



UNIVERSITY OF HYDERABAD
School of Computer and Information Sciences
(SCIS)

Jointly with



CR RAO ADVANCED INSTITUTE OF
MATHEMATICS, STATISTICS
AND COMPUTER SCIENCE (AIMSCS)

COURSE CURRICULUM
FOR
M.Tech in
INFORMATION SECURITY
[with “Cyber Security” as Specialized Stream]
(2 Years Full Time Programme)

(May 19, 2018)

Course Structure

Code	Subjects	Credits		
		L	T	P
	Semester - I			
IS01	Mathematical Foundation for Information Security	4	0	0
IS02	Secure Operating System and Computer Organization	3	0	1
IS03	Computer Networks	3	0	1
IS04	Software Engineering and Databases	3	0	1
IS05	Laboratory: Reverse Engineering and Malware Analysis	1	0	2
	Elective-1/Optional core-1	3	0	0/1
Credits	Min:22/Max:23			
	Semester – II			
IS06	Principles and Standards of Information Security	4	0	0
IS07	Security Tools and Technologies	3	0	1
IS08	Computer and Network Security	3	0	1
IS09	Laboratory: Side Channel Analysis	1	0	2
	Elective-2 (*)/Optional core-2	3	0	0/1
	Elective-3//Optional core-3	3	0	0/1
Credits	Min:21/Max:23			
	Semesters – III and IV			
IS10/CS10	Dissertation	18	0	0
Grand Total Credits	61(Min) / 64 (Max)			

IS (Information Security) Electives (BIN)	CS (Cyber Security) Optional Cores (BIN)
IS11 Introduction to Cryptography IS12 Finite Field Theory IS13 Computational Complexity IS14 Statistics and Probability IS15 Coding Theory and Information Theory IS16 Randomized Algorithms IS17 Advanced Cryptography IS18 Machine Learning IS19 Automata, Languages and Computation	CS11 Ethical Hacking & Computer Forensics CS12 Current trends in Web Security CS13 Information System Control and Audit CS14 Cloud Computing and Security CS15 Big Data Security

Syllabus

Semester I:

IS01: Mathematical Foundation for Information Security:

Propositional and predicate calculus, Basic set theory and functions, Mathematical proof , Techniques for specifying and analyzing algorithms, Basic asymptotic complexity and order notation (big-O), Induction, recursion, and recurrences, Introduction to relations, equivalence relations, and order relations, Introduction to graph theory and trees, random number generation, Elementary discrete probability.

Introduction to Number Theory, Pythagorean Triples, Pythagorean Triples and the Unit Circle, Sums of Higher Powers and Fermat's Last Theorem, Divisibility and the Greatest Common Divisor, Linear Equations and the Greatest Common Divisor, Factorization and the Fundamental Theorem of Arithmetic, Congruences: Powers, and Fermat's Little Theorem, Powers, and Euler's Formula., Euler's Phi Function, Prime Numbers: Counting Primes, Mersenne Primes, Mersenne Primes and Perfect Numbers, Powers Modulo m and Successive Squaring, Computing k'th Roots Modulo m, Powers, Roots, and "Unbreakable" Codes, Euler's Phi Function and Sums of Divisors, Powers Modulo p and Primitive Roots, Primitive Roots and Indices, Squares Modulo p, Quadratic Reciprocity, Which Primes Are Sums of Two Squares? Which Numbers Are Sums of Two Squares? The Equation $X^4+Y^4=Z^4$, Pell's Equation, Diophantine Approximation, Diophantine Approximation and Pell's Equation, Cubic Curves and Elliptic Curves, Elliptic Curves With Few Rational Points, Points on Elliptic Curves Modulo p, Defect Bounds and Modularity Patterns, Elliptic Curves and Fermat's Last Theorem

Text Book

- Kenneth H. Rosen, Discrete Mathematics and Its Applications, 7th Edition, McGraw-Hill
- J. Silverman, A Friendly Introduction to Number Theory, Prentice Hall, 1996

IS02 Secure Operating System and Computer Organization:

Number of Credits: 04

Prerequisites of the Course: Basic components of Computers and Operating Systems.

Details of the last revision: New Course (proposed in March 2018)

Objectives of the Course:

Teaching Outcome

1. To understand the computer organization and I/O operation with operating system.
2. To understand the representation of data at the machine level.
3. To understand the security requirements of Operating System.
4. To understand the, Operating System protection principles.
5. To understand the Trusted Operating System concepts.

Learning Outcome

1. Able to understand the basic computer components.
2. Ability to understand the instruction set, instruction formats and addressing modes.
3. Ability to understand the security in standard Operating System.
4. Ability to understand the features of Trusted Operating System.
5. Ability to understand the designing a Secure Operating System.
6. Ability to understand the security policy and security model of Operating System.

Mode of Teaching:

Face-to-face
Tutorials

Course Structure:

UNIT – I

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

UNIT – II

Memory Organization: Memory Hierarchy, Main Memory, Auxiliary Memory, Associate Memory, Cache Memory. Pipeline and Vector Processing: Parallel Processing, Pipelining, Arithmetic Pipeline, Instruction Pipeline, RISC Pipeline, Vector Processing, Array Processors. Multi Processors: Characteristics of Multiprocessors, Interconnection Structures, Interprocessor arbitration, Inter processor communication and synchronization.

UNIT – III

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

UNIT – IV

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

UNIT – V

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

Text Books

1. Computer System Architecture, M. Morris Mano, 3rd edition, Pearson, 2007.
2. Building a Secure Computer System, Morrie Gasser, 1st edition, Van Nostrand Reinhold, 1988.

3. Operating Systems Security, Michael Palmer, 4th edition, Thomson course Technology, 2006.

Reference Books

1. Computer Organization and Architecture, William Stallings, 9th edition, Pearson, 2012
2. Computer Organization and Design – The Hardware / Software Interface, David A. Patterson, John L. Hennessy, 4th Edition, Elsevier, 2009.
3. Software Security Engineering, Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead, 1st Edition ,Addison-Wesley Professional,2008.
4. Security Engineering: A Guide to Building Dependable Distributed Systems, Ross J Anderson, 2nd edition, Wiley, 2008.5
5. Operating System Security, Trent Jaeger, 1st Edition, Morgan & Claypool, 2008
6. A Provably Secure Operating System, P.G Neumann (PI), Final Report published by Stanford Research Institute, California, US.

IS03 Computer Networks

Introduction, OSI 7-layer architecture, Data Link Layers, Framing, error detection, Elementary Data Link Protocols.Sliding Window Protocols.Protocol Specification and Verification. Example Data Link Protocols, Retransmission Algorithms, Multiple access & Aloha, Stabilized Aloha, Tree Algorithms, Media Access Sub Layer: The Channel Allocation Problem. Multiple Access Protocols. IEEE Standard 802 for LANS and MANS, CSMA, CSMA/CD and Ethernet, High-speed LANs, Token rings, High Speed Switch Scheduling,Broadcast routing & Spanning trees, Shortest path routing , Distributed routing algorithms, optimal routing, Flow Control, Transport layer and TCP/IP, Optical Networks, Wireless networks, Internetworking and Routing: Packet Switching, A Simple Network Architecture, The Internetworking Problem: The IP/TCP Split Connections, Scaling IP, Routers: Forwarding and Routing, The IP Forwarding Path, Unicast Internet Routing: Intra- and Inter-Domain Routing, Router Design and Implementation, IPv6, Communication and Network Services: P2P Networks, Distributed Hash Table (DHT) Abstraction and AlgorithmsDNS, Resource Discovery, Other Examples of Lookups, The Socket Interface, Electronic Mail Representation and Transfer File Transfer and Remote File Access, Technology for Active Web Documents, RPC and Middleware, Network Management-SNMP, Wireless Protocols: MAC Protocols, Routing, Data Transport and Sensor Data Dissemination (Cross-Layer Protocols)

Text book:

- Andrew S. Tanenbaum, *Computer Networks*, Fourth Edition, Pearson Education 2006 (ISBN 0-13-349945-6).
- William Stallings, *Computer Networking with Internet Protocols and Technology*, Pearson Education 2004.

IS04 Software Engineering and Databases

Modern database technology provides a rich set of functionality that is able to meet several requirements of software engineering applications in a satisfactory manner.

Measurement and evaluation of the software development process, collection of detailed software engineering data, describing all facets of the development process, and the archival of this data for future use, maintaining an online database for the storage and retrieval of software engineering data. DBMS architecture and associated processes and physical files, covering general concepts such as design, deployment and operation; data modeling, database design, management concepts and SQL3. managing a database, data security and integrity measures, access privileges.

Text Books

- Roger S. Pressman, (2005). *Software Engineering: A Practitioner's Approach* (6th ed.). Boston, Mass: McGraw-Hill. ISBN 0072853182
- Ian Sommerville, (2007) [1982]. *Software Engineering* (8th ed.). Harlow, England: Pearson Education. ISBN 0-321-31379-8.
- P. Beynon-Davies, (2004). *Database Systems*. 3rd Edition. Palgrave, Houndmills, Basingstoke.
- C. J. Date, (2003). *An Introduction to Database Systems, Fifth Edition*. Addison Wesley. ISBN 0-201-51381-1.
- David M. Kroenke and David J. Auer. *Database Concepts*. 3rd ed. New York: Prentice, 2007.
- AviSilberschatz, Henry F. Korth, S. Sudarshan, *Database System Concepts*, McGraw-Hill

IS05 Laboratory: Reverse Engineering and Malware Analysis

Semester II:

IS06 Principles and Standards of Information Security

Security Overview, Authentication, Attacks and Malicious Code, Remote Access, E-Mail, Web Security, Directory and File Transfer Services, Wireless and Instant Messaging, Network Security Topologies, Intrusion Detection, Security Baselines, Cryptography, Physical Security, Disaster Recovery and Business Continuity, Computer Forensics, Steganography and Advanced Topics.

BS 7799 British Standard for Information Security Management, Common Criteria for Information Technology Security Evaluation (CC), Intel's Common Data Security Architecture (CDSA), FIPS Pub 140 US Federal Government Standard for Security Requirements for Cryptographic Modules, Internet Security Standards: Internet Protocol (IP) Security, Kerberos, Public Key Cryptography Standards (PKCS), The Directory: Authentication Framework (X.509),

Text Books:

- Boswell, Calvert, Campbell, "Network Security Fundamentals", Cisco Learning Institute, ISBN: 0-619-12017-7 © 2003
- Thomas R. Peltier, Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management, CRC Press; 1st edition (December 20, 2001, ISBN: 0849311373

IS07 Security Tools and Technologies

Securing Information Using Authentication and Access Control: introduction to Access Control, Implementing an Authentication Strategy, Implementing an Access Control Strategy, Cryptography, PKI: Introduction to Certificates, Introduction to Public Key Infrastructure, Deploying and Managing Certificates, Perimeter Security Fundamentals, Packet Filtering: How packet filtering works, Problems with packet filters, Dynamic packet, Stateful firewalls: How stateful firewall works, The concept of a state, Stateful inspection and stateful filtering, Proxy firewalls: Proxy or application gateway firewalls, Protocol issues for proxies, Security policy, Router as a security device, Router hardening, Network Intrusion Detection: The roles of network IDS in a perimeter defence, IDS sensor placement, Virtual Private Networks: Advantages and Disadvantages of VPNs, IPSec basics, Other VPN, protocols PPTP & L2TP, Security protocols & Implementations: SSL/TLS, SSH, PGP, SHTTP, IPSec, Open SSL, Host hardening: Against local attacks, against network attacks, against application attacks, Antivirus solutions and deployment, Software updates and patches.

Text Book

- Jay Ramachandran, Designing Security Architecture Solutions (e-book available), Wiley
- Stephen Northcutt, "Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems", Pearson Education

IS08 Computer and Network Security

Syllabus:

Communications Model: Communications model, data communications tasks; networking, layering and design issues, ISO-OSI model, protocols, services, standards, network goals and applications.

Control hijacking attacks: exploits and defenses, Dealing with legacy code, sandboxing and isolation, Tools for writing robust application code, Principles of least privilege, access control, and operating systems security, Exploitation techniques and fuzzing.

Network Security: Data encryption strategies, authentication protocols.

Security issues in Internet protocols: TCP, DNS, and routing, Network defense tools: Firewalls, VPNs, Intrusion Detection, and filters, Unwanted traffic: denial of service attacks, Malware: Computer viruses, Spyware, and Key-loggers.

Books and References:

1. Keshav, S.: Computer Networks: an Engineering Approach, Addison-Wesley, Reading, 1997.
2. Stallings, W.: Network and Internetwork security, Prentice Hall International 1995.
3. Tanenbaum, A.S.: Computer Networks Third Edition, Prentice Hall of India, 1
4. Bertsekas, D and Gallager, B.: Data Networks, Prentice Hall of India 1992. (2nd Edition)
5. Black, U.D.: TCP/IP and Related Protocols, MacGraw Hill New York 1995.
6. Black, U.D.: Computer Networks, Protocols Standards and Interfaces, Prentice Hall International
7. Comer (includes Comer and Stevens, D.L. three Volumes): Internetworking with TCP/IP Principles protocols and architecture, Prentice Hall of India, 1995.
8. Stallings, W. Data and Computer Communication 5th Edition, Prentice Hall of India, 1997.
9. Stevens, W.R: TCP/IP Illustrated (Three Volumes), Addison-Wesley, Reading, Mass. 1995

IS09 Laboratory: Side Channel Analysis

IS10/CS10 Dissertation

Electives (IS)

IS11 Introduction to Cryptography

No. of Credits: 04

Prerequisites of the course: Discrete Mathematics (Mathematical Foundations for Computer Science), Algorithms

Details of the last revision of the course and approval of the content

Objectives of the course

- i. Teaching outcome: Introduction of the basic cryptographic algorithms and associated mathematical theory. Brief introduction to possible attacks and analysis of naïve algorithms against these attacks will also be discussed.
- ii. Learning outcome: Student should be able to understand the working of basic cryptographic algorithms and analyze them for their cryptographic strength.

Mode of Teaching:

- i. Face-to-face or
- ii. E-learning

Course Structure:

Unit I: Classical symmetric key ciphers: Substitution ciphers: Mono-alphabetic ciphers: additive ciphers, multiplicative ciphers, affine ciphers, key phrase ciphers, etc; Poly-alphabetic ciphers: Playfair cipher, Hill cipher, Vigenere cipher, one-time pad, etc.; Transposition ciphers; Stream ciphers and Block ciphers; Types of Cryptanalytic attacks: Cipher-text only attack, Known plaintext attack, Chosen plaintext attack, Brute force attack, Statistical analysis: Analysis of the above mentioned ciphers against these attacks.

Unit II: Mathematics of Cryptography: Division Algorithm, GCD, Euclidean algorithm, Modular arithmetic, Multiplicative inverse, Groups, Rings, Fields, Finite Fields, Polynomial arithmetic over finite fields

Unit III: Feistel structure, DES, importance of round key, Block cipher modes of operation, Double DES, Attacks on Double DES, Triple DES, RC5, etc.

Unit IV: Introduction to Number Theory, Prime numbers, Fermat and Euler theorems, primality testing, Chinese remainder theorem, primitive root, discrete logarithm problem, Diffie – Hellman Key exchange, RSA.

Unit V: Hash Functions, Message Authentication Code (MAC), Cryptographic Hash Functions, Secure Hash Algorithm (SHA), etc.

Text Books

1. William Stallings, Cryptography and Network Security: Principles and Practices, 6th Edition, Pearson Publication, 2013.
2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, 2nd Edition, Tata McGraw Hill Education Private Limited, 2011.

Reference Books

1. R. Stinson, Cryptography: Theory and Practice, 3rd Edition, Chapman & Hall / CRC, 2005.
2. A Das and C E Venimadhavan; Public Key Cryptography: Theory and Practice, 1 Edition, Pearson Education Inc, 2009.

IS14 Statistics and Probability

No. of Credits: 03

Prerequisites of the course: Prior knowledge of the Counting aspects of Discrete Mathematics is desirable

Details of the last revision of the course and approval of the content

Objectives of the course

- iii. Teaching outcome: Introduce (i) various measures of statistics such as measures of central tendency, measures of dispersion, moments, etc.(ii) discuss correlation, regression, measures of correlation, correlation analysis, least squares fit, etc. (iii) discuss basics of probability such as probability, conditional probability, Bayes theorem, random variables, probability distributions such as Binomial distribution, Normal distribution, Poisson distribution, etc. (iv) discuss testing of hypothesis
- iv. Learning outcome: Student should be able to understand and apply the statistical measures, should be able to compute various probabilities, apply Bayes theorem, understand and be able to apply the results of distributions, and should be able to test a given hypothesis.

Mode of Teaching:

- iii. Face-to-face or
- iv. E-learning

Course Structure:

Unit I: (i) Measures of Central Tendency: Arithmetic mean, Median, Quartiles, Deciles, Percentiles, the mode, geometric mean (ii) Measures of dispersion: the range, quartile deviation,

mean deviation, coefficient of mean deviation, standard deviation, variance, coefficient of variation

Unit II: Moments, moments about the mean, skewness, kurtosis

Unit III: Correlation and Regression: correlation, degree of correlation, causation of correlation, simple and multiple linear regression, Karl-Pearson's coefficient of correlation, multiple correlation analysis

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

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

Text Books

1. Douglas C Montgomery and George C Runger, Applied Statistics and Probability for Engineers, 5th Edition, John Wiley & Sons, 2010
2. Walter A Rosenkrantz, Introduction to Probability and Statistics for Science, Engineering, and Finance, 1st Edition, Chapman and Hall / CRC, 2008.

Reference Books

1. William Feller, An Introduction to Probability Theory and its Applications, 3rd Edition, Wiley, 1968.
2. Robert V Hogg, Joseph McKean, Allen T Craig, Introduction to Mathematical Statistics, 7th Edition, Pearson Education, 2012.

IS19 Automata Languages and Computation

Course Number: IS19

No. of Credits: 03

Prerequisites of the course: Understanding of Programming.

Details of the last revision of the course and approval of the content: New Course.

Objectives of the course:

- i. **Teaching outcome:**
 - Introduces basic Finite state machines and relates them to languages.
 - Explains about Turing Machines and their relation to computation.
 - Deals with various classes such as P, NP, NPH, NPC etc, and introduces complexity theory.
- ii. **Learning outcome:** The student should be able to identify

- Relation between languages and problems.
- Regular Languages, Context Free Languages etc.
- Difficulty in solving a given problem by relating it various classes.

Mode of Teaching:

i. Face-to- face

Course Structure:

UNIT I

Alphabets, Strings, Languages, Finite Automata , Deterministic Finite Automata , Nondeterministic Finite Automata, Equivalence of Deterministic and Nondeterministic Finite Automata, Finite Automata With Epsilon-Transitions , Regular Expressions and Languages, Properties of Regular Languages, Properties of Regular Languages, Context-Free Grammars, Parse Trees, Ambiguity in Grammars and Languages, Pushdown Automata, The Languages of a PDA

UNIT II

Equivalence of PDA and CFG, Deterministic Pushdown Automata, Properties of Context-Free Languages

UNIT III

The Turing Machine, Programming Techniques for Turing Machines, Extensions to the Basic Turing Machine, Restricted Turing Machines, Turing Machines and Computers,

UNIT IV

Undecidability, Recursively Enumerable, Recursive languages, Intractable Problems, The Classes P and NP, An NP-Complete Problem, Additional Classes of Problems

Reference Books

1. Introduction to Automata Theory, Languages, and Computation by John E. Hopcroft, Rajeev Motwani, Jeffrey Ullman, 3rd Edition, Pearson, 2006.

2. Introduction to the Theory of Computation by Michael Sipser, 1st Edition, Thomson, 1996.

3. Introduction to Computer Theory, Daniel A Cohen, 2nd Edition, Wiley , 2007.

Optional Cores (CS)

CS12 Current Trends in Web Security

No. of Credits: 03/01

Prerequisites of the course: Basics of Operating System and Web Technology.

Details of the last revision of the course and approval of the content: New Course.

Objectives of the course:

- i. **Teaching outcome:**
 - Importance of Security, Vulnerabilities in the Web and various Intrusion Detection Systems.
 - Some cryptographic techniques, architecture of Block ciphers and Stream Ciphers, Hash functions.
 - Different attacks in the web –Trojans, worms and virus.
 - Web security via firewalls, etc.,
- ii. **Learning outcome:** The student should be able to understand the various threats that the prevalent in the internet and different counter measures that have been developed to safeguard the systems form them.

Mode of Teaching:

- i. Face-to- face
- ii. Tutorials

Course Structure:

UNIT I

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

UNIT II

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

UNIT III

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

UNIT IV

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

UNIT V

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

Text Books

1. Chwan-Hwa Wu, J. David Irwin, Introduction to Computer Networks and Cyber Security, 1st Edition, CRC Press, 2017.
2. William Stallings, Cryptography and Network Security: Principles and Practices, 6th Edition, Pearson Publication, 2013.
3. Hanqing Wu, Liz Zhao, Web Security: A Whitehat Perspective, Auerbach Publications, 1st Edition, CRC Press, 2015.

Reference Books

1. James Graham, Ryan Olson, Rick Howard, Cyber security essentials, 1st Edition, Auerbach Publications, 2016.
2. Hanqing Wu, Liz Zhao, Web security: A White cat perspective, 1st Edition, Auerbach Publications, 2015.
3. Peter W.Singer, Allan Friedman, Cyber security and cyber war, Oxford University Press India, 2014.

CS13 Information Systems Control and Audit

No. of Credits: 03/01

Prerequisites of the course: Basic concepts of Information Systems.

Details of the last revision of the course and approval of the content: New Course.

Objectives of the course:

Teaching outcome:

1. An overview of Information Systems (IS) security, audit and control function.
2. Threats, attacks and security technology measures.
3. Legal, ethical and professional issues.
4. Planning for security.

Learning outcome:

1. Examine the multiple layers of IS security in organizations.
2. Analyze the risk management approach to information assets' security with respect to operational and organizational goals.
3. Evaluate physical and logical security controls, and the automated approaches in IS security.

Mode of Teaching:

- i. Face-to- face
- ii. Tutorials

Course Structure:**UNIT- I**

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

UNIT- II

The Management Control Framework, Security Management Controls: Conducting a Security Program, Major security Threats and remedial measures, Controls of last resort. Operations management Controls: Computer Operations, Network operations, data preparation and entry, Production control, File library, Management of outsourced operations, Application Control Framework Boundary Controls: Cryptographic controls and audit, access controls and audit, Personal identification numbers, digital signatures. Input Controls: Data input methods, Source document design, data entry screen design, data code controls, check digits, batch controls, validation of input data, instruction input, validation of instruction input. Communication Controls: Communication subsystem exposures, physical component controls, line error controls, flow controls, link controls, topological controls, channel access controls, controls over subversive controls.

UNIT-III

The Application Control Framework , Processing Controls: Processor controls, real memory controls, virtual memory controls, operating system integrity, application software controls, audit trail controls and existence controls, Database Controls: Conducting a Security Program, Major security Threats and remedial measures, Controls of last resort. Output Controls: batch output production and distribution controls, batch report design controls, online output production and distribution controls, audit trail controls and existence controls.

UNIT- IV

Evidence Collection: Audit Software : Generalized audit software, industry specific audit software, high level languages, utility software, expert systems, neural network software, specialized audit software, control of audit software, Code Review, Test Data, and Code Comparison, Concurrent Auditing techniques, Interviews, Questionnaires, and Control Flowcharts, Performance Management tools.

UNIT -V

Evidence Evaluation: Evaluating Asset Safeguarding and Data Integrity : Measures of asset safeguarding and data integrity, Audit technology to Assist the evaluation decision ,Cost Effectiveness considerations, Evaluating System Effectiveness: Approaches to measurement of system effectiveness, Types of Evaluations to system Effectiveness, Operational and Technical

Effectiveness objectives ,Evaluating System Efficiency: Performance indices, Indices-Throughput and Utilization, Workload Models.

Text Books

1. Frederick Gallegos, Daniel P. Manson, Sandra Senft, Carol Gonzales ,Information Technology Control and Audit,2nd Edition, Auerbach Publications ,2004.
2. Ron Weber, Information Systems Control and Audit, 1st edition, Pearson Education, 2002.

Reference Books

1. M.Revathy Sriram, Systems Audit, 2nd Edition ,PHI learning, 2013.
2. Jalote, Software Project Management in Practice, 1st Edition, Pearson Education, 2015.
3. Royce, Software Project Management, 1st Edition, Pearson Education, 2002.