Program Structure and Syllabus of

B. Tech III Year

Cyber Security

R22 Regulations

Venkatapur (V), Ghatkesar (M), Medchal-Malkajgiri (Dt.), Hyderabad, Telangana, INDIA

info@anurag.edu.in; http://anurag.edu.in

B. TECH III YEAR I SEMESTER [5 T + 3 P + 1 M]

S.No	Course Code	Category	Course	Hours per week			Credits
				L	T	P	
1	A55028	PCC	Introduction to Cryptography	3	0	0	3.0
2	A55029	PCC	Network Security	3	1	0	4.0
3	A55044	PEC-I	1. Software Engineering	3	0	0	3.0
	A55056		2. Artificial Intelligence				
	A55045		3. Formal Languages and Automata Theory				
4	A55025	PCC	Operating Systems	3	0	0	3.0
5	A55080	HSS& MC	Entrepreneurship Development	2	1	0	3.0
6	A55211	PCC LAB	Cryptography Lab	0	0	2	1
7	A55212	PCC LAB	Network Security Lab	0	0	3	1.5
8	A55288	BSC LAB	Quantitative Aptitude and Reasoning	0	0	3	1.5
9	A55091	MC	NSO and NSS	2	0	0	0
			TOTAL	**16**	**2**	**8**	**20**

B. TECH III YEAR II SEMESTER [4 T + 4 P]

S. No	Course Code	Category	Course	Hours per week			Credits
				L	T	P	
1	A56044	PCC	Web Application Security	3	0	0	3.0
2	A56045	PCC	Writing Secure Code	3	0	0	3.0
3	A56046	PEC-II	1. Fundamentals of Cyber Security	3	1	0	4.0
	A56047		2. Elliptical Curve Cryptography				
	A56048		3. Digital Forensics				
4	A56049	PEC-III	1. Cyber Law & Security Policy	3	1	0	4.0
	A56050		2. Security Assessment & Risk Analysis				
	A56051		3. Security for Cyber Physical Systems				
5	A56213	PCC LAB	Web Applications Security Lab	0	0	3	1.5
6	A56214	PCC LAB	Writing Secure Code Lab	0	0	3	1.5
7	A56288	BSC LAB	Verbal Ability and Critical Reasoning	0	0	3	1.5
8	A56231	HSS & MC LAB	Professional Skills Lab	0	0	3	1.5
			TOTAL	**12**	**2**	**12**	**20**

ANURAG UNIVERSITY

INTRODUCTION TO CRYPTOGRAPHY

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A55028	Core	L	T	P	C	CIE	SEE	Total
		3	0	0	3	50	50	100

Course Objectives

Course Objectives of Introduction to Cryptography are to:

1. Explain the basics of cryptography.
2. Examine secure a message through insecure channel by various means.
3. Illustrate how to maintain the Confidentiality, Integrity and Availability of a data.
4. Analyze private and public key cryptography algorithms.
5. Design digital signatures.

Course Outcomes

At the end of this Introduction to Cryptography course, students will be able to:

1. Outline the basics cryptography algorithms.
2. Distinguish Secure message transfer over insecure channel transfer.
3. Summarize the Confidentiality, Integrity and Availability of a data.
4. Explain various public and private key cryptography algorithms.
5. Apply digital signature to an application.

UNIT I

Private-Key (Symmetric) Cryptography

Private-Key Encryption: Computational Security, Defining Computationally Secure Encryption, Constructing Secure Encryption Schemes, Stronger Security Notions, Modes of Operation and Chosen-Cipher text Attacks.

UNIT II

Message Authentication Codes: Message Integrity, Message Authentication Codes- Definitions, Constructing Secure Message Authentication Codes, Authenticated Encryption.

Hash Functions and Applications: Definitions, Message Authentication Using Hash Functions (Hash-and-MAC, HMAC), Generic Attacks on Hash Functions and Additional Applications of Hash Functions

UNIT III

Practical Constructions of Symmetric-Key Primitives

Stream Ciphers: Linear-Feedback Shift Registers, Adding Nonlinearity, Trivium and RC4. **Block Ciphers:** Substitution-Permutation Networks, Feistel Networks, DES, 3DES and AES

Hash Functions: Hash Functions from Block Ciphers, MD5, SHA-0, SHA-1, and SHA-2 and SHA-3.

UNIT IV

Public-Key (Asymmetric) Cryptography

Cryptographic Assumptions in Cyclic Groups, Public-Key Encryption – An Overview, Security against Chosen-Plaintext Attacks, Multiple Encryptions, Security against Chosen-Cipher text Attacks, CDH/DDH-Based Encryption, RSA algorithm, RSA Implementation Issues and Pitfalls.

UNIT V

Advanced Topics in Public-Key Encryption

Digital Signature Schemes: Digital Signatures – An Overview, Definitions, The Hash-and-Sign Paradigm and RSA Signatures,Public-Key Encryption from Trapdoor Permutations, The Paillier Encryption Scheme, Secret Sharing and Threshold Encryption, The Goldwasser–Micali Encryption Scheme, The Rabin Encryption Scheme.

Text Book

1. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, Second Edition, CRC Press, 2015.

Reference Books

1. Hans delfs, Helmut Knebl, Introduction to Cryptography Principles and Applications, Third Edition, Springer, 2015.
2. Alfred J. Menezes et. Al, Handbook of Applied Cryptography, CRC Press.
3. Johannes A. Buchmann, Introduction to Cryptography, Second Edition, Springer-Verlag, 2003.

ANURAG UNIVERSITY

NETWORK SECURITY

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A55029	Core	L	T	P	C	CIE	SEE	Total
		3	1	0	4	50	50	100

Course Objectives

Course Objectives of Network Security are to:

1. Summarize the basics of network security and protocols.
2. Identify and classify various types of attacks and hacking techniques.
3. Describe the various authentication tools & services.
4. Discuss about Firewalls and Virtual Private Network (VPN).
5. Compare various types of Intrusion Detection System (IDS) and to construct safe hosts.

Course Outcomes

At the end of this Network Security course, students will be able to:

1. Identify some of the factors which are essential for the network security.
2. Differentiate various types of attacks and hacking methods / techniques.
3. Distinguish various authentication tools.
4. Discuss Firewalls and Virtual Private Network (VPN).
5. Compare different types of Intrusion Detection System (IDS).

UNIT I

Introduction: Security Truisms, Picking a Security Policy, Host-Based Security, Perimeter Security, Strategies for a Secure Network and The Ethics of Computer Security.

A Security Review of Protocols: Lower Layers Basic Protocols, Managing Addresses and Names, IP version 6, Network Address Translators and Wireless Security.

Security Review: The Upper Layers Messaging, Internet Telephony, RPC-Based Protocols, File Transfer Protocols, Remote Login, Simple Network Management Protocol-SNMP, The Network Time Protocol and Proprietary Protocols.

UNIT II

Classes of Attacks: Stealing Passwords, Social Engineering, Bugs and Back Doors, Authentication Failures, Protocol Failures, Information Leakage, Exponential Attacks-Viruses and Worms, Denial-of-Service Attacks, Botnets and Active Attacks.

The Hacker's Workbench, and Other Munitions: Introduction, Hacking Goals, scanning a Network, breaking into the Host, The Battle for the Host, Covering Tracks, Metastasis, Hacking Tools and Tiger Teams.

UNIT III

Safer Tools and Services:

Authentication: Remembering Passwords, Time-Based One-Time Passwords, Challenge/Response One-Time Passwords, Lamport's One-Time Password Algorithm, Smart Cards, Biometrics, RADIUS, SASL: An Authentication Framework and Host-to-Host Authentication.

Using Some Tools and Services: inetd-— Network Services, SSH—Terminal and File Access, Syslog, Network Administration Tools, chroot—Caging Suspect Software, Jailing the Apache Web Server, AFTPD—A Simple Anonymous FTP Daemon, Mail Transfer Agents, POP3 and IMAP, Samba: An SMB Implementation and Adding SSL Support with SSL wrap.

UNIT IV

Firewalls and VPNs

Kinds of Firewalls: Packet Filters, Application-Level Filtering, Circuit-Level Gateways, Dynamic Packet Fitters, Distributed Firewalls and What Firewalls Cannot Do.

Filtering Services: Reasonable Services to Filter, Digging for Worms, Services We Don't Like and Other Services.

Firewall Engineering: Rulesets, Proxies, Building a Firewall from Scratch, Firewall Problems and Testing Firewalls.

Tunnelling and VPNs: Tunnels, Virtual Private Networks (VPNs) and Software vs. Hardware.

UNIT V

Protecting an organization

Network Layout: Intranet Explorations, Intranet Routing Tricks, In Host We Trust, Belt and Suspenders and Placement Classes.

Safe Hosts in a Hostile Environment: Properties of Secure Hosts, Hardware Configuration, Field-Stripping a Host, Loading New Software and Administering a Secure Host. **Intrusion Detection:** Where to Monitor, Types of IDSs, Administering an IDS and IDS Tools.

Text Book

1. William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Firewalls and Internet Security, Second Edition, Addison-Wesley, 2003.

Reference Books

1. William Stallings, Cryptography and Network security, Seventh Edition, Pearson, 2017
2. Nicholas J. Daras, Michael Th. Rassias (eds.), Computation, Cryptography, and Network Security, Springer International Publishing, 2015.
3. Atul Kahate, Cryptography and network security, Tata McGraw-Hill, 2006

SOFTWARE ENGINEERING (PEC-I)

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A55044	Professional Elective-I	L	T	P	C	CIE	SEE	Total
		3	0	0	3	50	50	100

Course Objectives

Course Objectives of Software Engineering are to:

1. Identify an appropriate Process Model.
2. Deliberate Software Requirements-functional and nonfunctional.
3. Design various system models for a given scenario.
4. Elaborate about different testing techniques.
5. Describe role of risk management in Software Engineering.

Course Outcomes

At the end of this Software Engineering course, students will be able to:

1. Analyze process models.
2. Emphasize Software Requirements -functional and nonfunctional.
3. Appreciate the system models.
4. Compare and contrast various testing techniques.
5. Identify various risk strategies.

UNIT I

Introduction to Software Engineering: The evolving role of software, Changing Nature of Software, Software myths. A Generic view of process: Software engineering- A layered technology, a process framework, The Capability Maturity Model Integration (CMMI).

Process models: The waterfall model, Incremental process models, Evolutionary process model. [TB:1, CH:1,2,3]

UNIT II

Agile process Model: Agile principles, Extreme programming, Dynamic System Development Methods, Feature Driven Development, Scrum framework, Sprint, Scrum master, Roles of Scrum Master, Implementing Scrum - A case study. [TB:1, CH:4]

Software Requirements: Functional and non-functional requirements, the software requirements document. Requirements engineering process: Feasibility studies, Requirement's elicitation and analysis, Requirement's validation, Requirements management. [TB:2, CH:6,7]

UNIT III

System Models: Context Models, Behavioral models, Data models, Object models, structured methods. [TB:2, CH:8]

Design Engineering: Design process and Design quality, Design concepts, the design model. Modeling component level design: design class-based components, conducting component level design. Performing User interface design: Golden rules. [TB:1, CH:9,11]

UNIT IV

Testing Strategies: A strategic approach to software testing, test strategies for conventional software, Black-Box and White-Box testing, Validation testing, System testing.

Product metrics: Software Quality, Metrics for Analysis Model- function based metrics, Metrics for Design Model-object oriented metrics, class-oriented metrics, component design metrics, Metrics for source code, Metrics for maintenance. [TB:1, CH:13,14,15]

UNIT V

Risk Management: Reactive vs. Proactive Risk strategies, software risks, Risk identification, Risk projection, Risk refinement, RMMM, RMMM Plan.

Quality Management: Quality concepts, Metrics for Software Quality, Software Reviews, Formal Technical Reviews, Software Reliability, The ISO 9000 quality standards. [TB:1, CH:25, 26]

Text Books

1. Roger S. Pressman, Software Engineering - A practitioner's Approach, 6th edition. McGraw Hill International Edition, 2005.
2. Somerville, Software Engineering, 7th Edition, Pearson Education, 2009.

Reference Books

1. K.K. Agarwal & Yogesh Singh, Software Engineering, New Age International Publishers,3rd edition, 2008.
2. Pankaj Jalote, An Integrated Approach to Software Engineering, Narosa Publishing House, 3rd edition, 2005.
3. James F. Peters, Witold Pedrycz, Software Engineering - an Engineering approach, JohnWiely, 2007.
4. Waman S Jawadekar, Software Engineering Principles and Practice, The McGraw-Hill Companies, 2013.
5. https://nptel.ac.in/courses/106/105/106105182/

ARTIFICIAL INTELLIGENCE (PEC-I)

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
		L	T	P	C	CIE	SEE	Total
A55056	Professional Elective-I	3	0	0	3	50	50	100

Course Objectives

Course Objectives of Artificial Intelligence are to:

1. Summarize overview of artificial concepts.
2. Discuss uniform search and informed search.
3. Demonstrate how to solve the zero-sum gain problem.
4. Describe the logic in artificial intelligence and knowledge representation.
5. Elaborate notion of different production and expert systems in AI.

Course Outcomes

At the end of the Artificial Intelligence course, students will be able to:

1. Describe the concepts and applications of artificial intelligence.
2. Compare uniform search and informed search algorithms.
3. Solve problems using Zero Sum Game algorithms.
4. Represent logic for given problems using facts and rules.
5. Summarize functionalities of production and expert systems.

UNIT I

Overview of Artificial Intelligence: Introduction. The Turing Test, Strong AI Versus Weak AI, Identifying Problems Suitable for AI, Applications and Methods, Early History of AI, Recent History of AI to the Present, AI in the New Millennium.

UNIT II

Uninformed Search: Introduction: Search in Intelligent Systems, State-Space Graphs, Generate-and-Test Paradigm, Blind Search Algorithms, Implementing and Comparing Blind Search Algorithms.

Informed Search: Introduction, Heuristics, Informed Search Algorithms – Finding Any Solution, The Best-First Search, The Beam Search, Additional Metrics for Search Algorithms, Informed Search – Finding an Optimal Solution.

UNIT III

Search Using Games: Introduction, Game Trees and Minimax Evaluation, Minimax with Alpha-Beta Pruning, Variations and Improvements to Minimax, Games of Chance and the Expect minimax Algorithm.

UNIT IV

Logic in Artificial Intelligence: Introduction, Logic and Representation, Propositional Logic, Predicate Logic – Introduction, Several Other Logics, Uncertainty and Probability.

Knowledge Representation: Introduction, Graphical Sketches and the Human Window, Graphs and the Bridges of Königsberg Problem, Search Trees, Representational Choices, Production Systems, Object Orientation, Frames, Semantic Networks.

UNIT V

Production Systems: Introduction, Background, Production Systems and Inference Methods, Production Systems and Cellular Automata, Stochastic Processes and Markov Chains, Basic Features and Examples of Expert Systems.

Text Book

1. Stephen Lucci, Danny Kopec, Artificial Intelligence in the 21st Century-A Living Introduction, Mercury Learning and Information, Second Edition, 2016.

Reference Books

1. Russell, Norvig: Artificial Intelligence, A Modern Approach, Pearson Education, Second Edition, 2004.
2. Rich, Knight, Nair: Artificial Intelligence, Tata McGraw Hill, Third Edition, 2009
3. Saroj Kaushik. Artificial Intelligence. Cengage Learning, 2011.

FORMAL LANGUAGES AND AUTOMATA THEORY (PEC-I)

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A55045	Professional Elective-I	L	T	P	C	CIE	SEE	Total
		3	0	0	3	50	50	100

Course Objectives

Course Objectives of Formal Languages and Automata Theory are to:

1. Summarize the concepts of Formal Languages and different kinds of finite automata.
2. Interpret capabilities of context free grammar.
3. Identify the significance of pushdown automata.
4. Categorize various grammars of regular language.
5. Outline the importance of Turing Machines.

Course Outcomes

At the end of this Formal Languages and Automata Theory course, students will be able to:

1. Design of regular expressions for language constructs and conversions of NFA to DFA.
2. Demonstrate the derivations and properties of context free grammars.
3. Analyze the applications of pushdown automata.
4. Construct DFA for Right Linear Grammar and Left Linear Grammar.
5. Appreciate the role of the Turing machine as a computational and universal machine.

UNIT I

Fundamental concepts: Strings, Alphabets, Language operations, Regular Expressions, Regular Languages: Finite automata, Types of finite automata (FA)-Non deterministic Finite Automata (NFA), Deterministic Finite Automata (DFA), NFA with ε-Moves, regular expression representation; Regular expressions to NFA; NFA with ε-Moves to NFA without ε-Moves; NFA to DFA Conversions; Minimization of DFA (Proofs Not Required) [TB:1, CH:1]

UNIT II

DFA with more than two outputs: Moore and Melay machines, Pumping Lemma for Regular Sets: Closure properties of Regular Sets (Proofs Not Required): Context Free Grammars (CFG), Right most, Leftmost –derivations, Parse Trees; Operator Grammar: Unit productions; Chomsky normal forms; (Proofs Not Required) [TB:2, CH:2,3] [TB-1, CH:5,7]

UNIT III

Left recursion and Elimination of left recursion in CFG: Elimination of useless symbols and unit productions; Greibach Normal Form, Push Down automata (PDA): Types of PDA: Design of a PDA for a given CFG. (Proofs Not Required) [TB:2, CH:5,6] [TB:1, CH:6]

UNIT IV

Regular Grammars (RG), Design of DFA for a given RG: Right linear and left linear Grammars and conversions: Definition of Context Sensitive Grammar (CSG) and Linear bounded automata (LBA) (Proofs Not Required). [TB:2, CH:4,5]

UNIT V

Definition of unrestricted Grammar and Turing Machine (TM): Chomsky hierarchy on Languages, Grammars and recognizers; Design of TM as recognizer; Types of TM: Computational problems of TM with multiple tracks; Decidability Problem; Churches hypothesis (Proofs Not Required) [TB:2, CH:4]

Text Books

1. John Hopcroft, Rajeev Motwani, Jeffrey Ullman, Introduction to Automata Theory, Languages and Computation, Third Edition, Pearson, 2013.
2. Vivek Kulkarni, Theory of Computation, Oxford University press 2013, Fifth Edition, 2018.

Reference Books

1. Daniel I. A. Cohen, Introduction to Computer Theory, Second Edition, John Wiley, 1996.
2. John C Martin, Introduction to languages and the theory of Computation, Third Edition, TATA McGraw Hill, 2014.

OPERATING SYSTEMS

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A55025	Core	L	T	P	C	CIE	SEE	Total
		3	0	0	3	50	50	100

Course Objectives

Course Objectives of Operating System are to:

1. Introduce basic concepts of operating system and process management.
2. Discuss various CPU scheduling algorithms and problems of process. Synchronization.
3. Demonstrate different methods for handling deadlock.
4. Describe about memory management Techniques.
5. Explore the File system, system security and protection mechanisms.

Course Outcomes

At the end of the Operating System course, students will be able to:

1. Summarize operating system and process management concepts.
2. Apply process scheduling and synchronization related issues.
3. Outline Deadlock Prevention, Avoidance, Detection and recovery mechanisms.
4. Analyze effectively memory management concepts.
5. Illustrate various protection and security measures.

UNIT I

Operating Systems Overview and Process Management: Introduction-What operating systems do, uni-programmed and multi-programmed, Operating System operations, Operating system services, System calls, Types of System calls, Operating System structure.

Process Management: Process concepts, Operations on processes, Inter process communication. Threads: overview, Multithreading models.

UNIT II

Process Scheduling and Synchronization: Process Scheduling – Basic concepts, Scheduling criteria, Scheduling algorithms, Thread scheduling.

Process Synchronization: Background, The critical section problem, Peterson's solution, Synchronization hardware, Semaphore, Classical problems of synchronization, Monitors.

UNIT III

Deadlocks: System model, Deadlock characterization, Methods for handling deadlocks, Deadlock prevention, Detection and avoidance, Recovery from deadlock.

UNIT IV

Memory Management: Swapping, Contiguous memory allocation, Paging, Segmentation.

Virtual memory management - Demand paging, copy-on-write, page-replacement, Thrashing.

UNIT V

File System, System Protection and Security: Storage management – File concept, Access methods, Directory and disk structure, File-system mounting. System protection- Goals of protection, principles of protection, Domain of protection, Access matrix.

System Security – Security problem, Program threats, System and Network threats.

Text Book

1. Abraham Silberchatz, Peter B. Galvin, Greg Gagne, Operating System Concepts, 9th Edition, John Wiley, 2016.

Reference Books

1. D. M. Dharmdhere, Operating Systems – A Concept based Approach, 2nd Edition, TMH, 2007.
2. Andrew S Tanenbaum, Modern Operating Systems, Third Edition, PHI, 2008.
3. Behrouz A. Forouzan, Richard F. Gilberg, Unix and Shell programming, Cengage Learning, 2009.

ENTREPRENEURSHIP DEVELOPMENT

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A55080	HSS&MC	L	T	P	C	CIE	SEE	Total
		2	1	0	3	50	50	100

Course Objectives

The objective of this course is to familiarize the student with entrepreneurship, the issues involved in it, the potential of entrepreneurship and intrapreneurship, the legal environment and statutory issues and explore various funding opportunities.

Course Outcomes

At the end of this Entrepreneurship Development course, students will be able to:

1. Interpret the concepts of Entrepreneurship and Intrapreneurship.
2. Apply the opportunity identification techniques
3. Differentiate needs of different segments
4. Develop business model and MVP
5. Recognize organizational forms, IPR concerns and funding opportunities for startups.

UNIT I

Introduction to Entrepreneurship: Entrepreneurship and Intrapreneurship, Business Incubators, Rural entrepreneurship, Social Entrepreneurship, women entrepreneurs, Role of entrepreneurs in economic development, Types of entrepreneurs. Entrepreneurial mind set and stress, Causes of failure.

UNIT II

Opportunity identification: Myths and realities of entrepreneurship, Opportunity identification, Problem worth solving, idea generation techniques, Design thinking.

UNIT III

Customer analysis: Market segmentation, consumer persona, Product market fit, Unique Value proposition.

UNIT IV

Business model and MVP: Business model canvas, MVP, Risks and assumptions, Importance of financial planning.

UNIT V

Organizational forms Funding Opportunities: Organizational forms - Partnership, Sole proprietorship, Corporation. Intellectual Property Rights- Copyrights, Trademarks, Patents. Law Vs. Ethics, Informal capital- Friends and Family, Angels, Venture Capitalists, Idea/ Patent, Growth strategies

Text Books

1. D F Kuratko and T V Rao "Entrepreneurship- A South-Asian Perspective "Cengage Learning, 2012
2. Vasant Desai, Small Scale Industries and Entrepreneurship, HPH, 2012

Reference Books

1. Rajeev Roy, Entrepreneurship, Oxford University Press, 2/e, 2012
2. Dhruv Nath, Sushanto Mitra, Funding Your Startup: And Other Nightmares, 2020
3. V Srinivasa Rao, Lean Digital Thinking: Digitalizing Businesses in a New World Order, Bloomsbury India, 2021
4. S. K. Mohanty, Fundamentals of Entrepreneurship, PHI, 1/e,2005
5. MOOCS by Wadhwani Foundation

CRYPTOGRAPHY LAB

B. Tech III Year I Semester					Cyber Security			
Code	**Category**	**Hours / Week**			**Credits**	**Marks**		
A55211	Core	L	T	P	C	CIE	SEE	Total
		0	0	2	1	50	50	100

Course Outcomes

At the end of this Cryptography lab course, students will be able to:

1. Perform Encryption and Decryption Algorithms.
2. Demonstrate Double Transposition Cipher.
3. Implement Shared key using Diffie Hellman algorithm.
4. Evaluate RSA Encryption and Decryption model.
5. Construct El-Gamal Cryptographic Algorithm.

List of Experiments

Week 1- 2

1. Introduction of Caesar Cipher.
2. Implementation of Encryption using CAESAR CIPHER.
3. Implementation of Decryption using CAESAR CIPHER.

Week 3

Implementation of One time Pad.

Week 4

Implementation of Hill Cipher.

Week 5-6

1. Implementation of Transposition Cipher.
2. Implementation of Double Transposition Cipher.

Week 7

Implementation of Stream Cipher RC4.

Week 8-9

1. Implementation of Diffie Hellman Algorithm.
2. Implementation of RSA Algorithm.

Week 10

Implementation of El-Gamal Cryptographic Algorithm.

Week 11-12

Implementation of DES Algorithm.

Week 13-14

Implementation of SHA-1, SHA-2 and SHA-3 Algorithms.

Note: The above experiments are for indicative purposes only. However, the concerned faculty member can add a few more experiments in addition to the existing. In such cases the concerned faculty member should get the syllabus approved by the BoS.

NETWORK SECURITY LAB

B. Tech III Year I Semester					Cyber Security			
Code	**Category**	**Hours / Week**			**Credits**	**Marks**		
A55212	Core	L	T	P	C	CIE	SEE	Total
		0	0	3	1.5	50	50	100

Course Outcomes

At the end of this Network Security lab course, students will be able to:

1. Perform secure data transmission using digital signatures (GnuPG).
2. Build a honey pot & installation of rootkits.
3. Imitate reconnaissance tools and packet sniffer tools.
4. Demonstrate the installation process of Intrusion Detection System- IDS (e.g., SNORT).
5. Implement VPN (Virtual Private Network).

List of Experiments

Week 1

Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG).

Week 2

Setup a honeypot and monitor the honeypot on network (KF Sensor).

Week 3

Installation of rootkits and study about the variety of options.

Week 4

Defeating Malware:
a) Building Trojans.
b) Rootkit Hunter.

Week 5

Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

Week 6

Study of packet sniffer tools like Wireshark, ethereal, tcpdump etc. Use the tools to do the following
a) Observer performance in promiscuous as well as non-promiscuous mode.
b) Show that packets can be traced based on different filters.

Week 7

Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

Week 8

1. Install IDS (e.g., SNORT) and study the logs.
2. Use of iptables in Linux to create firewalls.

Week 9

Write a program to study the steps of implementation of Virtual Private Network

(VPNs) using Packet tracer or GNS3.

Week 10

Perform an experiment to grab a banner with telnet and perform the task using Netcat.

Week 11-12

Perform an experiment for Port Scanning with nmap, super scan or any other equivalent Using nmap
a) Find Open ports on a system.
b) Find machines which are active.
c) Find the version of remote OS on other systems.
d) Find the version of s/w installed on other system (using nmap or any other software).

Week 13

Install Rootkits and study variety of options.

Week 14

1. Generate minimum 10 passwords of length 12 characters using OpenSSL command.
2. wireless audit on an access point or a router and decrypt WEP and WPA (Net Stumbler).

Week 15

Review

All Software / Tools used in this lab are open source,

1. GnuPG, KF Sensor, WHOIS, dig, traceroute, nslookup.
2. Wireshark, ethereal, tcpdump.
3. Packet tracer / GNS3
4. nmap, Rootkits, Net Stumbler.

Note: The above experiments are for indicative purposes only. However, the concerned faculty member can add a few more experiments in addition to the existing. In such cases the concerned faculty member should get the syllabus approved by the BoS.

QUANTITATIVE APTITUDE AND REASONING

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A55288	BSC-Lab	L	T	P	C	CIE	SEE	Total
		0	0	3	1.5	50	50	100

UNIT I

Number System: Speed Maths, Numbers, Factors, Prime and Coprimes, LCM & HCF, Divisibility rules, Finding the unit digit and applications, Remainder theory.

Ratio and Proportion with Ages: Definition of ratio and proportion, finding the resultant ratio. Problems based on ratios and ages.

Percentages: Introduction to percentages, Percentage Increase /Decrease, Results on Population, Results on Depreciation, Variations, Applications of Percentage.

Profit and Loss: Classification of Profit and Loss, Profit/ Loss Percentages, Successive Discount.

UNIT II

Time and Distance: Difference between the average, Relative and Effective speed, reaching the destination late and early, stoppage time per hour, problems based on Trains and problems based on Boats.

Time and Work: Calculating Efficiency, alternate days concept, work and wages, Chain rule, problems based on Pipes and cisterns.

Simple and Compound Interest: Simple interest, Principle, Rate, Amount, Applications of Simple interest, Compound interest, compounded annually, Compounded Half yearly, Compounded Quarterly, Difference between simple and compound interest.

UNIT III

Permutations and Combinations: Fundamental rules, Problems on Permutations and Combinations.

Probability: Definition, Notations and Problems based on Probability.

Mean, Median and Mode: Introduction and problems on Mean, Median and Mode.

Partnership: Relation between Partners, Period of Investments and Shares.

Averages: Average of different groups, change in average by adding, deleting and replacement of objects.

Flow Charts: Introduction of symbols and problems on flow charts.

UNIT IV

Seating Arrangement: Circular, Row, Column, Square and Double row arrangement.

Puzzles: Paragraph puzzles, incomplete puzzles and problems on them.

Number Series: Number, Alphabet and Letter Series.

Analogy: Simple, Double, Word and Number Analogy.

Coding and Decoding: Classifications and Problems on Coding and Decoding.

UNIT V

Clocks: Relation between minute and hour hand, angle between hands of a clock, exceptional cases in clocks. Gaining and loosing of time.

Calendars: Classification of years, finding the day of any random calendar date, repetition of calendar years.

Direction Sense Test: Sort of directions in puzzle, distance between two points, Problems on shadows.

Blood Relations: Defining the various relations among the members of a family, solving blood relation puzzles by using symbols and notations. Problems on coded relations.

Text Books

1. R.S Agarwal, Verbal and Non-Verbal Reasoning, New Edition, S. Chand.
2. R.S Agarwal, Quantitative Aptitude, New Edition, S. Chand.

Reference Book

1. Abhijeet Guha, Quantitative Aptitude, New Edition, Mc Graw Hill.

NATIONAL SPORTS ORGANIZATION & NATIONAL SERVICE SCHEME

B. Tech III Year I Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A55091	Mandatory	L	T	P	C	CIE	SEE	Total
		2	0	0	0	--	--	--

Course Outcomes

At the end of this NSO & NSS course, students will be able to:

1. Apply knowledge of physical education, growth and development, sports and games knowledge, history of physical education and yoga to explain aim and objectives of physical education.
2. Learn health education, personal hygiene, health problems-prevention and control, physical fitness and wellness, health and first aid management.
3. Develop a broad understanding of NSS and Volunteerism for more involvement.
4. Understand the working of community service model for their all-round personality development.
5. Understand the entrepreneurship and its implementation to solve the community identified problems and work on a project by using learned skills on identified problem of the society.

UNIT I

HEALTH AND WELLNESS: Dimensions of Health: Physical, Mental and Social. Objectives of Health Education. Definition and Dimensions of Wellness – Physical, Emotional, Social, Spiritual, Intellectual and Environmental Wellness. Achieving Wellness.

Practical: Basketball, Cricket, Kho-Kho (Any Two) & Badminton (Mandatory), Layout of Courts / Fields, Skills, Rules & Lead-up Games.

UNIT II

FITNESS AND BODY COMPOSITION: Physical Fitness Components: Body Composition, Muscular Endurance, Strength, Cardiovascular Fitness and Flexibility, Importance of Cardio-Respiratory Endurance. Obesity and Health Risk Factors. Body Composition Indicators and Measurements.

Practical: Football, Kabaddi, Volleyball (Any Two) & Table Tennis (Mandatory) Layout of Courts / Fields, Skills, Rules & Lead-up Games.

UNIT III

Introduction and Basic Concepts of NSS: History, Philosophy, Aims & Objectives of NSS. Emblem, Flag, Motto, Song, Badge, Organizational Structure, Roles and Responsibilities of Various NSS functionaries. NSS Programs and Activities, Volunteerism and Shramdan.

UNIT IV

Personality Development Through Community Service: Importance and Role of Youth Leadership, Life Competencies, Social Harmony and National Integration, Youth Development Programs in India, Citizenship, Health, Hygiene and Sanitation, Environment Issues, Disaster Management, Life Skills.

UNIT V

Vocational and Entrepreneurship Skills Development: Definition and meaning of Entrepreneurship, Qualities of good entrepreneur, Steps /ways in operating an Enterprise and role of financial and support service Institutions. Project Cycle Management, Resource Mobilization and Documentation and Reporting.

Project work/ Practical: Conducting Surveys on Special Theme, Involving in Shramadan, Swachh Bharat, Blood Donation, Tree Plantation, Awareness Programs, Identify the Community Problems and List out the all-Possible Solutions, Educate the Villagers on Health, Hygiene, Sanitation and Environment Protection. Self-Review of the Students on their Improvements by Participating in the Community Service Programs.

References

NSO:

1. The Soul of Wellness: 12 holistic principles for achieving a healthy body, mind, heart and spirit, Rajiv Parti, Select book incorporation, New York.
2. H. & Walter, H., (1976). Turners School Health Education. Saint Louis: The C.Y. Mosby Company.
3. Nemir, A. (n.d.). The School Health Education. New York: Harber and Brothers.
4. Health Fitness Instructor's Handbook, Edward T Howley, Human Kinetics, USA.

NSS:

1. About NSS: National Service Scheme Manual by Government of India Ministry of Youth Affairs & Sports, New Delhi.
2. Robert N Lussier, Management Fundamentals - Concepts, Applications, Skill Development, Cengage Learning, First Edition, 2012.
3. Handbook of Personality Development – Mroczek Little (eds), 2006.
4. Richard Blundel, Exploring Entrepreneurship Practices and Perspectives, Oxford, 2011.

ANURAG UNIVERSITY

WEB APPLICATION SECURITY

B. Tech III Year II Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A56044	Core	L	T	P	C	CIE	SEE	Total
		3	0	0	3	50	50	100

Course Objectives

Course Objectives of Web Application Security are to:

1. Summarize History of Software Security and the Structure of a Modern Web Application.
2. Identifying methods for Secure Web Applications and Cross-Site Scripting (XSS).
3. Differentiate various types of SQL Injections and Exploiting Third-Party Dependencies.
4. Sketch the Software Architecture and Secure Application Architecture.
5. Distinguish various types of defending methods against XSS Attacks, Dos Attacks.

Course Outcomes

At the end of this Web Application Security course, students will be able to:

1. Discuss the History of Software Security.
2. Identify the Weak Points in Application Architecture and explore the techniques for Hacking Web Applications.
3. Describe the use of SQL injections.
4. Demonstrate different types of Injections and Reviewing Code for Security methods and can sketch the Architectures for Software and Secure Application.
5. Explore various types of XSS Attacks, Dos Attacks.

UNIT I

Introduction: The History of Software Security: The Origins of Hacking, Automated Enigma Code Cracking, Circa 1940, Telephone "Phreaking," Circa 1950, Anti-Phreaking Technology, Circa 1960.The Origins of Computer Hacking, Circa 1980, The Rise of the World Wide Web, Circa 2000, Hackers in the Modern Era, Circa 2015+.

Introduction to Web Application Reconnaissance: Information Gathering, Web Application Mapping.

The Structure of a Modern Web Application: Modern Versus Legacy Web Applications, REST APIs, JavaScript Object Notation, JavaScript. SPA Frameworks, Authentication and Authorization Systems, Web Servers, Server-Side Databases, Client-Side Data Stores. **Finding Subdomains.**

UNIT II

API Analysis: Endpoint Discovery, Authentication Mechanisms, Endpoint Shapes.

Identifying Third-Party Dependencies: Detecting Client-Side Frameworks, Detecting Server-Side Frameworks. **Identifying Weak Points in Application Architecture:** Secure Versus Insecure Architecture Signals, Multiple Layers of Security, Adoption and Reinvention.

Cross-Site Scripting (XSS): XSS Discovery and Exploitation, Stored XSS, Reflected XSS, DOM-Based XSS, Mutation-Based XSS.

Cross-Site Request Forgery (CSRF): Query Parameter Tampering, Alternate GET Payloads. CSRF against POST Endpoints.

UNIT III

XML External Entity (XXE) : Direct XXE , Indirect XXE.

Injection: SQL Injection, Code Injection, Command Injection.

Denial of Service (DoS): regex DoS (ReDoS), Logical DoS Vulnerabilities, Distributed DoS.

Exploiting Third-Party Dependencies: Methods of Integration, Package Managers, Common Vulnerabilities and Exposures Database.

UNIT IV

Securing Modern Web Applications: Defensive Software Architecture, Comprehensive Code Reviews, Vulnerability Discovery, Vulnerability Analysis, Vulnerability Management, Regression Testing, Mitigation Strategies, Applied Recon and Offense Techniques.

Secure Application Architecture: Analyzing Feature Requirements, Authentication and Authorization, PII and Financial Data, Searching.

Reviewing Code for Security: How to Start a Code Review, Archetypical Vulnerabilities Versus Custom Logic Bugs, Where to Start a Security Review, Secure-Coding Anti-Patterns.

Vulnerability Discovery, Vulnerability Management.

UNIT V

Defending Against XSS Attacks: Anti-XSS Coding Best Practices, Sanitizing User Input, CSS, Content Security Policy for XSS Prevention. **Defending Against CSRF Attacks:** Header Verification, CSRF Tokens, Anti-CRSF Coding Best Practices. **Defending Against XXE:** Evaluating Other Data Formats, Advanced XXE Risks. **Defending Against Injection:** Mitigating SQL Injection, Generic Injection Defenses. **Defending Against DoS:** Protecting Against Regex DoS, Protecting Against Logical DoS Protecting Against DDoS. **Securing Third-Party Dependencies.**

Text Book

1. Andrew Hoffman, Web Application Security Exploitation and Countermeasures for Modern Web Applications, O'Reilly Media,2020.

Reference Book

1. Sanjib Sinha, Bug Bounty Hunting for Web Security: Find and Exploit Vulnerabilities in Web Sites and Applications, Springer, 2019.

WRITING SECURE CODE

B. Tech III Year II Semester					Cyber Security			
Code	**Category**	**Hours / Week**			**Credits**	**Marks**		
A56045	Core	L	T	P	C	CIE	SEE	Total
		3	0	0	3	50	50	100

Course Objectives

Course Objectives of Writing Secure Code are to:

1. Demonstrate the need of secure systems.
2. Analyze the different secure coding techniques.
3. Explain access control mechanism and storing secretes.
4. Describe different types of attacks in networking applications.
5. Illustrate security in web-based applications.

Course Outcomes

At the end of this Writing Secure Code course, students will be able to:

1. Analyze the need of secure systems.
2. Explore the different Secure coding techniques.
3. Describe about how to run the code with least privileges.
4. Demonstrate different types of attacks in networking applications.
5. Design and develop Security applications to provide security in web-based applications.

UNIT I

The need for Secure Systems: Applications on the World Wide Web, Some Ideas for Instilling a Security Culture. **Designing Secure Systems:** Two Common Security Mistakes, Security Principles to Live By, Security Design by Threat Modeling, Security Techniques.

UNIT II

Secure Coding Techniques:

Public Enemy #1: The Buffer Overrun: Static Buffer Overruns, Heap Overruns, Array Indexing Errors, Format String Bugs, Unicode and ANSI Buffer Size Mismatches, Preventing Buffer Overruns. **Determining Good Access Control:** Why ACLs Are Important. What Makes Up an ACL? A Method of Choosing Good ACLs, Creating ACLs, NULL DACLs and Other Dangerous ACE Types, Other Access Control Mechanisms.

UNIT III

Secure Coding Techniques:

Running with Least Privilege: Least Privilege in the Real World, Brief Overview of Access Control, Brief Overview of Privileges, Brief Overview of Tokens**,** How Tokens, Privileges, SIDs, ACLs, and Processes Relate, A Process for Determining Appropriate Privilege, Low-Privilege Service Accounts in Windows XP and Windows .NET Server, Debugging Least-Privilege Issues.

Storing Secrets: Attack Methods, Sometimes You Don't Need to Store a Secret, Getting the Secret from the User, Raising the Security Bar, An Idea: Using External Devices to Encrypt Secret Data.

UNIT IV

Network-Based Application Considerations

Socket Security: Avoiding Server Hijacking, Choosing Server Interfaces, Accepting Connections, Writing Firewall-Friendly Applications, Spoofing and Host-Based and Port-Based Trust. **Securing RPC, ActiveX Controls, and DCOM:** Secure RPC Best Practices, Secure DCOM Best Practices, Secure ActiveX Best Practices. **Protecting Against Denial-of-Service Attacks:** Application Failure Attacks, CPU Starvation Attacks, Memory Starvation Attacks, Resource Starvation Attacks, Network Bandwidth Attacks.

UNIT V

Securing Web-Based Services

Never Trust User Input: User Input Vulnerabilities, User Input Remedies. **Web-Specific Canonicalization Bugs:** 7-Bit and 8-Bit ASCII, Hexadecimal Escape Codes, UTF-8 Variable-Width Encoding, UCS-2 Unicode Encoding, Double Encoding, HTML Escape Codes, Web-Based Canonicalization Remedies. **Other Web-Based Security Topics:** HTTP Trust Issues, ISAPI Applications and Filters, Don't Store Secrets in Web Pages. **Testing Secure Applications:** The Role of the Security Tester, Security Testing Is Different, Building the Security Test Plan, Testing Clients with Rogue Servers, Should a User See or Modify That Data? Testing with Security Templates, Test Code Should Be of Great Quality, Test the End-to-End Solution, Slightly Off-Topic: Code Reviews.

Text Book

1. Michael Howard and David LeBlanc, Writing Secure Code, Microsoft, 2001.

Reference Book

1. Robert C. Seacord, Secure Coding in C and C++, Second Edition**,** Pearson Education, Inc., 2013.

FUNDAMENTALS OF CYBER SECURITY (PEC-II)

B. Tech III Year II Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A56046	Professional Elective-II	L	T	P	C	CIE	SEE	Total
		3	1	0	4	50	50	100

Course Objectives

Course Objectives of Fundamentals of Cyber Security are to:

1. Summarize major types of cyber-attacks.
2. Discuss computer malware programs and their impact on the world.
3. Elaborate firewall and password management.
4. Describe major cyber-security prevention mechanisms.
5. Outline Cyber-Security aspects of wireless networks and routers.

Course Outcomes

At the end of this Fundamentals of Cyber Security course, students will be able to:

1. 1. Analyze the cyber security needs of an organization.
2. 2. Design operational and strategic cyber security strategies and policies.
3. 3. Demonstrate various network security applications.
4. 4.Analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
5. 5. Design and develop a security architecture for an organization.

UNIT I

Introduction to Cyber Security Basics, Importance of Cyber Security, Cyber- attacks, objectives of cyber- attacks, Types of Cyber-attacks, Denial of Service (DoS), Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM) Attacks, Crypto jacking, SQL Injection, Spamming, Cyber-terrorism, Digital Property Misappropriation, zero-day exploitation, phishing, digital vandalism, cyber-stalking, cyber frauds and forgery.

UNIT II

Introduction to Cyber-attacks and their impact, Equifax Data Theft, VPNFilter Cyber- attack, WannaCry Ransom Attack, Peta Cyber-attack, US Election Manipulation, Power Grid Hacking, Shadow Network attack, GitHub DDoS

Attack, Under Armor Account Hacking, Types of Computer Malware, Viruses, Trojan Horse, Rootkit, Spyware, Worms, Adware, Scare-ware, Browser Hijacker.

UNIT III

Introduction to Computer Security, Firewall Settings, Antivirus Software, Anti-Spyware Software, Anti-Spam Software, Security Updates, Secure Browsing Settings, Scan Devices before Data Transfer, Social Engineering Attack Precautions. Password Management, Basics of Passwords, Threats to Passwords, Good and Bad about Passwords, Hacking Password, Effective Password Management, Creating and Managing Secure Passwords, Strong Password, Use of Biometrics, Two-Factor Authentication, Multi-Factor Authentication, Password Manager Tools.

UNIT IV

Prevention from Cyber-attacks, Algorithms and Techniques, Cyber-attack Detection, Cyber-attack Prediction, Cyber-attack Prevention , Firewalls, Activating Windows Firewall, Windows 10 firewall, Windows 7 firewall, Enabling Windows 7 firewall, Enabling Windows firewall service, Traffic Issues and rules , firewall settings, Intrusion Detection/Prevention Systems, Intrusion Detection System (IDS) , Intrusion Prevention System (IPS),,Authentication Using Hash, Message Digest , Secure Hash Algorithm ., Multi-Factor Authentication, Activating Two-Factor Authentication, Creating Application Specific Passwords , What If Your Phone with All Apps Enabled Is Lost?, Mac Computer Firewall Configuration, Virtual Private Network.

UNIT V

Introduction to Wireless Security, LAN Vulnerabilities, Reconnaissance Vulnerability, Resource Stealing and Invasion, Rogue Access Points (APs), STA and AP Plain Text Transaction, Denial of Service (DoS), Default AP Configuration, Rogue Insiders, Protocol Vulnerabilities, Ad Hoc Network Mode Security Problems ,Wireless WAN Vulnerabilities ,IoT Vulnerabilities, Wireless Network Security Measures, Modify Default Configuration, Wireless Router Location, Update Router Software, Stronger Encryption Algorithms, MAC Address Filtering ,Useful Tips on Safe Use of Wireless Network.

Text Book

1. Dr Kutub Thakur Dr Al-Sakib Khan Pathan, Cyber-security Fundamentals Real-World Perspective, first edition published 2020 by CRC Press, © 2020 Taylor & Francis Group, LLC.

Reference Books

1. Rajkumar Singh Rathore, Aatif Jamshed, Mayank Bhusan, Fundamental of Cyber Security Principles and Theory and Practices, BPB Publications, 01-Jun-2018.
2. J. Pieprzyk, T. Hardjono and J. Seberry, Fundamentals of computer security, Springer, 2003.

ELLIPTICAL CURVE CRYPTOGRAPHY (PEC-II)

B. Tech III Year II Semester					Cyber Security			
Code	**Category**	**Hours / Week**			**Credits**	**Marks**		
A56047	Professional Elective-II	L	T	P	C	CIE	SEE	Total
		3	1	0	4	50	50	100

Course Objectives

Course Objectives of Elliptical Curve Cryptography are to:

1. Describe the need for Elliptic curve cryptography.
2. Differentiate Groups and Rings.
3. Outline the terms Elliptic curves and fields.
4. Summarize the arithmetic operations on elliptic curves.
5. Discuss Hardware and software security Implementation.

Course Outcomes

At the end of this Elliptical Curve Cryptography course, students will be able to:

1. Identify some of the factors driving the need for Elliptic curves.
2. Classify Groups and Rings.
3. Summarize arithmetic operations on elliptic curves.
4. Apply elliptic curves operations in real world applications.
5. Outline Hardware and Software security using Elliptic curves.

UNIT I

Finite Field Arithmetic: Introduction to finite fields, Prime field arithmetic, Binary field arithmetic and Optimal extension field arithmetic. **Elliptic Curve Arithmetic:** Introduction to elliptic curves, Point representation and the group law, Point multiplication, Koblitz curves, Curves with efficiently computable endomorphisms, Point multiplication using halving and Point multiplication costs.

UNIT II

Cryptography basics: Public-key cryptography: RSA systems, Discrete logarithm systems, Elliptic curve systems, Why elliptic curve cryptography?

Cryptographic Protocols: The elliptic curve discrete logarithm problem, Domain parameters, Key pairs, Signature schemes, Public-key encryption, Key establishment.

UNIT III

Elliptic Curve Arithmetic: Introduction to elliptic curves, Point representation and the group law, Point multiplication, Koblitz curves, Curves with efficiently computable endomorphisms, Point multiplication using halving, Point multiplication costs.

UNIT IV

Elliptic Curves over Finite Fields: Number of Rational Points, The Weil Conjectures, The Endomorphism Ring and Calculating the Hasse Invariant.

UNIT V

Software implementation: Integer arithmetic, Floating-point arithmetic, SIMD and field arithmetic, Platform miscellany and Timings. **Hardware implementation:** Design criteria and Field arithmetic processors. **Secure implementation:** Power analysis attacks, Electromagnetic analysis attacks, Error message analysis, Fault analysis attacks and Timing attacks.

Text Book

1. Darrel Hankerson, Alfred Menezes,Scott Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2004.

Reference Books

1. Joseph H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer, 1994.
2. Joseph H. Silverman, The Arithmetic of Elliptic Curves, Second Edition, Springer, 2000.

DIGITAL FORENSICS (PEC-II)

B. Tech III Year II Semester					Cyber Security			
Code	**Category**	**Hours / Week**			**Credits**	**Marks**		
A56048	Professional Elective-II	L	T	P	C	CIE	SEE	Total
		3	1	0	4	50	50	100

Course Objectives

Course Objectives of Digital Forensics are to:

1. Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
2. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools.
4. Describes Cellular Networks, Operating Systems, Cell Phone Evidence, Cell Phone Forensic Tools and global Positioning Systems.
5. Explores Image Capturing, Authenticating Evidence, Hidden Data Extraction, Data Storage, File Systems, Recovery of deleted files, Cracking Passwords, Internet Crime Investigations, Web Attack Investigations.

Course Outcomes

At the end of this Digital Forensics course, students will be able to:

1. Discuss rapidly changing and fascinating field of computer forensics.
2. Describe technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Explore Network security tools, Network attacks, inside threat, incident response, Network Evidence and Investigations.
4. Summarize Cellular Networks, Operating Systems, Cell Phone Evidence, Cell Phone Forensic Tools and global Positioning Systems.
5. Describe Image Capturing, Authenticating Evidence, Hidden Data Extraction, Data Storage, File Systems, Recovery of deleted files, Cracking Passwords, Internet Crime Investigations, Web Attack Investigations.

UNIT I

Introduction: What is digital forensics, uses of digital forensics, the digital forensic process, scientific process, role of the forensic examiner in the judicial system.
Labs and Tools: Forensic laboratories, policies and Procedures, quality assurance, digital forensic tools.

UNIT II

Collecting Evidence: Crime Scenes and Collecting Evidence, Protecting Cell Phones from Network Signals, Alert, Documenting the Scene, cloning, more advanced, final report.

Anti-Forensics: Hiding data, Password attacks, Data Destruction, Defragmentation as Anti-Forensic Technique.

UNIT III

Legal: Criminal Law—searches without a Warrant, Consent Forms, Cell Phone Searches: The Supreme Court Weighs In, Searching with a Warrant, Electronic Discovery, Expert Testimony.
Network Forensics: Introduction, Network security tools, Network attacks, inside threat, incident response, Network Evidence and Investigations, Training and Research.

UNIT IV

Mobile device forensics: Cellular Networks, Operating Systems, Cell Phone Evidence, Cell Phone Forensic Tools, Global Positioning Systems.
Internet and E-mail: Internet Overview, Additional Resources, Web Browsers, More advanced, E-mail, Shared E-Mail Accounts, Tracing E-Mail, Reading E-Mail Headers, Social Networking Sites.

UNIT V

Looking Ahead: Challenges and Concerns: Standards and Controls, Cloud Forensics, Additional Resources, Cloud Persistence-Dropbox.
Image Capturing, Authenticating Evidence, Hidden Data Extraction, Data Storage, File Systems, Recovery of deleted files, Cracking Passwords, Internet Crime Investigations, Web Attack Investigations.

Text Book

1.John Sammons, The Basics of Digital Forensics, Elsevier, 1st Edition, 2015.

Reference Books

1. Davidoff, S. and Ham, J., Network Forensics Tracking Hackers through Cyberspace, Prentice Hall, 2012.
2. Michael G. Solomon, K Rudolph, Ed Tittel, Broom N., and Barrett D., Computer Forensics Jump Start, Willey Publishing, Inc., 2011.
3. Marcella, Albert J., Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes, New York, Auerbach publications, 2008.
4. Davidoff, Sherri, Network forensics: Tracking hackers through cyberspace, Pearson education India private limited, 2017.

CYBER LAW AND SECURITY POLICY (PEC-III)

B. Tech III Year II Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A56049	Professional Elective-III	L	T	P	C	CIE	SEE	Total
		3	1	0	4	50	50	100

Course Objectives

Course Objectives of Cyber Law and Security Policy are to:

1. Describe legal and jurisdictional issues regarding Cyber Security.
2. Discuss legal and ethical implications involving Social Networks and Virtual Worlds.
3. Summarize Legal and Ethical Implications in Cyberspace: An International Perspective.
4. Outline Security Policy Sets without Frameworks, Information Security Policy Sets with Frameworks.
5. Explain Information Security Procedures and Standards.

Course Outcomes

At the end of this Cyber Law and Security Policy course, students will be able to:

1. Identify relevant Legal and Jurisdictional issues regarding Cyber Security.
2. Discuss Legal and Ethical Implications Involving Social Networks and Virtual Worlds.
3. Describe Legal and Ethical Implications in Cyberspace: An International Perspective.
4. Explore Security Policy Sets without Frameworks, Information Security Policy Sets with Frameworks.
5. Explore Information Security Procedures and Standards.

UNIT I

Legal and Jurisdictional Issues Regarding Cyberspace: Responsibility, Jurisdiction, and the Future of "Privacy by Design", Hacking: Legal and Ethical Aspects of an Ambiguous Activity, Emerging Cybercrime Trends: Legal, Ethical, and Practical Issues, Law and Technology at Crossroads in Cyberspace: Where Do We Go From Here?, Cyber Law, Cyber Ethics and Online Gambling. **[TB-1]**

UNIT II

Legal and Ethical Implications Involving Social Networks and Virtual Worlds: An Overview of Child Abuses in 3D Social Networks and Online Video Games, Ethics and Legal Aspects of Virtual Worlds, Narbs as a Measure and Indicator of Identity Narratives, Cloud Based Social Network Sites: Under Whose Control? **[TB-1]**

UNIT III

Legal and Ethical Implications in Cyberspace: An International Perspective: Al-Qaeda on Web 2.0: Radicalization and Recruitment Strategies, Google in China: Corporate Responsibility on a Censored Internet, All's WELL that Ends WELL: A Comparative Analysis of the Constitutional and Administrative Frameworks of Cyberspace and the United Kingdom, A UK Law Perspective: Defamation Law as it Applies on the Internet, The Hellenic Framework for Computer Program Copyright Protection Following the Implementation of the Relative European Union Directives, Internet Advertising: Legal Aspects in the European Union. **[TB-1]**

UNIT IV

Introduction: Information Security Policy Types, Information Security Policy Sets without Frameworks**,** Information Security Policy Sets with Frameworks, Common Information SPFs, Tailoring Information SPFs, deriving a Policy Set from a Framework, Policy Statements, Specific Information Security Policies, Policy Document Examples. **[TB-2]**

UNIT V

Information Security Procedures and Standards, Scoping the Project, Information Security Policy Project Roles, Information Security Policy Project Phases, Information Security Policy Revision Project, Information Security Policy Project Application. **[TB-2]**

Text Books

1. Alfreda Dudley, James Braman, Giovanni Vincenti, Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices, Information Science Reference, 2011.
2. Douglas J Landoll, Information security policies, procedures and standards practitioner's Reference, CRC Press, 2016,

Reference Books

1. Anthony Reyes, Richard Brittson, Kevin O'Shea, James Steele, Cybercrime investigations: bridging the gaps between security professionals, law enforcement, and prosecutors, Syngress Publishing, 2007
2. Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus Sachs, Jeffrey Schmidt, Joseph Weiss, Cyber security policy guidebook, Wiley, 2012

SECURITY ASSESSMENT AND RISK ANALYSIS (PEC-III)

B. Tech III Year II Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A56050	Professional Elective-III	L	T	P	C	CIE	SEE	Total
		3	1	0	4	50	50	100

Course Objectives

Course Objectives of Security Assessment and Risk Analysis are to:

1. Describe the concepts of risk management, Contingency Planning and Its Components.
2. summarize IR Planning Process, Developing the Incident Response Policy.
3. Illustrate Digital Forensics Methodology, eDiscovery and Anti-Forensics.
4. Explore Disaster Classifications, Forming the Disaster Recovery Team, Disaster Recovery Planning Functions.
5. Demonstrate BC Plan, Continuous Improvement of the BC Process, Maintaining the BC Plan.

Course Outcomes

At the end of this Security Assessment and Risk Analysis course, students will be able to:

1. Explore Risk Management, Contingency Planning and Its Components.
2. Develop the Incident Response Policy using IR planning process.
3. Explore Digital Forensics Methodology, eDiscovery and Anti-Forensics.
4. Summarize Disaster Classifications, Forming the Disaster Recovery Team, Disaster Recovery Planning Functions.
5. Design BC Plan, Continuous Improvement of the BC Process, Maintenance of BC Plan.

UNIT I

Introduction: Information Security, Overview of Risk Management, Contingency Planning and Its Components, Role of Information Security Policy in Developing Contingency Plans.
Planning for Organizational Readiness: Beginning the Contingency Planning Process, Elements Required to Begin Contingency Planning, Business Impact Analysis, BIA Data Collection, Budgeting for Contingency Operations.

UNIT II

Incident Response: Planning: Introduction, The IR Planning Process, Developing the Incident Response Policy, Incident Response Planning, Information for attack success end case, planning for "Before the Incident", The CCDC, Assembling and Maintaining the Final IR Plan.

Incident Response: Detection and Decision Making: Introduction, Detecting Incidents, Technical Details: Rootkits, Intrusion Detection and Prevention Systems, Technical Details: Processes and Services, Incident Decision Making.

UNIT III

Incident Response: Organizing and Preparing the CSIRT: Introduction, Building the CSIRT, A Sample Generic Policy and High-Level Procedures for Contingency Plans, Outsourcing Incident Response.
Incident Response: Response Strategies: Introduction, IR Response Strategies, The Cuckoo's Egg, Incident Containment and Eradication Strategies for Specific Attacks, Handling Denial of Service (DoS) Incidents.
Incident Response: Recovery and Maintenance: Introduction, Recovery, Maintenance, Incident Forensics, Digital Forensics Methodology, eDiscovery and Anti-Forensics.

UNIT IV

Disaster Recovery: Preparation and Implementation: Introduction, Disaster Classifications, Forming the Disaster Recovery Team, Disaster Recovery Planning Functions, Information Technology Contingency Planning Considerations, Sample Disaster Recovery Plans.
Disaster Recovery: Operation and Maintenance: Introduction, Facing Key Challenges, Preparation: Training the DR Team and the Users, Disaster Response Phase, Recovery Phase, Resumption Phase, Restoration Phase.

UNIT V

Business Continuity Planning: Introduction, Business Continuity Team, Business Continuity Policy a Plan Functions, Implementing the BC Plan, Continuous Improvement of the BC Process, Maintaining the BC Plan.
Crisis Management and International Standards in IR/DR/BC: Introduction, Crisis Management in the Organization, Preparing for Crisis Management, International Standards in IR/DR/BC.

Text Book

1. Whitman & Mattord, Principles of Incident Response and Disaster Recovery, Course Technology, 2013.

Reference Books

1. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf
2. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security Fifth Edition, 2014, Cengage Learning.

SECURITY FOR CYBER PHYSICAL SYSTEMS (PEC-III)

B. Tech III Year II Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A56051	Professional Elective-III	L	T	P	C	CIE	SEE	Total
		3	1	0	4	50	50	100

Course Objectives

Course Objectives of Security of Cyber Physical Systems are to:

1. Describe the challenges and scientific foundation of cyber-security in various domains and networks.
2. Discuss metrics for information in cyber-security.
3. Summarize national security legal aspects and Privacy laws.
4. Compare different types key management strategies and challenges.
5. Outline Secure Registration and Remote Attestation of IoT Devices.

Course Outcomes

At the end of this Security of Cyber Physical Systems course, students will be able to:

1. Discuss the standards and Topologies of Cyber Physical Systems.
2. Explain outsourcing in Cyber Physical Systems.
3. Describe Cyber Physical Systems security and safety aspects.
4. Design Security keys for Cyber Physical Systems.
5. Design Registration and Remote Attestation of IoT Devices.

UNIT I

Introduction to security in cyber physical System, Defining Security and Privacy, Defining Cyber-Physical Systems, Examples of Security and Privacy in Action, Approaches to Secure Cyber-Physical Systems, Ongoing Security and Privacy Challenges for CPSs. Network Security and privacy for cyber-physical systems, Security and Privacy Issues in CPSs, Local Network Security for CPSs, Secure Local Communication, Internet-Wide Secure Communication, Security and Privacy for Cloud-Interconnected CPSs.

UNIT II

Information Theoretic Metrics Quantifying Privacy in Cyber-Physical Systems, Social Perspective and Motivation, Information Theoretic Privacy Measures, Privacy Models and Protection, Smart City Scenario: System Perspective, Conclusion and Outlook.

UNIT III

Cyber-Physical Systems and National Security Concerns, National Security Concerns Arising from Cyber-Physical Systems, National Security Implications of Attacks on Cyber- Physical Systems, Legal Considerations of Cyber-Physical Systems and the Internet of Things, Privacy and Technology in Recent History, Privacy Law, Future Challenges.

UNIT IV

Key Management in CPSs, Security Goals and Threat Model, CPS Key Management Design Principles, CPS Key Management, Dynamic versus Static, Public Key versus Symmetric Key, Public Key Cryptography, Symmetric Key Cryptography, Centralized versus Distributed, Deterministic versus Probabilistic, Standard versus Proprietary, Key Distribution versus Key Revocation, Key Management for SCADA Systems, CPS Key Management Challenges and Open Research Issues.

UNIT V

Case Study: Secure Registration and Remote Attestation of IoT Devices, Joining the Cloud, Cloud Integration with IoT, Security and Privacy in Cloud and IoT, Technologies, Web Connectivity, Reference Scenario and Motivation, Stack4Things Architecture, Capabilities for Making IoT Devices Secure Over the Cloud, Adding Security Capabilities to Stack4Things, Conclusions.

Text Book

1. Houbing Song, Glenn A. Fink, Sabina Jeschke, Security and Privacy in Cyber-Physical Systems Foundations, Principles, and Applications, First edition, IEEE PRESS Wiley, 2017.

Reference Books

1. Song, Houbing, et al., eds. Cyber-physical systems: foundations, principles and applications. Morgan Kaufmann, 2016.
2. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson edition, 2016.

ANURAG UNIVERSITY

WEB APPLICATIONS SECURITY LAB

B. Tech III Year II Semester					Cyber Security			
Code	**Category**	**Hours / Week**			**Credits**	**Marks**		
A56213	Core	L	T	P	C	CIE	SEE	Total
		0	0	3	1.5	50	50	100

Course Outcomes

At the end of this Web Applications Security Lab course, students will be able to:

1. Design static web pages and validate using JavaScript.
2. Build a dynamic web page using Servlets and JSP.
3. Implement database connectivity using JDBC.
4. Demonstrate N-STALKER based Web Application Security solutions and JCrypt tool.
5. Implement a case for Cross-Site Scripting (XSS) and Secure API access.

List of Experiments

Week 1

Practice Basic HTML Programs:

- Basic Tags
- Lists
- Tables
- Frames
- Forms

Week 2

Design the following static web pages required for online book store application.

- Registration page
- Login page
- User profile page
- Shopping page
- Catalog page

Apply internal and external CSS (Cascading Style Sheets) for "Online Book Store Application".

Week 3

Implement Alert Box, Confirm Box, Prompt Box. & Control Structures, Conditional Statements using JavaScript.

Week 4

Write JavaScript to validate the following fields of registration page [Book Store Application]: for the fields like Username, Password, Phone Number, Email-id.

Week 5-6

Apache Tomcat Installation Procedure.

Write a program to display the HELLO WORLD message using Java servlet.

Develop a Java Servlet application to implement and demonstrate get() and post()

methods (Using HTTPServlet Class)

Week 7

Write a Java Servlet program to implement a dynamic HTML using servlet (Username and password should be accepted using HTML and displayed using Servlet)

Write a JAVA Servlet to track HttpSession by accepting user name and password using HTML and display the profile page on successful login.

Week 8

Write a program to display the HELLO WORLD message using JSP.

Write a JSP program which uses jsp:include and jsp:forward action to display a Webpage.

Write a Java JSP program which uses ＜jsp:plugin＞ tag to run a applet.

Week 9

Perform Data Definition Language (DDL) and Data Manipulation Language (DML) commands using MySql.

Week 10

Implement Database connectivity using JDBC and perform the following:

- Table creation
- Data Manipulation.

Week 11

A case study using N-STALKER in Web Application Security solutions.

Week 12

Install JCrypt tool (or any other equivalent) and demonstrate Symmetric, Asymmetric crypto algorithms.

Week 13

Implement a case for Cross-Site Scripting (XSS)

Week 14

Implementation of Secure API access (Authentication Mechanisms).

Week 15

Review

All Software / Tools used in this lab are open source, like

- HTML, JAVA, Servlets, JSP etc.
- Snort , OSSEC , Suricata.
- CSS, nmap, N-STALKER.
- https://www.nstalker.com/about/nstalker/
- https://www.cryptool.org/en/jct/
- https://www.netfilter.org/

Note: The above experiments are for indicative purposes only. However, the concerned faculty member can add a few more experiments in addition to the existing. In such cases the concerned faculty member should get the syllabus approved by the BoS.

ANURAG UNIVERSITY

WRITING SECURE CODE LAB

B. Tech III Year II Semester					Cyber Security			
Code	**Category**	**Hours / Week**			**Credits**	**Marks**		
A56214	Core	L	T	P	C	CIE	SEE	Total
		0	0	3	1.5	50	50	100

Course Outcomes

At the end of this Writing Secure Code lab course, students will be able to:

1. Write Secure Code for a software application.
2. Appreciate security vulnerabilities and how they are exploited.
3. Explore various tools to implement secure code.
4. Develop skills to provide high secured security-oriented software techniques.

List of Experiments

Week 1

1. Writing Secure Code – An introduction.

Week 2

2. Introduction to various Tools and Libraries to write secure code.
3. Secure Software Tools Installation.

Week 3-4

4. Write a program to handle Array Indexing Errors.
5. Write a program to Safe String Handling.

Week 5

6. Implement a program to Avoiding Server Hijacking.
7. Write a program to Limiting the Domain Usage.
8. Write a program to test User Input Vulnerabilities.

Week 6-7

9. Implement SQL Injection technique.
10. Implement X-Frame options.

Week 8-9

11. Write a program to implement HTTP security headers.
12. Write a program to implement HTTP Cookies.

Week 10-11

13. Write a program for Testing Sockets-Based Applications.
14. Write a program for Testing HTTP-Based Applications.

Week 12-15

15. Write a program for Testing File-Based Applications.
16. Write a program for Testing Command Line Arguments.
17. Write a program for Testing Cross-Site Scripting and Script-Injection Bugs.

Week 16

Review.

TEXT BOOK:

1. Michael Howard and David LeBlanc, Writing Secure Code, Microsoft, 2001.

Note: The above experiments are for indicative purposes only. However, the concerned faculty member can add a few more experiments in addition to the existing. In such cases the concerned faculty member should get the syllabus approved by the BoS.

VERBAL ABILITY AND CRITICAL REASONING

B. Tech III Year II Semester					Cyber Security			
Code	Category	Hours / Week			Credits	Marks		
A56288	BSC	L	T	P	C	CIE	SEE	Total
		0	0	3	1.5	50	50	100

UNIT I

Data Interpretation: Tabular, Pie-charts, Bar and line graphs and Problems on all models.
Data Sufficiency: Introduction and Problems based on all Quant and logical topics.

Allegations and Mixtures: Allegation rule, mean value of the mixture, Replacement of equal quantity of mixtures.

UNIT II

Geometry: Line, line segment, angle, Triangles and Polygons with their Properties.

Mensuration: Area and perimeter of Triangle, Rectangle, Square, Parallelogram, Trapezium, Surface area & Volume of 3D figures.

Logarithms: Formulas and Problems based on Logarithms.

Progressions and Quadratic Equations: Arithmetic, Geometric and Harmonic Progressions and their relations. General forms of Quadratic equations and finding the roots and their nature.

UNIT III

Syllogisms: Statements and Conclusions by using vein diagrams.

Odd One Out: Classification and problems based of Odd one out.

Cubes and Dice: Types of cubes and dice with Examples.

Statement and Conclusions: Introduction, Types of conclusions and different cases.

UNIT IV

Tenses: Types, usages, question solving.
Vocabulary: Types, usage and error spotting.

Inference: Conclusion reached on the basis of evidence and reasoning, question solving.

Para jumbles: Arranging the jumbled sentences by using the strategies.

Sentence completion: Completing a sentence by filling the gaps by understanding & analyzing the meaning of the sentence along with the approaches.

UNIT V

Subject Verb Agreement: Rules and examples for finding the right subject and verb.

Sentence Correction: Error spotting and correcting the sentence.

Reading Comprehension: Understanding Meaning. Understanding the meaning of a text means figuring out what the passage is trying to tell you. ...Drawing Connections. ...Summarizing and Synthesizing.

Direct & Indirect Speeches: What is Direct & Indirect Speech? reporting the message of the speaker in the exact words as spoken by the speaker and examples.

Active Voice & Passive Voice: Types of active and passive voice, rules and examples.

Text Books

1. R.S Agarwal, Verbal and Non-Verbal Reasoning, New Edition, S. Chand.
2. R.S Agarwal, Quantitative Aptitude, New Edition, S. Chand.

Reference Book

1. Abhijeet Guha, Quantitative Aptitude, New Edition, Mc Graw Hill.

ANURAG UNIVERSITY

PROFESSIONAL SKILLS LAB

B. Tech III Year II Semester					Cyber Security			
Code	**Category**	**Hours / Week**			**Credits**	**Marks**		
A56231	HSS & MC	L	T	P	C	CIE	SEE	Total
		0	0	3	1.5	50	50	100

Introduction

The world needs skillful employees who can contribute towards organizational growth. The professionals are expected to be confident and maintain amicable relations with clients and customers. With this backdrop, this course helps the students understand the importance of various aspects of professional life.

The course aims at making the students familiar with the corporate world and grooms them accordingly. This course is designed to improvise communication principles, interpersonal communication and public speaking of learners.

Course Objectives

Course Objectives of Professional Skills Lab are to:

1. Prepare the students to understand and acquire different personality traits.
2. Mould the students for global challenges and international careers.
3. Excel the students in areas of self - management and ethics at the workplace.

Course Outcomes

At the end of this Professional Skills Lab course, students will be able to:

1. Demonstrate their listening skills and effectively use verbal and non-verbal communication.
2. Identify and analyze their self-discovery skills.
3. Develop their efficient work habits and self-management skills in the workplace.
4. Exhibit their leadership, empowering and influencing skills to promote change and innovation.
5. Analyze their professional interests' qualifications and other required skills for their career development.

EXERCISE- I: Self – Improvement

Self Esteem – SWOT Analysis – Attitude - Image Matters.

EXERCISE – II: Communication Essentials

Communication Basics - Barriers to Communication - Listening Skills - Communication Styles - Fitting in and Getting Along - Communicating Electronically.

EXERCISE – III: Work Skills

Self - Management Tools - Efficient Work Habits - Our Diverse Society - Understanding Other Cultures - Fairness in the Workplace - Right and Wrong in the Workplace.

EXERCISE – IV: Leadership Skills

What Makes a Leader - Empowering and influencing others - Leading change and Innovation.

EXERCISE – V: Career Planning

Analyse your interest and qualifications- Networking and other sources of Job Leads- Job Search Documents- the Job Interview- Planning your Career - Networking – It never stops.

Minimum Requirement of infrastructural facilities for Professional Skills Lab

A Spacious room with movable chairs, Public Address System, etc.

References

1. Carnegie, Dale. How to win friends & Influence People. Maanu Graphics Publishers.
2. Covey, Stephen. Seven Habits of Highly Effective People. New York: Simon and Schuster, Inc., 1989.
3. Peale, Norman.V. The Power of Positive Thinking. New York: Simon and Schuster, 2002.
4. Sharma, Robin. The Monk Who Sold His Ferrari. Jaico.
5. Wallace, Masters. Personal Development for Life and Work. CENGAGE Learning.