GANDHI INSTITUTE OF TECHNOLOGY AND MANAGEMENT (GITAM)

(Deemed to be University) (Estd. u/s 3 of the UGC Act, 1956)

VISAKHAPATNAM ★ HYDERABAD ★ BENGALURU

NAAC accredited with 'A+' Grade

REGULATIONS AND SYLLABUS
of
Master of Technology
in
Cyber Forensics and Information Security

(w.e.f 2017-18 admitted batch)

GITAM Committed to Excellence

VISION

To become a global leader in higher education.

MISSION

To impart futuristic and comprehensive education of global standards with a high sense of discipline and social relevance in a serene and invigorating environment.

GANDHI INSTITUTE OF TECHNOLOGY AND MANAGEMENT (GITAM)

(Deemed to be University) (Estd. u/s 3 of the UGC Act, 1956)

VISAKHAPATNAM ★ HYDERABAD ★ BENGALURU

NAAC accredited with 'A+' Grade

REGULATIONS & SYLLABUS

OF

M.Tech. (Cyber Forensics and Information Security)

(w.e.f 2017-18 admitted batch)

GITAM Committed to Excellence

M.Tech. in Cyber Forensics and Information Security
REGULATIONS
(w.e.f. 2017-18 admitted batch)

1. ADMISSION

1.1 Admission into M.Tech. in CFIS program of GITAM is governed by GITAM admission regulations.

2. ELIGIBILITY CRITERIA

2.1
- First class or equivalent grade in the qualifying examination from recognized university with a minimum of 60% aggregate marks and rank obtained in GAT (PGT).
- B.E./B.Tech./AMIE in CSE / IT / ECE / EEE / EI / CSIT or its equivalent.

2.2 Admissions into M.Tech. will be based on the following:

(i) Score obtained in GAT (PG), if conducted.

(ii) Performance in Qualifying Examination / Interview.

2.3 The actual weightage to be given to the above items will be decided by the authorities before the commencement of the academic year. Candidates with valid GATE score shall be exempted from appearing for GAT (PG).

3. CHOICE BASED CREDIT SYSTEM

3.1 Choice Based Credit System (CBCS) is introduced with effect from the admitted Batch of 2015-16 based on UGC guidelines in order to promote:

- Student Centered Learning
- Cafeteria approach
- Students to learn courses of their choice
- Learning at their own pace
- Inter-disciplinary learning

3.2 Learning goals/ objectives and outcomes are specified leading to what a student should be able to do at the end of the program.

4. STRUCTURE OF THE PROGRAM

4.1 The Program Consists of

i) Core Courses (compulsory) which give general exposure to a Student in CFIS and subject related area.

ii) Programme Electives.

iii) Interdisciplinary Electives.

4.2 Each course is assigned a certain number of credits depending upon the number of contact hours (lectures/tutorials/practical) per week.

4.3 In general, credits are assigned to the courses based on the following contact hours per week per semester.

- One credit for each Lecture / Tutorial hour per week.
- One credit for two hours of Practicals per week.
- Two credits for three (or more) hours of Practicals per week.

5. MEDIUM OF INSTRUCTION

The medium of instruction (including examinations and project reports) shall be English.

6. REGISTRATION

Every student has to register himself/herself for each semester individually at the time specified by the Institute / University.

7. ATTENDANCE REQUIREMENTS

7.1 A student whose attendance is less than 75% in all the courses put together in any semester will not be permitted to attend the end - semester examination and he/she will not be allowed to register for subsequent semester of study. He/she has to repeat the semester along with his / her juniors.

7.2 However, the Vice Chancellor on the recommendation of the Principal / Director of the Institute/School may condone the shortage of attendance to the students whose attendance is between 66% and 74% on genuine grounds and on payment of prescribed fee.

8. EVALUATION

8.1 The assessment of the student's performance in a Theory course shall be based on two components: Continuous Evaluation (40 marks) and Semester-end examination (60 marks).

8.2 A student has to secure an aggregate of 40% in the course in the two components put together to be declared to have passed the course, subject to the condition that the candidate must have secured a minimum of 24 marks (i.e. 40%) in the theory component at the semester-end examination.

8.3 Practical/ Project Work/ Industrial Training/ Viva voce/ Seminar etc. course are completely assessed under Continuous Evaluation for a maximum of 100 marks, and a student has to obtain a minimum of 40% to secure Pass Grade. Details of Assessment Procedure are furnished below in Table 1.

Table 1: Assessment Procedure

S.No.	Component of Assessment	Marks Allotted	Type of Assessment	Scheme of Evaluation
1	Theory	40	Continuous Evaluation	i) Thirty (30) marks for mid Semester examinations. Three mid examinations shall be conducted for 15 marks each; performance in best two shall be taken into consideration. ii) Ten (10) marks for Quizzes, Assignments and Presentations.
		60	Semester-end Examination	Sixty (60) marks for Semester-end examinations
	Total	100		
2	Practicals	100	Continuous Evaluation	i) Fifty (50) marks for regularity and performance, records and oral presentations in the laboratory. Weightage for each component shall be announced at the beginning of the Semester. ii) Ten (10) marks for case studies. iii) Forty (40) marks for two tests of 20 marks each (one at the mid-term and the other towards the end of the Semester) conducted by the concerned lab Teacher.
3	Project work (III Semester)	100	Continuous Evaluation	i) Forty (40) marks for periodic evaluation on originality, innovation, sincerity and progress of the work, assessed by the Project Supervisor. ii) Thirty (30) marks for mid-term evaluation for defending the Project, before a panel of examiners. iii) Thirty (30) marks for final Report presentation and Viva-voce, by a panel of examiners
4	Project work (IV Semester)	50	Continuous Evaluation	i) Twenty (20) marks for Periodic evaluation on originality innovation, sincerity and progress of the work, assessed by the Project Supervisor. ii) Fifteen (15) marks for mid-term evaluation for defending the Project, before a panel of examiners*.

		50	Semester-end Examination	iii) Fifteen (15) marks for interim Report presentation and Viva-voce. Fifty (50) marks for final Report presentation and Viva-voce assessed by external examiners.
	Total	100		
5	Technical Seminar	100	Continuous Evaluation	
6	Comprehensive Viva-voce (II Semester)	100	Continuous Evaluation	Through five periodic Viva-voce exams for 20 marks each, conducted by a panel of examiners. The course content for Viva exams shall be announced at the beginning of the Semester.

**Panel of Examiners shall be appointed by the concerned Head of the Department*

9. REAPPEARANCE

9.1 A student who has secured 'F' grade in a Theory course shall have to reappear at the subsequent Semester end examination held for that course.

9.2 A student who has secured 'F' grade in a Practical course shall have to attend Special Instruction Classes held during summer.

9.3 A student who has secured 'F' Grade in Project work / Industrial Training etc shall have to improve his/her report and reappear for Viva – voce at the time of Special Examination to be conducted in the summer vacation.

10. SPECIAL EXAMINATION

10.1 A student who has completed his/her period of study and still has "F" grade in a maximum of three theory courses is eligible to appear for Special Examination normally held during summer vacation.

11. BETTERMENT OF GRADES

A student who has secured only a Pass or Second class and desires to improve his/her Class can appear for Betterment Examinations only in Theory courses of any Semester of his/her choice, conducted in Summer Vacation along with the Special Examinations. Betterment of Grades is permitted 'only once' immediately after completion of the program of study.

12. GRADING SYSTEM

12.1 Based on the student performance during a given semester, a final letter grade will be awarded at the end of the semester in each course. The letter grades and the corresponding grade points are as given in Table 2.

Table 2: Grades & Grade Points

Sl.No.	Grade	Grade Points	Absolute Marks
1	O (outstanding)	10	90 and above
2	A+ (Excellent)	9	80 to 89
3	A (Very Good)	8	70 to 79
4	B+ (Good)	7	60 to 69
5	B (Above Average)	6	50 to 59
6	C (Average)	5	45 to 49
7	P (Pass)	4	40 to 44
8	F (Fail)	0	Less than 40
9	Ab. (Absent)	0	-

12.2 A student who earns a minimum of 4 grade points (P grade) in a course is declared to have successfully completed the course, and is deemed to have earned the credits assigned to that course, subject to securing a GPA of 5 for a Pass in the semester.

13. GRADE POINT AVERAGE

13.1 A Grade Point Average (GPA) for the semester will be calculated according to the formula:

$$\text{GPA} = \frac{\Sigma_i C_i G_i}{\Sigma_i G_i}$$

Where

C_i = number of credits obtained for the ith course
G_i = number of credits obtained for the ith course

13.2 To arrive at Cumulative Grade Point Average (CGPA), a similar formula is used considering the student's performance in all the courses taken, in all the semesters up to the particular point of time.

13.3 CGPA required for classification of class after the successful completion of the program is shown in Table 3.

Table 3: CGPA required for award of Class

Class	CGPA Required
First Class with Distinction	> 8.0*
First Class	> 6.5
Second Class	> 5.5
Pass Class	> 5.0

* In addition to the required CGPA of 8.0 or more, the student must have necessarily passed all the courses of every semester in first attempt.

14. ELIGIBILITY FOR AWARD OF THE M.Tech. DEGREE

14.1 Duration of the program: A student is ordinarily expected to complete the M.Tech. program in four semesters of two years. However a student may complete the program in not more than four years including study period.

14.2 However the above regulation may be relaxed by the Vice Chancellor in individual cases for cogent and sufficient reasons.

14.3 A student shall be eligible for award of the M.Tech. Degree if he / she fulfills all the following conditions.

a) Registered and successfully completed all the courses and projects.

b) Successfully acquired the minimum required credits as specified in the curriculum corresponding to the branch of his/her study within the stipulated time.

c) Has no dues to the Institute, hostels, Libraries, NCC / NSS etc, and

d) No disciplinary action is pending against him / her.

15. DISCRETIONARY POWER

Not withstanding anything contained in the above sections, the Vice Chancellor may review all exceptional cases, and give his decision, which will be final and binding.

M.Tech.in Cyber Forensics and Information Security (CFIS)

Department of Computer Science and Engineering

Effective from academic year 2017-2018 admitted batch

Semester I

S. No.	Course Code	Course Title	Category	L	T	P	C
1	ECS701	Advanced Data Structures & Algorithms	CE	4	0	0	4
2	ECS703	Advanced Operating Systems	CE	4	0	0	4
3	ECS709	Number Theory & Cryptography	CE	4	0	0	4
4	ECS7XX	Program Elective-I	PE(PE)	3	0	0	3
5	ECS7XX	Program Elective-II	PE(PE)	3	0	0	3
6	ECS7XX/ EID7XX	Interdisciplinary Elective-I	IDE	3	0	0	3
7	ECS721	Advanced Data Structures & Algorithms Lab	CE	0	0	3	2
8	ECS727	Network Security & Cryptography Lab	CE	0	0	3	2
							25

Semester II

S. No.	Course Code	Course Title	Category	L	T	P	C
1	ECS702	Advanced Computer Networks	CE	4	0	0	4
2	ECS710	Cyber Forensics	CE	4	0	0	4
3	ECS712	Pragmatics of Information Security	CE	4	0	0	4
4	ECS7XX	Program Elective -III	PE(PE)	3	0	0	3
5	ECS7XX	Program Elective -IV	PE(PE)	3	0	0	3
6	EID7XX/ ECS7XX	Interdisciplinary Elective-II	IDE	3	0	0	3
7	ECS728	Cyber Forensics Lab	CE	0	0	3	2
8	ECS730	IOT Security Lab	CE	0	0	3	2
9	ECS792	Technical Seminar	CE	0	0	3	2
							27

Semester III

S. No.	Course Code	Course Title	Category	L	T	P	C
1	ECS891	Project Work-I	PP(PW)				8
2	ECS893	Comprehensive Viva Voce	CE				2
							10

Semester IV

S. No.	Course Code	Course Title	Category	L	T	P	C
1	ECS892	Project work-II	PP(PW)				14
							14

Number of Credits:

Semester	I	II	III	IV	Total
Credits	25	27	10	14	76

Interdisciplinary Elective - I

S. No.	Course Code	Course Title	Category	L	T	P	C
1.	ECS749	Internet of Things	IDE	3	0	0	3
2.	EID763	Multivariate Techniques for Data Analysis	IDE	3	0	0	3
3.	EID769	Cyber Laws and IT Protection	IDE	3	0	0	3

Interdisciplinary Elective - II

S. No.	Course Code	Course Title	Category	L	T	P	C
1.	ECS751	Service Oriented Architecture	IDE	3	0	0	3
2.	EID760	Programming with R	IDE	3	0	0	3
3.	EID771	Enterprise Cyber Security	IDE	3	0	0	3

PROGRAMME ELECTIVES

Programme Elective-I

S. No.	Course Code	Course Title	Category	L	T	P	C
1	ECS763	Ethical Hacking	PE(PE)	3	0	0	3
2	ECS765	Introduction to Machine Learning	PE(PE)	3	0	0	3
3	ECS767	Steganography	PE(PE)	3	0	0	3

Programme Elective-II

S. No.	Course Code	Course Title	Category	L	T	P	C
1	ECS769	Secure Systems Engineering	PE(PE)	3	0	0	3
2	ECS771	Web Applications Security	PE(PE)	3	0	0	3
3	ECS773	Operating Systems Security	PE(PE)	3	0	0	3

Programme Elective-III

S. No.	Course Code	Course Title	Category	L	T	P	C
1	ECS764	Advanced Cryptography	PE(PE)	3	0	0	3
2	ECS766	Forensic Psychology	PE(PE)	3	0	0	3
3	ECS768	Mobile Device Forensics	PE(PE)	3	0	0	3

Programme Elective-IV

S. No.	Course Code	Course Title	Category	L	T	P	C
1	ECS770	Computer Forensics and Investigations	PE(PE)	3	0	0	3
2	ECS772	Biometric Security	PE(PE)	3	0	0	3
3	ECS774	Cloud Computing and Security	PE(PE)	3	0	0	3

ECS701: ADVANCED DATA STRUCTURES AND ALGORITHMS

L	T	P	C
4	0	0	4

Module I **12hrs**

Introduction to Data Structures and Algorithms, Performance Analysis: Time Complexity, Space Complexity, Amortized Complexity, Asymptotic Notations, Randomized Algorithms, Linked List, Stacks, Queues, Sparse Matrices. Algebraic Problems: General Method, Evaluation and Interpolation.

Module II **10hrs**

Introduction to Graphs, Graph Traversal. Introduction to Trees and Tree Traversals, Binary Search Trees, AVL Trees, B-Trees, Priority Queues.

Module III **10hrs**

Divide and Conquer: General Method, Selection Problem, Strassen's Matrix Multiplication, and Convex Hull Problem. The Greedy Method: General Method, Knapsack, Job Sequencing with Dead Lines, Minimum Cost Spanning Trees using Kruskal's Algorithm, using union and find, Dijkstra's algorithm for single source shortest path.

Module IV **10hrs**

Dynamic Programming: General Method, Matrix Chain Multiplication, Longest Common Subsequence, Reliability Design, Traveling Sales Person Problem. Back Tracking: General Method, 8 Queens Problem, Hamiltonian Cycle, Graph Coloring Problem.

Module V **10hrs**

Branch-and-Bound: General Method, FIFO Branch and Bound, LIFO Branch and Bound, LC Branch and Bound, Traveling Sales Person Problem. P-Class Problem, NP-Class Problems, NP-Complete Problems, NP-Hard problems.

Text Book(s)

1. Ellis Horowitz, Sartaz Sahni, Sanguthevar Rajasekharan , Fundamentals of Computer Algorithms , 2/e, University Press.
2. Sartaj Sahni, Data Structures, Algorithms and Applications in C++, 2/e, Universities Press.
3. Varsha H Patil, Data Structures using C++, Oxford Higher Education.

References

1. Thomas H. Cormen, et al., Introduction to Algorithms,3/e, MIT Press.
2. Mark Allen Weiss, Data Structures and Algorithms.
3. Adam Drozdek, Data Structures and Algorithms in C++, 3/e, Cengage Learning.
4. Michel T. Goddrich,Roberto Tamassia, Algorithm Design, John Weily and Sons.

Web Resources

http://www.personal.kent.edu/~rmuhamma/Algorithms/ algorithm.html

ECS702: ADVANCED COMPUTER NETWORKS

L	T	P	C
4	0	0	4

Module I **10 hrs**

Introduction - Building a Network, Applications, Requirements, Connectivity, Cost-Effective Resource Sharing, Support for Common Services, Network Architecture, Layering and Protocols, OSI Architecture, Internet Architecture, Implementing Network Software, Application Programming Interface (Sockets), Protocol Implementation Issues, Performance, Bandwidth and Latency, Delay × Bandwidth Product, High-Speed Networks, Application Performance Needs, Ubiquitous Networking.

Module II **10 hrs**

Direct Link Networks - Reliable Transmission - Stop-and-Wait, Sliding Window, Concurrent Logical Channels; Ethernet (802.3) - Physical Properties, Access Protocol, Experience with Ethernet; Rings - Token Ring Media Access Control, Token Ring Maintenance, FDDI, Resilient Packet Ring (802.17); Wireless -Bluetooth (802.15.1), Wi-Fi (802.11), WiMAX (802.16), Cell Phone Technologies; Sensor Networks; Packet Switching - Switching and Forwarding, Datagrams, Virtual Circuit Switching, Source Routing; Bridges and LAN Switches - Learning Bridges, Spanning Tree Algorithm, Broadcast and Multicast, Limitations of Bridges.

Module III **10 hrs**

Internetworking - Simple Internetworking (IP) - What Is an Internetwork? Service Model, Global Addresses, Datagram Forwarding in IP, Address Translation (ARP), Host Configuration (DHCP), Error Reporting (ICMP), Virtual Networks and Tunnels; Routing - Network as a Graph, Distance Vector (RIP), Link State (OSPF), Metrics, Routing for Mobile Hosts; Subnetting - Classless Routing (CIDR),Inter- domain Routing (BGP), Routing Areas, IP Version 6 (IPv6); Multiprotocol Label Switching - Destination-Based Forwarding, Explicit Routing, Virtual Private Networks and Tunnels ;Deployment of IPv6.

Module IV **12 hrs**

End-to-End Protocols - Simple Demultiplexer (UDP); Reliable Byte Stream (TCP) - End-to-End Issues, Segment Format, Connection Establishment and Termination, Sliding Window Revisited, Triggering Transmission,

Adaptive Retransmission, Record Boundaries, TCP Extensions, Alternative Design Choices; Transport for Real-Time Applications (RTP) - Requirements, RTP Details, Control Protocol ; Performance; Application-Specific Protocols; Congestion Control and Resource Allocation - Issues in Resource Allocation - Network Model, Taxonomy, Evaluation Criteria; Queuing Disciplines - FIFO, Fair Queuing; TCP Congestion Control - Additive Increase/Multiplicative Decrease, Slow Start, Fast Retransmit and Fast Recovery; Congestion-Avoidance Mechanisms - DECbit, Random Early Detection (RED), Source-Based Congestion Avoidance; Quality of Service - Application Requirements, Integrated Services (RSVP), Differentiated Services (EF, AF), Equation-Based Congestion Control; Inside versus Outside the Network.

Module V **10 hrs**

Applications - Traditional Applications - Electronic Mail (SMTP, MIME, IMAP), World Wide Web (HTTP), Name Service (DNS), Network Management (SNMP); Web Services - Custom Application Protocols (WSDL, SOAP), A Generic Application Protocol (REST), Multimedia Applications, Session Control and Call Control (SDP, SIP, H.323), Resource Allocation for Multimedia Applications; Overlay Networks - Routing Overlays, Peer-to-Peer Networks (Gnutella, BitTorrent), Content Distribution Networks.

Text Books

1. Larry L. Peterson,Bruce S. Davie, Computer Networks, A Systems Approach, 4/e, Morgan Kaufmann.
2. D. Bertsekas, R. Gallager, Data Networks, PHI.

References

1. W.R. Stevens, Unix Network Programming, Vol.1, Pearson Education
2. J.Walrand, P. Varaiya, High Performance Communication Networks, Morgan Kaufmann
3. Y. Zheng, S. Akhtar, Networks for Computer Scientists and Engineers,. Oxford.
4. A.S. Tanenbaum, Computer Networks, 4/e, Prentice Hall.
5. James D. McCabe, Practical Computer Analysis and Design, Harcourt Asia.
6. Darren L Spohn, Data Network Design, TMH.

ECS703: ADVANCED OPERATING SYSTEMS

L	T	P	C
4	0	0	4

Module I **11 hrs**

Introduction : Overview, Functions of an Operating System, Design Approaches, Types of Advanced Operating System, Synchronization Mechanisms, Concept of a Process, Concurrent Processes, The Critical Section Problem, Other Synchronization Problems, Language Mechanisms for Synchronization, Axiomatic Verification of Parallel Programs,Process Deadlocks : Preliminaries, Models of Deadlocks, Resources, System State,Necessary and Sufficient conditions for a Deadlock, Systems with Single-Unit Requests, consumable Resources, Reusable Resources.

Module II **11 hrs**

Distributed Operating Systems: Introduction, Issues, Communication Primitives, Inherent Limitations, Lamport's Logical Clock; Vector Clock; Causal Ordering; Global State; Cuts; Termination Detection. Distributed Mutual Exclusion : Non-Token Based Algorithms, Lamport's Algorithm, Token-Based Algorithms, Suzuki-Kasami's Broadcast Algorithm.
Distributed Deadlock Detection: Issues, Centralized Deadlock Detection Algorithms, Distributed Deadlock Detection Algorithms, Agreement Protocols: Classification , Solutions , Applications.

Module III **10 hrs**

Distributed Resource Management: Distributed File systems, Architecture, Mechanisms, Design Issues, Distributed Shared Memory: Architecture, Algorithm, Protocols, Design Issues , Distributed Scheduling: Issues, Components, Algorithms.

Module IV **10 hrs**

Failure Recovery And Fault Tolerance: Basic Concepts, Classification of Failures, Basic Approaches to Recovery, Recovery in Concurrent System, Synchronous and Asynchronous Check pointing and Recovery, Check pointing in Distributed Database Systems, Fault Tolerance, Issues, Two-phase and Non-blocking Commit Protocols, Voting Protocols, Dynamic Voting Protocols;

Module V **10 hrs**

Multiprocessor and Database Operating Systems: Structures, Design Issues, Threads , Process Synchronization , Processor Scheduling, Memory Management , Reliability / Fault Tolerance. Database Operating Systems: Introduction , Concurrency Control , Distributed Database Systems, Concurrency Control Algorithms.

Text Book

1. Mukesh Singhal and N. G. Shivaratri, Advanced Concepts in Operating Systems, McGraw- Hill, 2000

References

1. Abraham Silberschatz, Peter B. Galvin, G. Gagne, Operating System Concepts, 6/e, Addison Wesley 2003.

2. Andrew S. Tanenbaum, Modern Operating Systems, 2/e, Addison Wesley, 2001.

ECS709: NUMBER THEORY AND CRYPTOGRAPHY

L	T	P	C
4	0	0	4

Module I **9 hrs**

Topics in elementary number theory: O and ? notations, time estimates for doing arithmetic, divisibility and the Euclidean algorithm. Congruence's: Definitions and properties, linear congruencies, residue classes, Euler's phi function, Fermat's Little Theorem, Chinese Remainder Theorem, Applications to factoring, finite fields, quadratic residues andReciprocity: Quadratic residues, Legendre symbol, Jacobi symbol.

Module II **9 hrs**

Simple Cryptosystems: Enciphering Matrices - Block ciphers Principles -Data Encryption Standard (DES) -The Strength of DES- Differential & Linear Crypt analysis-Block Cipher Design principles.

Module III **10 hrs**

Public Key Cryptosystems: The idea of public key cryptography ,The Diffie-Hellman Key Agreement Protocol .RSA Cryptosystem ,Bit security of RSA, ElGamal Encryption, Discrete Logarithm, Knapsack problem, Zero-Knowledge Protocols From Cryptography to Communication Security - Oblivious Transfer.

Module IV **9 hrs**

Primality and Factoring: Pseudo primes, the rho (?) method, Format factorization and factor bases , the continued fraction method, the quadratic seieve method.

Module V **9 hrs**

Number Theory and Algebraic Geometry: Elliptic curves, basic facts, elliptic curve cryptosystems, elliptic curve primality test - elliptic curve factorization.

Text Book(s)

1. Neal Koblitz, A Course in Number Theory and Cryptography, 2/e, Springer, 2002.
2. William Stallings, Cryptography and Network Security, 5/e, Pearson education, 2010

References

1. R. P. Feynman, Feynman lectures on computation, Penguin Books, 1996.
2. Gennady P. Berman, Gary D. Doolen, Ronnie Mainiri & Valdmis Itri Frinovich, Introduction to quantum computers, World Scientific, Singapore, 1998.
3. Jonathan Katz, Yehuda Lindell,Introduction to Modern Cryptography, Principles And Protocols", CRC Press.

ECS710: CYBER FORENSICS

L	T	P	C
4	0	0	4

Module I **10 hrs**

Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime, Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

Module II **10 hrs**

Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

Module III **10 hrs**

Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

Module IV **10 hrs**

Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, Email Recovery, Hands on Case Studies, Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

Module V **10 hrs**

Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.

Text Book(s)

1. Bernadette H Schell, Clemens Martin, Cybercrime, ABC , CLIO Inc, California, 2004.
2. Understanding Forensics in IT , NIIT Ltd, 2005.
3. Nelson Phillips and Enfinger Steuart, Computer Forensics and Investigations, Cengage Learning, New Delhi, 2009.

References

1. Kevin Mandia, Chris Prosise, Matt Pepe, Incident Response and Computer Forensics, Tata McGraw -Hill, New Delhi, 2006.
2. Robert M Slade, Software Forensics, Tata McGraw - Hill, New Delhi, 2005.

ECS712: PRAGMATICS OF INFORMATION SECURITY

L	T	P	C
4	0	0	4

Module I **10 hrs**

Overview: Computer Security Concepts, Requirements, Architecture, Trends, Strategy Perimeter Security: Firewalls, Intrusion Detection, Intrusion Prevention systems, Honeypots Case Study: Readings, Intrusion and intrusion detection by John McHugh.

Module II **10 hrs**

User Authentication: Password, Password-based, token based, Biometric, Remote User authentication. Access Control: Principles, Access Rights, Discretionary Access Control, Unix File Access Control, Role Based Access Control Internet Authentication, Applications: Kerberos, X.509, PKI, Federated Identity Management.

Module III **10 hrs**

Cryptographic Tools: Confidentiality with symmetric encryption, Message Authentication & Hash Functions, Digital Signatures, Random Numbers. Symmetric Encryption and Message Confidentiality: DES, AES, Stream Ciphers, Cipher Block Modes of Operation, Key Distribution.

Module IV **10 hrs**

Internet Security Protocols: SSL, TLS, IPSEC, S/ MIME. Public Key Cryptography and Message Authentication: Secure Hash Functions, HMAC, RSA, Diffie Hellman Algorithms Case Study: Readings, Programming Satan's Computer Ross Anderson and Roger Needham.

Module V **10 hrs**

Malicious Software: Types of Malware, Viruses & Counter Measures, Worms, Bots, Rootkits Software Security: Buffer Overflows, Stack overflows, Defense, Other overflow attacks Case Study. Readings: Smashing The Stack for Fun and Profit, Aleph One http://www.phrack.com/issues.html?issue=49&id=14#article

Text Book

1. William Stalling, Lawrie Brown, Computer Security: Principles and Practice, Pearson Indian Edition, 2010

References

1. Chuck Easttom, Computer Security Fundamentals, Pearson, 2012.

ECS721: ADVANCED DATA STRUCTURES AND ALGORITHMS LAB

L	T	P	C
0	0	3	2

1. Program to perform insertion, deletion and search operations on the following:
   a. Single Linked List b. Doubly Linked List c. Circular Linked List
2. Develop programs to demonstrate at least 3 applications of Stacks.
3. Develop a program to demonstrate the concept of double ended queue.
4. Program to represent a graph by using Adjacency Matrix and Adjacency List representation for the given set of Vertices and Edges. Traverse it by using Breadth First Search and Depth First Search Techniques.
5. Develop a program to perform insertion, deletion and search operationson the following Trees
   a. Binary Search Tree b. AVL Tree
6. Develop programs for
   a) Heap Sort b) Merge Sort c) Quick sort by taking random element as pivot d) Selection
7. Implement the code for the following problems by using Greedy Method:
   a. Finding Minimum Cost Spanning Tree by using Kruskal's Algorithm.
   b. Single Source Shortest Path Problem.
8. Implement the code for the following problems using Dynamic Programming:
   a. Matrix Chain Multiplication Problem.
   b. String Editing.
   c. Traveling Sales man Problem
9. Implement code for the following problems by using Back-Tracking:
   a. Hamiltonian Cycle b. 8 Queens Problem
10. Implement code for Traveling Salesperson Problem by using Least-Cost Branch-and- Bound

ECS727: NETWORK SECURITY AND CRYPTOGRAPHY LAB

L	T	P	C
0	0	3	2

The following programs should be implemented preferably on platform Windows/Unix using C language (for 1-5) and other standard utilities available with UNIX systems (for 6-15) :-

1. Implement the encryption and decryption of 8-bit data using Simplified DES Algorithm (created by Prof. Edward Schaefer) in C
2. Write a program to break the above DES coding
3. Implement Linear Congruential Algorithm to generate 5 pseudo-random numbers in C
4. Implement Rabin-Miller Primality Testing Algorithm in C
5. Implement the Euclid Algorithm to generate the GCD of an array of 10 integers in C
6. a)Implement RSA algorithm for encryption and decryption in C

   b) In an RSA System, the public key of a given user is e=31,n=3599. Write a program to find private key of the User.
7. Configure a mail agent to support Digital Certificates, send a mail and verify the correctness of this system using the configured parameters.
8. Configure SSH (Secure Shell) and send/receive a file on this connection to verify the correctness of this system using the configured parameters.
9. Configure S/MIME and show email-authentication.
10. Implement encryption and decryption with openssl.
11. Implement Using IP TABLES on Linux and setting the filtering rules.
12. Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication

ECS728: CYBER FORENSICS LAB

L	T	P	C
0	0	3	2

The following exercises have to be performed using various software tools/ utilities mentioned Software Tools:

1. CyberCheck 4.0 - Academic Version
2. CyberCheckSuite
3. MobileCheck
4. Network Session Analyser
5. Win-LiFT
6. TrueImager
7. TrueTraveller
8. PhotoExaminer Ver 1.1
9. CDRAnalyzer

Forensics Exercises:

I) Disk Forensics:

1. Identify digital evidences
2. Acquire the evidence
3. Authenticate the evidence
4. Preserve the evidence
5. Analyze the evidence
6. Report the findings

II) Network Forensics:

- Intrusion detection
- Logging (the best way to track down a hacker is to keep vast records of activity on a network with the help of an intrusion detection system)
- Correlating intrusion detection and logging

III) Device Forensics

1. PDA
2. Mobile phone
3. Digital Music
4. Printer Forensics
5. Scanner Forensics

ECS730: IOT SECURITY LAB

L	T	P	C
0	0	3	2

Arduino

1) Programming the Arduino to make the LED Blink using delay.
2) Integration of analog/digital sensors/componentswith Arduino and Programming

Analog Sensor	Digital Sensor
Gas Sensor (MQ2) - Analog	PIR Sensor
Temperature Sensor (LM35)	IR Sensor
LDR Sensor	DC/Gear/Stepper Motor

3) Serial Communication in Arduino with Wireless Module and Programming
   - Bluetooth (HC-05)
   - ZigBee (TI -CC2500)

Raspberry Pi

1) Programming the Raspberry Pi to make the LED Blink using Python.
2) Integration of sensors/components with Raspberry Pi and Programming
   - LED
   - PIR Sensor
   - Ultra-Sonic Sensor (HC-SR04)
   - DC/Gear/Stepper Motor (using Motor Drivers)
3) Serial Communication Between Arduino and Raspberry Pi using Universal Serial Bus(USB)

Security

1. Program to generate Hash of given data using Hash Algorithms (MD5, SHA1, SHA256)
2. Program to Encrypt and Decrypt given data using RSA and AES Algorithms
3. Program to Obfuscate a given data using python

Arduino - Security

1. Implementing Hash Algorithms (MD5, SHA1, SHA256) in Arduino using Hash Functions.
2. Implementing RES and AES Algorithms in Arduino using Arduino Cryptographic Library.
3. Using Hash and Cryptographic Algorithms to secure the Sensor Data in Arduino

Raspberry Pi- Security

1. Implementing Hash Algorithms (MD5, SHA1, SHA256) in Raspberry Pi
2. Implementing RES and AES Algorithms in Raspberry Pi using Cryptographic Algorithms
3. Using Hash and Cryptographic Algorithms to secure the Sensor Data in Raspberry Pi

Arduino - Raspberry Pi- Security

1. Implementing Hashand Cryptographic Algorithmsto secure data between 2 Arduino using ZigBee/Bluetooth
2. ImplementingHash and Cryptographic Algorithms to secure data between Serial Communication of Arduino and Raspberry Pi

Implementing the Obfuscation techniques to secure Arduino and Raspberry Pi Programming

ECS749: INTERNET OF THINGS

L	T	P	C
3	0	0	3

Module I **10 hrs**

Introduction: The Internet of Things, An Overview, the flavour of the internet of things, the internet of things, the technology of the internet of things, enchanted objects, who is making the internet of things, Design principles for connected devices: Calm and ambient technology, magicas metaphor, privacy, web thinking for connected devices, affordances.

Module II **10 hrs**

Internet Principles: Internet communications,An overview (IP, TCP, the IP protocol suite (TCP/IP), UDP), IP addresses (DNS, Static IP Address assignment, dynamic IP address assignment,IPv6), MAC addresses, TCP and UDP ports, application layer protocols.

Module III **10 hrs**

Prototyping: Thinking About Prototyping: Sketching, familiarity, costs versus ease of prototyping, prototypes and production, open source versus closed source, tapping into the community.Prototyping embedded devices : Electronics, embedded computing basics, developing on the arduino, raspberry pi beaglebone black, electric imp, mobile phone and tablets, plug computing, always on internet of things.

Module IV **10 hrs**

Prototyping the Physical Design: Preparation, sketch, iterate and explore, non digital methods, laser cutting, 3D printing, CNC milling, repurposing/ recycling.Techniques for Writing Embedded Code: Memory management, performance and battery life, libraries, debugging.

Module V **10 hrs**

Prototype to Reality: Business Models,A short history of business models, the business model canvas, models, funding an internet of things startup, lean startups.Moving to manufacture : Designing kits, designing printed circuit boards, manufacturing printed circuit boards, mass producing the case and other fixtures, certification, costs, scaling up software.

Text Book

1. Adrian McEwen, Hakim Cassimally, Designing the Internet of Things, 1/e, Wiley publication, 2013

References

1. Charalampos Doukas , Building Internet of Things with the Arduino, Create space, 2002.
2. Dieter Uckelmann (et.al), Architecting the Internet of Things, Springer, 2011.
3. Luigi Atzor (et.al), The Internet of Things: A survey, Journal on Networks, Elsevier Publications, 2010.

ECS751: SERVICE ORIENTED ARCHITECTURE

L	T	P	C
3	0	0	3

Module I **8 hrs**

Fundamentals of SOA: Introduction, defining SOA, evolution of SOA, service oriented enterprise, comparing SOA to client server and distributed internet architectures, basic SOA architecture concepts, key service characteristics, technical benefits, business benefits.

Module II **10 hrs**

Combining SOA and Web Services: Web services , service descriptions , messaging with SOAP ,message exchange patterns, web service platform, service contract, service level data model, service discovery, service level security, service level interaction patterns, atomic and composite services, service enabling legacy system, enterprise service bus pattern.

Module III **10 hrs**

Multi Channel Access and Web Services Composition: SOA for multi, channel access, business benefits, tiers, business process management, web service composition, BPEL, RESTFUL services, comparison of BPEL and RESTFUL services.

Module IV **10 hrs**

Java Web Services:SOA support in J2EE , Java API for XML, basedweb services(JAX,WS), Java architecture for XML binding (JAXB) , Java API for XML registries(JAXR), Java API for XML based RPC (JAX,RPC), web services interoperability, SOA support in .NET , ASP.NET web services, case studies, web services enhancements (WSE).

Module V **8 hrs**

Web Services Security and Transaction: Meta datamanagement, advanced messaging, addressing , reliable messaging, policies, WS- policy, security, WS- security, notification and eventing, transaction management.

Text Book(s)

1. Eric Newcomer, Lomow, Understanding SOA with Web Services, Pearson Education, 2005.
2. James McGovern, Sameer Tyagi, Michael E Stevens, Sunil Mathew, Java Web Services Architecture, Elsevier, 2003.

References

1. Thomas Erl, Service Oriented Architecture, Pearson Education, 2005.
2. Sandeep Chatterjee, James Webber, Developing Enterprise Web Services, An Architect's Guide, Pearson Education, 2005.
3. Dan Woods and Thomas Mattern, Enterprise SOA: Designing IT for Business Innovation, O'REILLY, 1/e, 2006.
4. Frank Cohen, FastSOA, Elsevier, 2007.
5. Jeff Davies, The Definitive Guide to SOA, Apress, 2007.

ECS763: ETHICAL HACKING

L	T	P	C
3	0	0	3

Module I **10 hrs**

Casing the Establishment: What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring.

Module II **10 hrs**

Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access., After hacking root.

Module III **10 hrs**

Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, Brute-Force Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media.

Module IV **10 hrs**

Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of DoS Attackers, Types of DoS attacks, Generic DoS Attacks, UNIX and Windows DoS.

Module V **10 hrs**

Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.

Text Book(s)

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata Mc Graw Hill Publishers, 2010.
2. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall of India, 2010

References

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed Network Security Secrets & Solutions, 5/e, Tata Mc Graw Hill Publishers, 2010.
2. Rafay Baloch, A Beginners Guide to Ethical Hacking.
3. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gray Hat Hacking The Ethical Hackers Handbook, 3/e , McGraw-Hill Osborne Media paperback(January 27, 2011)

ECS764: ADVANCED CRYPTOGRAPHY

L	T	P	C
3	0	0	3

Module I **10 hrs**

OSI security architecture: Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality.

Module II **10 hrs**

Key management: Diffie Hellman key exchange, Elliptic curve architecture and cryptography, Introduction to number theory, Confidentiality using symmetric encryption,Public key cryptography and RSA.

Module III **10 hrs**

Authentication requirements: Authentication functions, Message authentication codes, Hash functions, Security of hash functions and MACS, MD5 Message Digest algorithm, Secure hash algorithm, Ripend, HMAC digital signatures, Authentication protocols.

Module IV **10 hrs**

Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. non local interactions, entanglements, EPR paradox, Bell's theorem, Bell basis, teleportation of a single qubit theory and experiments.

Module V **10 hrs**

Future trends: Review of recent experimental achievements, studyon technological feasibility of a quantum computer candidate physical systems and limitations imposed by noise.

Text Book(s)

1. William Stallings, Cryptography and Network Security -Principles and Practices, 3/e , Prentice Hall of India, 2003.
2. Atul Kahate, Cryptography and Network Security, Tata McGraw -Hill, 2003.
3. William Stallings, Network Security Essentials: Applications and Standards, Pearson Education Asia, 2000.

References

1. R. P. Feynman, Feynman lectures on computation, Penguin Books, 1996.
2. Gennady P. Berman, Gary D. Doolen, Ronnie Mainiri, Valdmis Itri Frinovich, Introduction to quantum computers, World Scientific, Singapore, 1998.
3. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography Principles And Protocols ,CRC Press.

ECS765: INTRODUCTION TO MACHINE LEARNING

L	T	P	C
3	0	0	3

Module I **10 hrs**

Introduction: overview of machine learning, related areas, applications, parametric regression: linear regression, polynomial regression, locally weighted regression, numerical optimization, gradient descent, kernel methods.

Module II **10 hrs**

Introduction, Concept Learning and Decision Trees: Learning Problems - Designing Learning systems, Perspectives and Issues - Concept Learning - Version Spaces and Candidate Elimination Algorithm - Inductive bias - Decision Tree learning - Representation - Algorithm - Heuristic Space Search.

Module III **9 hrs**

Neural Networks And Genetic Algorithms: Neural network representation, problems, perceptions, multilayer networks and back propagation algorithms, advanced topics, Genetic algorithms, hypothesis space search, genetic programming, models of evaluation and learning.

Module IV **9 hrs**

Bayesian and Computational Learning: Bayes theorem , concept learning, maximum likelihood, minimum description length principle, Bayes optimal classifier, Gibbs Algorithm, Naïve Bayes Classifier, Bayesian belief network, EM algorithm, probability learning, sample complexity, finite and infinite hypothesis spaces, mistake bound model

Instance Based Learning: K-Nearest neighbor learning, locally weighted regression, radial basis functions, case based learning.

Module V **9 hrs**

Hidden Markov Models: Introduction, discrete Markov processes, hidden Markov models, three basic problems of HMMs evaluation problem, finding the state sequence, learning model parameters, continuous observations, the HMM with input, model selection in HMM.

Text Book(s)

1. Tom M. Mitchell, Machine Learning, McGraw Hill , 2013.
2. Ethem Alpaydin, Introduction to Machine Learning (Adaptive Computation and Machine Learning), The MIT Press, 2004

References

1. T. Hastie, R. Tibshirani, J. H. Friedman, The Elements of Statistical Learning, 1/e, Springer, 2001.
2. M Narasimha Murty, Introduction to Pattern Recognition and MachineLearning, World Scientific Publishing Company, 2015

ECS766: FORENSIC PSYCHOLOGY

L	T	P	C
3	0	0	3

Module I **10 hrs**

Historical roots: Modern major perspectives of psychology, distinguishing professional and pseudo-psychology, types of psychological professionals. The science and research methods, professional ethics of research, research challenges.

Module II **10 hrs**

The biology underlying behavior: Nerves and neurons, structure and functions of neurons, neurotransmitters, Central Nervous System, peripheral nervous system. The human brain: its structure and function, sensory system and endocrine system, Stages of sleep, REM sleep, sleep disturbances, States of consciousness, altered states of consciousness, attention and awareness, sensation of perception, problems in attention and perception.

Module III **10 hrs**

Learning process: Latent learning, observational learning. Memory: Recalling long term memories, Retrieval clues, constructive purposes in memory, memory in courtroom, autobiographical memory. Stages in memory: Encoding, storage and retrieval of memory. Forgetting: Proactive and retroactive interference. Memory dysfunctions: Afflictions of forgetting.

Module IV **10 hrs**

Cognition: Thinking and reasoning, thinking mental images, concepts, reasoning. Problem solving: Production, judgment, impediments to problems solving. Language and Intelligence Language: Grammar, language development, influence of language on thinking. Intelligence: Measuring intelligence (IQ), practical intelligence-measuring commonsense. Motivation and Emotion: Types of approaches of motivation. Emotion: Understanding emotional experiences, functions of emotions and determining range of emotions, Coping with stress.

Module V **10 hrs**

Personality: Theories-Psychoanalytic approaches to personality, Trait approaches, learning approaches, biological approaches, and humanistic approaches. Assessing personality: Self report measures of personality, projective methods and behavioral assessment.

Text Book

1. Understanding Psychology by Robert S. Feldman, 4th edition, Mcgraw Hill, 1996.

References

1. Study Guide for Psychology: from science to practice by Baron, R.A. & Kolsher MJ
2. Forensic Psychology by Christopher Cronin
3. Introduction to Psychology by Dennis Coon
4. Introduction to forensic psychology: Research and Application, 3rd edition (paperback) by Curt R Bartol, Anne M Bartol

ECS767: STEGANOGRAPHY

L	T	P	C
3	0	0	3

Module I **hrs**

Introduction: Information Hiding, Steganography. History of Steganography. Importance of Steganography. Hiding data in multimedia files, least significant bit method, Latest algorithms for data hiding. Comparison of different steganographic techniques, Applications of steganography .

Module II **10 hrs**

Properties of Steganography and Steganalysis Systems : Embedding , Steganographic Capacity, Embedding Capacity, Embedding Efficiency, and Data Payload, Blind or Informed Extraction, Blind or Targeted Steganalysis, Statistical Undetectability, False Alarm Rate ,Robustness, Security, Stego Key, Evaluating and Testing Steganographic Systems, Summary.

Module III **10 hrs**

Steganography : Steganography communication, the channel, the building blocks, notation and terminology, information, theoretic foundations of Steganography, cachin's definition of Steganography security, practical Steganography methods, statistics preserving Steganography, model based Steganography, masking embedding as natural processing, minimizing the embedding impact, matrix embedding, non-shared selection rule.

Module IV **9 hrs**

Steganalysis : Steganalysis scenarios, detection, forensic steganalysis, the influence of the cover work on steganalysis, some significant steganalysis algorithms, LSB embedding and the histogram attack, sample pairs analysis, blind steganalysis of JPEG images using calibration, blind steganalysis in the spatial domain.

Module V **9 hrs**

Applications:Applications of Steganography, Steganography for Dissidents, Steganography for Criminals.

Text Book

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, Digital Watermarking and Steganography, 2/e, Morgan Kaufmann Publishers, 2008.

Reference

1. John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Eastern Publications, 2005

ECS768:MOBILE DEVICE FORENSICS

L	T	P	C
3	0	0	3

Module I **10 hrs**

Android and mobile forensics: Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics

Module II **10 hrs**

Android hardware platforms: Overview of core components, Overview of different device types, Read-only memory and boot loaders, Manufacturers, Specific devices

Module III **10 hrs**

Android software development kit and android debug bridge: Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK.

Module IV **10 hrs**

Android file systems and data structures: Data in the shell, Type of memory, File systems, Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques

Module V **10 hrs**

Android device data and app security: Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies. Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis

Text Book

1. Android Forensics Investigation, Analysis, and Mobile security for Google Android, Andrew Hoog, John McCash, Technical Editor, Elsevier, 2011.

References

1. Satish Bommisetty, Rohit Tamma, Heather Mahalik Practical Mobile Forensics, Kindle Edition, Packet Publishing
2. Andrew Martin, Mobile Device Forensics, SANS Institute, 2009

Web Resources

1. http://data.ceh.vn/Ebook/ebooks.shahed.biz/ANDROID/Android%20Forensics.pdf
2. https://viaforensics.com/resources/android-forensics-mobile-security-book/

ECS769: SECURE SYSTEMS ENGINEERING

L	T	P	C
3	0	0	3

Module I **9 hrs**

Introduction, Purpose and applicability, Target audience, the fundamentals, system security engineering, system and system elements

Module II **10 hrs**

System Security perspective, protection capability and Security, System Security and failure, strategy for system security, beyond verification and validation-demonstration, system characteristics and system security, role of system security engineering

Module III **10 hrs**

System Life Cycle Process: Agreement Processes, Acquisition process, Supply process, Organizational project -enabling processes : Life Cycle Model Management process, Infrastructure Management process, Portfolio Management process, Human Resource Management process, Quality Management process, Knowledge Management process,

Module IV **10 hrs**

Technical Management Processes: Project Planning Process, Project Assessment and Control Process, Decision Management Process, Management Process Configuration Management Process , Information Management Process , Measurement Process Quality Assurance Process

Module V **10 hrs**

Technical Processes: Business or Mission Analysis Process, Stakeholder Needs and Requirements ,Definition Process , System Requirements Definition Process, Architecture Definition Process, Design Definition Process, System Analysis Process , Implementation Process , Integration Process, Verification Process , Transition Process , Validation Process , Operation Process , Maintenance Process Disposal Process

Text Book

1. Ron Ross Michael, Mcevilley, Janet Carrier Oren, Systems Security Engineering, NIST Special Publication 800-160.

Reference

1. Ross Anderson, Security Engineering, 2/e, Wiley Publishers

ECS770: COMPUTER FORENSICS AND INVESTIGATIONS

L	T	P	C
3	0	0	3

Module I **10 hrs**

Introduction Forensics and Investigations: Understanding Computer Forensics, Preparing for Computer Investigations, Taking a systematic Approach, Preparing For Corporate High-Tech Investigations, Conducting an Investigations.

Module II **10 hrs**

Data Acquisition: Understanding Storage Formats for Digital Evidence, Using Acquisition Tools, Validating Data Acquisitions, Performing RAID Acquisition Tools, Using Remote Acquisition Tools.

Module III **10 hrs**

Processing Crime and Incident Scenes: Identifying Digital Evidence, Preparing for a Search, Seizing Digital Evidence at the Scene, Storing Digital Evidence, Computer Forensics Software Tools, Computer Forensics Hardware Tools, Validating and Testing Forensics Software.

Module IV **10 hrs**

Computer Forensics Analysis and Validation: Determining what Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques, Performing Remote Acquisitions, Investigating E-mail Crimes and Violations, Understanding Mobile Device Forensics.

Module V **10 hrs**

Report Writing for High-Tech Investigations: Understanding the Importance of Reports, Guidelines for Writing Reports, Generating Report Findings with Forensics Software Tools, Applying Ethics and Codes to Expert Witnesses, Organizations with Codes Ethics, Ethical Difficulties in Expert Testimony.

Textbook

1. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips and Christopher Steuart, Cengage Learning.

References

1. A Practical Guide to Computer Forensics Investigations by Darren R. Hayes.
2. Computer Investigation by Elizabeth Bauchne.

ECS771: WEB APPLICATIONS SECURITY

L	T	P	C
3	0	0	3

Module I **9 hrs**

Web Application (In) security: The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications, Web Application Security. Core Defense Mechanisms: Handling User Access Authentication, Session Management, Access Control, Handling User Input, Varieties of Input Approaches to Input Handling, Boundary Validation. Multistep Validation and Canonicalization: Handling Attackers, Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks.

Module II **9 hrs**

Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, Client-Side Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks.

Module III **9 hrs**

Mapping the Application: Enumerating Content and Functionality, Web Spidering, UserDirected Spidering, Discovering Hidden Content, Application Pages Versus Functional Paths, Discovering Hidden Parameters, Analyzing the Application, Identifying Entry Points for User Input, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface.

Module IV **11 hrs**

Attacking Authentication: Authentication Technologies, Design Flaws in Authentication Mechanisms, Bad Passwords, Brute-Forcible Login, Verbose Failure Messages, Vulnerable Transmission of Credentials, Password Change, Functionality, Forgotten Password Functionality, "Remember Me" Functionality, User Impersonation, Functionality Incomplete, Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords, Insecure Distribution of Credentials. Attacking Access Controls: Common Vulnerabilities, Completely Unprotected, Functionality Identifier-Based Functions, Multistage Functions, Static Files, Platform Misconfiguration, Insecure Access Control Methods.

Module V **12 hrs**

Attacking Data Stores: Injecting into Interpreted Contexts, Bypassing a Login, Injecting into SQL, Exploiting a Basic Vulnerability Injecting into Different Statement Types, Finding SQL Injection Bugs, Fingerprinting the Database, The UNION Operator, Extracting Useful Data, Extracting Data with UNION, Bypassing Filters, Second-Order SQL Injection, Advanced Exploitation Beyond SQL Injection: Escalating the Database Attack, Using SQL Exploitation Tools, SQL Syntax and Error Reference, Preventing SQL Injection.

Text Book

1. Security Defydd Stuttard, Marcus Pinto,The Web Application Hacker's Handbook: Finding and Exploiting, 2/e, Wiley Publishing.

References

1. Andres Andreu,Professional Pen Testing for Web application, Wrox Press
2. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, Web Application Security, 1/e, Springer.
3. Joel Scambray, Vincent Liu, Caleb Sima ,Hacking exposed, McGraw-Hill; 3/e, 2010
4. OReilly Web Security Privacy and Commerce 2/e, 2011
5. Richard sinn,Software Security Theory Programming and Practice, Cengage Learning
6. Hassan, Database Security and Auditing, Cengage Learning

ECS772: BIOMETRIC SECURITY

L	T	P	C
3	0	0	3

Module I **10 hrs**

Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy in biometric systems.

Module II **10 hrs**

Physiological Biometric Technologies: Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, weaknesses, deployment. Iris scan: Technical description, characteristics, strengths, weaknesses, deployment. Retina vascular pattern: Technical description, characteristics, strengths, weaknesses, deployment. Hand scan: Technical description, characteristics, strengths, weaknesses, deployment , DNA biometrics.

Module III **10 hrs**

Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke dynamics, Voice, data acquisition, feature extraction, characteristics, strengths , weaknesses deployment.

Module IV **10 hrs**

Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.

Module V **10 hrs**

Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

Text Book(s)

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Biometrics ,Identity verification in a networked World, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Eastern Publications, 2005.

Reference

1. John Berger, Biometrics for Network Security, Prentice Hall, 2004.

ECS773: OPERATING SYSTEMS SECURITY

L	T	P	C
3	0	0	3

Module I **10 hrs**

Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system.

Module II **10 hrs**

Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.

Module III **10 hrs**

Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.

Module IV **10 hrs**

Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement.

Module V **10 hrs**

Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration. Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

Text Book

1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008

References

1. Michael Palmer, Guide to Operating system Security Thomson
2. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition
3. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont

ECS774: CLOUD COMPUTING AND SECURITY

L	T	P	C
3	0	0	3

Module I **10 hrs**

Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.

Module II **10 hrs**

Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.

Module III **10 hrs**

Traditional Security: Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).

Module IV **10 hrs**

Data Center Operations: Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations.

Module V **10 hrs**

Identity and Access Management: Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise

Architecture with IDaaS , IDaaS Security Recommendations. Virtualization: Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations

Text Book

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance, Oreilly Media 2009.

Reference

1. Vic (J.R.) Winkler, Securing the Cloud, Cloud Computer Security Techniques and Tactics, Syngress, 2011.

EID760: PROGRAMMING WITH R

L	T	P	C
3	0	0	3

Module I **10 hrs**

Introduction to R programming, Introduction to Functions, Preview of Important R Data Structures, Vectors, Recycling, Common Vector Operations, Vectorized Operations, Filtering Matrices and Arrays

Module II **9 hrs**

Lists, Creating Lists, General List Operations Accessing List Components and Values, Applying Functions to Lists, Recursive Lists, Data Frames, Creating Data Frames, Other Matrix-Like Operations, Merging Data Frames, Applying Functions to Data Frames, Factors and Tables, Factors and Levels, Common Functions Used with Factors, Working with Table,Table-Related Functions

Module III **10 hrs**

R Programming Structures, Control Statements, Arithmetic and Boolean Operators and Values, Default Values for Arguments, Environment and Scope Issues, Recursion Replacement Functions, Anonymous Functions Data Frames, Creating Data Frames, Other Matrix-Like Operations, Merging Data Frames, Applying Functions to Data Frames, Factors and Tables Factors and Levels, Common Functions Used with Factors, Working with Table, Table- Related Functions, R Programming Structures, Control Statements Arithmetic and Boolean Operators and Values, Default Values for Arguments, Environment and Scope Issues, Recursion Replacement Functions, Anonymous Functions Corporate Digital Library - Document Library, digital Document types, corporate Data Warehouses.

Module IV **9 hrs**

Math and Simulations in R, Math Functions, Functions for Statistical Distributions, Sorting,Linear Algebra Operations on Vectors and Matrices, Set Operations, Simulation Programming in R, Object-Oriented Programming, S3 Classes, S4 Classes, S3 Versus S4, Managing Your Objects

Module V **10 hrs**

Input/Output, Accessing the Keyboard and Monitor, Reading and Writing Files, Accessing the Internet,String Manipulation, String-Manipulation

Functions, Regular Expressions, Use of String Utilities in the edtdbg Debugging Tool, Creating Graphs, Customizing Graphs, Saving Graphs to Files Creating Three-Dimensional Plots

Text Book

1. Norman Matloff, Art of R programming, Safari books online Publisher, Nostarch Press

References

1. Mark gardener, Beginning R: The Statistical Programming Language , Wrox publication
2. lary pace, Beginning R, Appress Publishers
3. Andrie De Vries and Joris Meys , R Programming for Dummies, 1/e,Wiley India Private Limited,

EID763: MULTIVARIATE TECHNIQUES FOR DATA ANALYSIS

L	T	P	C
3	0	0	3

Module I **8 hrs**

Introduction To Multivariate Analysis: Meaning of Multivariate Analysis, Measurements Scales - Metric measurement scales and Non- metric measurement scales, Classification of multivariate techniques (Dependence Techniques and Inter-dependence Techniques), Applications of Multivariate Techniques in different disciplines.

Module II **8 hrs**

Factor Analysis: Meanings, Objectives and Assumptions, Designing a factor analysis, Deriving factors and assessing overall factors, Interpreting the factors and validation of factor analysis.

Module III **8 hrs**

Cluster Analysis: Objectives and Assumptions, Research design in cluster analysis, Deriving clusters and assessing overall fit (Hierarchical methods, Non Hierarchical Methods and Combinations), Interpretation of clusters and validation of profiling of the clusters.

Module IV **8 hrs**

Discriminant Analysis- concept, objective and applications. Procedure for conducting discriminant analysis. Stepwise discriminate analysis and Mahalanobis procedure. Logit model.

Module V **8 hrs**

Linear Programming problem - Formulation, graphical method, simplex method. Integer Programming. Transportation and Assignment problem.

Text Book(s)

1. Joseph F Hair, William C Black, Multivariate Data Analysis, Pearson Education,7/e, 2013.

References

1. T. W. Anderson, An Introduction to Multivariate Statistical Analysis, Wiley, 2003.
2 . William r Dillon, Multivariate Analysis methods and applications, Wiley, 1984.
3. Hamdy A Taha, Operations Research, Pearson, 2012.

EID769: CYBER LAWS AND IT PROTECTION

L	T	P	C
3	0	0	3

Module I **10 hrs**

Understanding Computers Internet and Cyber Laws, Modern Era: The Scene and Problems, Need for Cyber Laws, Historical Perspective, Impact of the Internet and Information Technology (IT) on Business and Society The Character and Use of Internet Technologies .

Conceptual Framework of E-commerce: E-governance what is E-commerce? Growth and Development of E-commerce Various Modes of E-commerce, Mechanism Involved in the Operation of Internet Type of Players in E-commerce, Web Development and Hosting Agreements Web Hosting The Problem of Internet Jurisdiction Illustrative Cases about Cyberspace Jurisdiction Type of Websites

Module II **10 hrs**

The Role of Electronic Signatures in E-commerce with Reference to Free Market Economy in India: Introduction to Basic Laws of Digital and Electronic Signature in India, Authentication of Digital Signatures and Electronic Records , UNCITRAL: Model Law on Electronic Commerce, 1996 UNCITRAL: Draft Rules of November, 1998 ,Securing Electronic Transactions Cryptography and Securing, Electronic Transactions ,The Concept of Hash Function ,Utility of Digital Signature's Verification ,Certification, Certifying Authorities and the Status of Electronic, Signature under the Indian Law, The Appointment of Controller and Other Officers and Their Functions ,Authentication and Verification of Electronic/Digital Signatures, The Cost and Benefits of Implementing Electronic/Digital, Signatures in E-commerce in India, Security Privacy of Electronic/Digital Signatures, Private Key Escrow and Key Recovery Systems Obligation of a Certifying Authority and Certificate Management ,Different Approaches of Digital Signatures

Module III **10 hrs**

Legal Aspects of Electronic Records/Digital Signatures: Recognition of Electronic Records, UNCITRAL Model Law, The Legal Recognition of Electronic/Digital Signatures , UNCITRAL Model Law, The Position in the US, The Position in Australia, Electronic Records and Electronic Signatures/Digital Signatures, and Their Use by the Government and its Agencies in India, Contents F v Retention of Electronic Records in India, UNCITRAL Model Law Relating to Retention of Data Messages, Position in the US, Position in India ,The Central Government's Power to Make

Rules in India, Electronic Records: Attribution Acknowledgement and Dispatch in India, UNCITRAL Model Law on Attribution of Data Messages, The Position in the US, Acknowledgement of Receipt of Electronic Record in India, UNCITRAL Model Law Relating to Acknowledgement of Data Message, The Position in the US, The Time and Place of Dispatch and Receipt of Electronic, Records in India, UNCITRAL Model Law on Time and Place and Receipt of Data Messages, Position in the US, Securing Electronic Record and Electronic/Digital Signatures in India, Verification of Electronic Signatures in India, Central Government's Power to Prescribe Security Procedure

Module IV **10 hrs**

Protection of Intellectual Property Rights in Cyberspace in India: The Cyberspace The Relevance of Domain Names in Intellectual Property Rights, Deception by Squatting in Cyberspace, Bad Faith in Relation to Domain Name Infringement, Some Leading Cases Involving Complaints from India before WIPO, Protection of Copyright on Cyberspace, Rights of Software Copyright Owners, Infringement of Copyright on Cyberspace, Cyberspace, the Internet, Websites and the Nature of the Copyright, Linking, Hyper-Linking and Framing, Remedies for Infringement of Copyright on Cyberspace, The Liabilities of an Internet Services Provider (ISP) in Cyberspace, Cyberspace and the Protection of Patents in India, Patent as a Form of Intellectual Property

Module V **10 hrs**

Penalties, Compensation and Adjudication of Violations of Provisions of IT Act and Judicial Review: Penalty and Compensation for Damage to Computer, Computer System, Compensation for Failure to Protect Data, Penalty for Failure to Furnish Information, Return or any Other Penalty , Adjudication of Disputes under the IT Act, Cyber Appellate Tribunal, Its Functions and Powers under the IT Act,

Some Important Offences under the Cyberspace Law and the Internet in India :

Obscenity and Pornography on Cyberspace, Hacking on the Cyberspace and Internet, Other Offences-Computer Resource, Violation of the Right of Privacy on Cyberspace/Internet, Punishment for Violation of Privacy, Breach of Confidentiality, and Privacy under the IT Act , Terrorism on Cyber Space/Internet

Text Book

1. Harish Chander, Cyber Laws and IT protections, PHI Edition

Reference

1. Dumortier, International Encyclopedia Of Cyber Law (3vol) , Jos

EID771: ENTERPRISE CYBER SECURITY

L	T	P	C
3	0	0	3

Module I **9 hrs**

The Cyber security Challenge: Defining the Cybersecurity Challenge, The Cyberattacks of Today, Types of Cyberattackers, The Steps of a Cyberintrusion, Why Cyberintrusions succeed

Module II **9 hrs**

Enterprise Cyber security Architecture: Systems Administration, Network Security, Identity, Authentication, and Access Management, Application Security, Data Protection and Cryptography, Policy, Audit, E-Discovery, and Training,

Module III **10 hrs**

Implementing Enterprise Cybersecurity: IT Organization, IT System Life Cycle, Defining Security Policies, Defining Security Scopes, Identifying Security Scopes, Selecting Security Controls, Selecting Security Technologies.

Module IV **9 hrs**

Operating Enterprise Cyber security: Operational Responsibilities, High-Level IT and Cyber security Processes, Operational Processes and Information Systems, Functional Area Operational Objectives.

Module V **9 hrs**

Managing a Cyber security Crisis: Devastating Cyber attacks and Falling Off the Cliff, Keeping Calm and Carrying On, Recovering Cyber security and IT Capabilities, Ending the Crisis.

Text Book

1. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam, Enterprise Cybersecurity, 1/e, Apress.

Reference

1. Gurpreet Dhillon, Enterprise Cyber Security,2/e,Chegg Publishers

Chandrahas ICT Bhavan - Institute of Technology, Visakhapatnam Campus

School of Technology, Hyderabad Campus

Sir Visvesvaraya Bhavan - GITAM School of Technology, Bengaluru Campus

www.gitam.edu

GANDHI INSTITUTE OF TECHNOLOGY AND MANAGEMENT (GITAM)
Gandhi Nagar Campus, Rushikonda,Visakhapatnam-530 045, A.P. INDIA
Phones: +91-0891-2795311, 2840501, EPABX: +91-891-2790101, Fax: +91-891-2795311

A Publication of GITAM Press