B. Sc. - CYBER SECURITY
Syllabus

MANONMANIAM SUNDARANAR UNIVERSITY
Tirunelveli, Tamil Nadu, India
(Effective from Academic Year 2023-24 onwards)

B. Sc. - CYBER SECURITY
Manonmaniam Sundaranar University
Tirunelveli, Tamil Nadu
(Effective from Academic Year 2023-24 onwards)

Scheme, Regulations and Syllabus

Title of the course: Bachelor of Science (B. Sc.) Degree course in Cyber Security

Duration of the course: Three years under semester pattern

Eligibility: Candidates for the BSc Degree in Cyber Securityshould have passed higher secondary examination in any group conducted by the Board of Secondary Education, Government of Tamil Nadu or any other equivalent examination prescribed and accepted by the Syndicate / SCAA of the Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu.

Objectives of the course:

- ***To make the students conversant with the causes and consequences of cybercrimes and security breaches in cyber space.***

- ***To get the students acquainted with the structure and functioning of the Cyberspace and its security.***

- ***To develop in students, skill sets such as Communication, Analytical Thinking, Problem Solving, Decision Making, Imbibe Value Systems and to construct a regard for cyber security, Cyber forensic and information security– Through effective participatory teaching methodology, Practical Training and Internship.***

- ***To prepare the students to take up a career in the field of Cyber Security, Cyber Forensic and Information Security,***

Programme Outcomes of the Course

On completion of the programme, students will be able to comprehend and complete the programme outcomes, such as

Program Out comes

PO 1	Propose novel idea(s) towards solutions to problem in cyber space and securing data with utmost care
PO 2	Develop scientific outlook and see the relevance of science concepts in all aspects of cyber security
PO 3	Identify and analyse complex scientific problems of cyber space using principles of applied sciences and cyber security
PO 4	Formulate solutions to problems in cyber space and cyber security
PO 5	Analyse critically the given cyber data, ascribe meaning to them and draw objective conclusions
PO 6	Developing epithetical concern towards various cyber security and ways to solve which will be very beneficial to society
PO 7	Imbibe ethical, moral, social and cyber values to become cultured and civilized global netizens

Programme Specific Outcomes

PSO 1	Articulate diverse aspects of cyber and information security using cyber forensic via scientific methods, software's and instrumentations.
PSO 2	Illustrate the functioning of the cyber space and securing cyber information /data
PSO 3	Differentiate between and among methods/ protocols, and evaluative procedures required in the investigative process that is required for solving cybercrimes and also document the same as per norms.
PSO 4	Assist in forensic investigation using established principles of forensic and step by step development of the investigative procedures.
PSO 5	Recommend and develop various aspects of cyber forensic investigation protocols based on the type of cybercrimes, evidences collected, evaluative procedures conducted and aid in solving cases keeping in mind the laws and justice systems pertaining to the same.

Structure of the programme: This B.Sc. programme will consist of following courses compulsory for all students:

- *4- Language courses/ papers*
- *4-Englishcourses/ papers*
- *16- Core courses/ papers (including Practical's)*
- *8- Electives courses/ papers (including Practical's)*
- *7- Skill Enhancement courses/ papers(including Non- Major Electives &Practical's)*
- *4- Ability Enhancement Compulsory courses/ papers*
- *1- Skill Enhancement courses/ papers (Foundation Course)*
- *2- EVS courses/ papers*
- *1- Value Education courses/ papers*
- *1- Summer Internship/ Industrial Training courses/ papers*
- *1- Extension Activity courses/ papers*
- *1- Professional Competency Skill courses/ papers*

Semester wise breakup of courses/ papers

- ***I Semester: 2 LanguageCourses/ Papers,2 Core Courses/ Papers, 1 Elective Course/ Paper, 1 Skill Enhancement Course/ Paper (NME)- Practical's, 1 Ability Enhancement Compulsory Course/ Paper- Soft Skill and 1 Skill Enhancement (Foundation) Course/ Paper***
- ***II Semester: 2 LanguageCourses/ Papers,2 Core Courses/ Papers, 1 Elective Course/ Paper, 1 Skill Enhancement Course/ Paper (NME),1 Skill Enhancement Course/ Paper- Practical's and 1 Ability Enhancement Compulsory Course/ Paper- Soft Skill***
- ***III Semester: 2 Language Courses/ Papers,2 Core Courses/ Papers, 1 Elective Course/ Paper, 1 Skill Enhancement Course/ Paper (Entrepreneur Skill), 1 Skill Enhancement Course/ Paper - Practical's, 1 Ability Enhancement Compulsory Course/ Paper- Soft Skill and 1 EVS Course/ Paper***
- ***IV Semester: 2 Language Courses/ Papers,2 Core Courses/ Papers, 1 Elective Course/ Paper, 2 Skill Enhancement Course/ Paper (including one practical's, 1***

Skill Enhancement Courses/ Papers, 1 Ability Enhancement Compulsory Course/ Paper- Soft Skill and 1 EVS Course/ Paper

- *V Semester: 4 Core Courses/ Papers (including one project), 2Elective Courses/ Papers, 1 Value Education Course/ Paper and 1 Summer Internship/ Industrial Training Course/ Paper*
- *VI Semester: 4 Core Courses/ Papers, 2Elective Courses/ Papers, 1 Extension Activity Course/ Paper and 1 Professional Competency Course/ Paper*

Note: All courses/ papers listed above are compulsory papers

Examinations

Theory Papers

There will be a continuous internal assessment (CIA) comprising of tests, seminars and assignments and one End- semester examination during each semester. The internal assessments will form 25 % of the marks (including 15 marks for CIA, 5 marks for assignments and seminar presentation) and the end semester examination will form 75 % of the total marks.Passing minimum: 40% in the Internal(10 marks) and External (30 marks),respectively.

Practical Papers

In practical papers the continuous internal assessments will form 50 % of the marks and the end semester examination will form 50 % of the total marks.

Phase of Examinations	Marks	Practical
Phase I – Continuous Internal Assessment	Total – 50 Continuous Assessment (Internal)- 25 marks Test – 25 marks. Three tests should be conducted and average of two test marks will be taken.	"N" number of practical's be conducted based on the practical's prescribed in the syllabus and the marks should be distributed equally for each practical. There is no passing minimum in the Internal Continuous Assessment.
	Calculation of marks: Sum of marks awarded to number of practical's + the Average marks of two tests.	Passing minimum: 40% (20 marks) in the Internal.
Phase II–	Total – 50	Only one practical examination shall be

End semester assessment (March/April)– Practical Examinations	Marks awarded by the Course teacher– 25 marks (20 for practical's + 5 for Records) Marks awarded by the External Examiner– 25 marks (20 for practical's + 5 for Records)	conducted at the end of semester for the students on lot basis by appointing TWO examiners from the same college / one from the other institution. 1. Course Teacher 2. External Examiner (From Other Institution/ Department/ from the same Department) Passing minimum: 40% (20 marks) in the External.

Theory Paper- QUESTION PAPER – Outline

Time: Three hours Maximum: 75 Marks

PART – A (10X1=10 Marks)

Answer ALL the Questions, choose the correct answer.

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

PART – B (5X5=25 Marks)

Answer ALL the Questions, choosing either (a) or (b), in about 150 words.

11. (a)

(or)

(b)

12. (a)

(or)

(b)

13. (a)

(or)

(b)

14. (a)

(or)

(b)

15. (a)

(or)

(b)

PART – C (5X8=40 Marks)

Answer ALL the Questions, choosing either (a) or (b), in about 250 words.

16. (a)

(or)

(b)

17. (a)

(or)

(b)

18. (a)

(or)

(b)

19. (a)

(or)

(b)

20. (a)

(or)

(b)

SEMESTER I

	Title of the Paper	Teaching hrs/ week	Credits
1.1	Tamil/Other Languages	4	3
1.2	English	4	3
1.3 (CCI)	Basics of Computersand Problem Solving	4	4
1.4 (CCII)	Basics of Computer Networks	4	4
1.5 (Elective 1)	Fundamentals of Operating Systems	3	3
1.6 SEC 1 (NME) Practical's	Network Lab and Kali Linux Lab-Practical's	2	2
1.7 AECC	Soft Skill 1	2	2
1.8 Skill Enhancement (Foundation Course)	Basics of Programming (C++)	2	2
	Total	25	23

SEMESTER II

	Title of the Paper	Teaching hrs/ week	Credits
2.1	Tamil/Other Languages	4	3
2.2	English	4	3
2.3 (CC III)	Introduction to Cyber Security	4	4
2.4 (CC IV)	Advanced Networking and Communication Protocols	4	4
2.5 (Elective II)	Forms of Cyber Crime	3	3
2.6 SEC- 2 (NME)	Advance Programming- Python	2	2
2.7 SEC- 3 Practical's	SQL and Internet Security Lab-Practical's	2	2
AECC	Soft Skill 2	2	2
	Total	25	23

SEMESTER III

	Title of the Paper	Teaching hrs/week	Credits
3.1	Tamil/Other Languages	4	3
3.2	English	4	3
3.3 (CC V)	Mobile andWebApplication Security	4	4
3.4 (CC VI)	Fundamentals of Criminology and Cyber Criminology	3	4
3.5 (Elective III)	Data Privacy- Technology and Law	3	3
3.6 (SEC 4)	Fundamentals of Cloud Computing	3	1
3.7 SEC 5-Practical's	Advanced Internet Security Tools (Lab)-Practical's	2	2
3.8 AECC	Soft Skill 3	2	2
3.9 EVS	Environmental Studies	-	-
	Total	25	26

SEMESTER IV

	Title of the Paper	Teaching hrs/week	Credits
4.1	Tamil/Other Languages	4	3
4.2	English	4	3
4.3 (CC VII)	Intrusion Detection and Prevention System	4	4
4.4 (CC VIII)	Data Storage	4	4
4.5 (Elective IV)	Criminal Laws and Cybercrimes	3	3
4.6 SEC- 6	Intrusion Detection and Prevention Lab-Practical's	2	2
4.7 SEC- 7	Database Management and Data structure	2	2
4.8 AECC-	Soft Skill 4	2	2
4.9 EVS	Environmental Studies	-	2
	Total	**25**	**26**

SEMESTER V

	Title of the Paper	Teaching hrs/week	Credits
5.1 (CCIX)	Cryptography	4	4
5.2 (CC X)	Cyber Laws and Intellectual Property Rights	4	4
5.3 (CC XI)	Information Security and Audit	4	4
5.4 (CC XII)	Project / Case Study Presentation (Non- Programming)	4	4
5.5 (Elective V)	Basics of Ethical Hacking	3	3
5.6 (Elective VI)	Cryptography Lab- Practical's	3	3
5.7 Value Education	Value Education	2	2
5.8Mini Project	Summer Internship/ Industrial Training	1	2
	Total	**25**	**26**

SEMESTER VI

	Title of the Paper	Teaching hrs/week	Credits
6.1 (CC XIII)	Cyber Forensics and Investigation	4	4
6.2 (CC XIV)	Security Architecture and Designs	4	4
6.3 (CC XV)	Cloud Technology and Security	4	4
6.4 (CC XVI)	Computational Intelligence	4	4
6.5 (Elective VII)	Cyber Risk Management	3	3
6.6 (Elective VIII)	Firewall and Internet Security	3	3
6.7 Extension Activity	Extension Activity	1	1
6.8 Professional Competency Skill	Cybercrime Investigation and Cyber Forensics Lab- Practical's	2	2
	Total	**25**	**25**
Total Credits for 6 Semester (Three Years) is 144			

Teaching Methodology

NOTE ON TEACHING METHODOLOGY

A. The teaching methodology adopted for the course will utilize participatory learning methods, like workshops, discussions, assignments, short education tours, seminars, peer teaching, and group work, apart from regular lectures.
B. The syllabus indicates the type of teaching mety89hod, to be adopted for a particular topic, in the footnote of the same page.
C. The method suggested is only indicative; the concerned course teacher can use other methods or a combination of many methods, in order to improve the quality of knowledge transfer.
D. Course teachers adopting participatory teaching methods may please take extra care on the following issues
    a) Set a brief, clear task rather than lecturing
    b) Use hands-on, multi-sensory materials rather than rely only on verbal communication
    c) Create an informal, relaxed atmosphere
    d) Choose growth-producing activities Evoke feelings, beliefs, needs, doubts, perceptions, aspirations
    e) Encourage creativity, analysis, planning
    f) Decentralize decision-making
E. The following portions give details of some contemporary techniques that may be followed by course teachers, who teach various subjects in criminology.

1. BRAINSTORMING

Brainstorming is a familiar technique in which the teacher asks a specific question or describes a particular scenario, and students offer many different ideas. These ideas are then usually written on a flipchart or chalkboard and considered for further discussion.

2. CASE ANALYSIS

A case study is a written scenario that usually involves an important community situation. Since it is written beforehand, it can be specifically created to address relevant local issues.

3. DEMONSTRATIONS / PRACTICAL EXPOSURE

A demonstration is a structured performance of an activity to show, rather than simply tell, a group how the activity is done. This method brings to life some information that you may have already presented in a lecture.

4. DRAMATIZATION

A dramatization is a carefully scripted play where the characters act out a scene related to a learning situation. It is designed to bring out the important issues to be discussed or messages to be learned.

5. SMALL GROUP DISCUSSION

A small group discussion is a structured session in which three to six students exchange ideas and opinions about a particular topic or accomplish a task together. After the groups have had an opportunity to work together, they report the highlights of their work back to the large group, and the teacher helps the group process the activity. Begin the learning activity by briefly presenting a topic to the large group. Then, divide the group into smaller groups and set a clear task for the small groups to accomplish. Write directions, goals and time allotted for the task on a chalkboard, flipchart or handout. As groups are working, walk around and listen in briefly to each group. Keep groups focused by announcing the time remaining periodically. After the small group work, students typically reassemble in the large group and a representative from each small group shares their findings to the large group for a whole group discussion. Help the group process the activity to be sure the intended message was conveyed.

6. LECTURETTE

A lecturette is a short, oral presentation of facts or theory. No more than 15-20 minutes in length, the goal of a lecturette is to impart information in a direct, highly organized fashion. The course teacher presents knowledge on a topic, sometimes using flipcharts, computer software presentations or other media to guide the discussion.

Teaching Methodology

7. FISHBOWL

In a fishbowl discussion, most of the students sit in a large circle, while a smaller group of students sits inside the circle.

The fishbowl can be used in two distinct ways:

- As a structured brainstorming session: Choose a specific topic based on the group's needs or interests. A handful of seats are placed inside a larger circle. Students who have something to say about the topic at hand sit in the center. Anyone sitting inside the fishbowl can make a comment, offer information, respond to someone else in the center, or ask a question. When someone from the outside circle has a point to make, he or she taps the shoulder of someone in the center and takes that person's seat. This continues, with people from the outside tapping and replacing people on the inside, as a lively brainstorm takes place. You will need to process the many ideas after the fishbowl exercise.
- For structured observation of a group process: Students in the fishbowl are given a specific task to do, while students outside the fishbowl act as observers of the group process. The inner group works on its task together, and the outer group is asked to note specific behaviours. To process the activity, ask the inner group to reflect on the group process, and ask the outer group to describe what they observed.

8. GAMES

Games are appropriate participatory tools when they are used to encourage students to take charge of their own learning, and to test and reinforce new knowledge or skills. Adapt a popular game to convey or test knowledge of a particular topic, or create a new game to test or reinforce learning. Divide the students into groups, if necessary, to play the game. Use games after information has already been shared using another method (e.g., lecturette, demonstration, jigsaw learning, etc.) or to assess students' knowledge at the start of a learning activity.

9. JIG SAW LEARNING

In a jigsaw activity, evenly divided groups are given a topic to learn (a piece of the puzzle to master). Once these small groups have mastered the content, the groups are reorganized so that each new group contains one member from each original group (now each group contains all essential pieces of the puzzle to put together). Each new group now contains an "expert" on the content that they have mastered in the original groups, and one at a time, each expert teaches the new content to the newly formed groups. The teacher then processes the activity and emphasizes key learning.

10. PANEL DISCUSSIONS

This method usually involves the presentation of an issue by several teachers at a table in front of a group. Usually, each teacher speaks briefly on the topic and then a moderator solicits questions from the audience. The moderator introduces the presenters/ teachers, keeps the discussion on the topic and within time limits and summarizes the discussion at the end. Each teacher typically speaks for a set period of time (for example, five minutes). After all teachers have spoken, the moderator invites questions from students. At the end of the session, the moderator may summarize the discussion and thank the presenters for their participation.

11. SKIT

A skit is an impromptu performance by students to demonstrate something they know. Skits can be created by students to show concerns they have about such things as peer pressure, victim issues in their community or lack of resources. Give students a topic, the maximum length of the skit and the amount of time they have to prepare (depending on the complexity, 30 minutes or an afternoon, for example).

Teaching Methodology

Reading list for Participatory Teaching Methodology

Cross, K. P. (1991). Effective College Teaching. ASEE Prism, (1)2, 27-29.

Eitington, Julius E. (2002). The Winning Trainer: Winning Ways to Involve People in Learning. Boston: Butterworth Heinemann.

Hamer, L.O. (2000). The Additive Effects of Semi-structured Classroom Activities on Student Learning: An Application of Classroom-Based Experiential Learning Techniques. Journal of Marketing Education, (22)1, 25-34.

Holzer, S. M. &Andruet, R.H. (2000). Active Learning in the Classroom. Proceedings, ASEE South-eastern Section Annual Meeting, April 2-4, 2000.

Kolb, David A. (1984). Experiential Learning. New York: Prentice-Hall, Inc.

Lyra. (1990). Tools for Community Participation: A Manual for Training Trainers in Participatory Techniques. Washington, DC: PROWWESS/UNDP.

Narayan, D. and Srinivasan, L. (1994). Participatory Development Toolkit: Materials to Facilitate Community Empowerment. Washington: World Bank.

Newstrom, John W. (1993). Even More Games Trainers Play. New York: McGraw-Hill, Inc.

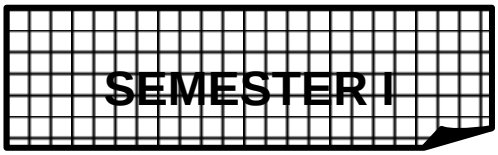
Pike, Bob and Christopher Busse. (1995). 101 Games for Trainers: A Collection of Best Activities from Creative Training Newsletter. Minneapolis, MN: Lakewood Publications.

Pretty, J N, Guijt I, Thomson, J and Scoones, I (1995). A Trainer's Guide for Participatory Learning and Action.

Silberman, Mel. (1995). 101 Ways to Make Training Active. San Francisco: Jossey-Bass Pfeiffer.

Srinivasan, (2000). Technology of Participation: Group Facilitation Methods: Effective Methods for Participation. Phoenix, AZ: Institute for Cultural Affairs.

CHOICE BASED CREDIT SYSTEM (CBCS)



Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 1		BASICS OF COMPUTERS AND PROBLEM SOLVING	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

Basics

The main objectives of this course are

- To Know the Basics of Computers.
- To Understand the Basics of Operating systems
- To Understand how to solve problems using Algorithms and Flowcharts.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Learn the fundamental concepts of computers and its function.	K1
CO2	Appreciate the computing devices.	K2
CO3	Elucidate the components of the computer.	K2 K6
CO4	Understand operating systems and its service	K3
CO5	Develop the logic of problem solving.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Apply		

Course Outline:

UNIT I: **Introduction to Computers**

Computer Overview- Characteristics of Computers- Block diagram of computer- Types of computers and features- Mini Computers- Micro Computers- Mainframe Computers- Super Computers. Hardware and software- Components of a computer system, including the processor, memory, storage, and input/output devices - Operating systems, their functions, and types. Introduction to Data Structures, Arrays, Stacks, Queues, Linked Lists, Trees, and Graphs.

UNIT II: Computer Languages

Types of Programming Languages- Machine Languages- Assembly Languages- High Level Languages- Data Organization- Drives- Files- Directories- Number Systems- Introduction to Binary, Octal, Hexadecimal system- Conversion- Simple Addition, Subtraction, Multiplication, Division.

UNIT III: Computer Devices

CPU- Types of Memory (Primary and Secondary)- RAM- ROM- PROM- EPROM- Secondary Storage Devices (CD, HD, Pen drive)- I/O Devices- Scanners- Digitizers- Plotters- LCD- Plasma Display- Network Devices- Hub- Switch- Router- Bridge- Gateway- Modem- Repeater- Access Point and Ports.

UNIT IV: Operating System and its Services

DOS – History- Files and Directories- Internal and External Commands- Batch Files- Types of OS.

UNIT V: Fundamentals of Problem Solving

Concept: problem solving- Problem solving techniques (Trial & Error, Brain storming, Divide & Conquer)- Steps in problem solving (Define Problem, Analyse Problem, Explore Solution)- Algorithms and Flowcharts (Definitions, Symbols)- Characteristics of an algorithm- Conditionals in pseudo-code- Loops in pseudo code- Time complexity: Big-Oh notation, efficiency- Simple Examples: Algorithms and flowcharts (Real Life Examples)- Simple Arithmetic Problems.

RECOMMENDED READINGS

Rajaraman V., Fundamental of Computers– B.P.B. Publications
Sinha P. K., Fundamental of Computers
Suresh Basandra, Computer Today
Sumitabha Das, Unix Concepts and Application
Computer Networks – By Tennenbum Tata MacGrow Hill Publication
Dromy R. G., How to solve it by Computer
Cormen, Leiserson, Rivest, Stein, Introduction to algorithms

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	High	High	Medium	Medium	Low	High	High
CO3	Medium	Medium	High	Low	Medium	Medium	Medium
CO4	Low	High	Low	Low	Low	Low	High
CO5	Medium	Low	High	Low	Medium	Low	Medium

Low = 13/35 = 37.14% Medium = 11/35 = 31.42% High = 11/35 = 31.42%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5

CO1	High	Medium	High	Medium	High
CO2	High	Medium	High	Low	High
CO3	Medium	Low	Medium	Low	High
CO4	Medium	Medium	Low	High	Low
CO5	Low	Low	Low	High	Medium
Correlation Levels:		**Low**	**Medium**	**High**	

Low = 8/25 = 32.0% Medium = 8/25 = 32.00% High = 9/25 = 36.0%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 2		**BASICS OF COMPUTER NETWORKS**	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To prepare students with basic networking concept.
- To understand process of data communication using protocols and standards
- To learn various topologies and applications of network.
- To understand the concept of network layer, transport layer and application layer

Course Outcomes (COs): At the end of this course of study, the students will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Understand the components of the Network.	K1
CO2	Understand the concepts and devices used networks and communication	K2
CO3	Appreciate computer networks	K2 K6
CO4	Understand the data communication	K3
CO5	Detect the problem in netwroks and devices.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Apply		

Course Outline:

UNIT I: **Introduction to Network**

Concept of communication, components of data communication (sender, receiver, message, communication media, protocols), measuring capacity of communication media (bandwidth, data transfer rate), IP address, switching techniques (Circuit switching, Packet switching). Basic Models of Network- Network Topologies- Network of Network-Modem, Ethernet card, RJ45, Repeater, Hub, Switch, Router, Gateway, WIFI card.

Network topologies and Network types: types of networks (PAN, CAN, LAN, MAN, WAN, WLAN), networking topologies (Bus, Star, Tree).
Wired communication media (Twisted pair cable, Co-axial cable, Fibre-optic cable), Wireless media (Radio waves, Micro waves, Infra-Red waves). Cloud computing.

UNIT II: OSI / TCPIP Model
Introduction to OSI Model with all layers and Devices required at each layer TCP/IP Protocol Suite Addressing-Physical, Logical, Port addresses and Special addresses. Subnetting - Subnet Masks and Network Prefix- Address Classes (A, B, C, D, E) - Private IP Addresses and NAT - Variable Length Subnet Mask (VLSM) and CIDR Notation - Subnet Design and Address Allocation - Subnetting and Routing - Broadcast and Multicast Addresses – Ipv4 Addressing and Subnetting (brief introduction).
TCP/IP Model- MAC Address representation- Organisationally Unique Identifier- Internet Protocol- Versions and Header lengths- IP Identification- IP Flags- IP fragmentation and reassembly structure- Transport Layer protocols- Port numbers- TCP Flags- Segmentation- TCP 3- way handshake and Options- encapsulation and De-encapsulation- Payload.

UNIT III:Physical Layer: Protocols
Analog and Digital data, Analog and Digital signals, Digital Signals-Bit rate, Bit length Baseband Transmission, Broadband Transmission, Transmission Impairments– Attenuation, Distortion and Noise Data Rate Limits– Noiseless channel: Nyquist's bit rate, noisy channel : Shannon's law Performance of the Network Bandwidth, Throughput, Latency(Delay),Bandwidth – Delay Product, Jitters Line Coding Characteristics, Line Coding Schemes–Unipolar -NRZ, Polar-NRZ-I, NRZ-L, RZ-Transmission Modes, Parallel Transmission and Serial Transmission–Asynchronous and Synchronous Switching-Circuit Switching, Message Switching and Packet Switching.

UNIT IV: Data Link Layer: Protocols
Subnetting IP network- Class A, B, C subnetting- Classless Inter-domain Routing (CIDR)- Subnet mask- Wild card mask- WAN Technologies- Frame Relay- Data link Connection Identifiers (DLCI)- Committed Information Rate (CIR)- Permanent Virtual Circuits (PVCs)- Multiprotocol Label Switching (MPLS)- Edge Routers- Label Switching- CE and PE Routers- Data Terminal Equipment (DTE)- Data Communication Equipment (DCE)- Clock speed.
Framing–Concept, Methods–Character Count, Flag bytes with Byte Stuffing, Starting & ending Flags with Bit Stuffing Error detection code– Hamming Distance, CRC Elementary data link protocols - Simplex stop & wait protocol, Simplex protocol for noisy channel, PPP, HDLC Sliding Window Protocols– 1-bit sliding window protocols, Pipelining – Go-Back N and Selective Repeat Random Access Protocols - ALOHA– pure and slotted, CSMA-1- persistent, p-persistent and non-persistent CSMA/CD,CSMA/CA Controlled Access - Reservation, Polling and Token Passing Channelization – Definitions – FDMA, TDMA and CDMA.

UNIT V: Network Layer and Transport Layer: Protocols
IPv4 addresses: Address space, Notation, Classful addressing, Classless addressing,

NAT, Sub netting, Super netting IPv4: Datagram, Fragmentation, checksum, options IPv6 addresses: Structure, address space, IPv6: packet format, Extension headers. Process-to-Process Delivery, Multiplexing and De-multiplexing User Datagram Protocol (UDP) - Datagram Format, Checksum, Transmission Control Protocol (TCP) - TCP Services –Process to-Process Communication, Stream Delivery Service, Sending and Receiving Buffers, Segments, Full –Duplex Communication, Connection oriented service, Reliable service TCP Features, TCP Segment Format TCP Vs UDP Static and Dynamic Routing- IP Routing Protocols- Classful and Classless Routing- RIPv1- RIPv2, Broadcast and Multicast domain- OSPF, EIGRP- Network Address Translation- IP Classes- Private IP- Public IP- Reserved IP- APIPA.

RECOMMENDED READINGS

Andrew S. Tanenbaum, Pearson, Andrew S. Tanenbaum, Computer Networks,Fifth Edition, ISBN-13: 978-0-13- 212695-3.

McGraw Hill, Behrouz Forouzan, Data Communications and Networking,Fifth Edition, ISBN 978-0-07-337622-6.

Donaldson, S., Siegel, S., Williams, C.K., Aslam, A., "Enterprise Cyber security -How to Build a Successful Cyber defense Program against Advanced Threats", Apress, 1st Edition, 2015.

Nina Godbole, Sumit Belapure, "Cyber Security", Willey, 2011.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	High	High	Medium	Medium	Low	High	High
CO3	Medium	Medium	High	Low	Medium	Medium	Medium
CO4	Low	High	Medium	Low	Low	Low	High
CO5	Medium	Low	High	Medium	Medium	Low	High

Low = 11/35 = 31.42% Medium = 12/35 = 34.28% High = 12/35 = 34.28%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	Medium	High
CO2	High	Medium	High	Low	High
CO3	Medium	Low	Medium	Low	High
CO4	Medium	Medium	Low	High	Low
CO5	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 9/25 = 36.0% Medium = 7/25 = 28.00% High = 9/25 = 36.0%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Elective 1		FUNDAMENTALS OF OPERATING SYSTEMS	3	0	0	3

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To understand the principles of Operating Systems
- To study different system calls, system programs, functions and services of Operating System
- To understand the concept of process, memory and deadlock handling.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Gain knowledge and basic understanding of Array and Structure	K1
CO2	Critically identify and gain knowledge of algorithms.	K2
CO3	Understand the functioning of the operating systems	K2
CO4	Learn scheduling algorithms and synchronization.	K3 K6
CO5	Handle Deadlock and Demand Paging.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Basics of Operating Systems**

What is an Operating System? - Interaction between- Types of Operating Systems- Time- Sharing Systems, Personal Computer Systems, Parallel Systems, Distributed Systems, Real Time Systems- System Components hardware and software's- Operating System Services- System Calls- System Programs.

UNIT II: **Processes and CPU Scheduling**

Process Concepts- Process Scheduling- Operations on Processes- Cooperating Processes- Threads- Basic Concepts of CPU Scheduling- Scheduling Criteria- Scheduling Algorithms.

UNIT III: **Concurrency: Mutual Exclusion and Synchronization**

Principles of Concurrency- Mutual Exclusion: Hardware Support- Semaphores- Monitors- Message Passing- Readers/Writers Problem.

UNIT IV: **Deadlocks and File System**

Resources- Deadlocks- Deadlock Detection and Recovery- Deadlock Avoidance-

Deadlock Prevention- Other Issues connected to deadlocks.
File concept- File Access Methods- Directory Structure- File System Structure- File Allocation Methods- Free-Space Management

UNIT V: **Memory Management and Virtual Memory**
Defining Memory and its forms- Background- Logical versus Physical Address Space Swapping- Contiguous Allocation- Paging- Segmentation- Segmentation with Paging- Demand Paging- Performance of Demand Paging- Page Replacement- Page Replacement Algorithms.

RECOMMENDED READINGS

Modern Operating Systems - By Andrew Tanenbaum, Prentice-Hall
Operating System Concep - By Silberschatz, Galvin, Wiley publication
Operating Systems - By Deitel, Deitel and Choffnes, Pearson Education
Operating Systems: Internals and Design Principles, Seventh Edition, William Stallings, Pearson Education.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	Low	Low	Low	Low	Medium	Low	High
CO2	Medium	High	Low	Medium	Low	Low	High
CO3	High	Medium	Medium	Low	Medium	Medium	Medium
CO4	Medium	High	High	Low	Low	Low	High
CO5	High	High	Medium	Low	Medium	Low	High

Low = 14/35 = 40.0% Medium = 11/35 = 31.42% High = 10/35 = 28.57%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	High	Medium
CO2	Medium	Medium	High	High	Medium
CO3	High	High	Medium	High	Low
CO4	High	Medium	Medium	Medium	High
CO5	Low	High	Low	Medium	Low
Correlation Levels:	Low	Medium	High		

Low = 5/25 = 20.0% Medium = 10/25 = 40.0% High = 10/25 = 40.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
SEC 1		NETWORK LAB AND KALI LINUX LAB- Practical's	0	0	2	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:
The main objectives of this course are

- To get hands-on Kali and Ubuntu Linux.
- To get acquainted with various algorithms in operating systems.
- The student learns to work with various Redundancy Check Algorithms, Sliding Window Protocol, Routing Algorithm, Subnetting Procedures.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Knowledge on operating systems and its functions	K1
CO2	Basic understating of the networks	K2
CO3	Install Linux distribution.	K2 K6
CO4	Install security tools on operating systems	K3
CO5	Implement algorithm from operating systems concepts.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

List of Programs:

1. To detect Errors using Vertical Redundancy Check (VRC).
2. To detect Errors using Longitudinal Redundancy Check (LRC).
3. To detect Errors using Cyclic Redundancy Check (CRC).
4. Socket programming to implement Asynchronous Communication.
5. Socket programming to implement Isochronous Communication.
6. To implement Stop & Wait Protocol.
7. To implement Sliding Window Protocol.
8. To implement the Shortest Path Routing using Dijkstra algorithm.
9. Socket Programming to Perform file transfer from Server to the Client.
10. To implement Remote Procedure call under Client / Server Environment.
11. Code simulating PING and TRACEROUTE commands
12. Implementing of Subnetting.

Note: Any 8 practical's or more as per choice of the teacher and resources available.

RECOMMENDED READINGS

Course Faculty to share the material, E-sources, books and practical guide including instructions for this course.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Medium	High	Low	Medium	Low	High
CO2	Medium	Medium	High	Medium	Low	Low	High
CO3	High	Low	High	Medium	Medium	Medium	Medium
CO4	Medium	Medium	Medium	Low	Low	Low	High
CO5	High	Medium	High	Low	Medium	Low	High

Low = 10/35 = 28.57% Medium = 14/35 = 40.0% High = 11/35 = 42.85%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Low	High	Low	Medium
CO2	Medium	Low	High	Low	Medium
CO3	Low	High	Medium	Low	High
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 9/25 = 36.0% Medium = 8/25 = 32.0 % High = 7/25 = 28.00%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Skill Enhancement Foundation Course		BASICS OF PROGRAMMING- C++	2	0	0	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- Understand the process of programming
- Appreciate the functions of programming
- Examine the important concept in programming.
- Explain the primary concepts of C.
- Describe the primary concepts of C ++.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Write basic programme in C.	K1
CO2	Write basic programme in C++	K2
CO3	Explain the problems in programmes, if any.	K2 K6
CO4	Alter the programmes according to needs	K3 K5
CO5	Correct he programmes as per the requirements.	K4

K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Apply

Course Outline:

UNIT I: **Basics of C Programming**

C fundamentals Character set - Identifier and keywords - data types - constants - Variables - Declarations - Expressions - Statements - Arithmetic, Unary, Relational and logical, Assignment and Conditional Operators - Library functions. Data input output functions - Simple C programs - Flow of control - if, if-else, while, do-while, for loop, Nested control structures - Switch, break and continue, go to statements - Comma operator.

UNIT II: **Definitions & Functions**

Proto-types- Passing arguments - Recursions. Storage Classes - Automatic, External, Static, Register Variables- Multi-file programs. Arrays - Defining and Processing - Passing arrays to functions – multi-dimension arrays- Arrays and String. Structures - User defined data types- Passing structures to functions - Self-referential structures – Unions - Bit wise operations. Pointers- Declarations - Passing pointers to Functions - Operation in Pointers - Pointer and Arrays - Arrays of Pointers - Structures and Pointers - Files: Creating, Processing, Opening and Closing a data file.

UNIT III: **Introduction to C++**

Tokens, Keywords, Identifiers, Variables, Operators, Manipulators, Expressions and Control Structures in C++; Pointers - Functions in C++ Main Function Function Prototyping Parameters Passing in Functions - Values Return by Functions - Inline Functions - Friend and Virtual Functions

Classes and Objects; Constructors and Destructors; and Operator Overloading and Type Conversions - Type of Constructors - Function overloading. Inheritance : Single Inheritance Multilevel Inheritance Multiple Inheritance Hierarchical Inheritance Hybrid Inheritance. Pointers, Virtual Functions and Polymorphism; Managing Console I/O operations.

UNIT IV: **Working with Files**

Classes for File Stream Operations Opening and Closing a File End of File Deduction File Pointers Updating a File Error Handling during File Operations Command line Arguments. Data Structures: Definition of a Data structure primitive and composite Data Types, Asymptotic notations, Arrays, Operations on Arrays, Order.

UNIT V: **DATA STRUCTURES USING C++ (Lab practice)**

1. Implement PUSH, POP operations of stack using Arrays.
2. Implement PUSH, POP operations of stack using Pointers.
3. Implement add, delete operations of a queue using Arrays.
4. Implement add, delete operations of a queue using Pointers.
5. Conversion of infix to postfix using stack operations
6. Postfix Expression Evaluation.

7. Addition of two polynomials using Arrays and Pointers.
8. Creation, insertion, and deletion in doubly linked list.
9. Binary tree traversals (in-order, pre-order, and post-order) using linked list.
10.Depth First Search and Breadth first Search for Graphs using Recursion.

Note: Select Lab Work- Demonstration and practice only (No need for record), however during examinationquestions may give in internal and external assessment.

RECOMMENDED READINGS

Balaguruswamy E., 1995, Programming in ANSI C, TMH Publishing Company Ltd.
Kernighan B.W., and Ritchie D.M., 1988,The C Programming Language, 2nd Edition, PHI.
Schildt C. H., 2004, The Complete Reference, 4th Edition, TMH iii. Gottfried,B.S, 1996, Programming with C, Second Edition, TMH Pub. Co. Ltd., New Delhi.
Kanetkar Y., 1999, Let us C, BPB Pub., New Delhi.
Horowitz E., and Shani S.,1999, Fundamentals of Data Structures in C++, Galgotia Pub.
Robert Lafore, Object Oriented Programming in Microsoft C++, Galgotia publication.
Schildt H., C++,1998,The Complete Reference-1998-TMH Edition, 1998
Kruse C.L. Tondo R., and Leung B.,1997, Data Structures and Program design in C, PHI.
Cangsam, Auguenstein, Tenenbaum. Data Structures using C & C++,PHI
D. Samantha, 2005, Classic Data Structures, PHI,New Delhi.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	Medium	Medium	Medium	Medium	Medium	Low	High
CO2	Medium	High	High	Low	Low	Low	High
CO3	High	High	High	High	Medium	Medium	Medium
CO4	High	High	Medium	High	Low	Low	High
CO5	High	Low	High	Low	Medium	Low	High

Low = 10/35 = 28.57% Medium = 11/35 = 31.42% High = 14/35 = 40.0%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	Low	High	Low	Medium
CO2	High	Low`	High	Medium	Medium
CO3	High	High	Medium	Low	Low
CO4	High	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels:		**Low**	**Medium**	**High**	

Low = 9/25 = 36.0% Medium = 8/25 = 32.00% High = 8/25 = 32.0%

SEMESTER II

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 3		INTRODUCTION TO CYBER SECURITY	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- Identify Key concept and Terminology of Cyber Security.
- Examine the concept of privacy and its legal protections.
- Explain the primary concepts involving encryption.
- Describe the social implications of cyber security.
- Understand the risks and benefits of social networks.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Evaluate fundamental cyber security concepts, theories, and strategies as they apply to real world case studies.	K1
CO2	Understand the principles of cryptography- Encryption	K2
CO3	Explain technical and non-technical security solutions on different types of cyber systems.	K2 K6
CO4	Assess risks, vulnerabilities, and threats to sample cyber systems.	K3 K5
CO5	Identify attributes associated with cyber security professionals Understand of Indian criminal justice system and functioning of various institutions of the criminal justice system.	K4
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Apply		

Course Outline:

UNIT I: Basics of Cyber Security

Introduction to Cyber Security - Importance and challenges in Cyber Security- Cyberspace - Cyber threats - Cyber warfare - CIA Triad - Cyber Terrorism- Cyber Security of Critical Infrastructure - Cyber security -Organizational Implications.

UNIT II: Vulnerability in Cyber Space and Security

Types of Hackers- Hackers and Crackers - Cyber-Attacks and Vulnerabilities- Malware threats- Sniffing - Gaining Access - Hiding Files - Covering Tracks- Worms - Trojans- Viruses- Backdoors. Vulnerabilities- Overview, Vulnerabilities in Software, System administration, Threat Actors, Attacks, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications. Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

UNIT III: Ethical Hacking and Social Engineering

Ethical Hacking Concepts and Scopes- Threats and Attack Vectors - Information Assurance- Threat Modeling- Enterprise Information Security Architecture- Vulnerability Assessment and Penetration Testing- Types of Social Engineering- Insider Attack- Preventing Insider Threats- Social Engineering Targets and Defence Strategies.

UNIT IV: Cyber Forensics and Auditing

Introduction to Cyber Forensics- Computer Equipment and associated storage media- Role of forensics Investigator- Forensics Investigation Process - Collecting Network based Evidence- Writing Computer Forensics Reports - Auditing - Plan an audit against a set of audit criteria- Information Security Management System Management. Introduction to ISO 27001:2013.

UNIT V: Architecture of Cyberspace

DefiningCyberspaceandOverviewofComputer and Web-technology, Architectureofcyberspace,Complex Network Architectures, Internet,Worldwideweb,Advent of internet, Internet infrastructurefor data transfer and governance, Internetsociety,Regulationofcyberspace,Conceptof cyber security,Issuesandchallengesofcyber security.

RECOMMENDED READINGS

Donaldson, S., Siegel, S., Williams, C.K., and Aslam, A. (2015). "Enterprise Cyber security -How to Build a Successful Cyber defense Program against Advanced Threats", Apress, 1st Edition.

Franke, Don Cyber Security Basics: Protect your organization ... (Paperback)

Nina Godbole, Sumit Belapure, (2011). "Cyber Security", Willey.

Roger Grimes, "Hacking the Hacker", Wiley, 1st Edition, 2017.

Yuri Diogenes and Erdal Ozkaya (2018). Cyber security– Attack and Defense Strategies: 2nd Edition Paperback.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	Medium	Medium	Medium	Medium	Medium	Low	High
CO2	Medium	High	High	Low	Low	Low	High
CO3	High	High	High	High	Medium	Medium	Medium
CO4	High	High	Medium	High	Low	Low	High
CO5	High	Low	High	Low	Medium	Low	High

Low = 10/35 = 28.57% Medium = 11/35 = 31.42% High = 14/35 = 40.0%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	Low	High	Low	Medium
CO2	High	Low`	High	Medium	Medium
CO3	High	High	Medium	Low	Low
CO4	High	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels:		**Low**	**Medium**	**High**	

Low = 9/25 = 36.0% Medium = 8/25 = 32.00% High = 8/25 = 32.0%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 4		ADVANCED NETWORKING AND COMMUNICATION PROTOCOLS	4	0	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To prepare students with basic networking concept.
- To understand process of data communication using protocols and standards
- To learn various topologies and applications of network.
- To understand the concept of network layer, transport layer and application layer

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Appreciate forms of computer networks	K1
CO2	Understand the concept of OSI Reference Model and TCP/IP.	K2
CO3	Knowledge of the components of the Network.	K2 K6
CO4	Understand top-down approach of data communication	K3

	from one user to another user	
CO5	To detect the IP address and route.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Apply		

Course Outline:

UNIT I: SessionLayers

Introduction to the Session Layer and its functions, including establishing, managing, and terminating sessions between applications. Overview of the Session Layer protocols, NetBIOS, RPC, and ZIP, and their features and uses. Overview of the Session Layer services, dialog control, token management, and synchronization. Introduction to the

UNIT II: Presentation and Application Layers

Presentation Layer and its functions, including data representation, data encryption, and data compression. Overview of the Presentation Layer protocols, including JPEG, MPEG, and ASCII, and their features and uses. Overview of the Presentation Layer services, including data conversion, data compression, and data encryption. Introduction to application layer Protocol: Domain Name System (DNS), WWW– Architecture, HTTP Transaction.

UNIT III: Protocols in Network

Introduction to IPv4 Addressing and Subnetting- Subnet Masks and Network Prefix- Address Classes (A, B, C, D, E) - Private IP Addresses and NAT - Variable Length Subnet Mask (VLSM) and CIDR Notation - Subnet Design and Address Allocation - Subnetting and Routing - Broadcast and Multicast Addresses - IPv6 Addressing and Subnetting.

Network protocol: HTTP, FTP, PPP, SMTP, TCP/IP, POP3, HTTPS, TELNET, VoIP.

UNIT IV: Protocols and Services

Communication protocols- Address Resolution Protocol (ARP)- Reverse Address Resolution Protocol (RARP)- Internet Control Message Protocol (ICMP)- Internet Protocol (IP)- Transmission Control Protocol (TCP)- User Datagram Protocol (UDP)- American Standard Code for Information Interchange (ASCII)- Hypertext Transfer Protocol (HTTP)- File Transfer Protocol (FTP)- Simple Mail Transfer Protocol (SMTP)- Telnet- Trivial File Transfer Protocol (TFTP)- Post Office Protocol version 3 (POP3) - Internet Message Access Protocol (IMAP)- Simple Network Management Protocol (SNMP)- Domain Name System (DNS)- DNS Flags- Dynamic Host Configuration Protocol (DHCP).

Virtual LANs- Access links and Trunk links- Switchport modes- Vlan Trunking- Server, Client and Transparent modes- VTP Domain- Configuration Revision numbers- Inter Vlan Communications- Broadcast domain- Collision Domain

UNIT V: Principles of Web Services
WWW, Hyper Text Markup Language (HTML), Extensible Markup Language (XML), domain names. Web services- URL, website, web browser, web servers, web hosting.

RECOMMENDED READINGS

Donaldson, S., Siegel, S., Williams, C.K., Aslam, A., "Enterprise Cyber security -How to Build a Successful Cyber defense Program against Advanced Threats", Apress, 1st Edition, 2015.
Behrouz Forouzan,Data Communications and Networking, Fifth Edition, ISBN 978-0-07-337622-6 McGraw Hill.
Andrew S. Tanenbaum,Computer Networks, Fifth Edition, ISBN-13: 978-0-13-212695-3, Pearson
Nina Godbole, Sumit Belapure, "Cyber Security", Willey, 2011.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	High	High	Medium	Medium	Low	High	High
CO3	Medium	Medium	High	Low	Medium	Medium	Medium
CO4	Low	High	Medium	Low	Low	Low	High
CO5	Medium	Low	High	Low	Medium	Low	High

Low = 12/35 = 34.28% Medium = 11/35 = 31.42% High = 12/35 = 34.28%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	Medium	High
CO2	High	Medium	High	Low	High
CO3	Medium	Low	Medium	Low	High
CO4	Medium	Medium	Low	High	Low
CO5	Low	Medium	Low	High	Medium
Correlation Levels:	Low	Medium	High		

Low = 9/25 = 36.0% Medium = 7/25 = 28.00% High = 9/25 = 36.0%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Elective 2		FORMS OF CYBER CRIME	3	0	0	3

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- This course will expose the introductory concepts of cyber crimes
- The impact of cybercrimes and its counter measures
- The contemporary challenges in cyberspace.
- List the preventive and precautious measure.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Appreciate the forms of cybercrimes	K1
CO2	Critically identify the counter measures for cybercrimes	K2
CO3	Identify modus operandi of the cyber criminals	K2
CO4	Profile the cybercriminals-based on types, crimes, locations and etc.	K3 K6
CO5	Understand the impact of cybercrime in real space.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Cyber Crimes- Overview**

Introduction– History and Development– Definition, Nature and Extent of Cyber Crimes in India and other countries- Classification of Cyber Crimes– Trends in Cyber Crimes across the world.

UNIT II: **Forms of Cyber Crimes and Cyber Frauds**

Hacking, cracking, DoS– viruses, works, bombs, logical bombs, time bombs, email bombing, data diddling, salami attacks, phishing, steganography, cyber stalking, spoofing, pornography, defamation, computer vandalism, cyber terrorism, cyber warfare, crimes in social media, malwares, adware, scareware, ransomware, social engineering, credit card frauds & financial frauds, telecom frauds. Cloud based crimes– understanding fraudulent behaviour, fraud triangle, fraud detection techniques, Intellectual Property Rights and Violation of Intellectual Property rights, Ecommerce Frauds and other forms.

UNIT III: **Modus Operandi of various Cybercrimes and Frauds**

Definition of various types of cyber frauds – Modus Operandi - Fraud triangle – fraud detection techniques including data mining and statistical references - countermeasures.

UNIT IV: **Profile of Cyber criminals**

Cyber Crime Psychology–Theories dealing with cyber criminals.

UNIT V: Impact of Cybercrimes
Impact on individual, property and to the corporates / companies, to government and the nation.

RECOMMENDED READINGS

Albert J. Marcellaa and Robert S. Greenfiled (Ed) (2002) Cyber Forensics, A Field Manual for collecting, examining and preserving evidence of computer crimes, Auerbach publications.
Derek Atkins et. al., (1997). Internet Security: Professional Reference, Techmedia, Daryaganj, New Delhi
IT Act 2000.
Seymour Goodman and Abraham Soafer (ed.) (2002) The Transnational dimensions of cybercrime, Hoover Institution Press Washington.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	High	Low	High	Low	Medium	Low	High	Medium
CO2	Medium	High	High	Medium	Low	Low	High	Medium
CO3	High	Medium	High	Low	Medium	Medium	Medium	Medium
CO4	Medium	High	Medium	Low	Low	Low	High	Medium
CO5	High	Low	High	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High								

Low = 8/35 = 22.85% Medium = 11/35 = 31.42% High = 15/35 = 42.85%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Low	High	Low	Medium
CO2	High	Low	High	Low	Medium
CO3	Medium	High	Medium	Medium	Medium
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 7/25 = 28.00% Medium = 9/25 = 36.0% High = 9/25 = 36.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
SEC 2 NME		ADVANCE PROGRAMMING-PYTHON	1	0	1	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To learn the systematic way of solving problem
- To understand the different methods of programming in organizing large amount of data
- To efficiently implement the different data structures
- To efficiently implement solutions for specific problems.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Enhance the problem-solving computational skill	K1
CO2	Use well-organized data structures in solving various problems.	K2
CO3	Differentiated the usage of various structures in the problem solution.	K2 K6
CO4	Implement the algorithms to solved problems using appropriate data structures	K3
CO5	Apply python on different data structure.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Apply		

Course Outline:

UNIT I **Introduction to Python**

Define Python - Advantages of Python - History - Features - Uses - Variable and Data Types - Python Interpreter - Identifiers and keywords - Literals – Operators (Arithmetic operator, Relational operator, Logical or Boolean operator, Assignment, Operator, Ternary operator, Bit wise operator) - Defining Functions.

UNIT II **Objects and Data Structure**

Structure of a Python Program - Elements of Python Input and Output Statements - Control statements (Branching, Looping, Conditional Statement) - Exit function, Difference between break, continue and pass.) - Default arguments - Multiple assignment - while statement - for statement - A find function - Looping and counting.

UNIT III **Functions, Strings and Lists**

Strings and Lists – String Manipulation - Accessing Strings - Basic Operations with String slices - Function and Methods - Recursion, Stack diagrams for recursive functions. List - Working with list - List values - Accessing elements - List membership - List operations - List deletion - Cloning lists - Nested lists - Using Python as calculator - Python shell - Indentation and Atoms.

UNIT IV Object Oriented Programming

Introduction to Classes - Objects and Methods - Standard Libraries - Tuples - Accessing tuples - Exception handling - Iteration - Conditional execution - Return statement and Operations – Opening and closing file - Reading and writing files - Dictionaries - Working with dictionaries - Exception Handling - Except clause - Try ?Finally clause.

UNIT V CASE STUDIES

Basic Syntax - Setting up path - Working with Python – CGI – Networking – Multithreading - Generators and closures - Importing module - Math module - Packages - Composition – Sample Programs- Analyze Sales Outcome in Business - Automate the School Details to Analyze Performance.

LIST OF PROGRAMS: For practices

1. Compute the GCD of two numbers.
2. Find the square root of a number (Newton's method)
3. Exponentiation (power of a number)
4. Find the maximum of a list of numbers
5. Linear search and Binary search
6. Selection sort, Insertion sort
7. First n prime numbers
8. Multiply matrices
9. Programs that take command line arguments (word count)
10. Find the most frequent words in a text read from a file
11. Simulate elliptical orbits and bouncing ball using in Pygame

RECOMMENDED READINGS

Data Structure and Algorithmic Thinking with Python: Data Structure and Algorithmic Puzzles by Karumanchi, Narasimha

Data Structures using C and C++--YedidyahLangsam, Moshe J. Augenstein, Aaron M. Tenenbaum

Data Structures using Python 2021 Edition by Dr Shriram K. Vasudevan

Fundamentals of Computer Algorithms--Horowitz, Sahani--Computer Science Press

Fundamentals of Data Structures--Horowitz, Sahani—Galgotia

Hands-On Data Structures and Algorithms with Python_second Edition by Benjamin Baka Dr Basant Agarwal Dr. Basant Agarwal

Introduction to Algorithms—Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein--MIT Press

Introduction to Data Structures using C, Ashok Kamthane, Pearson Education

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	High	High
CO2	Medium	High	High	Medium	Low	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	Low	High

CO5	High	Low	High	Low	Medium	Low	High

Low = 9/35 = 25.71% Medium = 10/35 = 28.57% High = 16/35 = 45.71%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	High	High
CO2	High	Low	High	High	High
CO3	Medium	High	Medium	Low	Low
CO4	Medium	High	High	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 5/25 = 20.0% Medium = 7/25 = 28.00% High = 13/25 = 52%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
SEC 3		SQL AND INTERNET SECURITY LAB- Practical's	0	0	2	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To present the concepts and techniques relating to query processing
- To acquire a knowledge of procedures and functions supported by SQL and python.
- To make use of PL/SQL and python language component, variables and data types.
- To understand the scope of the Block, Nested blocks and Labels.
- The student learns to work with various Redundancy Check Algorithms, Sliding Window Protocol, Routing Algorithm, Subnetting Procedures.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcomes	Cognitive Levels
CO1	Design and implement the database schema for a general problem domain	K1 K6
CO2	Normalize the database.	K2
CO3	Populate and query a database using SQL- DDL / DML commands.	K2
CO4	Programming PL/SQL and python including stored procedures, stored functions, cursors, packages.	K3
CO5	Exploring the ideas on SQL internet security.	K4 K5
K1: Remember K2: Understand K3: Apply K4: Analyze K5: Evaluate K6: Create		

Course Outline:

List of Programs:

1. Creation of database and use SQL queries to retrieve information from the database.
2. Performing insert, delete, modify, alter, update operations based on conditions using SQL
3. Study of PL/SQL block
4. Write a PL/SQL block to satisfy some conditions after accepting input from the user.
5. Write a PL/SQL block that handles all types of exceptions.
6. Perform packet sniffing and spoofing using Python.
7. Develop a Python script that can scan a network for open ports and identify potential vulnerabilities.
8. Develop a Python script that can capture and analyse network traffic in real-time, using tools like Scapy and Wireshark.
9. To bypass firewall using VPN
10. Authentication and access control, password and attack methods
11. Firewall, experimenting security tools and software's.
12. Analyse the security vulnerabilities of E-commerce services.
13. Analyse the security vulnerabilities of any email application.

Note: Any 8 practical's or more as per choice of the teacher and resources available.

RECOMMENDED READINGS

Course Faculty to share the material, E-sources, books and practical guide including instructions for this course.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	Low	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	High	High
CO5	High	Low	High	High	Medium	High	High
Correlation Levels:	**Low**	**Medium**	**High**				

Low = 8/35 = 22.85% Medium = 10/35 = 28.57% High = 17/35 = 48.57%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	Low	High	Low	Medium
CO2	High	Low	High	Low	Medium
CO3	Medium	High	Medium	High	High
CO4	Medium	Low	High	High	High
CO5	Low	Medium	High	High	Medium
Correlation Levels:	**Low**	**Medium**	**High**		

Low = 6/25 = 24.14% Medium = 7/25 = 28.00% High = 9/25 = 44.0 %

SEMESTER III

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core *5*		MOBILE AND WEB APPLICATION SECURITY	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To address the growing threat to mobile devices & web applications, networks and services delivered over the mobile & web application infrastructure.
- To provide an introduction to mobile and web application security.
- To explore the unique challenges facing mobile and web security.
- This course also covers the security of mobile and web application services (WAS), such as VoIP, text messaging, WAP and mobile HTML.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Detect Mobile and Web application security threats and classify the threats and develop a Security model to prevent, detect and recover from the attacks.	K1
CO2	Familiar with Mobile and web app security designs using	K2

	available secure solutions and advanced security and malware issues.	
CO3	Develop the skills to overcome the security threats	K2 K6
CO4	Enable web applications to maintain high performance in the face of numerous users and attackers.	K3
CO5	Manage the scalability of the web application, and provide prominent service to large numbers of simultaneous users	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: Introduction to Mobile Security
Introduction to Mobile Security– Building Blocks– Basic security and cryptographic techniques. Security of GSM Networks– Security of UMTS Networks- LTE Security- WiFi and Bluetooth Security- SIM/UICC Security

UNIT II: Mobile Security Implementation
Mobile Malware and App Security- Android Security Model– IOS Security Model- Security Model of the Windows Phone– SMS/MMS, Mobile Geo location and Mobile Web Security-Security of Mobile. VoIP Communications– Emerging Trends in Mobile Security

UNIT III: Security Fundamentals
Introduction to WWW security-Input Validation- Attack surface Reduction-Classifying and prioritizing threats- Hacking Methodology. Security Policies relating to mobile devices- Operation guidelines for implementing mobile devices and security policies

UNIT IV: Web Application Security Principles
Authentication-Authorization- Browser Security Principles- Common Web Application Security Threats: Injection attacks, broken authentication, Cross site Scripting- Cross site Request Forgery, insecure direct object references, security misconfigurations, missing function level access control.

UNIT: Case Studies
Mobile Application Protection Suite- Internet and Service (MAPS): Find & Fix Security issues– Evaluate smart phone security issues- Web Applications Security and Vulnerability Analysis Financial Web Applications Security Audit– Securing Web Applications.

RECOMMENDED READINGS

Bryan Sullivan,Vincent Liu, "Web Application Security-A Beginner's Guide", Mc Graw Hill, 1st edition, 2011.
Himanshu Dviwedi, Chris Clark and David Thiel, "Mobile Application Security", 1st Edition, 2010.

Michael Cross, "Developer's Guide to Web Application Security", Syngress Publications, 1st edition, 2007.
Noureddine Boudriga, "Security of Mobile Communications", 2009.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	Low	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	High	High
CO5	High	Low	High	High	Medium	High	High
Correlation Levels:		**Low**	**Medium**	**High**			

Low = 8/35 = 22.85% Medium = 10/35 = 28.57% High = 17/35 = 48.57%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	Low	High	Low	Medium
CO2	High	Low	High	High	Medium
CO3	Medium	High	Medium	High	Low
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	High
Correlation Levels:		**Low**	**Medium**	**High**	

Low = 9/25 = 36.0% Medium = 6/25 = 28.00% High = 10/25 = 36.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 6		**FUNDAMENTALS OF CRIMINOLOGY AND CYBER CRIMINOLOGY**	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- *This course will expose the introductory concepts of crime and criminology along with emphasizes on cyber criminology.*
- *This course will introduce various crimes to students.*
- *This paper enables students to understand the functioning of criminal justice system in India.*
- *The fundamentals of criminology and role cyber criminology in contemporary times.*

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels

CO1	Introduction to criminology its origin and the interdisciplinary nature of Criminology	K1
CO2	Critically identify the contributions cyber criminology in understating the cybercrimes.	K2
CO3	Understand of Indian criminal justice system and functioning of various institutions of the criminal justice system.	K2
CO4	Understanding different typologies of crime including cybercrimes against human body, property and types of offenders and impact.	K3
CO5	Exploring modern day crime and influence of technology in committing crime in cyber space	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate		

Course Outline:

Unit I: **Principles and Concepts of Crime**
Crime, Tort, Misdemeanor, - Conventional crimes vs Cyber Crimes. Crimes in India: Statistics, Crime Clock, Crime rate, National Crime records Bureau[1], State Crime records Bureau, and District crime records bureau; Crime patterns and Trends in India[2] (latest trends should be introduced).

Unit II: Criminology and Cyber Criminology
Criminology, Crime-Definitions[3]; historical perspectives; nature, origin and scope. Schools of Criminology. Crime Typology Introduction to crimes against persons and crimes against property[4]; Adult and Juvenile – Habitual offenders, Professional offenders, and violent offenders. Cyber Space, Cyber Crime, Cyber Criminology, Information Security, Penetration Testing, Incident Response, GRC, etc.

Unit III: Cyber Crime– Sociological and Criminological Perspectives
Causes of Cyber Crimes - Criminological Theories and Cyber Crime – Routine Activity Theory, Social Learning Theory, Differential Association Theory, Differential Opportunity Theory, Media and Crime and latest theories and other related theories.

Unit IV:Criminal Justice System
Structure of Criminal Justice System in India[5]; Roles of legislature, police, judiciary and prison system in Criminal Justice; Cooperation and coordination among the various sub

[1] Practical Exposure
[2] Seminar
[3] Discussion
[4] Assignment
[5] Jig saw learning

systems of criminal justice system[6]. Cognizable and non-cognizable offences, bailable and non-bailable offences – arrest, search, seizure – Interrogation of suspects and witnesses – charge sheet – Cybercrime cells – structure & investigation of cybercrime cases.

Unit V:Contemporary Forms of Crimes and Cybercrimes

White Collar Crimes, Economic Offences, Organized Crimes, Cybercrimes, Terrorism, Cyber Warfare, Cyber Bullying & Stalking, Online Sextortion, Sexting, and other contemporary forms of crimes.

RECOMMENDED READINGS

Ahmed Siddique, (1993), *Criminology, Problems and Perspectives*, III Edn. Eastern Book House, Lucknow.

Allen, Friday, Roebuck and Sagarin, (1981), *Crime and Punishment: An introduction to Criminology.* The Free press. New York.

Brenda S. Griffin and Charles T.Griffin, (1978), *Juvenile Delinquency in perspective, Harper and Row*, New York

Brendan Maguire & Polly F. Radosh, (1999), *Introduction to Criminology*, Wadsworth Publishing Company, Boston, U.S.A.

Chockalingam, K. (1997), *'Kuttraviyal'* (Criminology) in Tamil, Parvathi Publications, Chennai.

Crime in India (Latest edition). National Crime Record Bureau, Ministry of Home Affairs, New Delhi.

Edwin H. Sutherland and Donald R. Cressey (1974), *Principles of Criminology*, Lippincott, Philadelphia.

George Vold and Thomas J. Bernard, (1986), *Theoretical Criminology*, Oxford University Press, New York

Harries, K., (1999) *Mapping Crime – principle and practice*, Crime Mapping Research Center, National Institute of Justice, U.S Department of Justice, Washington, DC

Harry Elmer Barnes and Negley K. Teeters, (1966), *New Horizons in Criminology, Prentice Hall*, New Delhi.

John E.Conklin, J.E., (1981), *Criminology*, Macmillan, London.

Paranjepe, N.V., (2002). *Criminology and Penology*, Central Law Publications, Allahabad.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Medium	Low	High
CO5	High	Medium	High	High	Medium	High	High

[6] Seminar

Low = 12/35 = 34.28% Medium = 7/35 = 20.01% High = 16/35 = 45.71%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	High	High	Low	Medium
CO2	High	High	High	Low	Medium
CO3	Medium	High	Medium	Low	Low
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 7/25 = 28.0% Medium = 7/25 = 28.00% High = 11/25 = 44.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Elective 3		DATA PRIVACY - TECHNOLOGY AND LAW	3	0	0	3

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To understand the legal and ethical issues surrounding data privacy in the digital age.
- To identify and evaluate the technical measures used to protect data privacy in various contexts such as online communications, social media, e-commerce, and data storage.
- To explore the impact of emerging technologies such as artificial intelligence, machine learning, and the Internet of Things on personal data privacy.
- To examine the global and local regulations and standards governing data privacy and their implications for businesses and individuals.
- To develop critical thinking and analytical skills in assessing the data privacy risks and benefits associated with different technology- enabled activities.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Understand about data privacy threats and apply data privacy principles to protect personal data.	K2
CO2	Evaluate legal frameworks for privacy protection, including	K4, K5

	international and national laws related to data privacy.	
CO3	Assess ethical considerations surrounding data privacy, including surveillance, big data, and artificial intelligence.	K4, K5
CO4	Critically evaluate the impact of data privacy on business, including marketing, e-commerce, cloud computing, and social media.	K5
CO5	Develop strategies for safeguarding data privacy in various contexts, including the workplace, social networks, and research.	K6
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: Introduction to DataPrivacy and Data Protection
Concept of Privacy and Data Protection – The concept of data privacy in Indian and global legal systems - Importance of Privacy and Data Protection – Evolution of Data Privacy and Data Protection – Data Privacy and Protection Laws - Comparison of data privacy laws in India and other countries.

UNIT II: Technical Aspects of Data Privacy
Data Privacy Threats– Data Privacy Principles– Data Privacy Enhancing Technologies– Encryption– Authentication– Anonymity – Pseudonymity– Data Privacy and Social Networks.

UNIT III: Ethical Aspects of Data Privacy
Ethical Issues Surrounding Data Privacy– Data Privacy and Surveillance– Data Privacy and Big Data– Data Privacy and Artificial Intelligence– Ethics of Data Privacy in Research.

UNIT IV: Data Privacy and Business
Data Privacy and Marketing– Data Privacy and E-Commerce– Data Privacy and Cloud Computing– Data Privacy and Social Media– Data Privacy in the Workplace.

UNIT V: Legal Aspects of Data Privacy
Fundamental Concepts of Law Related to Data Privacy– Legal Frameworks for Data Privacy Protection – International Law and Privacy – Regional and National Data Privacy Laws– Privacy and Cybercrime. IT Act, 2000 and data privacy.

RECOMMENDED READINGS

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World by Bruce Schneier
Privacy Engineering: A Dataflow and Ontological Approach by Martin Degeling, Sebastian Pape, and Hannes Federrath
Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family by Theresa M. Payton and Theodore Claypoole

Privacy Law: Cases and Materials by Daniel J. Solove, Paul M. Schwartz, and Daniel J. Weitzner
The Right to Privacy by Samuel D. Warren and Louis D. Brandeis.
The Information Technology Act, 2000 (Amended 2008)

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	Low	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	High	High
CO5	High	Low	High	High	Medium	High	High
Correlation Levels:	**Low**	**Medium**	**High**				

Low = 8/35 = 22.85% Medium = 10/35 = 28.57% High = 17/35 = 48.57%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Low	High	Low	Medium
CO2	High	Low	High	High	Medium
CO3	Medium	High	Medium	High	Low
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	High
Correlation Levels:	**Low**	**Medium**	**High**		

Low = 9/25 = 36.0% Medium = 6/25 = 28.00% High = 10/25 = 36.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
SEC 4		FUNDAMENTALS OF CLOUD COMPUTING	3	0	0	1

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To provide students with the fundamentals and essentials of Cloud Computing.
- To adopt Cloud Computing services and tools in their real-life scenarios.
- To enable students exploring some important cloud computing driven commercial systems and applications.
- To design cloud applications using Amazon Web Services (AWS).
- To appreciate the emergence of cloud as the next generation computing paradigm

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO	Course Outcome	Cognitive

No.		Levels
CO1	Describe the main concepts, key technologies, strengths, and limitations of cloud computing and the possible applications for state-of-the-art cloud computing	K1
CO2	Explain the architecture and infrastructure of cloud computing, including SaaS, PaaS, IaaS, public cloud, private cloud, hybrid cloud, etc.	K2
CO3	Identify problems, and explain, analyze, and evaluate various cloud computing solutions.	K2
CO4	Choose the appropriate technologies, algorithms, and approaches for the related issues.	K3
CO5	Discover new ideas and innovations in cloud computing.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate		

Course Outline:

UNIT I: INTRODUCTION

Computing Paradigms – Motivation for Cloud Computing – Defining Cloud Computing – Principles of Cloud Computing – Cloud Ecosystem – Requirements for Cloud Services – Cloud Architecture – Anatomy of the Cloud – Network Connectivity in Cloud Computing– Applications on the Cloud – Managing the Cloud – Migrating Application to Cloud.

UNIT II: CLOUD MODELS

Cloud Deployment Models – Introduction – Private Cloud – Public Cloud – Community Cloud – Hybrid Cloud - Cloud Service Models – Introduction – Infrastructure as a Service – Platform as a Service – Software as a Service – Other Cloud Service Models.

UNIT III: TECHNOLOGIES DRIVERS FOR CLOUD COMPUTING

SOA and Cloud – Virtualization – Approaches in Virtualization – Hypervisor and its role - Types of Virtualizations – Multicore Technology - Memory and Storage Technologies – Networking Technologies - Programming Models for Cloud – MapReduce.

UNIT IV: CLOUD SERVICE PROVIDERS

EMC – Google – Amazon Web Services – Microsoft – IBM – SAP Labs – Salesforce – Rackspace – Vmware – Manjrasoft – Open-Source Tools for IaaS – Open-Source Tools for PaaS - Open-Source Tools for SaaS - Open Source Tools for Research - Distributed Computing Tools.

UNIT V: ADVANCED CONCEPTS IN CLOUD COMPUTING

Security Aspects – Data Security – Virtualization Security – Network Security – Audit and Compliance - Advanced Cloud – Intercloud – Cloud Management - Mobile Cloud – Media Cloud - Cloud Governance – Green Cloud – Cloud Analytics – High Performance Computing.

RECOMMENDED READINGS

K. Chandrasekaran, "Essentials of Cloud Computing", Taylor and Francis Group, CRC Press, 2015.
RajkumarBuyya, Christian Vecchiola, S. ThamaraiSelvi, "Mastering Cloud Computing", Tata Mcgraw Hill, 2013.
Rittinghouse, John W., and James F. Ransome, "Cloud Computing: Implementation, Management and Security", CRC Press, 2017.
Toby Velte, Anthony Velte, Robert Elsenpeter, "Cloud Computing - A Practical Approach", Tata Mcgraw Hill, 2009.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	High	Medium	Low	High
CO2	Medium	High	High	High	Low	Low	High
CO3	High	Medium	High	Medium	Medium	Medium	Medium
CO4	Medium	High	Medium	Low	Low	Low	High
CO5	High	Low	High	Low	Medium	Low	High

Low = 10/35 = 28.54% Medium = 10/35 = 28.54% High = 15/35 = 42.85%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Low	Low	Low	Medium
CO2	High	High	Medium	Low	Medium
CO3	Medium	High	Low	Low	Low
CO4	Medium	Low	Low	High	Medium
CO5	High	Medium	Low	High	Medium
Correlation Levels:	Low	Medium	High		

Low = 10/25 = 40.0% Medium = 8/25 = 32.00% High = 7/25 = 28.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
SEC 5		ADVANCED INTERNET SECURITY TOOLS LAB - Practical's	0	0	2	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- Cyber security Plan- cyber security policy, cyber crises management plan, Business continuity, Risk assessment.
- To understand the types of security controls and their goals, Cyber security audit and compliance
- National cyber security policy and strategy.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Prepare password policy for computer and mobile device.	K1
CO2	List out security controls for computer.	K2
CO3	implement technical security controls in the personal computer.	K2
CO4	Log into computer system as an administrator	K3
CO5	Check the security policies in the system.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate		

Course Outline:

Practical

1. Prepare password policy for computer and mobile device.
2. List out security controls for computer and implement technical security controls in the personal computer.
3. List out security controls for mobile phone and implement technical security controls in the personal mobile phone.
4. Log into computer system as an administrator and check the security policies in the system.
5. Perform packet sniffing using wire shark tool.
6. Perform port scanning using Nmap tool.
7. Perform Web Server finger printing using Nmap tool.
8. Setup a honey pot and monitor the honey pot on network using KF sensor tool or any other equivalent tool.
9. Model Saftey Audit
10. Model Risk Assessment
11. Qualis Guard
12. Nessus tool.

Note: Any 8 practical's or more as per choice of the teacher and resources available.

RECOMMENDED READINGS

Auditing IT Infrastructures for Compliance By Martin Weiss, Michael G. Solomon, 2nd Edition, Jones Bartlett Learning.
Cyber Crime Impact in the New Millennium, by R. C Mishra, Auther Press. Edition 2010.
Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)

Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.
Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
Fundamentals of Network Security by E. Maiwald, McGraw Hill.
Information Security Governance, Guidance for Information Security Managers by
Information Warfare and Security by Dorothy F. Denning, Addison Wesley.
Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.
Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson, 13th November, 2001)
W. KragBrothy, 1st Edition, Wiley Publication.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	Low	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	Low	Low	Low	High
CO5	High	Low	High	Low	Medium	Low	High

Low = 10/35 = 28.57% Medium = 10/35 = 28.57% High = 15/35 = 37.14%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	Low	High	Low	High
CO2	High	Low	High	Low	High
CO3	High	High	Medium	Low	Medium
CO4	Low	Low	Low	High	Low
CO5	Medium	Medium	Low	Medium	Medium
Correlation Levels:	**Low**	**Medium**	**High**		

Low = 10/25 = 40.0% Medium = 6/25 = 24.0% High = 9/25 = 36.0 %

SEMESTER IV

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 7		INTRUSION DETECTION AND PREVENTION SYSTEM	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To prepare students to know regarding the common threats faced today and the necessity of intrusion detection systems for securing the systems.
- To understand the essential concepts of intrusion detection and prevention. Be familiar with principles and techniques used in intrusion detection and taxonomy of intrusion detection systems.
- Acquiring knowledge on the state of art of the research in intrusion detection and prevention systems. Enable students to do independent research and be able to model and implement intrusion detection systems.

Course Outcomes (COs):

At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Understand the physical location, the operational characteristics and the various functions performed by the intrusion detection and prevention system	K1
CO2	The concepts of prior strong experience in operating system and prior hands-on experience.	K2 K4
CO3	Describe how components in different layers inter-operate in the intrusion detection and prevention system	K2
CO4	Understand the current and effective architecture to deal with network security threats.	K3 K6
CO5	Apply intrusion detection alerts and logs to distinguish attack by using SNORT tool.	K3 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Introduction to Intrusion Detection**

Understanding Intrusion Detection –Intrusion detection and prevention basics– IDS and IPS. Analysis schemes, Attacks, Detection approaches– Misuse detection– anamoly detection– specification-based detection– hybrid detection.

UNIT II: **Theoretical Foundations of Detection**

Taxonomy of anomaly detection system–fuzzy logic– Bayes theory– Artificial Neural networks- Support vector machine– Evolutionary computation– Association rules– Clustering. Confirgure Network- Identify the Malware-fiunction.

UNIT III: **Architecture and Implementation**

Centralized – Distributed –Cooperative Intrusion Detection -Tiered architecture.

UNIT IV: **Justifying Intrusion Detection**

Intrusion detection in security –Threat Briefing –Quantifying risk –Return on Investment (ROI)

UNIT V: **Case Studies**

Tool Selection and Acquisition Process - Bro Intrusion Detection– Prelude Intrusion Detection- Cisco Security IDS- Snorts Intrusion Detection– NFR security Legal Issues

and Organizations Standards: Law Enforcement / Criminal Prosecutions– Standard of Due Care– Evidentiary Issues, Organizations and Standardizations.

RECOMMENDED READINGS

Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010.
Ankit Fadia and Mnu Zacharia, "Intrusion Alert", Vikas Publishing house Pvt., Ltd, 2007.
Carl Enrolf, Eugene Schultz, Jim Mellander, "Intrusion detection and Prevention", McGraw Hill, 2004.
Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006.
Paul E. Proctor, "The Practical Intrusion Detection Handbook ", Prentice Hall, 2001.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	High	High
CO2	Medium	High	High	Medium	Low	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	High	High
CO5	High	Low	High	High	Medium	High	High

Low = 6/35 = 17.14% Medium = 10/35 = 28.57% High = 19/35 = 54.28%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	High	High	High	High
CO2	High	High	High	High	High
CO3	Medium	High	Medium	Low	Low
CO4	High	Low	High	High	Medium
CO5	High	Medium	Low	High	Medium
Correlation Levels:	Low	Medium	High		

Low = 4/25 = 16.0% Medium = 5/25 = 20.0% High = 16/25 = 64%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 8		DATA STORAGE	4	0	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To comprehend about the different types of data.
- To acquire knowledge about networks, databases and the Internet.
- To explain the design of a data center and storage requirements

- To discuss the various types of storage and their properties
- To explain physical and virtualization of storage
- To explain the backup, archiving with regard to recovery and business continuity

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Understand data storage in the computer.	K1
CO2	Explain the Optical, Semiconductor media and techniques for read/write operations	K2 K6
CO3	Overview of Virtualization Technologies, Storage Area Network	K2
CO4	Discuss the Networked Attached Storage and Networking issues	K3 K6
CO5	Classify the applications as per their requirements and select relevant SAN solutions.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT-1: Fundamentals of Storage

Introduction to Storage: Overview of data storage and its importance in the digital world. Volatile Storage: Introduction to volatile storage, Random Access Memory (RAM) and Cache memory, and their characteristics. Non-Volatile Storage: Introduction to non-volatile storage, hard disk drives, solid-state drives, and optical storage devices, and their characteristics- Types of Backups: Introduction to types of backups, full backups, incremental backups, differential backups, and mirror backups - Backup Strategies: Introduction to backup strategies, local backups, offsite backups, and cloud backups, and their advantages and disadvantages - Backup Tools: Overview of backup tools, native operating system backup tools, third-party backup software, and backup appliances.

UNIT-II: **Storage Media and Technologies its Usage and Access**

Magnetic, Optical and Semiconductor Media, Techniques for read/write Operations, Issues and Limitations. Data center: Introduction, Site Selection and Environmental Considerations, Hierarchical or Layered Architecture, Architect Roles, Goals and Skills, Architecture Precursors, Positioning in the Memory Hierarchy, Hardware and Software Design for Access, Performance issues.

UNIT-III: **Large Storages**

Hard Disks, Networked Attached Storage, Scalability issues, Networking issues. Storage Virtualization: Forms, Configurations and Challenges, Types of Storage Virtualization: Block-level and File-Level.

UNIT-IV: **Storage Architecture**

Storage Partitioning, Storage System Design, Caching, Legacy Systems. Information Security, Critical security attributes for information systems, Storage security domains, Analyze the common threats in, each domain.

UNIT-V: Storage Area Networks

Hardware and Software Components, Storage Clusters/Grids. Storage QoS– Performance, Reliability and Security issues. Evolution of networked storage, Architecture, components, and topologies of FC-SAN, NAS, and IP-SAN, Benefits of the different networked storage options, need for long-term archiving solutions and describe how CAS fulfil the need, Appropriateness of the different networked storage options for different application environments

RECOMMENDED READINGS

Catell, R.G.G., Barry, D.K., Berler, M., et al, "The Object Data Standard: ODMG 3.0", Morgan Kaufmann, 2000.

Charles F. Goldfarb, Paul Prescod, "The XML Handbook, Prentice Hall", 5th Edition, 2004.

Date C. J, "An Introduction to Database Systems", Addison Wesley Longman, 8th Edition, 2003.

Gustavo Santana, Data Center Virtualization Fundamentals: Understanding Techniques and Designs for Highly Efficient Data Centers with Cisco Nexus, UCS, MDS, and Beyond, Cisco Press; 1 edition, 2013

Implementation and Management", Pearson Education Limited, 6th edition, 2012.

Silberschatz A., Korth H., and Sudarshan S, "Database System Concepts", McGraw-Hill, 6th Edition, 2010.

Somasundaram, Alok Shrivastava, Information Storage and Management, EMC Education Series, Wiley, Publishing Inc., 2011.

The Complete Guide to Data Storage Technologies for Network-centric Computing Paperback– Import, Mar 1998 by Computer Technology Research Corporation

Thomas M. Connolly, Carolyn Begg, "Database Systems: Practical approach to Design,

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Medium	Medium	Low	High
CO2	Medium	High	High	Medium	Low	Low	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	Medium	Low	Medium	High
CO5	High	Low	High	Medium	Medium	Medium	High

Low = 7/35 = 20.01% Medium = 15/35 = 42.85% High = 13/35 = 37.14%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Low	High	Low	Medium
CO2	High	Low	High	Low	Medium

CO3	Medium	High	Medium	Low	Low
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 10/25 = 40.0% Medium = 4/25 = 16.00% High = 11/25 = 44.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Elective 4		CRIMINAL LAWS AND CYBERCRIMES	3	0	0	3

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- *This course will expose the students on criminal laws of India namely Indian Penal Code, Criminal Procedure Code and Indian Evidence Act and its relevance to cybercrimes and punishments.*

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Students will able to connect cybercrimes with IPC	K1
CO2	Students will able to connect cybercrimes with CrPC	K2
CO3	Students will able to connect cybercrimes with IEA	K2
CO4	Students will appreciate the court room procedures	K3
CO5	Investigation of Cybercrimes and its procedure	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate		

Course Outline:

UNIT I:**Crime and Criminality**

Definitions – Vices, Sin, Tort and Crime – History of criminal law – Constitution, IPC and IEA- Nature and Scope- Doctrine of Actus Reus and Mens Rea, Elements of crime[7]. Evolution of Law.

UNIT II:**Legal provisions in Indian Penal Code**

Crimes against property– Theft– Robbery– Dacoity. Crimes against persons: Defamation, Extortion, Bullying, Crimes against public tranquillity: Riot, Unlawful assembly.

UNIT III: **Criminal Procedure Code (CrPC)**

[7] Assignment

Organizational setup of courts in India. Complaint – inquiry – investigation – police report – public prosecutor – defence counsel – Arrest. Bail, Search. Seizure. Summons – Warrant – Information regarding cognizable and non-cognizable offence. Trials: Summary, Summon, and warrant trials

UNIT IV:**Indian Evidence Act**
Indian Evidence Act – History in India. Evidence – Meaning, principles, and concept of relevancy and admissibility. Confessions and Dying Declaration. Presumption of fact and law, Burden of proof.

UNIT V:**Information Technology Act, 2000 (amended 2008)**
Relevance of IT Act- Section 63, 64, 65, 66 (all relevant section and sub sections)

RECOMMENDED READINGS

Guar K.D., (1995) Criminal Law, Oxford University Press
IT Act, 2000- Bare Act with recent amendments
Kelkar,R.V.,(2003)Lectures on Criminal Procedure Eastern book Co., Lucknow.
Krishnamurthy S, (1987), Impact of Social Legislations, on the Criminal Law in India, R R Publishers, Bangalore.
Pillai, A.P. S., (1996) Criminal Law, N.M. Tripathi.
Ratanlal and Dhirajlal (1995) Code of Criminal Procedure
SarathyVeppaP.(1994) Elements of Law of Evidence, Eastern book Co., Lucknow.
Singh, A., (1995) Law of Evidence, Allahabad Law agency.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	Low	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	High	High
CO5	High	Low	High	High	Medium	High	High

Low = 10/35 = 28.57% Medium = 7/35 = 20.01% High = 18/35 = 51.42%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	High	High	Low	Low
CO2	High	High	High	High	Medium
CO3	Medium	High	Medium	High	Low
CO4	Medium	Low	High	High	High

CO5	Low	Medium	High	High	High
Correlation Levels:		Low	Medium	High	

Low = 6/25 = 24.0% Medium = 5/25 = 20.0% High = 14/25 = 56.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
SEC 6		INTRUSION DETECTION AND PREVENTION SYSTEM LAB- Practical's	0	0	2	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To obtain practical knowledge of finding vulnerabilities in network using IDS.
- To understand legal usage of industry standard security tools intrusion detection.
- To gain hands-on practical on current intrusion threats and its approach.
- To practice and assimilate the tools in IDS/ NIDS
- To understand vulnerabilities in networks.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Perform internal and external vulnerability analysis in network.	K1 K6
CO2	Comprehend the reconnaissance tools in IDS	K2
CO3	Understand functioning of LOGS.	K2
CO4	Understand functioning and identify the Registries	K3
CO5	Install and and Uninstall IDS.	K4 K5 K6
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate		

Course Outline:

List of Programs:

1. Study the network reconnaissance tools like WHOIS, Dig, Tracecreate, nslookup together information's about the network.
2. Detect ARP spoofing using 'ARPWATCH' tool or any other equivalent tool.
3. Scan the network for vulnerabilities using NESSUS tool or any other equivalent tool.
4. Implement a code to stimulate buffer overflow attack.
5. Install and Uninstall IDS such as 'SNORT'.
6. Study the LOGS and REGISTRIES.
7. Create firewall using IP tables.
8. Demonstrate intrusion Detection System using tools.
9. Demonstrate iptraceback

10. Explore 'N- stacker' tool for vulnerability assessment.

Note: Any 8 practical's or more as per choice of the teacher and resources available.

RECOMMENDED READINGS

Course Faculty to share the material, E-sources, books and practical guide including instructions for this course.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	High	High	Medium	Medium	Low	Low	Low
CO3	High	Medium	High	Low	Medium	Medium	Low
CO4	Medium	High	Medium	High	Low	Low	Low
CO5	High	Low	High	Medium	Medium	Low	Low

Low = 14/35 = 40.0% Medium = 10/35 = 28.57% High = 12/35 = 34.28%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Low	High	Low	Medium
CO2	High	Low	High	Low	Medium
CO3	High	High	Medium	Low	Low
CO4	High	Low	Low	Medium	Medium
CO5	Low	Medium	Low	Medium	Medium
Correlation Levels:	Low	Medium	High		

Low = 11/25 = 44.0% Medium = 8/25 = 32.0 %High = 6/25 = 24.0%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
SEC 7		DATABASE MANAGEMENT AND DATA STRUCTURE	2	0	0	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To understand the internal storage structures using different file and indexing techniques which will help in physical DB design.
- To know the fundamental concepts of transaction processing- concurrency control techniques and recovery procedure.
- To have an introductory knowledge about the emerging trends in the area of distributed databases, Object Oriented Databases, Data mining and Data Warehousing etc.
- To explain physical, network and virtualization of storages
- To explain the backup, archiving with regard to data recovery from storages.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Compare and contrast database models.	K1
CO2	Understand the concepts and techniques of transaction processing, concurrency control and recovery.	K2 K6
CO3	Understand the emerging trends and applications of database	K2
CO4	Differentiated the usage of various data structures in the problem solution.	K3 K6
CO5	Apply logic for different data structures .	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

Unit 1: **Understanding Data structures**
Definition, basic terminology, different types of data structures - array, Stacks, Linked list, Queue, Trees and Graph: Different types, Applications, Recursion, Maze Problems - Queues Operations on Queues, Queue Applications, Circular Queue. Singly Linked List Operations, Application Representation of a Polynomial, Polynomial Addition; Doubly Linked List Operations, Applications.

UNIT II: **Database System**
Introduction and Database Applications- Evolution of Database and DBMS- Need for Data Management- File System Vs Database Systems- Data Models (Relational, Network, and Hierarchical)- DBMS Architecture- Data Independence- Data Modeling using ER model.

UNIT III: **Relational Database Concept and Design**
Introduction to Relational Databases- Structure of Relational Database- Relational Model Terminology- Domains, Attributes, Tuples, Relations- Relational Database schema- Relational Algebra: Basic operations (Select, Project, set theoretic operations, Union, Intersection, Set Difference and Division)- Join operations (Inner and outer join, left outer, right outer and full outer join).
Functional Dependency- Definition, trivial and non-trivial FD- Normalization (1NF, 2NF, 3NF)- Decomposition using FD dependency preserving- BNF, Multi-valued Dependency, 4NF- Join Dependency and 5NF- Database storage and querying- Basic Concepts of Indexing and Hashing- Query Processing- Measures of Query cost, Query Processing for select, sort join operations- Basics of query optimization.

UNIT IV: **Transaction Management, Concurrency, Recovery and Security**
Transaction Processing: Introduction- Need for Concurrency control- Desirable properties of Transaction- Schedule and Recoverability- Serializability and Schedules with examples. Concurrency Control Definition- Types of Locks- Two Phases locking- Deadlock- Time stamp-based concurrency control- Recovery Techniques- Concepts-

Lost Update, Dirty Read, Immediate Update, Deferred Update- Incorrect Summary Problem due to concurrency- Shadow Paging- Multi-versioning.

UNIT V: SQL- concepts

SQL- query, examples and programs- MySQL Create Table, SELECT Statement, WHERE Clause, INSERT INTO Query, DELETE Query, UPDATE Query, ORDER BY in MySQL, SQL GROUP BY and HAVING Clause, Wildcards, Regular Expressions (REGEXP), Functions, Aggregate Functions- IS NULL & IS NOT NULL-AUTO_INCREMENT-ALTER, DROP, RENAME, MODIFY - LIMIT & OFFSET -SubQuery - JOINS -UNION - Views - Index

RECOMMENDED READINGS

Catell, R.G.G., Barry, D.K., Berler, M., et al, "The Object Data Standard: ODMG 3.0", Morgan Kaufmann, 2000.

Charles F. Goldfarb, Paul Prescod, "The XML Handbook, Prentice Hall", 5th Edition, 2004.

Date C. J, "An Introduction to Database Systems", Addison Wesley Longman, 8th Edition, 2003.

Gustavo Santana, Data Center Virtualization Fundamentals: Understanding Techniques and Designs for Highly Efficient Data Centers with Cisco Nexus, UCS, MDS, and Beyond, Cisco Press; 1 edition, 2013

Implementation and Management", Pearson Education Limited, 6th edition, 2012.

Silberschatz A., Korth H., and Sudarshan S, "Database System Concepts", McGraw-Hill, 6th Edition, 2010.

Somasundaram, Alok Shrivastava, Information Storage and Management, EMC Education Series, Wiley, Publishing Inc., 2011.

The Complete Guide to Data Storage Technologies for Network-centric Computing Paperback– Import, Mar 1998 by Computer Technology Research Corporation

Thomas M. Connolly, Carolyn Begg, "Database Systems: Practical approach to Design,

Data Structure and Algorithmic Thinking with Python: Data Structure and Algorithmic Puzzles by Karumanchi, Narasimha

Data Structures using C and C++--YedidyahLangsam, Moshe J. Augenstein, Aaron M. Tenenbaum

Data Structures using Python 2021 Edition by Dr Shriram K. Vasudevan

Fundamentals of Computer Algorithms--Horowitz, Sahani--Computer Science Press

Fundamentals of Data Structures--Horowitz, Sahani—Galgotia

Hands-On Data Structures and Algorithms with Python_second Edition by Benjamin Baka Dr Basant Agarwal Dr. Basant Agarwal

Introduction to Algorithms—Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein--MIT Press

Introduction to Data Structures using C, Ashok Kamthane, Pearson Education

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	High	High

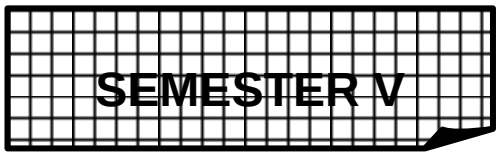
CO2	Medium	High	High	Medium	Low	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	Low	High
CO5	High	Low	High	Low	Medium	Low	High

Low = 9/35 = 25.71% Medium = 10/35 = 28.57% High = 16/35 = 45.71%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	High	High
CO2	High	Low	High	High	High
CO3	Medium	High	Medium	Low	Low
CO4	Medium	High	High	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 5/25 = 20.0% Medium = 7/25 = 28.00% High = 13/25 = 52%



Course Code	SubjectCode	TITLE OF THE COURSE	L	T	P	C
Core 9		CRYPTOGRAPHY	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To understand the basics of cryptography for learning and to find the vulnerabilities in programs
- To overcome them, know the different kinds of security threats in networks and its solution.
- To understand the different kinds of security threats in databases and solutions available and to learn about the models and standards for security.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Apply cryptographic algorithms for encrypting and decryption for secure data transmission.	K1 K6
CO2	Understand the importance of Digital signature for secure e-documents exchange and the program threats and apply good programming practice	K2
CO3	Gain the knowledge of security models and published standards.	K2
CO4	Apply security principles to system design.	K3
CO5	Analyze and design network security protocols	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Introduction to Cryptography**
Introduction to Cryptography, Security Threats, Vulnerability, Active and Passive attacks, Security services and mechanism, Conventional Encryption Model- Classical Cryptography: Dimensions of Cryptography, Classical Cryptographic Techniques.

UNIT II: **Block Ciphers and Public Key Cryptography**
Data Encryption Standard-Block cipher principles-block cipher modes of operation - CBCM (Cipher-Block Chaining Message Authentication Code) vulnerabilities and mitigation measures - CFB (Cipher Feedback) vulnerabilities and mitigation measures - OFB (Output Feedback) vulnerabilities and mitigation measures - Advanced Encryption Standard (AES). Public key cryptography: Principles of public key cryptosystems-The RSA algorithm- Key management– Diffie- Hellman Key Exchange-Elliptic curve cryptosystem.

UNIT III: **Hash Functions and Digital Signature**
Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC–MD4 & MD5. Message Digest Algorithm– SHA–HMAC– CMAC– Digital signature and authentication protocols – DSS – EIgamal – Schnorr signature.

UNIT IV: **Security Practice and System Security**
Authentication applications – Kerberos – X.509 Authentication services – Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls – Firewall designs – SET for E-Commerce Transactions.

UNIT V: **E- Mail Security and Case Studies**
E-mail Security: Security Services for E-mail-attacks possible through E-mail– Establishing keys privacy- Authentication of the source- Message Integrity- Non-

repudiation- Good Privacy-S/MIME- Internet Key Exchange Case Studies on Cryptography and security: Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.

RECOMMENDED READINGS

Atul Kahate, "Cryptography and Network Security", Mc Graw Hill, 3rd Edition, 2011.
Bart Preneel, Christof Paar, Jan Pelzl, "Understanding Cryptography", Springer-Verlag Berlin Heidelberg, 2010.
Behrouz A.Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", Tata McGraw Hill Second Edition, 2010.
Douglas R. Stinson, "Cryptography: Theory and Practice", CRC press, 3rd Edition, 2005.
Wenbo Mao, "Modern Cryptography: Theory and Practice", Prentice Hall PTR, 1st Edition, 2003.
William Stallings, "Cryptography and Network Security: Principles and Practices", 6th Edition, Pearson Education Ltd, 2016.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	High	High
CO2	Low	High	High	Medium	Low	Medium	High
CO3	High	High	High	High	Medium	High	Medium
CO4	Low	High	Medium	Medium	High	Medium	High
CO5	Low	Low	High	Low	Medium	High	High

Low = 8/35 = 22.85% Medium = 10/35 = 28.57% High = 17/35 = 48.57%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	High	High	High	Medium
CO2	High	High	High	High	Medium
CO3	Medium	High	Medium	Low	Low
CO4	Medium	High	Low	High	High
CO5	Low	High	Low	High	High
Correlation Levels: Low Medium High					

Low = 5/25 = 20.0% Medium = 5/25 = 20.0% High = 15/25 = 60.0%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 10		CYBER LAWS AND INTELLECTUAL PROPERTY RIGHTS	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To understand the origin and development of cyber laws
- Learn various rules and procedures for the applicability of the cyber space
- Appreciate the copyrights and its violations in cyberspace
- To understand the cybercrime investigation- rules and regulations
- Learn the origin and development of IPRs.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Analyze the copyright issues in cyber space	K1
CO2	Understand the legalities through analysis of crime investigation	K2
CO3	Learn the general principles in introduction of IPRs.	K2
CO4	Appreciate and understand the legalities in analysis of cybercrime investigation rules and regulations.	K3
CO5	Understand the importance and relationship of E-commerce and IPR	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Introduction**

Reorganization of Electronic Records - UNICITRAL Model Law, Legal Aspects of Electronic Records / Digital Signatures - UNICITRAL Model Law, UNICITRAL Model. Law:relating to the retention of Data Messages, Attributes of Data Messages, Acknowledgement of Data Messages, Time and Place receipt of Data Messages – Securing Electronic Record and electronic / Digital Signature in India – Verification of electronic Signature in India.

UNIT II: **Cyber Space**

The Cyberspace – Protection of Copyrights of Cyber Space – Rights of Software Owners – Infringement of Copyright – remedies for infringement of Copyright on Cyberspace – The liabilities of an Internet Service Provider (ISP) in Cyberspace – Cyberspace and the Protection of Patents in India.

UNIT III: **Tribunal**

Cyber Appellate tribunal - Its Function and Powers under IT Act – Obscenity and pornography on Cyberspace – Hacking on Cyberspace on Internet – Other Offences – violation of the Right of Privacy on Cyberspace / Internet – Punishment for violation of Privacy, Breach of Confidentiality and Privacy under the IT Act – Terrorism on Cyberspace / Internet.

UNIT IV: **Cyber Crimes Investigation**

An Overview of Cyber Crimes – Indian Evidence Act – Examiner of Electronics Act – Amendments Introduced in Indian Evidence Act, 1872 – Relevant Provisions under IT Act as Amended up to 2008 – IT (Certifying Authorities) Rules, 2000 – Ministerial Order on Blocking of Websites – The IT (Use of Electronics Records and Digital Signatures) Rules 2004.

UNIT V: Intellectual Property Rights

Concept of IPR- Patents- Indian Patent Act - Patent databases- patent information system- preparation of patent documents-trademarks- copyrights-industrial designs-geographical indication- protection of trade secrets-management and valuation of intellectual property.

RECOMMENDED READINGS

Cyber Law & IT Protection, Eastern Economy Edition, by Harish Chander.
Cyber Law: the law of Internet – Jonathan Rose nor, Springer, 1997.
Mark F Grady, Francesco Parisi August 2011. The Law and Economics of Cyber Security
Cyber law: National and International Perspectives by Roy J. Girasa and 2001
Intellectual Property Rights – Law and Practice Institute of Company Secretaries of India 2014
Law Relating to Patents, Trademarks, Copyright, Designs and Geographical Indications by B L Wadehra ISBN-13: 978-8175341852 Universal Book Traders; 2nd edition
IT Act, 2000 (Bare Act with amendments)

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	High	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	Low	High
CO3	High	High	High	High	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	Low	High
CO5	High	High	High	Low	Medium	Low	High

Low = 8/35 = 22.85% Medium = 9/35 = 25.71% High = 18/35 = 51.42%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	High	High	High	High
CO2	High	Low	High	High	Medium
CO3	Medium	High	Medium	Low	Low
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	High	High	High
Correlation Levels:		Low	Medium	High	

Low = 6/25 = 24.0.0% Medium = 6/25 = 24.0% High = 13/25 = 52.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 11		INFORMATION SECURITY AND AUDIT	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To introduce the fundamental concepts and techniques in computer and network security, giving students an overview of information security and auditing,
- To expose students to the latest trend of computer attack and defense.

Course Outcomes (COs):

At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Describe various information security issues and encryption principles	K1
CO2	Identify IP addresses range owned/used by the organization/systems in target	K2
CO3	Implemented measures such as policies, systems to protect organizations from unauthorized access/transactions	K2 K6
CO4	Identify threats within the organization and surrounding the information systems.	K3
CO5	Perform external audit through professional agencies to ensure that organizations security systems.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: Model for Internetwork Security

Conventional Encryption Principles & Algorithms (DES, AES, RC4, Blowfish), Block Cipher Modes of Operation, Location of Encryption Devices, Key Distribution, Public key cryptography principles, public key cryptography algorithms (RSA, Diffie-Hellman, ECC), public Key Distribution.

UNIT II: Approaches of Message Authentication

Secure Hash Functions (SHA-512, MD5) and HMAC, Digital Signatures, Kerberos, X.509 Directory Authentication Service, Email Security: Pretty Good Privacy (PGP) IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

UNIT III: Web Security Requirements

Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET). Firewalls: Firewall Design principles, Trusted Systems, Intrusion Detection Systems.

UNIT IV: Security Audit
Introduction, Basic Terms Related to Audits, Security audits, The Need for Security Audits in
Organization, Organizational Roles and Responsibilities for Security Audit, Auditors responsibility in Security Audits, Types of Security Audits.

UNIT V: Case Studies
Approaches to Audits, Technology based Audits Vulnerability Scanning and Penetration Testing, Resistance to Security Audits, Phase in security audit, Security audit Engagement Costs and other aspects, Budgeting for security audits, Selecting external Security Consultants, Key Success factors for security audits.

RECOMMENDED READINGS

A.J. Elbirt, "Understanding and Applying Cryptography and Data Security", CRC Press, Taylor Francis Group, New York, 2015.
M. Merkow and J. Breithaupt," Information Security: Principles and Practices", Pearson Education, 2006.
Mark Stamp, "Information Security", Wiley– INDIA, 2006.
Rick Lehtinen, Deborah Russell & G. T. Gangemi Sr., "Computer Security Basics", SPD O'REILLY 2006.
Robert Bragg, Mark Rhodes, "Network Security: The complete reference", TMH, 2017.
W. Stalling, "Cryptography and Network Security Principles and Practices", 7th Edition, Pearson of India, 2018.
Wenbo Mao, "Modern Cryptography", Pearson Education 2007.
Whitman, "Principles of Information Security", CENGAGE Learning Custom Publishing; 4th ed. Edition, 2011.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	High	High	High
CO3	High	Medium	High	High	Medium	Medium	Medium
CO4	Medium	High	Medium	High	High	High	High
CO5	High	Low	High	High	Medium	Low	High

Low = 7/35 = 20.01% Medium = 10/35 = 28.57% High = 18/35 = 51.42%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	High	High	High	Medium

CO2	High	High	High	High	Medium
CO3	Medium	High	Medium	Low	Low
CO4	Medium	High	Low	High	High
CO5	Low	High	Low	High	High
Correlation Levels:		Low	Medium	High	

Low = 5/25 = 20.0% **Medium** = 5/25 = 20.00% **High** = 15/25 = 60.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 12		**PROJECT/ CASE STUDY PRESENTATION**	1	1	2	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- Demonstrate an understanding of cloud computing architecture and storage systems.
- To understand cyber security Investigation, Elements of investigation, Guidelines
- Learn report writing
- To understand the Importance of report writing and presentation of cases.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Present a Case study analysis Reports	K1
CO2	State the types of cases relating to cyber security, forensics and information security	K2
CO3	State the mechanism of writing a case report	K3, K4
CO4	Learn the Importance of report cases and presentation	K5
CO5	Write a project report	K6
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

List of Programs:

1. Case Study 1. Computer Forensic Analysis
2. Case Study 2. Counterfeiting and Fraud: A Forensic Computer Investigation
3. Case Study 3: Development of a Database Application.
4. case study on different file organisation
5. Case Study on Graph Data Structure
6. Case study on Planning a Project
7. Case study Internet Information System
8. Case Study on Preparation for a Software Audit
9. Case study to develop Test Plan for an Application
10. Case Study of a Real time Web Service.

11. Case Study on Architecture of two operating systems
12. Case study on Tools and Software related to Database
13. Case study on IT architecture and project planning of an company
14. Case study - Security in the cloud
15. Case study on Conventional Cryptographic Algorithm
16. Case study on creating IPsec Tunnel mode tunnels.
17. Case study - Security in the cloud
18. Case study on configuring NMS
19. Case study on Configuring SNMP Agent
20. Case study on Network Architecture Analysis
21. Case Study on configuring routers using different protocols
22. Case Study on the Communication Network of an Organization
23. Case Study on Live Streaming technique in an University
24. Case study on simulating the routing protocols
25. Case Study on Distributed Communication System Models

Note: Any 5 cases including one on real time or more as per choice of the teacher and resources available.

RECOMMENDED READINGS

Course Faculty to share the material, E-sources, books and practical guide including instructions for this course.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	High	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	Low	Low	High	High
CO5	High	Low	High	Medium	Medium	High	High

Low = 6/35 = 17.14% Medium = 11/35 = 31.42% High = 17/35 = 48.57%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	Medium	High	High	Medium
CO2	High	Medium	High	Low	Medium
CO3	Medium	High	Medium	High	Low
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels:		**Low**	**Medium**	**High**	

Low = 6/25 = 24.0% Medium = 10/25 = 40.00% High = 9/25 = 36.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C

Elective 5		BASICS OF ETHICAL HACKING	3	0	0	3

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To understand ethics and legalities related to hackers
- To process of ethical hacking
- To appreciate different type of attacks and its respective security
- To identify different vulnerabilities and misconfigurations
- To understand security risks and its impact.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Remember the advantage of the ethical hacking	K1
CO2	Operationalize the area of his/her hacking competent.	K2
CO3	Critically appreciate the knowledge gained and strengthen the skills required for ethical hacking	K2
CO4	Analyse the knowledge the required for securing the system and network from hacking	K3
CO5	Analyse, evaluate and Implement industry standard security protocols to minimize cyber attacks	K4 K5 K6
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Introduction to Ethical Hacking and Network Refresher**

Essential Terminologies Confidentiality Integrity Availability (C.I.A) Triad Types of Hackers Ethical Hacking Process OSI Model and TCP/IP Suite Network Addressing Common Ports and Protocols.

UNIT II: **Reconnaissance, Scanning and Enumeration**

Introduction to Reconnaissance Active and Passive Reconnaissance- Open-Source Intelligence (OSINT)- Passive OSINT- Scanning and Enumeration- Scanning IP Address, Network and it's Services- Enumerating Open Ports - HTTP/S, SMB, SNMP, SMPT- Finding Vulnerabilities and its Proof-of-Concept (POC).

UNIT III: **System Hacking and Network Sniffing and Social Engineering**

Basics of Shells - Reverse Shell, Bind Shell Automated Exploitation - Metasploit Manual Exploitation - Scripts Password Attacks - Brute Force, Wordlist, Spraying Malware Attacks - Trojans, Backdoors.

Introduction To Sniffing Attacks Traffic and Packet Analysing- Social Engineering- Social Engineering Techniques- Phishing and Vishing.

UNIT IV: **Privilege Escalation**

Introduction To Escalation Linux Privilege Escalation - SUDO, Kernel, SUID, Misconfiguration Windows Privilege Escalation - Impersonation, Registry, DLL, CVE Pivoting and Maintaining Access Cleaning Up.

UNIT V: **Web Application Hacking and Wi-Fi Hacking**
Introduction To Basics of Web Application OWASP Top 10 Web Application Vulnerabilities Subdomain Enumeration Injection Techniques - SQL, XML, CRLF, Cookie Authentication Issues Sensitive Data Exposure Cross-Site Scripting and Cross-Si.
Introduction To 802.11 Protocol Types of 802.11 Attacks WEP, WPA and WPA2 Cracking Evil Twin Attack.

RECOMMENDED READINGS

Ankit Fadia "Ethical Hacking" second edition Macmillan India Ltd, 2006
Lomeaskeshkumar (September 1, 2014). Ethical hacking countermeasures - An Ultimate Guide for Ethical Hackers [Paperback] (Author),.
Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts... by Ali Jahangiri (Oct 21, 2009)
Michael Gregg,"Certified Ethical Hacker", Version 10, Third Edition, Pearson IT Certification, 2019.
Roger Grime, "Hacking the Hacker", 1st Edition, Wiley, 2017.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Medium	Low	High
CO5	High	Medium	High	High	Medium	High	High

Low = 12/35 = 34.28% Medium = 7/35 = 20.01% High = 16/35 = 45.71%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	High	High	Low	Medium
CO2	High	High	High	Low	Medium
CO3	Medium	High	Medium	Low	Low
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels:	**Low**	**Medium**	**High**		

Low = 7/25 = 28.0% Medium = 7/25 = 28.00% High = 11/25 = 44.0 %

Course	Subject	TITLE OF THE COURSE	L	T	P	C

Code	Code					
Elective 6		CRYPTOGRAPHY LAB- Practical's	0	0	3	3

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- This course is to understand the principles of encryption algorithms, conventional and public key cryptography practically with real time applications.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Code well designed web applications with validations using JavaScript.	K1 K6
CO2	Understand the properties of the Public and Private keys	K2
CO3	Develop secure mobile applications using cryptographic functions.	K2 K6
CO4	Apply algorithm to solve a crypto problem	K3 K6
CO5	JAVA program to implement the BlowFish algorithm logic and a Rijndael algorithm logic.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

List of Programs: - Any 10 may be given to students

1. Write a program to implement Linear Congruential Algorithm to generate 5 pseudo random numbers in C.
2. Write a program to implement Fermat Primality Testing Algorithm in C.
3. Write a program to implement Rabin-Miller Primality Testing Algorithm in C.
4. Write a program to implement the Euclid Algorithm to generate the GCD of an array of 10 integers in C.
5. Write a Java program to perform encryption and decryption using the algorithms: a) Ceaser Cipher b) Substitution Cipher c) Hill Cipher
6. Write a Java program to perform encryption and decryption using the algorithms: a) Playfair Cipher b) Vigenere Cipher
7. Write a Java program to implement the DES algorithm logic
8. Write a JAVA program to implement the BlowFish algorithm logic
9. Write a JAVA program to implement the Rijndael algorithm logic.
10. Using Java Cryptography, encrypt the text "Hello world" using BlowFish. Create your own key using Java keytool.
11. Write a Java program to implement RSA Algorithm
12. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.

Note: Any 8 practical's or more as per choice of the teacher and resources available.

RECOMMENDED READINGS

Atul Kahate, "Cryptography and Network Security", Mc Graw Hill, 3rd Edition, 2011.
Bart Preneel, Christof Paar, Jan Pelzl, "Understanding Cryptography", Springer-Verlag Berlin Heidelberg, 2010.
Behrouz A.Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security",
Douglas R. Stinson, "Cryptography: Theory and Practice", CRC press, 3rd Edition, 2005.
Tata McGraw Hill Second Edition, 2010.
Wenbo Mao, "Modern Cryptography: Theory and Practice", Prentice Hall PTR, 1st Edition, 2003.
William Stallings, "Cryptography and Network Security: Principles and Practices", 6th Edition, Pearson Education Ltd, 2016.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	Low	Low	High
CO3	High	Medium	High	High	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	Low	High
CO5	High	Low	High	High	Medium	Low	High

Low = 10/35 = 28.57% Medium = 10/35 = 28.57% High = 15/35 = 42.85%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	High	High	Low	High
CO2	High	High	High	Low	High
CO3	Medium	High	Medium	Low	High
CO4	Medium	High	Low	High	High
CO5	Low	Medium	High	High	Medium
Correlation Levels:	Low	Medium	High		

Low = 5/25 = 20.0% Medium = 5/25 = 20.0% High = 15/25 = 60.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Mini Project		SUMMER INTERNSHIP/ INDUSTRIAL TRAINING	0	1	0	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- This internship will give you an opportunity to implement the skills you learned throughout this program, through dedicated mentoring sessions and learn how to solve a real-world, industry-aligned problem.
- To expose the students to the functioning of the agencies of the dealing with cyber security
- To make the students to understand the importance of the Allied/ parallel systems

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Provide field level to exposure to students	K1
CO2	Operationalize the cyber security area of his/her interest.	K2
CO3	Influence/ Change the attitude of students towards working place	K2
CO4	Analyse the knowledge the required for securing the system and network from hacking	K3
CO5	Analyse, evaluate and Implement industry standard security protocols to minimize cyber attacks	K4 K5 K6
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

All the students are expected to take this paper compulsorily. The Objectives of this paper is to provide field level experience to the students of criminology and professionally equip them to find appropriate places in the allied fields of Criminology. The students will be placed for internship at anyone of the following agencies for a period of 30 days. Certificates should be issued for the particular student(s). The agencies to be covered for internship includes

- Governmental agencies – Law enforcement/ Cybercrime Wing
- Non- governmental agencies working in the areas of Cyber Security
- CERT-In
- CFSL/ SFSL/ MFSL
- BSFI's
- Corporate Data Protection
- Data Security agencies
- Agencies working on cyber security
- Agencies working data penetration testing
- Cybercrime Lawyer
- Anyother agenciesorganising or conducting cyber activities or as suggested by the mentor or teachers.

During this period the students are expected to work for the organization under the guidance of an experienced person. The students will take up the regular activities of

the organization work in the agency and continue to work in the areas entrusted by the agency or supervisor. Each student will be evaluated by his/her supervisor in the organization during the internship period, through a Confidential performance appraisal report filled and sent to the Head of the Department, directly. The students are required to submit a record based on activities/roles performed by them during the internship- a daily report. The student will be evaluated at the end of the semester based on the performance appraisal report, record, and a public viva-voce.

RECOMMENDED READINGS

Course Faculty to share the material format, E-sources and books including instructions for this course.

Mapping of Course Outcomes to Programme Outcomes

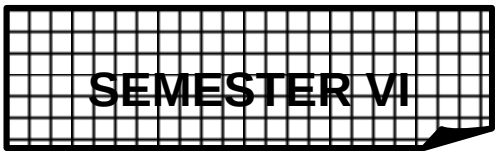
	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	Medium	Low	High	Low	Medium	Medium	High
CO2	Medium	High	High	Medium	Low	Medium	High
CO3	Medium	Medium	High	Medium	Medium	Medium	Medium
CO4	Medium	High	Medium	Medium	Low	Low	High
CO5	High	Low	High	Medium	Medium	Low	High

Low = 7/35 = 20.0% Medium = 18/35 = 51.42% High = 11/35 = 31.52%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	Medium	Medium
CO2	High	Medium	High	Medium	Medium
CO3	Medium	Low	Medium	Medium	Low
CO4	Medium	Medium	Low	Medium	Medium
CO5	Low	Medium	Low	Medium	Medium
Correlation Levels: Low Medium High					

Low = 5/25 = 20.0% Medium = 16/25 = 64.0% High = 4/25 = 16.0 %



PAPER 23

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 13		CYBER FORENSICS AND INVESTIGATION	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To explain the basic principles of digital forensics
- To choose appropriate digital forensics tools to identify, classify, locate and recover the evidence
- To infer the emerging digital forensic trends and technologies.
- To understand how to recover data.

Course Outcomes (COs):

At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Describe cyber forensics and the knowledge required to do the forensic analysis and extend Scientific approaches to forensics that helps to identify, classify, locate and recover the evidence	K1
CO2	Choose and apply current cyber forensics tools.	K2
CO3	Devise basic network forensic analysis	K2
CO4	Identify the emerging forensic technology	K3
CO5	Show the required knowledge and expertise to become a proficient forensic investigator	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate		

Course Outline:

UNIT I: Principles and methods Scientific approaches to cyber forensics

Cyber forensics – Understanding the science of forensics – cyber forensics knowledge needed: Operating Systems, Hardware, Networks – fundamental principles of cyber forensics – maintaining the chain of custody – law and cyber forensics: Principles and methods Scientific approaches to forensics – Identify and classify evidence – Locations where evidence may reside: storage media, Hardware interfaces, File systems, file format, file types, header analysis – Recovering data – media file forensic steps

UNIT II: Forensic Analysis

Hard drive specifications – Recovering data from the damaged media– Operating system specifics– Extracting deleted files– Encrypted files- Cryptography– Steganography– Cryptanalysis- Log tampering– Other techniques: spoofing, wiping, Tunneling– Case notes and reports, forensic tools for Password recovery.

UNIT III: Network Forensics

Network packet analysis– Wireless– Router forensics– Firewall forensics– Logs to examine– Operating system utilities– network structure. Windows System Forensics- Linux System Forensics.

UNIT IV: Emerging forensics technology

Social Networks– New devices: Google Glass, Cars, Medical devices– control systems and infrastructure– Online gaming– Electronic discovery: types of investigation, liability and proof, big data, steps in electronic data discover, disaster recovery.

UNIT V: Digital Forensics - Present and future

Forensic tools– Open-source forensic suite– Proprietary forensic suite– Drive Imaging and validation tools– forensic tool for integrity verification and hashing– Applying Digital Forensics in social media.

RECOMMENDED READINGS

Andrew hoog& Katie Strzempka," iPhone and iOS Forensics Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS devices", Syngress, 2011, ISBN: 9781597496605.

Andrew hoog, "Andriod Forensics: Investigation, Analysis and Mobile Security for Google Android", Illustrated Edition2011, Syngress. ISBN -13: 978 – 1597496513.

Androulidakis, losif. I, "Mobile phone security and Forensics: A practical approach", Springer – Verlag, New York, 2012, ISBN: 978 – 1 – 4614 – 1650 – 0

Anthony J. Bertino. Forensic Science- Fundamentals & Investigation, Cengage Learning, 2009.

Bill Nelson Amelia Phillips Christopher Steuart, "Guide to Computer Forensics and Investigations: Processing Digital Evidence", Fifth Edition, Cengage Learning, ISBN: 978-1-285-06003-3

Chuck Easttom, "CCFPSM Certified Cyber Forensics Professional Certification ALL-IN-ONE (Exam Guide)", McGraw-Hill Education, 2015, ISBN: Book p/n 978-0-07-183611-1 2.

Cory Altheide, Harlan Carvey, "Digital Forensics with Open-Source Tools", 2011, Elsevier, ISBN: 978-1-59749-586-8

Dejey, Murugan, "Cyber Forensics", Oxford University Press; First edition (1 June 2018), ISBN13: 978-0199489442

John Vacca, "Computer Forensics: Computer Crime Scene Investigation", Charles River Media; Second Edition, ISBN-13: 978-1-58450-389-7

Marjie T. Britz, "Computer Forensics and Cyber Crime: An Introduction", 3rd Edition, Prentice Hall, ISBN-13: 978-0-13-267771-4

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	Low	Low	High	High	Medium	High	High
CO2	Medium	High	High	Medium	Low	High	High
CO3	High	Medium	High	Low	Medium	High	Medium
CO4	Medium	High	Medium	Low	Low	High	High
CO5	High	Low	High	Low	Medium	High	High

Low = 9/35 = 25.71% Medium = 9/35 = 25.71% High = 17/35 = 48.57%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	High	High	Low	Medium
CO2	High	High	High	High	Medium
CO3	Medium	High	Medium	High	Low
CO4	Medium	Medium	Low	High	High
CO5	Low	High	Low	High	High
Correlation Levels: Low Medium High					

Low = 3/25 = 12.0% Medium = 6/25 = 24.00% High = 16/25 = 64.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 14		**SECURITY ARCHITECTURE AND DESIGNS**	3	1	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- This course introduces the basic concepts of Security and its needs, architecture and models
- To gain knowledge about security, information, components, issues, analysis, architecture, various models, security types and its applications.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Become proficient in concepts like Security components, balancing and Access	K1
CO2	To understand the basics of security needs in business, threats etc., and ability to Understand Ethical and Professional issues concepts.	K2
CO3	Become proficient in security technologies like IDS, cryptography.	K3 K6
CO4	Understand the concepts of Access control, physical security and personnel	K2
CO5	Become proficient in various Architectures like Low, Mid and High level	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Securing Information**

Introduction: Information Security, Critical Characteristics of Information, Components of an Information System, Securing the Components, Balancing Security and Access- CIA

UNIT II: Security Analysis and Security Models
Need for security, Business needs, Threats, Attacks, Legal, Ethical and Professional Issues. Basic Security Models: Bell- LaPadula model- Biba model- Clark- Wilson model- Non-Interference model.

UNIT III: Logical Design
Blueprint for security, Information Security policy, NIST Models, VISA International security Models, Design of Security Architecture, planning for continuity. COBiT (Control Objectives of Information and Related Technology- The information security management maturity model.

UNIT IV: Physical Design
Security Technology, IDS, Cryptography, Access Control Devices, Physical Security, Security and Personnel.

UNIT V: Architecture Types and Case Studies
Architecture: Types- Low- level, Mid-level and High-level Architecture, Case study- Business cases for Security.

RECOMMENDED READINGS

Bill Nelson Amelia Phillips Christopher Steuart, "Guide to Computer Forensics and Investigations: Processing Digital Evidence", Fifth Edition, Cengage Learning, ISBN: 9781285060033

Chuck Easttom, "CCFPSM Certified Cyber Forensics Professional Certification ALL-IN-ONE (Exam Guide)", McGraw-Hill Education, 2015, ISBN: 9780071836111

Cory Altheide, Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011, ISBN: 9781597495868

Dejey, Murugan, "Cyber Forensics", First edition, Oxford University Press, 2018, ISBN: 9780199489442

John Sammons, "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics", Elsevier, 2012, ISBN: 9781597496612

John Vacca, "Computer Forensics: Computer Crime Scene Investigation", Laxmi Publications; First edition, 2015, ISBN: 9788170083412.

Marjie T. Britz, "Computer Forensics and Cyber Crime: An Introduction", 3rd Edition, Prentice Hall, 2013, ISBN: 978-0132677714

Matt Bishop, "Computer Security Art and Science", Addison Wesley, 2018.

Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi, 4th Edition, 2012.

Micki Krause, Harold F. Tipton, "Handbook of Information Security Management", Vol 1-3, CRC Press LLC, 2004.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	Medium	Medium	High	Low	High	Medium	High
CO2	Medium	Medium	High	Medium	High	Low	High

CO3	High	Medium	High	High	Medium	Medium	Low
CO4	Medium	Medium	Medium	High	High	Low	High
CO5	High	Low	High	Low	Low	Medium	Medium

Low = 9/35 = 25.71% Medium = 12/35 = 34.28% High = 14/35 = 40.0%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	Medium	High	High	High	High
CO2	Medium	Medium	Medium	High	High
CO3	Low	High	Low	High	Medium
CO4	Medium	Low	High	High	Medium
CO5	Medium	Medium	High	High	Low
Correlation Levels: Low Medium High					

Low = 4/25 = 16.0% Medium = 9/25 = 36.00% High = 12/25 = 48.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 15		CLOUD TECHNOLOGY AND SECURITY	4	0	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- The course introduces the fundamental concepts of cloud computing, its services and Tools. It concentrates the basic concepts of security systems and cryptographic protocols, which are widely used in the design of cloud security.
- The issues related multi tenancy operation, virtualized infrastructure security and methods to improve virtualization security are also dealt with in this course.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Understand the importance of virtualization in distributed computing and how this has enabled	K1
CO2	Identify the appropriate cloud services for a given application.	K2
CO3	Analyze Cloud infrastructure including Google Cloud and Amazon Cloud.	K2
CO4	Assess the security of virtual systems and evaluate the security issues related to multi-tenancy.	K3

CO5	Analyze authentication, confidentiality and privacy issues in cloud computing and identify security implications in cloud computing.	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate		

Course Outline:

UNIT I: Cloud Computing
History of Cloud Computing – Cloud Architecture – Cloud Storage – Why Cloud Computing Matters– Advantages of Cloud Computing – Disadvantages of Cloud Computing – Companies in the Cloud Today – Cloud Services.

UNIT II: Web Based Application
Pros and Cons of Cloud Service Development– Types of Cloud Service Development– Software as a Service– Platform as a Service– Web Services- IAAS– On-Demand Computing – Discovering Cloud Services Development Services and Tools– Amazon Ec2– Google App Engine– IBM Clouds.

UNIT III: Security Concepts
Confidentiality – Privacy – Integrity – Authentication - Non-repudiation – Availability - Access control - Defence in depth – Least privilege - How these concepts apply in the cloud - Importance in PaaS, IaaS and SaaS. User authentication in the cloud- Cryptographic Systems: Symmetric cryptography - Stream ciphers - Block ciphers - Modes of operation - Public-key cryptography – Hashing - Digital signatures- Public-key infrastructures - Key management - X.509 certificates - OpenSSL.

UNIT IV: Multi-Tenancy Issues
Isolation of users/VMs from each other- Virtualization System Security Issues- ESX and ESXi Security- ESX file system security- Storage considerations - Backup and Recovery- Virtualization System Vulnerabilities- Management console vulnerabilities- Management server vulnerabilities- Administrative VM vulnerabilities- Guest VM vulnerabilities- Hypervisor vulnerabilities- Hypervisor escape vulnerabilities- Configuration issues- Malware.

UNIT V: Legal, Compliance Issues and Case Studies
Responsibility- Ownership of data - Right to penetration test - Examination of modern Security Standards- How standards deal with cloud services and virtualization- C compliance for the cloud provider vs. compliance for the customer– Case Studies: Cryptography for Remote Access and Support- A Secure Network for a Private Cloud.

RECOMMENDED READINGS

Haley Beard, "Cloud Computing Best Practices for Managing and Measuring Processes for On-demand Computing, Applications and Data Centers in the Cloud with SLAs", Emereo Pty Limited, July 2008.
J.R. ("Vic") Winkler, "Securing the Cloud", Syngress [ISBN: 1597495921], 2011.

John Rittinghouse, James Ransome, "Cloud Computing", CRC Press; 1st Edition [ISBN: 1439806802], 2009.
Michael Miller, "Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online", Que Publishing, August 2008.
Ronald L. Krutz, Russell Dean Vines, "Cloud Security", [ISBN: 0470589876], 2010.
Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media; 1 edition [ISBN: 0596802765], 2009.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Medium	Medium	Low	High
CO2	Medium	High	High	Medium	Medium	Medium	High
CO3	High	Medium	High	Medium	Medium	Medium	Medium
CO4	Medium	High	Medium	Medium	Low	Medium	High
CO5	High	Low	High	Low	Medium	Medium	High

Low = 6/35 = 17.14% Medium = 17/35 = 48.57% High = 12/35 = 34.28%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	Medium	Medium
CO2	High	Medium	High	Medium	Medium
CO3	Medium	High	Medium	Low	Low
CO4	Medium	Medium	Medium	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels:	Low	Medium	High		

Low = 4/25 = 16.0% Medium = 14/25 = 56.0% High = 7/25 = 28.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Core 16		COMPUTATIONAL INTELLIGENCE	4	0	0	4

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To summarize the basics of problem solving using computational thinking.
- To organize and process data using computers.
- To apply software development procedures.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Summarize the basics of computers and data and solve problems using different elements of computational thinking and logic.	K1
CO2	Analyze problems and represent solutions using algorithms and activity diagrams.	K4
CO3	Organize and process data using different data structures.	K2 K6
CO4	Apply software testing procedures.	K3
CO5	Illustrate the importance of the foundations of concurrency and information security.	K4 K5 K6
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: Computational Thinking
Computers and Computational Thinking– From Abacus to Machine– The first Software– What makes it a Modern Computer?– The first Modern Computer– Moore's Law– Information and Data: Converting Information into Data– Data Capacity– Data Types and Data Encoding– Data Compression.

UNIT II: Logic
Boolean Logic– Applications of propositional logic– Solving Problems: Problem Definition– Logical Reasoning– Decomposition– Abstraction– Class Diagrams and Use Case Diagrams.

UNIT III: Fuzzy Logic
Non-Monotonic reasoning- Fuzzy Logic- Fuzzy rules- Fuzzy inference- Temporal Logic- Temporal reasoning- Neural Networks- Neuro Fuzzy Inferences.

UNIT IV: Computational Intelligence and its Application
Natural Language Processing- Morphological analysis- syntax analysis- Semantic analysis- All NLP applications- Language models- Information Retrieval- Information Extraction- Machine Translation- Machine Learning.
UNIT V: Concurrent Activity
Parallelism– Scheduling– Sorting Networks– Measuring Concurrency's Effect– Information Security: What is Security? – Foundations– Common Forms of Cyber Crime– Securing Data– Securing Techniques– Strategies.

RECOMMENDED READINGS

David D. Riley, Kenny A. Hunt, "Computational Thinking for the Modern Problem Solver", CRC Press, 2014, ISBN: 9781466587793
Heidi Williams, "No Fear Coding: Computational Thinking across the K-5 Curriculum", International Society for Technology in Education, 2017, ISBN: 9781564843876.

Karl Beecher, "Computational Thinking, A Beginner's Guide to Problem Solving and Programming", 2017, ISBN: 9781780173641.
Paolo Ferragina, Fabrizio Luccio, "Computational Thinking, First Algorithms, Then Code", Springer Publications, 2018, ISBN: 9783319979397.
Paul S. Wang, "From Computing to Computational Thinking", Routledge, 2015, ISBN: 9781482217650.
Peter J Denning, Matti Tedre, "Computational Thinking", MIT Press, 2019, ISBN: 9780262536561.
Peter William McOwen, Paul Curzon, "Power of Computational Thinking: The Games, Magic and Puzzles to help you become a Computational Thinker", World Scientific Europe Ltd, 2017, ISBN: 9781786341846.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	High	High
CO2	Medium	High	High	Medium	Low	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	Low	High
CO5	High	Low	High	Low	Medium	Low	High

Low = 9/35 = 25.71% Medium = 10/35 = 28.57% High = 16/35 = 45.71%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	High	High
CO2	High	Low	High	High	High
CO3	Medium	High	Medium	Low	Low
CO4	Medium	High	High	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels:	Low	Medium	High		

Low = 5/25 = 20.0% Medium = 7/25 = 28.00% High = 13/25 = 52%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Elective 7		CYBER RISK MANAGEMENT	3	0	0	3

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- To understand the concept of cyber risk management and its importance in the field of cybersecurity.
- To identify and assess various types of cyber risks that an organization can face and develop strategies to mitigate them.

- To learn the various steps involved in the risk management cycle and their application in real-world scenarios.
- To understand the legal and regulatory frameworks related to cyber risk management and compliance requirements.
- To develop skills to communicate effectively with stakeholders and decision-makers on the risks and potential impact of cyber threats.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Recognize the importance of cyber risk management in the context of cyber security	K1
CO2	Understand the key elements of the risk management cycle and how it applies to cyber security	K2
CO3	Understand the key elements of the risk management cycle and how it applies to cyber security	K3
CO4	Analyze the effectiveness of risk mitigation strategies and evaluate their suitability for specific cyber risks	K4, K5
CO5	Create a comprehensive cyber risk management plan that addresses cyber risks and protects against potential threats	K6
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Introduction to Cyber Risk Management, Threats and Vulnerabilities Assessment**

Overview of Risk Management - Cyber Risk Management Framework - Risk Analysis and Evaluation - Types of Risks - Risk Assessment Methods - Risk Management Standards - Risk Management Process - Cyber Risk Management Cycle. Threats and Vulnerabilities - Common Threat Actors - Attack Methods - Vulnerability Scanning and Penetration Testing - Security Controls - Risk Mitigation and Remediation.

UNIT II: **Frameworks for Digital Forensics**

Introduction to digital forensics – Introduction to Frameworks for Digital Forensics - NIST SP800-86 - ISO27041:2015 - Computer Forensic Tool Testing (CFTT) – “Electronic Evidence Analysis Methodology" (EEAM) by UNODC.

UNIT III: **Business Impact Analysis and Continuity Planning**

Business Impact Analysis - Disaster Recovery Planning - Business Continuity Planning - Crisis Management - Incident Response Planning - Communication Planning - Business Continuity Standards.

UNIT IV: **Legal and Compliance Considerations**

Legal Frameworks for Cyber Security - Data Protection and Privacy Laws - Regulations and Compliance Requirements - International Cyber Security Law and Cyber Diplomacy - Cyber Insurance.

UNIT V: **Risk Monitoring and Risk Communication**
Risk Monitoring - Continuous Monitoring and Auditing - Risk Metrics - Risk Reporting - Risk Communication - Information Sharing and Collaboration - Cyber Security Awareness and Training.

RECOMMENDED READINGS

- "Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats" by Scott Donaldson, Stanley Siegel, Chris K. Williams, Abdul Aslam
- "Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls" by Hanno Heintzenberg
- "The Manager's Guide to Cybersecurity Law: Essentials for Today's Business" by Tari Schreider
- "Cybersecurity for Executives: A Practical Guide" by Gregory J. Touhill and C. Joseph Touhill
- "Introduction to Risk Management and Insurance" by Mark S. Dorfman and David L. Northrup

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	High	High
CO2	Medium	High	High	Medium	Low	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium
CO4	Medium	High	Medium	High	Low	Low	High
CO5	High	Low	High	Low	Medium	Low	High

Low = 9/35 = 25.71% Medium = 10/35 = 28.57% High = 16/35 = 45.71%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	High	Medium	High	High	High
CO2	High	Low	High	High	High
CO3	Medium	High	Medium	Low	Low
CO4	Medium	High	High	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels:		**Low**	**Medium**	**High**	

Low = 5/25 = 20.0% Medium = 7/25 = 28.00% High = 13/25 = 52%

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Elective 8		FIREWALL AND INTERNET SECURITY	3	0	0	3

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- This course introduces the basic concept of Firewalls, fundamentals of internet security and security architecture.
- To understand the different kinds of security threats in networks, databases and their solutions.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	To understand the fundamentals of firewalls and internet security.	K1
CO2	To differentiate malicious and non-malicious code and to list and explain various type of threats in networks.	K2
CO3	Understand the security requirements and multilevel database and about file protection mechanism and authentication.	K2 K6
CO4	Understanding different typologies of crime including crimes against human body, property and types of offenders.	K3
CO5	Exploring the concept of Intrusion detection systems and virtual private networks and implement multilevel security	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

UNIT I: **Firewalls and Security Mechanism**

Introduction– Types of Firewalls– Packet filters– Application gate ways– Limitations of firewalls- Internet Security - Email security– PGP- S/MIME - IP security– Overview– IP Security Architecture- Web security- SSL, TLS, SET.

UNIT II: **Program Security**

Secure programs– Non-malicious Program Errors– Viruses– Targeted Malicious code– Controls against Program Threat – Control of Access to General Objects– User Authentication– Good Coding Practices– Open Web Application Security Project Top

10 Flaws – Common Weakness Enumeration- Top 25 Most Dangerous Software Errors.

UNIT III: Operating System Security

Protected objects and methods of protection- Memory address protection- Control of access to general objects- File protection mechanism-Authentication: Authentication basics- Password- Challenge response- Biometrics.

UNIT IV: Security in Databases

Security requirements of database systems – Reliability and Integrity in databases – Two Phase Update– Redundancy/ Internal Consistency– Recovery– Concurrency/ Consistency– Monitors– Sensitive Data– Types of disclosures– Inference.

UNIT V: Security in Networks and Case Studies

Threats in networks – Encryption– Virtual Private Networks– PKI– SSH– SSL– IPSec –Content Integrity– Access Controls– Wireless Security– Honeypots– Traffic Flow Security– Firewalls– Intrusion Detection Systems– Secure e-mail.

RECOMMENDED READINGS

Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Fourth Edition, Pearson Education, 2007.

Eric Maiwald, "Network Security: A Beginner's Guide", TMH, 1999.

Kaufman, Perlman, Speciner, "Network Security", Prentice Hall, 2nd Edition, 2003.

Macro Pistoia, Java Network Security, Pearson Education, 2nd Edition, 1999.

Matt Bishop, "Computer Security: Art and Science", Pearson Education, 2003.

Michael Howard, David LeBlanc, John Viega, "24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them", First Edition, Mc Graw Hill Osborne Media, 2009.

Whitman, Mattord, Principles of Information Security, Thomson, 2nd Edition, 2005.

William Stallings, "Cryptography and Network Security: Principles and Practices", Fifth Edition, Prentice Hall, 2010.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	High	Medium	Low	High
CO2	Medium	High	High	High	Low	Low	High
CO3	High	Medium	High	Medium	Medium	Medium	Medium
CO4	Medium	High	Medium	Low	Low	Low	High
CO5	High	Low	High	Low	Medium	Low	High

Low = 10/35 = 28.54% Medium = 10/35 = 28.54% High = 15/35 = 42.85%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Low	Low	Low	Medium
CO2	High	High	Medium	Low	Medium
CO3	Medium	High	Low	Low	Low
CO4	Medium	Low	Low	High	Medium
CO5	High	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 10/25 = 40.0% Medium = 8/25 = 32.00% High = 7/25 = 28.0 %

Course Code	Subject Code	TITLE OF THE COURSE	L	T	P	C
Professional Competency Skill		CYBERCRIME INVESTIGATION AND CYBER FORENSICS LAB-Practical's	0	0	2	2

L: Lecture T: Tutorial P: Practical C: Credits

Course Objectives:

The main objectives of this course are

- Explain the basic principles of digital forensics
- To choose appropriate digital forensics tools to identify, classify, locate and recover the evidence
- To infer the emerging digital forensic trends and technologies.
- This Course provides basic insight of Computer Forensics Analysis and to perform E-Mail Investigations.
- To get deep Knowledge in various Computer Forensic Tools used in Investigation of different Operating System Environments.

Course Outcomes (COs): At the end of this course of study, the student will be able to

CO No.	Course Outcome	Cognitive Levels
CO1	Describe cyber forensics and the knowledge required to do the forensic analysis	K1
CO2	Extend Scientific approaches to forensics that helps to identify, classify, locate and recover the evidence	K2 K6
CO3	Choose and apply current cyber forensics tools and devise basic network forensic analysis	K2 K6
CO4	Identify the emerging forensic technology	K3 K6
CO5	Explore and identify the required knowledge and expertise to become a proficient forensic investigator	K4 K5
K1: Remember **K2:** Understand **K3:** Apply **K4:** Analyze **K5:** Evaluate **K6:** Create		

Course Outline:

List of Programs: Any ten may be selected by the course faculty

1. Computer Hacking & Network Intrusion.
2. Survey of Latest developments in Cyber Forensics.
3. Registry Editing and Viewing using native tools of OS.
4. Hex analysis using Hex Editors.
5. Bit level Forensic Analysis of evidential image using FTK, Encase and ProDiscover Tools.
6. Hash code generation, comparison of files using tools like HashCalcetc.
7. File analysis using Sleuthkitetc and Graphical File analysis and Image Analysis.
8. Email Analysis involving Header check, tracing route.
9. Performing a check on Spam mail and Non- Spam mail.
10. Create a file on a USB drive and calculate its hash value like FTK Imager. Change the file and calculate the hash value again to compare the files.
11. Extracting of files that have been deleted.
12. Locate and extract Image (JPEG) files with altered extensions.
13. Perform Digital evidence identification and isolation.
14. Examination of Windows event log and perform log correlation.
15. Perform forces analysis on last activity (LastActivityView).
16. Windows Password cracking (Hiren's Boot).
17. Perform Mobile data analysis using forensics tool (SUNTOKU_0.5).
18. Perform USB and HDD write blocker for forensic acquisition.
19. Capture volatile memory and perform analysis (FTK).
20. Analysis on Digital photography image (https://29a.ch).
21. Creating MAC timeline of a directory (Mac-Robber) DIGITAL SCIENCES (2020)
22. Windows malware detection and mitigation (Sys internals Suite).
23. Perform browser forensic analysis.
24. Forensics - md5sum, sha1sum, and sha256sum
25. Demonstrate data retrieval from a pen drive, hard disk, etc using any free and open-source tool.

Note: Any 8 practical's or more as per choice of the teacher and resources available.

RECOMMENDED READINGS

Course Faculty to share the material, E-sources, books and practical guide including instructions for this course.

Mapping of Course Outcomes to Programme Outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7
CO1	High	Low	High	Low	Medium	Low	High
CO2	Medium	High	High	Medium	High	High	High
CO3	High	Medium	High	Low	Medium	Medium	Medium

CO4	Medium	High	Medium	Low	Low	High	High
CO5	High	Low	High	Medium	Medium	High	High

Low = 6/35 = 17.14% Medium = 11/35 = 31.42% High = 17/35 = 48.57%

Mapping of Course Outcomes to Programme Specific Outcomes (PSOs)

	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	High	Medium	High	High	Medium
CO2	High	Medium	High	Low	Medium
CO3	Medium	High	Medium	High	Low
CO4	Medium	Low	Low	High	Medium
CO5	Low	Medium	Low	High	Medium
Correlation Levels: Low Medium High					

Low = 6/25 = 24.0% Medium = 10/25 = 40.00% High = 9/25 = 36.0 %