BHARATHIAR UNIVERSITY: COIMBATORE 641 046

B.Sc – INFORMATION SECURITY AND DIGITAL FORENSICS (3 YEARS)
(For the CCII students admitted during the academic year 2017 -2018)

SCHEME OF EXAMINATION – CBCS PATTERN

Part	Study Components	Course Title	Ins. Hrs/ week	Credits	EXAMINATIONS			
					Hours	Internals	Externals	Marks
Semester I								
I		Language-I	6	4	3	25	75	100
II		English-I	6	4	3	25	75	100
III		CORE I – Introduction to Operating System	4	4	3	25	75	100
III		CORE LAB I – Operating System Lab	4	4	3	40	60	100
III		CORE II – Fundamentals of Information Security	4	4	3	25	75	100
III		ALLIED PAPER I - Basic Mathematics for Computing	4	4	3	25	75	100
IV		Environmental Studies#	2	2	3	-	50	50
Semester II								
I		Language-II	6	4	3	25	75	100
II		English-II	6	4	3	25	75	100
III		CORE III – Introduction to Data Structures	4	4	3	25	75	100
III		CORE LAB II – Data Structures Lab	4	4	3	40	60	100
III		CORE IV– Operating System Design and Implementation	3	4	3	25	75	100
		CORE LAB III – Operating System Design and Implementation Lab	2	2	3	20	30	50
III		ALLIED PAPER II – Basic Statistical methods for Computing	3	4	3	25	75	100
IV		Value Education – Human Rights #	2	2	3	-	50	50
Semester III								
III		CORE V - Networking Fundamentals	6	4	3	25	75	100
III		CORE VI – Cryptography	6	4	3	25	75	100
III		CORE LAB IV - Networking Fundamentals Lab	5	4	3	40	60	100
III		ALLIED PAPER III - Cyber Criminology	6	4	3	25	75	100
IV		Skill based Subject : 1 - Introduction to web design	5	3	3	20	55	75
IV		Tamil @ / Advanced Tamil # (OR) Non-major elective - I (Yoga for Human Excellence) # / Women's Rights #/ Constitution of India#	2	2	3	-	50	50
Semester IV								
III		CORE VII - OSI Layers & Security Protocols	6	4	3	25	75	100
III		CORE VIII - Ethical hacking Fundamentals	6	4	3	25	75	100
III		CORE LAB V - Ethical hacking Lab	6	4	3	40	60	100
III		ALLIED PAPER IV - ISO 27000 standards	6	4	3	25	75	100

IV	Skill based Subject : 2 Case Studies and Report Writing in Cyber Crimes	4	3	3	20	55	75
IV	Tamil@/Advanced Tamil # (OR) Non-major elective -II (General Awareness #)	2	2	3	-	50	50
Semester V							
III	CORE IX - Mobile, Wireless and VOIP Security	6	4	3	25	75	100
III	CORE X - Computer Forensics and Investigation	6	4	3	25	75	100
III	CORE LAB VI - Computer Forensics Lab	6	4	3	40	60	100
III	Elective –I -	6	4	3	25	75	100
IV	Skill based Subject : 3 - Mini Project on Information Security / Digital Forensics	6	3	3	20	55	75
Semester VI							
III	CORE XI - Database Security	5	4	3	25	75	100
III	CORE XII - Web applications Security	5	4	3	25	75	100
III	CORE LAB VII - Web applications Security Lab	6	4	3	40	60	100
III	Elective –II	5	4	3	25	75	100
III	Elective –III	5	4	3	25	75	100
IV	Skill based Subject : 4 – Biometrics	4	3	3	20	55	75
V	Extension Activities @		2			50	50
Total		-	140	-	-	-	3500

Code	**Name of the Course**
Elective –I	Virtualization & Cloud Security / Forms of Cyber Crime/ Cyber Law
Elective –II	IT Governance, Risk & Compliance Management / IT and Telecommunication Frauds/ Ecommerce Application
Elective - III	Information Ethics / Incident Management/ Data Mining

@ No University Examinations. Only Continuous Internal Assessment (CIA)
# No Continuous Internal Assessment (CIA). Only University Examinations.
%% see Guidelines for Project Work.

CORE I – Introduction to Operating System

Subject Code: **Number of Credits: 04**
Subject Description: This subject deals with the fundamentals and the overview of Operating System.

Goals: To learn about the Operating System and its platform

Objective: On successful completion of the course the student should have:

- Known the basic concepts of Operating System
- How to operate and work in Operating System platform

Contents

Unit 1: Windows Operating System - Introduction to Windows Using Windows Date and Time Settings -Working with Windows Using Help - Working with Multiple Windows - Shutting down Windows Files and Folders Using Computer -Working with Folders - Working with Files Using Shortcuts Using Notepad - Creating a graphic using Paint Copying between Applications

Unit 2: Word Processing - Introduction to Microsoft Word - Creating New Documents - Entering Text -Moving through Text - Auto Correct Saving, Closing and Opening files - Navigating a Document - Editing a Document - Formatting a Document - Working with graphics - Previewing and Printing a Document - Revising a Document - Moving and Copying Selections - Working with Multiple Documents - Controlling Document - Paging Finding and Replacing text - Inserting the Current Date - Modifying Page Layout - Paragraph Formatting in detail - Character Formatting in detail - Creating Lists Using Hyperlinks - Adding an AutoText entry Using AutoShapes - Editing while previewing - Inserting Objects Creating and Modifying an Outline - Saving to a new folder - Hiding Spelling and Grammar errors - Formatting Documents automatically - Creating a Table of Contents - Formatting a Document Section - Footnoting a document section - Footnoting a document Adding Bookmarks - Formatting picture layout - Referencing figures - Creating a Simple Table - Sorting a List - Creating Headers and Footers - Checking the document - Updating the Table of Contents - Printing Selected Pages - Creating Newsletter Style Columns Using Word Art - Inserting Symbols - Adding a Drop Cap - Using Mail Merge - Printing Mailing Labels - Preparing and Printing envelopes - Merging for sending emails using Outlook - Using a Template from Word - Selecting the Template type

Unit 3: Brief Introduction Features of Microsoft Excel Parts of a worksheet - Navigating the Excel worksheet - Creating a new workbook - Entering and editing data - Changing Column Width Saving , closing and opening a workbook - Moving cells - Centering and Merging cells Using formulae Duplicating cell contents - Using functions - Formatting the worksheet - Working with Graphics - Entering the date - Previewing and printing - Learning about charts - Creating a chart - Correcting errors - Working with sheets - Managing large sheets - Forecasting values - Customizing print settings - electronic spreadsheet - Introduction to Access - Creating a new database - Creating a Table Entering and editing data Changing column width Preview and print a table Close and open a table and database Customizing and inserting fields Finding and replacing data Sorting records - Using form wizard - Adding records in a form Using queries - Creating reports - Modifying report design - Printing a report - Creating report from query – database - Introduction to DBMS - Creating a new

database - Entering and editing table data Changing column width Close, open a table and database - Inserting fields Sorting records Using queries Using Reports

Unit 4: Introduction to Presentation Graphics - Using the AutoContent Wizard - View and edit a presentation - Save and open a presentation Check spellings - Delete, Move, and Insert slides Size and move placeholders - Run a slide show - Change Fonts and Formatting - Inserting clips and clip art - Preview And Print A Presentation - Find and Replace Text - Create and Enhance a Table Modify graphics objects and create a text box - Changing the Presentation Design and Color Scheme - Change slide and title masters - Hide the Slide Footer Duplicate and hide slides - Create and Enhance AutoShapes - Adding animation, sound, transition and effects Control and annotate a slide show - Create speaker notes - Check style consistency - Document a file Print scaled and framed handouts - Creating a new presentation from existing slides - Delivering Presentations - Adding Action Buttons

Unit 5: Introduction to Microsoft Calendar - Creating an Appointment Creating a recurring appointment Creating an event - Changing the calendar view - Creating a task list - Categorizing tasks - Sorting tasks - Using a task timeline - Updating the task status - Printing tasks and calendar items - Creating Notes - Address Book in Outlook - Adding Contacts Removing Contacts - Importing & Exporting Contacts - Searching Address Books - Creating and editing mailing lists.

Text Books:

- Milan Milenkovic, "Operating Systems", TATA McGRAW HILL, 2009
- Andrew S. Tanenbaum, "Operating Systems: Design and Implementation" (Second Edition)., , 2010

Reference Books:

- D. Irtegov, "Operating Systems Fundamentals" 2005
- M. Burgess, "A Short Introduction to Operating Systems" , 2010

CORE LAB I – Operating System Lab

Subject Code: **Number of Credits: 04**

List of Experiments:

- Installing Windows 7
- Using Windows Upgrade Advisor or Upgrade Assistance
- Migrating to Windows 7 using Windows Easy Transfer and User State Migration Tool.
- Capturing image of existing installed operating system and deploy it to another system using imagex.
- Configuring disk partitions, Virtual HD in Disk Management.
- Installing and configuring device drivers.
- Configuring User Account Control Policy.
- Configuring Shared Folders.
- Configuring NTFS permissions.
- Encrypting and compressing Files.
- Installing printer and configuring basic functions.
- Configuring wireless Ad-Hoc network.
- Configuring Local Security policies.

- Configuring Bit Locker and Bit Locker to Go.
- Configuring application restriction using software restriction policy and AppLocker.
- Configuring Basic and Advanced Windows Firewall.
- Configuring IE8 properties.
- Configure scanning using Windows Defender.
- Configure Remote Desktop and Remote Assistance.
- Configuring Home Group.

CORE II – Fundamentals of Information Security

Subject Code: **Number of Credits: 04**
Subject Description: This subject deals with Security Threats and Vulnerabilities, Information Security Domains

Goals: It helps the students to acquire knowledge on confidentiality, integrity and authenticity, Security Threats and Vulnerabilities

Objective: Students will be able to:

- State the basic concepts in information security, including security policies, security models, and various security mechanisms
- Understand the fundamentals of information security risk assessments.
- Identify and Analyze the vulnerabilities in any computing system
- Identify and classify the assets as per asset classification policy

Contents:
Unit 1: Basics of Information Security and Threats: Introduction to Information Security – Common threats: Errors and Omissions – Fraud and Theft – Malicious hackers – Malicious Code – Denial of Service attacks – Social Engineering – Common types of Social Engineering

Unit 2: Information Classification – Definitions – Information, Data, Information System, Difference between data and information - Information system Asset inventory, Asset Classification criteria, roles and responsibilities – Methodology - Declassification or Reclassification - Retention and Disposal of Information Assets - Provide Authorization for Access.

Unit 3: Access Control – Definition of Access control – Types of Access Control - Access control policies – User access management – System and network Access Control – Operating System - Access Control – Monitoring system access

Unit 4: Risk Analysis and risk Management – Definition of Risk , Information Security Risk, Risk Management - Risk analysis, Information Security Lifecycle – Risk analysis process - Need for Risk Assessment - Risk Assessment Methodology - Risk Assessment Components - Risk Mitigation Techniques.

Unit 5: Introduction to Security Domains – Application Security, Legal & Compliance, Business Continuity Management, Cryptography, Physical & Environmental Security and Security Operations

Text Books:

- Thomas R. Peltier, "Information Security Fundamentals", Second Edition, Auerbach Publications, (19 November 2013)

- Dr. Timothy Shimeall & Jonathan Spring "Introduction to Information Security - A Strategic based approach", 1st Edition, Syngress Publication.

Reference Books:

- Ronald L. Krutz, Russel Dean Vines "The CISSP Prep Guide: Gold Edition", Gold Edition, Wiley Publication.
- Ed Tittel, Mike Chapple, James Michael Stewart "Certified Information Systems Security Professional, Study Guide", 6th Edition, Sybex Publication.

ALLIED PAPER I - Basic Mathematics for Computing

Subject Code: **Number of Credits: 04**
Subject Description: This course presents the properties of matrices and concepts of probability.

Goals: To enable the student to learn the mathematical foundations of computer science.

Objective: On successful completion of the course the student should have:
- Understood the mathematical logic grammars and languages.
- Learned probability concepts.

Contents:

Unit 1: Matrices: Types of Matrices - Matrix Operations - Inverse of a Matrix - Properties of Determinants - Eigen Values - Cayley-Hamilton Theorem. Set Theory: Basic Set Operations - Relations and Functions – Relation Matrices - Principle of Mathematical Induction.

Unit 2: Introduction to Probability: Sample Space and Events - Axioms of Probability - Conditional Probability – Independence of Events - Bayes Theorem. Regression and Correlation: Introduction – Linear Regression – Method of Least Squares – Normal Regression Analysis – Normal Correlation Analysis.

Unit 3: Grammars and Languages: Context Free Grammars – Introduction – Context Free Grammars – Derivation Trees. Finite Automata: Finite State Systems – Basic Definitions – Non Deterministic Finite Automata**.**

Unit 4: Mathematical Logic: Statements and Notations – Connectives – Consistency of Premises and Indirect Method of Proof – Automatic Theorem Proving.

Unit 5: Numerical Methods Finding Roots: Bisection Method – Regular –Falsi Method - Newton–Raphson Method. Solution of Simultaneous Linear Equations: Gaussian Elimination - Gauss-Seidal Method. Numerical Integration: Trapezoidal Rule - Simpson s Rule**.**

Text Books:

- M. K. Venkataraman, "Engineering Mathematics", Volume II, National Publishing Company.
- John E. Freunds, Irwin Miller, Marylees Miller, "Mathematical Statistics, Pearson Education, Sixth Edition.
- Hopcroft and Ullman, "Introduction to Automata Theory, Languages and Computation , Pearson Education, Second Edition.
- Tremblay and Manohar, "Discrete Mathematical Structures with Applications to Computer Science , Tata McGraw-Hill.

Reference Books:

- Rama B. Bhat, Snehashish Chakraverty, "Numerical Analysis in Engineering , Narosa Publishing House, 2004.
- Radha Muthu, T. Santha, "Discrete Mathematics for Computer Science and Applications, Kalaikathir Achchagam, Coimbatore, 2003.

CORE III – Introduction to Data Structures

Subject Code: **Number of Credits: 04**
Subject Description: This subject deals with Data Structures

Goals: It helps the students to understand the Data Structure Array, Stack and Recursion, Linear Linked List, Binary Search Trees, Data Structure Graphs

Objective: To inculcate knowledge on Data Structures, Queues, Linked List

Contents:
Unit 1: Introduction to Data structure Array – Introduction to Data Structure Array – Array operations – Number of elements in an array - Representation of Array in memory

Unit 2: Stack and Recursion - Stack, Queue and Recursion, Stacks: Array Representation - Linked Representation - Arithmetic Expression - Polish Notation – Recursion - Towers of Hanoi - Queues: Array Representation, Circular – Queues - Linked Representation, D-Queues - Priority Queues.

Unit 3: Linear Linked List - Linear Linked List - Singly Linked List: Representation in Memory - Traversing, Searching - Memory Allocation - Insertion into a linked list - Deletion from a linked list - Header Linked List - Polynomial Addition - Circular Linked List - Operations on Doubly Linked List.

Unit 4: Data Structure and Binary Search Trees -Non-Linear Data Structure Graphs Binary Trees - Representation of binary Trees in Memory - Traversing binary trees - Traversal algorithm using stacks - Header nodes – Threads - Binary search trees – Searching - Inserting and Deleting in a binary search trees - AVL search tree - Insertion and Deletion in an AVL search Tree - m-way search tree - Searching Insertion and Deletion in an m-way search tree - Searching, Insertion and Deletion in a B-tree

Unit 5: Representation of Graphs - Non-Linear Data Structure Graphs - Graph theory terminology - Sequential Representation of Graphs - Adjancy Matrix - Path Matrix - Warshall's algorithm - Shortest Paths - Linked Representation of a Graph - Operations on Graph - Traversing on Graphs – Posets - Topological Sorting.

Text Books:

- G. A. V. Pai, "Data Structures and Algorithms: Concepts - Techniques and Applications", McGraw Hill Education (30 January 2008)
- Jean Paul Tremblay, Paul G. Sorenson, "An Introduction to Data Structures with Applications", Tata McGraw Hill, Second Edition.

Reference Books:

- Aho "Data Structures and Algorithms", Pearson Education India; 1 edition (2002)
- Sahini, "Data Structures, Algorithms and Applications in C++", Mc GrawHill, 1998.

CORE LAB II – Data Structures Lab

Subject Code: **Number of Credits: 04**

List of Experiments:

- Linear Search
- Finding the maximum element in an array
- Create 5 nodes in singly linked list
- Insert an element in the beginning of singly linked list.
- Insert an element in the end of singly linked list.
- Insert an element at any position in singly linked list.
- Counting the number of nodes in singly linked list.
- Implement stack using array.
- Implement stack using linked list.
- Implement circular queue
- Insert an element at any position in doubly linked list.
- Delete a node at given position in doubly linked list.
- Tower of Hanoi.

CORE IV: Operating System Design and Implementation

Subject Code: **Number of Credits: 04**

Subject Description: This subject deals with the fundamentals and the concepts of LINUX/ UNIX.

Goals: To learn about the fundamentals and exploring the concepts of LINUX/ UNIX

Objective: On successful completion of the course the student should be able to understand

- Basics in LINUX/ UNIX.
- File Systems
- System Structure
- Process control in Linux

Contents

Unit 1: Introduction - Introduction to LINUX - LINUX distributions - Operating System and LINUX – History of LINUX/ UNIX – LINUX overview – LINUX software – online LINUX information sources – LINUX documentation

Unit 2: General Overview of the System - System Structure - User Perspective - Operating System Services -Assumption about Hardware - The Kernel and Buffer Cache Architecture of UNIX Operating System - System Concepts - Buffer Headers - Structure of the Buffer Pool - Scenarios for Retrieval of the Buffer - Reading and Writing Disk Units - Advantages and Disadvantages of Buffer Cache.

Unit 3: Exploring Linux Flavors – Software management – Software packaging types – Red hat package Manager – Debian – Installing software from compressed software archives – command and program directories - Ubuntu – History – Versions - Installation – Features - Ubuntu one - Fedora: History, Versions, Installation, Features

Unit 4: File Systems – File Systems: inodes – blocks – super blocks – ext 3 – ext4 – managing file systems: mounting and unmounting local disks – using fsck – Adding a new disk: Overview of partitions – traditional disk and partition naming conventions – Volume Management – Creating file systems

Unit 5: Structures of Processes and Process Control - Process States and Transitions Layout of System Memory - The Context of a Process - Manipulation of the Process Address Space - Sleep Process Creation/Termination -The User ID of a Process - Changing the Size of a Process - The Shell - Case Study of Various LINUX Versions.

Text Books:

- Wale Soyinka, "Linux Administration: A Beginners Guide", Sixth Edition (Networking & Communication - OMG), 6 edition, McGraw-Hill Education, 1 April 2012
- Neil Matthew, Richard Stones, "Beginning Linux Programming", Third Edition, Wrox, Wiley Publishing Inc., 2004

Reference Books:

- Kenneth Rosen, Douglas Host, Rachel Klee, Richard Rosinski, "UNIX: The Complete Reference", Second Edition, McGraw Hill Education, 2007
- Knowledge flow, "Beginning Linux Programming", Kindle Edition, Knowledge flow (21 April 2015)

CORE LAB III – Operating System Design and Implementation Lab

Subject Code: **Number of Credits: 02**

List of Experiments:

- Basic Shell Commands

Shell Programs:

- Fibonacci Series
- Designing Calculator
- File Operations
- Base conversion
- Usage of cut and grep commands
- Usage of user defined functions

Administration

- Managing User Accounts
- User Quota Management
- Installation of RPM software and Zipping,tar
- Configuring RAID
- Configuring Web server

ALLIED PAPER II – Basic Statistical methods for Computing

Subject Code: **Number of Credits: 04**
Subject Description: This subject deals with the concepts of Statistical methods for Computing.

Goals: To learn about the fundamentals and exploring the concepts of Statistical methods for Computing

Objective: On successful completion of the course the student should be able to understand

- Graphical methods
- Descriptive Statistics
- Symmetric frequency distribution
- Probability and Non Probability Methods of Statistics

Contents

Unit 1 : Data condensation and Graphical methods - Raw data, attributes and variables, discrete and continuous variables - Presentation of data using frequency distribution and cumulative frequency distribution - Graphical Presentation of frequency distribution –histogram, stem and leaf chart, less than and more than type of curves - Numerical problems related to real life situations.

Unit 2: Review/Revision of Descriptive Statistics - Measures of Central tendency: Mean, Mode, Median. Examples - Partition values - Quartiles, Box-Plot - Measures of Dispersion: Variance, Standard Deviation, and Coefficient of Variation.

Unit 3: Concept of symmetric frequency distribution, skewness, positive and negative skewness - Measures of skewness - Pearson's measure, Bowley's measure, $\beta 1$, $\gamma 1$. - Kurtosis of a frequency distribution, measure of kurtosis($\beta 2$,$\gamma 2$) based upon moments, type of kurtosis: leptokurtic, platykurtic and mesokurtic - Numerical problems related to real life situations - Discrete Random variable.

Unit 4: Correlation (for bivariate raw data) - Bivariate data, Scatter diagram - Correlation, Positive Correlation, Negative Correlation, Zero Correlation – Karl Pearson's coefficient of correlation (r), limits of r ($-1 \leq r \leq 1$), interpretation of r, Coefficient of determination (r2), Auto-correlation upto lags 2 – Numerical Problems – Regression – Types of Regression – Application of Regression techniques.

Unit 5: Probability and Non Probability Methods of Statistics - Theories of Probability - Counting Principles, Permutation, and Combination - Deterministic and non-determination models- Random Experiment, Sample Spaces (finite and countably infinite) - Events: types of events, Operations on events- Probability - classical definition, probability models, axioms of probability, probability of an event.

Text Books:

- Geof H. Givens, Jennifer A. Hoeting, Computational Statistics (Wiley Series in Probability and Statistics), Wiley-Blackwell (18 February 2005)
- James E. Gentle, Computational Statistics (Statistics and Computing), Springer; 2009 edition (14 March 2012)

Reference Books:

- Günther Sawitzki, Computational Statistics: An Introduction to R, 1st , Kindle Edition, Chapman and Hall/CRC; 1 edition (26 January 2009)
- James E. Gentle, Elements of Computational Statistics (Statistics and Computing), Springer; Softcover reprint of the original 1st ed. 2002 edition (4 December 2010)

CORE V - Networking Fundamentals

Subject Code: **Number of Credits: 04**
Subject Description: This course deals with the networking fundamentals

Goals: The goal of this course is to make a student understand the fundamentals of networking

Objective: End of this course a candidate will be able to understand:

- LAN Configuration Contents
- IP Addressing
- Routing Protocols
- WAN
- Networking to the end user

Contents:

Unit 1: Fundamentals of Networking – Definition and concepts of networking and their importance – Networking, Protocols - Routers, Firewalls, Hub, Port, Internet, Intranet - WWW – Types of networking, functioning, advantages and disadvantages – Application of networking in information security.

Unit 2: IP Address – Definition IP Address and VoIP – Components of IP Address **–** IP address location **-**Implementing an IP addressing scheme and IP services to meet network requirements for a small branch office - Implement an IP addressing scheme and IP Services to meet network requirements in a medium-size Enterprise branch office network

Unit 3: Routing Protocols - Implement a small routed network - Configure and troubleshoot basic operation and routing on Cisco devices - Open Shortest Path First (OSPF) - Routing Information Protocol (RIP) - Intermediate System to Intermediate System (IS-IS), EIGRP

Unit 4: LAN & WAN - LAN Configuration **-** Describe the operation of networks - Implement a small switched network - Configure - verify and troubleshoot a switch with VLANs and inter-switch communications - Identify security threats to a network and describe general methods to mitigate those threats – WAN - Explain and select the appropriate administrative tasks required for a WLAN – Implement – verify and troubleshoot NAT and ACLs in a medium-size Enterprise branch office network - Implement and verify WAN links

Unit 5: Networking to the end user - Configuring Server for enterprise networking - Introduction to Domains and Work groups - Understanding DNS and configuring DNS - Introduction to ADS (Active Directory Service) - File sharing within network - Understanding DHCP - Introduction to Mail Exchange server and ISA server - Network operating system - Client Server applications - Peer to Peer Applications - Measuring performance - Monitoring tools.

Text Books:

- Bill Ferguson, "CompTIA Network+ review guide", Second Edition, Pub: John Wiley & Sons Inc. 2008
- Todd Lamle, "Ccna Cisco Certified Network Associate Study Guide Exam 640-802", Sybex, 2009

Reference Books:

- Wendell Odom, "CCNA INTRO exam certification guide: CCNA self-stud", Cisco Press
- Deal, Richard, "CCNA Cisco Certified Network Associate Study Guide (Exam 640-802)" McGraw Hill

CORE VI – Cryptography

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with an overview of Cryptography

Goals: The goal of this paper is to make a student learn the basic concepts of Cryptography, Algorithms, Key Management, and Encryption Techniques

Objective: To inculcate knowledge on Cryptography and its Techniques

Contents

Unit 1: Introduction to Cryptography - Defining Cryptography , Privacy, Authentication, Shift Cipher - The Confidentiality - Integrity & Availability (CIA) Triad - Cryptographic concepts - methodologies &practices - Symmetric& Asymmetric cryptography - public& private keys - Cryptographic algorithms and uses - Construction& use of Digital signatures

Unit 2: Types of Algorithms - The basic functionality of hash/crypto algorithms (DES, RSA, SHA, MD5, HMAC, DSA) and effects on key length concepts in Elliptical Curve Cryptography & Quantum Cryptography

Unit 3: Key Management - The basic functions involved in key management including creation – distribution – verification - revocation and destruction – storage - recovery and life span and how these functions affect cryptographic integrity

Unit 4: Application of Cryptography - Major key distribution methods and algorithms including Kerberos - ISAKMP etc., - Vulnerabilities to cryptographic functions - the Use and functions of Certifying Authorities (CAs) - Public Key Infrastructure (PKI) and System architecture requirements for implementing cryptographic functions

Unit 5: Cryptology - Classical Encryption Techniques - Substitution Techniques - Transposition Techniques –- Permutation Methods - Confidentiality using conventional encryption - Placement of Encryption - Symmetric and Asymmetric crypto systems – common crypto standards and applications

Text Books:

- V. V. I Ashchenko, "Cryptography: An Introduction", Pub: American Mathematical Society – 2002
- John E. Hershey, "Cryptography demystified", McGraw-Hill Education (1 September 2002)

Reference Books:

- Song Y. Yan, "Cryptanalytic attacks on RSA", Springer; Softcover reprint of hardcover 1st ed. 2008 edition (12 February 2010)
- Harold F. Tipton, "Official (ISC)2 Guide to the CISSP CBK", Second Edition - 2005

CORE LAB IV - Networking Fundamentals Lab

Subject Code: **Number of Credits: 04**

List of Experiments:

- Types of Network Topologies
- Configuring Local Area Network
- Configuring Client – Server Architecture
- Configuring Domain Controller
- Configuring User Controller and assigning the user rights
- Configuring Static routers
- Configuring Dynamic routers
- Configuring Firewalls
- Configuring Intrusion Detection Systems
- Configuring Intrusion Prevention Systems

ALLIED PAPER III - Cyber Criminology

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with the fundamentals of cyber Criminology

Goals: The goal of this paper is to make a student learn the basic concepts of Criminology and Cyber Criminology

Objective: On successful completion of the course the student should have understood both investigative and preventative techniques

Contents

Unit 1: Cyber Criminology Concepts – Definitions of Cyber Crime, Cyber Criminology, Cyber Psychology, Criminal Psychology, Offender, Victimology, Victim Assistance, GRC, Incident Response

Unit 2: Understanding criminal behavior – Psychological Perspective – Theories of Personality – Freud, Erickson, Eysenck, Theories of Motivation – Maslow, Alderfer's ERG theory, Acquired Needs Theory (mcclellan) – Theories of Learning – Reinforcement learning, social learning, Sutherland's Differential Association Theory

Unit 3: Understanding criminal behavior – Sociological Perspective – Robert Merton's Anomie theory, Social Control Theories, Labelling Theory, Broken Window Theory, Shaming and Reintegration theory , Routine Activities Theory, Rational Choice Theory

Unit 4: Understanding Victimological perspectives – Victim precipitation, Victim proneness, victim responsiveness, – Life Style Exposure theory – Victim Assistance – Compensation and Restitution – UN Basic Principles of the Rights of Victims of Crime and Abuse of Power.

Unit 5: Criminal Justice System – Three Pillars of CJS – Setup, Role and Functions of State and Central Police – F.I.R., Charge Sheet, Investigation and Investigation Procedure - Central Police Establishments – Cyber Crime Police Stations – Courts, Types of Courts, setup and their functions – Cyber Crime Appellate Tribunals - Sentencing

Text Books:

- Sudhir Naib, "The Information Technology Act, 2005: A Handbook", OUP, New York,(2011)
- S. R. Bhansali, "Information Technology Act, 2000", University Book House Pvt. Ltd, Jaipur (2003).
- Vasu Deva, "Cyber Crimes and Law Enforcement", Commonwealth Publishers, New Delhi,(2003).

Reference Books:

- Chris Reed & John Angel, "Computer Law", OUP, New York, (2007).
- Justice Yatindra Singh, "Cyber Laws", Universal Law Publishing Co, New Delhi, (2012).
- Verma S, K, Mittal Raman, "Legal Dimensions of Cyber Space", Indian Law Institute, New Delhi, (2004)
- Jonthan Rosenoer, "Cyber Law", Springer, New York, (1997).

Skill based Subject: 1 Introduction to Web Design

Subject Code: **Number of Credits: 03**

Subject Description: This course deals with the Basics of Web Design

Goals: The goal of this paper is to make a student learn the basic concepts of Web Design

Objective: On successful completion of the course the student should have understood

- Web Design Principles
- Basics of Web Design
- Cascading Style Sheets
- Web Publishing or Hosting
- Image & Graphics

Contents

Unit 1: Web Design Principles - Basic principles involved in developing a web site - Planning process - Five Golden rules of web designing - Designing navigation bar - Page design - Home Page Layout - Design Concept.

Unit 2: Basics of Web Design : Brief History of Internet - What is World Wide Web - Why create a web site - Web Standards - Audience requirement - Introduction to HTML - - HTML Documents - Basic structure of an HTML document - Creating an HTML document- Mark up Tags - Heading-Paragraphs - Line Breaks - HTML Tags - Elements of HTML - Introduction to elements of HTML - Working with Text - Working with Lists, Tables and Frames - Working with Hyperlinks, Images and Multimedia - Working with Forms and controls.

Unit 3: Introduction to Cascading Style Sheets - Concept of CSS - Creating Style Sheet - CSS Properties – CSS Styling(Background, Text Format, Controlling Fonts) - Working with block elements and objects - Working with Lists and Tables - CSS Id and Class - Box Model(Introduction, Border properties, Padding Properties, Margin properties) - CSS Advanced(Grouping, Dimension,

Display,Positioning, Floating, Align,Pseudo class, Navigation Bar, Image Sprites, Attribute sector) - CSS Color - Creating page Layout and Site Designs.

Unit 4: Introduction to Web Publishing or Hosting - Creating the Web Site - Saving the site - Working on the web site - Creating web site structure - Creating Titles for web pages - Themes- Publishing web sites.

Unit 5: Introduction to Image & Graphics - Why are image & graphics important in Multimedia - Integrating image & graphics in Multimedia - Understanding kinds of Graphics - Concept of Graphics-2D & 3D Graphics.

Text Books:

- Jon Duckett, Web Design with HTML, CSS, JavaScript and jQuery Set, Wiley; Pck edition (15 August 2014)
- DT Editorial Services, HTML 5 Black Book, Covers CSS 3, JavaScript, XML, XHTML, AJAX, PHP and jQuery, Dreamtech Press; Second edition (2016)

Reference Books:

- Laura Lemay, Rafe Colburn, Jennifer Kyrnin, Mastering HTML, CSS & Javascript Web Publishing, BPB Publications; First edition (15 July 2016)
- Jon Duckett, HTML and CSS: Design and Build Websites, Wiley (18 November 2011)

CORE VII - OSI Layers & Security Protocols

Subject Code: **Number of Credits: 04**
Subject Description: This course deals with OSI Layers & Security Protocols

Goals: The students will be expected to understand the OSI Layers & Security Protocols

Objective: On successful completion of the course the student should have understood

- Open Systems Interconnection (OSI) Model
- Security Protocols
- Transport Layer
- Network Layer
- Data Link Layer

Contents
Unit 1: Open Systems Interconnection (OSI) Model - Introduction to the 7 layers of the OSI model - concept of the OSI model - the Application Layer - the Presentation Layer - the Session Layer - the Transport Layer - the Network Layer - the Data Link Layer &the Physical layer

Unit 2: Security Protocols - Application Layer - Introduction to Protocol concepts - Border Gateway Protocol (BGP) - Dynamic Host Configuration Protocol (DHCP) - Domain Name System (DNS) - File Transfer Protocol (FTP) - Hyper Text Transfer Protocol (HTTP) - Lightweight Directory Access Protocol (LDAP) - Media Gateway Control Protocol (MGCP) - Network News Transfer Protocol (NNTP) - Network Time Protocol (NTP) - Post Office Protocol (POP) - Internet Message Access Protocol (IMAP) - Routing Information Protocol (RIP) - Remote Procedure Call (RPC) - Real Time Streaming Protocol (RTSP) - Session Initiation Protocol (SIP) - Simple Mail Transport Protocol (SMTP) - Simple Network Management Protocol (SNMP) - SOCket Secure (SOCKS) - Secure Shell (SSH) - Remote Terminal Control Protocol (Telnet) - Transport Layer Security/Secure Sockets Layer

(TLS/SSL) - eXtensible Messaging & Presence Protocol (XMPP) - Wireless Application Protocol (WAP) & Internet Relay Chat (IRC)

Unit 3: Transport Layer - Introduction to Transport Layer - TCP/IP - User Datagram Protocol (UDP) - Real-time Transport Protocol (RTP) - Datagram Congestion Control Protocol (DCCP) - Stream Control Transmission Protocol (SCTP) - Resource reSerVation Protocol (RSVP)&Explicit Congestion Notification (ECN)

Unit 4: Network Layer - Introduction to Network Layer - Internet Protocol Version 4 (IP4) - Internet Protocol Version 6 (IP6) - Internet Protocol SECurity (IPSEC) - Internet Control Message Protocol (ICMP) & Internet Group Management Protocol (IGMP)

Unit 5: Data Link Layer: Introduction to Data Link Layer - the Address Resolution Protocol (ARP) - the Open Shortest Path First (OSPF) - the Neighbour Discovery Protocol (NDP) - the Tunneling Protocol (Tunnels) &the Point to Point Protocol (PPP)

Text Books:

- James F. Kurose, Keith W. Ross, "Computer Networking: A Top-Down Approach",5th Edition
- Uyless D. Black "Internet security protocols: protecting IP traffic", Pub: Prentice Hall PTR; 1st edition

Reference Books:

- Vivek Acharya, "TCP/IP Distributed System", Pub: Firewall Media / Laxmi Publications.
- Charles M. Kozierok "TCP/IP Guide – A Comprehensive, Illustrated Internet Protocols Reference", No Starch Press; 1st edition, ISBN-10: 159327047X

CORE VIII - Ethical hacking Fundamentals

Subject Code: **Number of Credits: 04**

Subject Description: This subject deals with the information systems security assessment

Goals: To learn about the Ethical Hacking, Attacking methodology, Web and Network hacking, Report writing & Mitigation

Objective: On successful completion of this subject the students should have understood basic of Hacking and Penetration

Contents

Unit 1: Introduction to Ethical Hacking – Ethical Hacking – Difference between hacking and ethical hacking - Hacking Methodology - Process of Malicious Hacking - Foot printing and Scanning - Enumeration - System Hacking and Trojans and Black Box Vs White Box Techniques

Unit 2: Attacking methodology - Denial of Service – Sniffers - Session Hijacking and Hacking Web Servers - Session Hijacking - Hacking Web Servers - Web Application Vulnerabilities and Web Techniques Based Password Cracking - Web Application Vulnerabilities - Web Based Password Cracking Techniques

Unit 3: Web and Network hacking - SQL Injection - Hacking Wireless Networking – Viruses - Worms and Physical Security - Linux Hacking - Evading IDS and Firewalls

Unit 4: Report writing - Introduction to Report Writing - Demonstration of vulnerabilities

Unit 5: Mitigation - Mitigation - requirements for low level reporting & high level reporting of Penetration testing results - Mitigation of issues identified including tracking

Text Book:

- Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed" 7th Edition, McGraw Hill, 1 August 2012
- Dexter Jackson, "Hacking: Ultimate Beginner's Guide to Computer Hacking in 2016; Hacking for Beginners, Hacking University, Hacking Made Easy, Hacking Exposed, Hacking Basics", Create Space Independent Publishing Platform (30 August 2016)

Reference Books:

- Patrick Engerbrestson, "Basic of Hacking and Penetration: Ethical Hacking and Penetration Testing Made Easy", Syngress; 2 edition (12 September 2013)
- Justin Hatmaker, "Hacking:: Penetration Testing, Basic Security and How To Hack", CreateSpace Independent Publishing Platform (19 January 2016)

CORE LAB V - Ethical hacking Lab

Subject Code: **Number of Credits: 04**

List of Experiments:

- Passive Reconnaissance using "Who is" and Online tools
- Active Reconnaissance using "Sampad" and web site details
- Full Scan, Half Open Scan and Stealth scan using "nmap"
- UDP and Ping Scanning using "Advance Lan Scanner" and "Superscan"
- Packet crafting using "Packet creator" tools
- Exploiting NetBIOS vulnerability
- Password Revelation from browsers and social networking application
- Creating and Analyzing spoofed emails
- Creating and Analyzing Trojans
- OS password cracking

ALLIED PAPER IV - ISO 27000 standards

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with ISO 27000 standards

Goals: To learn about the Information Security Management Principles

Objective: On successful completion of this subject the students should have understood

- Information Security Management Principles and Information Risk
- Information Security Framework
- Procedural / People Security Controls
- Technical Security Controls
- Software Development and Lifecycle

Contents

Unit 1: Information Security Management Principles and Information Risk - Concepts and Definitions - the need for - and the benefits of Information Security Threats and vulnerabilities of Information Systems Risk Management

Unit 2: Information Security Framework - Organization and Responsibilities - Security Organizational Policy - Standards and Procedures - Information Security Governance - Information Security - Implementation Security Information Management - Legal Framework - Security Standards and Procedures

Unit 3: Procedural / People Security Controls - People - User Access Controls – Communication - Training and Awareness

Unit 4: Technical Security Controls - Protection from Malicious Software - Networks and Communications - External Services - Cloud Computing - IT Infrastructure

Unit 5: Software Development and Lifecycle - Testing - Audit and Review Systems - Development and Support - Physical and Environmental Security Controls - Disaster Recovery and Business Continuity Management - Other Technical Aspects - Investigations and Forensics - Role of Cryptography

Text Books:

- W. KragBrotby, "Information Security Governance: Guidance for Information Security Managers", 1st Edition, Wiley Publication, 13 April 2009
- W. KragBrotby, "Information Security Governance: Guidance for Boards of Directors and Executive Management", 2nd Edition, ISACA Publication, 01 Mar 2006

Reference Books:

- Fred Cohen, "Security Governance Checklists: Business Operations, Security Governance, Risk Management, and Enterprise Security Architecture", Large Print Edition, Fred Cohen & Assosciates Publication, 2005
- Shon Harris and Fernando Maymi, "CISSP All-in-One Exam Guide", 7th Edition, McGraw-Hill Education, 1 June 2016
- James J., "IT Compliance and Controls: Best Practices for Implementation", Illustrated Edition, Wiley Publication, 2008

Skill based Subject: 2 Case Studies and Report Writing in Cyber Crimes

Subject Code: **Number of Credits: 03**

Subject Description: This course deals with case studies and report writing in cyber crimes

Goals: To learn about the case studies, planning a case study, case studies in cyber crimes, report writing

Objective: On successful completion of this subject the students should have understood case studies and report writing in cyber crimes

Contents

Unit 1: Introduction to Case Study - Different types of case Studies – Case Study models with examples.

Unit 2: Planning a Case Study - Researching a Case Study - Strengths and Weaknesses of Case Studies - Writing a Case Study

Unit 3: Case Studies in Cyber Crimes – Select case studies for various types of cyber crimes and frauds in India and abroad.

Unit 4: Case study research in cyber crimes – Pilot Study – Main Study – Choosing a case study – Tools and softwares for understanding case studies – Plagarism – Popular websites for social sciences and scientific researches.

Unit 5: Report Writing – Definition – Types of Report Writing – Templates and sample report writing for cyber crime cases and information security field – ethics of report writing

Text Books:

- Jonathan Reuvid, Managing Cybersecurity Risk: Cases Studies and Solutions, Legend Press; 2 edition (31 October 2017)
- Prakash Prasad, A Brief Introduction on Cyber Crime Cases under Information Technology Act: Details & Analysis | Handbook | Cyber Law Cases Indian Context, CreateSpace Independent Publishing Platform; First edition (14 March 2017)

Reference Books:

- M Dasgupta, Cyber Crime in India: A Comparative Study, Eastern Law House Pvt Ltd (1993)

CORE IX - Mobile, Wireless and VOIP Security

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with Mobile, Wireless and VOIP Security

Goals: Knowledge on Mobile communication, Wireless Security, Voice over Internet Protocol (VOIP) Security, Mobile Forensics & Data Extraction

Objective: On successful completion of this subject the students should have understood

- Mobile communication
- Wireless Security
- Voice over Internet Protocol (VOIP) Security
- Mobile Forensics & Data Extraction

Contents

Unit 1: Introduction to Mobile communication - Mobile & Telecommunication protocols and their vulnerabilities - Gain knowledge of managerial - technical and procedural controls to address Mobile & Telecommunication vulnerabilities

Unit 2: Wireless Security - Wireless protocols and their vulnerabilities - Gain knowledge of managerial - technical and procedural controls to address Wireless vulnerabilities

Unit3: Voice over Internet Protocol (VOIP) Security - VOIP concepts - protocols and vulnerabilities - Gain knowledge of managerial - technical and procedural controls to address VOIP vulnerabilities

Unit 4: Mobile Forensics & Data Extraction - Mobile forensics process including seizure - data acquisition types like Physical – Logical – Manual - External & Internal memory – storage - analysis using tools & techniques

Unit 5: Vulnerabilities, Threats of Mobile Devices and Countermeasures - Understanding Attack vectors, Overview of various Mobile Malwares, Network Attacks, Mobile malware defenses: Advantages and disadvantages

Text Books:

- John R. Vacca, "Computer and Information Security Handbook (The Morgan Kaufmann Series in Computer Security)", Morgan Kaufmann (7 July 2009)
- Himanshu Dwivedi, "Mobile Application Security", 1st Edition, McGraw-Hill Education, February 5, 2010
- Jim Doherty, "Wireless and Mobile Device Security", 1st Edition, Jones and Barlett Publication, 2014

Reference Books:

- Timothy Speed, Darla Nykamp, Mary Heiser, Joseph Anderson, Jaya Nampalli, "Mobile Security: How to Secure, Privatize, and Recover your devices", reprint edition, Packt Publication, 2013
- Stephen Fried, "Mobile Device Security: A comprehensive guide to securing your Information in a Moving World", illustrated edition, Taylor & Francis Publication, 2010

CORE X - Computer Forensics and Investigation

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with Computer Forensics and Investigation

Goals: Knowledge on Computer Forensics and Investigation

Objective: On successful completion of this subject the students should have understood

- Computer Forensics
- Storage Devices
- Forensics Techniques
- Cyber Law

Contents

Unit 1: Computer Forensics - Introduction to Computer Forensics - Forms of Cyber Crime - First Responder Procedure- Non-technical staff - Technical Staff - Forensics Expert and Computer Investigation procedure

Unit 2: Storage Devices & Data Recover Methods - Storage Devices- Magnetic Medium - Non-magnetic medium and Optical Medium - Working of Storage devices-Platter - Head assembly-spindle motor - Data Acquisition - Data deletion and data recovery method and techniques

Unit 3: Forensics Techniques - Windows forensic - Linux Forensics - Mobile Forensics – Steganography - Application Password cracking - Brute force -Dictionary attack - Rainbow attack - Email Tacking – Header option of SMTP, POP3, IMAP

Unit 4: Cyber Law - Corporate espionage - Evidence handling procedure - Chain of custody - Main features of Indian IT Act 2008 (Amendment)

Unit 5: Role of Digital Evidence - Digital Evidence – Authentication of Evidence - Importance of digital evidences in investigation and in court of law – Capabilities of a digital forensic investigator.

Text Books:

- B. Nelson, "Guide to Computer Forensics and Investigations", 3rd Edition, Cengage, 2010 BBS
- Marie-Helen Maras, "Computer Forensics: Cyber Criminals, Laws and Evidence", 1st edition, Jones and Bartlett Publishers, 1 February 2011
- John.R.Vacca, "Computer Forensics, Computer Crime Scene Investigation", 2nd Edition, Charles River Media Publication, 15 June 2002

Reference Books:

- Aaron Philipp, David Cowen, Chris Davis, "Hacking Exposed Computer Forensics", Pub: McGraw Hill-2011
- Albert Marcella, Jr., Doug Menendez, "Cyber Forensics: A field manual for collecting, Examining, preserving evidence of computer crimes", Second Edition, CRC Press 2007
- Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations, Processing Digital Evidence", 4th edition, Delmar Cengage Learning, 28 Oct 2009
- Larry Daniel, Lars Daniel, "Digital Forensics for Legal Professionals - Understanding Digital Evidence from the Warrant to the Courtroom", 1st edition, Syngress, 14 October 2011

CORE LAB VI - Computer Forensics Lab

Subject Code: **Number of Credits: 04**

List of Experiments:

- Physical Collection of electronic evidence using forensic standards
- Dismantling and re-building PCs in order to access the storage media safely
- Boot sequence and Power On Self-Test mode analysis
- Examination of File systems of Windows, Linux and Mac
- Analysing Word processing and Graphic file format
- Network data sniffing and analysing
- Password and encryption techniques
- Internet forensic and Malware analysis

- Data recovery techniques for hard drive
- Data recovery techniques for Pen drive and CD

Skill based Subject: 3 - Mini Project on Information Security / Digital Forensics

Subject Code: **Number of Credits: 03**

Rules for the Project:

- The project can be done by seeking prior approval of the institution. For the purpose of approval, Students have to submit their project titles and proposals with the name of internal and external guides to the project coordinator of Institution within 15 days of the commencement of the semester. In case, if the student proposal is rejected, the revised proposal in the same or other area is required to submit and get it sanctioned within next 10 days. Failing to do this, his/her term will not be granted.
- Once the project proposal is approved, it is not allowed to do any change without the approval of the Project Coordinator.
- The external examiners appointed by the University will give the external marks on the basis of the heads like Presentation, Demonstration, Viva Voice, and Documentation etc. The distribution of the marks to different heads may be decided at the time of evaluation of the project but it is expected to have the same distribution.
- The Project Coordinator will be responsible to award the internal marks based on performance and keeping records for the same.

CORE XI - Database Security

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with the fundamentals of database security
Goals: The goal of this paper is to make a student learn the basic concepts Database

Objective: It helps the students by providing guidance on how to

- The Database and DBMS Architecture
- Database Interface Languages
- Accessing Databases through the Internet
- Data Warehousing

Contents
Unit 1: The Database and DBMS Architecture - Introduction to Database & DBMS Architecture - Hierarchical Database Management Systems - Network Database Management Systems - Relational Database Management System - Object-Oriented Database Management Systems - End-User Database Management Systems –Spreadsheets

Unit 2: Database Interface Languages - Introduction to Database Interface Languages - Concepts of Database Interface Languages - Open Database Connectivity (ODBC) and Object Linking and Embedding Database (OLE DB)

Unit 3: Accessing Databases through the Internet - Introduction to Accessing Databases through the Internet - Concept of Accessing Databases through the Internet - the Three tier approach - ActiveX Data Objects (ADO) - Java Database Connectivity (JDBC) - eXtensible Markup Language (XML) - the Security Assertion Markup Language (SAML)

Unit 4: Data Warehousing - Introduction to Data Warehousing concepts - the concept of Data Warehousing - Metadata and Online Analytical Processing (OLAP)Data mining - Database Vulnerabilities and threats.

Unit 5: Database Security - Overview of Database - Database application security models - Database auditing models - Application data auditing - Practices of database auditing

Text Book:

- Silvana Castano, "Database security" , 2nd Edition, Pub: Addison-Wesley Professional , 2008
- Natan, "Implementing database security and auditing", Elsevier India; First edition (7 December 2005)

Reference Books:

- Ronald L. Krutz, Russel Dean Vines, "The CISSP Prep Guide: Gold Edition", Gold Edition, Wiley Publication, 31 Oct 2002
- Ed Tittel, Mike Chapple, James Michael Stewart, "Certified Information Systems Security Professional, Study Guide", 6th Edition, Sybex Publication, 06 July 2012

CORE XII - Web applications Security

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with Web applications security

Goals: To learn about the Secure Development Lifecycle, Application Security, Web Security, Attacks & Trend

Objective: To inculcate knowledge on Web Security

Contents

Unit 1: Secure Development Lifecycle - Benefits management practices (feasibility studies, business cases etc.) - Project Governance practices (steering committee, project oversight board etc,) - Project Management practices - tools and control frameworks - Risk Management practices applied to projects - Project Success criteria and risks - Configuration - Change and Release management in relation to development and maintenance of systems and infrastructure - Control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data with IT systems applications

Unit 2: Application Security - Enterprise architecture related to data - applications and technology (distributed applications, web-based applications, web services, m-applications etc.) - Requirements analysis and management practices (requirements verification, traceability and gap analysis) - Acquisition and contract management processes (evaluation of vendors, preparation of contracts, vendor management, escrow etc.)

Unit 3: Systems development methodologies and tools and strengths and weaknesses (agile development practices, prototyping, rapid application development (RAD), object oriented design techniques etc.) - Quality assurance methods - Management of testing processes (test strategies, test plans, test environments, entry and exit criteria etc.) - Business application systems and control - Controls for OWASP Top 10 threats for web-based applications

Unit 4: Web Security - Web 2.0 and vulnerabilities – AJAX - Flash and interactive technology vulnerabilities and controls - Common web security vulnerabilities - attack vectors and technical controls - Web application vulnerability assessment and testing using tools and techniques - Advanced Persistent Threats (APTs) and technical controls for mitigation. Basic level of application code review

Unit 5: Web Attacks & Trend - Introduction to Web Attacks & Trends - URL Interpretation attacks - Input Validation attacks - SQL Injection attacks, Impersonation attacks & Buffer Overflow attacks - their effects and the technical & managerial controls to be put in place to address such attacks

Text Books:

- Neil Dawwani, Christoph Kern and Anita Kesavan, "Foundations of Security", Apress (February 15, 2007)
- Joel Scambray, Mike Shema, Caleb Sima, "Hacking Exposed Web Application", 2nd Edition. 2010

Reference Books:

- Mike Shema, "Hack Notes Web Security Pocket",2010
- Steven Splaine, "Testing Web Security: Assessing the Security of Web Sites and Applications", 2011

CORE LAB VII - Web applications Security Lab

Subject Code: **Number of Credits: 04**

List of Experiments:

- URL Interpretation attacks
- Input Validation attacks
- SQL Injection attacks,
- Impersonation attacks
- Buffer Overflow attacks

Skill based Subject: 4 – Biometrics

Subject Code: **Number of Credits: 03**

Subject Description: This course deals with Biometrics and Leading Technologies

Goals: To learn about Benefits of Biometrics, Leading Technologies, biometric applications, Privacy and Standards

Objective: To inculcate knowledge on Leading Technologies and Biometric Standards

Unit 1: Biometrics: Benefits of Biometrics versus Traditional – Benefits of Biometrics in Identification systems – Verification, Identification and biometric matching – Performance measures in biometric systems

Unit 2: Leading Technologies: Finger scan – facial scan – Iris scan – Voice scan – and scan, Retina scan – components, working principles, competing technologies, strengths and weaknesses

Unit 3: Other Leading Technologies: Automated fingerprint identification systems - Signature-scan – Keystroke scan - components, working principles, strengths and weaknesses.

Unit 4: Categorizing biometric applications - citizen identification – criminal identification – Surveillance – PC/ Network Access – Physical Access/ Time/ Attendance – Customer facing applications: e Commerce/ Telephony – Retail/ ATM/ Point of sale

Unit 5: Privacy and Standards in Biometric System Design: Assessing the privacy risks of Biometrics – designing privacy – sympathetic biometric systems – Biometric Standards

Text Books:

- Samir Nanavati, Michael Thieme, Raj Nanavati, "Biometrics: Identity Verification in a Networked World (Technology Briefs Series)", John Wiley & Sons (12 April 2002)
- Paul Reid, "Biometrics for Network Security", Pearson Education, New Delhi, 2004

Reference Books:

- John R Vacca, "Biometric Technologies and Verification Systems", Elsevier Inc, 2007
- Anil K Jain, Patrick Flynn, Arun A Ross, "Handbook of Biometrics", Springer, 2008

Elective –I

Virtualization & Cloud Security

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with Virtualization and Cloud computing concepts

Goals: To learn about the Virtualization and Cloud computing concepts, Cloud Security, Cloud Trust Protocol and Transparency, Cloud Controls Matrix & Top Cloud Threats

Objective: To inculcate knowledge on Virtualization and Cloud

Contents

Unit 1: Introduction to Virtualization & Cloud - Virtualization and Cloud computing concepts - Private cloud vs Public cloud - IAAS, PAAS & SAAS concepts - Virtualization security concerns - Hypervisor Security -Host/Platform Security - Security communications - Security between Guest instances - Security between Hosts and Guests

Unit 2: Cloud Security - Cloud Security vulnerabilities and mitigating controls - Cloud Trust Protocol - Cloud Controls Matrix - Complete Certificate of Cloud Security Knowledge (CCSK)

Unit 3: Cloud Trust Protocol & Transparency - Introduction to Cloud Trust Protocol & Transparency - Cloud Trust Protocol and Transparency - Transparency as a Service - Concepts, Security, Privacy & Compliance aspects of cloud

Unit 4: Cloud Controls Matrix &Top Cloud Threats - Introduction to Cloud Controls Matrix & Top Cloud Threats - Cloud Controls Matrix - Trusted Cloud Initiative architecture and reference model - requirements of Security as a Service (Secaas) model and Top Security threats to the cloud model

Unit 5 – Best practices and the future of cloud computing – Establishing a baseline and metrics – Phased in vs flash cut approaches – Researcher predictions – Responding to change

Text Books:

- Andi Mann, Kurt Miline and Jeanne Morain, "Visible Ops Private Cloud", IT Process Institute, Inc.; first edition (April 8, 2011)
- Toby Velte, Anthony Velte, Robert C. Elsenpeter, "Cloud Computing, A Practical Approach", 1st Edition, McGraw-Hill Education, 1 November 2009

Reference Books:

- Denise Gonzales, "Cloud Computing Bible: A Practical Approach to Cloud Computing Security, Cloud Problems To Be Aware of and More", Kindle Edition
- Zaigham Mahmood, "Cloud Computing: Methods and Practical Approaches (Computer Communications and Networks)", 2013 edition, Springer, 4 June 2013
- Derrick Rountree, Ileana Castrilo, "The basics of Cloud Computing – Understanding the fundamentals of cloud computing in theory and practice", Illustrated Edition, Syngress Publication, 01 Nov 2013

Forms of Cyber Crime

Subject Code: **Number of Credits: 04**
Subject Description: This course deals with various forms of cyber crimes and frauds

Goals: To learn about the various forms of cyber crimes and understanding fraudulent behaviour

Objective: Students will be able to:

- Define the frauds and related concepts
- Define fraud triangle
- Understand forms of frauds
- Understand the fraud types
- State fraudulent behavior
- Understand fraud detection techniques

Contents

Unit 1: Definition of Frauds, fraud detection, fraud risk management, red flags

Unit 2: Types of Frauds – Internal Fraud, External Fraud – Fraud Triangle

Unit 3: Various forms of cyber crimes – Definition, nature & Modus Operandi and countermeasures

Unit 4: Major Forms of Frauds - Telecom Frauds- ATM Frauds - Bank Frauds - Card Frauds - Mobile frauds.

Unit 5: Understanding fraudulent behaviour - Fraud detection techniques – through statistical analysis, pattern and relationship analysis, vagueness in fraud detection & signatures in fraud detection - Building a Fraud Analysis Model – 7 Stages.

Text Books:

- Rick Howard, "Cyber Fraud: Tactics, Techniques and Procedures", Auerbach Publications; 1st edition.
- Vasu Deva, "Cyber Crimes and Law Enforcement", Commonwealth Publishers, New Delhi.

Reference Books:

- Albert J. Marcellaa and Robert S. Greenfiled (Ed), "Cyber Forensics, A Field Manual for collecting, examining and preserving evidence of computer crimes", Auerbach publications.

Cyber law

Subject Code: **Number of Credits: 04**
Subject Description: This course deals with Cyber Law

Goals: To learn about the Indian Cyber Law System

Objective: Students will be able to
- Cyber Jurisprudence,
- Indian Cyber Law System,
- Important Indian Case Laws

Contents
Unit 1: Description and scope of Cyber Jurisprudence, Techno – legal concepts.

Unit 2: Regional and Global approaches - G8 initiative, EU initiatives/ directives, UNCITRAL MODEL LAW.

Unit 3: Indian Cyber Law System – Information Technology Act 2000, 2002, 2008 and Amendments - Principles of Evidence, Banking Evidence Act and Indian Penal Code.

Unit 4: Practices in Cyber Jurisprudence – Regional and Global.

Unit 5: Important Indian Case Laws.

Text Books:

- Albert J. Marcellaa and Robert S. Greenfiled (Ed), "Cyber Forensics, A Field Manual for collecting, examining and preserving evidence of computer crimes", Auerbach publications.
- Hossein Bidgoli, "Information Warfare; Social, Legal, and International Issues; and Security Foundations", Hoboken, NJ: John Wiley & Sons.

Reference Books:

- Derek Atkins et. al., "Internet Security: Professional Reference", Techmedia, Daryaganj, New Delhi
- Vasu Deva, "Cyber Crimes and Law Enforcement", Commonwealth Publishers, New Delhi.

Elective II

IT Governance, Risk & Compliance Management

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with IT Governance, Risk & Compliance Management

Goals: To learn about the Best Practices for IT Governance and Risk Management Process

Objective: To inculcate knowledge on IT Governance, Information Systems Strategy, Risk Management Program, and Information Security Management

Contents:
Unit 1: IT Governance - Information Security Governance – Governance, Risk, Compliance – Internal Company culture – Security strategy development techniques – Security planning

Unit 2: Security Management Organization – Security functions – Assessing Risks – Implement policies and control functions – Promote awareness – Logging and monitoring – Vulnerability Assessment – Internet monitoring – Incident Response – Forensic Investigation

Unit 3: Risk Management Program – Risk Management process: Risk analysis involvement – Risk mitigation options: Risk assumption – risk avoidance – risk limitation – risk planning - risk research – risk transference

Unit 4: Information Security policies: Security policy best practices – types of security policies – Standards – procedures – baselines – Guidelines – policy review process – Security compliance using control frameworks

Unit 5: Best Practices for IT Governance – ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT) - The Information Security Management Maturity Model - Capability Maturity Model – latest standards and compliance technologies.

Text Books:

- Todd Fitzgerald, "Information Security Governance Simplified: From the Boardroom to the Keyboard", CRC Press; 1 edition (14 December 2011)
- Peter Weill and Jeanne Ross**, "**IT Governance" Harvard Business Review Press; 1 edition (June 1, 2004)
- Malcolm Harkins, "Managing Risk and Information Security", Apress; 1 edition (December 17, 2012)

Reference Books:

- W. KragBrotby, "Information Security Governance: Guidance for Information Security Managers", 1st Edition, Wiley Publication, 13 April 2009

- W. KragBrotby, "Information Security Governance: Guidance for Boards of Directors and Executive Management", 2nd Edition, ISACA Publication, 01 Mar 2006

IT and Telecommunication Frauds

Subject Code: **Number of Credits: 04**

Subject Description: This course deals with IT Frauds and Telecom Frauds

Goals: To learn about the IT Frauds, Telecom Frauds, Fraud Management, Mobile network Fraud

Objective: To inculcate knowledge on frauds in software development, frauds in telecom, fraud management

Contents:
Unit 1 : Frauds in IT - IT Frauds (Theft of Proprietary Information, Insider abuse of internet access, system penetration, unauthorised access to information, laptop/mobile theft, financial fraud, misuse of public web application, virus, abuse of wireless network) – Countermeasures.

Unit 2: Frauds in Software development and Management – Software industry frauds – counter measures.

Unit 3: Introduction to Telecom – Telecommunication – Types of Telecommunication – Telecommunication networks – Types of frauds in telecom - Frauds in different segments of Telco operations (such as Customer Care, Operational Support Systems, Network Management Systems) - Organizational or Non-Technical Fraud (involving Administration services, processes) - Human Fraud - Insider Fraud - Call-sell Fraud - Facilitation Fraud - Creeping Fraud - Chaining Fraud - Calling-Card Fraud - Phantom Account - Partnership Fraud - Process Fraud – Ghosting - Abuse of test or emergency lines or accounts - Unauthorized Feature/Service Activation – Accounting - Dealer or Reseller Fraud - Subscription Fraud - Roaming Subscription Fraud - Premium-Rate Services Fraud- Illustrative Cases - Technical Fraud (involving Network Systems, Billing Systems) – Cloning – Tumbling - Voice-mail Hacking - PBX Hacking - SIM Stuffing- Clip-on Fraud - Line Tapping - War Dialing - Handset Fraud

Unit 4: Mobile network Fraud - The security of mobile networks - Frauds in wireless domain - Before Pre-Call Validation - After Pre-Call Validation - Fraud Detection Systems - Subscription Fraud - The best ways to reduce the risk of mobile network fraud - **Frauds in 3G Networks -** Introduction to 3G Technology and Services - The 3G Business Model - Telecom Frauds in a 3G environment - Subscription Fraud - Credit-card Fraud on M-commerce - Micro-payment Fraud - Premium rate Services (PRS) Frauds - Copyright Infringement and content resale frauds ('piracy') - IP Security issues in 3G – Hacking - DOS Attacks - Virus, Worms and Trojans - Data Interception - Database attacks – Spam - How network security needs to change with the move to 3G - Security and Law enforcement issues in 3G

Unit 5: Fraud Management – A Strategic Perspective - Telecom Laws – Domestic and International - Fraud Detection and Prevention - Data mining applied to Fraud Detection and Prevention - Data Warehouse Data Modeling - Data mining techniques - Application of data mining to fraud - Tools and techniques - External knowledge and experience - Awareness about Telecom Fraud - Fraud Training - Fraud Awareness - Profiling a Fraud- Identifying the Fraudster - FMS – Fraud Management System - Architecture of an FMS solution

Text Books:

- Marc Goodman, Future Crimes: A Journey to the Dark Side of Technology – and How to Survive It, Bantam Press (26 February 2015)
- Ian Watts, Fraud Overview: Understand what fraud is, who commits fraud, how it is perpetrated and what to do about it (Fraud Prevention How to Guides Book 1) Kindle Edition, Lifelong Learning (London) International Limited; 1 edition (21 September 2016

Reference Books:

- I.I. Androulidakis, Mobile Phone Security and Forensics: A Practical Approach (SpringerBriefs in Electrical and Computer Engineering) 2,012th , Kindle Edition, Springer; 2012 edition (29 March 2012)

E-commerce Application

Subject Code: **Number of Credits: 04**
Subject Description: This subject deals with E-commerce

Goals: To learn about E-commerce

Objective: On successful completion of this subject the students should have understood

- E-commerce
- E- Market
- EDI
- Business Strategies

Contents:

Unit 1: Introduction to Electronic Commerce: Scope of electronic commerce – Definition of electronic commerce – electronic commerce and the trade cycle – electronic market – electronic data interchange – internet perspective – ecommerce in perspective

Unit 2: Business Strategy: Introduction to business strategy – Strategic implication of IT – Technology – business environment – business capability – existing business strategy – strategy formulation and implementation planning – ecommerce implementation – ecommerce evaluation

Unit 3: E market: Markets – Electronic Markets – Usage of electronic markets – Advantages and disadvantages of electric market – future of electronic markets

Unit 4: The Internet – Internet – development of internet – TCP/ IP – Internet components – uses of Internet – Internet age systems – A page on the web: HTML, the basics - Introduction to HTML – Client side scripting – server side scripting – HTML Editors and editing

Unit 5: Elements of ecommerce: Elements – e-visibility – e-shop – online payments – delivering the goods – internet e – commerce security – E-business: internet bookshops – grocery supplies – software supplies and support – electronic newspapers – internet banking – virtual auctions – online share dealing – gambling on the net – e-diversity

Text Books:

- David Whiteley, E-Commerce: Strategy, Technologies And Applications (Information Systems Series), McGraw-Hill Higher Education (1 March 2000)

- Mehdi Khosrow-Pour, Cases on Electronic Commerce Technologies and Applications (Cases on Information Technology Series), IGI Publishing (15 December 2006)

Reference Books:

- Wen-Chen Hu, Selected Readings on Electronic Commerce Technologies: Contemporary Applications (Premier Reference Source), Information Science Reference (15 October 2008)
- Marilyn Greenstein, Todd Feinman, Electronic Commerce: Security Risk Management and Control, McGraw-Hill Inc.,US (1 December 1999)

Elective III

Information ethics

Subject Code: **Number of Credits: 04**

Subject Description: This course explores the ethical and professionalization issues that arise in the context of designing and using information technologies. This will comprise study the major ethical theories and frameworks that have shaped the field of information ethics and use them to address topics relevant to the informatics profession

Goals: To increase the candidate's ability to develop mature stances with regard to issues of professional ethics in general and computing ethics in particular

Objective: On successful completion of the course the student should be able to understand

- Fundamentals of computer ethics
- The theoretical underpinnings of development of various thoughts that have shaped the emergence of information ethics as a discipline
- Contemporary thoughts and approaches to development of information ethics frameworks

Contents

Unit 1: Underlying theories of information ethics: information ethics - need of information ethics- Ethical theory vs. ethical practices - Social contract theory and utilitarianism - Equity and information access - Ethical Relativism - Subjectivism and egoism in the information world - Introduction to moral reasoning – values in information context

Unit 2: Conceptual foundations in applying information ethics to real world scenarios - Due care, due diligence and prudent man's rule - Applying rationale for freedom of speech to information context - Information power and social stratification - Ethical and legality – thin lines at the border - Enforcement *vs* voluntary compliance of security baselines and policies - Digital speech in a democratic culture - Digital speech in a democratic culture - Responsible End User computing

Unit 3: Frameworks for information ethics: Taxonomy of computer ethics - Codes of ethics, codes of conduct and codes of professional behavior - First principle of information ethics – do no harm - IAB RFC 1087: Ethics and the Internet - Steven Levy's Hacker ethics - Ten commandments of Computer Ethics Institute - Fallacies in computer ethics - The ethics of ethical hacking

Unit 4: Issues and concerns: On-line privacy – concerns about loss of privacy on-line - Digital Gambling – ethical implications - Videogames addiction - Cyber bullying - Race, Gender and identity in digital space - Right to Privacy – the impact of right to stop people from speaking about you - Privacy in the Facebook era - Information and the environment – impacts of reuse / recycling of PCs - Silver surfers – power through access to information - Information divide - Human computer interaction

Unit 5: Areas requiring policy level attention: Net neutrality and internet governance–Global networked societies and power of access - Network infrastructure – access, power, competition and governance - Surveillance on access and use of information - Wealth and division of labor in networked society - Who controls the Internet – the illusions of a borderless world - An economic theory of privacy - Introduction to intellectual property rights – patents, trade / service marks and copyrights - Big data and data mining – interpretation of findings

Text Books:

- Floridi, L. (2013). The ethics of information. Oxford: Oxford University Press.
- Brier, S. (2008). Cybersemiotics: why information is not enough. Toronto: University of Toronto Press

Reference Books:

- Bawden, D. & Robinson, L. (2012). Introduction to information science. London: Facet.
- Bawden, D. & Robinson, L. (2016). Library and Information Science. In International Encyclopedia of Communication Theory and Philosophy, K.B. Jensen and R.T. Craig(eds.), New York NY: Wiley.
- Capurro, R. (1991). What is information science for? A philosophical reflection, in Vakkari, P. and Cronin, B. (eds.), Conceptions of library and information science:Historical, empirical and theoretical perspectives. London: Taylor Graham,
- Floridi, L. (2011). The Philosophy of Information. Oxford: Oxford University Press.
- Stonier, T. (1990). Information and the internal structure of the universe, Berlin: Springer-Verlag.
- Stonier, T. (1992). Beyond information: the natural history of intelligence, Berlin: Springer-Verlag.
- Stonier, T. (1997). Information and meaning: an evolutionary perspective, Berlin: Springer-Verlag.

Incident Management

Subject Code: **Number of Credits: 04**
Subject Description: This Subject deals with the incident management

Goal: To learn about incident management, Types of incidents, **Collecting Digital evidence**

Objective: On Successful Completion of this subject the students should have knowledge

- Incident management
- Types of incidents and their categorization
- Digital evidence collection
- Honeypots

Contents:
Unit 1: Incident Management - Introduction to incident management - Incident management - ITIL – perspective - Incident management - COBIT perspective - Incident management – National Institute of Standards and Technology (NIST) SP 800- 61 perspectives - Stages in Incident management - Initial preparation required for incident response - Need for incident response team - CERT (Computer Emergency Response Team) - CSIRT (Computer Security Incident Response Team) -

Roles and responsibilities of Incident response team - Need for User awareness for better incident response.

Unit 2: Handling incidents - Types of incidents and their categorization - Incident prioritization - Sources of incidents – Precursor - Indicators - End Users - Methods of identifying incidents - User reporting procedures - Incident containment eradication and recovery

Unit 3: Collecting Digital evidence – 1 - Forensic analysis methodology - Introduction to Digital Evidence - Investigative process - Incident reconstruction - Identifying the methodology involved for carrying out attacks - Identifying the motive behind the attacks - Identifying the technology used for carrying out the attacks - Preparing evidence for courtroom - Guidelines for Digital evidence handling and examination.

Unit 4: Collecting Digital evidence – 2 - Collecting evidence from windows system - Collecting evidence from non windows system - Collecting digital evidence from the internet - Investigating routers and network topology - Investigating servers and end user PCs

Unit 5: Learning from incidents and Pro active incident detection - Improving security policies after learning from an incident - Honeypots – Introduction - Types of honeypots - Tools used for setting up honeypots - Collecting evidence from honeypots - Looking out for attack signatures

Text Books:

- Chris Prosise, Kevin Mandia, Incident Response: Investigating Computer Crime, Osborne/McGraw-Hill (1 July 2001)
- Eoghan Casey BS MA, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press; 3 edition (17 June 2011)

Reference Books:

- Lance Spitzner, Honeypots: Tracking Hackers, Pearson Addison-Wesley Professional; Pap/Cdr edition (10 September 2002)
- NIST SP 800- 61 – Computer Security Incident Handling Guide

Data Mining

Subject Code: **Number of Credits: 04**
Subject Description: This Subject deals with the Data Mining

Goal: To learn about Data Mining

Objective: On Successful Completion of this subject the students should have knowledge on Data mining Concepts

Contents:
Unit 1: Basic Data Mining Tasks – Data Mining Versus Knowledge Discovery in Data Bases – Data Mining Issues – Data Mining Matrices – Social Implications of Data Mining – Data Mining from Data Base Perspective.

Unit 2: Data Mining Techniques – a Statistical Perspective on data mining – Similarity Measures – Decision Trees – Neural Networks – Genetic Algorithms

Unit 3: Classification: Introduction – Statistical – Based Algorithms – Distance Based Algorithms – Decision Tree – Based Algorithms – Neural Network Based Algorithms – Rule Based Algorithms – Combining Techniques.

Unit 4: Clustering: Introduction – Similarity and Distance Measures – Outliers – Hierarchical Algorithms. Partitional Algorithms.

Unit 5: Association Rules: Introduction - Large Item Sets – Basic Algorithms – Parallel & Distributed Algorithms – Comparing Approaches – Incremental Rules – Advanced Association Rules Techniques – Measuring the Quality of Rules.

Text Books:

- Margaret H.Dunbam, "Data Mining Introductory and Advanced Topics", Pearson Education – 2003.
- Jiawei Han & Micheline Kamber, "Data Mining Concepts & Techniques", Elsevier; Third edition (2007)

Reference Books:

- Pang-Ning Tan, Michael Steinbach, Vipin Kumar, "Introduction to Data Mining", Pearson Education; First edition (10 July 2016)