MAHATMA GANDHI UNIVERSITY
KOTTAYAM

M Sc PROGRAMME
IN
CYBER FORENSICS

(Exclusively for School of Technology and Applied Sciences)

REGULATIONS, SCHEME AND SYLLABUS
(Effective from 2018 Admissions)

M.Sc. PROGRAMME IN CYBER FORENSICS

1. Eligibility

The eligibility for admission to M Sc Cyber Forensics programme in STAS under Mahatma Gandhi University is a B Sc Degree with Cyber Forensics /Computer Science /Information Technology/Electronics or BCA or equivalent with not less than 55% marks.

Note: Candidates having degree in Cyber Forensics shall be given a weightage of 20% in their qualifying degree examination marks considered for ranking for admission to MSc Cyber Forensics.

2. Admission

The admission to the M Sc programme shall be as per the rules and regulations of the University.
Students admitted under this programme are governed by the Regulations in force.

3. Programme Structure and Duration

The duration of the programme shall be 4 semesters. The duration of each semester shall be 90 working days. Odd semesters from June to October and even semesters from December to April. There shall be two semester breaks of one month each in November and May.

A student may be permitted to complete the programme, on valid reasons, within a period of 8 continuous semesters from the date of commencement of the first semester of the programme.

The programme shall include two types of courses, Core courses and Elective Courses.

There will be four core courses and one practical course per semester for the first three semesters. In the last semester there will be one core course, two elective courses to be selected from two separate groups and one project. At the end of the programme, there will be a comprehensive viva-voce which covers questions from all courses in the programme.

4. Attendance

The minimum requirement of aggregate attendance during a semester for appearing for the end semester examination shall be 75%. A student who does not satisfy the requirements of attendance shall not be permitted to take the end Semester examinations.

5. Promotion

A student who registers for the end semester examination shall be promoted to the next semester.

6. Examinations

There shall be University examination at the end of each semester.
Practical examinations shall be conducted by the University at the end of each semester.
Project evaluation and Viva -Voce shall be conducted at the end of the programme only. Practical examination, Project evaluation and Viva-Voce shall be conducted by two external examiners and one internal examiner.

End-Semester Examinations: The examinations shall be normally at the end of each semester. There shall be one end-semester examination of 3 hours duration in each lecture based course and practical course.

7. Evaluation and Grading

Evaluation: The evaluation scheme for each course shall contain two parts; (a) internal evaluation and (b) external evaluation. 25% weightage shall be given to internal evaluation and the remaining 75% to external evaluation and the ratio and weightage between internal and external is 1:3. Both internal and external evaluation shall be carried out using Direct grading system.

Internal evaluation*:* The internal evaluation shall be based on predetermined transparent system involving periodic written tests, assignments, seminars and attendance in respect of theory courses and based on written tests, lab skill/records/viva and attendance in respect of practical courses. The weightage assigned to various components for internal evaluation is as follows.

Components of Internal Evaluation

Component	**Weightage**
i) Assignment	1
ii) Seminar	2
iii) Attendance	1
iv) Two Test Papers	2

Letter Grade	**Performance**	**Grade Point (G)**	**Grade Range**
A	Excellent	4	3.50 to 4.00
B	Very Good	3	2.50 to 3.49
C	Good	2	1.50 to 2.49
D	Average	1	0.50 to 1.49
E	Poor	0	0.0 to 0.49

Grades for Attendance

% of attendance	**Grade**
>90%	A
Between 85 and 90	B
Between 80 and below 85	C
Between 75 and below 80	D
< 75	E

Assignment

Components	**Weight**
Punctuality	1
Review	1
Content	2
Conclusion	1
Reference	1

Seminar

Components	Weight
Area / Topic selected	1
Review / Reference	1
Content	2
Presentation	2
Conclusion	1

Practical – Internal

Components	Weights
Attendance	1
Laboratory Involvement	2
Written / Lab Test	2
Record	2
Viva-voce / Quiz	1

Practical – External

Components	Weights
Design and Coding	2
Output	2
Record	2
Viva-voce	1

To ensure transparency of the evaluation process, the internal assessment grade awarded to the students in each course in a semester shall be published on the notice board at least one week before the commencement of external examination. There shall not be any chance for improvement for internal grade.

The course teacher and the faculty advisor shall maintain the academic record of each student registered for the course which shall be forwarded to the University through the college Principal and a copy should be kept in the college for at least two years for verification.

External evaluation*:* The external Examination in theory courses is to be conducted by the University with question papers set by external experts. The evaluation of the answer scripts shall be done by examiners based on a well-defined scheme of valuation. The external evaluation shall be done immediately after the examination preferably through Centralized Valuation

8. Direct Grading System

Direct Grading System based on a 5 - point scale is used to evaluate the performance (External and Internal Examination of students)

DIRECT GRADING SYSTEM

Letter Grade	Performance	Grade point(G)	Grade Range
A	Excellent	4	3.5 to 4.00
B	Very Good	3	2.5 to 3.49
C	Good	2	1.5 to 2.49
D	Average	1	0.5 to 1.49
E	Poor	0	0.00 to 0.49

The overall grade for a programme for certification shall be based on CGPA with a 7-point scale given below

CGPA	Grade
3.80 to 4.00	A+
3.50 to 3.79	A
3.00 to 3.49	B+
2.50 to 2.99	B
2.00 to 2.49	C+
1.50 to 1.99	C
1.00 to 1.49	D

A separate minimum of C Grade for Internal and External are required for a pass for a course. For a pass in a programme a separate minimum Grade C is required for all the courses and must score a minimum CGPA of 1.50 or an overall grade of C and above.

Each course is evaluated by assigning a letter grade (A, B, C, D or E) to that course by the method of direct grading. The internal (weightage =1) and external (weightage =3) components of a course are separately graded and then combined to get the grade of the course after taking into account of their weightage.

A separate minimum of C grade is required for a pass for both internal evaluation and external evaluation for every course.

A student who fails to secure a minimum grade for a pass in a course will be permitted to write the examination along with the next batch. There will be no supplementary examinations.

After the successful completion of a semester, Semester Grade Point Average (SGPA) of a student in that semester is calculated using the formula given below. For the successful completion of semester, a student should pass all courses and score a minimum SGPA of **1.50.** However, a student is permitted to move to the next semester irrespective of her/his SGPA.

For instance, if a student has registered for ‗n' courses of credits C1, C2 ……,Cn in a semester and if she/he has scored credit points P1, P2……..,Pn respectively in these courses, then SGPA of the student in that semester is calculated using the formula.

SGPA= (P1+P2+…….+Pn)/ (C1+C2+…….+Cn)
CGPA = [(SGPA)1*S1 + (SGPA)2*S2 + (SGPA)3*S3 + (SGPA)4*S4]/ (S1+S2+S3+S4)
Where S1, S2, S3, and S4 are the total credits in semester1, semester2, semester3 and semester4.

9. Pattern of Questions

Questions shall be set to assess knowledge acquired, standard application of knowledge, application of knowledge in new situations, critical evaluation of knowledge and the ability to synthesize knowledge. The question setter shall ensure that questions covering all skills are set. He/She shall also submit a detailed scheme of evaluation along with the question paper. A question paper shall be a judicious mix of short answer type, short essay type / problem solving type and long essay type questions.

Weight : Different types of questions shall be given different weights to quantify their range as follows :

Sl. No.	**Type of Questions**	**Weight**	**Number of questions to be answered**
1	Short Answer type questions (not exceeding 1 page)	1	5 out of 8
2	Short essay / problem solving type questions (not exceeding 2 pages)	2	5 out of 8
3	Long Essay Type questions	5	3 out of 6

The Final Grade Card issued at the end of the final semester shall contain the details of all courses taken during the entire programme including those taken over and above the prescribed minimum credits for obtaining the degree. The Final Grade Card shall show the CGPA and the overall letter grade of a student for the entire programme.

CURRICULUM DESIGN ABSTRACT

Semester I

MCF 1C1 – DIGITAL ELECTRONICS AND COMPUTER ORGANIZATION
MCF 1C2 – DISCRETE MATHEMATICS AND OPERATIONS RESEARCH
MCF 1C3 – NETWORKING AND CYBER LAWS
MCF 1C4 – INTRODUCTION TO CYBER FORENSICS
MCF 1P5 -- LAB I [JAVA PROGRAMMING]

Semester II

MCF 2C1 – APPLIED CRYPTOGRAPHY
MCF 2C2 – PENETRATION TESTING AND VULNERABILITY ASSESS MENT
MCF 2C3 – STORAGE MANAGEMENT AND SECURITY
MCF 2C4 – FORENSICS AND INCIDENT RESPONSE
MCF 2P5 -- LAB II [ETHICKAL HACKING - SECURITY LAB I]

Semester III

MCF 3C1 – PRINCIPLES OF SECURE CODING
MCF 3C2 – MOBILE AND WIRELESS SECURITY
MCF 3C3 – MALWARE ANALYSIS
MCF 3C4 – DIGITAL IMAGE PROCESSING
MCF 3P5 – LAB III [ETHICKAL HACKING - SECURITYLAB II] AND MINI PROJECT

Semester IV

MCF 4C1 – RISK ASSESSMENT AND SECURITY AUDIT
MCF 4EA* - ELECTIVE1
MCF 4EB* - ELECTIVE 2
PROJECT
VIVA-VOCE

ELECTIVE GROUP A

MCF 4EA1 – USER INTERFACE DESIGN
MCF 4EA2 – SECURE SOFTWARE ENGINEERING
MCF 4EA3 – MULTIMEDIA SECURITY
MCF 4EA4 – BIOMETRIC SECURITY
MCF 4EA5 – INTERACTIVE PROGRAMMING IN PYTHON
MCF 4EA6 – DATABASE SECURITY

ELECTIVE GROUP B

MCF 4EB1 – STEGANOGRAPHY AND DIGITAL WATERMARKING
MCF 4EB2 - SECURITY THREATS AND VULNERABILITIES
MCF 4EB3 – PROFESSIONAL ETHICS AND CYBER SECURITY
MCF 4EB4 – DISTRIBUTED SYSTEM SECURITY
MCF 4EB5 – CLOUD ARCHITECTURES AND SECURITY
MCF 4EB6 -- COMPUTER AND INFORMATION SECURITY MANAGEMENT

SEMESTER	COURSE	TEACHING HOURS		CREDIT	TOTAL CREDITS
		THEORY	PRACTICALS		
I	MCF 1C1	4		4	19
	MCF 1C2	4		4	
	MCF 1C3	4		4	
	MCF 1C4	4		4	
	MCF 1P5		9	3	
II	MCF 2C1	4		4	19
	MCF 2C2	4		4	
	MCF 2C3	4		4	
	MCF 2C4	4		4	
	MCF 2P5		9	3	
III	MCF 3C1	4		4	19
	MCF 3C2	4		4	
	MCF 3C3	4		4	
	MCF 3C4	4		4	
	MCF 3P5		9	3	
IV	MCF 4C1	6		4	23
	MCF 4EA*	5		4	
	MCF 4EB*	5		4	
	PROJECT		9	8	
	VIVA-VOCE			3	

SEMESTER I

MCF 1C1 – DIGITAL ELECTRONICS AND COMPUTER ORGANIZATION

Module I **(Hours 12)**

Logic Gates, K-Map Simplification(Upto Four Varible),Combinational Circuits: Adder Circuits Multiplexer, Demultiplexer, Encoder And Decoder Circuits, Sequential Circuits: Flip-Flops, Shift Registers.

Module II **(Hours 12)**

Basic Computer Organization And Design: Instruction Codes, Computer Registers, Computer Instructions, Timing And Control.

Data Reprensation: Sign Magnitude,1's Compliment And 2's Compliment.

Module III **(Hours 12)**

Memmory Organization: Memmory Heirarchy, Main Memmory, Ram,Rom, Cache Memory: Assosiative Mapping, Direct Mapping, Set Assosiative Mapping.

Module IV **(Hours 17)**

Intel 8086 Processor: Architecture, Pins And Signals

Intel 80286 Processor: Internal Block Diagram, Signal Discriptions , Real Address Mode Operation,Protected Mode Operation.

Pentium Processor: Architecture- System Architecture, Branch Prediction.

Module V **(Hours 17)**

8051 Micro Controller: Architecture, Pins And Signals, Addressing Modes,Instruction Sets.

REFERENCES:

1.Digital Fundamentals, Thomas L Floyd, 8th Edition, Pearson publication

2.Computer System Architecture, M Morris Mano, 3rd Edition, Prentice Hall of India publication

3.Advanced Microprossers And Peripherals , A K Ray And K M Bhurchandi, 2nd Edition, Tata Mc Graw Hill Education Private Limited

4.Microprossers And Microcontrolers, A Nagoor Kani, 2nd Edition, Mc Graw Hill publication

MCF 1C2 – DISCRETE MATHEMATICS AND OPERATIONS RESEARCH

Module I **(Hours 8)**

Foundation Logic and proofs ;Basic Structures :Sets,Functions,Sequence,Sum and Matrices, Relations

Module II **(Hours 14)**

Graph: Graphs and Graphs models,Terminology and special types of Graphs,Representing Graphs and Graph isomorphism,connecitivity,Euler and Hamilton Path,Shortest path problems,plannar graphs and Graph Colouring.

Module III **(Hours 12)**

Linear programming problems - Mathematical formulation, graphical method of solution, simplex method.

Module IV **(Hours 16)**

Duality in linear programming problems, dual simplex method, sensitivity analysis, transportation and assignment problems, Traveling salesman Problem.

Module V **(Hours 18)**

Game theory Introduction, two-person zero-sum games, some basic terms, the maxminimiminimax principle, games without saddle points-Mixed Strategies, graphic solution of 2 * n and m*2 games, dominance property. CPM & PERT- project scheduling, critical path calculations, Crashing.

REFERENCES:

1.Discrete Mathematics and its Applications, 7th Edition,Kenneth H Rosen,McGraw Hill

2.Taha.H.A ,operation Research : An Introduction, McMilan publishing Co.1982.7th ed. Ravindran A, Philips D.T & Solbery.J.J,

3.Operations Research: Principles and practice, John Wiley & Sons, New York, 1987.

4.Joseph.G.Ecker & Michael Kupper Schimd, Introduction to operations Research, John Wiley & Sons, 1988.

5.Discrete Mathematical Structures with Applications to CS; Tremblery, R.Manohar, TMH

6.Discrete Mathematical for computer Scientists• & Mathematicians , Molt, Kandel, Baker, PHI

MCF 1C3 – NETWORKING AND CYBER LAWS

Module I **(Hours 10)**

Network and Internet basics,TCP/IP reference model, Comparison with OSI reference model, Network Layer: Services of Network layer, protocols-Internet Protocol(IP). IP addressing: Classful addressing, Classless addressing, Subnetting, VLSM, Supernetting. Other Network layer Protocols.

Module II **(Hours 18)**

Transport Layer: Services, elements of transport protocol, simple transport protocol.

UDP: Process to Process Communication, User Datagram and Header format, UDP operation, Use of UDP. TCP:- TCP Services, TCP features, TCP Segment Header, TCP Connection management, TCP Sockets, TCP State Transition Diagram, Flow Control, Error Control Silly Window Syndrome, TCP Congestion control, TCP timer management.

Introduction to Application Layer-HTTP,DHCP.

Module III **(Hours 10)**

Computer Crimes,Nature Of Crimes,Definition of cyber crime, Need for Cyber law, Cyber law in India, History of cyber law in India, overview of the information technology act, 2000. Important provisions of the Act:- Evidence Management,e-governce

Module IV **(Hours 16)**

Cyber crimes:- Cyber pornography, Online gambling, Intellectual Property crimes, Email spoofing, Forgery, Cyber Defamation , Cyber stalking, Unauthorized access to computer systems or networks, Theft of information contained in electronic form, Email bombing, Data diddling, Salami attacks, Denial of Service attack.

Privacy : Privacy Laws,Data Protection, data protection authority, identitytheft, medical privacy, consumer information security breaches

Module V **(Hours 16)**

Digital signature and Electronic signature, Digital Signature under the IT Act, 2000, E-Governance, Attribution, Acknowledgement and Dispatch of Electronic Records, Certifying Authorities, Duties of Subscribers, Jurisdiction, Intermediaries, Electronic Commerce, E-commerce in India, Electronic Contracts. Penalties and offences under the IT Act, 2000:- important Sections.

REFERENCES:

1.TCP/IP Protocol Suite (Mcgraw-hillForouzan Networking) 4th Edition by Behrouz A. Forouzan

2.Barkha and U. Rama Mohan, “Cyber Law Crimes”, Asia Law House, New Edition Sood,

"Cyber Laws Simplified", Mc Graw Hill

MCF 1C4 - INTRODUCTION TO CYBER FORENSICS

MODULE I **(14 Hours)**

Computer forensics fundamentals-What is computer forensics, use of computer forensics in law enforcement, Computer forensics assistance to human resource/employment proceedings, Computer forensics services, benefits of professional forensics methodology, steps taken by Computer forensics specialists, who can use Computer forensics evidence. Types of Computer forensics technology - types of military Computer forensics technology, types of law enforcement, Computer forensic technology, types of business Computer forensic technology. Types of vendor and computer forensics services- Occurrence of cyber crime, cyber detectives, computer forensics investigative services, forensics process improvement.

MODULE II **(16 Hours)**

Data recovery- Data recovery defined, data back-up and recovery, the role of back-up in data recovery, the data recovery solution. Evidence collection and data seizure- Why collective evidence, Collection options, obstacles, types of evidence, the rules if evidence, volatile evidence, general procedure, collection and archiving, methods of collection, artifacts, collection steps, controlling contamination: the chain of custody. Duplication and preservation of digital evidence - Preserving the digital crime scene, computer evidence processing steps, legal aspects of collecting and preserving Computer forensics evidence.

MODULE III **(16 Hours)**

Conducting Digital Investigations-Digital Investigation Process Models, Scaffolding for Digital Investigations, Applying the Scientific Method in Digital Investigations, Investigative Scenario: Security Breach. Handling a Digital Crime Scene-Published Guidelines for Handling Digital Crime Scenes, Fundamental Principles, Authorization, Preparing to Handle Digital Crime Scenes, Surveying the Digital Crime Scene , Preserving the Digital Crime Scene .Investigative Reconstruction with Digital Evidence -Equivocal Forensic Analysis , Victimology, Crime Scene Characteristics ,Threshold Assessments.

MODULE IV **(14 Hours)**

Violent Crime and Digital Evidence - The Role of Computers in Violent Crime, Processing the Digital Crime Scene, Investigative Reconstruction, Digital Evidence as Alibi - Investigating an Alibi, Time as Alibi, Location as Alibi. Sex Offenders on the Internet - Old

Behaviors, New Medium, Legal Considerations, Identifying and Processing Digital Evidence, Investigating Online Sexual Offenders, Investigative Reconstruction, Case Example: Scott Tyree, Case Example: Peter Chapman. Computer Intrusions - How Computer Intruders Operate, Investigating Computer Intrusions, Forensic Preservation of Volatile Data, Post-Mortem Investigation of a Compromised System, Investigation of Malicious Computer Programs, Investigative Reconstruction. Cyberstalking - How Cyberstalkers Operate, Investigating Cyberstalking, Cyberstalking, Case Example.

MODULE V **(12 Hours)**

Computer Basics for Digital Investigators - A Brief History of Computers, Basic Operation of Computers, Representation of Data, Storage Media and Data Hiding, File Systems and Location of Data, Dealing with Password Protection and Encryption Applying, Forensic Science to Computers – Preparation, Survey, Documentation , Preservation, Examination and Analysis, Reconstruction, Reporting, Digital Evidence on Windows Systems - File Systems, Data Recovery, Log Files, Registry, Internet Traces, Program Analysis. Digital Evidence on UNIX Systems - UNIX Evidence Acquisition Boot Disk, File Systems, Overview of Digital Evidence Processing Tools, Data Recovery, Log Files, File System Traces, Internet Traces, Digital Evidence on the Internet- Role of the Internet in Criminal Investigations, Internet Services: Legitimate versus Criminal Uses, Using the Internet as an Investigative Tool, Online Anonymity and Self-Protection, E-mail Forgery and Tracking, Usenet Forgery and Tracking, Searching and Tracking on IRC.

REFERENCES:

1. John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Charles River Media, 2005

2. Eoghan Casey, Digital Evidence and Computer Crime Forensic Science, Computers and the Internet Third Edition

MCF 1P5 - LAB I [JAVA PROGRAMMING]

- Program to implement the usage of packages
- Program to create our own exception
- Program for handling file operation
- Implement the concept of thread
- Applet program for passing parameters
- Applet program for running an audio file
- Program for event-driven paradigm in Java
- Event driven program for Graphical Drawing Application
- Program that uses Menu driven Application
- Program to implement JDBC in GUI and Console Application
- Web page design using HTML and client side validation using Javascript

SEMESTER II

MCF 2C1 – APPLIED CRYPTOGRAPHY

MODULE I **(12 Hours)**

Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols.

MODULE II **(12 Hours)**

Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block ChainingMode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode – Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving -Block Ciphers versus Stream Ciphers - Choosing an Algorithm - Public Key Cryptography versus Symmetric cryptography

MODULE III **(12 Hours)**

Encrypting Communications Channels - Encrypting Data for Storage -Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption -Detecting Encryption – Hiding and Destroying Information.

MODULE IV **(18 Hours)**

Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation -Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) Double Encryption - Triple Encryption .Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs . N- Hash - MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) .Message Authentication Codes

MODULE V **(16 Hours)**

RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) -Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes - Ongchnorr-Shamir -Cellular Automata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -Shamir's Three-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture.

REFERENCES:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley & Sons, Inc, 2nd Edition, 1996.

2. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004

3. Atul Kahate, "Cryptography and Network Security", Tata McGrew Hill, 2003.

MCF 2C2 – PENETRATION TESTING AND VULNERABILITY ASSESMENT

MODULE I **(12 hours)**

Ethical Hacking terminology- Five stages of hacking- Vulnerability Research- Legal implication of hacking- Impact of hacking.

MODULE II **(12 hours)**

Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks.

MODULE III **(14 hours)**

Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration.

MODULE IV **(12 hours)**

Password cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.

MODULE V **(16 hours)**

Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS Spoofing- Conduct SQL Injection attack - Countermeasures.

REFERENCES

1. Kimberly Graves, "*CEH: Official Certified Ethical Hacker Review Guide*", Wiley Publishing Inc., ISBN: 978-0-7821-4437-6, 2007.

2. Shakeel Ali &Tedi Heriyanto, "*Backtrack -4: Assuring security by penetration testing*", PACKT Publishing., ISBN: 978-1-849513-94-4, 2011.

MCF 2C3 – STORAGE MANAGEMENT AND SECURITY

MODULE I **(12 hours)**

Storage System - Introduction to Information Storage and Management, Storage System Environment, Data Protection Raid, Intelligent Storage System.

MODULE II **(14 hours)**

Storage Networking Technologies and Virtualization, Storage Networks, Network Attached Storage, IP SAN, Content Addressed Storage, Storage Virtualization.

MODULE III **(12 hours)**

Introduction to Business Continuity, Backup and Recovery, Local Replication, Remote Replication.

MODULE IV **(18 hours)**

Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking.

MODULE V **(14 hours)**

Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in
Practice.

REFERENCES:

1. Information Storage and Management, "*Storing, Managing, and Protecting Digital Information"*, Wiley; 1 edition, EMC Corporation, 2009.

2. John Chirillo, Scott Blaul, "*Storage Security: Protecting SAN, NAS and DAS"*, Wiley Publishers, 2003.

3. David Alexander , Amanda French , David Sutton ,"*Information Security Management Principles"* The British Computer Society, 2008.

MCF 2C4 – FORENSICS AND INCIDENT RESPONSE

MODULE I (12 hours)

Introduction to Incident - Incident Response Methodology – Steps - Activities in Initial Response Phase after detection of an incident.

MODULE II (18 hours)

Initial Response & Volatile Data Collection from Windows system – Initial Response & Volatile Data Collection from Unix system - Forensic Duplication: Forensic duplication:Forensic Duplicates as Admissible Evidence,Forensic Duplication Tool Requirements,Creating a Forensic Duplicate/Qualified Forensic Duplicate of a Hard Drive.

MODULE III (14 hours)

File Systems-FAT,NTFS - Forensic Analysis of File Systems – Storage Fundamentals-Storage Layer, Hard Drives Evidence Handling-Types of Evidence, Challenges in evidence handling, Overview of evidence handling procedure.

MODULE IV (12 hours)

Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud.

MODULE V (14 hours)

Data Analysis Techniques - Investigating Live Systems (Windows &Unix) - Investigating Hacker Tools - Ethical Issues – Cybercrime.

REFERENCES

1. Kevin Mandia, Chris Prosise, "*Incident Response and computer forensics*",Tata McGrawHill, 2006.

2. Peter Stephenson, "*Investigating Computer Crime: A Handbook for Corporate Investigations*", Sept 1999.

3. Eoghan Casey, *"Handbook Computer Crime Investigation's Forensic Tools and Technology"*, Academic Press, 1st Edition, 2001.

4. Skoudis. E., Perlman. R. Counter Hack: "*A Step-by-Step Guide to Computer Attacks and Effective Defenses",* .Prentice Hall Professional Technical Reference. 2001.

5. Norbert Zaenglein, "*Disk Detective: Secret You Must Know to Recover Information From a Computer*", Paladin Press, 2000.

6. Bill Nelson,Amelia Philips and Christopher Steuart, "*Guide to computer forensics and investigations*", course technology, Cengage Learning; 4thedition, ISBN: 1-435-49883-6, 2009.

MCF 2P5 - LAB II [ETHICKAL HACKING – SECURITY LAB I]

- Introduction to ethickal hacking
- Footprinting and reconnaissance
- Scanning networks
- System hacking
- Malware threats
- Sniffing
- Social engineering

SEMESTER III

MCF 3C1 – PRINCIPLES OF SECURE CODING

MODULE I **(10 hours)**

Need for secure systems- Proactive security development process- Security principles to live by and threat modelling.

MODULE II **(16 hours)**

Character strings- String manipulation errors – String Vulnerabilities and exploits – Mitigation strategies for strings- Pointers – Mitigation strategies in pointer based vulnerabilities – Buffer Overflow based vulnerabilities.

MODULE III **(14 hours)**

Dynamic memory management- Common errors in dynamic memory management- Memory managers- Double –free vulnerabilities –Integer security- Mitigation strategies.

MODULE IV **(12 hours)**

Quoting the Input – Use of stored procedures- Building SQL statements securely- XSS related attacks and remedies.

MODULE V **(18 hours)**

Requirements engineering for secure software: Misuse and abuse cases- SQUARE process model- Software security practices and knowledge for architecture and design.

REFERENCES

1. Michael Howard , David LeBlanc, "*Writing Secure Code*", Microsoft Press, 2nd Edition, 2003.

2. Robert C.Seacord, " *Secure Coding in C and C++*", Pearson Education, 2nd edition, 2013.

3. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, " *Software Security Engineering : A guide for Project Managers*", Addison-Wesley Professional, 2008.

MCF 3C2 – MOBILE AND WIRELESS SECURITY

MODULE I **(14 hours)**

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.

MODULE II **(18 hours)**

Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS Security & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security.

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, mobile phone codes, catalog tricks and AT command set- SMS security issues.

MODULE III **(12 hours)**

Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting Bluetooth, Zigbee Security, Zigbee Attacks

MODULE IV **(10 hours)**

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.

MODULE V **(16 hours)**

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 contamination.

Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locations- Seven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context

REFERENCES

1. Kia Makki, Peter Reiher, "Mobile and Wireless Network Security and Privacy ", Springer, ISBN 978-0-387-71057-0, 2007.

2. C. Siva Ram Murthy, B.S. Manoj, "Adhoc Wireless Networks Architectures and Protocols", Prentice Hall, x ISBN 9788131706885, 2007.

3. NoureddineBoudriga, "*Security of Mobile Communications"*,ISBN 9780849379413, 2010.

4. Johny Cache, Joshua Wright and Vincent Liu," *Hacking Wireless Exposed: Wireless Security Secrets & Solutions* ", second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010.

5. Gregory Kipper, "*Wireless Crime and Forensic Investigation"*, Auerbach Publications, 2007.

6. Iosif I. Androulidakis, *" Mobile phone security and forensics: A practical approach",* Springer publications, 2012.

7. Angus M.Marshall, *" Digital forensics: Digital evidence in criminal investigation",* John – Wiley and Sons, 2008.

MCF 3C3 – MALWARE ANALYSIS

MODULE I **(14 Hours)**

Introduction, Computer Virus Basics, Taxonomy, Techniques and Tools- Introduction General Aspects of Computer Infection Programs , Definitions and Basic Concepts Action Chart of Viruses or Worms, Viruses or Worms Life Cycle, Analogy Between Biological and Computer Viruses, Numerical Data and Indices, Designing Malware. Non Self-reproducing Malware (Epeian), Logic Bombs ,Trojan Horse and Lure Programs, How Do Viruses Operate, Overwriting Adding Viral Code: Appenders and Prependers Code Interlacing Infection or Hole Cavity Infection, Companion Viruses, Source Code Viruses

MODULE II **(16 Hours)**

Computer Viruses in Interpreted Programming Language - Design of a Shell Bash Virus under Linux, Fighting Over infection , Anti-antiviral Fighting: Polymorphism, Increasing the Vbash Infective Power, Including a Payload. Some Real-world Examples The Unix owr Virus, The Unix head Virus, The Unix Coco Virus, The Unix bash virus. Companion - Viruses Introduction, The vcomp ex companion virus, Analysis of the vcomp ex Virus , Weaknesses and Flaws of the vcomp ex virus .

MODULE III **(16 Hours)**

Worms – Introduction, The Internet Worm, The Action of the Internet Worm, How the Internet Worm Operated, Dealing With the Crisis, IIS Worm Code Analysis ,Buffer Overflows ,Buffer IIS Vulnerability and Buffer Overflow, Detailed Analysis of the Source Code, Xanax Worm Code Source Analysis, Main Spreading Mechanisms: Infecting E-mails, Executable Files Infection, Spreading via the IRC Channels, Final Action of the Worm. The Various Procedures of the Worm. Analysis of the UNIX. LoveLetter Worm - Variables and Procedures, How the Worm Operates.

MODULE IV **(14 Hours)**

Anti-Anti-Virus Techniques - How a Virus Detector Works, Stealth for Boot Sector Viruses, Polymorphic Viruses, Retaliating Viruses, Advanced Anti-Virus Techniques, Genetic Viruses, Who Will Win?

MODULE V **(12 Hours)**

BIOS Viruses – Introduction, bios Structure and Working, Disassembly and Analysis of the BIOS Code, Detailed Analysis of the BIOS Code , vbios Virus Description . Viral Boot Sector Concept, Installation of vbios .Computer Viruses and Applications Introduction - The State of the Art, The Xerox Worm, The KOH Virus, Military Applications, Fighting against Crime, Environmental Cryptographic Key Generation .

REFERENCES

1. ErciFiliol, "*Computer Viruses: from theory to applications*", Springer, 1st edition.

2. Mark.A .Ludwig, "*The Giant black book of computer viruses*, Create Space Independent Publishing Platform, 2 nd edition.

MCF 3C4 – DIGITAL IMAGE PROCESSING

MODULE I : (14 Hours)

Introduction – steps in image processing, Image acquisition, representation, sampling and quantization, relationship between pixels. – color models – basics of color image processing.

MODULE II : (16 Hours)

Image enhancement in spatial domain – some basic gray level transformations – histogram processing – enhancement using arithmetic , logic operations – basics of spatial filtering and smoothing.

MODULE III : (12 Hours)

Image enhancement in Frequency domain – Introduction to Fourier transform: 1- D, 2 –D DFT and its inverse transform, smoothing and sharpening filters.

MODULE IV : (16 Hours)

Image restoration: Model of degradation and restoration process – noise models – restoration in the presence of noise- periodic noise reduction.. Image segmentation: Thresholding and region based segmentation.

MODULE V : (12 Hours)

Image compression: Fundamentals – models – information theory – error free compression – Lossy compression: predictive and transform coding.JPEG and MPEG standard.

REFERENCES:

1. R.C. Gonzalez, R.E.Woods, 2002, Digital Image processing, 2nd Edition, Pearson Education.
2. Anil K. Jain, 1994, Fundamentals of Digital image Processing, 2nd Edition, Prentice Hall of India, New Delhi.
3. Pratt. W.K., Digital Image Processing, 3rd Edition, John Wiley & Sons.

4. Rosenfled A. & Kak, A.C, 1982, Digital Picture Processing, vol .I & II, Academic Press.

Website, E-learning resources (i) http://www.imageprocesssingplace.com/DIP/dip-downloads/

MCF 3P5 – LAB III [ETHICKAL HACKING - SECURITYLAB II] AND MINI PROJECT

- Denial of service
- Session hijacking
- Hacking web
- Sql injection
- Hacking wireless networks
- Hacking mobile platforms

SEMESTER IV

MCF 4C1 – RISK ASSESSMENT AND SECURITY AUDIT

MODULE I **(12 hours)**

What is Risk? –Information Security Risk Assessment Overview- Drivers, Laws and Regulations- Risk Assessment Frame work – Practical Approach.

MODULE II **(14 hours)**

The Sponsors- The Project Team- Data Collection Mechanisms- Executive Interviews- Document Requests- IT Assets Inventories- Profile & Control Survey- Consolidation.

MODULE III **(14 hours)**

Compiling Observations- Preparation of catalogs- System Risk Computation- Impact Analysis Scheme- Final Risk Score.

MODULE IV **(16 hours)**

System Risk Analysis- Risk Prioritization- System Specific Risk Treatment- Issue Registers- Methodology- Result- Risk Registers- Post Mortem.

MODULE V **(16 hours)**

Pre-planning audit- Audit Risk Assessment- Performing Audit- Internal Controls- Audit Evidence- Audit Testing- Audit Finding- Follow-up activities.

REFERENCES

1. Mark Talabis, "*Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis*", Syngress; 1 edition, ISBN: 978-1-59749-735-0, 2012.

2. David L. Cannon, "*CISA Certified Information Systems Auditor Study Guide*", John Wiley & Sons, ISBN: 978-0-470-23152-4, 2009.

MCF 4EA - ELECTIVE1

ELECTIVE GROUP A

MCF 4EA1 – USER INTERFACE DESIGN

MODULE I (12 Hours)

Introduction Introduction-Importance-Human-Computer interface-characteristics of graphics interface-Direct manipulation graphical system - web user interface-popularity-characteristic & principles

MODULE II (18 Hours)

Human Computer Interaction User interface design process- obstacles-usability-human characteristics in design - Human interaction speed-business functions-requirement analysis-Direct-Indirect methods-basic business functions-Design standards-system timings - Human consideration in screen design - structures of menus - functions of menus-contents of menu-formatting -phrasing the menu - selecting menu choice-navigating menus-graphical menus.

MODULE III (14 Hours)

Windows Windows: Characteristics-components-presentation styles-types-managementsorganizations-operations-web systems-device-based controls: characteristics-Screen -based controls: operate control - text boxes-selection control-combination control-custom controlpresentation control.

MODULE IV (12 Hours)

Multimedia Text for web pages - effective feedback-guidance & assistance-Internationalizationaccesssibility-Icons-Image-Multimedia -coloring.

MODULE V (14 Hours)

Windows Layout - Test Windows layout-test :prototypes - kinds of tests - retest - Information search - visualization - Hypermedia - www - Software tools.

REFERENCES:

1. Wilbent. O. Galitz ,"The Essential Guide to User Interface Design", John Wiley& Sons, 2001.

2. Ben Sheiderman, "Design the User Interface", Pearson Education, 1998.

3. Alan Cooper, "The Essential of User Interface Design", Wiley – Dream Tech Ltd., 2002.

MCF 4EA2 – SECURE SOFTWARE ENGINEERING

MODULE I (12 Hours)

Problem, Process, and Product - Problems of software practitioners -software reliability engineering- SRE process – defining the product – Testing acquired software

MODULE II (14 Hours)

Reliability concepts- software and hardware reliability. Implementing Operational Profiles - Developing, identifying, crating, reviewing the operation–concurrence rate–occurrence probabilities- applying operation profiles

MODULE III (18Hours)

Engineering "Just Right" Reliability - Defining "failure" for the product - Choosing a common measure for all associated systems. - Setting system failure intensity objectives - Determining user needs for reliability and availability, overall reliability and availability objectives, common failure intensity objective, developed software failure intensity objectives. - Engineering software reliability strategies. Preparing for Test - Preparing test procedures

MODULE IV (16 Hours)

Executing Test - Planning and allocating test time for the current release. - Invoking test identifying - identifying failures - Analyzing test output for deviations. – Determining which deviations are failures.. Guiding Test - Tracking reliability growth – Estimating failure intensity. - Using failure intensity patterns to guide test - Certifying reliability.

MODULE V (14 Hours)

Using UML for Security - UM L diagrams for security requirement -security business process physical security - security critical interaction - security state. Analyzing Model - Notation – formal semantics - security analysis - important security opportunities. Model based security engineering with UML - UML sec profile- Design principles for secure systems - Applying security patterns.

REFERENCES:

1. John Musa D, “Software Reliability Engineering”, 2nd Edition, Tata McGraw-Hill, 2005

2. Jan Jurjens, “Secure Systems Development with UML”, Springer; 2004

MCF 4EA3 – MULTIMEDIA SECURITY

MODULE 1 **(12 Hours)**

Digital Watermarking Basics: Models of Watermarking, Basic Message Coding, Error Correction Coding. Digital Watermarking and Digital Communications: Mutual Information and Channel Capacity.

MODULE 2 **(16 Hours)**

How to Design a Good Digital Watermark, Spread Spectrum Watermarking, Block DCT domain Watermarking, Watermarking with Side-Information (Dirty-paper Coding), Improved Spread Spectrum Watermarking, Affine-Resistant Watermarking.

MODULE 3 **(14 Hours)**

Media Specific Digital Watermarking: Image Watermarking, Video Watermarking, Audio Watermarking, Watermarking for CG-models, Watermarking for Binary Images, Watermarking for 3D Contents, Data Hiding through watermarking techniques.

MODULE 4 **(12 Hours)**

Digital Watermarking Protocols: A Buyer-Seller Watermarking Protocol, An Efficient and Anonymous Buyer-Seller, Watermarking Protocol, Extensions of Watermarking Protocols, Protocols for Secure Computation.

MODULE 5 **(16 Hours)**

Cryptography and Multimedia Encryption: Introduction to Cryptography, Multimedia Processing in the Encryption Domain, Privacy preserving Information Processing, Information Theory and Digital Forensics, Forgeries Detection, New ways for making Forgeries.

REFERENCES:

1. Digital Watermarking and Steganography, 2nd Edition, by Cox, Miller, Bloom, Fridrich, and Kalker, 2008

2. Multimedia Security Handbook, Borko Furht, Darko Kirovski, CRC Press, 2004

3. Multimedia Security Technologies for Digital Rights Management, Wenjun Zeng, HeatherYu, Ching-Yung Lin, Elsevier, 2006

MCF 4EA4 – BIOMETRIC SECURITY

MODULE I (14 Hours)

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

MODULE II (18 Hours)

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

MODULE III (16 Hours)

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 (12 Hours)

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

MODULE V (12 Hours)

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

REFERENCES:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics -Identity verification in a network”, Wiley Eastern, 2002.

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

3. John Berger,” Biometrics for Network Security”, Prentice Hall, 2004.

MCF 4EA5 – INTERACTIVE PROGRAMMING IN PYTHON

MODULE I (14 Hours)

Introduction to Interpreted Languages and Python - Data Types and variables - Operators and Expressions - Program Structure and Control - Functions and Functional Programming - Classes, Objects and other OOPS concepts.

MODULE II (12 Hours)

I/O in Python - File and Directory Access - Multithreading and Concurrency – Inter Process Communication (IPC) - Permissions and Controls

MODULE III (18 Hours)

Raw Socket basics -Socket Libraries and Functionality - Programming Servers and Clients - Programming Wired and Wireless Sniffers - Programming arbitrary packet injectors - PCAP file parsing and analysis.

MODULE IV (16 Hours)

Web Servers and Client scripting - Web Application Fuzzers - Scraping Web Applications – HTML and XML file analysis - Web Browser Emulation – Attacking Web Services - Application Proxies and Data Mangling - Automation of attacks such as SQL Injection, XSS etc.

MODULE V (12 Hours)

Exploit Development techniques - Immunity Debuggers and Libs - Writing plugins in Python - Binary data analysis - Exploit analysis Automation.

REFERENCES

1. Mike Dawson,”*More Python programming for Absolute Beginner*”, Cengage Learning PTR; 3rd edition, ISBN-10: 1435455002, ISBN-13: 978- 14354550092, 2010.

2. Mark Lutz," *Python Pocket reference",* O'Reilly Media; 4 th edition ,ISBN-10: 0596158084, ISBN-13: 978-0596158088, 2009

MCF 4EA6 – DATABASE SECURITY

MODULE I (16 Hours)

Introduction to Databases Security ,Problems in Databases Security Controls, SecurityModels – 1: Introduction Access Matrix Model .Take-Grant Model, Aclcn Model , PN Model for Distributed databases Security Models – 2:Bell and LaPadula's Model, Biba's Model, Dion's Model ,Sea View Model, Jajodia and Sandhu'r Model

MODULE II (16 Hours)

Security Mechanisms: Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System

MODULE III (14 Hours)

Security Software Design: Methodological Approach to Security Software Design ,Secure Operating System Design , Secure DBMS Design ,Security Packages ,Database Security Design

MODULE IV (14 Hours)

Statistical Database Protection & Intrusion Detection Systems: Concepts and Definitions ,Types of Attacks, Inference Controls evaluation Criteria for Control Comparison. Introduction to IDES System ,RETISS System and ASES System Discovery

MODULE V (12 Hours)

Models For The Protection Of New Generation Database Systems, Model for the Protection of Frame Based Systems, Model for the Protection of Object Oriented Systems .

REFERENCES:

1. Database Security by Castano, Silvana; Fugini, Maria Grazia; Martella, Giancarlo, Pearson Edition, 1994

2. Database Security and Auditing: Protecting Data Integrity and Accessibility 1st Edition,Hassan Afyouni Thomos Edition, 2006

MCF 4EB - ELECTIVE 2

ELECTIVE GROUP B

MCF 4EB1 – STEGANOGRAPHY AND DIGITAL WATERMARKING

MODULE I (16 Hours)

Introduction to Information hiding – Brief history and applications of information hiding– Principles of Steganography – Frameworks for secret communication – Security of Steganography systems –Information hiding in noisy data – Adaptive versus non adaptive algorithms.

MODULE II (14 Hours)

steganographic techniques – Substitution system and bitplane tools – Transform domain techniques – Spread spectrum and information hiding – Statistical Steganography - Distortion and code generation techniques – Automated generation of English text.

MODULE III (12 Hours)

Steganalysis – Detecting hidden information – Extracting hidden information - Disabling hidden information

MODULE IV (14 Hours)

Watermarking techniques – History – Basic Principles – applications – Requirements of algorithmic design issues – Evaluation and benchmarking of watermarking system.

MODULE V (16 Hours)

Watermarking techniques – Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bets - Merging the watermark and the cover – Optimization of the watermark receiver – Extension from still images to video – Robustness of copyright making systems.

REFERENCES:

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, “Information hiding techniques for Steganography and Digital Watermarking”, ARTECH House Publishers, January 2004.
2. Jessica Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications”, Cambridge university press, 2010.
3. Steganography, Abbas Cheddad, Vdm Verlag and Dr. Muller, “Digital Image” Aktienge sells chaft & Co. Kg, Dec 2009.
4. Ingemar Cox, Matthew Miller,Jeffrey Bloom,Jessica Fridrich and Ton Kalker, “Digital Watermarking And Steganography”, Morgan Kaufmann Publishers, Nov 2007.

MCF 4EB2 – SECURITY THREATS AND VULNERABILITIES

MODULE 1 **(12 Hours)**

Threats and Vulnerabilities to Information and Computing Infrastructures: Internal Security Threats, Physical Security Threats, Fixed-Line Telephone System Vulnerabilities, E-Mail Threats and Vulnerabilities, E-Commerce Vulnerabilities, Hacking Techniques in Wired Networks , Hacking Techniques in Wireless Networks, Computer Viruses and Worms, Trojan Horse Programs, Hoax Viruses and Virus Alerts, Hostile Java Applets, Spyware.

MODULE 2 **(10 Hours)**

Wireless Threats and Attacks: Wireless Threats and Attacks, WEP Security, Bluetooth Security, Cracking WEP, Denial of Service Attacks, Network Attacks, Fault Attacks, Side-Channel Attacks.

MODULE 3 **(18 Hours)**

Prevention: Keeping the Hackers and Crackers at Bay RFID and Security ,Cryptographic Privacy Protection Techniques, Cryptographic Hardware Security Modules, Smart Card Security, Client-Side Security, Server-Side Security ,Protecting Web Sites, Database Security, Medical Records Security, Access Control: Principles and Solutions, Password Authentication ,Computer and Network Authentication, Antivirus Technology, Biometric Basics and Biometric Authentication.

MODULE 4 **(16 Hours)**

Detection and Recovery: Intrusion Detection Systems Basics, Host-Based Intrusion Detection Systems , Network-Based Intrusion Detection Systems, Use of Agent Technology for

Intrusion Detection, Contingency Planning Management, Computer Security Incident Response Teams (CSIRTs) , Implementing a Security Awareness Program, Risk Assessment for Risk Management, Security Insurance and Best Practices. Auditing Information Systems Security, Evidence Collection and Analysis Tools, Information Leakage: Detection and Countermeasures.

MODULE 5 **(14 Hours)**

Management and Policy Considerations: Digital Rights Management , Web Hosting , Managing a Network Environment , E-Mail and Internet Use Policies, Forward Security: Adoptive Cryptography Time Evolution , Security Policy Guidelines , The Asset-Security Goals Continuum: A Process for Security , Multilevel Security, Multilevel Security Models ,Security Architectures , Quality of Security Service: Adaptive Security, Security Policy Enforcement , Guidelines for a Comprehensive Security System.

REFERENCES:

1. Hossein Bidgoli, Information Security, Volume 3, Threats, Vulnerabilities, Prevention, Detection,and Management, Wiley, 2006

2. Lawrence J Fennelly, Loss Prevention and Crime Prevention , Elsevier, 2004

3. Tipton Ruthbe Rg, Information Security Management, Auerbach, 1997

MCF 4EB3 – PROFESSIONAL ETHICS AND CYBER SECURITY

MODULE I **(18 Hours)**

Computer ethics and philosophical ethics: Vacuum of policies, conceptual muddles, social context, moral and legal issues, uniqueness of ethical issues, role of analogy, descriptive and normative claims, ethical relativism, utilitarianism, other theories. professional Ethics: Characteristics, the system of professions, computing as a profession, professional relationships, responsibilities, code of ethics and professional conduct. Privacy: Computers and privacy issue, reframing this issue,legislative background, better privacy protection.

MODULE II **(12 Hours)**

Intellectual property issues in cyberspace: Introduction to intellectual property Protections via Copyright, Trade Secrets, Trademarks, Patents, Contracting to protect intellectual property,

MODULE III **(16 Hours)**

Protection options –Encryption, copyright on web-content, copyright on software. Ethical Decision Making: Types of ethical choices, Making defensible decisions, Ethical dilemmas, law and ethics

MODULE IV **(14 Hours)**

Crime incident Handling Basics: Hacking, cyber activism, Tracking hackers, clues to cyber crime,privacy act, search warrants, common terms, organizational roles, procedure for responding to incidents, reporting procedures, legal considerations

MODULE V **(12 Hours)**

Information Technology Act 2000:Scope, jurisdiction, offense and contraventions, powers of police, adjudication.

REFERENCES:

1.Deborah G Johnson, " Computer Ethics", 4th Edition, Pearson Education

2.Earnest A. Kallman, J.P Grillo, "Ethical Decision making and IT: An Introduction with Cases",McGraw Hill Publication, 2008

3.John W. Rittinghouse, William M. Hancock, “Cyber security Operations Handbook”, ElsevierPub,2003
4.Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, 2nd Edition,,Cengage Learning Pub., 2012
5.Randy Weaver, Dawn Weaver, “Network Infrastructure Security”, Cengage Learning Pub., 2006
6.Barkha and U. Rama Mohan, “Cyber Law Crimes”, Asia Law House, New Edition
7.Sood,“Cyber Laws Simplified”, Mc Graw Hill

MCF 4EB4 – DISTRIBUTED SYSTEM SECURITY

MODULE I **(16 Hours)**

Introduction – Distributed Systems, Distributed Systems Security. Security in Engineering: Secure Development Lifecycle Processes - A Typical Security Engineering Process - Security Engineering Guidelines and Resources. Common Security Issues and Technologies: Security Issues, Common Security Techniques.

MODULE II **(18 Hours)**

Host-level Threats and Vulnerabilities: Transient code Vulnerabilities - Resident Code Vulnerabilities - Malware: Trojan Horse – Spyware - Worms/Viruses – Eavesdropping - Job Faults. Infrastructure- Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities - Grid Computing Threats and Vulnerabilities – Storage Threats and Vulnerabilities – Overview of Infrastructure Threats and Vulnerabilities.

MODULE III **(16 Hours)**

Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities –Injection .Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues. Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-Level Attacks - Services Threat Profile.

MODULE IV **(14 Hours)**

Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code - Memory Firewall – Antimalware. Infrastructure-Level Solutions: Network-Level Solutions - Grid- Level Solutions - Storage-Level Solutions. Application-Level Solutions: Application-Level Security Solutions.

MODULE V **(12 Hours)**

Service-Level Solutions: Services Security Policy - SOA Security Standards Stack – Standards in Dept - Deployment Architectures for SOA Security - Managing Service-Level Threats - Compliance in Financial Services - SOX Compliance - SOX Security Solutions - Multilevel Policy-Driven Solution Architecture

REFERENCES:

1. Abhijit Belapurakar, Anirban Chakrabarti and et al., "Distributed Systems Security: Issues. Processes and solutions", Wiley, Ltd., Publication, 2009.

2. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, "Distributed Systems Security: Issues, Processes and Solutions", Wiley publications, 2009.

3. Rachid Guerraoui and Franck Petit, "Stabilization, Safety, and Security of Distributed Systems",Springer, 2010

MCF 4EB5 – CLOUD ARCHITECTURES AND SECURITY

MODULE 1 **(16 Hours)**

Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

MODULE II **(14 Hours)**

Technologies and the processes required when deploying web services-Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages-Development environments for service development; Amazon, Azure, Google App.

MODULE III **(14 Hours)**

Security Concepts - Confidentiality, privacy, integrity, authentication, nonrepudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud.

MODULE IV **(14 Hours)**

Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file system security- storage considerations, backup and recovery- Virtualization System Vulnerabilities.

MODULE V **(12 Hours)**

Security management in the cloud – security management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud.

REFERENCES

1. Gautam Shroff, "*Enterprise Cloud Computing Technology Architecture Applications",* Cambridge University Press; 1 edition [ISBN: 978- 0521137355], 2010.

2. Toby Velte, Anthony Velte, Robert Elsenpeter, "*Cloud Computing, A Practical Approach",* Tata McGraw-Hill Osborne Media; 1 edition 22, [ISBN: 0071626948], 2009.

3. Tim Mather, Subra Kumaraswamy, Shahed Latif, "*Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance",* O'Reilly Media; 1 edition, [ISBN: 0596802765], 2009.

4. Ronald L. Krutz, Russell Dean Vines, "*Cloud Security",* Wiley [ISBN: 0470589876], , 2010.

MCF 4EB6 – COMPUTER AND INFORMATION SECURITY MANAGEMENT

MODULE I (14 hours)

The big picture-Learning from experience-Weaknesses in Information Security- The extent of crime in cyberspace- The cyberspace crinoids syndrome-Policies and technologies- A new framework for information security

MODULE II (14 hours)

Risk assessment-Richard Baskerville's risk assessment methodology-Generations of risk assessment techniques- Quantitative approach to risk assessment-Problems with Quantitative approach – NIST ALE- Baseline
approach.

MODULE III (16 hours)

Measuring ROI on security- Security patch management- Purposes of Information Security management- The building blocks of information security- Human side of information security-Security management- Securing new information technology.

MODULE IV (16 hours)

Overview of SSE CMM- SSE CMM relationship to other initiatives- Capability levels-Security Engineering- Security Engineering process overview- Basic process areas-Configuration management- Base practices- Establish configuration management.

MODULE V (12 hours)

Maintaining information security during downsizing- Business case for Information Security-Information Security Management in healthcare industry- Protecting high tech trade secrets-Outsourcing Security.

REFERENCES

1. Donn Parkers, " *Fighting Computer Crime: "A New Framework for Protecting Information"*, John Wiley&Sons, 2003.

2. Micki Krause, Harold F.Tripton, *" Information Security Management Handbook",* Auerbach Publications, 2012.

PROJECT

The projects should be in the field of network security, operating system security or software security. The Students should demonstrate the project using their own laptops or machines arranged by the college authorities.

The total weight of the project evaluation is 60 with a credit of 8 points.

Maximum WGP (Weighted Grade Point) = 240
Total WGP Scored = sum (grade points [A-4/B-3/C-2/D-1/E-0] X weights [20/5/7/15/2/3/8]).
GPA (Grade Point Average) = Total WGP scored / 60 (sum of the weights)

VIVA-VOCE

In Viva – voice, the examiner shall ask questions from all core courses, (including languages) and selected elective courses in the programme.

The total weight of the viva-voce is 7 with a credit of 3 points.

Maximum WGP (Weighted Grade Point) = 28

Total WGP Scored = sum (grade points [A-4/B-3/C-2/D-1/E-0] X weights [4 or 3]).

GPA (Grade Point Average) = Total WGP scored / 7 (sum of the weights)