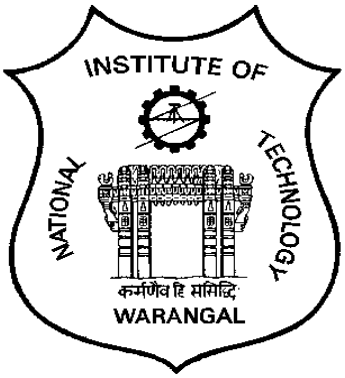
NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



SCHEME OF INSTRUCTION AND SYLLABI

Effective from academic year 2019-20

FOR PROGRAM

M.Tech. (Computer Science and Information Security)

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 AND 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

M.TECH IN COMPUTER SCIENCE AND INFORMATION SECURITY

PROGRAM EDUCATIONAL OBJECTIVES

1.	Apply knowledge of computer science to provide information security.
2.	Design and develop secure software systems using models as per user requirements.
3.	Work in teams using common security tools and environment to achieve project objectives
4.	Communicate effectively, demonstrate leadership qualities and exhibit professional ethics.
5.	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 Offered	Min. credits to be earned
Program Core Courses (PCC)	26	26
Departmental Elective Courses (DEC)	≥ 18	18
Seminar, Comprehensive Viva-voce	4	4
Program major Project (PCC)	27	27
Total	**≥ 75**	**75**

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
1	CS5101	Advanced Algorithms	3	0	0	3
2	CS5201	Web and Database Security	3	0	0	3
3	CS5202	Foundations of Cryptography	3	0	0	3
4	CS5203	Data Mining	3	0	0	3
5	CS5204	Cryptography Lab	0	1	2	2
6	CS5205	Web and Database Security Lab	0	1	2	2
7	CS51--/CS52--	Elective – 1	3	0	0	3
8	CS51--/CS52--	Elective – 2	3	0	0	3
9	CS5241	Seminar – I	0	0	2	1
		Total	**18**	**2**	**6**	**23**

M. Tech. I - Year II - Semester

S. No.	Course No.	Course Name	L	T	P	Credits
1	CS5251	Network Security	3	0	0	3
2	CS5252	Data Privacy	3	0	0	3
3	CS5253	Network Security Lab	0	1	2	2
4	CS5254	Data Privacy Lab	0	1	2	2
5	CS51--/CS52--	Elective - 3	3	0	0	3
6	CS51--/CS52--	Elective - 4	3	0	0	3
7	CS51--/CS52--	Elective – 5	3	0	0	3
8	CS51--/CS52--	Elective – 6	3	0	0	3
9	CS5291	Seminar- II	0	0	2	1
		Total	**18**	**2**	**6**	**23**

M. Tech II Year - I Semester

S. No.	Course No.	Course Name	L	T	P	Credits
1	CS6242	Comprehensive Viva	0	0	0	2
2	CS6249	Dissertation Work – Part A	0	0	0	9
		Total	**0**	**0**	**0**	**11**

M. Tech II Year - II Semester

S. No.	Course No.	Course Name	L	T	P	Cr
1	CS 6299	Dissertation Work – Part B	0	0	0	18
		Total	**0**	**0**	**0**	**18**
		Total Credits	**0**	**0**	**0**	**75**

Electives

Elective Courses – I year – I Semester			
Course No.	**Course Name**	**L-T-P**	**C**
CS5211	Computational Number Theory	3-0-0	3
CS5212	Mathematical models for Internet	3-0-0	3
CS5213	Cryptanalysis	3-0-0	3
CS5214	Computability and Complexity	3-0-0	3
CS5215	Information Systems Control and Auditing	3-0-0	3
CS5216	Probabilistic Algorithms	3-0-0	3
CS5221	Biometric Security	3-0-0	3
CS5222	Unix Internals	3-0-0	3
CS5223	Secure Software Engineering	3-0-0	3
CS5224	Secure Cloud Computing	3-0-0	3
CS5225	Algorithmic Game Theory	3-0-0	3
CS5226	Digital Video Processing	3-0-0	3

Elective Courses – I year II semester			
CS5261	Foundations of Block Chain Technology	3-0-0	3
CS5262	Secure Operating Systems	3-0-0	3
CS5263	Design of Secure Protocols	3-0-0	3
CS5264	Secure Multiparty Computation	3-0-0	3
CS5265	Secure Protocols for Electronic Commerce	3-0-0	3
CS5266	Research study on Information Security	3-0-0	3
CS5267	Network Coding	3-0-0	3
CS5268	Public Key Infrastructure and Trust Management	3-0-0	3
CS5269	Cyber laws and Intellectual Property Rights	3-0-0	3
CS5270	Algorithm Coding Theory	3-0-0	3
CS5271	Digital Forensics	3-0-0	3
CS5272	Secure Dependable and Distributed Computing	3-0-0	3
CS5273	Data Hiding	3-0-0	3
CS5274	Identity Based Cryptography	3-0-0	3
CS5275	Information Security Risk Management	3-0-0	3
CS5276	Privacy Enhancing Technologies.	3-0-0	3
CS5277	Security of E-Based Systems	3-0-0	3
CS5278	Secure Group Communication	3-0-0	3
CS5279	Mobile Security	3-0-0	3
CS5280	Cyber crime and Information Warfare	3-0-0	3
CS5281	Cryptography and Game Theory	3-0-0	3
CS5282	Malware Analysis	3-0-0	3
CS5283	Cyber Security	3-0-0	3
CS5284	Elliptic Curve Cryptosystems	3-0-0	3

DETAILED SYLLABUS

CS5101	Advanced Algorithms	Core	3 – 0 – 0	3 Credits

Pre-requisites: Data Structures and algorithms, Discrete Mathematics

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	Prove the correctness of algorithms using inductive proofs and invariants.
CO3	Analyze randomized algorithms (expected running time, probability of error) using tail inequalities
CO4	Classify problems into different complexity classes corresponding to both deterministic and randomized algorithms
CO5	Analyse approximation algorithms including algorithms that are PTAS and FPTAS.

Mapping of course outcomes with program outcomes

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

Detailed Syllabus

Algorithm design techniques – Dynamic programming: Matrix chain multiplication, Optimal BST, Greedy algorithms – Shortest path algorithm, MST, Amortized analysis, Data structures for disjoint sets, Divide-and-Conquer- Karatsuba integer multiplication, Large integer multiplications using FFT, NP-Completeness: Poly-time, Poly-time verification, reducibility, NP-Complete problems, Approximation algorithms, Randomized algorithms: Las Vegas and Monte Carlo, Game-Theoretic Techniques: Game Tree Evaluation, The Minimax Principle, Randomness and Non-uniformity, Moments and Deviations: Occupancy Problems, The Markov and Chebyshev, Inequalities, Randomized Selection, Two-Point Sampling, The Stable Marriage Problem, The Coupon Collector's Problem, Tail Inequalities: The Chernoff Bound, Routing in a Parallel Computer, A Wiring Problem.

Reading:

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, *Introduction to Algorithms*, 2nd Edition, The MIT Press, 2001.
2. C.H. Papadimitriou. *Complexity Theory.* Addison-Wesley, 1994.
3. Rajeev Motwani and PrabhakarRaghavan, *Randomized Algorithms,* Cambridge Univ. Press, 1995.
4. Garey Michael R, Johnson Davis S, *Computers and Intractability: A Guide the theory of NP-Incompleteness,*W.H. Freeman & Co.1979.

CS5201	Web and Database Security	Core	3 – 0 – 0	3 Credits

Pre-requisites: Database Management Systems, Practical exposure on Commercial Database Management Systems

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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

CS5202	Foundations of Cryptography	Core	3 – 0 – 0	3 Credits

Pre-requisites: Algorithms, Discrete Mathematics

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
CO3	Analyse and compare symmetric-key encryption public-key encryption schemes based on different security models
CO4	Apply Interactive proofs, Commitment protocols, Zero-knowledge proofs, Non-interactive proofs,
CO5	Design and analyze digital cash system and electronic voting system

Mapping of course outcomes with program outcomes

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

Detailed Syllabus

Number Theory – Divisibility, Congruences, Quadratic residues and residuacity, Abstract Algebra – Groups, rings, fields, construction of finite fields, cryptography, Stream Ciphers – One-time Pad (OTP), Perfect secrecy, Pseudo-random generators (PRG), Attacks on stream ciphers and OTP, Real world stream ciphers, Semantic security, Block ciphers- DES, attacks, AES, Block ciphers from PRG, Modes of operation – one-time key and many-time keys, CBC, CTR modes, Message Integrity – MAC, MAC based on PRF, NMAC, PMAC, Collision resistance – Birthday attack, Merkele-Damgard construction, HMC, Case study:SHA-256, Authenticated encryption, Key exchange algorithms, Public key cryptosystems – RSA, ElGamal, Rabin, Elliptic curve cryptosystems – PKC, key exchange, IBE, Lattice based cryptosystem.

Reading:

1. N. Koblitz, *Number Theory and Cryptography*, Springer, 2001
2. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC press, 2008.
3. Menezes, et.al, *Handbook of Applied Cryptography*, CRC Press, 2004.
4. Golreich O, *Foundations of Cryptography*, Vol.1.2, Cambridge University Press, 2004.

CS5203	Data Mining	Core	3 – 0 – 0	3 Credits

Pre-requisites: None

Understand stages in building a Data Warehouse CO2 Apply preprocessing techniques for data cleansing CO3 Analyze multi-dimensional modeling techniques CO4. CO5

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.

Mapping of course outcomes with program outcomes

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

Detailed 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;

Reading:

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.

CS5204	Cryptography Laboratory	Core	0 – 1 – 2	2 Credits

Pre-requisites: programming in C, C++

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

Mapping of course outcomes with program outcomes

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

Detailed Syllabus

Programming Assignment Set 1:

1. Euclidean and Extended Euclidean algorithm for finding the Greatest Common Divisor of two large integers. Computing the Multiplicative inverses in Z_n.
2. Repeated square and multiply algorithm for modular exponentiation in Z_n.
3. Determining the order of a group element. Finding a generator of a cyclic group.
4. Chinese remainder theorem.
5. Computation of Legendre symbol and Jacobi symbol
6. Modular polynomial arithmetic
7. RSA public key algorithm
8. Elgamal Cryptosystem
9. Rabin cryptosystem
10. Diffie-Hellman Key exchange protocol.

Programming Assignment Set II:

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

Programming Assignment Set III:

1. Sieve of Eratosthenes
2. Fermat primality test
3. Solovay-Strassen probabilistic primality test
4. Miller-Rabin probabilistic primality test
5. Lucas-Lehmer primality test

Instructions:

1. C/C++ Programming Language under Linux Operating System
2. PARI C library by Henry Cohen et.al. http://pari.math.u-bordeaux.fr/
3. The pairing-based cryptography library by B. Lynn. http://crypto.stanford.edu/pbc/.
4. Code should be wellmodularised and documented
5. Use the standard coding style

Reading:

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

CS5205	Web &Database Security Laboratory	Core	0 – 1 – 2	2 Credits

Pre-requisites: Database Management Systems, Practical exposure on Commercial Database Management Systems, Web Security,

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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.

CS5251	Network Security	Core	3 – 0 – 0	3 Credits

Pre-requisites: Foundations of Cryptography, Basics of Computer Networks

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.

Mapping of course outcomes with program outcomes

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

Detailed 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.

References:

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.

CS5252	Data Privacy	Core	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed Syllabus

Promise of Differential Privacy, Definition of differential privacy, Randomized response, The laplace mechanism, The exponential mechanism, Composition theorems, The sparse vector technique, Releasing Linear Queries with Correlated Error, Mechanisms via α-nets, The iterative construction mechanism, Boosting for Queries, Worst-Case Sensitivity, Lower bounds, Computational Complexity, 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, risk minimization; Generalization of randomized response, Relaxation to the assumption of trusted curator.

Reading:

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

CS5253	Network Security Laboratory	Core	0 – 1 – 2	2 Credits

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.

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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.

CS5254	Data Privacy Lab	Core	0 – 1 – 2	2 Credits

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.

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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

CS5211	Computational Number Theory	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Algorithms

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

Mapping of course outcomes with program outcomes

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

Detailed 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 andisomorphisms, 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; Subexponential-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.

Reading:

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

CS5212	Mathematical Models for Internet	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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

CS5213	Cryptanalysis	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Number Theory, Cryptography

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.

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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

CS5214	Computability and Complexity	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Discrete Mathematics, Automata Theory and Algorithms.

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.

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading

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.

CS5215	Information Systems Control and Auditing	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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

CS5216	Probabilistic Algorithms	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Algorithms

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

Mapping of course outcomes with program outcomes

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	

Detailed 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

Reading:

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

CS5221	Biometric Security	Elective	3 – 0 – 0	3 Credits

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.

Mapping of course outcomes with program outcomes

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

Detailed 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,

Reading:

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.

CS5222	Unix Internals	Elective	3 – 0 – 0	3 Credits

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.

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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

CS5223	Secure Software Engineering	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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.

CS5224	Secure Cloud Computing	Elective	3 – 0 – 0	3 Credits

Pre-requisites: None

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

CO1	Define Cloud Computing.
CO2	Analyse data outsourcing in cloud
CO3	Identify privacy and security concerns.
CO4	Develop business models.
CO5	Prove data possession

Mapping of course outcomes with program outcomes

Course Outcomes	PO1	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

Detailed Syllabus

Definition of Cloud computing (NIST): Cloud computing technology components, Cloud services delivery, Cloud varieties, Key drivers for adopting the cloud. Cloud computing models: SaaS, IaaS, PaaS. Secure data outsourcing: Data-in-transit, Data-at-rest, Processing of data, including multitenancy, Data lineage, Data provenance, Data remanence, Infrastructure Security: The Network Level, The Host Level, The Application Level. Trusted computing technology and clouds :Aspects of Data Security, Identity and Access Management, Trust Boundaries and IAM, IAM Challenges& Definitions, IAM Architecture and Practice, Relevant IAM Standards and Protocols for Cloud Services. Virtual machine security. Key Privacy Concerns in the Cloud, Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing. Cloud-centric regulatory compliance issues and mechanisms :Governance, Risk, and Compliance, Benefits of GRC for CSPs, Illustrative Control Objectives for Cloud Computing.

Applications of secure cloud computing: Security Management in the Cloud, Security Vulnerability, Patch, and Configuration Management. Business and security risk models: Key Privacy Concerns in the Cloud, Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing. Query on encrypted data; Proof of data possession / retrievability.

Reading:

1. Anthony T Velte, Toby J Velte, Robert Elsenpeter, *Cloud Computing: A Practical Approach*, MGH, 2011
2. Gautam Shroff, *Enterprise Cloud Computing*, Cambridge University Press, 2010
3. Ronald Krutz and Russell Dean Vines, *Cloud Security*, 1st Edition, Wiley, 2010
4. Tim Mather, SubraKumaraswamy, and ShahedLatif, *Cloud Security and Privacy*, O'Reilly Publication, 2009

CS5225	Algorithmic Game Theory	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Advance Algorithms

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

Mapping of course outcomes with program outcomes

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

Detailed 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,

Reading:

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.

CS5226	Digital Video Processing	Elective	3 – 0 – 0	3 Credits

Pre-requisites: none

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

CO1	Identify different video acquisition and representation methods.
CO2	Analyze 3D reconstruction techniques
CO3	Identify different techniques of video watermarking
CO4	Apply video surveillance procedure
CO5	Analyze different content based video retrieval mechanisms

Mapping of course outcomes with program outcomes

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

Detailed Syllabus

Introduction – Introduction to digital image and video processing, Basic Image Processing techniques – basic gray level and binary image processing, basic tools for Image Fourier analysis; Image and Video Enhancement and Restoration – Linear filtering, Non-linear filtering, morphological filtering, Wavelet denoising for image enhancement, basic methods for image restoration and identification, regularization, multichannel image recovery, multiframe and iterative image restoration, motion detection and estimation; Reconstruction from Multiple Image – 3-D shape reconstruction from multiple views, image sequence stabilization, mozaicking, and super resolution; Image and Video Analysis – Image representation and image models, Image and Video classification and segmentation, multiband stechniques for texture classification and segmentation, adaptive and neural methods for image segmentation, edge and boundary detection, Algorithms for image processing; Image Compression – lossless coding, block truncation coding, fundamentals of vector quantization, wavelet image compression, JPEG lossy image compression standard, JPEG lossless image compression standard, multispectral image coding; Video Compression – basic concepts and techniques of video coding and the H.261 Standard, spatiotemporal subband/Wavelet Video Compression, Object-based video coding, MPEG-1 and MPEG-2 Standard, Emerging MPEG Standards: MPEG-4 and MPEG-7*; Image and Video Acquisition – Image scanning sampling and interpolation, video sampling and interpolation; Image and Video Rendering and Assessment – Image quantization, halftoning and printing, perceptual criteria for image quality evaluation; Image and Video Storage, Retrieval and Communication – Image and Video Indexing and retrieval, A unified framework for Video browsing and retrieval, image and video communication networks, Image watermarking for copyright protection and authentication; Applications of Image Processing – Synthetic aperture radar algorithms, computed tomography, cardiac image processing, computer aided detection for screening mammography, Fingerprint classification and matching, probabilistic view-based and modular models for human face recognition; Human Face Recognition – Confocal Microscopy, Bayesian Automated Target Recognition.

Reading:

1. Alan C Bovik, *Handbook of Image and Video Processing*, 2nd Edition, Academic Press, 2005.
2. Todd R. Reed, *Digital Image Sequence Processing, Compression and Analysis*, CRC Press, 2004.

CS5261	Foundations of Block Chain Technology	Elective	3 – 0 – 0	3 Credits

Pre-requisites: none

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

CO1	Familarize the functional/operational aspects of cryptocurrency ecosystem
CO2	Understand emerging abstract models for Blockchain Technology
CO3	Explore platforms such as Ethereum,Zcash to build applications on blockchain
CO4	Design and implement new ways of using blockchain for applications other than cryptocurrency
CO5	Identify major research challenges and technical gaps between theory and practice in cryptocurrency domain

Mapping of course outcomes with program outcomes

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

Detailed Syllabus

The consensus problem – Asynchronous Byzantine Agreement – AAP protocol and its analysis – Nakamoto Consensus on permission-less, nameless, peer-to-peer network – Abstract models for blockchain – Garay model – RLA Model – Proof of work as random oracle – formal treatment of consistency, liveness and fairness – protocol for Stake based chains – Hybrid models.

Cryptographic basics for cryptocurrency - Overview of hashing, signature schemes, encryption schemes and elliptic curve cryptography

Bitcoin – Wallet – Blocks – Merkle Tree – Hardness of mining – transaction verifiability- anonymity – forks – double spending – mathematical analysis of properties of Bitcoin.

Ethereum – Ethereum Virtual Machine – wallets for Ethereum – Solidarity – Smart Contracts – Attacks on smart contracts. Other applications of Blockchain.

Zero-knowledge proofs and protocols in Blockchain – Succcinctonn-interactive argument for Knowledge (SNARK) – pairing in elliptic curves- Zcash.

Reading:

1. Arvind Narayanan, J. Bonneau, E Felten, A Miller, and S Goldfeder, Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction, Princeton University Press, 2016

2. Relevant Research papers

CS5262	Secure Operating Systems	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Operating Systems

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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

CS5263	Design of Secure Protocols	Elective	3 – 0 – 0	3 Credits

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.

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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.

CS5264	Secure Multiparty Computation	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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

CS5265	Secure Protocols for Electronic Commerce	Elective	3 – 0 – 0	3 Credits

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

Detailed 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

Reading:

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

CS5266	Research study on Information Security	Elective	3 – 0 – 0	3 Credits

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.

Mapping of course outcomes with program outcomes

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

Detailed Syllabus

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

CS5267	Network Coding	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Computer Networks, Algorithms

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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.

CS5268	Public Key Infrastructure and Trust Management	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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.

CS5269	Cyber Laws and Intellectual Property Rights	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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

CS5270	Algorithmic Coding Theory	Core	3 – 0 – 0	3 Credits

Pre-requisites: Advanced Algorithms

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading::

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

CS5271	Digital Forensics	Elective	3 – 0 – 0	3 Credits

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.

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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

CS5272	Secure Dependable and Distributed Computing	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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.

CS5273	Data Hiding	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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

Reading:

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

CS5274	Identity Based Cryptography	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Foundations of Cryptography, AdvancedAlgorithms

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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

CS5275	Information Security Risk Management	Elective	3 – 0 – 0	3 Credits

Pre-requisites: None

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

CO1	Understand risk-planing 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

Mapping of course outcomes with program outcomes

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

Detailed 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;

Reading:

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

CS5276	Privacy Enhancing Technologies	Elective	3 – 0 – 0	3 Credits

Pre-requisites: None

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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.

CS5277	Security of E-Based Systems	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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

CS5278	Secure Group Communications	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Readings:

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.

CS5279	Mobile Security	Elective	3 – 0 – 0	3 Credits

Pre-requisites: None

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

CO1	Understand Normal and Light Weight Cryptography techniques.
CO2	Verify cryptography techniques using Cryptool
CO3	Analyze the security system of mobile phones and mobile communication channels
CO4	Design and develop Mobile Application and mobile website and test their security
CO5	Develop mobile services for mobile governance, mobile payments and social media

Mapping of course outcomes with program outcomes

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

Detailed Syllabus:

Light Weight Cryptography: Security Properties, Access Control Models, Authentication Techniques, Biometrics, Random Number & Key Generation, Hash Functions, Encryption & Decryption, PKI, Signature Generation Schemes, Key agreement protocols, ECC, Block chains, Cryptool.

Mobile Device Security: Internals of Mobile Device, Mobile Security Threats and Vulnerabilities, Mobile Operating systems, Android, SCOSTA, TINY OS, Mobile Databases, SQLITE, SIM / USIM, UICC, Micro SD-Card, Wafers, Security Library Functions, User Interfaces, Sensors, Location & Localization service security.

Mobile Communication Security: Cellular Communication, Wireless Channels, GSM, Mobile IPV6, Bluetooth, RFID, Wi-Fi, NFC, BLE, SMS, USSD, GPRS, DTMF, IVRS, WAP, 2G,3G,4G,5G, LTE, VOLTE, LTE Advanced, LTE Direct, Wireless LAN and related standards of IEEE / ITU / ETSI / ISO.

Mobile Application Security: Mobile Application Development (MAD) Environment, Application Programming Interface (API), Secure Coding Practices, Mobile Cloud Computing (MCC) & Services, Antivirus, Mobile App Testing, Security Testing Tools and Vetting process, Mobile Forensics, Case Studies of Mobile Banking, Mobile Wallet, M-Commerce & Mobile Governance Applications.

Mobile Web, M-Commerce & Social Media Security: Mobile Website & Mobile Browsers, Cross Platform Development Tools, Identity, privacy, security, trust & reliability measures in social media groups and communities.

Reading:

1. Boudriga, Noureddine, *Security of Mobile Communications*, CRC Press, 2010
2. Schäfer, Günter, *Security in fixed and wireless networks : an introduction to securing data communications*, Wiley, 2003.
3. Lim, Ian.,Hourani, Paul, Coolidge, E. Coleen, *Securing cloud and mobility*, CRC Press, 2013.
4. Jamalipour, Abbas, *The wireless mobile Internet*, John Wiley, 2003.
5. Pashtan, Ariel, *Mobile Web services*, Cambridge University Press,2005.

6. Hu, Wen Chen, Zuo, Yanjun, *Handheld computing for mobile commerce*, Information Science Reference, 2010.

CS5280	Cyber Crime and Information Warfare	Elective	3 – 0 – 0	3 Credits

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.

Mapping of course outcomes with program outcomes

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

Detailed 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

Readings:

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.

CS5281	Cryptography and Game Theory	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Algorithms, 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.

Mapping of course outcomes with program outcomes

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		

Detailed 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).

Reading:

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

CS5282	Malware Analysis	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Algorithms, Discrete Mathematics, 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.

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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.

CS5283	Cyber Security	Elective	3 – 0 – 0	3 Credits

Pre-requisites: Foundations of Cryptography

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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

CS5284	Elliptic Curve Cryptosystems	Elective	3 – 0 – 0	3 Credits

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

Mapping of course outcomes with program outcomes

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

Detailed 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.

Reading:

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.