**MAHATMA GANDHI UNIVERSITY**
**KOTTAYAM**

# M. Sc. (CYBER FORENSICS)

## PROGRAMME STRUCTURE AND SYLLABUS
**2019-20 Admissions Onwards**

**(UNDER MAHATMA GANDHI UNIVERSITY PGCSS REGULATIONS 2019)**

**EXPERT COMMITTE IN CYBER FORENSICS (PG)**
**MAHATMA GANDHI UNIVERSITY**

## EXPERT COMMITTE IN CYBER FORENSICS (PG)

### Convenor

Dr. Bindu V R, Associate Professor, School of Computer Sciences, Mahatma Gandhi University.

### Members

1. Mr. Krishnakumar M R, Associate Professor, SAS SNDP Yogam College, Konni.
2. Ms. Soumya M V, Assistant Professor, SAS SNDP Yogam College, Konni.
3. Mr. Jobin P Varghese, Assistant Professor, K E College, Mannanam.
4. Ms. Soumya M R, Assistant Professor, Sree Sankara College, Kalady.

The Expert Committee acknowledges the contributions of Ms. Rajasree G, Mr. Abdul Muhammed Rasheed, Mr. Vinu R and all other faculty members of STAS Pathanamthitta.

## Table of Contents

## M. Sc. (CYBER FORENSICS)

### 1. Aim of the Programme

Cyber Forensics is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of cyber forensics is to examine digital media in a forensically sound and constructive manner with the aim of identifying, preserving, recovering, analysing and presenting facts and evidence in a court of law. This post graduate programme in Cyber Forensics aims to mould high-quality skilled professionals in the field of computer forensics. The courses are designed with a focus on strengthening students' knowledge in all areas of cyber security and digital forensics so as to offer a wide range of research and employment prospects to the graduates.

### 2. Eligibility for Admissions

The eligibility for admission to M Sc Cyber Forensics programme offered by Mahatma Gandhi University is a B.Sc. Degree with Cyber Forensics /Computer Science /Information Technology/Electronics/Computer Applications or BCA or an equivalent degree with not less than 50% 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.

### 3. Medium of Instruction and Assessment

The medium of instruction shall be English and all internal/external assessment, examinations and evaluation shall be conducted as per Mahatma Gandhi University PG CSS Regulations 2019.

### 4. Faculty Under Which The Degree is Awarded

For the MSc Cyber Forensics programme Mahatma Gandhi University, the degree will be awarded under the Faculty of Technology and Applied Science.

### 5. Specializations Offered

Two specializations are offered by means of two groups of electives with three courses each, spread over the third and fourth semesters of the programme. Any one group can be selected and selection of courses from different groups is not allowed.

| Name Of the Programme | Specialization I (Group-A)<br>**Software Design and Digital Forensics** | | Specialization II (Group-B)<br>**Data and Cyber Security** | |
|---|---|---|---|---|
| | Course Codes | Name of the Courses | Course Codes | Name of the Courses |
| M. Sc. (Cyber Forensics) | CF800301 | Advanced Software Engineering | CF810301 | Database Concepts and Security |
| | CF800402 | Network Forensic Analysis | CF810402 | Cloud Architectures and Security |
| | CF800403 | Mobile Forensic Analysis | CF810403 | Image Processing and Security |

### 6. Compliance with the UGC Minimum Standards for the Conduct and Award of Degree

The programme is offered in accordance with the UGC Minimum Standards for the Conduct and Award of Post Graduate Degrees. A student has to secure 80 credits to complete the programme successfully.

## CURRICULUM DESIGN ABSTRACT

### SEMESTER 1

| | |
|---|---|
| CF 010101: | COMPUTER ORGANIZATION AND EMBEDDED NETWORKING |
| CF010102: | LINEAR ALGEBRA AND NATURAL LANGUAGE PROCESSING |
| CF010103: | SECURITY ANALYSIS USING PYTHON |
| CF010104: | INTRODUCTION TO CYBER FORENSICS |
| CF010105: | CYBER FORENSIC TOOLS AND PROGRAMMING IN PYTHON |

### SEMESTER 2

| | |
|---|---|
| CF 010201: | ADVANCED NETWORKING AND IOT |
| CF010202: | PENETRATION TESTING AND VULNERABILITY ASSESSMENT |
| CF010203: | ADVANCED OPERATING SYSTEMS AND STORAGE MANAGEMENT |
| CF010204: | INCIDENT RESPONSE AND CYBER LAWS |
| CF010205: | ETHICKAL HACKING AND CASE STUDIES IN JAVA-LAB 1 |

### SEMESTER 3

| | |
|---|---|
| CF010301: | CRYPTOGRAPHY AND APPLICATIONS |
| CF010302: | MOBILE AND WEB SECURITY |
| CF010303: | MALWARE ANALYSIS |
| CF8*0301: | ELECTIVE |
| CF010304: | ETHICKAL HACKING AND MINI PROJECT-LAB 2 |

### SEMESTER 4

| | |
|---|---|
| CF010401: | CYBER SECURITY RISK ASSESSMENT |
| CF8*0402: | ELECTIVE |
| CF8*0403: | ELECTIVE |
| CF010402 | PROJECT |
| CF010403 | VIVA-VOCE |

### ELECTIVE I GROUP A : SOFTWARE DESIGN AND DIGITAL FORENSICS

| | |
|---|---|
| CF800301: | ADVANCED SOFTWARE ENGINEERING |
| CF800402: | NETWORK FORENSIC ANALYSIS |
| CF800403: | MOBILE FORENSIC ANALYSIS |

### ELECTIVE II GROUP B : DATA AND CYBER SECURITY

| | |
|---|---|
| CF810301: | DATABASE CONCEPTS AND SECURITY |
| CF810402: | CLOUD ARCHITECTURES AND SECURITY |
| CF810403: | IMAGE PROCESSING AND SECURITY |

## SCHEME

| Sem | Course Code | Course Name | Course Type | Teaching Hours | | Credits | Total Credits |
|---|---|---|---|---|---|---|---|
| | | | | Theory | Practical | | |
| I | CF 010101 | COMPUTER ORGANIZATION AND EMBEDDED NETWORKING | Core | 4 | | 4 | 19 |
| | CF010102 | LINEAR ALGEBRA AND NATURAL LANGUAGE PROCESSING | Core | 4 | | 4 | |
| | CF010103 | SECURITY ANALYSIS USING PYTHON | Core | 4 | | 4 | |
| | CF010104 | INTRODUCTION TO CYBER FORENSICS | Core | 4 | | 4 | |
| | CF010105 | CYBER FORENSIC TOOLS AND PROGRAMMING IN PYTHON | Core | | 8 | 3 | |
| II | CF010201 | ADVANCED NETWORKING AND IOT | Core | 4 | | 4 | 19 |
| | CF010202 | PENETRATION TESTING AND VULNERABILITY ASSESSMENT | Core | 4 | | 4 | |
| | CF010203 | ADVANCED OPERATING SYSTEMS AND STORAGE MANAGEMENT | Core | 4 | | 4 | |
| | CF010204 | INCIDENT RESPONSE AND CYBER LAWS | Core | 4 | | 4 | |
| | CF010205 | ETHICKAL HACKING AND CASE STUDIES IN JAVA-LAB 1 | Core | | 9 | 3 | |
| III | CF010301 | CRYPTOGRAPHY AND APPLICATIONS | Core | 4 | | 4 | 20 |
| | CF010302 | MOBILE AND WEB SECURITY | Core | 4 | | 4 | |
| | CF010303 | MALWARE ANALYSIS | Core | 4 | | 4 | |
| | CF8*0301 | ELECTIVE | Elective | 4 | | 4 | |
| | CF010304 | ETHICKAL HACKING AND MINI PROJECT-LAB 2 | Core | | 9 | 4 | |
| IV | CF010401 | CYBER SECURITY RISK ASSESSMENT | Core | 5 | | 4 | 22 |
| | CF8*0402 | ELECTIVE | Elective | 5 | | 4 | |
| | CF8*0403 | ELECTIVE | Elective | 5 | | 4 | |
| | CF010402 | PROJECT | | | 10 | 8 | |
| | CF010403 | VIVA-VOCE | | | | 2 | |

*=0 or 1 since only one group shall be selected from the elective groups.

## FIRST SEMESTER COURSES

| | |
|---|---|
| CF010101 | Computer Organization and Embedded Networking |
| CF010102 | Linear Algebra and Natural Language Processing |
| CF010103 | Security Analysis Using Python |
| CF010104 | Introduction To Cyber Forensics |
| CF010105 | Cyber Forensic Tools and Programming in Python |

## Semester I

## CF010101 COMPUTER ORGANIZATION AND EMBEDDED NETWORKING

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To ensure the students acquire knowledge of organization and architecture of digital computers and embedded systems.

### UNIT I

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

Data Representation: Signed Magnitude, 1’s Complement and 2’s Complement.

### UNIT II

Memory Organization: Memory Hierarchy, Main Memory, RAM, ROM, Cache Memory: Associative Mapping, Direct Mapping, Set Associative Mapping.

### UNIT III

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

Intel 80386: Architecture pins and signals.

Pentium Processor: Architecture- System Architecture, Branch Prediction.

### UNIT IV

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

### UNIT V

Introduction to Embedded Systems: Embedded systems, Processor embedded into a system, Embedded hardware units and devices in system.

Embedded Networking- Introduction, I/O devices ports and buses- serial bus communication protocols, RS 232 standard, RS 485, RS422, CAN bus. Serial Peripheral Interface (SPI), Inter integrated circuits. Need for device drivers.

### References

1. Computer System Architecture, M Morris Mano, 3rd edition, Prentice Hall of India (PHI), 2007.
2. Advanced microprocessors and peripherals, A K Ray and K M Bhurchandi, 2nd edition, The McGraw Hill Pvt Ltd, 2012.
3. Embedded System, Architecture, Programming and Design, Raj Kamal, 2nd edition, The McGraw Hill Companies, 2009.

## CF010102 LINEAR ALGEBRA AND NATURAL LANGUAGE PROCESSING

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** This course provides the mathematical concepts of data processing in computers.

### UNIT I

Linear Algebra: Matrices and operations, Linear Systems, Vectors: Addition and Scalar Multiplication, Linear Systems of Equations.

Gauss Elimination: Linear Independence, Rank of a Matrix.

Vector Space: Solutions of Linear Systems: Existence, Uniqueness.

### UNIT II

Linear Algebra and Vector differential calculus: Determinants, Vector space,

Cramer’s Rule- Inverse of a Matrix. Gauss–Jordan Elimination- Vector Spaces, Inner Product Spaces, Linear Transformations- Vectors in 2 space and 3 space-Inner product-Vector product

### UNIT III

Linear Algebra: The Matrix Eigen value Problem, Determining Eigen values and Eigenvectors-Some Applications of Eigen value Problems- Symmetric, Skew-Symmetric, and Orthogonal Matrices –Eigen bases, Diagonalization, Quadratic Forms.

Set theory: Set notation and description, Basic set operations, Venn diagrams, Laws of set theory, Partition -min sets- Principle of inclusion and exclusion.

### UNIT IV

Logic: Propositions, Logical operators, Truth tables, Normal forms - Laws of logic - Proofs in propositional calculus – Predicates – variables – Quantifiers – Standard Forms – Inference in

Predicate calculus – Mathematical induction.

Functions and Relations: Injective, Surjective, Bijective functions - composition, identity, inverse; Relations - properties of relations - closure operations on relations.

**UNIT V**

Formal languages: Four classes of grammars (Phrase Structure, Context sensitive, Context Free, Regular) - definitions - Context free Grammar : Right most, Left most derivations – Syntax trees – Unambiguity, Ambiguity – Construction of grammars for languages – Derivation of languages from grammars – Regular expressions.

Finite automata: Definition of Deterministic Finite state Automaton (DFA), Non deterministic Finite state Automaton (NFA) - equivalence of DFA and NFA - Equivalence of regular grammars and finite automata.

Push Down Automata (PDA): Informal description - definition - Deterministic PDA - Equivalence of acceptance by final state and empty stack - Equivalence of PDA's and Context Free languages.

**References**

1. Advanced Engineering Mathematics, Erwin Kreyzig, 9th edition, John Wiley & Sons, Inc, 2006
2. Discrete mathematics and its applications, Kenneth H Rosen, 7th edition, McGraw-Hill Higher Education, 2012
3. Introduction to Automata Theory, Languages and Computation, John E Hopcroft, Rajeev Motwani, and Jeffrey D.Ullman, Addison-Wesley/Pearson, 2006.
4. Introduction to Languages and the Theory of Computation, John C Martin, 3rd edition, Tata McGraw-Hill Education Pvt. Ltd., 2007

## CF010103 SECURITY ANALYSIS USING PYTHON

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To identify and analyse the computer and network security risks using python.

**UNIT I**

Introduction-Running Python, Variables and Arithmetic Expressions, Conditionals, File Input and Output ,Strings, Lists, Tuples, Sets, Dictionaries, Iteration and Looping, Functions, Generators, Coroutines , Objects and Classes, Exceptions , Modules ,Getting Help .

Lexical Conventions and Syntax-Line Structure and Indentation, Identifiers and Reserved Words, Numeric Literals, String Literals ,Containers ,Operators, Delimiters, and Special Symbols, Documentation Strings, Decorators, Source Code Encoding.

Types and Objects-Terminology, Object Identity and Type, Reference Counting and Garbage Collection, References and Copiesm, First-Class Objects, Built-in Types for Representing Data, Built-in Types for Representing Program Structure, Built-in Types for Interpreter Internals, Object Behaviour and Special Methods.

**UNIT II**

Operators and Expressions-Operations on Numbers, Operations on Sequences, String Formatting, Advanced String Formatting, Operations on Dictionaries, Operations on Sets, Augmented Assignment The Attribute (.) Operator, The Function Call () Operator, Conversion Functions, Boolean Expressions and Truth Values, Object Equality and Identity, Order of Evaluation, Conditional Expressions

Program Structure and Control Flow-Program Structure and Execution, Conditional Execution, Loops and Iteration, Exceptions, Built-in Exceptions, Defining New Exceptions.

Functions and Functional Programming-Functions, Parameter Passing and Return Values, Scoping Rules.

**UNIT III**

Classes and Objects: Oriented Programming, The class Statement, Class Instances, Scoping Rules, Inheritance, Modules, Packages, and Distribution- Modules and the import Statement. Built-in Functions and Types.

**UNIT IV**

Network Programming and Sockets: Network Programming Basics, asyn chat, asyncore, select, socket, ssl, SocketServer. Internet Application Programming: ftp lib, http Package, smtplib, urllib Package. Web Programming-cgi, cgitb, wsgiref, web browser. Cryptographic Services.

**UNIT V**

Introducing the scope of pentesting, Approaches to pentesting , Scanning Pentesting-Ping sweep, The TCP scan concept and its implementation using a Python script, How to create an efficient IP scanner, The concept of a port scanner, How to create an efficient port scanner. Introducing a network sniffer, Implementing a network sniffer using Python. Wireless SSID finding and wireless traffic analysis by Python, Wireless attacks, The concept of foot printing of a web server, Introducing information gathering.

**References**

1. Python Essential Reference, David M. Beazley, 4 th Edition, Pearson Education, Inc., 2009
2. Python Penetration Testing Essentials, Mohit Raj, 2nd Edition, Packt Publishing Ltd, 2015
3. Python Programming: An Introduction to Computer Science , John Zelle , Michael Smith, Franklin, Beedle & Associates Inc; 2nd edition , 2010

## CF010104 INTRODUCTION TO CYBER FORENSICS

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** This course provides a broad knowledge of computer crimes and forensics**.**

**UNIT I**

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.

**UNIT II**

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.

**UNIT III**

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.

**UNIT IV**

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.

**UNIT V**

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. Computer Forensics: Computer Crime Scene Investigation, John R. Vacca, 1$^{ST}$ Edition, Charles River Media, 2005.

2. Digital Evidence and Computer Crime Forensic Science, Computers and the Internet, Eoghan Casey, 3 rd edition, Elsevier, Academic Press, 2011

## CF010105 CYBER FORENSIC TOOLS AND PROGRAMMING IN PYTHON

**Total Hours: 72**

**Total Credits: 3**

**Objective of Course:** To provide expertise in forensic tools and analysis language**.**

### CYBER FORENSIC TOOLS

- Disk Imaging Tools
- Registry Analysis
- Network Analyser

### PROGRAMMING IN PYTHON

- Basic Programmes
- Network Analysis

## SECOND SEMESTER COURSES

| | |
|---|---|
| CF010201 | Advanced Networking and IoT |
| CF010202 | Penetration Testing and Vulnerability Assessment |
| CF010203 | Advanced Operating Systems and Storage Management |
| CF010204 | Incident Response and Cyber Laws |
| CF010205 | Ethical Hacking and Case Studies in Java-Lab 1 |

## Semester II

## CF010201 ADVANCED NETWORKING AND IoT

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** This course aims to mould experts in advanced network tools and IoT

### UNIT I

Internetworking: Concepts, Architecture, and Protocols, Internet Addressing, Datagram Forwarding, Support Protocols and Technologies.

### UNIT II

The Future IP (IPv6), TCP: Reliable Transport Service, Internet Routing And Routing Protocols.

### UNIT III

Network Performance (QoS and DiffServ), Multimedia and IP Telephony (VoIP), Network Security, Trends in Networking Technologies and Uses.

### UNIT IV

Internet of Things: An Overview, Programming Frameworks for Internet of Things, Security and Privacy in the Internet of Things, Internet of Things: Robustness and Reliability.

### UNIT V

Governing Internet of Things: Issues, Approaches, and New Paradigms, Obfuscation and Diversification for Securing the Internet of Things (IoT), Applied Internet of Things, Internet of Vehicles and Applications.

### References

1. Computer Networks and Internets, Douglas E. Comer , Fifth Edition, Pearson,2009
2. Internet of Things Principles and Paradigms, Rajkumar Buyya, Amir Vahid Dastjerdi, 1 st

edition, Morgan Kaufman, 2016.

## CF010202  PENETRATION TESTIG AND VULNERABILITY ASSESSMENT

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To provide expertise in tools for finding forensic related data

### UNIT I

Penetration Testing Primer, Using Kali Linux, Programming, Information Gathering.

### UNIT II

Finding Vulnerabilities: From Nmap Version Scan to Potential Vulnerability, Nessus , The Nmap Scripting Engine, Running a Single NSE Script, Metasploit Scanner Modules, Metasploit Exploit Check Functions, Web Application Scanning, Manual Analysis.

### UNIT III

Exploitation: Revisiting MS08-067, Exploiting WebDAV Default Credentials, Exploiting Open phpMyAdmin, Downloading Sensitive Files, Exploiting a Buffer Overflow in Third-Party Software, Exploiting Third-Party Web Applications, Exploiting a Compromised Service, Exploiting Open NFS Shares.

Password Attacks- Password Management, Online Password Attacks, Offline Password Attacks, Dumping Plaintext Passwords from Memory with Windows Credential Editor.

### UNIT IV

Social Engineering: The Social-Engineer Toolkit, Spear-Phishing Attacks, Web Attacks, Mass Email Attacks, Multipronged Attacks.

Web Application Testing: Using Burp Proxy, SQL Injection, XPath Injection, Local File Inclusion, Remote File Inclusion, Command Execution, Cross-Site Scripting, Cross-Site Request Forgery, Web Application Scanning with w3af.

**UNIT V**

Wireless Attacks: Setting Up, Monitor Mode ,Capturing Packets ,Open Wireless ,Wired Equivalent Privacy, Wi-Fi Protected Access ,WPA2, Wi-Fi Protected Setup.

Using the Smartphone Pentest Framework: Mobile Attack Vectors, The Smartphone Pentest Framework, Remote Attacks, Client-Side Attacks, Malicious Apps, Mobile Post Exploitation.

**References**

1. Penetration testing A Hands-On Introduction to Hacking, Georgia Weidman, William Pollock, 2014

## CF010203 ADVANCED OPERATING SYSTEMS AND STORAGE MANAGEMENT

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** This course enables the students to learn mechanisms of operating systems and storage systems.

**UNIT I**

OS overview, Scheduling: Uniprocessor, multiprocessor, real time systems, Embedded operating system

**UNIT II**

Storage System Environment, Storage Networking Technologies and Virtualization, Storage Network, Network attached Storage, IP SAN, Content Addressed Storage, Storage Virtualization

**UNIT III**

Local And Remote Replication, Managing and monitoring the storage Infrastructure, Storage Management Activities

**UNIT IV**

Hard disk data Acqusition: Reading source data, Writing the output data

PC Based partitions: DOS partitions, Analysis Considerations, Apple Partition, Removable media

Server based partitions: BSD partition, Sun Solaris slices, GPT partition, Multiple disk volume-RAID, Disk spanning, File system analysis.

**UNIT V**

FAT concepts and analysis ,NTFS concepts, NTFS Analysis ,Ext 2 and Ext 3 concepts and analysis ,UFS 1 and UFS 2 concepts and analysis

**References**

1. File system forensic analysis, Brian Carrier, Addison Wesley, 2005.
2. Information storage and management, "storing managing and protecting digital information" G Somasundaram, Alok Shrivastava, 1st edition, wiely, 2009.

## CF010204 INCIDENT RESPONSE AND CYBER LAWS

**Total Hours: 72**

**Total Credits: 4**

**Objective Of Course:** The course provides the knowledge to produce valuable and acceptable evidence to the court of law.

**UNIT I**

The incident response process, The incident response plan, The incident response playbook Forensic Fundamentals: Digital forensic fundamentals, The digital forensic process. Acquiring Host-Based Evidence-Preparation, Evidence volatility, Evidence acquisition, Evidence collection procedures, Non-volatile data.

**UNIT II**

Network Evidence Collection: Preparation, Network device evidence, Packet capture, Evidence collection, Network Evidence Analysis-Analyzing packet captures, Analyzing network log files.

**UNIT III**

Analyzing System Memory-Memory evidence overview, Memory analysis. Forensic Reporting-Documentation overview, Incident tracking, Written reports.

**UNIT IV**

Concept of cyber crime and IT Act 2000.

Jurisdiction: Civil Law of Jurisdiction in India, Cause of Action, Jurisdiction and IT Act 2000.Indian Evidence Act Vs IT Act 2000

### UNIT V

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, Intermediaries, Electronic Commerce, E-commerce in India, Electronic Contracts. Penalties and offences under the IT Act, 2000.

### References

1. Digital Forensics and Incident Response , Gerard Johansen, 1st edition, Packt Publishing, 2017

2. Cyber Law Crimes, Barkha and U. Rama Mohan, 3rd Edition , Asia Law House, 2017

3. Cyber Laws Simplified, Vivek Sood, 3 rd edition, Mc Graw Hill Education, 2014

## CF010205 ETHICKAL HACKING AND CASE STUDIES IN JAVA - LAB 1

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To make students familiarize with various security attacks on white hackers point of view

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

### CASE STUDIES IN JAVA

- SERVLETS
- SOCKETS
- JDBC
- JAVA BEAN

## THIRD SEMESTER COURSES

| | |
|---|---|
| CF010301 | Cryptography and Applications |
| CF010302 | Mobile and Web Security |
| CF010303 | Malware Analysis |
| CF8*0301 | Elective |
| CF010304 | Ethickal Hacking  and  Mini Project-Lab 2 |

## Semester III

## CF010301 CRYPTOGRAPHY AND APPLICATIONS

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To make students learn the tools, technique and algorithms of cryptography and its applications.

**UNIT 1**

Foundations: Protocol Building Blocks, Basic Protocols, Intermediate Protocols.

**UNIT 2**

Key Length, Key Management, Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, 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

**UNIT 3**

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

**UNIT 4**

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.

**UNIT 5**

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

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

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

## CF010302 MOBILE AND WEB SECURITY

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To provide students deep knowledge of wireless and web security.

### UNIT I

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.

### UNIT II

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

CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools

### UNIT III

Web Application security, Core Defence Mechanisms, Web Application Technologies: The HTTP Protocol, Web Functionality. Mapping the Application-Enumerating Content and Functionality

### UNIT IV

Bypassing Client: Side Controls-Transmitting Data Via the Client-Hidden Form Fields,HTTP Cookies ,URL Parameters. Attacking Authentication: Design Flaws in Authentication Mechanisms, Implementation Flaws in Authentication, Securing Authentication.

### UNIT V

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.

Attacking Users: Cross-Site Scripting-Varieties of XSS, XSS Attacks in Action, Finding and Exploiting XSS Vulnerabilities, Preventing XSS Attacks

### References

1. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Dafydd Stuttard, Marcus Pinto, Second edition, Wiley, 2011

2. Mobile and Wireless Network Security and Privacy, Kia Makki, Peter Reiher, Springer, 2007.

3. Security of Mobile Communications, Noureddine Boudriga, 2010

## CF010303 MALWARE ANALYSIS

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** Ensure deep knowledge in malware mechanisms.

### UNIT I

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

**UNIT II**

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.

**UNIT III**

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.

**UNIT IV**

Anti-Anti-Virus Techniques: How a Virus Detector Works, Stealth for Boot Sector Viruses, Polymorphic Viruses, Retaliating Viruses, Advanced Anti-Virus Techniques, Genetic Viruses.

**UNIT V**

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. Computer Viruses: from theory to applications, Eric Filiol, Springer-Verlag France, 1st edition, 2005

2. The Giant black book of computer viruses, Mark.A .Ludwig, 2 nd edition, Create Space Independent Publishing Platform, 2009.

## CF010304 ETHICKAL HACKING AND MINI PROJECT – LAB 2

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To familiarize with various security attacks on white hackers point of view**.**

### ETHICKAL HACKING – LAB II

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

### MINI PROJECT

Related to Cyber Security using Python

## FOURTH SEMESTER COURSES

| | |
|---|---|
| CF010401 | Cyber Security Risk Assessment |
| CF8*0402 | Elective |
| CF8*0403 | Elective |
| CF010402 | PROJECT |
| CF010403 | VIVA-VOCE |

## Semester IV

## CF010401 CYBER SECURITY RISK ASSESSMENT

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To mould best security consultants.

### UNIT I

Security Risk Assessment: The Role of the Security Risk Assessment , Definition of a Security Risk Assessment ,The Need for a Security Risk Assessment ,Checks and Balances ,Periodic Review ,Risk-Based Spending ,Requirement , Security Risk Assessment Secondary Benefits, Related Activities : Gap Assessment , Compliance Audit , Security Audit ,Vulnerability Scanning , Penetration Testing Ad Hoc Testing , Social Engineering , Wardialing .

### UNIT II

Information Security Risk Assessment Basics: Project Definition ,Project Preparation ,Data Gathering Risk Analysis : Assets, Threat Agents and Threats-Threat Agents, Threats, Vulnerabilities, Security Risk, Risk Mitigation- Safeguards, Residual Security Risk, Risk Reporting and Resolution, Risk Resolution

Security Risk Assessment Preparation: Introduce the Team, Review Business Mission, Identify Critical Systems, Identify Assets, Asset Valuation, Identifying Threats, Determine Expected Controls

### UNIT III

Data Gathering: Sampling, The RIIOT Method of Data Gathering, Administrative Data Gathering- Threats and Safeguards, The RIIOT Method: Administrative Data Gathering, Technical Data Gathering- Technical Threats and Safeguards, The RIIOT Method: Technical Data Gathering, Physical Data Gathering- Physical Threats and Safeguards, The RIIOT Method of Physical Data Gathering.

### UNIT IV

Security Risk Analysis: Determining Risk, Creating Risk Statements, Team Review of Security Risk Statements, Security Risk Mitigation: Selecting Safeguards, Safeguard Solution Sets Establishing Risk Parameters, Security Risk Assessment Reporting: Cautions in Reporting, Pointers in Reporting, Report Structure, Document Review Methodology, Assessment Brief, Action Plan.

### UNIT V

Security Risk Assessment Project Management: Project Planning, Project Tracking, Taking Corrective Measures, Project Status Reporting, Project Conclusion and Wrap-Up, Security Risk Assessment Approaches: Quantitative vs. Qualitative Analysis, Tools

### Reference

1. The Security Risk Assessment Handbook, Douglas J. Landoll, 1st edition Reprinted 2018.

## CF010402 PROJECT

**Total Hours: 72**

**Total Credits: 8**

**Objective of Course:** The projects should be in the field of network security, operating system security or software security.

## CF010403 VIVA-VOCE

In Viva – Voce, the examiner shall ask questions from all core courses and selected elective courses in the programme.

## ELECTIVE I GROUP A: SOFTWARE DESIGN AND DIGITAL FORENSICS

### CF800301 ADVANCED SOFTWARE ENGINEERING

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course:** To familiarize with advanced software design, modelling and engineering.

**UNIT I**

Software processes: Software process models, Process activities, coping with change, The rational unified process. Requirements engineering-Functional and non-functional requirements, The software requirements document, Requirements specification, Requirements engineering processes, Requirements elicitation and analysis Requirements validation, Requirements management.

**UNIT II**

System modelling: Context models, Interaction models, Structural models, Behavioural models, Model-driven engineering. Architectural design: Architectural design decisions, Architectural views, Architectural patterns Application architectures.

**UNIT III**

Design and implementation: Object oriented design using the UML, Design patterns, Implementation issues Open source development, Software testing: Development testing, Test: driven development, Release testing, User testing. Software evolution: Evolution processes, Program evolution dynamics, Software maintenance, Legacy system management.

**UNIT IV**

Software reuse: The reuse landscape, Application frameworks, Software product lines, COTS product reuse. Component-based software engineering: Components and component models, CBSE processes, Component composition. Distributed software engineering: Distributed systems issues, Client–server computing, Architectural patterns for distributed systems, Software as a service.

**UNIT V**

Service-oriented architecture: Services as reusable components, Service engineering. Risk management. Plan driven development, Project scheduling, agile planning, Estimation techniques.

**References**

1. Software Engineering, Ian Sommerville , 9th Edition, Pearson, 2011.

## CF800402 NETWORK FORENSIC ANALYSIS

**Total Hours: 72**

**Total Credits: 4**

**Objective Of Course:** To make experts in network forensics.

**UNIT 1**

Network Intrusion Detection and Analysis: Typical NIDS/NIPS Functionality, Modes of Detection, Types of NIDS/NIPSs, NIDS/NIPS Evidence Acquisition, Comprehensive Packet Logging, Snort. Event Log Aggregation, Correlation, and Analysis: Sources of Logs, Network Log Architecture, Collecting and Analyzing Evidence.

**UNIT II**

Switches, Routers, and Firewalls: Storage Media, Switches, Routers, Firewalls, Interfaces, Logging, Web Proxies: Web Proxy Functionality, Evidence, Squid, Web Proxy Analysis, Encrypted Web Traffic.

**UNIT III**

Wireless: Network Forensics Unplugged: The IEEE Layer 2 Protocol Series, Wireless Access Points, Wireless Traffic Capture and Analysis, Common Attacks, Locating Wireless Devices.

**UNIT IV**

Packet Analysis: Protocol Analysis, Packet Analysis, Flow Analysis, Higher-Layer Traffic Analysis.

Statistical Flow Analysis: Sensors, Flow Record Export Protocols, Collection and Aggregation, Analysis.

**UNIT V**

Network Tunneling: Tunneling for Functionality, Tunneling for Confidentiality, Covert Tunneling. Malware Forensics: Trends in Malware Evolution, Network Behavior of Malware.

**Reference**

1 Network Forensics: Tracking Hackers through Cyberspace, Sherri David off, Jonathan Ham, Pearson Education, 2012

## CF800403 MOBILE FORENSIC ANALYSIS

**Total Hours: 72**

**Total Credits: 4**

**Objective Of Course:** To make experts in mobile forensic world.

**UNIT I**

Introduction to Mobile Forensics: Mobile forensics Mobile phone evidence extraction process, The preparation phase, The isolation phase, The processing phase, The verification phase.

Practical mobile forensic approaches: Mobile operating systems overview, Mobile forensic tool leveling system, Data acquisition methods. Potential evidence stored on mobile phones, Rules of evidence.

**UNIT II**

Windows Phone Forensics: Windows Phone OS, Windows phone file system, Data acquisition, Extracting the data

CASE STUDY: BlackBerry Forensics

**UNIT III**

Understanding Android: The Android model, Android security, Android file hierarchy, Android file system. A forensic environment setup-Android Software Development Kit, Android Virtual Device, Accessing the connected device, Android Debug Bridge. Accessing the device using adb-Detecting connected devices, Killing the local adb server, Accessing the adb shell. Screen lock bypassing techniques, Gaining root access.

**UNIT IV**

Android Data Recovery Techniques: Data recovery. Android App Analysis and Overview of Forensic Tools: Android app analysis, Reverse engineering Android apps, Forensic tools overview, Cellebrite – UFED, MOBILedit. CASE STUDY: Android Data Extraction Techniques

**UNIT V**

Understanding the Internals of iOS Devices: iPad hardware, File system, The HFS Plus file system. iPhone operating system. iOS security. Data Acquisition from iOS Devices: Operating modes of iOS devices, Physical acquisition, Acquisition via a custom ramdisk. Building a custom ramdisk, Booting the custom ramdisk, Bypassing the passcode, Imaging the data partition, Decrypting the data partition, Recovering the deleted data.

CASE STUDY: iOS Forensic Tools.

**Reference**

1. Practical Mobile Forensics, Satish Bommisetty,Rohit Tamma, Heather Mahalik, Packt Publishing Ltd, 2014.

## ELECTIVE II GROUP B : DATA AND CYBER SECURITY

### CF810301 DATABASE CONCEPTS AND SECURITY

**Total Hours: 72**

**Total Credits: 4**

**Objective Of Course:** To familiarize with database and its security**.**

**UNIT I**

Databases and Database Users: Introduction, Characteristics of the Database Approach, Actors on the Scene, Workers behind the Scene, Advantages of Using the DBMS Approach, A Brief History of Database Applications. Database System Concepts and Architecture: Data Models, Schemas, and Instances, Three-Schema Architecture and Data Independence, Database Languages and Interfaces, The Database System Environment, Centralized and Client/Server Architectures for DBMSs, Classification of Database Management Systems. The Relational Data Model and Relational Database Constraints-Relational Model Concepts, Relational Model Constraints and Relational Database Schemas, Update Operations, Transactions, and Dealing with Constraint Violations.

**UNIT II**

Data Modeling Using the Entity-Relationship (ER) Model-Using High-Level Conceptual Data Models for Database Design, A Sample Database Application, Entity Types, Entity Sets, Attributes, and Keys,Relationship Types, Relationship Sets, Roles, and Structural Constraints, Weak Entity Types ,ER Diagrams.

The Enhanced Entity-Relationship (EER) Model: Subclasses, Superclasses, and Inheritance, Specialization and Generalization, Constraints and Characteristics of Specialization and Generalization Hierarchies, Modeling of UNION Types Using Categories. Basics of Functional Dependencies and Normalization for Relational Databases - Functional Dependencies, Normal Forms Based on Primary Keys, General Definitions of Second and Third Normal Forms, Boyce-Codd Normal Form, Multivalued Dependency and Fourth Normal Form, Join Dependencies and

Fifth Normal Form.

### UNIT III

Introduction to Transaction Processing Concepts and Theory -Introduction to Transaction Processing, Transaction and System Concepts, Desirable Properties of Transactions, Characterizing Schedules Based on Recoverability. Concurrency Control Techniques: Two-Phase Locking Techniques for Concurrency Control, Concurrency Control Based on Timestamp Ordering.

### UNIT IV

Database Security -Introduction to Database Security Issues, Discretionary Access Control Based on Granting and Revoking Privileges, Mandatory Access Control and Role-Based Access Control for Multilevel Security, SQL Injection, Introduction to Statistical Database Security, Introduction to Flow Control, Encryption and Public Key Infrastructures, Privacy Issues and Preservation, Challenges of Database Security, Oracle Label-Based Security.

### UNIT V

Introduction: Data Mining, KDD Process, Mining Databases, Data Mining Functionalities: Characterization and Discrimination, Mining frequent patterns, Association and correlation, Classification and Prediction, Cluster Analysis.

Data Warehouse and OLAP technology: Data Warehouse, Multidimensional data Model, Data warehouse architecture, Data Warehouse implementation, OLAP, Data Warehouse and data mining.

### References

1. Fundamentals of database systems , ramez elmasri, shamkant b navathe , – 6th edition, Addison Wesley-Pearson, 2010

2. Data Mining - Concepts and Techniques, Jiawei Han and Micheline Kamber , Second Edition, Elsevier, 2006.

## CF810402 CLOUD ARCHITECTURES AND SECURITY

**Total Hours: 72**

**Total Credits: 4**

**Objective of Course**: Ensure deep knowledge in cloud systems.

**UNIT 1**

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.

**UNIT II**

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.

**UNIT III**

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.

**UNIT IV**

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.

**UNIT V**

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

**References**

1. Enterprise Cloud Computing Technology Architecture Applications, Gautam Shroff, Cambridge University Press; 1 st edition, 2010.

2. Cloud Computing, A Practical Approach, Toby Velte, Anthony Velte, Robert Elsenpeter, Tata McGraw-Hill Osborne Media; 1st edition, 2009.

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

4. Cloud Security, Ronald L. Krutz, Russell Dean Vines, Wiley, 2010.

## CF810403 IMAGE PROCESSING AND SECURITY

**Total Hours: 72**

**Total Credits: 4**

**Objective Of Course:** To familiarize with image processing and its security mechanisms.

**UNIT I**

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

**UNIT II**

Image enhancement in spatial domain: some basic gray level transformations, histogram processing, enhancement using arithmetic / logic operations, basics of spatial filtering and smoothing. Image restoration: Model of degradation and restoration process, noise models, restoration in the presence of noise, periodic noise reduction.

**UNIT III**

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

**UNIT IV**

Information Hiding, Steganography, and Watermarking, Importance of Digital Watermarking, Importance of Steganography, Applications of Watermarking, Applications of Steganography, Properties of Watermarking Systems, Properties of Steganographic and Steganalysis Systems

**UNIT V**

Models of water marking: Communications, Communication based models, geometric models, detection by correlation. Basic message coding: mapping messages into meaasge vectors. Whater marking with side information: informed embedding, watermarking using side information.

**References**

1**.** Digital Image processing, R.C. Gonzalez, R.E.Woods, 2nd Edition, Pearson Education, 2002.

2. Digital Watermarking and Steganography, Ingemar J. Cox, MattheW, L. Miller Jeffrey A. Bloom , Jessica Fridrich Ton Kalker, Second Edition, 2008.

***Model Question Paper - Format***

***QP Code (to be assigned by Exam Section)*** **Reg. No. …..**

**Name ……………**

**M Sc Cyber Forensics …….. Degree (C.S.S) Examination, ………**

**First Semester**

**Faculty of ……………**

**CF 010101 COMPUTER ORGANIZATION AND EMBEDDED NETWORKING**

**(2019 admissions onwards)**

**Time: Three hours** **Max. Weight: 30**

## Section- A

(Answer any **eight** questions. Each question carries a weight of 1)

1. What are the differences between Microprocessor and Microcontroller?

2. What are the steps to complete an instruction cycle?

3. Explain different types of data representation.

4. Explain memory hierarchy.

5.What is PSW of 8051?

6. What are the operating modes of timers of an 8051?

7. What is meant by embedded system? Mention any two examples.

8. What are the needs for device drivers?

9. What are the add mode of 8051.

10. What is the difference between real mode and protected mode?

**( 8 x 1 = 8 )**

## Section B

(Answer any **six** questions. Each question carries a weight of 2)

11. Draw the architecture of Pentium processor.
12. Explain about instruction codes.
13. What is SPI? Explain.
14. What are the hardware units inside an embedded system?
15. Explain interrupt and timer signals of 8051.
16. Explain SFR of 8051.
17. Explain timing and control unit inside a computer.
18. Explain modes of 80386 processor.

**(6 x 2 = 12)**

## Section C

(Answer any **two** questions. Each question carries a weight of 5)

19. Explain in detail about serial communication protocols.
20. Explain architecture of Intel 80286 processor.
21. Explain cache mapping methods.
22. What is meant by addressing mode? Explain with example.

**(2 x 5 = 10)**

***Model Question Paper - Format***

***QP Code ( to be assigned by Exam Section)*** **Reg. No. …..**

**Name ……………**

**M Sc Cyber Forensics Degree (C.S.S) Examination, ………**

**First Semester**

**Faculty of ……………**

**CF010103 SECURITY ANALYSIS USING PYTHON**

**(2019 admissions onwards)**

**Time: Three hours** **Max. Weight: 30**

## Section- A

(Answer any **eight** questions. Each question carries a weight of 1)

1. Write a program to calculate simple and compound interest.
2. Write a note on tuples.
3. What are the operators available in python?
4. What do you mean by augmented assignment?
5. Explain duck typing.
6. What is a package?
7. What is pickle module?
8. Explain asychat.
9. What is the need for pentesting?
10. Explain network sniffer.

**( 8 x 1 = 8 )**

## Section B

(Answer any **six** questions. Each question carries a weight of 2)

11. Explain string formatting in python.

12. Explain exceptions.

13. Write a note on object memory management.

14. What is meant by scoping rules?

15. Explain operator overloading.

16. Write a note on socket.

17. What is ftplib?

18. Write a note on ping sweep.

**(6 x 2 = 12)**

## Section C

(Answer any **two** questions. Each question carries a weight of 5.)

19. Explain inheritance with an example.

20. Explain cryptographic services in python.

21. Explain http package.

22. How do we create a port scanner? Explain with an example.

**(2 x 5 = 10)**

***Model Question Paper - Format***

***QP Code ( to be assigned by Exam Section)*** **Reg. No. …..**

**Name ……………**

**M Sc Cyber Forensic…….. Degree (C.S.S) Examination, ………**

**…..….. Semester**

**Faculty of ……………**

**CF010104- INTRODUCTION TO CYBER FORENSICS**

**(2019 admissions onwards)**

**Time: Threehours** **Max. Weight: 30**

## Section- A

(Answer any **eight** questions. Each question carries a weight of 1)

1. Define the term Computer Forensics? What are the roles of computer in a crime?

2. State the objectives of Digital Recovery and list who can use the evidence collected during Digital Recovery.

3. Differenciate between Computer Forensics and Data Recovery.

4. Mention some obstacles faced during evidence collection process.

5. Define Computer crime and Cyber crime.

6. Differenciate between FAT and NTFS.

7. Explain MBR and state its properties.

8. Define Network forensics and state the use of Network logs.

9. Explain the basics of process models.

10. What are the different services performed by specialists during computer examination?

**( 8 x 1 = 8 )**

## Section B

(Answer any **six** questions. Each question carries a weight of 2)

11. Explain how Internet could be used as an Investigative tool.
12. List the guidelines to be followed during Digital Evidence examination.
13. Explain the process for preserving the Digital crime scene.
14. Explain the benefits of Computer Forensics methodology.
15. Explain with an example how cyber stalkers operate.
16. Explain the process of recovering deleted files on Unix system.
17. Explain Digital Evidence as Alibi.
18. What are the possible sources of evidence in sex offense investigation. Explain it with figure?

(**6 x 2 = 12**)

## Section C

(Answer any **two** questions. Each question carries a weight of 5.)

19. Explain

    (i) Data back-up and recovery.

    (ii) Role of back-up in data recovery.

20. Briefly explain Digital Investigation **Process Models** with appropriate diagrams.
21. Explain

    (i) Evidence and its categories.

    (ii) Rules to be obeyed while collecting evidence.

    (iii) Basic do’s and don’ts of evidence collection.

22. Explain the Role of computers in Violent Crime. **(2 x 5 = 10)**