SACRED HEART COLLEGE (AUTONOMOUS)

Tirupattur – 635 601, Tamil Nadu, S.India

Resi : (04179) 220103
College : (04179) 220553
Fax : (04179) 226423

Ready for
Every Good Work

A Don Bosco Institution of Higher Education, Founded in 1951 * Affiliated to Thiruvalluvar University, Vellore * Autonomous since 1987

Accredited by NAAC (4th Cycle – under RAF) with CGPA of 3.31 / 4 at 'A+' Grade

Postgraduate Diploma in Cyber Security

Regulations and Curriculum

(Effective for the Batches admitted from the Academic Year 2021-2022)

PG AND RESEARCH DEPARTMENT OF COMPUTER APPLICATIONS SACRED HEART COLLEGE(AUTONOMOUS), TIRUPATTUR

TIRUPATTUR DT, TAMILNADU.

Postgraduate Diploma in Cyber Security(PGDCS)

1. Programme Objectives

The Post Graduate Diploma in Cyber Security (PGDCS) is designed to prepare the students for careers in cyber security. This course is designed to provide a foundational platform for Cyber Security Aspirants by teaching the basics and core of Cyber Security that enables them to identify and remove a scam or attack before it is fully enacted, thus minimizing damage to the resources and ensuring the protection of information technology assets.

2. Eligibility for Admission

Any Bachelor's Degree with Mathematics/Statistics/Business Mathematics as an Allied Subject / Mathematics/Statistics in +2 Level.

3. Duration of the Programme

To fulfill the requirements for acquiring PGDCS, a student may clear all the courses in a minimum of one year and a maximum of 2 years.

4. Medium of Instruction

The medium of instruction is only in **English.**

5. Examination

The course will follow the Continuous Internal Assessment (CIA) and End semester examination.

6. Outcomes

i. Makes the professional qualified to deal with information systems security, control and auditing the security protocols and ensuring the integrity of the information system.

ii. Teaches to identify vulnerabilities and check whether the information system in question is complying with the required standards and rules of information systems security.

iii. Enables to control and govern an IT system and helps you understand the implementation of information systems.

iv. Prepares to have complete understanding and control of the information system.

7. Programme Structure

Semester	Code	Title of the Subject	L	TCP	P	IM	SM	TM	CD
I	CADC101	Fundamentals of Information Security	4			50	50	100	4
	CADC102	Data Communication and Networking	4			50	50	100	4
	CADC103	Vulnerability Analysis, Penetration Testing, and Incident	4			50	50	100	4
	CADC104	Security Strategies in	4	1		50	50	100	4
			16	**1**		**200**	**200**	**400**	**16**
II	CADC201	Network Cyber Security	4			50	50	100	4
	CADC202	Cyber Forensics	4			50	50	100	4
	CADC203	Application Cyber Security	3	1		50	50	100	4
	CADC204	Big Data & IOT	3	1		50	50	100	4
	CADC205	Advanced Ethical Hacking	3	1		50	50	100	4
	CADC206P	Internship			10	50	50	100	9
			17	**3**	**10**	**300**	**300**	**600**	**29**
	Total Credits								**45**

List of Theory Combined Practical Papers

Semester	Code	Course Title
I	CADC104	Security Strategies in Operating Systems
II	CADC203	Application Cyber Security
II	CADC204	Big Data & IOT Security
II	CADC205	Advanced Ethical Hacking

7.1 Coding Scheme

PGD	X	X	X	X
Programme	Semester	Curriculum Revision	Course Serial Number 0-9	Course Type*

Course Type: T–Theory, I – Internal Papers, J - Internship.

7.2. Conduct of Theory and Practical Courses

7.2.1. Theory Papers will follow the regular lecturing method.

7.2.2. Theory Combined Practical papers will follow lecturing and demonstrations and lab exercises fixed by the course teacher**., the practical exercises will be done as self-learning by the students outside the classes in their laptops and submitted to the faculty for evaluation**. **The regular lab shall not be used for the diploma programmes.** The practical exercises shall be assigned by the course teacher.

8 SYLLABI IN DETAIL

I SEMESTER

CADC101 FUNDAMENTALS OF INFORMATION SECURITY 4-0-0:100

OBJECTIVES

- To learn the fundamentals of Cryptography and its applications.
- To undertand the types of malwares.
- To learn the ethical issues in information security.

Unit I

Information Security Concepts and Cryptography Information Security Concepts: Information security issues, goals, architecture, attacks, Security Services and Mechanisms.

Unit II

Introduction to Cryptography: Network security model, Cryptographic systems, Cryptanalysis, Steganography. Types of Cryptography: Symmetric key and Asymmetric Key Cryptography, Encryption and Decryption Techniques.

Unit III

Cryptographic Algorithms: Cryptographic hash, Message Digest, Data Encryption Standard, Advanced Encryption Standard, RSA

Unit IV

Malware: Viruses, Worms, Trojan horses Security Counter Measures; Intrusion Detection

Systems, Antivirus Software

Unit V

Ethical Issues in Information Security & Privacy Information Security, Privacy and Ethics

Cyber Crime and Cyber Terrorism Hacking: Ethical issues

TEXT

1. Bruce Schneier, “Secrets & Lies: Digital Security in a Networked World” Tata McGraw Hill, 2000.

2. Christopher Hadnagy, “Social Engineering”, PHI, 2010

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

CADC102 DATA COMMUNICATION AND NETWORKING 4-0-0:100

OBJECTIVES

- To learn the architecture of Data communication and networking.
- To understand the layerd architecture of TCP/IP.

Unit I

Introduction to Data communication and Networking Fundamentals of data communication and networking Network Reference Models: OSI and TCP/IP Models - Transmission media and network devices

Unit II

Physical and data link layer functionalities - Analog and Digital Signals - Encoding Multiplexing and Switching: FDM,TDM,WDM,SDM, Message Switching and Circuit Switching and Packet Switching –

Unit III

Data Link Control Protocols: Token Passing, CSMA/CD,CSMA,CSMA/CA

Unit IV

Network Layer : Internetworking, and IP addressing, ARP, RARP,ICMP,IGMP Unit-2

Transport Layer protocols: TCP& UDP

Unit V

Application Layer protocols: HTTP, HTTPs, SMTP, POP, DNS, TELNET, FTP Unit-4

Internet and its Services: Intranet, Extranet, www, Email

TEXT

1. Forouzan, “Data Communications and Networking”, Pearson, 2017

2. William Stallings, “Data and Computer Communications” , Pearson, 2017

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

CADC103 VULNERABILITY ANALYSIS, PENETRATION TESTING, AND INCIDENT HANDLING

4-0-0:100

OBJECTIVES

- To Learn the core concepts of Vulnerability Analysis.
- To understand the process of penetration testing.
- To learn about incident handling technique.

Unit I

Vulnerability Analysis – Introduction – Hardware and Software defects – Unsecured Networks – Vulnerability management programs – Maintaining an Asset Inventory

Unit II

Vulnerability Analysis – Establishing Secure Connections – Maintaining awareness and Detecting vulnerabilities – Mitigating and remediating identified vulnerabilities – Continuously monitoring the organizations IT environment.

Unit III

Penetration Testing – introduction – method – penetration testing vs vulnerability analysis – types – Manual – Automated – Tools – Infrastructure – Testers – Limitations – Remediation – Legal Issues.

Unit IV

Incident Handling – Preparing for a cyber security incident – Detecting and Identifying potential cyber security incidents – categories of incidents – methods to detect incidents.

Unit V

Incident Handling - Handling and actual incident – contain , eradicate and recover – Communication during a cyber security incident – Incident follow-up and closure.

TEXT

1. http://www.amazon.com/dp/0470170778.

2. http://www.amazon.com/The-Tangled-Web-Securing-Applications/dp/1593273886.

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

CADC104 SECURITY STRATEGIES IN OPERATING SYSTEMS 4-1-0:100

OBJECTIVES

- To Learn the fundamentals of security strategies in Operating Systems.
- To Learn Operating system security tools.

Unit I

Introduction – Operating Systems hardening – Removing all unnecessary software alerts – removing all unessential services – alter default accounts – apply the principle of least privilege – perform updates – turn on logging and auditing

Unit II

Protecting against malware – anti malware tools – executable space protection – software firewalls and host intrusion detection

Unit III

Operating systems security tools – scanners – vulnerability assessment tools – exploit frameworks

Unit IV

Case Study : Security features in windows operating system

Unit V

Case Study : Security features in Linux operating system

TEXT

1. Michael Palmer, “Guide to Operating Systems Security”, PHI, 2018

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

II SEMESTER

CADC201 NETWORK CYBER SECURITY 4-0-0:100

OBJECTIVES

- To Understand the basics of network cyber security.
- To Learn the issues in wireless networks and internet.

Unit I

Network Security Model, Network Security Threats - Firewalls: Overview, Types, Features, User Management - Intrusion Detection System , Intrusion Prevention System

Unit II

Public Key Infrastructure, Digital Signature Schemes- Internet and Web Application Security - Email security: PGP and SMIME - Web Security: Web authentication, Injection Flaws, SQL Injection

Unit III

Web Browser Security - E-Commerce Security - Wireless Network Security - Wireless

Network Components

Unit IV

Security issues in Wireless Networks - Securing a Wireless Network - Mobile Security

Unit V

Case Study : Security in Google Chrome , Security in WAP and Android OS

TEXT

1. Chris Sanders and Jason Smith, “Applied Network Security Monitoring”, PHI, 2019

2. William Stallings, “Data and Computer Communications”, Pearson, 2017

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

CADC202	CYBER FORENSICS	4-0-0:100

OBJECTIVES

- To learn the basics of cyber forensics.
- To understand the types of cyber forensic systems.

Unit I

Introduction to Cyber forensics: Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases. Analyzing malicious software. Types of Computer Forensics Technology, Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems

Unit II

Types of Computer Forensics Systems: Internet Security Systems, Intrusion Detection Systems, Firewall Security Systems, Storage Area Network Security Systems, Network Disaster Recovery Systems, Public Key Infrastructure Systems, Wireless Network Security Systems, Satellite Encryption Security Systems, Instant Messaging (IM) Security Systems, Net Privacy Systems, Identity Management Security Systems, Identity Theft, Biometric Security Systems ,Router Forensics. Cyber forensics tools and case studies. Ethical Hacking: Essential Terminology, Windows Hacking, Malware, Scanning, Cracking.

Unit III

Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles,

Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Investigating Web attacks, Investigating network Traffic ,Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events.

Unit IV

Basic of law, Understanding cyber space, Defining cyber law, Scope and jurisprudence ,

Concept of jurisprudence, Overview of Indian legal system, Introduction to IT Act 2000, Amendment in IT Act.

Unit V

Cyber Crimes – Types of cyber crimes –against individuals institution, and states-various offenses and punishments, digital signature-concepts of public key and private key, certification authorities and their role, creation and authentication of digital signature. E-contracting –salient features of E-contracts, formation of E-contracts and types, E-governance, E-governance models, E-commerce- salient features and advantages.

Text

1. John R. Vacca, "Computer Forensics: Computer Crime Scene Investigation", Second Edition, Charles River Media, 200

2. Ravi Kumar & B Jain, "Cyber Forensics - Concepts and Approaches", icfai university press, 2006.

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

CADC203	APPLICATION CYBER SECURITY	3-1-0:100

OBJECTIVES

- To learn the concepts in application level cyber security.
- To understand the concepts of ethical hacking and cyber laws.

Unit I

System Security - Desktop Security - Programming Bugs and Malicious code - Database Security

Unit II

Operating System Security – Designing Secure Operating System – OS Security Vulnerabilities – Security Management – Disaster recovery – Digital signature

Unit III

Ethical Hacking – Penetration testing – Computer Forensics

Unit IV

Cyber Laws and Standards - ISO 27001, Cyber Law (Information Technology Act, 2000)- International Standards maintained for Cyber Security

Unit V

Security Audit ,Investigation by Investing Agency - Cyber Security Solutions

TEXT

1. Andrew Honig and Michael Sikorski “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”, , Pearson, 2019

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

CADC204 **BIG DATA & IOT SECURITY** **3-1-0:100**

OBJECTIVES

- To undertand the consequences of security in BigData and IoT.
- To learn the security mechanisms applied in BigData and IoT.

Unit I

IOT-SECURITY OVERVIEW IoTReference Model- Introduction -Functional View,IoT Security Challenges-Hardware Security Risks - Hardcoded/Default Passwords -Resource Constrained Computations -Legacy Assets Connections - Devices Physical Security, Software Security Risks - Software Vulnerabilities -Data Interception - Identification of Endpoints - Tamper Detection, Lack of Industrial Standards

Unit II

SECURED PROTOCOLS FOR IOT Infrastructure-IPv6 -LowPAN , Identification-Electronic Product Code -uCode, Transport-Bluetooth - LPWAN, Data -MQTT -CoAP, Multi-layer Frameworks-Alljoyn,-IoTivity

Unit III

SECURING INTERNET OF THINGS ENVIRONMENT IoT Hardware -Test Device Range- Latency and Capacity -Manufacturability Test -Secure from Physical Attacks, IoT Software - Trusted IoT Application Platforms, -Secure Firmware Updating -Network Enforced Policy - Secure AnalyticsVisibility and Control

Unit IV

Big Data Security – Introduction – Implementation of Security in Big Data - Reasons to Implement security in Big Data – Big Data Security Technologies – Encryption – User Access Control – Physical Security – Centralized Key Management

Unit V

Big data Security – Use Cases – Cloud Security Monitoring – Network traffic analysis – Insider Threat Detection – Threat Hunting – User Behaviour Analysis – Big data Security Issues

TEXT

1. Harley Hahn, “Internet Complete Reference”, Second Edition, Osborne/McGrawHill 1996,

2. Ramesh Bangia Firewall Media, “Internet and Web Design”, (An imprint of Lakshmi Publications Pvt. Ltd.). Second Edition 2006

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

CADC205 **ETHICAL HACKING** **3-1-0:100**

OBJECTIVES

- To understand the basics of Ethical hacking.
- To learn the types of hacking and DDOS attacks.

Unit I

Basics – Definition – Types – Advantages – Disadvantages – Purpose – Hacker Types – Terminologies – Tools – Skills – Process

Unit II

Types of Hacking – Foot printing – Fingerprinting – sniffing – sniffing tools – ARP Poisoning – DNS Poisoning –

Unit III

Types of Hacking – Exploitation – Enumeration – Metasploit – Trojan Attacks –

Unit IV

TCP/IP Hijacking – Email Hijacking – Password Hacking – Wireless Hacking – Social Engineering

Unit V

DDOS Attacks – Cross Site Scripting – SQL Injection – Pen Testing

TEXT

1. ChristofPaar, Jan Pelzl, “Understanding Cryptography: A Textbook for Students and Practitioners”, Second Edition, Springer’s, 2010.

2. Ali Jahangiri, “Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts”, First Edition, 2009.

QUESTION PAPER PATTERN

CA Tests **Max. Marks: 50**

The time duration for the examination is 2 Hrs. The question paper format is:

Section A Answer **ALL** the Questions.

[Atleast four questions from each unit] 6 x 2 = 12

Section B Answer **ALL** the Questions

[Atleast three questions from each unit. Either or Type] 3 x 6 = 18

Section C Answer **ANY TWO** Questions out of THREE Questions.

[Atleast one question from each unit] 2 x 10 = 20

End-Semester Examinations **Max. Marks: 100**

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Section A Answer **ALL** the Questions.

[Atleast two questions from each unit] 10 x 2 = 20

Section B Answer **ALL** Questions.

[Either or Type, atleast one question from each unit] 5 x 7 = 35

Section C Answer **ANY THREE** Questions out of FIVE Questions.

[Atleast one question from each unit] 3 x 15 = 45

9. EVALUATION & CERTIFICATION

9.1 Continuous Assessment

S. No.	Course Type	Internal Components	Marks	Total
1	Theory	2 CA Tests	30	**50**
		Online Test / Quiz	5	
		*Other Components	15	
		Paper Work		
		Problem Solving / Group Discussion /		
		Technical reports		
		Application Development		
		Seminar		
		Demonstration		
		Open Book Assignment		
2	Theory Combined Practical	2 CA Tests	30	**50**
		Online Test / Quiz	5	
		Paper Work	5	
		Demonstration/Technical Report		
		Lab Exercises	10	

Note: ***Other components can be fixed up by the course teacher with the endorsement of the HOD.***

9.2 CA Tests

The time duration for the examination is 2 Hrs. The question paper format is:

Max. Marks : 50	
Section A	
Answer ALL the Questions [atleast 3 questions from each unit]	6 X 2 = 12 Marks
Section B	
Answer ALL the Questions [Either or Type, atleast 3 questions from each unit]	3 X 6 = 18 Marks
Section C	
Answer ANY TWO Questions out of Three Questions [atleast 1 question from each unit]	2 X 10 = 20 Marks

9.3 End-Semester Examinations

9.3.1 Theory

The time duration for the examination is 3 Hrs. The question paper format for the end-semester examination is:

Max. Marks : 100	
Section A	
Answer ALL the Questions [atleast 2 questions from each unit]	10 X 2 = 20 Marks
Section B	
Answer ALL the Questions [Either or Type, atleast 1 question from each unit]	5 X 7 = 35 Marks
Section C	
Answer ANY THREE Questions out of FIVE Questions [atleast 1 question from each unit]	3 X 15 = 45 Marks

9.3.2 Internship :: CADC206P

- Internship will be carried out during the summer vacation after the Ist Semester.
- The total duration for the internship will be three weeks.
- Preparatory work for the internship will be one week, followed by two weeks of internship in a IT/Non-IT Companies where network Security is applied / to be applied.
- During the preparatory work, the students has to work with their respective supervisors allotted by the Department.
- At the end of the preparatory work, the student has to submit a technical report not less than 20 pages, describing the knowledge acquired by the student in the respective field of study.
- After the completion of the Internship in the respective company, the student has to produce the intership completion certificate issued by the company to the Department.
- The student's internship will be evaluated through a review and a viva will be conducted through external members,.

Internal Assessment (Internship Guide) **Total - 50 Marks**

- Industry, Domain and Problem Study - 10 Marks
- Technical Report - 25 Marks
- Presentation of the Technical Report - 15 Marks

External Assessment **Total - 50 Marks**

- Review of the internhip - 30 Marks
- Viva Voce - 20 Marks