ALAGAPPA UNIVERSITY

(A State University Established in 1985)

Karaikudi - 630003. Tamil Nadu, India

2017 Accredited with A+ Grade By NAAC (CGPA : 3.64)

2018 MHRD Govt. of India UGC Graded as Category - I & Granted Autonomy

2018 MHRD Swachh Campus Rank : 4

2021 nirf National Institutional Ranking Framework Rank : 33

2021 QS University Rankings Asia Rank : 199

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

M.Sc., CYBER FORENSICS

REGULATIONS AND SYLLABUS

(For the candidates admitted from the Academic Year 2023 - 2024)

DEPARTMENT OF COMPUTER SCIENCE
M.Sc., Cyber Forensics

REGULATIONS AND SYLLABUS

[For the candidates admitted from the Academic Year 2023–2024onwards]

ALAGAPPAUNIVERSITY
(A State University Accredited with "A+" grade by NAAC (CGPA: 3.64) in the Third Cycle and Graded as Category-I University by MHRD-UGC)
Karaikudi-630003,TamilNadu.

The panel of Members-Broad Based Board of Studies

Chairperson: **Dr.T.MEYYAPPAN** Professor & Headi/c, Department of Computer Science Alagappa University, Karaikudi Teaching Experience:31years Research Experience:16years Area of Research: Big Data Analytics, Image Processing and Networks	
Subject Expert: (Online Mode) **Dr. M. Thangaraj** Professor & Head Department of Computer Science Madurai Kamaraj University, Madurai TeachingExperience:28years Research Experience:18years Area of Research: Big Data Analytics, Emotional Intelligence, Wireless Sensor Networks	
Subject Expert: **Dr.M. BALAMURUGAN** Professor, Department of Computer Science Bharathidasan University, Trichy Teaching Experience: 28 years Research Experience:16years Area of Research: Big Data Analytics, Computational Intelligence, Digital Image Processing	
Members: **1.Dr.A.PADMAPRIYA** Professor, Department of Computer Science, Alagappa University, Karaikudi Teaching Experience: 19 years Research Experience:15years Area of Research: Data Mining, Big Data Analytics, Information and Network Security, Communication Networks	
2.Dr.S.SANTHOSHKUMAR Assistant Professor, Department of Computer Science, Alagappa University, Karaikudi Teaching Experience:19years Research Experience:14years Area of Research: Data Mining, Machine Learning, Health Care Analytics, IoT	
Alumnus/Alumna: **Dr.S. Alagu** Assistant Professor Department of Information Technology Dr.Umayal Ramanathan College for Women, Karaikudi Teaching Experience:15years Research Experience: 10 years Area of Research: Data Mining, Big Data Analytics	

Ex-Officio Member: **Dr.V. SIVAKUMAR** The Director Curriculum Design & Development Cell, Alagappa University, Karaikudi	

ALAGAPPA UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE
Karaikudi-630003,Tamil Nadu.

REGULATIONS AND SYLLABUS-(CBCS-University Department)
[For the candidates admitted from the Academic Year 2023 – 2024 onwards]

Name of the Department	: Computer Science
Name of the Programme	: M.Sc., Cyber Forensics
Duration of the Programme	: Full Time (Two Years)

Choice-Based Credit System

A choice-Based Credit System is a flexible system of learning. This system allows students to gain knowledge at their own tempo. Students shall decide on electives from a wide range of elective courses offered by the University Departments in consultation with the Department committee. Students can undergo additional courses and acquire more than the required number of credits. They can also adopt an inter-disciplinary and intra-disciplinary approach to learning and make the best use of the expertise of available faculty.

Programme

"Programme" means a course of study leading to the award of a degree in a discipline.

Courses

'Course' is a component (apaper) of a programme. Each course offered by the Department is identified by a unique course code. A course contains lectures / tutorials / laboratory / seminar/ project/ practical training/ report writing / Viva-voce, etc or a combination of these, to meet the teaching and learning needs effectively.

Credits

The term "Credit" refers to the weightage given to a course, usually in relation to theinstructionalHoursassignedtoit.Normallyineachofthecourse'screditswillbeassigned on the basis of the number of lectures/tutorial/laboratory and other forms of learning required to complete the course contents in a 15-week schedule. One credit is equal to one hour of lecture per week. For laboratory/field work, one credit is equal to two Hours.

Semesters

An Academic year is divided into two **Semesters.** In each semester, courses are offered in 15 teaching weeks and 5 more weeks are devoted to conduct of examination and evaluation purposes. Each week has 30 working Hours spread over 5 days a week.

Medium of Instruction

English

Departmental committee

The Departmental Committee consists of the faculty of the Department. The Departmental Committee shall be responsible for admission to all the programmes offered by the Department including the conduct of entrance tests, verification of records, admission, and evaluation. The Departmental Committee determine the deliberation of courses and specifies the allocation of credits semester-wise andcourse-wise. For each course, it will also identify the number of credits for lectures,tutorials,practical,seminars etc.

The courses (Core/ Discipline Specific Elective / Non-Major Elective) are designed by teachers and approved by the Departmental Committees. Courses approved by the Departmental Committees shall be approved by the Board of Studies/ Broad Based Board of Studies. A teacher offering a course will also be responsible for maintaining attendance and performance sheets (CIA – I, CIA – II, assignments, and seminar) of all the students registered for the course. The Non-major elective programme, MOOCs coordinator and Internship Mentor are responsible for submitting the performance sheet to the Head of the department. The Head of the Department consolidates all such performance sheets of courses pertaining to the programmes offered by the department and forward the same to be Controller of Examinations.

Programme Educational Objectives-(PEO)

PEO-1	**Comprehensive Understanding:** Provide students with a comprehensive understanding of cyber forensics principles, techniques, and tools.
PEO-2	**Technical Proficiency:** Develop students' technical proficiency in conducting digital investigations, including data acquisition, preservation, analysis, and presentation.
PEO-3	**Legal and Ethical Compliance:** Familiarize students with the legal and ethical considerations surrounding cybercrime investigations, including chain of custody, privacy laws, and rules of evidence.
PEO-4	**Risk Management:** Enable students to identify, assess, and mitigate cyber security risks through effective forensic analysis and incident response strategies.
PEO-5	**Research and Innovation:** Foster students' research and innovation capabilities in the field of cyber forensics, encouraging them to contribute to advancements in theory and practice.
PEO-6	**Malware Analysis:** Familiarize students with methods for analyzing malware samples to understand their behavior, functionality, and impact on systems.
PEO-7	**Digital Evidence Collection:** Train students in methods for identifying, preserving, and collecting digital evidence from various sources, such as computers, mobile devices, networks, and cloud services.

PEO-8	**Forensic Tools and Techniques:** Introduce students to a variety of forensic tools and techniques used to analyze digital evidence, including forensic imaging, data recovery, file analysis, and memory forensics.
PEO-9	**Investigation Methodologies:** Teach students systematic approaches to conducting cyber investigations, including incident response procedures, evidence handling protocols, and chain of custody documentation.
PEO-10	**Network Forensics:** Provide instruction on how to analyze network traffic and logs to identify unauthorized access, malware infections, data exfiltration, and other suspicious activities.

Programme Specific Objectives-(PSO)

PSO-1	**Cybersecurity Fundamentals:** Ensure students grasp foundational concepts in cybersecurity, including network security, cryptography, malware analysis, and penetration testing.
PSO-2	**Case Studies and Practical Exercises:** Engage students in real-world case studies and hands-on exercises to apply forensic techniques and methodologies in simulated scenarios.
PSO-3	**Legal and Regulatory Frameworks:** Educate students about relevant laws, regulations, and standards governing cybercrime investigations, including those related to digital evidence admissibility and courtroom procedures.
PSO-4	**Timeline Analysis:** Train students to reconstruct timelines of events based on digital evidence, aiding in understanding the sequence of actions taken during an incident.
PSO-5	**Incident Response Management:** Equip students with the skills needed to respond to cybersecurity incidents promptly and effectively, including incident detection, containment, eradication, and recovery.

Programme Outcome-(PO)

PO-1	**Proficiency in Digital Forensic Tools:** Graduates should demonstrate proficiency in using a range of digital forensic tools and software for data acquisition, analysis, and reporting.
PO-2	**Ability to Conduct Forensic Investigations:** Graduates should be capable of conducting thorough forensic investigations into various types of cybercrimes, including hacking, data breaches, intellectual property theft, and fraud.
PO-3	**Understanding of Legal and Ethical Issues:** Graduates should possess a solid understanding of the legal and ethical issues surrounding cybercrime investigations and be able to apply this knowledge in practice.

PO-4	**Effective Communication Skills:** Graduates should be able to communicate their findings clearly and effectively to diverse stakeholders, including technical and non-technical audiences, both orally and in writing.
PO-5	**Continuous Learning and Adaptation:** Graduates should demonstrate a commitment to continuous learning and adaptation to keep pace with evolving cybersecurity threats, technologies, and best practices.
PO-6	**Technical Expertise in Forensic Tools and Techniques:** Students will gain technical expertise in using a variety of forensic tools and techniques for analyzing digital evidence, including forensic imaging, file system analysis, memory forensics, and network packet analysis.
PO-7	**Malware Analysis and Threat Intelligence:** Students will be able to analyze malware samples to understand their behavior and impact on systems, as well as leverage cyber threat intelligence sources to enhance incident response efforts
PO-8	**Documentation and Reporting Abilities:** Students will be able to document forensic findings in clear, concise, and well-structured reports suitable for legal and investigative purposes, ensuring the integrity and admissibility of evidence in court proceedings.
PO-9	**Critical Thinking and Problem-Solving Skills:** Students will develop critical thinking and problem-solving skills necessary for analyzing complex cyber incidents, identifying root causes, and developing effective mitigation strategies.
PO-10	**Risk Assessment and Mitigation:** Students will gain the ability to assess cybersecurity risks, identify vulnerabilities, and implement appropriate controls and mitigation measures to protect digital assets and information systems.

Programme Specific Outcomes-(PSO)

PSO-1	Mastery of forensic investigation techniques for digital devices and networks.
PSO-2	Ability to analyze and interpret digital evidence within legal and ethical frameworks.
PSO-3	Proficiency in using advanced tools and technologies for cybercrime detection and prevention.
PSO-4	Understanding of cyber security principles and practices to mitigate vulnerabilities.
PSO-5	Development of critical thinking and problem-solving skills in cyber forensic investigations.

Eligibility for admission

Candidates for admission to the first year of the Master of Science in Cyber Forensics [M.Sc. (Cyber Forensics) programme is required to pass in any one of the following Examinations of any recognized University with a minimum of 55% marks in Part-III (minimum 50% marks for SC/STcandidates):
B.Sc. Computer Science /Information Technology / Cyber Forensics / Cyber Security /Software / Data Science / Artificial Intelligence / B.C.A. / B. Voc(Software Development) / B. Sc Forensics (with +2 level Mathematics) / or any other qualification equivalent thereto in10+2+3 pattern (with a minimum of 55% marks in Part-III for others and 50% marks for SC/ST candidates)

Minimum Duration of programme

The programme is for a period of two years. Each year shall consist of two semesters viz. Odd and Even semesters. Odd semesters shall be from June /July to October / November and even semesters shall be from November /December to April / May. Each semester there shall be 90 working daysconsistingof6teachingHours per working day (5days/week).

Components

A PG programme consists of a number of courses. The term "course" is applied to indicate a logical part of the subject matter of the programme and is in variably equivalent to the subject matter of a "paper" in the conventional sense. The following are the various categories of the courses suggested for the PG programmes:

A. Core courses (CC)– "Core Papers" means "the core courses" related to the programme concerned including practicals and project work offered under the programme and shall cover core competency, critical thinking, analytical reasoning, and research skill.

B. Discipline-Specific Electives –(DSE) means the courses offered under the programme related to the major but are to be selected by the students, shall cover additional academic knowledge, critical thinking, and analytical reasoning.

C. Non-Major Electives(NME)–Exposure beyond the discipline

- Students have to undergo a total of two Non Major Elective courses with 2 credits offered by other departments (one in II Semester another in III Semester).
- A uniform time frame of 3 Hours on a common day (Tuesday) shall be allocated for the Non-Major Electives.
- Non-Major Elective courses offered by the departments pertaining to a semester should be announced before the end of previous semester.
- Registration process: Students must register for the Non-Major Elective course within 15days from the commencement of the semester either in the department or NME Portal (University website).

D. Self Learning Courses from MOOCs platforms.

- MOOCs shall be on voluntary for the students.
- Students have to undergo a total of 2 Self Learning Courses

(MOOCs) one in II semester and another in III semester.

- The actual credits earned through MOOCs shall be transferred to the credit plan of programmes as extra credits. Otherwise, 2 credits/course be given if the self Learning Course (MOOCs) is without credit. While selecting the MOOCs, preference shall be given to the course related to employability skills.
- While selecting the MOOCs, preference shall be given to the course related to employability skills.

E. Projects/Dissertation/Internships(MaximumMarks:200)

The student shall undertake the Project/ Dissertation/ internship during the fourth semester.

Project/Dissertation

The candidate shall undergo Project/ Dissertation Work during the final semester. The candidate should prepare a scheme of work for the dissertation/project and should get approval from the guide. The candidate, after completing the dissertation /project work, shall be allowed to submit it to the university departments at the end of the final semester. If the candidate is desirous of availing the facility from other departments /universities /laboratories/ organizations, they will be permitted only after getting approval from the guide and HOD. In such a case, the candidate shall acknowledge the same in their dissertation/project work.

Internship

The students who have opted for an Internship must undergo industrial training in the reputed organizations to accrue industrial knowledge in the final semester. The student must find industry related to their discipline (Public limited/ Private Limited /owner /NGOsetc.,) in consultation with the faculty in charge/Mentor and get approval from the head of the department and Departmental Committee before going for an internship.

Project/Dissertation/Internship format details are given in

Annexure-I

Teaching methods

Teaching method includes chalk and talk, ICT tools such as Power Point Presentation, Interactive board, online live lectures and web resources.

Attendance

Students must have earned 75% of attendance in each course to appear in the examination. Students who have earned 74% to 70% of attendance need to apply for condonation in the prescribed form with the prescribed fee. Students who have earned 69% to 60% of attendance need to apply for condonation in the prescribed form with the prescribed fee along with the Medical Certificate. Students who have below 60% of attendance are not eligible to appear for the End Semester Examination (ESE). They shall re- do the semester(s) after completion of the programme.

Examination

The examinations shall be conducted separately for theory and practical's to assess (remembering, understanding, applying, analysing, evaluating, and creating) the knowledge required during the study. There shall be two systems of examinations viz., internal and external examinations. The internal examinations shall be conducted as Continuous Internal Assessment tests I and II (CIA Test I&II).

A)Internal Assessment

The internal assessment shall comprise a maximum of 25 marks for each subject. The following procedure shall be followed for awarding internal marks.

Theory-25marks

Sr.No.	Content	Marks
1	Average marks of two CIA test	15
2	Seminar/group discussion/quiz	5
3	Assignment/field trip report/case study report	5
	Total	25

Practical-25Marks

1	Major Experiment	10marks
2	Minor Experiment	5marks
3	Spotter(2x5/4x4) or any other mode	10marks
	Total	25Marks

Project/Dissertation/Internship–50 Marks (assessed by Guide /incharge /HOD/ Supervisor)

1	Two presentations(mid-term)	30Marks
2	Progress report	20Marks
	Total	50Marks

B. External Examination

- There shall be examinations at the end of each semester, for odd semesters in the month of October / November; for even semesters in April /May.
- A candidate who does not pass the examination in any course(s) may be permitted to appear in such failed course(s) in the subsequent examinations to be held in October /November or April/ May. However, candidates who have arrears in Practical shall be permitted to take their arrear Practical examination only along with Regular Practical examination in the respective semester.
- A candidate should get registered for the first semester examination. If registration is not possible owing to shortage of attendance beyond condonation limit / regulation prescribed OR belated joining OR on medical grounds, the candidates are permitted to move to the next semester. Such candidates shall re-do the missed semester after completion of the programme.
- For the Project Report/ Dissertation Work/ internship the maximum marks will be100 marks for project report evaluation and for the Viva-Voce it is 50 marks (if in some programmes, if the project is equivalent to more than one course, the project marks would be in proportion to the number of equivalent courses).
- Viva-Voce: Each candidate shall be required to appear for Viva-Voce Examination (in defense of the Dissertation Work/ Project /Internship).

C) Scheme of External Examination (Question Paper Pattern)

Theory-Maximum75Marks

Section A	10questions.Allquestionscarryequalmarks.(Objective type questions)	10x1=10 Marks	10 questions – 2each from every unit
Section B	5questionsEither/or type like 1.a (or) b. All questions carry equal marks	5x5=25	5 questions – 1eachfromevery unit
Section C	5questionsEither/or type like 1.a (or) b. All questions carry equal marks,	5x8=40	5 questions – 1eachfromev eryunit

Practical–Maximum75Marks

Section A	Aim, procedure/Algorithm and Program(2Nos.)	20Marks
Section B	Coding and Compilation	20Marks
Section C	Debugging and Output	20Marks
Section D	Record work	5Marks
Section E	Vivo voce	10Marks

Dissertation/Project report/Internship report Scheme of evaluation

Dissertation/Projectreport/Internship report	100Marks
Vivo voce	50Marks

Results

The results of all the examinations will be published through the Department where the student underwent the course as well as through University Website

Passing minimum

- A candidate shall be declared to have passed in each course if he/she secures not less than 40% marks in the End Semester Examinations and 40% marks in the Internal Assessment and not less than 50% in the aggregate, taking Continuous assessment and End Semester Examinations marks together.
- The candidates not obtained 50% in the Internal Assessment are permitted to improve their Internal Assessment marks in the subsequent semesters (2 chances will be given) by writing the CIA tests and by submitting assignments.
- Candidates, who have secured the pass marks in the End-Semester Examination and in the CIA but failed to secure the aggregate minimum pass mark (E.S.E + C I.A), are permitted toimprovetheirInternalAssessmentmarkinthefollowingsemesterand/orinUniversity examinations.
- A candidate shall be declared to have passed in the Project /Dissertation / Internship if he /she gets not less than 40% ineach of the Project / Dissertation / Internship Report and Viva-Voce and not less than 50% in the aggregate of both the marks for Project Report and Viva-Voce.
- Acandidatewhogetslessthan50%intheProject/Dissertation/Internship Report must resubmit the thesis. Such candidates need to take again the Viva-Voce on the resubmitted Project report.

Grading of the Courses

The following table gives the marks, Grade points, Letter Grades and classifications meant to indicate the overall academic performance of the candidate.
Conversion of Marks to Grade Points and Letter Grade (Performance in Paper/Course)

RANGE OF MARKS	GRADE POINTS	LETTER GRADE	DESCRIPTION
90-100	**9.0–10.0**	**O**	**Outstanding**
80-89	**8.0–8.9**	**D+**	**Excellent**
75-79	**7.5–7.9**	**D**	**Distinction**
70-74	**7.0–7.4**	**A+**	**VeryGood**
60-69	**6.0–6.9**	**A**	**Good**
50-59	**5.0–5.9**	**B**	**Average**
00-49	**0.0**	**U**	**Re-appear**
ABSENT	**0.0**	**AA A**	**ABSENT**

a) Successful candidates passing the examinations and earning GPA between 9.0 and 10.0 and marks from 90–100 shall be declared to have Outstanding(O).
b) Successful candidates passing the examinations and earning GPA between 8.0 and 8.9 and marks from 80- 89 shall be declared to have Excellent(D+).
c) Successful candidates passing the examinations and earning GPAbetween7.5–7.9 and marks from 75-79 shall be declared to have Distinction(D).
d) Successful candidates passing the examinations and earning GPA between7.0–7.4 and marks from 70- 74 shall be declared to have Very Good (A+).
e) SuccessfulcandidatespassingtheexaminationsandearningGPAbetween6.0–6.9andmarksfrom 60- 69shallbedeclared tohaveGood(A).
f) SuccessfulcandidatespassingtheexaminationsandearningGPAbetween5.0–5.9andmarksfrom 50- 59shallbedeclaredtohaveAverage(B).
g) CandidatesearningGPAbetween0.0andmarksfrom00-49shallbedeclaredtohaveRe-appear(U).
h) Absence from an examination shall not be taken as an attempt.

From the second semester onwards the total performance within a semester and continuous performance starting from the first semester are indicated respectively **by Grade Point Average (GPA) and Cumulative Grade Point Average(CGPA).**

These two are calculated by the following formulate

GRADEPOINTAVERAGE (GPA) =□iCiGi/□iCi

GPA = Sum of the multiplication of Grade Points by the credits of the courses
Sum of the credits of the courses in a Semester

Classification of the final result

CGPA	Grade	Classification of Final Result
9.5 – 10.0 9.0and abovebutbelow9.5	**O+** **O**	First Class–Exemplary*
8.5and abovebut below9.0 8.0and abovebut below8.5 7.5and abovebut below8.0	**D++** **D+** **D**	First Class with Distinction*
7.0and abovebut below7.5 6.5and abovebut below7.0 6.0and abovebut below6.5	**A++** **A+** **A**	First Class
5.5andabovebut below6.0 5.0and abovebut below5.5	**B+** **B**	Second Class
0.0and abovebutbelow5.0	**U**	Re-appear

The final result of the candidate shall be based only on the CGPA earned by the candidate.

a) Successfulcandidatespassingtheexaminationsandearning CGPAbetween9.5and 10.0 shall be given Letter Grade (O+), those who earned CGPA between 9.0 and 9.4shallbegivenLetter Grade(O)and declared to have Firs Class–Exemplary*.
b) Successful candidates passing the examinations and earning CGPA between 7.5 and 7.9shall be given Letter Grade (D), those who earned CGPA between 8.0 and 8.4 shall be given Letter Grade (D+), those who earned CGPA between 8.5 and 8.9 shall be given Letter Grade(D++) and declared to have First Class with Distinction*.
c) Successful candidates passing the examinations and earning CGPA between 6.0 and 6.4shall be given Letter Grade (A), those who earned CGPA between 6.5 and 6.9 shall be given Letter Grade (A+), those who earned CGPA between 7.0 and 7.4 shall be given Letter Grade(A++) and declared to have First Class.
d) Successful candidates passing the examinations and earning CGPA between 5.0 and 5.4shall be given Letter Grade (B), those who earned CGPA between 5.5 and 5.9 shall be given Letter Grade (B+) and declared to have passed in Second Class.

i)Candidates those who earned CGPA between 0.0 and4.9shallbe given Letter Grade (U) and declared to have Re-appear.

e) Absence from an examination shall not be taken as an attempt.

CUMULATIVEGRADEPOINTAVERAGE (CGPA)= $\sum_{i}^{n} C_{ni} G_{ni} / \sum_{i}^{n} C_{ni}$

CGPA = $\frac{\text{Sum of the multiplication of Grade Points by the credits of the entire Programme}}{\text{Sum of the credits of the courses for the entire Programme}}$

Where '**Ci**' is the Credit earned for Course i in any semester; '**Gi**' is the Grade Point obtained by the student for Course i and 'n' refers to the semester in which such courses were credited.

CGPA (Cumulative Grade Point Average) = Average Grade Point of all the Courses passed starting from the first semester to the current semester.

Note: * The candidates who have passed in the first appearance and withintheprescribedSemestersofthePGProgrammearealoneeligibleforthisclassification
ANNEXURE –I

- **No.of copies of the dissertation/ project report /internship report**

The candidate should prepare three copies of the dissertation/project/report and submit the same for the evaluation of examiners. After evaluation, one copy will be retained in the department library, one copy will be retained by the guide and the student shall hold one copy.

- **Format to be followed for dissertation/project report**

Theformat/certificateforthesistobefollowedbythestudentaregivenbelow

- Title page
- Certificate
- Acknowledgment
- Content as follows:

Chapter No	Title	Pagenumber
1	Introduction	
2	Aim and objectives	
3	Review of literature	
4	Materials and methods	
5	Result	
6	Discussion	
7	Summary	
8	References	

Format of the title page

Title of Dissertation/Projectwork

Dissertation/Project submitted in partial fulfilment of the requirement for thedegreeofMasterofSciencetotheAlagappaUniversity,Karaikudi-630003.

By

(Student Name)

(Register Number)

University Logo

Department of----------

Alagappa University

(A State University Accredited with "A+" grade by NAAC (CGPA: 3.64) in the Third Cycle and Graded as Category-I University by MHRD-UGC, 2019: QS ASIA Rank-216,QS BRICSRank-104,QSIndiaRank-20)

Karaikudi -

630003(Year)

Format of certificates
Certificate-Guide

This is to certify that the **Dissertation/Project** entitled"----------
----------" submitted to Alagappa University, Karaikudi-630 003 in partial fulfilment forthedegreeof Masterof Science in----------byMr/Mis----------(RegNo ----------) under my supervision. This is based on the results of studies carried out by him/her inthe Department of----------, Alagappa University, Karaikudi-630 003. This dissertation/Project or any part of this work has not been submitted elsewhere for any other degree, diploma, fellowship, or any other similar titles or record of any University or Institution.

Place:
KaraikudiDate:__
ResearchSupervisor

Certificate-(HOD)

This is to certify that the thesis entitled**"----------"**
Submitted by Mr/Mis----------(RegNo:----------)to the Alagappa University,
in partial fulfillment for the award of the degree of Master of----------in----------
is a bonafide record of research work done under the supervision of Dr---------- ,
*<<Designation>>,*Department of----------, Alagappa
University. This is to further certify that the thesis or any part thereof has not formed the basis of the award to the student of any degree, diploma, fellowship, or any other similar title of any University or Institution.

Place:Karaikudi HeadoftheDepartment
Date:

Declaration (student)

I hereby declare that the dissertation entitled**"----------"**
Submitted to the Alagappa University for the award of the degree of Master of--------in------
------- has been carried out by me under the guidance of Dr. ---------- , *<<Designation>>*,Department of , Alagappa University, Karaikudi – 630 003.This is my original and independent work and has not previously formed the basis of the award of any degree, diploma, associateship, fellowship, or any other similar title of any University or Institution.

Place:Karaikudi **(----------)**
Date:

Internship

- **Format to be followed for Internship report**

The format /certificate for internship report to be followed by the student aregiven below

- Acknowledgment
- Content as follows:

Chapter No	Title	Page number
1	Introduction	
2	Aim and objectives	
3	Organisation profile/details	
4	Methods/Work	
5	Observation and knowledge gained	
6	Summary and outcome of the Internship study	
7	References	

- Title page-**Format of the title page**

Title of internship report

Internship report submitted in partial fulfilment of
the requirement for the Master of degree into the
AlagappaUniversity,Karaikudi-630003.

By

(Student Name)

(Register Number)

University Logo

Department of----------

Alagappa University

(A State University Accredited with "A+" grade by NAAC (CGPA: 3.64) in the ThirdCycle and Graded as Category-I University by MHRD-UGC, 2019: QS ASIA Rank-216,QS BRICSRank-104,QSIndiaRank-20)

Karaikudi -
630003(Year)

Certificate-(**Format of certificate–faculty in-charge)**

This is to certify that the report entitled“ ---------- ” submitted to Alagappa University, Karaikudi-630 003 in partial fulfilment for the Master of Science in----------byMr/Mis----------(RegNo----------) under my supervision. This is based on the work carried out by him/her in the organization M/S --. This Internship report or any part of this work has not been submitted elsewhere for any other degree, diploma, fellowship, or any other similar record of any University or Institution.

Place: ResearchSupervisor
Date:

Certificate(HOD)

This is to certify that the Internship report entitled**“ ---------- ”** Submitted by Mr/Mis**.----------(RegNo ----------)** to the Alagappa University, in Partial fulfillment for the award of the Master of Science in ---------- is a bonafide record of Internship report done under the supervision of ----------,<<Designation>>,Department of ----------, Alagappa University and the work carried out by him/her in the organization M/S ----------. This is to further certify that the thesis or any part there of has not formed the basis of the award to the student of any degree, diploma, fellowship, or anyother similar title of any University or Institution.

Place:Karaikudi Head of the Department
Date:

Certificate-(**Format of certificate – Company supervisor or Head of the Organization)**

This is to certify that the Internship report entitled“----------”submitted to Alagappa University,Karaikudi-630003 in partial fulfillment for the Master of Science in----------by Mr/Mis----------(RegNo----------)under my supervision. This is based on the work carried out by him/her in our organization M/S----------for the period of three months or-------- --.This Internship report or any Part of this work has not been submitted elsewhere for any other degree, diploma, fellowship, or any other similar record of any University or Institution.

Place: Supervisor or incharge
Date:

Declaration (student)

I hereby declare that the Internship Report entitled**"----------"** Submitted to the Alagappa University for the award of the **Master of Science in----------**has Been carried out by me under the supervision of---------- ,Designation, Department of , Alagappa University,Karaikudi–630003.This is my original and independent work carried out by me in the organization M/S ---------- for the period of three months or---------- and has not previously formed the basis of the award of any degree, diploma, associateship, fellowship, or any other similar title of any University or Institution.

Place: Karaikudi
Date:_____

(----------)

Maximum duration of the completion of the programme

The maximum period for completion of **M.Sc.,** in **CYBER FORENSICS** shall not exceed eight semesters continuing from the first semester.

Conferment of the Master's Degree

A candidate shall be eligible for the conferment of the Degree only after he/she has earned the minimum required credits for the Programme prescribed there for (i.e. 90credits) Programme).

Village Extension Programme

The Sivaganga and Ramnad districts are very backward districts where most people Lives in poverty.

The rural mass is economically and educationally backward. Thus, the aim of the introduction of this Village Extension Programme is to extend out to reach environmental awareness, social activities, hygiene, and health to the rural people of this region. The students in their third semester must visit any one of the adopted villages within the jurisdiction of Alagappa University and can arrange various programs to educate the rural mass in the following areas for threedays based on the theme.1. Environmental awareness 2. Hygiene and Health. A minimum of two faculty members can accompany the students and guide them.

M.Sc., Cyber Forensics

S. No.	Paper Code	Courses	Title of the paper	T/P	Credits	Hours/ Week	Marks		
			I Semester				**I**	**E**	**Total**
1	556101	Core	Introduction to cyber forensics	T	4	4	25	75	100
2	556102	Core	Cyber crime issues and investigation	T	4	4	25	75	100
3	556103	Core	Advanced database Security	T	4	4	25	75	100
4	556104	Core	Cryptography and network security	T	4	4	25	75	100
5	556105	Core	Web and Information Security	T	4	4	25	75	100
6	556106	Core	Cryptography & Network Security Lab	P	2	3	25	75	100
7	556107	Core	Data Security Lab	P	2	3	25	75	100
			Elective Paper						
8	556501	DSE	Frauds and counter measures	T	3	3	25	75	100
	556502	DSE	Analysis of Algorithms in Forensics Science						
	556503	DSE	Advanced Software Engineering						
			Library/Yoga/Counseling/Fieldtrip	-		1			
			Total	--	**27**	**30**	**200**	**600**	**800**
			II Semester						
9	556201	Core	Distributed Operating System In Cyber Space	T	4	4	25	75	100
10	556202	Core	Python Programming	T	4	5	25	75	100
11	556203	Core	Python Programming Lab	P	2	3	25	75	100
12	556204	Core	ML For Digital Forensic	T	4	5	25	75	100
13	556205	Core	ML For Digital Forensic Lab	P	2	3	25	75	100
14	556206	Core	Digital Signatures	T	4	4	25	75	100
		NME	Non-Major Elective **		2	3	25	75	100
			Elective Paper						
15	556504	DSE	Cloud Environment and Forensics	T	3	3	25	75	100
	556505	DSE	Wireless Network Security						
	556506	DSE	WAP and XML						
			Total	--	**25**	**30**	**175**	**525**	**700**
			III Semester						
16	556301	Core	Ethical Hacking	T	4	5	25	75	100
17	556302	Core	Behavioral Biometrics	T	4	4	25	75	100
18	556303	Core	Ethical Hacking Lab	P	2	3	25	75	100
19	556304	Core	Mini Project		2	3	25	75	100
20	556305	Core	Cyber Law Policies and IT Act	T	4	5	25	75	100
21	556306	Core	Social Media Forensics	T	4	4	25	75	100
		NME	Non-Major Elective **		2	3	25	75	100
			Elective Paper						
22	556507	DSE	Data Analytics and Privacy	T	3	3	25	75	100
	556508	DSE	IOT and Digital Forensics						
	556509	DSE	Security Standards and Compliance						
			Total	--	**25**	**30**	**175**	**525**	**700**

		IV Semester							
			Option – I						
23	556401	Core	Reverse Engineering and Malware Analysis	T	2	2	25	75	100
24	556402	Core	Project Work	-	12	-	50	150	200
			Total	--	**14**		**150**	**150**	**300**
			Overall Total	---	**91**				**2500**

I – Semester					
Core	**556101**	**Introduction to Cyber Forensics**	**T**	**Credits:4**	**Hours:4**

Unit– I		
Objective 1	To Understand an Overview of cyber security	
CYBER CRIME INTRODUCTION: Networks and Network Security - Introduction to Cybercrime		
Outcome 1	Recognize the role of digital evidence in cyber forensic investigations and understand its collection, preservation, and analysis.	**K2**
Unit– II		
Objective 2	To Understand an basic idea about cyber forensics	
CYBER CRIME CLASSIFICATION: Classification of Cybercrime - Cybercrime—The Present and the Future		
Outcome 2	Apply appropriate techniques for acquiring and handling digital evidence while adhering to legal and ethical standards.	**K2**
Unit– III		
Objective 3	To Understand an overview of forensics science and its applications	
DATABASE SECURITY: Introduction to Cyber Forensics - Digital Evidence - Cyber Forensics		
Outcome 3	Utilize analytical tools and methodologies to examine and interpret digital evidence effectively.	**K3**
Unit–IV		
Objective 4	To provide students with a comprehensive understanding of cybercrimes, cyber forensics, and the techniques involved in acquiring, handling, and analyzing digital evidence	
DIGITAL EVIDENCE: Acquisition and Handling of Digital Evidence - Analysis of Digital Evidence		
Outcome 4	Evaluate the admissibility of digital evidence in legal proceedings and understand the challenges associated with its presentation.	**K4**
Unit–V		
Objective 5	Students will be equipped with the knowledge and skills necessary to investigate and mitigate cybercrimes effectively.	
CASE STUDIES: Admissibility of Digital Evidence - Cybercrime Case Studies		
Outcome 5	Provide guidance on presenting technical findings in a clear and understandable manner for legal proceedings	**K5**

Suggested Readings:

Cyber Forensics, Dejey and S.Murugan, Oxford University Press 2018
(Unit 1 to 5)

A Practical Guide to Computer Forensics Investigations, Dr. Darren R. Hayes, Pearson Education, Inc. ISBN-13: 978-0-7897-4115-8, ISBN-10: 0-7897-4115-6.2015

Online Resources

https://www.cybrary.it/

https://digitalforensicsmagazine.com/

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

Course designed by: Dr.S. Santhosh kumar

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M (2)	S (3)	M (2)	L (1)	S (3)	S (3)	S (3)	L (1)	L (1)	M (2)
CO2	L (1)	M (2)	S (3)	M (2)	S (3)	M (2)	L (1)	M (2)	L (1)	S (3)
CO3	S (3)	L (1)	M (2)	S (3)	M (2)	L (1)	M (2)	S (3)	M (2)	L (1)
CO4	M (2)	M (2)	L (1)	M (2)	L (1)	-	S (3)	M (2)	S (3)	M (2)
CO5	M (2)	L (1)	S (3)	L (1)	M (2)	M (2)	M (2)	L (1)	M (2)	M (2)
W.AV	**1.8**	**1.6**	**2**	**1.8**	**2**	**1.4**	**2**	**1.6**	**1.6**	**1.8**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	S (3)	L (1)	L (1)	M (2)
CO2	M (2)	M (2)	L (1)	S (3)	M (2)
CO3	M (2)	M (2)	M (2)	L (1)	L (1)
CO4	L (1)	M (2)	M (2)	S (3)	M (2)
CO5	L (1)	M (2)	M (2)	S (3)	M (2)
W.AV	**1.6**	**2**	**1.4**	**2**	**1.6**

S –Strong (3), M-Medium (2), L- Low (1)

I - Semester					
Core	**556102**	**Cyber crime Issues and Investigation**	**T**	**Credits:4**	**Hours:4**

Unit– I		
Objective 1	To equip students with a comprehensive understanding of cybercrime, investigative techniques, and legal considerations involved in cybercrime investigations.	
The Problem at Hand - Computer Crime Discussed		
Outcome 1	Demonstrate a comprehensive understanding of computer crimes and their impact and understand the roles and responsibilities of cyber investigative professionals and the process of preparing for prosecution and testifying in court.	**K3**
Unit– II		
Objective 2	Students will have the knowledge and skills necessary to effectively investigate cybercrimes and contribute to the prosecution of cybercriminals.	
Preparing for Prosecution and Testifying - Cyber Investigative Roles		
Outcome 2	Apply incident response techniques, including live forensics and investigations, to effectively respond to cyber incidents and gather digital evidence.	**K2**
Unit– III		
Objective 3	Develop incident response plans and simulate real-world scenarios.	
Incident Response: Live Forensics and Investigations - Legal Issues of Intercepting WiFi Transmissions		
Outcome 3	Student evaluate the legal and ethical considerations surrounding the interception of WiFi transmissions in cybercrime investigations	**K4**
Unit–IV		
Objective 4	Understand the role of digital evidence in cybercrime investigations	
Conducting Cyber Investigations - Communication device-based Investigation - Mobile Forensics		
Outcome 4	Analyze financial frauds and other types of cybercrimes through case studies to understand investigative techniques, challenges, and outcomes.	**K5**
Unit–V		
Objective 5	Explore cybercrimes related to financial fraud, including phishing and ransomware.	
Investigation of Financial Frauds & cybercrimes – case studies		
Outcome 5	Understand the financial motivations behind cybercriminal activities	**K6**

Suggested Readings:

Anthony Reyes, Kevin O'Shea, Jim Steele, Jon R. Hansen, Captain Benjamin, R. Jean Thomas Ralph (Chapter 1-6 covers unit 1,2,3)

Cybercrime Investigation Handbook For Police Officers, Ministry of Home Affairs, India 2018 (Chapter 3,4,5,6,7,10 covers unit 3,4,5)

Online Resources

https://www.fbi.gov/investigate/cyber

https://www.ncsc.gov.uk/

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

Course designed by: Dr.S.Santhoshkumar

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	S (3)	M (2)	L (1)	S (3)	M (2)	S (3)	L (1)	L (1)	M (2)
CO2	M (2)	M (2)	S (3)	M (2)	S (3)	L (1)	L (1)	L (1)	M (2)	S (3)
CO3	L (1)	L (1)	M (2)	S (3)	M (2)	S (3)	M (2)	M (2)	S (3)	L (1)
CO4	M (2)	-	L (1)	M (2)	L (1)	M (2)	S (3)	S (3)	M (2)	M (2)
CO5	L (1)	M (2)	S (3)	L (1)	M (2)	M (2)	M (2)	M (2)	L (1)	M (2)
W.AV	**1.6**	**1.4**	**2**	**1.8**	**2**	**1.8**	**2**	**1.6**	**1.6**	**1.8**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	M (2)	L (1)	S (3)	L (1)
CO2	M (2)	M (2)	L (1)	M (2)	S (3)
CO3	M (2)	L (1)	M (2)	M (2)	L (1)
CO4	L (1)	M (2)	M (2)	M (2)	S (3)
CO5	L (1)	M (2)	M (2)	M (2)	S (3)
W.AV	**1.6**	**1.6**	**1.4**	**2**	**2**

S –Strong (3), M-Medium (2), L- Low (1)

I - Semester					
Core	**556103**	**Advanced Database Security**	**T**	**Credits:4**	**Hours:4**

Unit– I		
Objective 1	Define the fundamental principles of database security	
WEB SECURITY: The Web Security Problem, Risk Analysis and Best Practices Cryptography and the Web: Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification.		
Outcome 1	Understand the Web architecture and application	**K2**
Unit– II		
Objective 2	Examine advanced access control models for databases	
WEB PRIVACY: The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Antitheft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration.		
Outcome 2	Understand client side and service side programming	**K2**
Unit– III		
Objective 3	Develop and enforce database security policies and procedures	
DATABASE SECURITY: Recent Advances in Access Control, Auditing, Authentication, Integrity controls, Backups, Access Control Models for XML, Database Issues in Trust Management and Trust Negotiation, Security in Data Warehouses and OLAP Systems		
Outcome 3	Analyze how common mistakes can be bypassed and exploit the application	**K4**
Unit–IV		
Objective 4	To Understand an Overview of information security	
SECURITY RE-ENGINEERING FOR DATABASES: Security Re-engineering for Databases Concepts and Techniques, Database Watermarking for Copyright Protection, Trustworthy Records Retention, Damage Quarantine and Recovery in Data Processing Systems, Hippocratic Databases: Current Capabilities.		
Outcome 4	Evaluate the common application vulnerabilities	**K5**
Unit–V		
Objective 5	To Understand an overview of Access control of relational databases	
FUTURE TRENDS PRIVACY IN DATABASE PUBLISHING: A Bayesian Perspective, Privacy-enhanced Location-based Access Control, Database driven websites Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment.		
Outcome 5	Understand and comply with industry-specific and regulatory security standards	**K5**

Suggested Readings:

Web Security, Privacy and Commerce, Simson G. Arfinkel, Gene Spafford, O' Reilly

Handbook on Database security applications and trends, Michael Gertz, Sushil Jajodia

"Web applications security" By Andrew Hoffman, O'Reilly

"Database and Applications Security" Bhavani Thuraisingham, Auerbach Publications

Online Resources https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/index.html#Oracle%C2%AE-Database https://learn.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server?view=sql-server-ver16					
K1-Remember	***K2-Understand***	***K3-Apply***	***K4-Analyze***	***K5-Evaluate***	***K6-Create***
Coursedesignedby: Dr.S.Santhoshkumar					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M (2)	L (1)	M (2)	L (1)	M (2)	S (3)	S (3)	S (3)	L (1)	S (3)
CO2	S (3)	M (2)	S (3)	L (1)	L (1)	S (3)	L (1)	M (2)	M (2)	M (2)
CO3	L (1)	S (3)	M (2)	M (2)	S (3)	M (2)	M (2)	L (1)	S (3)	L (1)
CO4	M (2)	M (2)	L (1)	S (3)	M (2)	L (1)	S (3)	-	M (2)	M (2)
CO5	M (2)	L (1)	S (3)	M (2)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)
W.AV	**1.8**	**1.8**	**2**	**1.6**	**1.8**	**2**	**2**	**1.4**	**1.6**	**1.6**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	M (2)	S (3)	L (1)	L (1)
CO2	M (2)	M (2)	M (2)	L (1)	S (3)
CO3	M (2)	L (1)	M (2)	M (2)	L (1)
CO4	M (2)	M (2)	L (1)	M (2)	S (3)
CO5	M (2)	M (2)	L (1)	M (2)	S (3)
W.AV	**2**	**1.6**	**1.6**	**1.4**	**2**

S –Strong (3), M-Medium (2), L- Low (1)

I - Semester					
Core	**556104**	**Cryptography and Network security**	**T**	**Credits:4**	**Hours:4**

Unit– I		
Objective 1	Enable students to learn the Introduction to Cryptography, Web Security and Case studies in Cryptography.	
INTRODUCTION: Introduction to Cryptography – Security Attacks – Security Services –Security Algorithm- Stream cipher and Block cipher - Symmetric and Asymmetric-key Cryptosystem Symmetric Key Algorithms: Introduction – DES – Triple DES – AES – IDEA – Blowfish – RC5.		
Outcome 1	Understand the process of the cryptographic algorithms	**K2**
Unit– II		
Objective 2	To gain knowledge on classical encryption techniques and concepts of modular arithmetic and number theory.	
CRYPTOSYSTEM: Public-key Cryptosystem: Introduction to Number Theory – RSA Algorithm–Key Management -Diffie- Hellman Key exchange–Elliptic Curve Cryptography Message Authentication and Hash functions – Hash and Mac Algorithm – Digital Signatures and Authentication Protocol.		
Outcome 2	Compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication	**K1**
Unit– III		
Objective 3	To explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms.	
NETWORK SECURITY: Network Security Practice: Authentication Applications –Kerberos– X.509Authentication services and Encryption Techniques. E-mail Security – PGP – S / MIME – IP Security.		
Outcome 3	Apply and analyze appropriate security techniques to solve network security problem	**K4**
Unit–IV		
Objective 4	To explore the design issues and working principles of various authentication Applications and various secure communication standards including Kerberos, IPsec, and SSL/TLS and email	
Web Security-Secure Socket Layer–Secure Electronic Transaction. System Security- Intruders and Viruses – Firewalls– Password Security.		
Outcome 4	Explore suitable cryptographic algorithms	**K3**
Unit–V		
Objective 5	Analyze cryptographic techniques used in popular block chain platforms	
Case Study: Implementation of Cryptographic Algorithms–RSA–DSA–ECC(C/JAVA Programming). Network Forensic – Security Audit - Other Security Mechanism: Introduction to: Stenography – Quantum Cryptography – Water Marking - DNA Cryptography		
Outcome 5	Analyze different digital signature algorithms to achieve authentication and design secure applications	**K5**

Suggested Readings:

William Stallings, "Cryptography and Network Security", PHI/Pearson Education

Bruce Schneir, "Applied Cryptography", CRC Press

A.Menezes, P Van Oorschot and S.Vanstone, "Hand Book ofApplied Cryptography", CRC Press, 1997

AnkitFadia,"NetworkSecurity",MacMillan

Online Resources

https://www.crypto101.io/

https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity

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

Coursedesignedby: Dr.A. Padmapriya

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	S (3)	M (2)	L (1)	M (2)	S (3)	M (2)	L (1)	L (1)	S (3)
CO2	L (1)	M (2)	S (3)	L (1)	L (1)	S (3)	S (3)	M (2)	M (2)	M (2)
CO3	M (2)	L (1)	M (2)	M (2)	S (3)	M (2)	L (1)	S (3)	S (3)	L (1)
CO4	S (3)	-	L (1)	S (3)	M (2)	L (1)	M (2)	M (2)	M (2)	M (2)
CO5	M (2)	M (2)	S (3)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)	L (1)
W.AV	**2**	**1.4**	**2**	**1.6**	**1.8**	**2**	**1.8**	**1.8**	**1.6**	**1.6**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	L (1)	S (3)	M (2)	L (1)
CO2	M (2)	S (3)	M (2)	M (2)	L (1)
CO3	M (2)	L (1)	M (2)	L (1)	M (2)
CO4	M (2)	S (3)	L (1)	M (2)	M (2)
CO5	M (2)	S (3)	L (1)	M (2)	M (2)
W.AV	**2**	**2**	**1.6**	**1.6**	**1.4**

S –Strong (3), M-Medium (2), L- Low (1)

I - Semester					
Core	**556105**	**Web and Information Security**	**T**	**Credits:4**	**Hours: 4**

Unit– I		
Objective 1	To understand the fundamental functioning of security patterns.	
FOUNDATION OF SECURITY: Overview of Security, Security Taxonomy, General Security Resources, Security Patterns - The History of Security Patterns, Scope of Pattern Characteristics of Security Patterns, Sources for Security Pattern Mining and Types of Patterns		
Outcome 1	Understand the conceptual foundation of information security awareness.	**K2**
Unit– II		
Objective 2	To understand the security Attack and Preventions.	
SECURITY ATTACK: Malicious Attacks, Threats, and Vulnerabilities-Malicious Activity on the Rise - What Are You Trying to Protect? - Whom Are You Trying to Catch? - Attack Tools - Security Breach - Risks, Threats, and Vulnerabilities - Malicious Attack - Malicious Software - Common Types of Attacks – Countermeasure		
Outcome 2	Study the physical and logical perimeters of information assets and its security.	**K2**
Unit– III		
Objective 3	To understand the need for Authentication, Access controls, Security operations.	
SECURITY OPERATIONS AND ADMINISTRATION: Security Operations and Administration-Security Administration – Compliance - Professional Ethics - The Infrastructure for an IT Security Policy - Data Classification Standards - Configuration Management - The Change Management Process - Application Software Security - Software Development and Security		
Outcome 3	Analysis the risk events, treatment plans, assessment	**K4**
Unit–IV		
Objective 4	Implement secure coding practices to mitigate web application vulnerabilities	
WEB SECURITY: The Web Security Problem, Risk Analysis and Best Practices Cryptography and the Web: Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification.		
Outcome 4	Examining the access controls, monitoring, management, and review process	**K5**
Unit–V		
Objective 5	Explore authentication mechanisms for web applications	
WEB PRIVACY: The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Antitheft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration.		
Outcome 5	Detail evaluation of information classification, roles, and responsibilities	**K5**

Suggested Readings:

Bryan Sullivan and Vincent Liu, Web Application Security: A Beginner's Guide, ISBN-13: 978-0071776168, 2011

Michael Goodrich, Web Application Security: A Hands-On Approach, Addison-Wesley, ISBN-13: 978-0321701780, 2014

Online Resources https://krebsonsecurity.com/ https://www.coursera.org/courseraplus?utm_source=gg&utm_medium=sem&utm_campaign=B2C_India_FTCOF_Branded_ARTE_EXP&utm_content=B2C&campaignid=20590309416&adgroupid=155702724684&device=c&keyword=coursera&matchtype=e&network=g&devicemodel=&adpostion=&creativeid=675426312952&hide_mobile_promo&gad_source=1&gclid=CjwKCAiAloavBhBOEiwAbtAJO8oZZ7BmukTNRABzOC2Xjdko4_azr6e8GUCsD45KW7i0adyhT0idrRoCrd4QAvD_BwE					
K1-Remember	*K2-Understand*	*K3-Apply*	*K4-Analyze*	*K5-Evaluate*	*K6-Create*
Course designed by: Dr.A. Padmapriya					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	L (1)	M (2)	L (1)	M (2)	S (3)	M (2)	S (3)	L (1)	S (3)
CO2	L (1)	M (2)	S (3)	L (1)	L (1)	S (3)	S (3)	M (2)	M (2)	M (2)
CO3	M (2)	S (3)	M (2)	M (2)	S (3)	M (2)	L (1)	L (1)	S (3)	L (1)
CO4	S (3)	M (2)	L (1)	S (3)	M (2)	L (1)	M (2)	M (2)	M (2)	-
CO5	M (2)	L (1)	S (3)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)	M (2)
W.AV	**2**	**1.8**	**2**	**1.6**	**1.8**	**2**	**1.8**	**1.6**	**1.6**	**1.4**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	L (1)	S (3)	M (2)	L (1)
CO2	M (2)	S (3)	M (2)	M (2)	L (1)
CO3	M (2)	L (1)	M (2)	L (1)	M (2)
CO4	L (1)	S (3)	M (2)	M (2)	M (2)
CO5	L (1)	S (3)	M (2)	M (2)	M (2)
W.AV	**1.6**	**2**	**2**	**1.6**	**1.4**

S –Strong (3), M-Medium (2), L- Low (1)

I – Semester					
Core	**556106**	**Cryptography & Network Security LAB**	**P**	**Credits:2**	**Hours:3**

Objectives	➢ Learn the principles of various cryptographic algorithms, including symmetric and asymmetric encryption, hash functions, and digital signatures. ➢ Understand the mathematical foundations behind cryptographic algorithms. ➢ Gain hands-on experience in implementing encryption and decryption algorithms. ➢ Understand the importance of key management and secure key exchange.

1. Implementation of Caesar Cipher
2. Implementation of Hill Cipher
3. Implementation of Vigenere Cipher
4. Implementation of Rail Fence – Row & Column Transformation Technique
5. Implementation of Encryption and Decryption
6. Implementation of Diffie Hellman Key Exchange Algorithm
7. Implementation of DES Algorithm
8. Implementation of Blowfish Algorithm
9. Implementation of Rijndael Algorithm
10. Implementation of RSA Algorithm
11. Implementation of SHA-1 Algorithm
12. Implementation of MD5 Algorithm

Outcomes	➢ Students will demonstrate a clear understanding of the mathematical principles and algorithms behind common cryptographic techniques. ➢ Students will gain practical skills in implementing encryption and decryption processes and understand the challenges and considerations in key management. ➢ Students will be proficient in configuring and securing network communications using established protocols, emphasizing the importance of confidentiality and integrity.

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)
CO2	S(3)	M(2)	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	M(2)	S(3)
CO3	S(3)	L(1)	M(2)	M(2)	S(3)	M(2)	M(2)	L(1)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)	S(3)
W.AV	**2.6**	**2**	**1.8**	**1.6**	**2**	**1.6**	**2**	**2.2**	**2.2**	**2.2**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	L(1)	M(2)	S(3)
CO2	M(2)	L(1)	M(2)	M(2)	L(1)
CO3	M(2)	M(2)	M(2)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)
CO5	M(2)	L(1)	M(2)	S(3)	L(1)
W.AV	**2.4**	**1.6**	**1.6**	**1.8**	**1.8**

S –Strong (3), M-Medium (2), L- Low (1)

I – Semester					
Core	**556107**	**Data Security LAB**	**P**	**Credits:2**	**Hours:3**

Objectives	➢ Understand the fundamental principles of web application security. ➢ Learn about common vulnerabilities and attacks targeting web applications. ➢ Gain hands-on experience with security testing tools and techniques.

1. WHOIS LOOKUP
2. NSLOOKUP
3. WAPPALYZER
4. VIRUSTOTAL
5. DNS DURMPSTER
6. WIRESHARK

Outcomes	➢ Students will demonstrate a strong understanding of web application security concepts, including common vulnerabilities and threats. ➢ Students will be proficient in using security testing tools to identify and exploit vulnerabilities in web applications. ➢ Students will be able to apply secure coding practices to develop resilient and secure web applications.

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)
CO2	S(3)	M(2)	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	M(2)	S(3)
CO3	S(3)	L(1)	M(2)	M(2)	S(3)	M(2)	M(2)	L(1)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)	S(3)
W.AV	**2.6**	**2**	**1.8**	**1.6**	**2**	**1.6**	**2**	**2.2**	**2.2**	**2.2**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	L(1)	M(2)	S(3)
CO2	M(2)	L(1)	M(2)	M(2)	L(1)
CO3	M(2)	M(2)	M(2)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)
CO5	M(2)	L(1)	M(2)	S(3)	L(1)
W.AV	**2.4**	**1.6**	**1.6**	**1.8**	**1.8**

S –Strong (3), M-Medium (2), L- Low (1)

I - Semester					
DSE	**556501**	**Frauds and Counter Measures**	**T**	**Credits:3**	**Hours:3**

Unit– I		
Objective 1	To provide students with a comprehensive understanding of fraud, its impact on society, and the techniques involved in detecting, investigating, and preventing fraudulent activities.	
Fraud in Society - Understanding the Basics of Financial Accounting		
Outcome 1	Understand the nature and types of fraud prevalent in society and recognize the basics of financial accounting that contribute to fraudulent activities.	**K2**
Unit– II		
Objective 2	Students will possess the knowledge and skills necessary to identify potential fraud risks, conduct effective investigations, and implement countermeasures to mitigate fraud in various organizational settings.	
Forms of Entities - Fundamental Principles of Financial Analysis		
Outcome 2	Identify different forms of entities and apply fundamental principles of financial analysis to detect potential fraud indicators.	**K2**
Unit– III		
Objective 3	Analyze factors contributing to fraud vulnerabilities	
The Role of the Accounting Professional - – Business as a Victim - Business Villains		
Outcome 3	Comprehend the role of accounting professionals in fraud prevention, detection, and investigation, and analyze the vulnerabilities that make businesses susceptible to fraud.	**K4**
Unit–IV		
Objective 4	Analyze case studies to understand the mindset of fraudsters	
The Investigative Process - Interviewing Financially Sophisticated Witnesses - Proving Cases through Documentary Evidence		
Outcome 4	Apply the investigative process to fraud cases and utilize analysis tools specific to fraud investigations.	**K5**
Unit–V		
Objective 5	Understand the process of collecting and preserving evidence for legal proceedings	
Analysis Tools for Investigators - Inferential Analysis - – Documenting and Presenting the Case		
Outcome 5	Develop skills in conducting fraud investigations	**K5**

Suggested Readings:

1. Forensic Accounting and Fraud Investigation, Stephen Pineault, Frank Rudewicz, Michael Sheetz, Howard Silverstone, Copyright © 2012 by John Wiley & Sons, Inc. All rights reserved
2. The Finger print – source book, Eric H. Holder, Jr. Attorney General Laurie O. Robinson Assistant Attorney General John H. Laub Director, National Institute of Justice by U.S. Department of Justice Office of Justice Programs 810 Seventh Street N.W. Washington, DC 20531
3. Laboratory and Scientific Section United Nations Office on Drugs and Crime Vienna Guide for the development of forensic document examination capacity, UNITED NATIONS New York, 2010.

Online Resources https://fraud.org/ https://consumer.ftc.gov/					
K1-Remember	*K2-Understand*	*K3-Apply*	*K4-Analyze*	*K5-Evaluate*	*K6-Create*
Course designed by: Dr.T. Meyyappan					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	L (1)	M (2)	L (1)	M (2)	S (3)	M (2)	S (3)	L (1)	S (3)
CO2	M (2)	M (2)	S (3)	L (1)	L (1)	S (3)	S (3)	M (2)	M (2)	L (1)
CO3	L (1)	S (3)	M (2)	M (2)	S (3)	M (2)	L (1)	L (1)	S (3)	M (2)
CO4	-	M (2)	L (1)	S (3)	M (2)	L (1)	M (2)	M (2)	M (2)	S (3)
CO5	M (2)	L (1)	S (3)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)	M (2)
W.AV	**1.4**	**1.8**	**2**	**1.6**	**1.8**	**2**	**1.8**	**1.6**	**1.6**	**2**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	L (1)	S (3)	M (2)	L (1)
CO2	M (2)	S (3)	M (2)	M (2)	L (1)
CO3	M (2)	L (1)	M (2)	L (1)	M (2)
CO4	L (1)	S (3)	M (2)	M (2)	M (2)
CO5	L (1)	S (3)	M (2)	M (2)	M (2)
W.AV	**1.6**	**2**	**2**	**1.6**	**1.4**

S –Strong (3), M-Medium (2), L- Low (1)

I - Semester					
DSE	**556502**	**Analysis of Algorithms in Forensic Science**	**T**	**Credits:3**	**Hours:3**

Unit– I

Objective 1	Enable the students to learn the Elementary Data Structures and algorithms

INTRODUCTION: Algorithm Definition and Specification – Space complexity-Time Complexity-Asymptotic Notations - Elementary Data Structure: Stacks and Queues – Binary Tree - Binary Search Tree - Heap – Heapsort- Graph.

Outcome 1	Get knowledge about algorithms and determines their time complexity. Demonstrate specific search and sort algorithms using divide and conquer technique.	**K2**

Unit– II

Objective 2	Presents an introduction to the algorithms, their analysis and design

TRAVERSAL AND SEARCH TECHNIQUES: Basic Traversal And Search Techniques: Techniques for Binary Trees-Techniques for Graphs -Divide and Conquer: - General Method – Binary Search – Merge Sort – Quick Sort.

Outcome 2	Gain good understanding of Greedy method and its algorithm	**K2**

Unit– III

Objective 3	Discuss various methods like Basic Traversal And Search Techniques, divide and conquer method, Dynamic programming, backtracking

ALGORITHMIC FOUNDATIONS: Basic Terms - -General Method – Knapsack Problem–Minimum Cost Spanning Tree– Single Source Shortest Path.

Outcome 3	Able to describe about graphs using dynamic programming technique.	**K4**

Unit–IV

Objective 4	Understood the various design and analysis of the algorithms

INFORMATION THEORY: Further Topics in Information Theory

Outcome 4	Demonstrate the concept of backtracking & branch and bound technique	**K5**

Unit–V

Objective 5	Define inference and its role in decision-making

INFERENCE THEORY: Probabilities and Inference

Outcome 5	Explore the traversal and searching technique and apply it for trees and graphs.	**K6**

Suggested Readings:

EllisHorowitz,"ComputerAlgorithms",GalgotiaPublications.

AlfredV.Aho,JohnE.Hopcroft,JeffreyD.Ullman,"DataStructuresandAlgorithms".

A Goodrich,"DataStructures&AlgorithmsinJava",Wiley3rd edition.

Skiena,"TheAlgorithmDesignManual",SecondEdition,Springer,2008

AnanyLevith,"IntroductiontotheDesignandAnalysisofalgorithm",PearsonEducation Asia, 2003.

Information Theory, Inference, and Learning Algorithms David J.C. MacKay, Cambridge University Press 2003. (Unit 4 and 5)

Online Resources https://forensicfield.blog/ https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics					
K1-Remember	*K2-Understand*	*K3-Apply*	*K4-Analyze*	*K5-Evaluate*	*K6-Create*
Course designed by: Dr.T. Meyyappan					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	L (1)	L (1)	M (2)	M (2)	M (2)	S (3)	S (3)	S (3)	L (1)	S (3)
CO2	M (2)	L (1)	S (3)	S (3)	L (1)	S (3)	M (2)	M (2)	M (2)	L (1)
CO3	S (3)	M (2)	M (2)	L (1)	S (3)	M (2)	L (1)	L (1)	S (3)	M (2)
CO4	M (2)	S (3)	L (1)	M (2)	M (2)	L (1)	-	M (2)	M (2)	S (3)
CO5	L (1)	M (2)	S (3)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)	M (2)
W.AV	**1.8**	**1.6**	**2**	**1.8**	**1.8**	**2**	**1.4**	**1.6**	**1.6**	**2**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	L (1)	L (1)	M (2)	S (3)
CO2	M (2)	S (3)	L (1)	M (2)	M (2)
CO3	M (2)	L (1)	M (2)	L (1)	M (2)
CO4	L (1)	S (3)	M (2)	M (2)	M (2)
CO5	L (1)	S (3)	M (2)	M (2)	M (2)
W.AV	**1.6**	**2**	**2**	**1.6**	**1.4**

S –Strong (3), M-Medium (2), L- Low (1)

I - Semester					
DSE	**556503**	**Advanced Software Engineering**	**T**	**Credits:3**	**Hours:3**

Unit– I		
Objective 1	Introduce to Software Engineering, Design, Testing and Maintenance	
Introduction: The Problem Domain – Software Engineering Challenges - Software Engineering Approach – Software Processes: Software Process – Characteristics of a Software Process – Software Development Process Models – Other software processes		
Outcome 1	Understand about Software Engineering process	**K1**
Unit– II		
Objective 2	Enable the students to learn the concepts of Software Engineering	
Software Requirements: Analysis and Specification : Requirement engineering – Type of Requirements – Feasibility Studies – Requirements Elicitation – Requirement Analysis – Requirement Documentation – Requirement Validation – Requirement Management – SRS - Formal System Specification – Axiomatic Specification – Algebraic Specification - Case study: Student Result management system. Software Quality Management –Software Quality, Software Quality Management System, ISO 9000, SEI CMM.		
Outcome 2	Understand about Software project management skills, design and quality management	**K2**
Unit– III		
Objective 3	Learn about Software Project Management, Software Design & Testing	
Software Project Management: Responsibilities of a software project manager – Project planning – Metrics for Project size estimation – Project Estimation Techniques – Empirical Estimation Techniques – COCOMO – Halstead‟s software science – Staffing level estimation – Scheduling– Organization and Team Structures – Staffing – Risk management – Software Configuration Management – Miscellaneous Plan.		
Outcome 3	Analyze on Software Requirements and Specification	**K4**
Unit–IV		
Objective 4	Explore advanced metrics for measuring software complexity and maintainability	
Software Design: Outcome of a Design process – Characteristics of a good software design – Cohesion and coupling - Strategy of Design – Function Oriented Design – Object Oriented Design - Detailed Design - IEEE Recommended Practice for Software Design Descriptions.		
Outcome 4	Analyze on Software Testing, Maintenance and Software Re-Engineering	**K5**
Unit–V		
Objective 5	Apply metrics in the context of software project management	
Software Testing: A Strategic approach to software testing – Terminologies – Functional testing– Structural testing – Levels of testing – Validation testing - Regression testing – Art of Debugging– Testingtools-Metrics-ReliabilityEstimation.SoftwareMaintenance -Maintenance Process - Reverse Engineering – Software Re-engineering - Configuration Management Activities.		
Outcome 5	Design and conduct various types and levels of software quality for a software project	**K6**

Suggested Readings:

An Integrated Approach to Software Engineering – Pankaj Jalote, Narosa Publishing House, Delhi, 3rd Edition.

Fundamentals of Software Engineering – Rajib Mall, PHI Publication,3rdEdition

Software Engineering – K.K. Aggarwal and Yogesh Singh, New Age International Publishers, 3rd edition.

A Practitioners Approach – Software Engineering, - R.S.Pressman, McGraw Hill.

Fundamentals of Software Engineering- Carlo Ghezzi, M.Jarayeri, D.Manodrioli, PHI Publication.

Online Resources

https://git-scm.com/book/en/v2

https://martinfowler.com/architecture/

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

Course designed by: Dr.T. Meyyappan

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	L (1)	M (2)	M (2)	M (2)	S (3)	L (1)	S (3)	L (1)	S (3)
CO2	M (2)	L (1)	S (3)	S (3)	L (1)	S (3)	M (2)	M (2)	M (2)	L (1)
CO3	L (1)	M (2)	M (2)	L (1)	S (3)	M (2)	S (3)	L (1)	S (3)	M (2)
CO4	-	S (3)	L (1)	M (2)	M (2)	L (1)	M (2)	M (2)	M (2)	S (3)
CO5	M (2)	M (2)	S (3)	M (2)	M (2)	M (2)	L (1)	L (1)	L (1)	M (2)
W.AV	**1.4**	**1.6**	**2**	**1.8**	**1.8**	**2**	**1.8**	**1.6**	**1.6**	**2**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	L (1)	L (1)	M (2)	S (3)
CO2	M (2)	S (3)	L (1)	M (2)	M (2)
CO3	M (2)	L (1)	M (2)	L (1)	M (2)
CO4	L (1)	S (3)	M (2)	M (2)	M (2)
CO5	L (1)	S (3)	M (2)	M (2)	M (2)
W.AV	**1.6**	**2**	**2**	**1.6**	**1.4**

S –Strong (3), M-Medium (2), L- Low (1)

II– Semester					
Core	**556201**	**Distributed Operating System in Cyber Space**	**T**	**Credits:4**	**Hours:4**
Unit–I					
Objective:1	To know the basic concepts of Distributed Operating System.				
Introduction of Distributed Operating System(DOS): Functions of DOS, Basic concepts, goals & challenges of distributed systems, architectures of DOS: Client-Server, Peer-to-Peer, and Hybrid. Revisit the inter process communication.					
Outcome:1	Understanding of Distributed Operating System Principles				**K2**
Unit–II					
Objective:2	To explore the unique security challenges in a distributed environment.				
Communication in DOS: Issues in communication, message-oriented communication, remote procedure call, remote method invocation, stream-oriented communication, communication between processes, unstructured Vs structured communication, blocking Vs non-blocking communication.					
Outcome:2	Acquire knowledge and skills in designing secure and privacy-preserving distributed operating systems.				**K2**
Unit –III					
Objective:3	Exploremechanismsformaintainingdataconsistencyandreplicationindistributed environments.				
Synchronization: Introduction of synchronization, Clocks, events, Time in distributed systems 1. Cristian's algorithm 2.The Berkeley Algorithm, 3. Network Time Protocol (NTP) 4.Logical time and logical clocks 5.Lamport logical clock 6.vector clock					
Outcome:3	Distributed Operating Systems Management and Monitoring.				**K4**
Unit – IV					
Objective:4	To gain knowledge of security models, authentication, and authorization mechanisms in distributed operating systems.				
Distributed and Shared Memory Management(DSM): Basic fundamentals of shared memory in DOS, Architecture and algorithm of distributed shared memory, advantages & challenges of DSM, Memory coherence, consistency model, consistency with uniprocessor system, consistency with multiprocessing environment. **Security in DOS**: Importance of security, Types of external attacks, Basic elements of Information System security and policy, Trust Management, Access control models, cryptography.					
Outcome:4	Understanding Security in Distributed Operated Systems.				**K5**
Unit –V					
Objective:5	To understand the security concepts in Open source Operating System.				
Open source operating system: Linux Kernel architecture- User administration in Linux- Services offered by Linux OS- Configuration of email service, web service, NFS, DNS in Linux. Securing servers with IP tables. Setting up Network and cryptographic services, SSL, Managing Certificate Security with Open SSL, working with the GNU Privacy guard.					
Outcome:5	Security and Privacy in Distributed Open Source Operating Systems				**K6**

Suggested Readings:

AndrewS.Tanenbaum&MaartenvanSteen, "DistributedSystem:PrinciplesandParadigms", PEARSON, Second Edition, 2002.

M.TamerOzsu,PatrickValduriez,"PrinciplesofDistributedDatabaseSystem",PatrickValduriez, Prentice Hall International.

RandychowandT.Johnson,"DistributedOperatingSystemsandAlgorithms",AddisonWesly, 1997.

Tom Adelstein and Bill Lubanovic, "Linux System Administration", O'ReillyMedia, Inc., 1st Edition, 2007.

SarathLakshman"LinuxShellScriptingCookbook",PacktPublishing,3rdEdition2017.

G.Coulouris,andJ.Dollimore"Distributedconceptand Design",AddisonWesly.

WilliamStallingandLawrieBrown"ComputerSecurity:PrinciplesandPractice"5th Edition, Pearson, 2023.

OlivierBonaventure"ComputerNetworking:Principles,ProtocolsandPractice" October 31, 2011, Saylor URL: http://www.saylor.org/courses/cs402/.

Online Resources

https://www.coursera.org/courseraplus?utm_source=gg&utm_medium=sem&utm_campaign=B2C_India_FTCOF_Branded_ARTE_EXP&utm_content=B2C&campaignid=20590309416&adgroupid=155702724684&device=c&keyword=coursera&matchtype=e&network=g&devicemodel=&adpostion=&creativeid=675426312952&hide_mobile_promo&gad_source=1&gclid=CjwKCAiAuYuvBhApEiwAzq_YiaOvHIi7vwfCsh1XbfZDjhI71iEio8LVgGD4PEEbu08m1ZTsKBlrxhoCtbcQAvD_BwE

https://www.edx.org/?utm_source=google&utm_campaign=20869335750&utm_medium=cpc&utm_term=edx&hsa_acc=7245054034&hsa_cam=18736834479&hsa_grp=156544624683&hsa_ad=685047827412&hsa_src=g&hsa_tgt=kwd-89882436&hsa_kw=edx&hsa_mt=e&

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

Course designed by: Dr.T. Meyyappan

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M (2)	L (1)	M (2)	L (1)	M (2)	S (3)	S (3)	S (3)	L (1)	S (3)
CO2	S (3)	M (2)	S (3)	L (1)	L (1)	S (3)	L (1)	M (2)	M (2)	M (2)
CO3	L (1)	S (3)	M (2)	M (2)	S (3)	M (2)	M (2)	L (1)	S (3)	L (1)
CO4	M (2)	M (2)	L (1)	S (3)	M (2)	L (1)	S (3)	-	M (2)	M (2)
CO5	M (2)	L (1)	S (3)	M (2)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)
W.AV	**1.8**	**1.8**	**2**	**1.6**	**1.8**	**2**	**2**	**1.4**	**1.6**	**1.6**

S–Strong(3),M-Medium(2),L-Low (1)

Course Outcome VS Programme Specific Outcomes

CO	**PSO1**	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	S (3)	M (2)	S (3)	L (1)	L (1)
CO2	M (2)	M (2)	M (2)	L (1)	S (3)
CO3	M (2)	L (1)	M (2)	M (2)	L (1)
CO4	M (2)	M (2)	L (1)	M (2)	S (3)
CO5	M (2)	M (2)	L (1)	M (2)	S (3)
W.AV	**2**	**1.6**	**1.6**	**1.4**	**2**

S–Strong(3),M-Medium(2),L-Low (1)

II - Semester					
Core	**556202**	**Python Programming**	**T**	**Credits:4**	**Hours:5**

Unit–I		
Objective:1	To learn how to design and program Python applications. To learn how to use lists, tuples, and dictionaries, to write loops and decision statements in Python.	
Introduction to Python Programming: Data Types - Variables - Basic Input - Output Operations - Basic Operators - Conditional Statements – **Python Collections:** List - Tuple - Sets and Dictionary - Loops in Python - String Manipulation-LambdaFunction-UserDefinedFunctions-TypesofFunctions- **Importing Modules:** Maths Module.		
Outcome:1	To capable of using basic functions like"if"and different Types of loops, data types, lists	**K3**
Unit–II		
Objective:2	To learn how to write Date & Time functions and Regular Expressions in Python.	
Date and Time: Sleep - Program execution time - methods on date and time. **Regular Expression:** Split - Working with special characters - date - emails - quantifiers - match and find all - character sequence and substitute - search methods.		
Outcome:2	To know the concept of functions in Python	**K4**
Unit–III		
Objective:3	To learn how to read and write files in Python.	
File Handling: Introduction to files and types of files (Text - Binary and CSV file). Textfile: Opening-Modes(r-r+-w-w+-a-a+)-Writing/Appending Datausing write() and writelines() -Seek And Tell Methods – **Binary file:** basic operations: Close A BinaryFile-dump()and load() method-**CSV file:**import csvmodule-open/close–write		
Outcome:3	Tocapableofhandlefileslikecsvopen,update	**K2**
Unit–IV		
Objective:4	Tolearnhowtodesignobject-orientedprogramswithPythonclasses.	
Generators and Iterators: Iterators - generators - the function any and all - with statement - data compression. **Classes in Python:** New style classes - creating classes-instance methods-inheritance-polymorphism-exception classes &Custom exceptions.		
Outcome:4	To know classes, objects in python	**K5**
Unit–V		
Objective:5	TolearnhowtodatabaseinPythonapplicationsfordatabasehandling.	
Unit–V	**Interface Python with MySQL:** Data Base Connection - Creating Table - Connecting SQL with Python - Performing Insert - Update - Delete Queries using Cursor - Rowcount - Creating Database.	
Outcome:5	TolearnhowtoconnectMysqlwithPython	**K6**

Suggested Readings:

ASmarterWaytoLearnPython,2017MarkMyers.

BeginningPythonfromNovicetoProfessional,SecondEdition,MagnusLie Hetland, APress 2008.

MySQL for Python, Integrate the flexibility of Python and the power of MySQL to boost the productivity of your applications, Albert Lukaszewski – PACKT - 2010.

Beginning Programming with Python for Dummies, A Wiley Brand, by John Paul Mueller2014.

PythonBasics:APracticalIntroductiontoPython3Real Python, DavidAmos, Dan Bader, Joanna Jablonski, Fletcher Heisler- Real Python 2012 - 2020

PythonandMySQLforBeginner,FatimahRahmatMohamadIqbalHakimChe Omar Nurul Shakirah Mohd Zawawi First Edition 2023.

PythonandMySQLDatabase:APracticalIntroduction,byChaitanyaBaweja– RealPython

Online Resources

https://www.coursera.org/specializations/python?utm_source=gg&utm_medium=sem&utm_campaign=B2C_INDIA_google-cybersecurity-certificates_PMax-arte-

https://www.codecademy.com/catalog/language/python?g_network=g&g_productchannel=&g_adid=624951457624&g_locinterest=&g_keyword=codecademy%27s%20learn%20python&g_acctid=243-039-7011&g_adtype=&g_keywordid=kwd-

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

Coursedesignedby: Dr.T. Meyyappan

CourseOutcomeVSProgrammeOutcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S(3)	S(3)	S(3)	M(2)	L(1)	M(2)	M(2)	M(2)	M(2)	S(3)
CO2	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	M(2)	M(2)
CO3	M(2)	M(2)	L(1)	M(2)	M(2)	S(3)	M(2)	S(3)	M(2)	M(2)
CO4	S(3)	L(1)	M(2)	M(2)	M(2)	M(2)	M(2)	M(2)	M(2)	L(1)
CO5	S(3)	M(2)	L(1)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)	M(2)
W.AV	**2.4**	**2.2**	**1.8**	**2.4**	**1.8**	**2.4**	**1.6**	**2.2**	**2**	**2**

S–Strong(3),M-Medium(2),L-Low(1)

CourseOutcomeVSProgrammeSpecificOutcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	M(2)	L(1)	S(3)	M(2)
CO2	S(3)	L(1)	M(2)	S(3)	M(2)
CO3	S(3)	L(1)	S(3)	M(2)	M(2)
CO4	M(2)	M(2)	S(3)	L(2)	L(1)
CO5	S(3)	M(2)	M(2)	L(1)	S(3)
W.AV	**2.6**	**1.6**	**2.2**	**2.2**	**2**

S–Strong(3),M-Medium(2),L-Low(1)

II - Semester				
556203	**Python Programming LAB**	**P**	**Credits:2**	**Hours:3**
Objectives	➢ Tounderstandtheproblemsolvingapproaches. ➢ TolearnthebasicprogrammingconstructsinPython. ➢ To practice various computing strategies for Python-based solutions to real world problems. ➢ TousePythondatastructures–lists,tuples,dictionaries. ➢ Todoinput/outputwithfilesinPython.			
1. Sort3numberswithoutusingloopsorconditionalstatements. 2. AppendtheContentofOneFiletotheEndofAnotherFile 3. CreateaClassinwhichOneMethodAcceptsaStringfromtheUserandAnother Prints it 4. Create a class by name Students, and initialize attributes like name, age, and grade while creating an object. 5. Createavalidemptyclasswiththename Students,withnoproperties. 6. WrittenmodulesandPythonStandardLibraries(pandas,numpy.Matplotlib,scipy) 7. Real-time/technical applications using File handling. (copy from one file toanother, word count, longest word) 8. Real-time/technicalapplicationsusingExceptionhandling. (dividebyzero error,voter's age validity, student mark range validation) 9. ExploringPygametool. 10. DevelopingagameactivityusingPygamelikebouncingball,carraceetc. 11. Findthenumberoflinesinthegivenfile. 12. Calculatethetimeelapsedtoexecutethecode. 13. Trimwhite-spacefromastringwithPython. 14. FetchHospitalandDoctorInformationusinghospitalIdanddoctorId 15. SelectEmployeesRecordsWhoseSalaryiswithintheGivenRangeinPython				
Outcomes	➢ Students should be able to apply their knowledge of Python to analyze problems, design algorithms, and implement solutions. ➢ Studentsshouldgainexperienceindebuggingcode. ➢ Familiarity with version control systems (e.g., Git) may be an outcome. Students should be able to commit changes, create branches,andunderstandthebasicsofcollaborativecodingusing versioncontrol. ➢ Students might learn how to read from and write to files using Python. ➢ Depending on the level of the lab, students may work with basic data structures such as lists, dictionaries, and sets.			

CourseOutcomeVSProgrammeOutcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)
CO2	S(3)	M(2)	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	M(2)	S(3)
CO3	S(3)	L(1)	M(2)	M(2)	S(3)	M(2)	M(2)	L(1)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)	S(3)
W.AV	**2.6**	**2**	**1.8**	**1.6**	**2**	**1.6**	**2**	**2.2**	**2.2**	**2.2**

S–Strong(3),M-Medium(2),L-Low(1)

CourseOutcomeVSProgrammeSpecificOutcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	L(1)	M(2)	S(3)
CO2	M(2)	L(1)	M(2)	M(2)	L(1)
CO3	M(2)	M(2)	M(2)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)
CO5	M(2)	L(1)	M(2)	S(3)	L(1)
W.AV	**2.4**	**1.6**	**1.6**	**1.8**	**1.8**

S–Strong(3),M-Medium(2),L-Low(1)

II - Semester					
CC	**556204**	**ML for Digital Forensic**	**T**	**Credits:4**	**Hours:5**

Unit–I

Objective1	To Understand an Overview of ML for forensics

INTRODUCTION TO MACHINE LEARNING: Brief Introduction to Machine Learning Well Posed Learning Problems, Motivation to Machine Learning, Applications of Machine Learning, Designing a Learning System, Perspective and Issues in Machine Learning, Concept Learning; Types of Machine Learning – Supervised Learning, Unsupervised Learning, Reinforcement Learning.

Outcome1	Understanding the important role of machine learning	**K2**

Unit–II

Objective2	To Understand a basic idea about ML for cyber forensics

DIMENSION ALITYREDUCTION: Subset Selection, Shrinkage Methods, Principle Components Regression; Linear Classification, Logistic Regression, Linear Discriminant Analysis; Optimization, Classification-Separating Hyperplanes Classification.

Outcome2	Analyzing large amounts of diverse datasets in order to reveal any criminal behavior	**K2**

Unit–III

Objective3	To Understand an overview of supervised learning techniques

SUPERVISED AND UNSUPERVISED LEARNING: Naïve Bayes Classification: Fitting Multivariate Bernoulli Distribution, Gaussian Distribution and Multinomial Distribution, K-Nearest Neighbors, Decision Trees.

Support Vector Machines: Hard Margin and Soft Margin, Kernels and Kernel Trick, Evaluation Measures for Classification, Ensemble Models, k-means and Hierarchical Agglomerative Clustering, Evaluation Measures for Clustering

Outcome3	Understanding various machine learning algorithms and techniques that can be useful in the process of extracting and analyzing digital evidence	**K3**

Unit–IV

Objective4	To provide students with a comprehensive understanding of ANN

ARTIFICIAL NEURAL NETWORK: Artificial Neural Networks (Early models, Back Propagation, Initialization, Training &Validation), Parameter Estimation (Maximum Likelihood Estimation, BayesianParameter Estimation), Decision Trees, Evaluation Measures, Hypothesis Testing, Ensemble Methods, Graphical ModeL

Outcome4	Evaluatetheadmissibilityof ANNanditsmodels.	**K4**

Unit–V

Objective5	Studentswillbeequippedtheknowledgeincasestudiesandapplications

CASESTUDIES AND APPLICATIONS: Malware Detection, Network Intrusion Detection, Email Forensics, Mobile Forensics

Outcome5	Toprovidestudentswithcompleteknowledgeoncase studies	**K5**

Suggested Readings:

TomMitchell,MachineLearning,TMH,McGraw-HillScience/Engineering/Math,ISBN:0070428077(Unit 1 to 4)

MarjieT.Britz,DigitalForensicsandCyberCrime(Unit5)

KishanMehrotra,ChilukuriMohanandSanjayRanka,ElementsofArtificialNeural Networks,

RajjanShinghal,PatternRecognition,TechniquesandApplications,OXFORD

AthemEalpaydin,IntroductiontoMachineLearning,PHI

Online Resources: https://www.udacity.com/course/ai-engineer-using-microsoft-azure-- https://www.fast.ai/					
K1-Remember	***K2-Understand***	***K3-Apply***	***K4-Analyze***	***K5-Evaluate***	***K6-Create***
Coursedesignedby: Dr. A. Padmapriya					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M (2)	S (3)	M (2)	L (1)	S (3)	S (3)	S (3)	L (1)	L (1)	M (2)
CO2	L (1)	M (2)	S (3)	M (2)	S (3)	M (2)	L (1)	M (2)	L (1)	S (3)
CO3	S (3)	L (1)	M (2)	S (3)	M (2)	L (1)	M (2)	S (3)	M (2)	L (1)
CO4	M (2)	M (2)	L (1)	M (2)	L (1)	-	S (3)	M (2)	S (3)	M (2)
CO5	M (2)	L (1)	S (3)	L (1)	M (2)	M (2)	M (2)	L (1)	M (2)	M (2)
W.AV	**1.8**	**1.6**	**2**	**1.8**	**2**	**1.4**	**2**	**1.6**	**1.6**	**1.8**

S–Strong(3),M-Medium(2),L-Low(1)

CourseOutcomeVSProgrammeSpecificOutcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	S (3)	L(1)	L (1)	M (2)
CO2	M (2)	M (2)	L (1)	S (3)	M (2)
CO3	M (2)	M (2)	M (2)	L (1)	L (1)
CO4	L (1)	M (2)	M (2)	S (3)	M (2)
CO5	L (1)	M (2)	M (2)	S (3)	M (2)
W.AV	**1.6**	**2**	**1.4**	**2**	**1.6**

S–Strong(3),M-Medium(2),L-Low(1)

<table>
<tr><th colspan="5">II - Semester</th></tr>
<tr><td>556205</td><td>ML for Digital Forensic LAB</td><td>P</td><td>Credits:2</td><td>Hours:3</td></tr>
<tr><td>Objectives</td><td colspan="4">➢ TolearnDigitalEvidenceAcquisition:
➢ ToknowaboutFeatureExtractionandSelectionTechniques
➢ To understand Supervised Learning/Unsupervised Model Implementation
➢ ModelValidationandEvaluation
➢ EthicalandLegalConsiderationsinPractice</td></tr>
<tr><td colspan="5">1. Extract the data from data base using python
2. Implementk-nearestneighboursclassificationusing python
3. Implement linear regression using python.
4. Implement Naïve Bayes theorem to classify the English text
5. Implement an algorithm to demonstrate the significance of genetic algorithm
6. How to Recover Deleted Files using Forensics Tools
7. How to View Last Activity of Your PC
8. How to Extracting Browser Artifacts
9. ComparisonoftwoFilesforforensicsinvestigationbyCompareITsoftware
10. How to Collect Email Evidence in Victim PC
11. Study the steps for hiding and extract anytext file behind an image file/ Audio file using Command Prompt</td></tr>
<tr><td>Outcomes</td><td colspan="4">➢ Students will practice acquiring digital evidence using forensically sound methods and tools, ensuring the integrity of the data.
➢ Students will apply various feature extraction and selection techniques to identify relevant patterns and characteristics in digital forensic data.
➢ Students will implement and experiment with supervised learning/Un supervised models, such as decision trees, support vector machines, and random forests, for classification tasks including clustering algorithms and anomaly detection, to uncover patterns in digital forensic data.
➢ Students will learn and implement model validation techniques, including cross-validation and hyperparameter tuning, to optimize and evaluate the performance of machine learning models.
➢ Students will navigate ethical and legal considerations in the practical application of machine learning in digital forensics, ensuring compliance with regulations and maintaining the integrity of the investigation.</td></tr>
</table>

CourseOutcomeVSProgrammeOutcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)
CO2	S(3)	M(2)	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	M(2)	S(3)
CO3	S(3)	L(1)	M(2)	M(2)	S(3)	M(2)	M(2)	L(1)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)	S(3)
W.AV	**2.6**	**2**	**1.8**	**1.6**	**2**	**1.6**	**2**	**2.2**	**2.2**	**2.2**

S–Strong(3),M-Medium(2),L-Low(1)

CourseOutcomeVSProgrammeSpecificOutcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	L(1)	M(2)	S(3)
CO2	M(2)	L(1)	M(2)	M(2)	L(1)
CO3	M(2)	M(2)	M(2)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)
CO5	M(2)	L(1)	M(2)	S(3)	L(1)
W.AV	**2.4**	**1.6**	**1.6**	**1.8**	**1.8**

S–Strong (3),M-Medium(2),L-Low(1)

II - Semester					
Core	**556206**	**Digital Signatures**	**T**	**Credits:4**	**Hours:4**

Unit–I

Objective1	UnderstandtheFundamentalsofcryptographyanddigitalsignature

Introduction to Cryptography: Overview of Cryptography_ Types of Cryptographic Algorithms Symmetric and Asymmetric Encryption Hash Functions

Outcome1	Understanding the important role of Cryptography and Digital Signature	**K2**

Unit–II

Objective2	ToSurveyDigitalSignatureAlgorithms.

Digital Signatures Basics: IntroductiontoDigitalSignatures_DigitalSignatureAlgorithms(RSA, DSA, ECDSA) Secure Hash Algorithms (SHA-256,SHA-3),Generating and Verifying Digital Signatures

Outcome2	UnderstandingForensicAnalysisSkills	**K2**

Unit–III

Objective3	ToConductForensic Analysis.

Public Key Infrastructure (PKI) in Forensics: PKI Concepts and Components_Certificate Authorities(CAs)_ Key Management_Certificate Revocation and Validation

Outcome3	UnderstandingQuantumComputingImpactAssessment	**K4**

Unit–IV

Objective4	ToAnalyzeBlockchainForensics

Digital Signature Forensics: Digital Signature Forensic Analysis Case Studies in Digital Signature Verification Challenges and Pitfalls in Digital Signature Forensics

Outcome4	Understandtheconceptofblockchainforensics	**K5**

Unit– V

Objective5	Toanalyzequantumcomputingtechniques

Quantum Computing: Quantum Computing and its Impact on Digital Signatures, Post-Quantum Cryptography Block chain Forensics and Digital Signatures, Emerging Trends and Technologies

Outcome5	Understandingaboutquantumcomputing.	**K1**

Suggested Readings:

1. CryptographyandNetworkSecurity:PrinciplesandPracticebyWilliamStallings
2. UnderstandingCryptography"byChristofPaarandJanPelzl
3. PublicKeyInfrastructure:BuildingTrustedApplicationsandWebServicesbyJohnR. Vacca
4. Digital Forensics for Legal Professionals: Understanding Digital Evidence From the Warrant to theCourtroom" by Lars E. Daniel and Larry E. Daniel.
5. QuantumComputingforComputerScientistsbyNosonS.YanofskyandMircoA. Mannucci

Online Resources

https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm
https://www.javatpoint.com/cyber-security-digital-signature

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

Coursedesignedby: Dr. A. Padmapriya

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	S(3)	M (2)	L (1)	M (2)	S (3)	M (2)	L (1)	L (1)	S (3)
CO2	L (1)	M (2)	S (3)	L (1)	L (1)	S (3)	S (3)	M (2)	M (2)	M (2)
CO3	M (2)	L (1)	M (2)	M (2)	S (3)	M (2)	L (1)	S (3)	S (3)	L (1)
CO4	S (3)	-	L (1)	S (3)	M (2)	L (1)	M (2)	M (2)	M (2)	M (2)
CO5	M (2)	M (2)	S (3)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)	L (1)
W.AV	**2**	**1.4**	**2**	**1.6**	**1.8**	**2**	**1.8**	**1.8**	**1.6**	**1.6**

S–Strong(3),M-Medium(2),L-Low(1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	L (1)	S (3)	M (2)	L (1)
CO2	M (2)	S (3)	M (2)	M (2)	L (1)
CO3	M (2)	L (1)	M (2)	L (1)	M (2)
CO4	M (2)	S (3)	L (1)	M (2)	M (2)
CO5	M (2)	S (3)	L (1)	M (2)	M (2)
W.AV	**2**	**2**	**1.6**	**1.6**	**1.4**

S–Strong(3),M-Medium(2),L-Low(1)

II–Semester					
DSE	**556504**	**Cloud Environment and Forensics**	**T**	**Credits:3**	**Hours: 3**

Unit– I

Objective:1	To understand cloud computing concepts, services, and architecture.

Introduction to Cloud Computing: Cloud Computing definition and Characteristics - Models of Cloud: Deployment- private, public and hybrid – Service- IaaS, PaaS, SaaS. Cloud Service Platforms: Amazon, Azure, Google App, IBM cloud- Challenges: Virtual Machine Migration, Security and Privacy, Accessibility issues.

Outcome:1	Understand Cloud Computing Fundamentals	**K2**

Unit –II

Objective:2	Toacquirein-depthknowledgeofcloudsecurity protocols.

Introduction to Cloud Security: Vulnerabilities and need of cloud security- Cloud Security Concepts: Multi –tenancy-Virtualization-Data outsourcing-Trust Management-Meta data security-Cloud Security Standards: ITIL- COBIT- ISO/ICE 2000 –SSAE – CSA.

Outcome:2	Able to implement security measures in a cloud environment.	**K1**

Unit –III

Objective:3	Tolearnadvancedforensicinvestigationtechniquesspecifictocloud environments.

Cloud Security and Privacy Issus: Security Concepts: Confidentiality, privacy, integrity, authentication, non repudiation, availability, access control-Privacy Issues: Defining role to actors – Complains – Legal and multi-location issues-Privacy issues on CIA – Protection of the data – User control lacking –Data movement.

Outcome:3	ConductDigitalForensicsinCloudEnvironments.,	**K4**

Unit –IV

Objective:4	Togainproficiencyinusingspecializedtoolsforcloud forensics.

Threat Model and Intrusion Detection: Threat Model-Taxonmoy of attacks: VMAT-VMMAT-HWAT-VSWAT-TENAT. Intrusion Detection Techniques: Misuse- Anomaly – VMI – Hypervisor – Hybrid.

Outcome:4	Developincidentresponseplansspecifictocloudenvironments.	**K3**

Unit –V

Objective:5	Tostayupdatedwithevolvingcloudtechnologies,securitythreats,and forensic methodologies.

Tools and Advances: Attack tools: Network level- VM level-VMM attack. Security tools:Network – VM and VMM.

Outcome:5	ExploreEmergingTrendsinCloudForensics.	**K5**

Suggested Readings:

1.Preeti Mishra, Emmanuel S Pilli, Joshi, "Cloud Security: Attacks, Techniques, Tools, and Challenges", Chapman and Hall/CRC, 1st Edition, 2022.

1.John W.Rittinghouse, James F.Ransome, "Cloud Computing: Implementation, Management, and Security", CRC Press, 2010.

Online Resources https://www.appdirect.com/blog/cloud-forensics-and-the-digital-crime-scene https://www.digitalforensics.com/?utm_source=google&utm_medium=cpc&utm_campaign=DF-BRS-					
K1-Remember	*K2-Understand*	*K3-Apply*	*K4-Analyze*	*K5-Evaluate*	*K6-Create*
Coursedesignedby: Dr. S. Santhoshkumar					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S(3)	S(3)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)	L(1)	S(3)
CO2	L(1)	M(2)	S(3)	L(1)	L(1)	S(3)	S(3)	M(2)	M(2)	M(2)
CO3	M(2)	L(1)	M(2)	M(2)	S(3)	M(2)	L(1)	S(3)	S(3)	L(1)
CO4	S(3)	-	L(1)	S(3)	M(2)	L(1)	M(2)	M(2)	M(2)	M(2)
CO5	M(2)	M(2)	S(3)	M(2)	M(2)	M(2)	M(2)	L(1)	L(1)	L(1)
W.AV	**2**	**1.4**	**2**	**1.6**	**1.8**	**2**	**1.8**	**1.8**	**1.6**	**1.6**

S–Strong(3),M-Medium(2),L-Low(1)

CourseOutcomeVSProgrammeSpecific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	L(1)	S(3)	M(2)	L(1)
CO2	M(2)	S(3)	M(2)	M(2)	L(1)
CO3	M(2)	L(1)	M(2)	L(1)	M(2)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	L(1)	M(2)	M(2)
W.AV	**2**	**2**	**1.6**	**1.6**	**1.4**

S–Strong(3),M-Medium(2),L-Low(1)

II – Semester					
DSE	**556505**	**Wireless Network Security**	**T**	**Credits:3**	**Hours:3**

Unit – I

Objective:1	To help the student will develop an understanding of security threats in Wireless networks.

Introduction: Wireless Network Security: Wireless Security, Mobile Device Security, Weaknesses in Network Security. Risks and Threats of Wireless: Wireless Security Objectives – Passive and Active Threat Model - Cryptography Primer -Performancevs. Security Tradeoffs - Wireless Security Toolbox. Wireless Physical Layer Technologies: Anti-jamming/Jamming-resistance - Frequency Hopping Spread Spectrum (FHSS) – Direct Sequence Spread Spectrum(DSSS)-Orthogonal Frequency Division Multiplexing(OFDM)

Outcome:1	To make students understand the basics of wireless sensor networks.	**K3**

Unit– II

Objective:2	To understand the main security goals and adversarial models of wireless and mobile networks

Security of WiFi Networks: The Standard 802.11 and its Extensions:802.11 – 802.11a -802.11b - 802.11d - 802.11g - 802.11h Wireless LAN Security. Wireless Fidelity - Wi-Fi Protected Access, the Physical Layer: Spread Spectrum, Medium Access Layer: Frames and Fragmentation - Avoidance of Collisions - MAC Addresses - SSID Network Name -Authentication Procedures - WPA and WPA, Security Requirements: Assuring Availability - Assuring Data Integrity-Assuring Authenticity -Assuring Confidentiality.

Outcome:2	To familiarize with learning of thearchitecture of WSN.	**K2**

Unit– III

Objective:3	To gain a broad knowledge regarding real-world security architectures of wlans, gsm/umts,wsns,rfids,etc.;

Wireless Wide Area Network: GSM – HSCSD, GPRS, UMTS – HSDPA, Services – SMS/EMS/MMS – WAP. Threats and Protection: General Organisational Measure - General Technical Measures, Attacker in Possession of the Device - Attacker Does Not PossesstheDevice,GeneralPrecautionaryMeasures:DataEncryption–Firewalls-Encryption on the Device–Backup.

Outcome:3	To understand the concepts of networking and security in wsn	**K1**

Unit– IV

Objective:4	To help the student to develop knowledge of security controls that is Applied to reduce the probability of a successful attack.

Security of Wireless Sensor Networks (WSNs): WSN Architectures and Protocols – Security Threats – Cryptographic Primitives – Key Establishment and Distribution – Security of Zig Bee WSNs – Security of Wireless Medical Devices – Future Trends. Security of Near Field Communications (NFCs) and RFIDs Introduction to NFC and RFIDTechnologies-TagsandReaders–SecurityandPrivacyIssues–Real-World Attacks– Standardisation Activities–Authentication and Access Control Protocols.

Outcome:4	To study the design security control and solution to the various problems.	**K5**

Unit– V		
Objective:5	To be able to reason about wireless security protocols and protection techniques, discuss proposed solutions and their limitations	
Security Policy: Introduction - Security Requirements –Risks – Measures , Scope : Legal Regulations – Guidelines and Standards – Standards -ISO/IEC 13335 - Standard ISO/IEC17799 - Standard 27001 Information and Communication Security :Strategic Involvement- Security Organisation- Approval Process–Confidentiality, Physical Security:Objects–Access–Threats–Equipment –UtilityServices–Disposal.		
Outcome:5	To study the design security policy, control and solution to the Various problems	**K4**

Text Books:

1. WirelessandMobileNetworkSecurity,HakimaChaouchi,MarylineLaurent–Maknavicius,Wiley2009.
2. WirelessNetworkSecurity,SecondEdition,WolfgangOsterhage,CRCPress, Taylor & Francis Group 2018.
3. SecurityinWirelessCommunicationNetworksYiQian,FengYe,Hsiao-Hwa Chen, John Wiley 2022.

Suggested Readings:

1. Wireless Networks Local and Ad Hoc Networks, From Principles to Successful Implementation Steve Rackley, Ivan Marsic Department of Electrical and Computer Engineering and the CAIP Center - Rutgers University

Online Resources

https://www.wi-fi.org/

https://www.edureka.co/cybersecurity-certification-training?utm_source=Google-Search&utm_medium=cpc&utm_campaign=ET-IND-Search-Cybersecurity&utm_term=ET-cybersecurity-

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

Coursedesignedby: Dr. S. Santhoshkumar

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)	L(1)	M(2)	S(3)
CO2	S(3)	L(1)	M(2)	M(2)	M(2)	L(1)	M(2)	M(2)	M(2)	M(2)
CO3	S(3)	L(1)	M(2)	M(2)	M(2)	M(2)	M(2)	L(1)	L(1)	M(2)
CO4	L(1)	M(2)	M(2)	L(1)	M(2)	M(2)	S(3)	M(2)	M(2)	S(3)
CO5	M(2)	M(2)	M(2)	M(2)	L(1)	M(2)	L(1)	S(3)	S(3)	M(2)
W.AV	**2.2**	**1.8**	**2**	**2**	**1.6**	**1.8**	**2**	**1.8**	**2**	**2.4**

S–Strong(3),M-Medium(2),L-Low(1)

CourseOutcomeVSProgrammeSpecificOutcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	M(2)	L(1)	M(2)	S(3)
CO2	L(1)	M(2)	M(2)	S(3)	M(2)
CO3	M(2)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	S(3)	L(1)	M(2)
CO5	S(3)	M(2)	L(1)	S(3)	L(1)
W.AV	**2**	**2.2**	**1.8**	**2.4**	**1.8**

S–Strong(3),M-Medium(2),L-Low(1)

II - Semester					
DSE	**556506**	**WAP and XML**	**T**	**Credits:3**	**Hours: 3**

Unit– I

Objective1	To understand wireless application protocol

Introduction to Wireless Technologies: Evolution of mobile communication_ Introduction to WAP and its significance_WAP Architecture Layers of the WAP protocol stack_WAP Gateway, Proxy, and Wireless Session Protocol(WSP)_Wireless Transaction Protocol(WTP) and Wireless Transport Layer Security(WTLS)

Outcome 1	Understanding the important of wireless application protocol	**K3**

Unit–II

Objective2	To understand wireless markup language

WML(Wireless Markup Language): Introduction to WML and its role in WAPWML syntax and structure_Designing WMLpages for mobile devices_Tools and platforms for WAP development

Outcome2	Understanding WAP security issues	**K2**

Unit–III

Objective3	To understand XML security protocol

WAP Security: Security issues in WAP_WTLS and secure WAP applications_Emerging trends in wireless technologies_ Best practices for secure WAP development _Mobile application security testing

Outcome3	Understanding various security issues	**K4**

Unit–IV

Objective4	Students explore XML security protocols

XML Security Protocols: XML Encryption and XML Digital Signature, Securing XML with SAML (Security Assertion Markup Language),OAuth and XML-based Authentication, XML Security Gateway Solutions

Outcome4	Students will understand the security protocols in XML.	**K5**

Unit– V

Objective5	Student will apply cyber security integration

XML and Cyber security Integration: XML Firewall and Intrusion Detection for XML,XML-based Web Services Security (SOAP and REST),XML and Threat Intelligence, XML Security Best Practices

Outcome5	Students will understand cyber security and web security integrations.	**K6**

Suggested Readings:

1. "WirelessApplicationProtocol:ADeveloper'sGuide"byPaulMichaelNagy
2. "WirelessInternetApplicationsandArchitecture:BuildingProfessionalWirelessApplications Worldwide" by Krishna Sankar, Vijay S. K. Gurbani
3. "WirelessWebDevelopment"byRay Rischpater
4. "WAP,Bluetooth,and3GProgramming:CrackingtheCode"byHiteshSeth
5. "Mobile Computing: Technology, Applications, and Service Creation" by Asoke K. Talukder, Roopa R. Yavagal
6. "MobileApplicationSecurity:ProtectingMobileDevicesandTheirApplications"byHimanshu Dwivedi, David Thiel, Andrew Hoog
7. "SecuringXML:KeepingYourXMLApplicationsSafe"byMark O'Neill
8. "XMLandWebServicesSecurity:RepellingtheWilyHacker"byBlakeDournaee

Online Resources https://www.udacity.com/course/ai-engineer-using-microsoft-azure-- https://www.fast.ai/

K1-Remember	*K2-Understand*	*K3-Apply*	*K4-Analyze*	*K5-Evaluate*	*K6-Create*
Coursedesignedby: Dr. S. Santhoshkumar					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	S(3)	M(2)	L(1)	S(3)	S(3)	S(3)	L(1)	L(1)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)
CO3	S(3)	L(1)	L(1)	S(3)	M(2)	L(1)	M(2)	M(2)	S(3)	M(2)
CO4	M(2)	-	M(2)	M(2)	L(1)	M(2)	S(3)	S(3)	M(2)	L(1)
CO5	M(2)	M(2)	M(2)	L(1)	M(2)	L(1)	M(2)	M(2)	L(1)	S(3)
W.AV	**1.8**	**1.4**	**1.8**	**1.8**	**2**	**1.6**	**2**	**1.6**	**1.6**	**2**

S –Strong(3),M-Medium(2),L-Low(1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	L(1)	S(3)	L(1)
CO2	M(2)	M(2)	L(1)	M(2)	S(3)
CO3	M(2)	L(1)	M(2)	M(2)	L(1)
CO4	M(2)	M(2)	M(2)	L(1)	S(3)
CO5	M(2)	M(2)	M(2)	L(1)	S(3)
W.AV	**2**	**1.6**	**1.4**	**1.6**	**2**

S –Strong(3),M-Medium (2),L-Low(1)

III – Semester					
Core	**556301**	**Ethical Hacking**	**T**	**Credits:4**	**Hours: 5**

Unit– I

Objective: 1	To understand the basics of computer based vulnerabilities.

INTRODUCTION: Ethical Hacking Overview - Role of Security and Penetration Testers - Penetration-Testing Methodologies- Laws of the Land - Overview of TCP/IP- The Application Layer - The Transport Layer - The Internet Layer - IP Addressing - Network and Computer Attacks - Malware -Protecting Against Malware Attacks- Intruder Attacks - Addressing Physical Security.

Outcome: 1	Understanding of Security Concepts.	**K2**

Unit –II

Objective: 2	To explore different foot printing, reconnaissance and scanning methods.

FOOT PRINTING, RECONNAISSANCE AND SCANNING NETWORKS: Foot printing Concepts - Foot printing through Search Engines, Web Services, Social Networking Sites, Website, Email - Competitive Intelligence - Foot printing through Social Engineering -Foot printing Tools - Network Scanning Concepts - Port-Scanning Tools - Scanning Techniques - Scanning Beyond IDS and Firewall.

Outcome: 2	Develop practical skills in using ethical hacking tools and techniques.	**K3**

Unit – III

Objective: 3	To expose the enumeration and vulnerability analysis methods.

ENUMERATION AND VULNERABILITY ANALYSIS :Enumeration Concepts - NetBIOS Enumeration – SNMP, LDAP, NTP, SMTP and DNS Enumeration - Vulnerability Assessment Concepts - Desktop and Server OS Vulnerabilities - Windows OS Vulnerabilities - Tools for Identifying Vulnerabilities in Windows- Linux OS
Vulnerabilities- Vulnerabilities of Embedded Oss.

Outcome: 3	Learn and apply a systematic and ethical hacking methodology**.**	**K4**

Unit – IV

Objective: 4	To explore the options for network protection.

SYSTEM HACKING : Hacking Web Servers - Web Application Components- Vulnerabilities - Tools for Web Attackers and Security Testers Hacking Wireless Networks - Components of a Wireless Network – Wardriving- Wireless Hacking - Tools of the Trade .

Outcome: 4	Understand the principles of Network Security and Defense Mechanisms.	**K5**

Unit – V

Objective: 5	To practice tools to perform ethical hacking to expose the vulnerabilities.

NETWORK PROTECTION SYSTEMS: Access Control Lists. - Cisco Adaptive Security Appliance Firewall - Configuration and Risk Analysis Tools for Firewalls and Routers - Intrusion Detection and Prevention Systems – Network Based and Host-Based IDSs and IPSs - Web Filtering - Security Incident Response Teams – Honeypots.

Outcome: 5	Understand the importance of security policies.	**K6**

Suggested Readings:

Michael T.Simpson, Kent Backman, and James E.Corley, "Hands-On Ethical Hacking and Network Defense", Course Technology, Delmer Cengage Learning, 2010.

Patrick Engebretson, "The Basics of Hacking and Penetration Testing", SYNGRESS, Elsevier, 2013.

Dafydd Stuttard and Marcus, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", Wiley Publishing, Inc. 2011.

Online Resources

https://www.hackthebox.com/

https://portswigger.net/web-security

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

Course designed by: Dr.S.Santhoshkumar

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	S (3)	M (2)	L (1)	S (3)	M (2)	S (3)	L (1)	L (1)	M (2)
CO2	M (2)	M (2)	S (3)	M (2)	S (3)	L (1)	L (1)	L (1)	M (2)	S (3)
CO3	L (1)	L (1)	M (2)	S (3)	M (2)	S (3)	M (2)	M (2)	S (3)	L (1)
CO4	M (2)	-	L (1)	M (2)	L (1)	M (2)	S (3)	S (3)	M (2)	M (2)
CO5	L (1)	M (2)	S (3)	L (1)	M (2)	M (2)	M (2)	M (2)	L (1)	M (2)
W.AV	**1.6**	**1.4**	**2**	**1.8**	**2**	**1.8**	**2**	**1.6**	**1.6**	**1.8**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	M (2)	L (1)	S (3)	L (1)
CO2	M (2)	M (2)	L (1)	M (2)	S (3)
CO3	M (2)	L (1)	M (2)	M (2)	L (1)
CO4	L (1)	M (2)	M (2)	M (2)	S (3)
CO5	L (1)	M (2)	M (2)	M (2)	S (3)
W.AV	**1.6**	**1.6**	**1.4**	**2**	**2**

S –Strong (3), M-Medium (2), L- Low (1)

III - Semester					
Core	**556302**	**Behavioral Biometrics**	**T**	**Credits:4**	**Hours:4**

Unit– I

Objective 1	To understand techniques used for behavioral biometrics	
BIOMETRICS FUNDAMENTALS: Introduction – Benefits of biometric security – Verification and identification Basic working of biometric matching – Accuracy – False match rate – False non-match rate – Failure to enroll rate – Derived metrics –Layered biometric solutions.		
Outcome 1	Understand the basic behavioral biometrics concepts	**K2**

Unit– II

Objective 2	To understand techniques used for building speech recognition systems	
SPEECH RECOGNITION: Introduction-Regular Expressions and automata-Words and transducers-N-grams Part of speech tagging Hidden Markov and Entropy models, Speech-Phonetics-Speech synthesis-Automatic speech recognition Speech Recognition advanced topics-Computational Phonology		
Outcome 2	Students will study the acoustic and behavioral features of speech to develop an understanding of voice recognition systems and their applications.	**K2**

Unit– III

Objective 3	To learn the syntax and semantics of speech recognition	
SPEECH PARSING&SEMANTICS OF SPEECH RECOGNITION: Formal grammar of English-Syntactic parsing-Statistical parsing-Features and Unification-Language and complexity, Semantics and Pragmatics-The representation of meaning-Computational Semantics-Lexicalsemantics- Computational lexical semantics-Computational discourse		
Outcome 3	Students will explore various behavioral biometric modalities, such as keystroke dynamics and voice recognition.	**K4**

Unit–IV

Objective 4	To Know the basic parameters of human gait	
GAIT PATTERN ANALYSIS: Fundamentals of Gait Analysis, Fundamentals of Gait Analysis, Gait Analysis: Considerations and Terminology, Motion Analysis Systems, Ground Reaction Forces, Introduction to EMG, Motion Analysis.		
Outcome 4	Students will explore the biomechanics of human gait and how gait analysis can be employed as a behavioral biometric for identity verification.	**K5**

Unit–V

Objective 5	To Characterize normal human gait and Identify type of gait disorder and pathologies	
Normal Gait: Ankle & Foot Complex , Normal Gait: Knee Joint , Normal Gait: Hip Joint, Normal Gait: Control of the whole body center of mass, Pathological Gait Voice Scan - Features – Components Operation(Steps) – Competing voice Scan (facial) technologies – Strength and weakness.		
Outcome 5	Students will learn how to assess the performance of behavioral biometric systems using metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR).	**K5**

Suggested Readings:

Samir Nanavati, Michael Thieme, Raj Nanavati "Biometrics – Identity Verification in a Networked World", WILEY- Dream Tech Edition 2009.(UNIT 1,2,3,4,)

Paul Reid "Biometrics for Network Security", Pearson Education.2009. (UNIT 5)

Daniel Jurafsky and James Martin "Speech and Language Processing", 2nd edition, Prentice- Hall, 2008.

Xuedong Huang, Alex Acero and Hsiao-Wuen Hon, "Spoken Language Processing", Prentice- Hall.

Online Resources https://www.nist.gov/programs-projects/biometrics https://www.biometricsinstitute.org/					
K1-Remember	*K2-Understand*	*K3-Apply*	*K4-Analyze*	*K5-Evaluate*	*K6-Create*
Coursedesignedby: Dr. A. Padmapriya					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M (2)	L (1)	M (2)	L (1)	M (2)	S (3)	S (3)	S (3)	L (1)	S (3)
CO2	S (3)	M (2)	S (3)	L (1)	L (1)	S (3)	L (1)	M (2)	M (2)	M (2)
CO3	L (1)	S (3)	M (2)	M (2)	S (3)	M (2)	M (2)	L (1)	S (3)	L (1)
CO4	M (2)	M (2)	L (1)	S (3)	M (2)	L (1)	S (3)	-	M (2)	M (2)
CO5	M (2)	L (1)	S (3)	M (2)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)
W.AV	**1.8**	**1.8**	**2**	**1.6**	**1.8**	**2**	**2**	**1.4**	**1.6**	**1.6**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	M (2)	S (3)	L (1)	L (1)
CO2	M (2)	M (2)	M (2)	L (1)	S (3)
CO3	M (2)	L (1)	M (2)	M (2)	L (1)
CO4	M (2)	M (2)	L (1)	M (2)	S (3)
CO5	M (2)	M (2)	L (1)	M (2)	S (3)
W.AV	**2**	**1.6**	**1.6**	**1.4**	**2**

S –Strong (3), M-Medium (2), L- Low (1)

III – Semester					
Core	**556303**	**Ethical Hacking LAB**	**P**	**Credits:2**	**Hours:3**

Objectives	➢ To identify and assess vulnerabilities within a simulated environment. ➢ To simulate real-world attacks to test the security defences of systems. ➢ To prepare for and respond to security incidents effectively. ➢ To educate students about the risks associated with social engineering attacks. ➢ To understand and secure wireless networks against potential attacks.

1. Aggregate information from public database using online free tools Robtex, Nessus.
2. Windows linux system security.
3. Proxy server
4. Hacking Lab setup.
5. System hacking and security.
6. Windows Linux scripting.
7. Network hacking and security.
8. Foot Printing and Information gathering.
9. Google hacking.
10. Hacking attacks.
11. Web application hacking.
12. Honeypots.
13. Wireless and mobile hacking and security.

Outcomes	➢ Vulnerability Identification and Assessment. ➢ Hands-On Experience with Hacking Tools. ➢ Learn to respond to security incidents and conduct digital forensics investigations. ➢ Ethical Hacking Reporting and Documentation.

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)
CO2	S(3)	M(2)	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	M(2)	S(3)
CO3	S(3)	L(1)	M(2)	M(2)	S(3)	M(2)	M(2)	L(1)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)	L(1)	S(3)	S(3)	M(2)	S(3)
W.AV	**2.6**	**2**	**1.8**	**1.6**	**2**	**1.6**	**2**	**2.2**	**2.2**	**2.2**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	L(1)	M(2)	S(3)
CO2	M(2)	L(1)	M(2)	M(2)	L(1)
CO3	M(2)	M(2)	M(2)	L(1)	M(2)
CO4	S(3)	M(2)	L(1)	L(1)	M(2)
CO5	M(2)	L(1)	M(2)	S(3)	L(1)
W.AV	**2.4**	**1.6**	**1.6**	**1.8**	**1.8**

S –Strong (3), M-Medium (2), L- Low (1)

III - Semester					
Core	**556304**	**Mini Project**		**Credits:2**	**Hours:3**

III - Semester					
Core	**556305**	**Cyber Law Policies and IT Act**	**T**	**Credits:4**	**Hours:5**

Unit– I		
Objective 1	To understand Introduction to Cyber Law and Policies	
CYBER SPACE: Fundamental definitions -Interface of Technology and Law – Jurisprudence and-Jurisdiction in Cyber Space - Indian Context of Jurisdiction - Enforcement agencies – Need for IT act - UNCITRAL – E-Commerce basics .Information Technology Act, 2000 - Aims and Objects — Overview of the Act – Jurisdiction		
Outcome 1	Students will gain a foundational understanding of cyber law, policies, and the regulatory landscape in the context of information technology.	**K2**
Unit– II		
Objective 2	To learn E-Governance and Digital Signatures	
ELECTRONIC GOVERNANCE: Legal Recognition of Electronic Records and Electronic Evidence -Digital Signature Certificates - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators under the Act -The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability– Powers of Police under the Act – Impact of the Act on other Laws . Cyber Crimes -Meaning of Cyber Crimes –Different Kinds of Cyber crimes – Cyber crimes under IPC,		
Outcome 2	Students will explore legal aspects of e-governance initiatives and the use of digital signatures, understanding their legal validity and implications.	**K1**
Unit– III		
Objective 3	To learn about data protection law	
CR.P.C AND INDIAN EVIDENCE LAW: Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber Terrorism Violation of Privacy on Internet - Data Protection and Privacy – Indian Court cases.		
Outcome 3	Students will learn about data protection laws and regulations governing the collection, processing, and storage of personal and sensitive information.	**K4**
Unit–IV		
Objective 4	To understand the legal aspects of intellectual property rights	
INTELLECTUAL PROPERTY RIGHTS: Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases		
Outcome 4	Students will understand the legal aspects of intellectual property rights in the digital realm, including copyright, trademark.	**K3**
Unit–V		
Objective 5	To understand patents	
PATENTS: Understanding Patents - European Position on Computer related Patents, Legal position on Computer related Patents - Indian Position on Patents – Case Law, Domain names -registration - Domain Name Disputes-Cyber Squatting-IPR cases		
Outcome 5	Students will understand the legal aspects including patents and IPR.	**K5**

Suggested Readings:

1.Justice Yatindra Singh: Cyber Laws, Universal Law Publishing Co., New Delhi

2. Farouq Ahmed, Cyber Law in India, New Era publications, New Delhi

3. S.R.Myneni: Information Technology Law(Cyber Laws), Asia Law House, Hyderabad.

4. Chris Reed, Internet Law-Text and Materials, Cambridge University Press.

5. Pawan Duggal: Cyber Law- the Indian perspective Universal Law Publishing Co., New Delhi

Online Resources

https://www.legalserviceindia.com/

https://www.csk.gov.in/

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

Course designed by: Dr. T. Meyyappan

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	S (3)	M (2)	L (1)	M (2)	S (3)	M (2)	L (1)	L (1)	S (3)
CO2	L (1)	M (2)	S (3)	L (1)	L (1)	S (3)	S (3)	M (2)	M (2)	M (2)
CO3	M (2)	L (1)	M (2)	M (2)	S (3)	M (2)	L (1)	S (3)	S (3)	L (1)
CO4	S (3)	-	L (1)	S (3)	M (2)	L (1)	M (2)	M (2)	M (2)	M (2)
CO5	M (2)	M (2)	S (3)	M (2)	M (2)	M (2)	M (2)	L (1)	L (1)	L (1)
W.AV	**2**	**1.4**	**2**	**1.6**	**1.8**	**2**	**1.8**	**1.8**	**1.6**	**1.6**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	L (1)	S (3)	M (2)	L (1)
CO2	M (2)	S (3)	M (2)	M (2)	L (1)
CO3	M (2)	L (1)	M (2)	L (1)	M (2)
CO4	M (2)	S (3)	L (1)	M (2)	M (2)
CO5	M (2)	S (3)	L (1)	M (2)	M (2)
W.AV	**2**	**2**	**1.6**	**1.6**	**1.4**

S –Strong (3), M-Medium (2), L- Low (1)

III - Semester					
Core	**556306**	**Social Media Forensics**	**T**	**Credits:4**	**Hours:4**

Unit– I

Objective 1	Understanding Online Social Networks

What is Online Social Networks, data collection from social networks, challenges, opportunities, and drawbacks in online social network, Cybercrimes related to social media and its awareness, scrapping of data from social media API's.

Outcome 1	Overview of Social Media Forensics	**K2**

Unit– II

Objective 2	Cybercrimes and Awareness in Social Media

Information privacy disclosure, revelation and its effects in OSM and online social networks, Privacy issues related to location-based services on OSM.

Outcome 2	Cyber Crimes related to social media	**K3**

Unit– III

Objective 3	Legal and Ethical Considerations in World Social Media

Tracking social footprint / identities across different social network, Identifying fraudulent entities in online social networks, Effective and usable privacy setting and policies on OSM, Policing & OSM.

Outcome 3	Open-Source tools for social media analytics	**K3**

Unit–IV

Objective 4	To provide students with understanding of spam and fraud detection

Detection and characterization of spam, phishing, frauds, hate crime, abuse and extremism via online social media, Data Collection & Analysis, Fake News & content on Social media.

Outcome 4	Students understand the online & social media spam and fraud detection	**K4**

Unit–V

Objective 5	Students to know the social media forensics

Social Media Forensics: Case Studies Open-Source tools or social media analytics, Safety on social media. Legal Issues in world social media, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Outcome 5	Students will understand and analyze the social media forensics	**K5**

Suggested Readings:

1. Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics
2. Social Network Analysis: Methods and Application by Katherine Faust and Stanley Wasserman.
3. Understanding Social Networks: Theories, Concepts by Charles Kadushin.
4. Social Media Data Extraction and Content Analysis by Shalin Hai-Jew

Online Resources

https://dfrws.org/

https://www.digitalforensics.com/?utm_source=google&utm_medium=cpc&utm_campaign=DF-BRS-

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

Course designed by: Dr. T. Meyyappan

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S (3)	M (2)	M (2)	L (1)	S (3)	M (2)	S (3)	L (1)	L (1)	S (3)
CO2	M (2)	S (3)	S (3)	M (2)	S (3)	L (1)	L (1)	M (2)	L (1)	M (2)
CO3	L (1)	L (1)	M (2)	S (3)	M (2)	S (3)	M (2)	S (3)	M (2)	L (1)
CO4	-	M (2)	L (1)	M (2)	L (1)	M (2)	S (3)	M (2)	S (3)	M (2)
CO5	M (2)	M (2)	S (3)	L (1)	M (2)	M (2)	M (2)	L (1)	M (2)	L (1)
W.AV	**1.4**	**1.8**	**2**	**1.8**	**2**	**1.8**	**2**	**1.6**	**1.6**	**1.6**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S (3)	S (3)	L (1)	L (1)	M (2)
CO2	M (2)	M (2)	S (3)	L (1)	M (2)
CO3	M (2)	M (2)	L (1)	M (2)	L (1)
CO4	M (2)	L (1)	S (3)	M (2)	M (2)
CO5	M (2)	L (1)	S (3)	M (2)	M (2)
W.AV	**2**	**1.6**	**2**	**1.4**	**1.6**

S –Strong (3), M-Medium (2), L- Low (1)

III - Semester					
DSE	**556507**	**Data Analytics and Privacy**	**T**	**Credits: 3**	**Hours:3**

Unit – I

Objective: 1	To study about the design of data and Information formats. Management of Analysis.

INTRODUCTION TO BIG DATA AND ANALYTICS

Classification of Digital Data, Structured and Unstructured Data - Introduction to Big Data: Characteristics – Evolution – Definition - Challenges with Big Data - Other Characteristics of Data - Why Big Data - Traditional Business Intelligence versus Big Data - Data Warehouse and Hadoop Environment Big Data Analytics: Classification of Analytics – Challenges - Big Data Analytics important - Data Science - Data Scientist - Terminologies used in Big Data Environments - Basically Available Soft State Eventual Consistency - Top Analytics Tools

Outcome: 1	To capable to the big data and data analytics basic concepts

Unit - II

Objective: 2	To study about the Management of Data Analysis.

DATA ANALYTICS LIFE CYCLE AND ADVANCED METHODS

Discovery: Learning Business Domain – Resources – Framing the Problem – Identifying key stakeholders – Interviewing Analytics Sponsor – Developing Initial Hypotheses – Identifying Potential Data Sources, Data Preparation: Preparing Analytic Sandbox – Performing ETLT – Learning about Data – Data Conditioning – Survey and Visualize – Common Tools for the Data Preparation, Model Planning: Data Exploration and Variable Selection – Model Selection – Common Tools for the Data Preparation Phase, Model Building: Common Tools for the Model Building Phase, Communicate Results, Operationalize

Outcome: 2	To study the various process of data analytics

Unit – III

Objective: 3	To study about the Data Analytics Techniques.

ADVANCED DATA ANALYTICS METHODS

Clustering: Overview of Cluster - K Means Cluster – Other Cluster Algorithms, Association Rules: Overview – Apriori Algorithm – Evaluation of Candidate Rules – Applications of Association Rules – Validating and Testing, Regression: Linear Regression – Logistic Regression, Classification: Decision Tree – Naïve Bayes, Time Series Analysis: Overview – ARIMA model, Text Analysis: Text Analysis Steps – Collecting Raw Text – Representing Text – TFIDF – Categorizing Documents by Topics

Outcome: 3	To able to learn machine learning algorithms for data analytics

Unit – IV

Objective: 4	To know the Data Analytics Tools

ADVANCED DATA ANALYTICS TOOLS

Analytics for Unstructured Data: Use Cases - MapReduce - Apache Hadoop, Hadeoop Ecosystem: Pig – Hive – HBase – Mahout – NoSQL, Database Analytics: SQL Essentials – Joins – Set Operations – Grouping Extension – Advanced SQL – Window Function – User Defined Functions and Aggregates – Ordered Aggregates – MADlib

Outcome: 4	To study big data tools for data analytics

Unit – V					
Objective: 5	To learn the Privacy of data in data analytics				
DATA PRIVACY AND ETHICS Ethical Considerations in Data Analytics - Data Privacy Laws and Regulations - Responsible Data Handling - Privacy Landscape – Preferences – Personalize – Relationships – Rights and Responsibility – Conscientious and Conscious Responsibility – Balancing for Counterintelligence					
Outcome: 5	To learn the privacy ethics in data analytics				
Text Books: 1. Big Data, Privacy, and the Public Good: Frameworks for Engagement" by Julia Lane, Victoria Stodden, et al, Cambridge university press Data and Privacy: A Practical Guide" by Heather L. Buchta and Alicia M. Anderson, Apress					
Online Resources **https://fpf.org/** **https://iapp.org/**					
K1-Remember	***K2-Understand***	***K3-Apply***	***K4-Analyze***	***K5-Evaluate***	***K6-Create***
Coursedesignedby: Dr. S. Santhoshkumar					

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	M(2)	L(1)	M(2)
CO2	M(2)	M(2)	S(3)	M(2)	M(2)	M(2)	L(1)	S(3)	M(2)	S(3)
CO3	M(2)	S(3)	L(1)	M(2)	L(1)	M(2)	M(2)	L(1)	L(1)	S(3)
CO4	M(2)	L(1)	S(3)	L(1)	M(2)	M(2)	S(3)	M(2)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	S(3)	M(2)	L(1)
W.AV	**2**	**2.2**	**2.4**	**1.8**	**1.6**	**1.8**	**2.2**	**2.2**	**1.6**	**2.2**

S –Strong (3), M-Medium (2), L- Low (1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	S(3)	L(1)	M(2)	S(3)
CO2	L(1)	M(2)	M(2)	S(3)	M(2)
CO3	S(3)	L(1)	M(2)	M(2)	L(1)
CO4	M(2)	S(3)	L(1)	L(1)	M(2)
CO5	M(2)	M(2)	S(3)	L(1)	M(2)
W.AV	**2**	**2.2**	**1.8**	**1.8**	**2**

S –Strong (3), M-Medium (2), L- Low (1)

III - Semester					
DSE	**556508**	**IOT and Digital Forensics**	**T**	**Credits:3**	**Hours:3**

Unit - I		
Objective 1	To learn the basics of IoT, its generations, digitization, and convergence of IT and OT	
Introduction to IoT: What is IoT? Genesis of IoT – IoT and Digitization – IoT Impact-Convergence of IT and OT – IoT Challenges.		
Outcome 1	Learners understand the fundamentals of IoT, impact on digitization, and its associated challenges.	**K1**
Unit - II		
Objective 2	To understand the IoT Network Architecture and Design and Smart objects.	
IoT Network Architecture and Design: Drivers Behind New Network Architectures-Comparing IoT Architectures-IoT Data Management and Compute Stack. **Smart Objects: The "Things" in IoT:** Sensors, Actuators, and Smart Objects-Sensor Networks-IoT Access Technologies IEEE 802.15.4.		
Outcome 2	Learners acquire knowledge on IoT Architecture and Access Technologies.	**K2**
Unit–III		
Objective 3	To learn the fundamental of digital forensics, key technical concepts and its related labs and tools	
Introduction to Digital Forensics: Introduction- What is Forensic Science? - What is Digital Forensics? - Users of Digital Forensics - Locard's Exchange Principle - Scientific Method - Organizations of Note - Role of the Forensic Examiner in the Judicial System. **Key Technical Concepts:** Bits, Bytes, and Numbering Schemes-File Extensions and File Signatures – Storage and Memory-Computing Environments – Data Types – File Systems- Allocated and Unallocated Space – How Magnetic Hard Drives Store Data-Basic Computer Function-Putting it All Together. **Labs And Tools:** Forensic Laboratories-Policies and Procedures-Quality Assurance-Digital Forensic Tools-Accreditation.		
Outcome 3	Learners gain knowledge on the digital data, role of digital forensics, policies, and procedures	**K3**
Unit–IV		
Objective 4	To understand Collecting Evidence, Windows System Artifacts and Antiforensics.	
Collecting Evidence: Crime Scenes and Collecting Evidence-Documenting the Scene-Chain of Custody-Cloning-Live System versus Dead System – Hashing-Final Report. **Windows System Artifacts:** Deleted Data-Hibernation File-Registry-Print Spooling – Recycle Bin – Metadata – Thumbnail Cache-Most Recently Used-Restore Points and Shadow Copy-Prefetch-Link Files. **Antiforensics:** Hiding Data-Password Attacks-Steganography-Data Destruction.		
Outcome 4	Learners understand how to collect the evidence, document it and protect it	**K4**
Unit–V		
Objective 5	To provide learners with knowledge in criminal law, legal search procedures, network forensics, and mobile device forensics.	
Legal: The fourth Amendment-Criminal Law-Searches without a Warrant-Searching with a Warrant-Searching with a Warrant-Electronic Discovery. **Network Forensics:** Introduction-Network Fundamentals-Network Security Tools - Network Attacks - Incident Response – Network Evidence and Investigations. **Mobile Device Forensics:** Introduction-Cellular Networks-Operating Systems-Cell Phone Evidence-Cell Phone Forensic Tools-GPS.		
Outcome 5	Learners gained proficiency in applying legal concepts, utilizing security tools, and legal challenges in digital environments.	**K5**

Textbooks:

1. Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., & Henry, J. (2017). *IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things*. Cisco Press.
2. John Sammons, The Basics of Digital Forensics, 2nd Edition, Elsevier, 2014

Suggested Readings:

1. Raj, P., & Raman, A. C. (2017). The Internet of Things: Enabling technologies, platforms, and use cases. Auerbach Publications.
2. Kranz, M. (2016). Building the internet of things: Implement new business models, disrupt competitors, transform your industry. John Wiley & Sons.
3. B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations, 4th Edition, Course Technology, 2010.
4. John Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Laxmi Publications, 2005.

Online Resources

https://iotsecurityfoundation.org/

https://sectrio.com/resources/compliance-kits/iot-ot-cybersecurity-self-assessment-tool-using-nist-csf/?utm_term=&utm_campaign=APAC-Request-

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

Course designed by: Dr. A. Padmapriya

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	L(1)	S(3)	S(3)	M(2)	L(1)	S(3)	S(3)	S(3)	M(2)	L(1)
CO2	L(1)	L(1)	M(2)	M(2)	L(1)	M(2)	S(3)	S(3)	S(3)	L(1)
CO3	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	S(3)	S(3)	M(2)	M(2)
CO4	L(1)	L(1)	M(2)	S(3)	L(1)	M(2)	S(3)	S(3)	S(3)	L(1)
CO5	L(1)	L(1)	L(1)	M(2)	M(2)	S(3)	S(3)	S(3)	M(2)	M(2)
W. AV	**1.2**	**2.2**	**1.8**	**2.2**	**1.6**	**2.4**	**2.8**	**3.0**	**2.4**	**1.4**

S–Strong(3),M-Medium(2),L-Low(1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	S(3)	L(1)	M(2)
CO2	M(2)	M(2)	M(2)	L(1)	M(2)
CO3	S(3)	S(3)	S(3)	S(3)	M(2)
CO4	S(3)	S(3)	S(3)	M(2)	M(2)
CO5	M(2)	M(2)	M(2)	M(2)	M(2)
W. AV	**2.6**	**2.4**	**2.6**	**2.0**	**2.0**

S–Strong(3),M-Medium(2),L-Low(1)

III - Semester					
DSE	**556509**	**Security Standards and Compliance**	**T**	**Credits:3**	**Hours:3**

Unit - I		
Objective 1	To understand the Governance, Risk, and Compliance (GRC) and the significance of governance standards.	
Governance, Risk & Compliance GRC: Definitions–Governance, Risk, Compliance, Risk Threshold, Risk Modelling, Risk Appetite, Governance Standards.		
Outcome 1	Learners gained knowledge in defining GRC terms, its risk thresholds, risk modelling and the role of governance standards.	**K1**
Unit - II		
Objective 2	To enable learners to grasp information on industry standards like ITIL, ISO/IEC 27001, COBIT, and other models in IT Governance.	
Best Practices for IT Governance: ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT) – The Information Security Management Maturity Model - Capability Maturity Model – latest standards and compliance technologies.		
Outcome 2	Learners acquire a deep understanding of IT Governance best practices.	**K2**
Unit–III		
Objective 3	To promote and give expertise to the learner in information security governance, its importance, outcomes, strategic planning, and policies and procedures.	
Information Security Governance: Effective Information Security Governance - Importance of Information Security Governance - Outcomes of Information Security Governance - Strategic alignment – Risk Management - Performance Measurement - Information System Strategy - Strategic Planning - Steering Committee- Policies and Procedures.		
Outcome 3	Learners gain a comprehensive understanding of Information Security Governance.	**K3**
Unit–IV		
Objective 4	To emphasize the learners' need to learn about personnel, financial, quality management, and risk assessment frameworks (COSO, NIST).	
Information Security Management Practices: Personnel Management - Financial Management–Quality Management - Information Security Management - Performance Optimization - Roles and Responsibilities - Auditing IT Governance Structure - Evaluation Criteria & Benchmark - Assessment Tools -Case Study Analysis - Risk Management framework–COSO - The Internal environment - Objective Setting -Event Identification - Risk assessment - Risk Response - Control activities - Information & communication–Monitoring–NIST - Risk Assessment - Risk Mitigation - Evaluation & Assessment - Case Study Analysis.		
Outcome 4	Learners acquire practical skills to implement information security management practices effectively.	**K4**

Unit–V		
Objective 5	To provide learners with a comprehensive understanding of compliance and the evolution of information systems security, its growth, and regulatory requirements in compliance.	
Compliance–Introduction-Information Technology and Security: Evolution of Information systems -Roles and responsibilities - Audit, Assessment and Review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance - Compliance officer activities - The requirements of a Compliance Officer		
Outcome 5	Learners will gain proficiency in implementing and managing compliance processes and apply best practices for IT compliance under various regulatory frameworks.	**K5**

Suggested Readings:

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

Information Security Governance: Guidance for Boards of Directors and Executive Management, 2ndEdition by W. Krag Brot by, 2nd Edition, ISACA Publication, 01 Mar 2006.

Security Governance Checklists: Business Operations, Security Governance, Risk Management, and Enterprise Security Architecture by Fred Cohen, Large Print Edition, Fred Cohen & Associates Publication, 2005.

CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016

IT Compliance and Controls: Best Practices for Implementation by James J., IV DeLuccia, Illustrated Edition, Wiley Publication, 2008

The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments by Craig S. Wright, Brian Freedman, Dale Liu, 1st Edition, Syngress Publication, 2008

Online Resources

https://www.pcisecuritystandards.org/

https://www.iso.org/standard/iso-iec-27000-family

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

Coursedesignedby: Dr. S. Santhoshkumar

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	L(1)	L(1)	S(3)	S(3)	L(1)	S(3)	M(2)	S(3)	L(1)	L(1)
CO2	M(2)	M(2)	S(3)	S(3)	M(2)	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	L(1)	S(3)	S(3)	L(1)	S(3)	M(2)	M(2)	M(2)	M(2)
CO4	L(1)	M(2)	M(2)	M(2)	L(1)	S(3)	S(3)	S(3)	M(2)	M(2)
CO5	M(2)	M(2)	M(2)	M(2)	L(1)	M(2)	M(2)	M(2)	L(1)	L(1)
W. AV	**1.4**	**1.6**	**2.6**	**2.6**	**1.2**	**2.8**	**2.2**	**2.6**	**1.6**	**1.4**

S–Strong(3),M-Medium(2),L-Low(1)

Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	M(2)	S(3)	S(3)
CO2	S(3)	M(2)	M(2)	S(3)	S(3)
CO3	M(2)	L(1)	L(1)	S(3)	S(3)
CO4	S(3)	M(2)	L(1)	S(3)	S(3)
CO5	S(3)	M(2)	M(2)	S(3)	S(3)
W. AV	**2.8**	**1.8**	**1.6**	**3.0**	**3.0**

S–Strong(3),M-Medium(2),L-Low(1)

IV - Semester					
Core	**556401**	**Reverse Engineering and Malware Analysis**	**T**	**Credits:2**	**Hours:2**

Unit - I		
Objective 1	To learn the basics of Reverse Engineering, identification and extraction of hidden components and static and dynamic reversing analyses.	
Reverse Engineering: Technical Requirements - Reverse engineering as a process – Tools - Malware handling - Basic analysis lab setup. **Identification and Extraction of Hidden Components:** Technical requirements operating system environment-Typical malware behavior-Tools. **Static and Dynamic Reversing:** Assessment and static analysis-Dynamic analysis.		
Outcome 1	Learners will develop how to execute reverse engineering processes, understand operating system environments, and recognize typical malware behaviour.	**K1**
Unit - II		
Objective 2	To provide learners with the basics of Malware Analysis, its types and their behaviour.	
Introduction to Malware Analysis: Types of Malware and their Behavior - Computer Infection Program - Life Cycle of a Malware - Virus Nomenclature - Worm Nomenclature - Tools used in Computer Virology.		
Outcome 2	Learners will gain knowledge in identifying and analyzing various types of malware.	**K2**
Unit–III		
Objective 3	To understand how to implement covert channels, explore Trojan Horses and a case study on the Conflicted C Worm.	
Implementation of Covert Channel: Non-Self-Reproducing Malware - Working Principle of Trojan Horse - Implementation of Remote Access and File Transfer - Working Principle of Logic Bomb - Case Study – Conflicted C Worm.		
Outcome 3	Learners will acquire practical skills in implementing covert channels in cyber security.	**K3**
Unit–IV		
Objective 4	To learn virus design components, malware design using open source, testing, and case studies	
Virus Design and Its Implications: Virus Components: Function of Replicator, Function of Concealer, Function of Dispatcher - Trigger Mechanisms - Testing Virus Codes - Case Study: Brute force logical bomb. **Malware Design using Open Source:** Computer Virus in Interpreted Programming Language - Designing Shell bash virus under Linux - Fighting over infection – Polymorphism - Case Study – Companion Virus.		
Outcome 4	Learners gain practical knowledge of virus design and malware creation skills through case studies.	**K4**
Unit–V		
Objective 5	To learn the analysis of a malware specimen and explore automated frameworks on it.	
Analysis of a Malware Specimen: Guidelines for Examining a Malicious File Specimen - Establishing the Environment Baseline S – Pre-Execution Preparation - System and Network Monitoring - Execution Artefact Capture - Digital Impression and Trace Evidence: Executing the Malicious Code Specimen, Execution Trajectory Analysis: Observing Network, Process, Api, File System, and Registry Activity - Automated Malware Analysis Frameworks		

Outcome 5	Learners gain knowledge in comprehensive malware analysis and master the guidelines, preparation, and advancement in malware specimens.	**K5**

Suggested Readings:

Mastering Reverse Engineering: Reginald Wong, Published by Packt Publishing Ltd. 2018.

Michael Sikorski, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, 2012, No Starch Press.

Learning Malware Analysis, K A Monnappa, Packt Publishing Limited.

Reversing Secrets of Reverse Engineering, Eldad Eilam , Wiley Publisher, 2011.

Malware Forensics Investigating and Analyzing Malicious Code, Eoghan Casey, Cameron H. Malin, James M. Aquilina, Elsevier Science, 2008

Online Resources

https://www.virustotal.com/gui/home/upload

https://www.malware-traffic-analysis.net/

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

Coursedesignedby: Dr. S. Santhoshkumar

CourseOutcomeVSProgrammeOutcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	L(1)	M(2)	M(2)	M(2)	M(2)	S(3)	S(3)	M(2)	M(2)
CO2	M(2)	M(2)	M(2)	S(3)	S(3)	M(2)	S(3)	S(3)	M(2)	L(1)
CO3	M(2)	L(1)	M(2)	M(2)	M(2)	S(3)	M(2)	M(2)	S(3)	M(2)
CO4	L(1)	M(2)	L(1)	L(1)	M(2)	M(2)	M(2)	M(2)	L(1)	L(1)
CO5	L(1)	L(1)	M(2)	M(2)	L(1)	S(3)	M(2)	M(2)	M(2)	L(1)
W. AV	**1.6**	**1.4**	**1.8**	**2.0**	**2.0**	**2.4**	**2.4**	**2.4**	**2**	**1.4**

S–Strong(3),M-Medium(2),L-Low(1)

CourseOutcomeVSProgrammeSpecificOutcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	S(3)	M(2)	M(2)	S(3)	L(1)
CO2	S(3)	M(2)	M(2)	S(3)	L(1)
CO3	S(3)	M(2)	S(3)	S(3)	M(2)
CO4	S(3)	M(2)	S(3)	S(3)	L(1)
CO5	S(3)	M(2)	S(3)	S(3)	L(1)
W. AV	**3.0**	**2.0**	**2.6**	**3.0**	**1.2**

S–Strong(3),M-Medium(2),L-Low(1)

IV - Semester					
Core	**556402**	**Project Work**		**Credits: 12**	**Hours--**

SCIENCE CAMPUS