SISTER NIVEDITA UNIVERSITY

SYLLABUS

FOR

THREE YEARS BACHELOR OF SCIENCE HONOURS DEGREE COURSE

IN

COMPUTER SCIENCE (CYBER SECURITY)

UNDER

UGC-CBCS SYSTEM

2019

Course Structure

Category	Course name	Code	Credit	Teaching Scheme		
				L	**T**	**P**
Semester – I						
	Digital Electronics	1203211	6	3	1	4
	Introduction to C-Programming	1203212	6	4	0	4
	Mathematics- I	1191111	4	3	1	0
	Generic Elective	*	4	3	1	0
	Communicative English	1216115	2	2	0	0
	Mentored Seminar – I	1207311	1	1	0	0
	Foreign Language – I (German /Spanish /Japanese)	1278111/ 1278112/ 1278113	2	2	0	0
Total Credit = 25				Teaching Hour = 29		
Semester – II						
	Computer Architecture	1201221	6	3	1	4
	Data Structures with Python	1201222	6	4	0	4
	Mathematics II	1192121	4	3	1	0
	Generic Elective	*	4	3	1	0
	Environmental Science	1154121	2	2	0	0
	Mentored Seminar – II	1205121	1	1	0	0
	Foreign Language – II (German /Spanish /Japanese)	1276121/ 1276122/ 1276123	2	2	0	0
Total Credit = 25				Teaching Hour = 29		
Semester – III						
	Information theory and coding	1203131	4	3	1	0
	Database Management System	1203231	6	4	0	4
	Operating System& System Programming	1203232	6	3	1	4
	Generic Elective	*	4	3	1	0
Total Credit = 20				Teaching Hour = 24		
Semester – IV						
	Blockchain	1203241	6	3	1	4
	Application and System Security	1203142	4	3	1	0
	Cyber Crimes and Legal Framework	1203143	4	3	1	0
	Information Security and Cryptography	1203244	6	3	1	4
Total Credit = 20				Teaching Hour = 20		
Semester –V						
	Computer Networks	1203251	6	3	1	4
	Malware Analysis	1203152	4	3	1	0

Security Architecture and Models	1203153	4	3	1	0
Minor Project	1207451	6	0	0	12
Total Credit = 20				**Teaching Hour = 28**	
Semester – VI					
Elective I	1204161	4	3	1	0
Elective II	1204162	4	3	1	0
Project Work II/ Dissertation	1207461	6	0	0	12
Total Credit = 14				**Teaching Hour = 20**	

Elective I

- Cloud Computing
- Mobile & Digital Forensics
- Ethical hacking
- Big Data

Elective II

- Quantum Cryptography
- Mobile Application Security and Penetration Testing
- Online Social Networks and Security
- Deep Learning

Credit Distribution

Name of Department: Cyber Security

Name of the UG program: B.Sc

Duration of program: 6 Semester (3 years)

Head/ In-Charge of the department: Hemanta Dey

Semester	Credit						
	CC	DSE	GE	AECC	SEC	USC	Total/ Sem
1st							25
2nd							25
3rd							20
4th							20
5th							20
6th							14
Total Credit / Course							
Total Credit							**124**

*To be chosen from the List of Electives

CC: Core Courses; **GE**: General Elective; **AECC:** Ability Enhancement Compulsory Course; **SEC**: Skill Enhancement Courses; **DSE**: Discipline Specific Elective; **USC:** University specified course

CORE COURSES (CC)

PAPER NAME: Digital Electronics

UNIT I: Number Systems & Codes (6L)
TOPICS

Decimal Number, Binary Number, Octal Number, Hexadecimal Number, Conversion – Decimal to Binary, Binary to Decimal, Octal to Binary, Binary to Octal, Hexadecimal to Binary, Binary to Hexadecimal, Octal to Binary to Hexadecimal, Hexadecimal to Binary to Octal; Floating Point Number Representation, Conversion of Floating Point Numbers, Binary Arithmetic, 1's and 2's Complement, 9's and 10's Complement, Complement Arithmetic, BCD, BCD addition, BCD subtraction, Weighted Binary codes, Non-weighted codes, Parity checker and generator, Alphanumeric codes

UNIT II: Logic Gates (2L)
TOPICS

OR, AND, NOT, NAND, NOR, Exclusive – OR, Exclusive – NOR, Mixed logic

UNIT III: Boolean Algebra (4L)
TOPICS

Boolean Logic Operations, Basic Law of Boolean Algebra, Demorgan's Theorem, Principle of

Duality

UNIT IV: Minimization Techniques (5L)
TOPICS

Sum of Products, Product of Sums, Karnaugh Map (up to 4 variables)

UNIT V: Multilevel Gate Network (3L)
TOPICS

Implementation of Multilevel Gate Network, Conversion to NAND-NAND and NOR-NOR Gate Networks

UNIT VI: Arithmetic Circuits (5L)
TOPICS

Half Adder, Full Adder, Half Subtractor, Full Subtractor, Carry Look Ahead Adder, 4-Bit Parallel Adder

UNIT VII: Combinational Circuits (5L)
TOPICS

Basic 2-input and 4-input multiplexer, Demultiplexur, Basic binary decoder, BCD to binary converters, Binary

to Gray code converters, Gray code to binary converters, Encoder

UNIT VIII: Sequential Circuits (5L)
TOPICS

Introduction to sequential circuit, Latch, SR Flip Flop, D Flip Flop, T Flip Flop, JK Flip Flop, Master Slave Flip

Flop

UNIT IX: Basics of Counters (2L)
TOPICS

Asynchronous (Ripple or serial) counter, Synchronous (parallel) counter

UNIT X: Basics of Registers (3L)
TOPICS

SISO, SIPO, PISO, PIPO, Universal Registers

Suggested Books:

1. Digital Circuit & Design, Salivahan,VIKAS
2. Digital Design, M. Morris. Mano & Michael D. Ciletti, PEARSON
3. Fundamentals of Digital Circuits; Anand Kumar; PHI
4. Digital Electronics; Tokheim; TMH
5. Digital Electronics; S. Rangnekar; ISTE/EXCEL

PAPER NAME: Introduction to C-Programming

UNIT I: TOPICS	Overview of C: History of C, Importance of C, Structure of a C Program. Elements of C: C character set, identifiers and keywords, Data types, Constants and Variables, Assignment statement, Symbolic constant. Input/output: Unformatted & formatted I/O function in C, Input functions viz. scanf(), getch(), getche(), getchar(), gets(), output functions viz. printf(),putch(), putchar(), puts().
UNIT II: TOPICS	Operators & Expression: Arithmetic, relational, logical, bitwise, unary, assignment, conditional operators and special operators. Arithmetic expressions, evaluation of arithmetic expression, type casting and conversion, operator hierarchy & associativity. Decision making & branching: Decision making with IF statement, IF-ELSE statement, Nested IF statement, ELSE-IF ladder, switch statement, goto statement
UNIT III: TOPICS	Decision making & looping: For, while, and do-while loop, jumps in loops, break, continue statement. Functions: Definition, prototype, passing parameters, recursion. The C Preprocessor.
UNIT IV: TOPICS	Storage classes in C: auto, extern, register and static storage class, their scope, storage, & lifetime. Arrays: Definition, types, initialization, processing an array, passing arrays to functions, Strings & arrays. Pointers: Pointers and address, Pointers and function arguments, Pointers and arrays, Address arithmetic, Character pointer arrays, Pointers and functions, Pointer arrays, Pointers to pointers, Multidimensional arrays, initialization of pointer arrays, Pointer vs. Multi-dimensional arrays, Command-line arguments, Pointer to functions.
UNIT V: TOPICS	Structures and I/O: Basic of structures, Structures and functions, Arrays of structures, Pointers to structures, Self- referential structures, Table lookup, Type of, unions and bit-fields. Input and Output: Standard input and output, formatted output-Print, Variable length argument lists, File access, File descriptor, Low level I/O- Read and Write, Open, Create, Close.

Suggested Books:
1. Programming With C, Gottfried, TMH
2. Practical C Programming,Oualline,SPD/O'REILLY
3. Let us C-YashwantKanetkar.
4. Programming in C- Ashok N Kamthane
5. The C programming Lang., Pearson Ecl – Dennis Ritchie.

PAPER NAME: Computer Architecture

UNIT I: TOPICS:	1.Number Systems – decimal, binary, octal, hexadecimal, alphanumeric representation, 2.Complements – 1's complement, 2' complement, 9's complement, 10' complement, (r-1)'s complement, r's complement, 3. Fixed point representation – Integer representation, arithmetic addition, arithmetic subtraction, overflow, decimal fixed point representation, 4. Floating point representation, 5. IEEE 754 floating point representation
UNIT II: TOPICS:	Computer arithmetic (5L) 1. Addition algorithm of sign magnitude numbers, 2. Subtraction algorithm of sign magnitude numbers, 3. Addition algorithms of signed 2's complement data, 4. Subtraction algorithms of signed 2's complement data, 5. Multiplication algorithm, Booth's algorithm, 6. Division algorithm
UNIT III: TOPICS	Register transfer and micro-operations (5L) 1. Register transfer language, 2. Register transfer, 3. Bus system for registers, 4. Memory transfers– memory read, memory write, 5. Micro operations – register transfer micro operations, arithmeticmicro operations, logic micro operations, shift micro operations, 6. Binary adder, binary adder, subtractor, binary incrementer, arithmetic circuit for arithmetic micro operations, 7. One stage logiccircuit, 8. Selective set, Selective complement, Selective clear, Mask, Insert, Clear
UNIT IV: TOPICS	Basic Computer organization and design (4L) 1. Instruction codes, 2. Direct address, Indirect address & Effective address, 3. List of basiccomputer registers, 4. Computer instructions: memory reference, register reference & input – outputinstructions, 5. Block diagram & brief idea of control unit of basic computer, 6. Instruction cycle
UNIT V: TOPICS	Micro programmed control (2L) 1. Control memory, 2. Address sequencing, 3. Micro program examples
UNIT VI: TOPICS	Central processing unit (5L) 1. General register organization, 2. Stack organization, Register stack, Memory stack, Stackoperations – push & pop, 3. Evaluation of arithmetic expression using stack, 4. Instruction format, 5.Types of CPU organization (single accumulator, general register & stack organization) & example oftheir instructions, 6. Three, two, one & zero address instruction, 7. Definition and example of datatransfer, data manipulation & program control instructions, 8. Basic idea of different typesofinterrupts (external, internal & software interrupts), 9. Difference between RISC & CISC
UNIT VII: TOPICS	Pipeline and vector processing (3L) 1. Parallel processing, 2. Flynn's classification, 3. Pipelining, Example of pipeline, space timediagram, speedup, 4. Basic idea of arithmetic pipeline, example of floating point

addition/ subtractionusing pipeline

UNIT VIII:
TOPICS

Input – output organization (6L)

1. Peripheral devices, 2. Input – output interface, 3. Isolated I/O, Memory mapped I/O, 4.Asynchronous data transfer: strobe & handshaking, 5. Programmed I/O, 6. Interrupt initiated I/O, 7.Basic idea of DMA & DMAC 8. Input – output processor

UNIT IX:
TOPICS

Memory organization (6L)

1. Memory hierarchy, 2. Main memory definition, types of main memory, types of RAM, ROM,difference between SRAM & DRAM, 3. Cache memory, Cache memory mapping – Direct,Associative, Set Associative, 4. CAM, hardware organization of CAM, 5. Virtual memory, mappingusing pages, page fault, mapping using segments, TLB, 6. Auxiliary memory, diagrammaticrepresentation of magnetic disk & hard disk drive, 7. Definitions of seek time, rotational delay,access time, transfer time, latency

Suggested Books:
1. Computer System Architecture, M. Morris Mano, PEARSON
2. Computer Organization & Architecture –Designing For Performance, William Stallings, PEARSON
3. Computer Architecture & Organisation, J.P. Hayes, TATA MCGRAW HILL
4. Computer Organization and Architecture, T. K. Ghosh, TATA MCGRAW-HILL
5. Computer Architecture, BehroozParhami, OXFORD UNIVERSITY PRESS

PAPER NAME: Data Structure with Python

UNIT I:
TOPICS

Introduction to Python (12L)

Introduction to Python

Python variables, expressions, statements:
Variables,Keywords,Operators&operands,Expressions , Statements, Orderof operations, String operations, Comments, Keyboard input, Example programs

Functions: Type conversion function, Math functions, Composition of functions, Defining own function, parameters, arguments, Importing functions, Example programs

UNIT II:
TOPICS

Conditions & Iterations (8L)

Conditions: Modulus operator, Boolean expression, Logical operators, if, if-else, if-elif-else, Nested conditions, Example programs.

 Iteration: while, for, break, continue, Nested loop, Example programs

UNIT III:
TOPICS

Recursion, Strings, List, Dictionaries, Tuples

Recursion:Python recursion, Examples of recursive functions, Recursion error, Advantages & disadvantages of recursion

Strings:Accessing values in string, Updating strings, Slicing strings, String methods – upper(), find(), lower(), capitalize(), count(), join(), len(), isalnum(), isalpha(), isdigit(),

islower(),isnumeric(), isspace(), isupper() max(), min(), replace(), split(), 2.5 Example programs

List:Introduction, Traversal, Operations,Slice, Methods, Delete element, Difference between lists and strings.

Dictionaries: Introduction, Brief idea of dictionaries & lists

Tuples: Introduction, Brief idea of lists & tuples, Brief idea of dictionaries & tuples.

UNIT IV: TOPICS	Data Structure using Array (4L) Stack, queue, circular queue, priority queue, dequeue and their operations and applications.
UNIT V: TOPICS	Searching and Sorting (6L) Searching: linear search, Binary search, their comparison, Sorting: insertion sort, Selection sort.Quick sort, Bubble sort Heap sort, Comparison of sorting methods , Analysis of algorithm,complexity using big 'O' notation
UNIT VI: TOPICS	Linked List (4L) Linear link lists, doubly linked lists, stack using linked list, queue using linked list, circular linked listand their operations and applications.
UNIT VII: TOPICS	Trees (5L) Binary trees, binary search trees, representations and operations, thread representations, sequentialrepresentations, B tree , B+ tree,
UNIT VIII: TOPICS	Graphs (5L) Introduction to graphs, Definition, Terminology, Directed, Undirected & Weighted graph, Representation of graphs, Graph Traversal: Depth first search and Breadth first search. SpanningTrees, minimum spanning Tree, Shortest path algorithm
UNIT IX: TOPICS	Hashing (4L) Definition, Hashing functions, Load factor and collision, open addressing (linear probing) andchaining method to avoid collision

Suggested Books:
1. Data Structures and Algorithms in Python, Michael T. Goodrich, Roberto Tamassia, Michael H. Goldwasser
2. Data Structures and Algorithmic Thinking with Python, Narasimha Karumanchi
3. Python Data Structures and Algorithms: Benjamin Baka

PAPER NAME: Information theory and coding

Module 1) Entropy, Relative Entropy, and Mutual Information:

Entropy, Joint Entropy and Conditional Entropy, Relative Entropy and Mutual Information, Chain Rules, Data-Processing Inequality, Fano's Inequality

Module 2) Typical Sequences and Asymptotic Equipartition Property:

Asymptotic Equipartition Property Theorem, Consequences of the AEP: Data Compression, High-Probability Sets and the Typical Set

Module 3) Source Coding and Data Compression:

Kraft Inequality, Huffman Codes, Optimality of Huffman Codes

Module 4) Channel Capacity:

Symmetric Channels, Properties of Channel Capacity, Jointly Typical Sequences, Channel Coding Theorem, Fano's Inequality and the Converse to the Coding Theorem

Module 5) Differential Entropy and Gaussian Channel:

Differential Entropy, AEP for Continuous Random Variables, Properties of Differential Entropy, Relative Entropy, and Mutual Information, Coding Theorem for Gaussian Channels

Module 6) Linear Binary Block Codes:

Introduction, Generator and Parity-Check Matrices, Repetition and Single-Parity-Check Codes, Binary Hamming Codes, Error Detection with Linear Block Codes, Weight Distribution and Minimum Hamming Distance of a Linear Block Code, Hard-decision and Soft-decision Decoding of Linear Block Codes, Cyclic Codes, Parameters of BCH and RS Codes, Interleaved and Concatenated Codes

Module 7) Convolutional Codes:

Encoder Realizations and Classifications, Minimal Encoders, Trellis representation, MLSD and the Viterbi Algorithm, Bit-wise MAP Decoding and the BCJR Algorithm

Text Books :

  Elements of Information Theory by Thomas Cover, Joy Thomas

  Channel Codes: Classical and Modern by William Ryan, Shu Lin

References :

  Information Theory and Reliable Communication by Robert Gallager

---

PAPER NAME: Database management System

UNIT I: Database System Concepts & Architecture: Data Independence, Schemas, Instances,
TOPICS Database Languages, Database System Environments Data Models, Basic Structure of
  Oracle System, Storage Organization in

Oracle.

UNIT II: TOPICS	Data Modelling: Use of High –level Conceptual Data Models, ER Diagrams, Subclasses, Superclasses and
	Inheritance, Specialization & Generalization, Conceptual Object Modeling using UML ClassDiagrams, Knowledge Representation Concepts, Exercises.
UNIT III: TOPICS	Relational Data Model: Relational constraints, domain constraints, key constraints referential integrity Constraints, relational algebra, fundamental operations of relational algebra & their Implementation, interdependence of operations, example queries.
UNIT IV: TOPICS	ER and EER to Relational Mapping: Mapping EER model concepts to relation, tuple relational calculus, domain relational Calculus queries.
UNIT V: TOPICS	Database Design: Functional dependencies, irreducible sets of dependencies, loss less decomposition, 1st, 2nd & 3rd NF, dependency preservation, Boyce Codd NF, Multivalued Dependency & 4th NF, join Dependency & 5 NF, domain key normal form, restriction –union normal form, Denormalization.
UNIT VI: TOPICS	Query Processing And Optimization: SQL Basic Queries in SQL, Sub queries, Retrieving a Query Plan – Table Space Span & I/O, Index Scan, Equal Unique Index Lookup, Clustered vs. Non Clustered Indexing, Index Only Scan, Methods for Joining Tables –Nested Loop Join Merge Join, Hybrid Join, Multiple table Join, Transforming Nested Queries to Joins, Object Relational SQL, Procedural SQL, Introduction to Embedded SQL.
UNIT VII: TOPICS	Transaction: Schedules, Serializability, Precedence Graph, Concurrency Control Techniques, Implementation of Transaction in Programs, Cursors and Transaction, Dynamic SQL, Locking Levels of Isolation, Recovery, Checkpoints.

Suggested Books:
1. Fundamental of Database Systems- Elmasri Navathe- Pearson Education Asia
2. Database- Principles, Programming and Performance- Parick O' Neil Elizabeth O'Niel, Harcort Asia PTE Limited
3. An Introduction to Database Systems- C.J.Date, Addison Wesley, Pearson EducationPress
4. Database System Concepts- Abraham Silberschat, Henry F. Korth, S.Sudarshan, Tata McGraw Hill.

PAPER NAME: Operating System & System Programming

UNIT I: TOPICS	Introduction : Importance of OS, Basic concepts and terminology, Types of OS, Different views, Journey of a command execution, Design and implementation of OS
UNIT II: TOPICS	Process : Concept and views, OS view of processes, OS services for process management, Scheduling algorithms, Performance evaluation; Inter-process communication and synchronization, Mutual exclusion, Semaphores, Hardware support for mutual exclusion, Queuing implementation of semaphores, Classical problem of concurrent programming, Critical region and conditional critical region, Monitors,

Messages, Deadlocks

UNIT III:
TOPICS

Storage Management: Memory Management- Backward, Swapping, Contiguous Memory Allocation, Paging, Segmentation, Segmentation with Paging.

UNIT IV:
TOPICS

File-System Interface and Implementation: File Concept, Access Methods, Directory Structure, Protection, File-System Structure, File-System Implementation, Directory Implementation; Allocation Methods, Free-Space Management.

UNIT V:
TOPICS

Mass-Storage Structure: Disk Structure; Disk Scheduling; Disk Management; Swap-Space Management

UNIT VI:
TOPICS

Assemblers: Elements of Assembly Language Programming, Design of the Assembler, Assembler Design Criteria, Types of Assemblers, Two-Pass Assemblers, One-Pass Assemblers, Single pass Assembler for Intel x86 , Algorithm of Single Pass Assembler, Multi-Pass Assemblers

UNIT VII:
TOPICS

Compilers: Causes of Large Semantic Gap, Binding and Binding Times, Data Structure used in Compiling, Scope Rules, Memory Allocation, Compilation of Expression, Compilation of Control Structure, Code Optimization

Suggested Books:
1. Operating Systems, Galvin, John Wiley
2. Operating Systems , Milankovic, TMH
3. An Introduction to Operating System, Bhatt,PHI
4. Modern Operating System, Tannenbaum,PHI
5. Guide to Operating Systems, Palmer, VIKAS
6. Operating Systems, Prasad, Scitech

PAPER NAME: Cyber Crimes and Investigation

Introduction to cybercrime, Data diddling, Data leakage, Eavesdropping, E-mail forgery, E-mail threats, Internet misinformation, Internet terrorism, Password cracking, Round downs, Salami Techniques, Scavenging/Corporate Espionage, Social Engineering, Software Piracy, Spamming, Super zapping, Piggybacking, Trap door, Trojan Horse, Virus, Worm Impersonation, Time bomb, Logic bomb, DOS Attack
Email Hacking& its security ,Social Media Hacking& its Security, Web Hacking& its Security, Mobile Hacking& its Security, Wi-Fi Network Hacking& its Security, Software Hacking, Reverse Engineering Cross site scripting & its Security, Email forgery and E-mail Tracing.
Intrusion Analysis, Intrusion Analysis as a Core Skillset, Methods to Performing Intrusion Analysis, Intrusion Kill Chain, Passively Discovering Activity in Historical Data and Logs, Detecting Future Threat Actions and Capabilities, Denying Access to Threats, Delaying and Degrading Adversary Tactics and Malware, Identifying Intrusion Patterns and Key Indicators

Text Books:
1) Cyber Law Law Of Information Technology And Internet (Lexix Nexis) Anirudh Rastogi
2) Understanding Laws– Cyber Laws And Cyber Crimes (Lexix Nexis)
3) Cyber Crime Manual by Bibhas Chatterjee, Lawman Publication

PAPER NAME: Computer Networks

Module I: (6L)

Definition of computer system, Block Diagram, Components of a computer system, generations of computers, storage devices, Memory Hierarchy, Software, Classification of software, Operating System and its functionalities

Module II: (6L)

Introduction to networking; Data communications: components, data representation (ASCII,ISO etc.), direction of data flow (simplex, half duplex, full duplex); network criteria, physical structure (type of connection, topology), categories of network (LAN, MAN,WAN);

Internet: brief history, Protocols and standards; Reference models: OSI reference model, TCP/IP reference model, their comparative study.

Overview of data(analog & digital), signal(analog & digital), transmission (analog & digital) & transmission media (guided & unguided);

Module III: (8L)

Local Area Networks and data link protocols, point-to-point links and sliding window flow control, CSMA/CD, Ethernet, wireless LAN, cellular networks, and advanced multi-user communication (CDMA, SDMA/MIMO), mobility

Internetworking using TCP/IP: network programming using socket API, network client/server design

Packet/circuit switching and wide-area networks: store-and-forward networks, source routing, virtual/permanent, circuits and call set-up, LAN/WAN addressing, hop-by-hop vs. end-to-end control

Module IV: (10L)

Routing techniques - intra-domain routing (OSPF, RIP), inter-domain policy routing (BGP) and network connectivity

Transport protocols - TCP and UDP, Congestion control, TCP window control, multimedia streaming

High-level network services - DNS, HTTP, SMTP, network management (SNMP), network security

Module V: (10L)

Introduction and history of Internet, WWW, Markup Language: HTML, XML and tags, Scripting Languages, Client-Server Architecture, websites, Internet security and threats, Firewall, Introduction to e-commerce

Text Books:

1. Fundamental of Computers, V.Rajaraman, Prentice Hall India

2. Computer Networks by AS Tanenbaum, Fourth Edition, 2002, Pearson Education

3. Data Communication and Networking by B. Forouzan

4. Data and Communication by W. Stallings

5. Web Technologies: AchyutGodbole, AtulKahate - McGraw Hill

PAPER NAME: Application and System Security

Module I: Introduction.
Protocols and standards, Hypertext Transfer Protocol (HTTP), Markup languages Hypertext Markup Language (HTML), Cascading Style Sheets (CSS).

Module II: Web Application.
Extensible Hypertext Markup Language (XHTML), CGI scripts and clickable maps,
JAVA applets, JAVA servlets, Perl. DHTML, XML, Client-side technologies, JavaScript, Server-side technologies , SQL , PHP.

Module III: Software and System Security.
Control hijacking attacks – buffer overflow, integer overflow, bypassing browser memory protection, Sandboxing and Isolation, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques – program analysis, Privilege, access control, and Operating System Security, Exploitation techniques, and Fuzzing.

Module IV: Network Security & Web Security.
Security Issues in TCP/IP – TCP, DNS, Routing (Topics such as basic problems of security in TCP/IP, IPsec, BGP Security, DNS Cache poisoning etc), Network Defense tools – Firewalls, Intrusion Detection, Filtering, DNSSec, NSec3, Distributed Firewalls, Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients, Web Application Security – Cross Site Scripting Attacks, Cross Site Request Forgery, Https, Threat Modeling, Attack Surfaces.

Module V: Security in Mobile Platforms.
Android security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection

Module VI: Introduction to Hardware Security, Supply Chain Security.
Threats of Hardware Trojans and Supply Chain Security, Side Channel Analysis based Threats, and attacks.

Text Books:
1. Principles of Computer Security: W.A.Coklin, G.White, Fourth Edition, McGrawHill

2. Cryptography and Network Security Principles and Practices*, William Stallings, Seventh Edition, Pearson*
3. Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing
Achyut S. Godbole, Tata McGraw-Hill Education, 2013

PAPER NAME: Information Security & Cryptography

Information Security: Introduction, History of Information security, What is Security, CNSS Security Model, Components of Information System, Balancing Information Security and Access, Approaches to Information Security Implementation, The Security Systems Development Life Cycle.

Cryptography: Concepts and Techniques, symmetric and asymmetric key cryptography, steganography, Symmetric key Ciphers: DES structure, DES Analysis, Security of DES, variants of DES, Block cipher modes of operation , AES structure, Analysis of AES , Key distribution Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Analysis of RSA, Diffie-Hellman Key exchange

Message Authentication and Hash Functions: Authentication requirements and functions, MAC and Hash Funtions, MAC Algorithms: Secure Hash Algorithm, Whirlpool, HMAC, Digital signatures, X.509, Kerberos UNIT – IV Security at layers(Network, Transport, Application): IPSec, Secure Socket Layer(SSL), Transport Layer Security(TLS), Secure Electronic Transaction(SET), Pretty Good Privacy(PGP), S/MIME

Inruders, Virus and Firewalls: Intruders, Intrusion detection, password management, Virus and related threats, Countermeasures, Firewall design principles, Types of firewalls

Introduction to Cryptoanalysis: Linear Cryptanalysis, Differential Cryptanalysis, Cryptanalysis of DLP

Cryptography Lab:

1) Perform Basic Encryption/Decryption (Text only)..
2) Diffie-Hellman key exchange and symmetric key cryptography.
3) Public key cryptography using RSA.
4) Implementing Private Key cryptography.
5) Perform Basic Encryption/Decryption
6) Perform Basic Hash Functions (Like MD4, MD5 etc.).
7) Perform Basic Fractal functions (Like Julia set etc.)
8) Generate Asymmetric Key Pair.
9) Generate Web Certificate from Key Pair.
10) Run Secure Web Server Using Web Certificate.
11) An Application on Watermarking Technique.

Text Books:

1. Principles of Information Security : Michael E. Whitman, Herbert J. Mattord, CENGAGE Learning, 4th Edition.
2. Cryptography and Network Security : William Stallings, Pearson Education,4th Edition
3. Cryptography and Network Security : Forouzan Mukhopadhyay, Mc Graw Hill, 2nd Edition

PAPER NAME: Malware Analysis

Introduction: Computer Infection Program- Life cycle of malware- Virus nomenclature- Worm nomenclature- Tools used in computer virology. Implementation of Covert Channel Non self-reproducing Malware- Working principle of Trojan Horse- Implementation of Remote access and file transfer- Working principle of Logical Bomb-Case Study: Conflicker C worm.

Virus Design And Its Implications :Virus components- Function of replicator, concealer and dispatcher- Trigger Mechanisms- Testing virus codes- Case Study: Brute force logical bomb.

Malware Design Using Open Source :Computer Virus in Interpreted programming language- Designing Shell bash virus under Linux- Fighting over infection- Anti –antiviral fighting – Polymorphism- Case study: Companion virus.

Virus And Worm Analysys Klez Virus- Clone Virus- Doom Virus- Black wolf worm- Sassar worm- Happy worm 99.

TEXT BOOKS:

1. ErciFiliol, "Computer Viruses: from theory to applications", Springer, 1st edition, 2005
2. Mark.A .Ludwig, "The Giant black book of computer viruses,CreateSpace Independent Publishing Platform, 2 nd edition, 2009,ISBN 10: 144140712X

PAPER NAME: Security Architecture and Models

Module I: Security Architecture And Information.
Introduction, History, Information Security, Critical Characteristics of Information, Components of an Information System, Securing the Components, Balancing Security and Access, Need for security, Business needs, Threats, Attacks, Legal, Ethical and Professional Issues.

Module II: Logical design and physical design.
Blueprint for security, Information Security policy, NIST Models, VISA International security model, Design of Security Architecture, Planning for continuity, Security Technology, IDS, Crytography, Access Control Devices, Physical Security, Security and Personnel.

Module III: Low-level architecture.
Security Assessments, Security Architecture Basics, Architecture Patterns in Security, Cryptography, Trusted Code, Secure Communications.

Module IV: Mid-level architecture.
Middleware Security, Web Security, Application and OS Security, Database Security.

Module V: High-level architecture.
Security Components, Security and Other Architectural Goals, Enterprise Security Architecture.

Module VI: Business cases and security.
Business Cases for Security.

PAPER NAME: Cloud Computing
Introduction: Cloud computing definition, reference model, Characteristics, Benefits,
Challenges, Distributed Systems, Virtualization, Service-oriented computing, Utility-oriented computing, Overview on computing platforms & technologies – AWS,Google AppEngine, MS Azure, Hadoop, Saleforce.com, Manjrasoft Aneka
Parallel & Distributed Computing: Parallel vs. Distributed computing, Elements of parallel computing, Parallel processing - hardware architecture & approaches, Concept & Component of Distributed Computing, RPC, Service-oriented computing Virtualization: Cloud reference model

– IaaS, PaaS, SaaS, Types of clouds – Public,Private, Hybrid, Community, Cloud interoperability & standards, scalability & fault tolerance, Security, trust & privacy

Concurrent Computing, High-throughput Computing and Data-Intensive Computing:Programming applications with Threads, Thread API, Parallel computation with Threads,Task computing, Frameworks for Task computing, Task-based application model,

Data-intensive computing, characteristics, technology Cloud Platforms and Applications: Overview on Amazon Web Services, Google AppEngine and Microsoft Azure, Cloud applications in scientific, business and consumer Domain

Text Books:
1. Buyya, Vecciola and Selvi, Mastering Cloud Computing: Foundations and Applications Programming, Tata McGraw Hill
2. Rittinghouse and Ransome, Cloud Computing: Implementation, Management, and Security, CRC Press
3. Aravind Doss, Cloud Computing, Tata McGraw Hill
4. Kris Jamsa, Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More, Jones & Bartlett Learning

---

PAPER NAME: Mobile & Digital Forensics

Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.

CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues

Mobile phone forensics: crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques

Digital forensics: Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contaminationUnit V (8 hours) Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locationsSeven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context

Text Books:
1. Gregory Kipper, "Wireless Crime and Forensic Investigation", Auerbach Publications, 2007
2. Iosif I. Androulidakis, " Mobile phone security and forensics: A practical approach", Springer publications, 2012

3. Andrew Hoog, " Android Forensics: Investigation, Analysis and Mobile Security for Google Android", Elsevier publications, 2011
4. Angus M.Marshall, " Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008

PAPER NAME: Penetration Testing & Vulnerability Assessment

Introduction Ethical Hacking terminology- Five stages of hacking- Vulnerability Research- Legal implication of hackingImpact of hacking.
Foot printing & Social engineering Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks.
Scanning & Enumeration Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS FingerprintingEnumeration.
System Hacking Password cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.
Sniffers & SQL Injection Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS Spoofing- Conduct SQL Injection attack - Countermeasures.

TEXT BOOKS:
1. Kimberly Graves, "CEH: Official Certified Ethical Hacker Review Guide", Wiley Publishing Inc., 2007. ISBN: 978-0-7821-4437-6.
2. Shakeel Ali &TediHeriyanto, "Backtrack -4: Assuring security by penetration testing", PACKT Publishing., 2011. ISBN: 978-1-849513-94-4.

PAPER NAME: Risk Management

Module I: Introduction to Information Risk Management. [9L]
Introduction to Risk Management, The Business Risk Model, Information and Technology Risk Management, Identifying IT Risks and Controls, Risk Information Processes, Assessing and Mitigating Risk at the Process Level, Managing Project Risk.
Module II: Introduction to Risk Assessments and Risk Semantics. [7L]
Assessing Information Risks and Controls, A Framework for Assessing IT Risks, The Role of IT Audit and Risk Assessments, IT Governance, Non-Technical Security Risks, The Risks Caused by People – Social Engineering & Behavioral Security.
Module III: Risk Issues in IT and Telecommunication. [9L]
The Risks of Connectivity, Risks Surrounding IT and Telecommunication Networks, Organizational Network and Application Security, Internet & Host Security, Firewalls & VPNs, IT Fraud in Organizations, Cyber Crime and Terrorism, Digital and Computer Forensics.
Module IV: Security Management. [6L]
Information Security Management, Corporate Security Policy, The Ongoing Management of Information Security, Measuring Security, Incident Response.
Module V: Incident Analysis. [4L]

Introduction, Log analysis, Event criticality, General log configuration and maintenance, Live Incident Response, Timelines, Other forensics topics

Text Books:

1. Manish Agrawal, Alex Campoe and Eric Pierce, "Information Security and IT Risk Management", Wiley.
2. Michael E. Whitman, "Principles of Information Security", Cengage Learning.

PAPER NAME: Hardware Security

Overview of Different Issues of Hardware Security

Preliminaries: Algebra of Finite Fields, Basics of the Mathematical Theory of Public Key Cryptography, Basics of Digital Design on Field-programmable Gate Array (FPGA), Classification using Support Vector Machines (SVMs)

Useful Hardware Security Primitives: Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA, Physically Unclonable Functions (PUFs), PUF Implementations, PUF Quality Evaluation, Design Techniques to Increase PUF Response Quality

Side-channel Attacks on Cryptographic Hardware: Basic Idea, Current-measurement based Side-channel Attacks (Case Study: Kocher's Attack on DES), Design Techniques to Prevent Side-channel Attacks, Improved Side-channel Attack Algorithms (Template Attack, etc.), Cache Attacks

Testability and Verification of Cryptographic Hardware: Fault-tolerance of Cryptographic Hardware, Fault Attacks, Verification of Finite-field Arithmetic Circuits

Modern IC Design and Manufacturing Practices and Their Implications: Hardware Intellectual Property (IP) Piracy and IC Piracy, Design Techniques to Prevent IP and IC Piracy, Using PUFs to prevent Hardware Piracy, Model Building Attacks on PUFs (Case Study: SVM Modeling of Arbiter PUFs, Genetic Programming based Modeling of Ring Oscillator PUF)

Hardware Trojans: Hardware Trojan Nomenclature and Operating Modes, Countermeasures Such as Design and Manufacturing Techniques to Prevent/Detect Hardware Trojans, Logic Testing and Side-channel Analysis based Techniques for Trojan Detection, Techniques to Increase Testing Sensitivity Infrastructure Security: Impact of Hardware Security Compromise on Public Infrastructure, Defense Techniques (Case Study: Smart-Grid Security)

Text Books:

1. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press

PAPER NAME: BIOMETRIC SECURITY

Introduction to Biometrics, Fingerprint Recognition, Face Recognition, Iris Recognition, Hand Geometry Recognition

Gait Recognition, The Ear as a Biometric, Voice Biometrics, A Palm print Authentication System, and OnLine Signature Verification

3D Face Recognition, Automatic Forensic Dental Identification, Hand Vascular Pattern Technology, Introduction to Multi biometrics, Multispectral Face Recognition

Multi biometrics Using Face and Ear, Incorporating Ancillary Information in Multi biometric Systems, The Law and the Use of Biometrics, Biometric System Security, Spoof Detection Schemes

Linkages between Biometrics and Forensic Science, Biometrics in the Government Sector, Biometrics in the Commercial Sector, Biometrics Standards, Biometrics databases

Text Books:

1. Jain, Anil K.; Flynn, Patrick; Ross, Arun A. (Eds.), Handbook of Biometrics, Springer, 2008.
3. Benjamin Muller, Security, Risk and the Biometric State: Governing Borders and Bodies, 1st Edition, Routledge, 2010.

PAPER NAME: Project – I

PAPER NAME: Project Work II/ Dissertation

To carry out a computer application based project individually or in groups

DISCIPLINE SPECIFIC ELECTIVES (DSE)

DSE – 1: Mathematics –I

UNIT I (10 lectures)

Matrix Algebra- Introduction & definition, properties of matrix, special type of matrices, arithmetic of matrices, symmetric & skew-symmetric matrices, orthogonal matrices, singular and non-singular matrices with their properties, Trace of a matrix, Eigen value and Eigen vector computation, Inverse of a matrix and related properties, numerical problems solving.

UNIT II (10 lectures)

Differential Calculus: Review of limit, continuity and differentiability, L-Hospital rule, Leibnitz rule, successive differentiation, Rolle's theorem, Mean value theorem, Taylor series expansion, Function of several variables, Euler's theorem on homogeneous function, Partial differentiation, Jacobian, Maxima and Minimum of functions of one and two variables.

UNIT III (10 lectures)

Integral Calculus: Review of integration and definite integral. Differentiation under integral sign, double integral, change of order of integration, transformation of variables. Beta and Gamma functions: properties and relationship between them.

UNIT IV (10 lectures)

Differential Equations: Exact differential equations, integrating factors, change of variables, Total differential equations, Differential equations of first order and first degree, Differential equations of first order but not of first degree, Equations solvable for x, y, q, Equations of the first degree in x and y, Clairaut's equations. Higher Order Differential Equations: Linear

differential equations of order n, Homogeneous and non-homogeneous linear differential equations of order n with constant coefficients.

SUGGESTED READING:

- Lay David C: Linear Algebra and its Applications, Addison Wesley, 2000.
- Schaum's Outlines: Linear Algebra, Tata McGraw-Hill Edition, 3rdEdition, 2006.
- Searle S.R: Matrix Algebra Useful for Statistics. John Wiley &Sons., 1982.
- Gorakh Prasad: Differential Calculus, Pothishala Pvt. Ltd., Allahabad (14th Edition - 1997).
- Gorakh Prasad: Integral Calculus, PothishalaPvt. Ltd., Allahabad (14th Edition - 2000).
- David C. Lay: Linear Algebra and Its Applications, 3rd Edn, Pearson Education, Asia.

DSE – 2: Mathematics II

UNIT I (10 lectures)

Theory of equations, statement of the fundamental theorem of algebra and its consequences. Relation between roots and coefficients or any polynomial equations. Solutions of cubic and biquadratic equations when some conditions on roots of equations are given. Evaluation of the symmetric polynomials and roots of cubic and biquadratic equations. Vector spaces, Subspaces, sum of subspaces, Span of a set, Linear dependence and independence, dimension and basis, dimension theorem.

UNIT II (10 lectures)

Algebra of matrices - A review, theorems related to triangular, symmetric and skew symmetric matrices, idempotent matrices, Hermitian and skew Hermitian matrices, orthogonal matrices, singular and non-singular matrices and their properties. Trace of a matrix, unitary, involutory and nilpotent matrices. Adjoint and inverse of a matrix and related properties.

UNIT III (10 lectures)

Determinants of Matrices: Definition, properties and applications of determinants for 3rd and higher orders, evaluation of determinants of order 3 and more using transformations. Symmetric and Skew symmetric determinants. Use of determinants in solution to the system of linear equations, row reduction and echelon forms, the matrix equations AX=B, solution sets of linear equations, linear independence, Applications of linear equations, inverse of a matrix.

UNIT IV (10 lectures)

Rank of a matrix, row-rank, column-rank, standard theorems on ranks, rank of the sum and the product of two matrices. Generalized inverse (concept with illustrations). Partitioning of matrices and simple properties. Characteristic roots and Characteristic vector, Properties of characteristic roots, Cayley Hamilton theorem.

SUGGESTED READINGS:

- Lay David C.: Linear Algebra and its Applications, Addison Wesley, 2000.
- Schaum's Outlines : Linear Algebra, Tata McGraw-Hill Edition, 3[rd]Edition, 2006.
- Krishnamurthy V., Mainra V.P. and Arora J.L.: An Introduction to Linear Algebra (II, III, IV, V).
- Jain P.K. and Khalil Ahmad: Metric Spaces, Narosa Publishing House, New Delhi, 1973
- Biswas, S. (1997): A Textbook of Matrix Algebra, New Age International, 1997.