attacks, investigative actions, Forensics analysis investigative action, Computer Forensic tools.

Information Warfare: Nature of information warfare including computer crime and information terrorism; Threats to information resources, including military and economic espionage, communications eavesdropping, computer break-ins, denial-of-service,

destruction and modification of data, distortion and fabrication of information, forgery, control and disruption of information flow, electronic bombs, and perception management.

Defenses: Countermeasures including authentication, encryption, auditing, monitoring, intrusion detection, and firewalls, and the limitations of those countermeasures. Introduction to Open Source Intelligence (OSINIT), web intelligence and social media intelligence. Cyberspace law and law enforcement, information warfare and the military, and intelligence in the information age

Text Books/Reference Books/Online Resources:

1. Information Warfare, Ventre, John Wiley & Sons, 15-Feb-2016
2. J. Wiles and A.Reyes, The Best Damn Cybercrime and Digital Forensics Book Period, Syngress, 2007.

Course Code: CS5280	Cryptography and Game Theory	Credits 3-0-0: 3

Pre-requisites: Foundations of Cryptography

Course Outcomes: At the end of the course the student will be able to:

CO1	Apply Cryptography to advance Game Theoretic goals
CO2	Enrich equilibria with additional properties
CO3	Design better mechanisms.
CO4	Apply Game Theory to advance Cryptographic protocol design
CO5	Combine game-theoretic arguments into cryptographic proofs, or vice versa.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1		1	1	2		2
CO2				2		2
CO3		1	1	2		1
CO4	2	1	2			1
CO5	2	2		2		

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Background in Cryptography: Basics: Indistinguishability, Encryption, Zero Knowledge, Secure Computation: Definitions, basic constructions, Fairness in secure computation: Definitions, constructions, impossibility results. Background in Game Theory:Zero-sum games, the min-max theorem, Normal form games: Nash equilibrium, correlated equilibrium, dominated strategies, approximate Nash equilibria.

Extensive form games: Subgame perfection, imperfect/incomplete information, Bayesian/sequential/trembling-hand equilibria. Cryptographic Game Theory:Computational notions of Nash Equilibria, Replacing trusted mediators via cryptographic means, Rational Secure computation: Basic formalisms, Rational secret sharing (Two-party and multi-party).

Text Books/Reference Books/Online Resources:

1. O. Goldreich, *Foundations of Cryptography*: Volumes 1 and 2. Cambridge University Press, 2004.
2. Noam Nisan, Tim Roughgarden, Eva Tardos, Vijay V. Vazirani, *Algorithmic Game Theory*, Cambridge University Press, 2007.
3. M. J. Osborne and A. Rubinstein, *A course in game theory*, MIT Press, 1994

Course Code: CS5281	Malware Analysis	Credits 3-0-0: 3

Pre-requisites: Foundations of Cryptography

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand nature of malware and its capabilities
CO2	Know scientific and logical limitations on ability to combat malware.
CO3	Understand social, economic and historical context in which malware occurs.
CO4	Apply static and dynamic analysis techniques to synthetic and real life examples
CO5	Apply suitable measures based on the context to detect and mitigate popular infection methods.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1			2	2	1
CO2	1	1		2	2	2
CO3		1		3	3	
CO4		1	2	1		2
CO5		2	3	3	2	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction: The taxonomy of malware and its capabilities: viruses, Trojan horses, rootkits, backdoors, worms, targeted malware; History of malware

The social and economic context for malware: crime, anti-malware companies, legal issues, the growing proliferation of malware

Basic Analysis: Signature generation and detection; clone detection methods Static analysis theory: program semantics, and abstract interpretation framework

Static Analysis: System calls: dependency analysis issues in assembly languages; semantic invariance of system call sequences; abstract interpretation as a formal framework for detection; constraint-based analyses; semantic clones
Dynamic Analysis: virtualization: semantic gap; reverse engineering; hybridisation with static analysis; Overview of Windows file format, PEView.exe, Patching Binaries , Disassembly(objdump, IDA Pro), Similarity metrics: Kolmogorov Complexity; association metrics; other entropy based metrics; NLP based approaches
Problems in large scale classification: scalability; triage methods; Required FP rate
Hiding: Polymorphism: compression encryption virtualization; Metamorphism: high level code obfuscation engines, on-board metamorphic engines, semantics-preserving rewritings; Frankenstein

The theory of malware: Rice's theorem and the undecidability of semantic equivalence; Adleman's proof of the undecidability of the presence of a virus; Cohen's experiments on detectability and self-obfuscation Advanced Dynamic Analysis: debugging tools and concepts, Malware Behavior - malicious activities and techniques, Analyzing Windows programs – WinAPI, Handles, Networking , COM, Data Encoding, Malware Countermeasures, Covert Launching and Execution, Anti Analysis- Anti Disassembly, VM, Debugging -, Packers – packing and upacking, Intro to Kernel – Kernel basics, Windows Kernel API, Windows Drivers, Kernel Debugging - Rootkit Techniques- Hooking, Patching, Kernel Object Manipulation, Rootkit Anti- forensics, Covert analysis.

Text Books/Reference Books/Online Resources:

1. Michael Sikorski, Andrew Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software,* No Starch Press, 2012 (for lab work).
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.

Course Code: CS5282	Cyber Security	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Understand the cyber security fundamentals
CO2	Identify & Evaluate cyber security threats and vulnerabilities in Information Systems and apply security measures to real time scenarios
CO3	Design and implement appropriate security techniques and cyber policies to protect computers and digital information.
CO4	Identify common trade-offs and compromises that are made in the design and development process of Information Systems
CO5	Demonstrate the use of standards and cyber laws to enhance information security in the development process and infrastructure protection

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1			1			1
CO2	2		2	2		2
CO3	2		2	2		2
CO4	1			1		
CO5	2	1	3	1		3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Cyber Security Fundamentals: Network and Security Concepts-Information Assurance Fundamentals, Basic Cryptography, Symmetric and Asymmetric Encryption, Public Key Encryption, The Domain Name System (DNS), Firewalls, Virtualization, Radio-Frequency Identification.

Threats and vulnerabilities: Types of Threats- Malware, Phishing, Ransomware, Adware and Spyware, Trojan, Virus, Worms, Man-in-the-middle-attack, Scareware, Distributed Denial-Of- Service Attack, Rootkits, click-fraud. Vulnerability-Shellcode, Integer Overflow Vulnerabilities, Buffer Overflows, SQL Injection.

Defense and mitigation measures: Anti-virus scanners, static and dynamic methods, anti-analysis, eavading obfuscations and run-time attacks.

Cyber Forensics: Memory and network Forensics for Winodws and Linux internals, Forensic tools, OS hardening and RAM dump analysis, data acquisition, data extraction, volatility analyses for OS artifacts and other information. Automated malicous code analysis.

Cybersecurity law and Regulations: Introduction, Cyber Warfare, Deception in the Cyber-World, Legal Framework of Cyber Security.

Text Books/Reference Books/Online Resources:

1. James Graham, Richard Howard, Ryan Olson, CYBER SECURITY ESSENTIALS, Taylor and Francis Group, 2011.
2. MarttiLehto, PekkaNeittaanmäki, Cyber Security: Analytics, Technology and Automation, Springer, 2015
3. David Salomon, Foundations of Computer Security, Springer, 2006

Course Code: CS5283	Elliptic Curve Cryptosystems	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Identify group properties of elliptic curves
CO2	Compute order of elliptic curve group
CO3	Design Public key cryptosystems
CO4	Analyse elliptic curves over C and hyper elliptic curves
CO5	Compute Wei and Tate pairing

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		2		1	
CO2		1				1
CO3			1		2	
CO4		2				
CO5	1	1			2	

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction: Wierstrauss Equation, The Group Law, Projective Space and the Point at Infinity, Proof of Associativity, Equations for Elliptic Curves, Coordinate Systems, The j-invariant, Endomorphisms, Singular Curves, Elliptic Curves mod n; Tortion Points: Introduction about Torsion Points, Division Polynomials, The Weil Pairing, The Tate-Lichtenbaum Pairing; Elliptic Curve over Finite Fields- Zeta Functions: Introduction, The Frobenius Endomorphism, Determining the Group Order, A Family of Curves, Schoof's Algorithm, Super singular Curves; Discrete Logarithm Problem: Introduction, The Index Calculus, General Attacks on Discrete Logs, Attacks with Pairings, Anomalous Curves, Other Attacks; Elliptic Curve Cryptography: Introduction, The Basic Setup, Diffie-Hellman Key Exchange, Massey-Omura Encryption, ElGamal Public Key Encryption; Primality and Factorization of Integers: Primality, Complexity of factoring, RSA; Elliptic Curve OVER Q - LUTZ-NAGELL Theorem: The Torsion Subgroup. The Lutz-Nagell Theorem, Descent and the Weak Mordell-Weil, Theorem Heights and the Mordell-Weil Theorem, Heights and the

Mordell-Weil Theorem, The Height Pairing, Fermat's Infinite Descent, 2-Selmer Groups; Shafarevich-Tate Groups, A Nontrivial Shafarevich-Tate Group, Galois Cohomology, Mordel-Weil Theorem; Elliptic Curve OVER C: Doubly Periodic Functions, Tori are Elliptic Curves, Elliptic Curves over C, Computing Periods, Division Polynomials, The Torsion Subgroup: Doud's Method, Division Polynomials; Complex Multiplication: Elliptic Curves over C, Elliptic Curves over Finite Fields, Integrality of j-invariants, Numerical Examples, Kronecker'sJugendtraum; Isogeny: The Complex Theory, The Algebraic Theory, Velu's Formulas, Point Counting, Complements; Hyperelliptc Curves: Basic Definitions, Divisors: Weil pairing, Tate-Lichtenbaum pairing, Cantor's Algorithm, The Discrete Logarithm Problem.

Text Books/Reference Books/Online Resources:

1. L.C. Washington, *Ellipptic curves: Number Theory and Cryptography*, CRC Press, 2008
2. H. Cohen and G.Frey, *Handbook of Elliptic curve and Hyperelliptic Curve Cryptography*, CRC Press, 2006.

Course Code: CS5284	Secure Systems Engineering	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course, the student will be able to

CO1	Identify and analyse vulnerabilities at hardware level
CO2	Identify micro architectural level security
CO3	Analyse and apply countermeasures to system level attacks
CO4	Apply malware analysis techniques at system level
CO5	Formally verify the security protocol

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2		2	2	1	1
CO2	2		3	2	1	1
CO3	3	2	2	3	3	3
CO4	2	1	2	3	3	3
CO5	1	3	2	2	1	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Hardware Security: Hardware Trojans and Detection – PUFs - Power Analysis Attacks and Countermeasures - Fault Attacks - Implementation Aspects of Crypto Algorithms (A case study of AES and ECC)

Micro Architectural Security: Timing attacks and Covert Channels - RAM based attacks - Cold boot - Rowhammer – Operating System Security Stack Smashing Attacks - Dynamic Memory Allocation Attacks - Format String Vulnerabilities - return-to-libc attacks - ROP attacks - Side Channel Attacks in Operating Systems – Countermeasures - Non-executable stacks - Capability based Systems - Canaries - Malware Analysis Techniques

Application Security: SQL Insertion - Shell Shock - Heart bleed bug – Formal Verification of Security Protocols

Text Books/Reference Books/Online Resources:

1. Timing Channels in Cryptography, A Micro- Architectural Perspective Timing Channels in Cryptography, Chester Rebeiro, Debdeep Mukhopadhyay and Sarani Bhattacharya, Springer, 2015
2. Secure Systems Engineering, ISEA Study Material, IIT Madras, Available by March 2017
3. Chris Wysopal, Backdoors and other Developer Introduced 'Features', OWAS and WASC AppSec 2007 Conference, San Jose, Nov. 2007
4. Samuel T. King et al., SubVirt: Implementing malware with virtual machines, http://web.eecs.umich.edu/~pmchen/papers/king06.pdf
5. Aleph One, Smashing the Stack for Fun and Profit, http://insecure.org/stf/smashstack.html
6. Thompson, Ken, "Reflections on Trusting Trust", Communication of the ACM Vol. 27, No. 8, http://www.acm.org/classics/sep95/, Sep. 1995.
7. Paul A. Karger and Roger Shell, Thirty Years Later: Lessons from the Multics Security Evaluation, http://hack.org/mc/texts/classic-multics.pdf

Course Code: CS5285	Privacy and Security for online social networks	Credits 3-0-0: 3

Pre-requisites: None

Course Outcomes: At the end of the course, the student will be able to:

CO1	Identify pitfalls in social networks
CO2	Analyse trust management in Online social networks
CO3	Analyse and apply countermeasures to control information sharing in Online social networks
CO4	Apply identity management in Online social networks
CO5	APIs to analyse the online social networks

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	1		1	2	2	2
CO2	2		2	2	1	1
CO3	2		2	2	3	1
CO4	2		2	3	2	3
CO5	3		2	2	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction to Online Social Networks: Introduction to Social Networks, From offline to Online Communities, Online Social Networks, Evolution of Online Social Networks, Analysis and Properties, Security Issues in Online Social Networks, Trust Management in Online Social Networks, Controlled Information Sharing in Online Social Networks, Identity Management in Online Social Networks, data collection from social networks, challenges, opportunities, and pitfalls in online social networks, APIs; Collecting data from Online Social Media

Trust Management in Online Social Networks: Trust and Policies, Trust and Reputation Systems, Trust in Online Social, Trust Properties, Trust Components, Social Trust and Social Capital, Trust Evaluation Models, Trust, credibility, and reputations in social systems; Online social Media and Policing, Information privacy disclosure, revelation and its effects in OSM and online social networks; Phishing in OSM & Identifying fraudulent entities in online social networks

Controlled Information Sharing in Online Social Networks: Access Control Models, Access Control in Online Social Networks, Relationship-Based Access Control, Privacy Settings in Commercial Online Social Networks, Existing Access Control Approaches

Identity Management in Online Social Networks : Identity Management, Digital Identity, Identity Management Models: From Identity 1.0 to Identity 2.0 , Identity Management in Online Social Networks, Identity as Self-Presentation, Identity theft...

Open Security Issues in Online Social Networks

Text Books/Reference Books/Online Resources:

1. Security and Privacy-Preserving in Social Networks, Editors: Chbeir, Richard, Al Bouna, Bechara (Eds.), Spinger, 2013.
2. Security and Trust in Online Social Networks, Barbara Carminati, Elena Ferrari, Marco Viviani, Morgan & Claypool publications.
3. Security and Privacy in Social Networks, Editors: Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A. (Eds.), Springer, 2013

Course Code: CS5253	Network Security Laboratory	PCC	Credits 0-0-2: 1

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Develop secure traffic communication techniques in Internet applications.
CO2	Analyze mobile threats and malwares
CO3	Design and Implement secure routing and medium access protocols in emerging Networks.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1				2		2
CO2				2		2
CO3				2		2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Implementation of secure Internet protocols, Access control protocols, Network Anomaly Detection methods, Mobile IPv6, https protocol, Firewalls and Intrusion Detection Systems, Malware detection, Mobile application security models, Mobile threats and malware, Trust based protocols, Mobile web app security, Secure protocols for mobile adhoc networks, secure neighbor discovery, Wormhole detection mechanisms in wireless sensor networks, Secure routing in wireless adhoc and sensor networks, Secure MAC protocols.

Text Books/Reference Books/Online Resources:

1. John R. Vacca, *Computer and Information Security Handbook,* Elsevier, 2009
2. L. Buttyan, J. P. Hubaux*, Security and Cooperation in Wireless Networks,* Cambridge University Press*, 2008.*
3. W. Trappe, L. C. Washington, *Introduction to Cryptography with Coding Theory,* Prentice-Hall 2005
4. NoureddineBoudriga, *Security of Mobile Communications,* Auerbach Publications, Taylor and Francis Group, 2010.

Course Code: CS5254	Data Privacy Lab	PCC	Credits 0-0-2: 1

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Implementation of differential privacy mechanism for numeric, non-numeric and linear queries
CO2	Implement composition techniques in the design of mechanisms
CO3	Implement utility measurement of differential privacy to evaluate mechanisms
CO4	Classify the existing mechanisms into several types: transformation, partitioning of dataset, query separation and iteration.
CO5	Build a system that supports that deferentially private data analysis.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	3	1	3	2	3	3
CO2	3	1	3	1	3	3
CO3	2	1	3	3	3	3
CO4	2	1	2	2	3	3
CO5	2	2	2	2	3	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

1. Implement differential privacy using the Laplace mechanism for numeric data
2. Implement differential privacy using the Exponential mechanism for non-numeric data
3. Implement differential privacy using the Gaussian mechanism for linear queries
4. Implement Sequential/parallel composition theorems in the design of the above mechanisms
5. Implement the utility measurements such as Noise size and error for data publishing and analysis to evaluate the performance of differential privacy mechanisms.
6. Use Machine learning approach to classify the mechanisms into several types

Text Books/Reference Books/Online Resources:

1. C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*, now Publishers, 2014.
2. Tianqing Zhu, Gang Li, Wanlei Zhou, Philip S. Yu, Differential Privacy and Applications, Springer International Publishing AG 2017.

Course Code: CS5154	Deep Learning Lab	PCC	Credits 0-1-2: 2

Pre-requisites: None

Course Outcomes: At the end of the course the student will be able to:

CO1	Implement Multilayer Feed Backward Neural network on MNIT digits dataset
CO2	Build RNN, LSTM, BiLSTM Networks for time series analysis classification problems.
CO3	Design Autoencoders to solve Unsupervised Learning problems
CO4	Implement Classical Supervised Tasks for Image Denoising, Segmentation and Object detection problems.

Course Articulation Matrix:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6
CO1	2	2	1	1	1	1
CO2		2	2	2		
CO3			1	2		1
CO4	1	1	2		2	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Implement perceptron learning algorithm and attempt to solve two input i) AND gate ii) Or Gate iii) EXOR gate problems.

1. Design and implement a perceptron learning algorithm and attempt to solve XOR problem
2. Implement a Multilayer Feed Backward Neural network algorithm on MNIT digits dataset.
3. Build your own Recurrent networks and Long short-term memory networks on IMDB movie reviews classification data.
4. Design and implement a BiLSTM and BERT on given a product review dataset to classify the review rating from 1 to 5 classes
5. Design and implement Autoencoders for credit card fraud detection.
6. Design and implement a Convolutional Neural Network for image classification on the Fashion-MNIST dataset.
7. Implement a VGG19 model for image classification with and without Transfer Learning on Grocery dataset.
8. Implement a U-Net convolutional neural network model on segmentation of electron microscopic (EM) images of the brain dataset.
9. Implement a FRCNN algorithm for object detection on small object dataset

Text Books/Reference Books/Online Resources:

1. Deep Learning- Ian Goodfelllow, Yoshua Benjio, Aaron Courville, The MIT Press.
2. Christopher Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.
3. Simon Haykin, “Neural Networks, A Comprehensive Foundation”, 2nd Edition, Addison Wesley Longman, 2001.

Course Code: CS5298	SEMINAR-II	Credits 0-0-2: 1

Pre-Requisites: None

Course Outcomes:

At the end of the course, the student will be able to

CO1	Analyze the selected topic, organize the content and communication to audience in an effective manner
CO2	Practice the learning by self study

Course Articulation Matrix:

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
CO1	2	3	1	1		
CO2	2	3	1	1		

1 - Slightly; 2 - Moderately; 3 – Substantially

Course Code: CS6247	COMPREHENSIVE VIVA	Credits 0-0-0: 2

Pre-Requisites: None

Course Outcomes:

At the end of the course, the student will be able to

CO1	Comprehend and correlate the understanding of all courses in post graduate curriculum of Computer Science and Engineering

Course Articulation Matrix:

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
CO1	3	3	3	3	3	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Course Code: CS6249	DISSERTATION WORK – PART A	Credits 0-0-0: 12

Pre-Requisites: None

Course Outcomes:

At the end of the course, the student will be able to

CO1	Identify the problem of a research project through literature survey
CO2	Analyze the technical feasibility of the project
CO3	Propose a solution for the research problem
CO4	Analyze, design and implement the proposed solution using software engineering practices

Course Articulation Matrix:

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
CO1	2	3	2	2	2	1
CO2	2	3	2	2	2	1
CO3	2	3	2	2	2	1
CO4	2	3	2	2	2	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Course Code: CS6299	DISSERTATION WORK – PART B	Credits 0-0-0: 20

Pre-Requisites: None

Course Outcomes:

At the end of the course, the student will be able to

CO1	Synthesize and apply prior knowledge to designing and implementing solutions to open-ended computational problems while considering multiple realistic constraints
CO2	Design and Develop the software with software engineering practices and standards
CO3	Evaluate the solution through various validation and verification methods
CO4	Analyze professional issues, including ethical, legal and security issues, related to computing projects

Course Articulation Matrix:

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
CO1	3	1	2	2	2	3
CO2	2	1	2	2	2	3
CO3	2	1	2	2	2	3
CO4		1	2	2	2	3

1 - Slightly; 2 - Moderately; 3 – Substantially