SWAMI VIVEKANAND SUBHARTI UNIVERSITY, MEERUT

FACULTY OF ENGINEERING & TECHONOLOGY

ORDINANCE No. V-42 (B2)

RELATING TO COURSE CURRICULUM & SYLLABUS OF PG PROGRAM

MASTER OF TECHNOLOGY (M.Tech.) CYBER SECURITY

(Effective from the Session – 2025-26)

Apporved by the Academic Council of the Meeting held on 06 May 2025

Apporved by the Executive Council of the Meeting held on 28 June 2025

Faculty of Engineering & Technology DEAN

SWAMI VIVEKANAND SUBHARTI UNIVERSITY, MEERUT
SUBHARTI INSTITUTE OF TECHNOLOGY AND ENGINEERING
STUDY & EVALUATION SCHEME as per NEP-2020

SWAMI VIVEKANAND

SUBHARTI UNIVERSITY, MEERUT

EVALUATION SCHEME & SYLLABUS
as per NEP 2020

M.TECH. (CYBER SECURITY)

W.E.F. SESSION 2025-26

SUBHARTI INSTITUTE OF TECHNOLOGY AND ENGINEERING
Subhartipuram, NH-58 Delhi-Haridwar Bypass Road
Meerut -250005 (UP)
www.subharti.org

DEAN

SWAMI VIVEKANAND SUBHARTI UNIVERSITY, MEERUT
SUBHARTI INSTITUTE OF TECHNOLOGY AND ENGINEERING
STUDY & EVALUATION SCHEME as per NEP-2020
M.Tech I Year/I Semester (CYBER SECURITY)
w.e.f academic Session 2025-26

SEMESTER I: Foundation and Advanced Core Concepts														
S. No.	Course Code	Course Name	Course Type	Periods			CCA				ESE		Total	Credit
				L	T	P	CT	TA	Total	PS	TE	PE		
1	PCS-101	Cyber Crime Investigations and Cyber Forensics	Core Subject	3	1	0	20	10	30	-	70	-	100	4
2	PCS -102	Research Methodology and IPR	Core Subject	3	1	0	20	10	30	-	70	-	100	4
3	PCS -103	Virtualization and Cloud Security	Core Subject	3	1	0	20	10	30	-	70	-	100	4
4	PCS -115 to PCS -118	Elective -I	Elective - I	3	0	0	20	10	30	-	70	-	100	3
5	PCS -119 to PCS-122	Elective -2	Elective - 2	3	0	0	20	10	30	-	70	-	100	3
6	PCSE -127 to PCSE -129	Open Elective - I	Open Elective - I	3	0	0	20	10	30	-	70	-	100	3
7	PCS -151	Security Lab - I	Lab	0	0	4	-	-	-	15	-	35	50	2
TOTAL													650	23

M.Tech I Year/II Semester (CYBER SECURITY)
w.e.f academic Session 2025-26

SEMESTER I: Foundation and Advanced Core Concepts														
S. No.	Course Code	Course Name	Course Type	Periods			CCA				ESE		Total	Credit
				L	T	P	CT	TA	Total	PS	TE	PE		
1	PCS -201	Legal Dimension of IPR in Cyber World	Core Subjects	3	1	0	20	10	30	-	70	-	100	4
2	PCS -202	Web Services Security	Core Subjects	3	1	0	20	10	30	-	70	-	100	4
3	PCS -203	English for Research Paper Writing	Core Subjects	3	1	0	20	10	30	-	70	-	100	4
4	PCS -215 to PCS -218	Elective -3	Elective -3	3	0	0	20	10	30	-	70	-	100	3
5	PCS -219 to PCS-222	Elective -4	Elective -4	3	0	0	20	10	30	-	70	-	100	3
6	PCSE -227 to PCSE -229	Open Elective–II	Open Elective–II	3	0	0	20	10	30	-	70	-	100	3
7	PCS -251	Security Lab - II	LAB	0	0	4	-	-	-	15	-	35	50	
	PCS -252	Industry Internship	Field Work	-	-	-	-	-	-	50	-	-	50	
TOTAL													700	

DEAN

M.Tech II Year/III Semester (CYBER SECURITY)
w.e.f academic Session 2025-26

SEMESTER III														
S. No	Course Code	Course Name	Course Type	Periods			CCA				ESE		Total	Credit
				L	T	P	CT	TA	Total	PS	TE	PE		
1	PCS -301	Cyber Incident Handling & Reporting	Core Subjects	3	1	0	20	10	30	-	70	-	100	4
2	PCS -351	Dissertation Phase -I	Project	0	0	12	-	-	-	100	-	200	300	12
TOTAL													400	16

M.Tech II Year/IV Semester (CYBER SECURITY)
w.e.f academic Session 2025-26

SEMESTER IV														
S. No	Course Code	Course Name	Course Type	Periods			CCA				ESE		Total	Credit
				L	T	P	CT	TA	Total	PS	TE	PE		
1	PCS-451	Dissertation Phase II	Project	0	0	20	-	-	-	200	-	300	500	20
TOTAL													500	20

M.TECH. (PE) TOTAL CREDITS - 84

DEAN

Electives [CYBER SECURITY]

	Course Code	Course Title
Elective-I	PCS -115	Public Key Infrastructure (PKI)
	PCS -116	Software Reliability and Fault Tolerant Systems
	PCS -117	Networking Protocols
	PCS -118	Information Security and Risk Management
Elective-II	PCS -119	Software Agents
	PCS -120	Biometric Security
	PCS -121	Text Mining
	PCS -122	Securing Windows & Linux
Elective-III	PCS -215	Intrusion Detection and Information Warfare
	PCS -216	Software Security
	PCS -217	Cryptography
	PCS -218	Database Security
Elective-IV	PCS -219	Data Base Management Systems
	PCS -220	Mobile & Wireless Network Security
	PCS -221	Object Oriented Programming Using C++
	PCS -222	Multimedia Presentation and Coding Techniques

Open Electives [CYBER SECURITY]

	Course Code	Course Title
Elective-I	PCSE -127	Business Analytics
	PCSE-128	Industrial Safety
	PCSE -129	Operations Research
Elective-II	PCSE -227	Cost Management of Engineering Projects
	PCSE -228	Composite Materials
	PCSE -229	Waste to Energy

DEAN

PCSE-101	Cyber Crime Investigations and Cyber Forensics	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand the fundamentals of cybercrime, its categories, motives, and legal perspectives.	K1, K2
CO2	Analyze various cybercrimes and identify the tools and techniques used by cybercriminals.	K2, K3
CO3	Demonstrate knowledge of digital forensics processes, tools, and investigative procedures.	K3, K5
CO4	Apply digital evidence collection, preservation, analysis, and reporting techniques in forensic investigations.	K3, K4
CO5	Evaluate the role of law enforcement agencies and legal frameworks in prosecuting cybercrimes.	K5, K6

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Introduction : Review of TCP/IP and TCP, IP Header analysis , Introduction to Cyber World, Cyber attacks and cyber security , Information warfare and cyber terrorism, Types of cyber attacks, Cyber Crime and Digital Fraud.	
Unit-2:	**8**
Overview of Types of computer forensics i.e. Media Forensics, Network forensics (internet forensics), Machine forensic, Email forensic (e-mail tracing and investigations).	
Unit-3:	**8**
Live Data collection and investigating windows environment : windows Registry analysis , Gathering Tools to create a response toolkit-Built in tools like netstat , cmd.exe , nbtstat , ARP , md5sum ,regdmp etc and tools available as freeware like Fport , Pslist , Obtaining volatile Data,Computer forensics in windows environment, Log analysis and event viewer, File auditing, identifying rogue machines, hidden files and unauthorized access points.	
Unit-4:	**8**
Live Data collection and investigating Unix/Linux environment : Proc file system overview , Gathering Tools to create a response toolkit (Built in tools like losetup , Vnode , netstat , df , md5sum , strace etc and tools available as freeware like Encase , Carbonite etc)Handling Investigations in Unix/Linux Environment: Log Analysis (Network, host, user logging details), Recording incident time/date stamps, Identifying rogue processes, unauthorized access points, unauthorized user/group accounts.	
Unit-5:	**8**

Forensic tools and report generation: Recovery of Deleted files in windows and Unix , Analyzing network traffic , sniffers , Ethical Hacking , Hardware forensic tools like Port scanning and vulnerability assessment tools like Nmap , Netscan etc . Password recovery (tools like John the ripper, L0phtcrack, and THC-Hydra), Mobile forensic tools and analysis of called data record Template for computer forensic reports.	

Reference Books:

1. Incident Response & Computer Forensics. Mandia, k., Prosise, c., Pepe, m. 2nd edition. Tata-McGraw Hill, 2003.
2. Guide to Computer Forensics and Investigations, 2nd edition, Bill Nelson, Amelia Phillips, Frank Enfinger, and Chris Steuart , Thomson Learning
3. Digital Evidence and Computer Crime, 2nd Edition , Eoghan Casey , academic Press File System Forensic Analysis by Brian Carrier , addition Wesley
4. Windows Forensic Analysis DVD Toolkit (Book with DVD-ROM), Harlan Carvey, syngress Publication
5. EnCE: The Official EnCase Certified Examiner Study Guide, 2nd Edition , Steve Bunting , sybex Publication

DEAN

PCS-102	Research Methodology and IPR	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Analyze research related information	$K1, K2$
CO2	Analyze research related information	$K3, K5$
CO3	Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.	$K3, K_4$
CO4	Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.	$K3, K_4$
CO5	Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.	$K3, K_4$

K1–Remember,K2–Understand,K3 –Apply,K4–Analyze,K5 –Evaluate,K6–Create

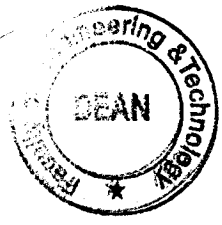
COURSE CONTENTS:

Content	Contact Hours
Unit 1	**8**
Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations	
Unit-2:	**8**
Research Design- Need, Features of good design, Induction and Deduction	
Unit-3:	**8**
Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee .	
Unit-4:	**8**
Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.	

Unit-5:	8
Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications.	

Reference Books:

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students'"
2. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction"
3. Ranjit Kumar, 2 ndEdition , "Research Methodology: A Step by Step Guide for beginnersHalbert, "Resisting Intellectual Property", Taylor & Francis Ltd ,2007.
4. Mayall , "Industrial Design", McGraw Hill, 1992.
5. Niebel , "Product Design", McGraw Hill, 1974.
6. Asimov , "Introduction to Design", Prentice Hall, 1962.
7. Robert P. Merges, Peter S. Menell, Mark A. Lemley, " Intellectual Property in New Technological Age", 2016.T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008



PCS-103	Virtualization and Cloud Security	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand the fundamentals of virtualization technologies and their role in cloud computing.	K1, K2
CO2	Compare various types of virtualization (server, storage, network, and desktop) and assess their use cases.	K2, K3
CO3	Identify and analyse security challenges and threats in virtualized and cloud environments.	K3, K5
CO4	Apply secure design principles and best practices for cloud infrastructure and service models (IaaS, PaaS, SaaS).	K3, K_4
CO5	Design a secure virtualization or cloud deployment plan that incorporates risk assessment and mitigation strategies.	K_5, K_6

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

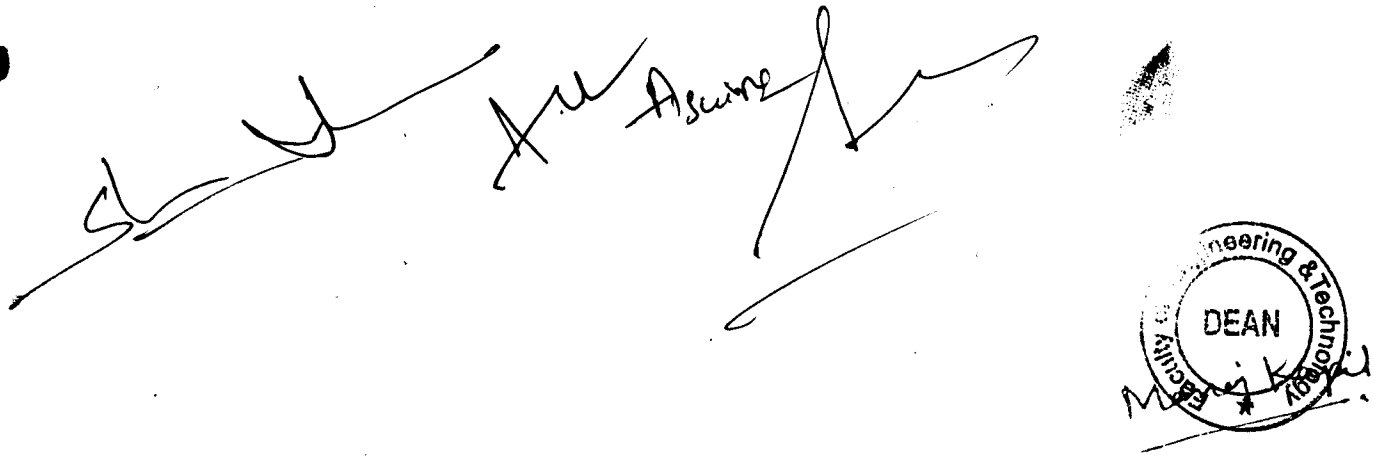
Content	Contact Hours
Unit-1:	**8**
Introduction: Basics of the emerging cloud computing paradigm, Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Virtualization Technology and Cloud Computing.	
Unit-2:	**8**
Cloud Computing: Cloud Service Models, cloud-computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing.	
Unit-3:	**8**
Virtualization: concept and properties of virtualization, CPU virtualization, memory virtualization, I/O virtualization, Forms of CPU virtualization. **Virtualization scenarios:** server consolidation, software development, debugging, fault tolerance, and security. Planning, Designing, Migrating and Deploying Virtual Infrastructure using Microsoft hyper-V, Citrix XenServer, QEMU and VMWare.	
Unit-4:	**8**
Cloud security: Cloud Security challenge, Principal Characteristics of Cloud Computing security, Data center security Recommendations, Encryption and key management in the cloud, identity and access management, trust models for cloud, Cloud forensics, traditional security, business continuity and disaster recovery.	
Unit-5:	

Faculty of Engineering & Technology DEAN

Data security tools and techniques for the cloud: Understanding the cloud architecture, Governance and enterprise risk management, design of customized cloud security measures, application security, targets of cyber crime. **Trustworthy cloud infrastructures**, Secure computations, Cloud related regulatory and compliance issues, Virtual Machines and Security Issues	

Reference Books:

1. Jim Smith, Ravi Nair, and Virtual Machines: Versatile Platforms for Systems and Processes, Morgan Kaufmann, 2005.
2. Cloud Computing: Implementation, Management, and Security, John Rittinghouse and James F.Ransome, CRC Press Taylor and Francis Grou



PCS-151	SECURITY LAB I	0L:0T:3P	1 Credit

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	To demonstrate basic cryptographic operations such as encryption, decryption, hashing, and digital signatures using programming tools.	K2, K3
CO2	To Implement classical and modern cryptographic algorithms (e.g., Caesar Cipher, RSA, AES, DES) in a secure manner.	K3
CO3	To analyze network traffic using tools like Wireshark to detect potential security threats and vulnerabilities.	K4, K5
CO4	To simulate and detect various attacks (e.g., brute-force, SQL injection, XSS) in a controlled environment using ethical hacking tools.	K6
CO5	To prepare technical reports documenting lab experiments, observations, and results with a focus on security best practices.	K3, K6

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

List of Experiments (Indicative & not limited to)

1. List and practice various "net" Commands on DOS & Linux.
2. Configure a system for various security experiments..
3. Configure Web browser security settings.
4. Draw Diagram of DoS, backdoors, trapdoors.
5. Draw diagrams of sniffing, spoofing, man in the middle & replay attacks
6. Draw diagram for Confidentiality, Integrity & Availability.
7. Write Ceaser's Cipher algorithm & Solve various examples based on Encryption & Decryption.

Reference Books:

1. William Stallings,"Cryptography and Network Security: Principles and Practice", Pearson Education.
2. Behrouz A. Forouzan, "Cryptography and Network Security", McGraw Hill Education.
3. Michael T. Goodrich, Roberto Tamassia, "Introduction to Computer Security", Pearson Education.
4. Nina Godbole and Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley India.

DEAN

PCS-201	Legal Dimension of IPR in Cyber World	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand the fundamentals and objectives of Intellectual Property Rights (IPR) in the context of cyberspace.	K1, K2
CO2	Examine various forms of IPR (copyright, patent, trademark, trade secrets) and their relevance in the digital environment.	K2, K3
CO3	Analyse the legal frameworks and cyber laws governing IPR at national and international levels.	K3, K5
CO4	Evaluate the challenges of enforcing IPR in cyberspace, including issues like piracy, plagiarism, and domain name disputes.	K3, K4
CO5	Apply legal principles to real-world cyber IPR infringement cases and propose appropriate legal remedies.	K5, K6

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Introduction to Intellectual Property Law – The Evolutionary Past - The IPR Tool Kit- Para -Legal Tasks in Intellectual Property Law – Ethical obligations in Para Legal Tasks in Intellectual Property Law - Introduction to Cyber Law – Innovations and Inventions Trade related Intellectual Property Right	
Unit-2:	**8**
IT Act; The rights the various parties have with respect to creating, modifying, using distribution. Computer Software and Intellectual Property-Objective, Copyright Protection, Reproducing, Defenses, Patent Protection. Database and Data Protection-Objective, Need for Protection, UK Data Protection Act, 1998, USSafe Harbor Principle.	
Unit-3:	**8**
Introduction to Trade mark – Trade mark Registration Process – Post registration Procedures – Trade mark maintenance - Transfer of Rights - Inter parties Proceeding – Infringement - Dilution Ownership of Trade mark – Likelihood of confusion - Trademarks claims – Trademarks Litigations – International Trade mark Law.	
Unit-4:	
Introduction to Copyrights – – Principles of Copyright Principles -The subjects Matter of Copy right – The Rights Afforded by Copyright Law – Copy right Ownership, Transfer and duration – Right to prepare Derivative works – Rights of Distribution – Rights of Perform the work Publicity Copyright Formalities and Registrations - Limitations - Copyright disputes and International Copyright Law – Semiconductor Chip Protection Act	
Unit-5:	**8**

Introduction to Trade Secret – Maintaining Trade Secret – Physical Security – Employee Limitation - Employee confidentiality agreement - Trade Secret Law - Unfair Competition – Trade Secret Litigation – Breach of Contract – Applying State Law.	

Reference Books:

1. Debirag E.Bouchoux: "Intellectual Property". Cengage learning , New Delhi
2. M.Ashok Kumar and Mohd.Iqbal Ali: "Intellectual Property Right" Serials Pub.
3. Cyber Law. Texts & Cases, South-Western"s Special Topics Collections
4. Prabhuddha Ganguli: „ Intellectual Property Rights" Tata Mc-Graw –Hill, New Delhi

DEAN

PCS 202	Web Services Security	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand the architecture, standards, and protocols associated with web services and service-oriented architecture (SOA).	K1, K2
CO2	Identify security vulnerabilities and threats in web services, including XML-based attacks and SOAP message tampering.	K2, K3
CO3	Apply authentication, authorization, and confidentiality techniques using security frameworks like WS-Security and SAML.	K3, K5
CO4	Evaluate the use of digital signatures, certificates, and key management in securing web services.	K3, K_4
CO5	Test and validate the security of web services using tools and security testing methodologies.	K_5, K_6

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

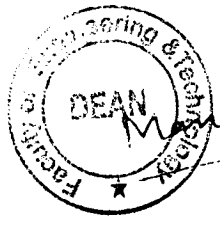
COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Introduction to Web Service Technologies Introduction to web services, Security for Web Services and Security Goals, Need of security and Privacy in web services, applications of web service security, SOA and Web Services Principles, Web Services Architecture, Web Services Technologies and Standards, SOAP, Web Services Description Language (WSDL), Service Discovery: Universal Description, Discovery, and Integration (UDDI) Considerations Web Services Infrastructure.	
Unit-2:	**8**
Web Services Threats, Vulnerabilities, and Countermeasures :Threats and Vulnerabilities, Threat Modeling, Vulnerability Categorizations and Catalogs, Threat and Vulnerabilities Metrics	
Unit-3:	**8**
Standards for Web Services Security: The Concept of Standard Web Services Security, Standards Framework, An Overview of Current Standards, XML Data Security ,Security Assertions Markup Language (SAML), SOAP Message Security, Key and Trust Management standards, Standards for Policy Specification, Access Control Policy Standards, Implementations of Web Services Security Standards.	
Unit-4:	**8**
Digital Identity Management and Trust Negotiation: Overview of Digital Identity Management, Overview of Existing Proposals Liberty Alliance, WS-Federation, Comparison of Liberty Alliance and WS-Framework, Other Digital Identity Management Initiatives, Discussion on Security of Identity Management Systems, Business Processes.	
Unit-5:	**8**

Access Control for Web Services :Approaches to Enforce Access Control for Web Services, WS-AC: An Adaptive Access Control Model for Stateless, Web Services, The WS-AC Model, WS-AC Identity Attribute Negotiation, WS-AC Parameter Negotiation	

Reference Books:

1. Elisa Bertino, Lorenzo D. Martino, Federica Paci, Anna C. Squicciarini, Security for Web Services and Service Oriented Architectures, Springer Science (2009).
2. Ramesh Nagappan, Christopher Steel, and Ray Lai,"Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management", Pearson Education, 2005.
3. Mark O'Neill, "Web Services Security", McGraw Hill/Osborne, 2003.
4. Jothy Rosenberg and David Remy, "Securing Web Services with WS-Security: Demystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption",
   Pearson Education, 2004.



PCS-203	ENGLISH FOR RESEARCH PAPER WRITING	3L:0T:0P	4 Credit

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand that how to improve your writing skills and level of readability	K1,K2
CO2	Learn about what to write in each section	K3, K5
CO3	Understand the skills needed when writing a Title	K3, K_4
CO4	Ensure the good quality of paper at very first-time submission	K3, K_4

K1–Remember,K2–Understand,K3 –Apply,K4–Analyze,K5 –Evaluate,K6–Create

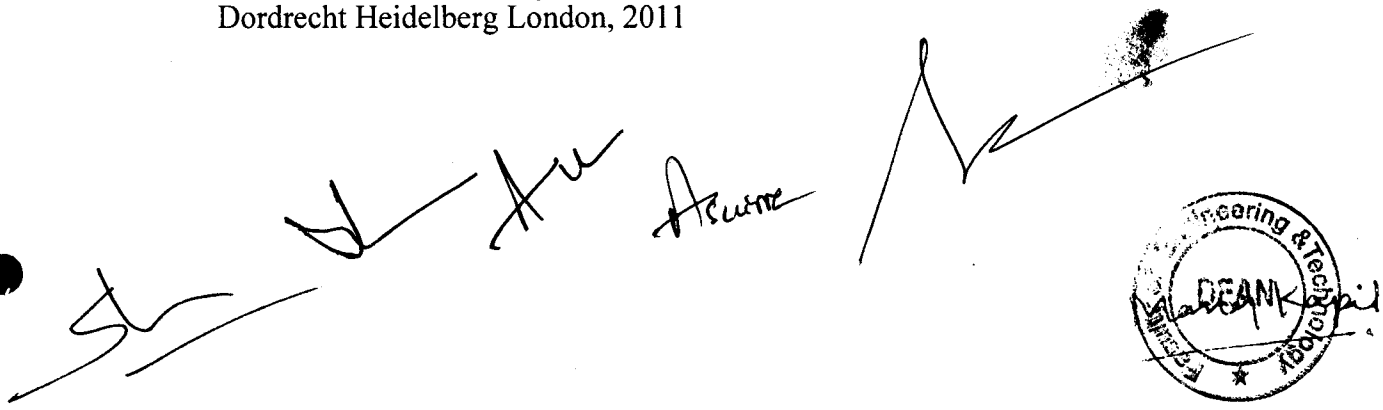
COURSE CONTENTS:

Content	Contact Hours
Unit 1	**8**
Planning and Preparation, Word Order, Breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness. General Structure of Research Paper.	
Unit-2:	**8**
Clarifying Who Did What, Highlighting Your Findings, Hedging and 4 Criticizing, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts. Introduction. Appropriate keywords for indexing and research	
Unit-3:	**8**
Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check	
Unit-4:	**8**
Key skills are needed when writing a Title, key skills are needed when writing an Abstract, key skills are needed when writing an Introduction, skills needed when writing a Review of the Literature, Ethical considerations in method reporting.	
Unit-5:	**8**
Skills are needed when writing the Methods, skills needed when writing the Results, skills are needed when writing the Discussion, skills are needed when writing the Conclusions useful phrases, how to ensure paper is as good as it could possibly be the 4 first- time submission. Limitation and Future work	

DEAN

Reference Books:

1. Goldbort R (2006) Writing for Science, Yale University Press (available on Google Books)
2. Day R (2006) How to Write and Publish a Scientific Paper, Cambridge University Press
3. Highman N (1998), Handbook of Writing for the Mathematical Sciences, SIAM. Highman'sbook .
4. Adrian Wallwork , English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011



PCS 251	SECURITY LAB–II	0L:0T:3P	1 Credit

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	To analyze advanced security threats and simulate real-world cyber-attacks using penetration testing tools.	K2, K3
CO2	To Perform vulnerability assessments and risk analysis using automated security scanners and frameworks (e.g., Nessus, OpenVAS).	K3
CO3	To demonstrate secure coding practices to prevent common software vulnerabilities such as buffer overflows, injection flaws, and insecure deserialization.	K4, K5
CO4	To conduct malware analysis using static and dynamic analysis techniques in sandbox environments.	K6
CO5	To develop and document secure system configurations for servers, web applications, and cloud services.	K3, K6

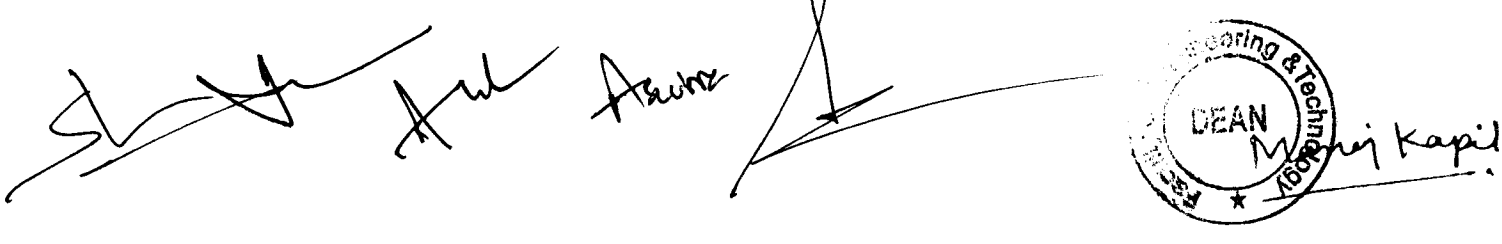
K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

List of Experiments (Indicative & not limited to)

1. Implementation of Caesar Cipher technique
2. Implement the Playfair Cipher
3. Implement the Pure Transposition Cipher
4. Implement DES Encryption and Decryption.
5. Implement the AES Encryption and decryption
6. Implement RSA Encryption Algorithm.
7. Write Ceaser's Cipher algorithm & Solve various examples based on Encryption & Decryption.

Reference Books:

1. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy",
2. Michael Sikorski and Andrew Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software".
3. Bryan Sullivan and Vincent Liu, "Web Application Security: A Beginner's Guide".
4. Jason Andress and Steve Winterfeld, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners", Syngress.



PCS 301	Cyber Incident Handling & Reporting	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Recall fundamental database concepts, types of users, data models, schemas, and architectures	K1
CO2	Explain relational models, relational algebra, SQL queries, constraints, and relational DBMS characteristics	K2
CO3	Apply Oracle architecture concepts and implement database operations using PL/SQL elements like triggers, UDFs	K3
CO4	Analyze relational schema using functional dependencies and normalization techniques (1NF–BCNF)	K4
CO5	Evaluate concurrency control, recovery mechanisms, and advanced concepts like object-oriented and distributed DBMS	K5

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Introduction: Concept of Computer security Incident, Types of Incident-denial of service-malicious code, unauthorized access, Inappropriate Usage. Need for incident Response, Policies, Plans and Procedure related to incident Response, Incident reporting organization.	
Unit-2:	**8**
Incident Response Team structure: Introduction to Response Team, Team Models, Staffing Models, Incident Response Personnel, Incident Response Team Services, Incident Response Life cycle- Preparation, Detection and Analysis, Containment Eradication and Recovery, Post - Incident Activity.	
Unit-3:	**8**
Incident Detection and Analysis: Profiling, Behaviors, Centralized logging , Event Correlation, Diagnosis matrix , Incident Analysis – Incident Documentation ,incident Prioritization, Incident Response SLA Matrix , Incident Notification.	
Unit-4:	
Incident Detection and Analysis: Profiling, Behaviors, Centralized logging , Event Correlation, Diagnosis matrix , Incident Analysis – Incident Documentation ,incident Prioritization, Incident Response SLA Matrix , Incident Notification.	

DEAN

Unit-5:	8
Handling Multiple Components Incidents: Preparation, Detection and Analysis, Containment Eradication and	

Reference Books :

1. *An introduction to computer security: the NIST handbook, Barbara Guttman, Edward Roback, NIST Special Publication 800-12*
2. *The effective incident response team, Julie Lucas, Brian Moeller, Addison-Wesley Professional*
3. *Principles of incident response and disaster recovery, Michael E. Whitman, Herbert J. Mattord, Thomson Course Technology, 2007*
4. *Incident response: a strategic guide to handling system and network security Breaches, E. Eugene Schultz, Russell Shumway, New Rider Publishing-2002*
5. *Incident Response & Computer Forensics, Mandia, Tata McGraw-Hill Education-2006*

DEPARTMENT ELECTIVES:

PCS-115	Public Key Infrastructure	3L:1T:0P	4 Credits

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Distinguish between public key technology and a public key infrastructure.	K1, K2
CO2	Understand the relationship of identity management to PKI.	K2, K3
CO3	Understand the issues related to Trust management mechanisms.	K3, K5
CO4	Understand Secure Crypto protocols like SSL and so on.	K3, K4

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

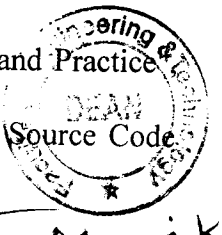
COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Public Key InfrastructurePKI Components: Certification Authority, Registration authority, PKI Repositories, Archives, PKI users.PKI Architecture: Hierarchical PKI Architecture, Mesh PKI Architecture, Bridge PKI Architecture, How the BCA enables B@B E-commerce based PKI Architecture. Physical Architecture.PKI Data Structures: X.509 Public Key Certificates, Certificate Revocation Lists (CRLs), Attribute Certificates.	
Unit-2:	**8**
PKI Interoperability:Interoperability Framework: Component-Level Interoperability, Application-Level Interoperability, Inter-Domain Interoperability. Interoperability Specification for PKI Components: Interoperability-Relevant CA Functional Specifications, Interoperability-Relevant RA Functional Specifications, Interoperability-Relevant PKI Certificate Holders Functional Specifications, Interoperability-Relevant PKI Client Functional Specifications.Data Formats: Certificate Format, Certificate Revocation List (CRL) PKI Transaction Message Formats: Overall PKI message components, PKI message header, PKI message body, PKI Message Protection.CA-CA Interoperability: Cross-Certification, Bridge CA	
Unit-3:	**8**

PKI Deployment and Assessment PKI Deployment: Draft a Certificate Policy, Establishing Policy mapping and Constraints, Local Certificate and CRL Profile(s) Select PKI Product or Service Provider, Develop Certification Practice Statement, Critical Deployment Issues, Apply for Licenses Certification Authority. PKI Assessment:Personnel Security Controls: Trusted roles, number of person required per task, Identification and Authentication for each role, Personnel controls.Backup Policy, Audit Logging Procedures.	
Unit-4:	**8**
CA Key Management:Key Pair Generation and Installation, Private Key Protection, Other Aspects of Key Pair management, Activation Data, Computer Security Controls, Life Cycle Technical Controls, Network Security Controls, Cryptographic Module Controls.	
Unit-5:	**8**
PKI Services and Operation Risks,Secure Business Services: Entity Authentication, Data Confidentiality, Data Integrity, and Non-Repudiation. PKI Ancillary Services: Key Recovery and Escrow, Privilege Management, Time Stamping. Risks of PKI Systems, Managing Digital Certificates.	

Reference Books:

1. Carlisle Adams and Steve Lloyd, "Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations", Sams Publishing
2. J. Michael Stewart, "Network Security, Firewalls, and VPNs", Jones & Bartlett Learning
3. William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education
4. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Wiley India



Manoj Kapil

PCS-116	Software Reliability and Fault Tolerant Systems	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Enumerate the need and necessity to consider fault-tolerant design in digital systems.	K1, K2
CO2	Explain vividly, the various techniques for fault modelling and tests generation.	K2, K3
CO3	Determine the various forms of redundancy for enhancing reliability of digital systems	K3, K5
CO4	Evaluate reliability of systems with permanent and temporary faults.	K3, K_4

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
SOFTWARE RELIABILITY:Measures of software reliability, Mean Time To Failure (MTTF), Mean Time Between Failure (MTBF), Mean Time To Recovery (MTTR), availability, maintainability, Musa's operational profiles and type-uncertainty, defect removal and type-2 uncertainty, reliability stability and reliability growth, hardware reliability vs. software reliability, failure probability density function and reliability function, Reliability prediction , reliability metrics.	
Unit-2:	**8**
DEVELOPMENT OF RELIABLE SOFTWARE:Reliable software, defect prevention, detection and removal, design for robustness, verification & validation, stabilization of requirements, design, code and test artifacts, active and passive fault detection, fault handling and correction, exceptions, survivability, reliability models, software availability model.	
Unit-3:	**8**
FAULT TOLERANCE IN HARDWARE SYSTEMS:Fault classification, fault tolerance attributes and system structure, fault prevention, anticipated and unanticipated fault, test generation for digital systems, combinational logic network,	

DEAN

Boolean difference method, test generation for sequential circuits, fault simulation, application of hardware fault tolerance in developing fault tolerant software systems.	
Unit-4:	**8**
SOFTWARE AND HARDWARE FAULT TOLERANCE:Software and hardware faults, failure intensity function, characterization of fault injection, detection and correction, techniques for prediction of remaining faults and fault injection, classification tree analysis, code coverage, coding technique, fault tolerant & self checking, fail safe circuits, synchronous and asynchronous fail safe circuits.	
Unit-5:	**8**
FAULT TOLERANT SOFTWARE:Concept of N-version programming (NVP) and methods, recovery block, acceptance tests, fault trees, validation of fault tolerant systems, security, fault tolerance in wireless/mobile networks and Internet.	

Reference Books:

1. Software Reliability Engineering, John D. Musa, Tata McGRAW Hill, 2005.
2. Fault-Tolerant Computer System Design, D.K. Pradhan, 2003.
3. Design and Analysis of Fault -Tolerant Digital Systems, B. W. Johnson, Addison-Wesley, 1989.
4. Fault-Tolerant Computing, Theory & Techniques, D.K. Pradhan, Prentice Hall, 1986.

DEAN

PCS-117	Networking Protocols	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Have a good understanding of the OSI Reference Model and in particular have a good knowledge of Layers 1-3.	K1, K2
CO2	Analyze the requirements for a given organizational structure and select the most appropriate networking architecture and technologies.	K2, K3
CO3	Have a basic knowledge of the use of cryptography and network security.	K3, K5
CO4	Specify and identify deficiencies in existing protocols, and then go onto formulate new and better protocols	K3, K4
CO5	Have an understanding of the issues surrounding Mobile and Wireless Networks	K3, K4

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

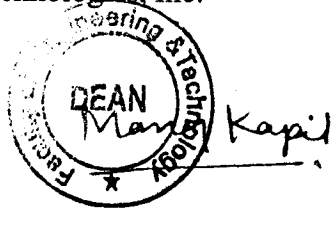
COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Protocols of Physical Layer: Overview of physical layer operations of wired and wireless networks, Protocol Architecture: IEEE 802.3Local Area Network Protocols, VLAN- Virtual Local Area Network, WLAN-Wireless LAN by IEEE 802.11 Protocols, FDDI-Fiber Distributed Data Interface, Token Ring- IEEE 802.5 LAN Protocol, DQDB-Distributed Queue Dual Bus(IEEE 802.6), SMDS- Switched Multimegabit Data Service, WiMAX- Broadband Wireless MAN (IEEE802.16).	
Unit-2:	**8**
Protocols of Data Link Layer:Overview of data link layer operations of wired and wireless networks, medium access control protocols including CSMA, collision free protocols, WDMA protocols, wireless LAN protocols, ARP, RARP, X.25.	
Unit-3:	**8**
Protocols of Network Layer:Overview of network layer operations of wired and wireless networks, IP-Internet Protocol (IPv4), IPv6-Internet Protocol version 6, ICMP & ICMPv6-Internet Message Control Protocol and ICMP version 6,BGP (BGP-4)-Border Gateway Protocol, EGP- Exterior Gateway Protocol, IRDP- ICMP Router Discovery Protocol, Mobile IP-IP Mobility Support Protocol for IPv4 & IPv6,	

NHRP- Next Hop Resolution Protocol, OSPF- Open Shortest Path First Protocol, RIP- Routing Information Protocol (RIP2), RIPng- Routing Information Protocol next generation for IPv6, RSVP- Resource ReSerVation Protocol, VRRP- Virtual Router Redundancy Protocol.	
Unit-4:	**8**
Protocols of Transport Layer:Overview of transport layer operations, Protocols: TCP-Transmission Control Protocol, UDP –User Datagram Protocol, RUDP-Reliable User Datagram Protocol, SCTP- Stream Control Transmission Protocol, CUDP-Cyclic UDP, DCCP-Datagram Congestion Control Protocol, FCP-Fiber Channel Protocol, IL-IL Protocol, NBF-NetBIOS Frames protocol, µTP-Micro Transport Protocol, RSVP , ECN, H.323, H.261- Video CODEC for Low Quality Videoconferencing,H.263: Video CODEC for Medium Quality Videoconferencing, H.264 / MPEG-4: Video CODEC For High Quality Video Streaming wireless TCP and UDP.	
Unit-5:	**8**
Protocols of Application Layer:Overview of application layer operations, Protocols: DNS, SMTP, HTTP, BGP, DHCP , FTP , LDAP, MGCP, NNTP , NTP, POP, RIP, RPC, RTP , SIP ,SNMP, SSH, Telnet , XMPP, security protocols.	

Reference Books:

1. Internetworking with TCP/IP Volume 1: Principles Protocols, and Architecture, Douglas Comer and Prentice Hall, fifth edition, 2006.
2. TCP/IP Protocol Suite, B.A. Forouzan, TMH, 3rd edition, 2006.
3. Computer Networks, S. Tanenbaum, 4th edition, Prentice Hall, 2003.
4. Network Protocols: Signature Edition, Matthew G. Naugle. Mcgraw-Hill Signature Series.
5. Network Protocols Handbook, Javlin, 4th edition, Javvin Technologies, Inc.



PCS-118	Information Security and Risk Management	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Students are able to define the concepts of confidentiality, availability and integrity as they relate to information security.	K1, K2
CO2	Students are aware of the relationships and tradeoffs among confidentiality, availability and integrity.	K2, K3
CO3	Students are aware that security applies to hardware, software and data	K3, K5
CO4	Students can define the following basic information security terms: threats and vulnerabilities, risk analysis, cost benefit analysis, attacks, exploits, controls	K3, K4

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

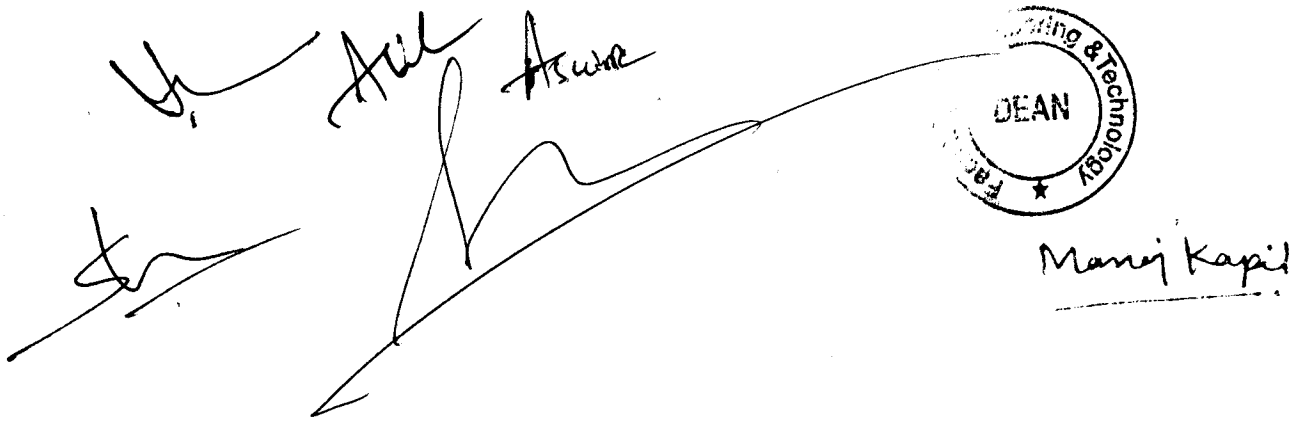
COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Risk Management : Definition, Overview of Risk management, Risk identification, Threat identification, Risk assessment, Risk determination, Risk control strategies, Selecting a risk control strategy, cost benefit analysis.	
Unit-2:	**8**
Development of concepts required for risk-based planning and risk management of computer and system, Incident response planning, Disaster recovery planning, Crisis management, Business continuity planning, model for a consolidated contingency plan.	
Unit-3:	**8**
Planning for security: Information security policy, Standards and practices, Enterprise information security policy(EISP), Issue- specific security policy(ISSP), System-specific policy(SSP), ACL policies, Rule policies, Policy management Visa international security model, Hybrid framework for a blueprint of an Information security system, Design of security architecture.	
Unit-4:	**8**
Technological hazards, and terrorist; implications for emergency response, vulnerability of critical infrastructures.	

Unit-5:	8
Management in Practice and Emerging Trends: Security audits and assessments, Vulnerability assessment and penetration testing (VAPT), Third-party/vendor risk management, Security metrics and reporting, Emerging trends: Cloud Security, Zero Trust, AI in Security, IoT Risk Management, Case studies and mini project on risk management plan or incident analysis.	

Reference Books:

1. Thomas , R Peltier, "Information risk analysis" , CRC Press-2005
2. Principles of information Security by Michael E. Whitman
3. Information Security and ethics by Nemati.h, IGI Global.
4. Handbook of information Security by bidgoli, hossein john willy & sons.



PCS-119	Software Agents	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Ability to understand various reference systems.	K1, K2
CO2	Ability to understand the physical meaning of double and triple integrals.	K2, K3
CO3	Ability understands the parameterized curves and vector operators.	K3, K5
CO4	Ability to solve the second & higher order linear differential equations.	K3, K4

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

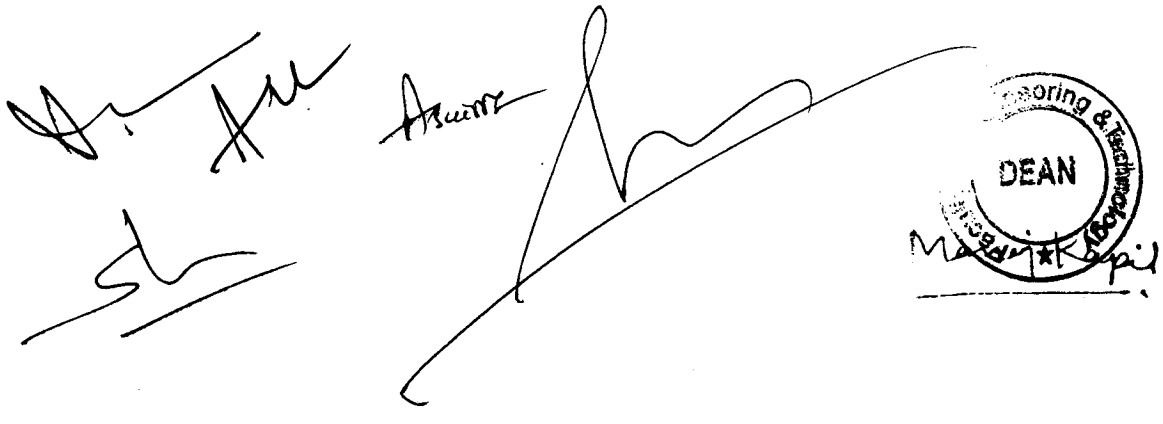
Content	Contact Hours
Unit-1:	**8**
SOFTWARE AGENTS PARADIAGM: Software agent, history, theoretical foundations for software agents, agent programming,agent programming paradigms, agent vs. object, aglet, mobile agents, agent frameworks, agent reasoning, agent applications.	
Unit-2:	**8**
AGENT TYPOLOGY:Software agents: collaborative agents, interface agents, mobile agents, information agents, reactive agent s, hybrid agents, heterogeneous agent system, smart agents.	
Unit-3:	**8**
MULTIAGENT SYSTEMS:Multi-agent system, interaction between agents, reactive agents, cognitive agents, interaction protocols, agent coordination, agent negotiation, agent cooperation, agent organization, self interested agents in e-commerce applications.	
Unit-4:	**8**
INTELLIGENT SOFTWARE AGENTS:Design and implementation of intelligent agents: reactive, deliberative, planning, interface agents, agent communication languages, agent knowledge representation, agent adaptability, mobile agent applications, languages & tools for design, implementation of intelligent agents.	
Unit-5:	**8**

Engineering & Technology DEAN Kapil

AGENTS AND SECURITY:Agent security issues, mobile agents security, protecting agents against malicious hosts, untrusted agent, black box security, authentication for agents, security issues for aglets.	

Reference Books:

1. Constructing Intelligent Agents with JAVA, Bigus & Bigus, Wiley, 1997.
2. Software Agents, Bradshaw, MIT Press, 2000.
3. Artificial Intelligence: A Modern Approach, von Stuart J. Russell, Peter Norvig, Prentice Hall, 1994.
4. Intelligent Software Agents, Richard Murch, Tony Johnson, Prentice Hall, 2000.
5. Hall, 1994.
6. Intelligent Software Agents, Richard Murch, Tony Johnson, Prentice Hall, 2000.



PCS-120	Biometric Security	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems.	K1, K2
CO2	Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications.	K2, K3
CO3	Be able to work effectively in teams and express their work and ideas orally and in writing.	K3, K5
CO4	Identify the sociological and acceptance issues associated with the design and implementation of biometric systems.	K3, K4

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

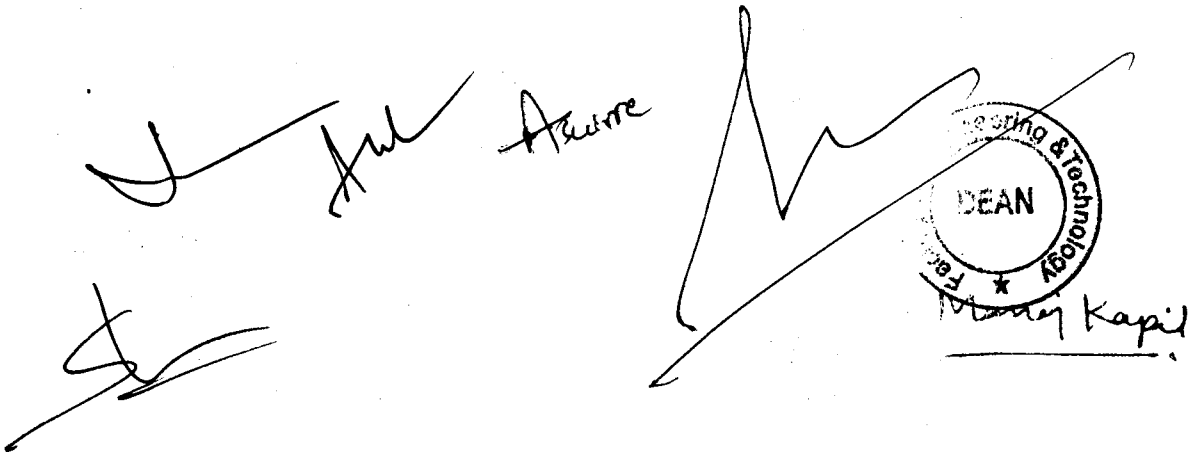
Content	Contact Hours
Unit-1:	**8**
Over view of bio metrics - Benefits of biometric security – Verification and identification and enrollment – Basic working of biometric matching – Accuracy – False match rate – False non-match rate – Failure to enroll rate – Derived metrics – Layered biometric solutions. Biometric system security	
Unit-2:	**8**
Finger scan – Features – Components – Operation (Steps) – Competing finger Scan technologies – Strength and weakness. Types of algorithms used for interpretation. Facial Scan - Features – Components – Operation (Steps)– Competing facial Scan technologies – Strength and weakness. Iris Scan - Features – Components – Operation (Steps) – Competing iris Scan technologies – Strength and weakness. Voice Scan - Features – Components – Operation (Steps) – Competing voice Scan (facial) technologies – Strength and weakness.	
Unit-3:	**8**
Authentication and Biometrics: Secure Authentication Protocols, Access Control Security Services, Authentication Methods, Authentication Protocols, Matching Biometric Samples, Verification by humans. . Matching: Two kinds of errors, Score distribution, Estimating Errors from Data, Error Rate of Match Engines, Definition of FAR and FRR. Correlation based biometric filters, Basic theory of Correlation filters	
Unit-4:	**8**
Other physiological biometrics – Hand scan – Retina scan – AFIS (Automatic Finger Print Identification Systems) – Behavioral Biometrics – Signature scan- keystroke scan. Hand Geometry, Signature Verification, Positive and Negative of Biometrics	
Unit-5:	**8**

Manoj Kapil

Biometrics Application – Biometric Solution Matrix – Bio privacy – Comparison of privacy factor in different biometrics technologies – Designing privacy sympathetic biometric systems. Biometric standards – (BioAPI , BAPI) – Biometric middleware Biometrics for Network Security. Statistical measures of Biometrics. Biometric Transactions.	

Reference Books:

1. Biometrics – Identity Verification in a Networked World – Samir Nanavati.
2. Biometrics for Network Security- Paul Reid, Pearson Education.
3. Biometrics- The Ultimate Reference- John D. Woodward, Jr. Wiley Dreamtech.



PCS-121	Text Mining	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand the concepts and algorithms of data mining.	K1, K2
CO2	Apply data mining techniques for business intelligence.	K2, K3
CO3	Be aware of the privacy and security issues in data mining	K3, K5

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

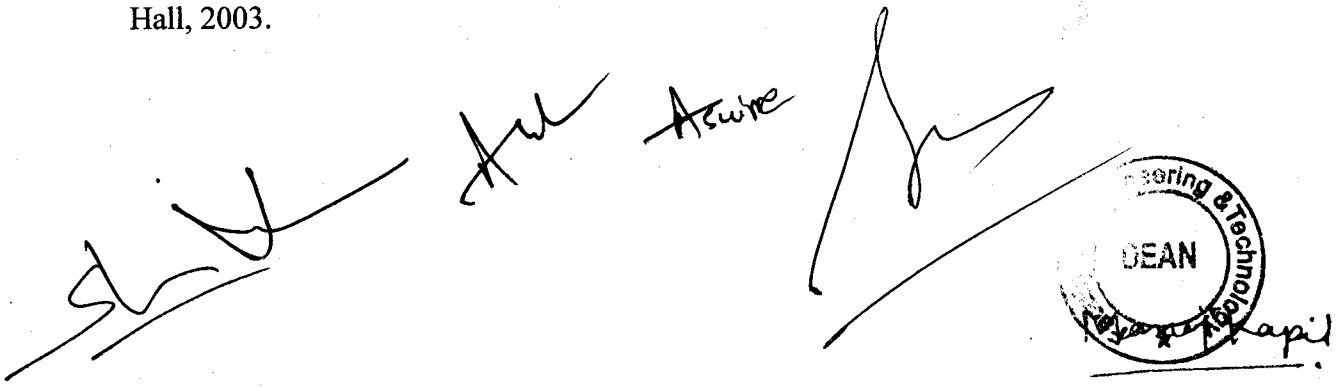
COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Data Mining Techniques-Data Mining Process-Process with a typical set of data-Big Data-Visualization of data through data mining software.	
Unit-2:	**8**
Data Mining Methods as Tools - Memory-Based reasoning methods of Data Mining - Algorithms with prototypical data based on real applications.	
Unit-3:	**8**
Data Stream Mining, Mining Time Series, Text Mining, Data Stream Clustering, mining Big Data.	
Unit-4:	**8**
Market Basket Analysis - Fuzzy Data Mining approaches - Fuzzy Decision Tree approaches Fuzzy Association Rule applications. Rough Sets - Support Vector Machines - Genetic algorithms.	
Unit-5:	**8**
Social Computing - Analysis -Graph Mining – Social Network Mining-Web Mining – Web Usage Mining-Privacy Preserving Data Mining-Recommender Systems.	

DEAN

Reference Books:

1. David L. Olson and Dursun Delen, "Advanced Data Mining Techniques", Springer, 2008.
2. Charu C. Aggarwal and Haixun Wang, "Managing and Mining Graph Data", Springer, 2010.
3. Ian H. Witten, Eibe Frank and Mark A. Hall, "Data Mining: Practical Machine Learning Tools and Techniques", Morgan Kaufmann Publishers, 2011.
4. Jiawei Han and Micheline Kamber, "Data Mining: Concepts and Techniques", Morgan Kaufmann Publishers, 2006.
5. Margaret H. Dunham, "Data Mining Introductory and Advanced Topics", Prentice Hall, 2003.



PCSE-122	Securing Windows & Linux	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Recall foundational security principles, standards, AAA mechanisms, and basic cryptographic concepts including PKI	K1
CO2	Explain network vulnerabilities, Internet security threats, and protective tools for networks and applications	K2
CO3	Apply system-level security techniques including Linux security, OS hardening, and virtualization security measures	K3
CO4	Analyze organizational security frameworks including physical security, firewall types, policies, and disaster recovery planning	K4
CO5	Evaluate security assessment techniques, audit tools, VPNs, and strong authentication systems used in secure environments	K5

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

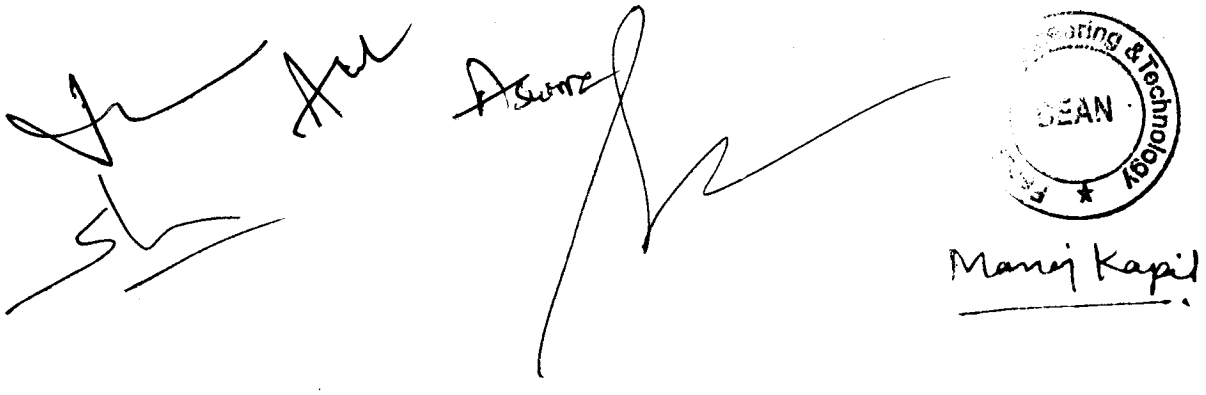
Content	Contact Hours
Unit-1:	**8**
Introduction to General Security Concepts: Principles of Information Security, Information Security Standards, Regulations, and Compliance, Authentication, Authorization, and Accounting (AAA). **Cryptography:** Basic Cryptography Concepts, PKI Concepts, Implementing PKI and Certificate Management,	
Unit-2:	**8**
Network Security: General Network Concepts and Vulnerabilities, Network Services and Network Devices, Internet Security and Vulnerabilities, Network Security Tools and Devices. **Application Security:** HTTP Security, Electronic Mail, Samba Security.	
Unit-3:	**8**
System Security: General System Security Threats, Hardware and Peripheral Devices, OS and Application Security, Virtualization, System-Based Security Applications, Understanding Linux Security, System Monitoring and Auditing.	
Unit-4:	**8**
Organizational and Operational Security: Physical Security Concepts and Vulnerabilities, Policies and Procedures, Risk Analysis, Business Continuity and Disaster Recovery, Network layer firewalls, transport layer firewalls, application layer firewalls.	
Unit-5:	

Engineering & Technology DEAN

Security Assessments and Audits: Vulnerability Assessments and Testing, Monitoring, Logging and Auditing **Remote Access and Authentication:** Virtual Private Networking, Strong User authentication. Study of various Network security tools and devices.	

Reference Books:

1. Security for Microsoft Windows System Administrators, Introduction to key Information Security concepts, Derrick Rountree, Elsevier
2. Linux Security, Ramón J. Hontañón, 2001 ,Sybex, ISBN: 0-7821-2741-X
3. Linux Security Cookbook, Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes, O'Reilly, June 2003 ISBN: 0-596-00391-9
4. Ross J. Anderson ,"Security engineering"
5. Debra S. Herrmann ,"A practical guide to security engineering and information assurance"
6. Ross Anderson ,"Security Engineering"
7. Network security private communication in public world, Kaufman Charlie ,Peman, radia , PHI
8. Security, Client/Server computer network by Davis, Peter T. McGraw hill.



OPEN ELECTIVES

PCSE-127	Business Analytics	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand the role of business analytics within an organization.	K1,K2
CO2	Analyze data using statistical and data mining techniques and understand relationships between the underlying business processes of an organization	K3, K5
CO3	To gain an understanding of how managers use business analytics to formulate and solve business problems and to support managerial decision making.	K3, K_4
CO4	To become familiar with processes needed to develop, report, and analyze business data.	K3, K_4
CO5	Use decision-making tools/Operations research techniques.	K3, K_4
CO6	Mange business process using analytical and management tools.	K3, K_4
CO7	Analyze and solve problems from different industries such as manufacturing, service, retail, software, banking and finance, sports, pharmaceutical, aerospace etc	K3, K_4

K1–Remember,K2–Understand,K3 –Apply,K4–Analyze,K5 –Evaluate,K6–Create

COURSE CONTENTS:

Content	Contact Hours
Unit 1	**8**
Business analytics: Overview of Business analytics, Scope of Businessanalytics,BusinessAnalytics Process, Relationship of Business Analytics Process and organisation,competitive advantages of Business Analytics. Statistical Tools: Statistical Notation, Descriptive Statistical methods,Review of probability distribution and data modelling, sampling andestimation methods overview.	
Unit-2:	**8**
Trendiness and Regression Analysis: Modelling Relationships and Trends inData, simple Linear Regression. Important Resources, Business Analytics Personnel, Data and models forBusiness analytics, problem solving, Visualizing and Exploring Data,Business. Analytics Technology.	
Unit-3:	**8**
Organization Structures of Business analytics, Team management, Management Issues, Designing Information Policy, Outsourcing, Ensuring Data Quality, Measuring contribution of Business analytics, Managing Changes.Descriptive	

Analytics, predictive analytics, predicative Modelling, Predictive analytics analysis, Data Mining, Data Mining Methodologies, Prescriptive analytics and its step inthe business analytics Process, Prescriptive Modelling, nonlinear Optimization.	
Unit-4:	**8**
Forecasting Techniques: Qualitative and Judgmental Forecasting, Statistical Forecasting Models, Forecasting Models for Stationary Time Series, Forecasting Models for Time Series with a Linear Trend, Forecasting Time. Series with Seasonality, Regression Forecasting with Casual Variables, Selecting Appropriate Forecasting Models. Monte Carlo Simulation and Risk Analysis: Monte Carle Simulation UsingAnalytic Solver Platform, New-Product Development Model, Newsvendor Model, Overbooking Model, Cash Budget Model.	
Unit-5:	**8**
Decision Analysis: Formulating Decision Problems, Decision Strategies withthe without Outcome Probabilities, Decision Trees, The Value ofInformation, Utility and Decision Making.	

Reference Books:

1. Business analytics Principles, Concepts, and Applications by Marc J. Schniederjans, Dara G. Schniederjans, Christopher M. Starkey, Pearson FT Press.
2. Business Analytics by James Evans, persons Education.

Manoj Kapil

PCSE-128	Industrial Safety	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Explain the principles and importance of industrial safety and its role in protecting human resources, assets, and the environment.	K1,K2
CO2	Identify potential hazards and risks in various industrial environments, including mechanical, electrical, chemical, and construction sites.	K3, K5
CO3	**Apply safety management systems, policies, and procedures** to prevent accidents and ensure workplace safety.	K3, K_4
CO4	Select and recommend appropriate personal protective equipment (PPE) and safety devices for different industrial situations.	K3, K_4

COURSE CONTENTS:

Content	Contact Hours
Unit 1	**8**
Industrial safety: Accident, causes, types, results and control, mechanical and electrical hazards,types, causes and preventive steps/procedure, describe salient points factories act 1948 for health and safety, wash rooms, drinking water layouts, light, cleanliness, fire, guarding, pressure vessels, etc, Safety color codes. Fire prevention and firefighting, equipment and methods.	
Unit-2:	**8**
Fundamentals of maintenance engineering: Definition and aim of maintenance engineering, Primary and secondary functions and responsibility of maintenance department, Types of maintenance, Types and applications of tools used for maintenance, Maintenance cost & its relation with replacement economy, Service life of equipment.	
Unit-3:	**8**
Wear and Corrosion and their prevention: Wear- types, causes, effects, wear reduction methods, lubricants-types and applications, Lubrication methods, general sketch, working and applications, i. Screw down grease cup, ii. Pressure grease gun, iii. Splash lubrication, iv. Gravity lubrication, v. Wick feed lubrication vi. Side feed lubrication, vii. Ring lubrication, Definition, principle and factors affecting the corrosion. Types of corrosion, corrosion prevention methods.	
Unit-4:	**8**

Fault tracing: Fault tracing-concept and importance, decision tree concept, need and applications, sequence of fault finding activities, show as decision tree, draw decision tree for problems in machine tools, hydraulic, pneumatic, automotive, thermal and electrical equipment's like, I. Any one machine tool, ii. Pump iii. Air compressor, iv. Internal combustion engine, v. Boiler, vi. Electrical motors, Types of faults in machine tools and their general causes.	
Unit-5:	**8**
Periodic and preventive maintenance: Periodic inspection-concept and need, degreasing, cleaning and repairing schemes, overhauling of mechanical components, overhauling of electrical motor, common troubles and remedies of electric motor, repair complexities and its use, definition, need, steps and advantages of preventive maintenance. Steps/procedure for periodic and preventive maintenance of: I. Machine tools, ii. Pumps, iii. Air compressors, iv. Diesel generating (DG) sets, Program and schedule of preventive maintenance of mechanical and electrical equipment, advantages of preventive maintenance. Repair cycle concept and importance	

Reference Books:

1. Maintenance Engineering Handbook, Higgins & Morrow, Da Information Services.
2. Maintenance Engineering, H. P. Garg, S. Chand and Company.
3. Pump-hydraulic Compressors, Audels, Mcgrew Hill Publication.
4. Foundation Engineering Handbook, Winterkorn, Hans, Chapman & Hall London.

DEAN
Faculty of Engineering & Technology

Manoj Kapil

PCSE-129	Operations Research	3L:1T:0P	3 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Students should able to apply the dynamic programming to solve problems of discreet and continuous variables.	K1,K2
CO2	Students should able to apply the concept of non-linear programming	K3, K5
CO3	Students should able to carry out sensitivity analysis	K3, K_4
CO4	Student should able to model the real world problem and simulate it	K3, K_4

K1–Remember,K2–Understand,K3 –Apply,K4–Analyze,K5 –Evaluate,K6–Create

COURSE CONTENTS:

Content	Contact Hours
Unit 1	**8**
Optimization Techniques, Model Formulation, models, General L.R , Formulation, Simplex Techniques, Sensitivity Analysis, Inventory Control Models	
Unit-2:	**8**
Formulation of a LPP - Graphical solution revised simplex method - duality theory - dual simplex method - sensitivity analysis - parametric programming	
Unit-3:	**8**
Nonlinear programming problem - Kuhn-Tucker conditions min cost flow problem - maxflow problem - CPM/PERT	
Unit-4:	**8**
Scheduling and sequencing - single server and multiple server models deterministic inventory models - Probabilistic inventory control models - Geometric Programming.	
Unit-5:	
Competitive Models, Single and Multi-channel Problems, Sequencing Models, Dynamic Programming, Flow in Networks, Elementary Graph Theory, Game Theory, Simulation	

Manoj Kapil

Reference Books:

1. H.M. Wagner, Principles of Operations Research, PHI, Delhi, 1982.
2. J.C. Pant, Introduction to Optimisation: Operations Research, Jain Brothers, Delhi, 2008
3. Hitler Libermann Operations Research: McGraw Hill Pub. 2009
4. Pannerselvam, Operations Research: Prentice Hall of India 2010
5. Harvey M Wagner, Principles of Operations Research: Prentice Hall of India 2010

PCS-215	Intrusion Detection and Information Warfare	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Recall the fundamentals of intrusion detection systems (IDS) and concepts of information warfare	K1
CO2	Explain the types, techniques, and architectures of IDS and strategies used in information warfare	K2
CO3	Apply intrusion detection tools and techniques to detect and respond to security breaches	K3
CO4	Analyze different attack patterns, IDS logs, and assess system vulnerabilities	K4
CO5	Evaluate the effectiveness of various intrusion detection methods and countermeasures against cyber warfare	K5

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Overview of Intrusion Detection systems: Introduction to networking basic concepts, Introduction about intrusion detection systems, Purpose and Scope of intrusion detection systems, Need of intrusion detection systems, applications of intrusion detection systems, Firewalls and intrusion detection systems, Challenges to Intrusion Detection Systems, Sample IDS Deployment examples.	
Unit-2:	**8**
Intrusion Detection Systems and Associated Methodologies :Uses of Intrusion detection technologies, Key Functions of Intrusion detection systems, Common Detection. Methodologies, Signature-Based Detection, Anomaly-Based Detection, stateful protocol analysis, Types of Intrusion detection technologies. **Intrusion detection Technologies and components:** Components and Architecture, Typical Components Network Architectures, Security capabilities, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities Prevention Capabilities and its implementation, Deploying IDS.	
Unit-3:	**8**
Network-Based Intrusion Detection Systems: Networking Overview, Application Layer, Transport Layer, Network Layer, Hardware Layer, Components and Architecture, Typical Components, Network Architectures and Sensor Locations, Security Capabilities, Information Gathering Capabilities, Logging Capabilities. **Wireless Network based Intrusion Detection Systems:** Wireless Networking Overview, WLAN Standards, WLAN Components, Threats against WLANs Components and Architecture, Typical Components, Network Architectures, Security Capabilities, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities, Handling Alerts.	

Unit-4:	**8**
Using and Integrating Multiple Intrusion Detection Systems Technologies: The Need for Multiple IDS technologies, Integrating Different IDS Technologies, Direct IDS Integration Indirect IDS Integration, Other Technologies with IDS Capabilities, Network Forensic Analysis Anti-Malware Technologies, Honeypots. **Host-Based IDS and Network Behaviour analysis:**Components and Architecture, Typical Components and Network Architectures, Host Architectures, Security Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities, Components and Architecture of network behaviour in presence of IDS, Components in presence of IDS, Network Architectures and Sensor Locations, Security Capabilities in presence of IDS, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities	
Unit-5:	**8**
Information Warfare: Nature of information warfare, including computer crime and information terrorism; Threats to information resources, including military and economic espionage, communications eavesdropping, computer break-ins, denial-of-service, destruction and modification of data, distortion and fabrication of information, forgery, control and disruption of information flow, electronic bombs and perception management. Information warfare policy and ethical issues.	

References Books:

1. Tim Crothers, Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network , John Wiley and Sons
2. Christopher Kruegel, Fedrick Valeur, Intrusion Detection and Correlation: Challenges and Solutions, Springer.
3. An unofficial guide to Ethical hacking by Ankit fadia, Macmillan India.
4. The Art of Intrusion: The Real Stories Behind... by Kevin D. Mitnick.
5. Intrusion Detection in Distributed Systems by NIng,Pe ng, KAP-2004.

PCS-216	Software Security	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Recall basic principles, goals, and terminology of software security	K1
CO2	Explain common software vulnerabilities such as buffer overflows, injection flaws, etc.	K2
CO3	Apply secure coding practices and techniques to mitigate known software vulnerabilities	K3
CO4	Analyze software systems to identify security flaws and potential threats	K4
CO5	Evaluate security tools and methods for software testing, verification, and validation	K5

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Software Engineering and Security Definition, software piracy, software piracy protection, security challenge in software engineering, Secure software development methodologies, multilevel security: The formal security model, waterfall model with security, comprehensive lightweight application security process (CLASP), Extreme programming and Security, Aspect-oriented programming and security.	
Unit-2:	**8**
Essential Public Key Infrastructure Introduction, The infrastructure of PKI, Services, More PKI enabled services, structure in PKI, certificates and certification, certificate path processing, certificate policy, key and certificate management, certificate revocation, different types of certificate revocation lists,	
Unit-3:	**8**
Trust and Threat Models Introduction, trust model, strict hierarchy trust model, distributed trust model, web trust model, user centric trust model, reputation trust model, trust model summary, threat model, creation process, more on risk management, DREAD, Identifying threats with attack trees, attack patterns.	
Unit-4:	**8**
JAVA programming Security Basic Development concept, JVM Security, Java language Level security, Java Security Code guidelines, java security model, protection mapping, permission overview, access control and permission, the policy tool, protection domain, access controller and privileged blocks.	
Unit-5:	**8**

Identity Management Introduction, definition – entity and identity, Identity management approach, the need for Identity management, Identity management – technical big picture, identity data layer, IdM Infrastructure services, IDM Platform specialized components, password management, provisioning module. PKI Management Module, Access management module, non-user related specialized identity management modules.	

References Books:

1. Michael Howard and David LeBlanc, **"Writing Secure Code"**, Microsoft Press, 2nd Edition, 2002.
2. Gary McGraw, **"Software Security: Building Security In"**, Addison-Wesley, 2006.
3. Mark G. Graff and Kenneth R. Van Wyk, **"Secure Coding: Principles and Practices"**, O'Reilly Media, 2003.
4. Jason Grembi, **"The Art of Software Security Assessment"**, Addison-Wesley, 2007.

DEAN

Manoj Kapil

PCS-217	Cryptography	3L:1T:0P	3 Credits

Course Outcomes:
On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Recall theoretical foundations of modern cryptography, including one-way functions, pseudorandomness, and steganography	K1
CO2	Explain key cryptographic techniques such as symmetric/asymmetric encryption, MACs, and digital signatures	K2
CO3	Apply cryptographic protocols for secure communication, key exchange, and remote user authentication	K3
CO4	Analyze zero-knowledge proofs, multi-party computations, and notions of security in cryptographic systems	K4
CO5	Evaluate cryptographic schemes and their vulnerabilities using cryptanalysis techniques like side-channel and replay attacks	K5

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

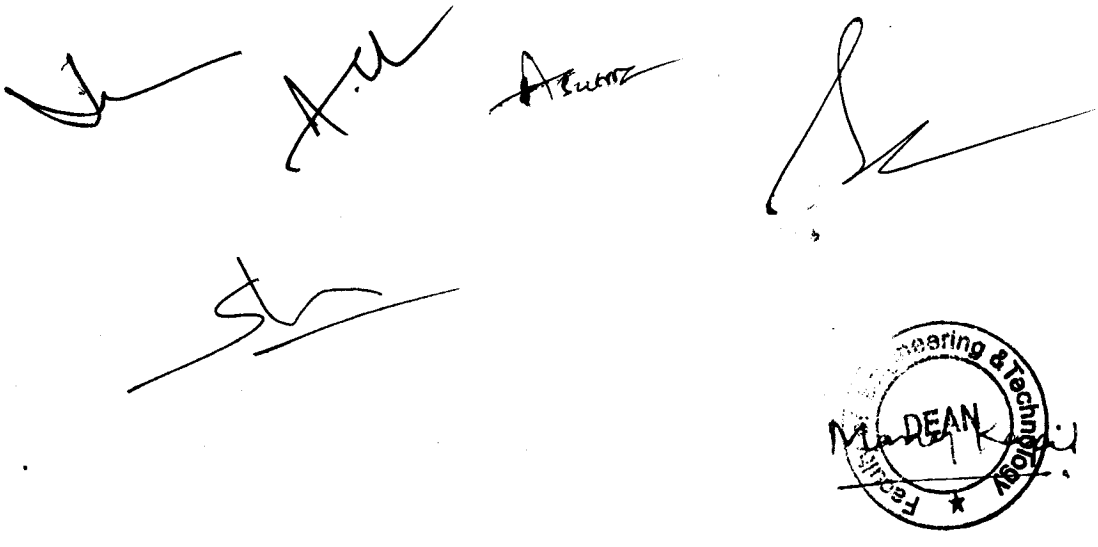
COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Theory, foundations, and applications of modern cryptography. Steganography, One-way functions; pseudorandomness and random number generators.	
Unit-2:	**8**
Encryption; authentication; symmetric cryptography, asymmetric cryptography: public-key cryptosystems; digital signatures, message authentication codes.	
Unit-3:	**8**
remote user authentication, notions of security; zero knowledge/ interactive proofs, multi-party cryptographic protocols, key exchange and applications.	
Unit-4:	**8**
Cryptanalysis of cryptographic primitives and protocols, such as by side-channel attacks, differential cryptanalysis, or replay attacks; and cryptanalytic techniques on deployed systems.	
Unit-5:	**8**
Advanced Topics - ECC, DNA cryptography, quantum cryptography, Digital Watermarking. **Digital signatures:** Definitions and applications, Lamport and Merkle schemes. overview of signatures based on discrete-log.certificates and trust management. , SSL/TLS and IPsec, Privacy mechanisms.	

Manoj Kapil

Reference Books:

1. Kahate, Atul, "Cryptography and Network Security." Tata McGraw Hill, 2007.
2. Delfs, Hans, "Introduction to cryptography." Springer, 2004.
3. Cryptography and Network Security by Stalling, PHI
4. Cryptography by Behrouz A. Forouzan,TMH
5. Cryptography & security services , Mechanism & application By Mogollon , Manuel , Cyber tech. Pub.
6. Cryptography and hardware security By Stalling, W PHI.
7. Introduction to Modern Cryptography by J. Katz and Y. Lindell.
8. Handbook of Applied Cryptography by A. Menezes, P. Van Oorschot, S. Vanstone



PCS-218	Database Security	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Identify key concepts of information security architecture and explain security methods for operating systems and databases	K1
CO2	Explain user administration techniques, authentication mechanisms, and remote user access management	K2
CO3	Apply password policies, user privilege management, and database application security models in various environments	K3
CO4	Analyze and implement Virtual Private Databases (VPD) using SQL Server and Oracle features for row and column-level security	K4
CO5	Evaluate database auditing models and processes using Oracle triggers, SQL Server triggers, and fine-grained auditing mechanisms	K5

Content	Contact Hours
Unit-1:	**8**
Security Architecture Introduction, Security, Information System, Database Management Systems, Information Security, Information Security Architecture, Database Security, Asset Types and their value, security methods, Operating System Security Environment, Authentication Methods, User Administration, Password policies, Vulnerabilities of operating System.	
Unit-2:	**8**
Administration of Users Introduction, Documentation of user Administration, Operating system authentication, creating users, creating a SQL Server user, Removing Users, modifying users, default users, remote users, database links, linked servers, remote servers, practices for administration and managers.	
Unit-3:	**8**
Password Policies, Privileges and Database Application Security Models Defining and using profiles, Designing and implementing password policies, Granting and Revoking user privileges, creating, assigning and Revoking user Roles. Types of users, security models, Application types, Application Security Models, Data Encryption.	
Unit-4:	**8**
Virtual Private Databases Introduction, Overview of virtual databases, implementing a VPD using views, implementing a VPD using Application context in Oracle, Implementing oracle virtual private Databases, Viewing VPD policies and application context using the Data Dictionary, Viewing VPD policies and application contexts using policy manager, implementing Row and Column level Security with SQL server.	

Unit-5:	**8**
Database Auditing Models and Application Data Auditing Auditing Overview, auditing environment, auditing process, auditing objectives, auditing classification and types, benefits and side effects of auditing, auditing models. DML action auditing architecture, oracle triggers, SQL Sever triggers, Fine grained Auditing (FGA) with Oracle, Auditing application errors with oracle, Creating DLL Triggers with oracle.	

Reference Books:

1. Ron Ben Natan, Implementing Database Security and Auditing, Elsevier Digital Press, 1st Edition, 2005.
2. David Litchfield, Chris Anley, John Heasman, Bill Grindlay, The Database Hacker's Handbook: Defending Database Servers, Wiley, 2005.
3. Michael Gertz and Sushil Jajodia, Handbook of Database Security: Applications and Trends, Springer, 2008.
4. Carlos Coronel, Steven Morris, Peter Rob, Database Systems: Design, Implementation, & Management, Cengage Learning, 13th Edition, 2019.

DEAN

PCS-219	Database Management Systems	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Recall fundamental database concepts, types of users, data models, schemas, and architectures	K1
CO2	Explain relational models, relational algebra, SQL queries, constraints, and relational DBMS characteristics	K2
CO3	Apply Oracle architecture concepts and implement database operations using PL/SQL elements like triggers, UDFs	K3
CO4	Analyze relational schema using functional dependencies and normalization techniques (1NF–BCNF)	K4
CO5	Evaluate concurrency control, recovery mechanisms, and advanced concepts like object-oriented and distributed DBMS	K5

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

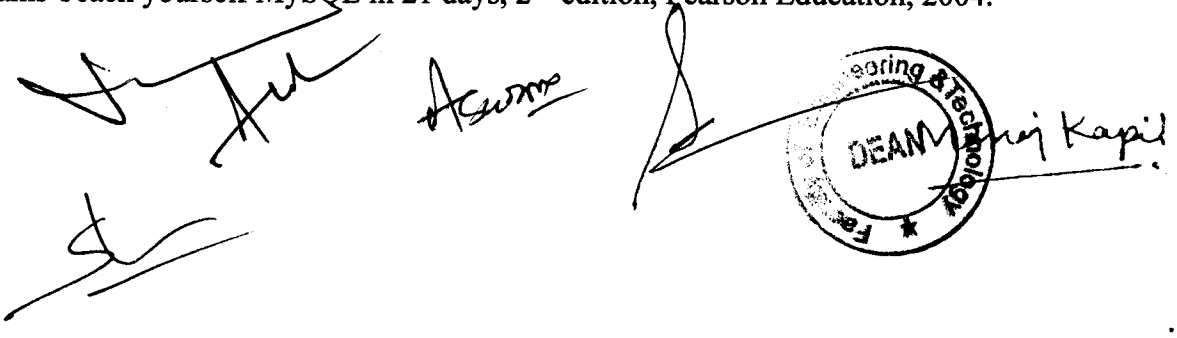
Content	Contact Hours
Unit-1:	**8**
Basic concepts Database & database users, characteristics of the database, database systems, concepts and architecture, date models, schemas & instances, DBMS architecture & data independence, database languages & interfaces, data modeling using the entity-relationship approach. Overview of hierarchical, Network & Relational Data Base Management Systems.	
Unit-2:	**8**
Relational model, languages & systems Relational data model & relational algebra: relational model concepts, relational model constraints, relational algebra, SQL- a relational database language: date definition in SQL, view and queries in SQL, specifying constraints and indexes in sql, a relational database management systems.	
Unit-3:	**8**
Oracle Architecture, Logical Data Structures Physical Data Structure, Instances, Table Spaces, Types of Tablespaces, Internal Memory Structure, Background Processes, Data Types, Roles & Privileges, Stored Procedures, User Defined Functions, Cursors, Error Handling, Triggers.	
Unit-4:	**8**
Relational data base design: Function dependencies & normalization for relational dataases: functional dependencies, normal forms based on primary keys, (1NF, 2NF, 3NF & BCNF), lossless join and dependency preserving decomposition.	

DEAN

Unit-5:	8
Concurrency control & recovery techniques Concurrency control techniques, locking techniques, time stamp ordering, granularity of data items, recovery techniques: recovery concepts, database backup and recovery from catastrophic failures. Concepts of object oriented database management systems, Distributed Data Base Management Systems.	

Reference Books:

1. Date, Kannan, Swaminathan, "An Introduction to Database Systems", 8th Edition Pearson Education, 2007
2. Singh S.K., "Database System Concepts, design and application", Pearson Education,2006
3. Ullman, J. D., "Principals of database systems", Galgotia publications, 1999
4. Rob, Coronell, "Database Systems Design, Implementation and Management", 5th edition, Thomson Course Technology, 2003.
5. Oracle Reference Manual.
6. Michael J. Donahoo, Gregory D. Speegle," SQL practical guide for developers", Elsevier Inc., 2005
7. Sams Teach yourself MySQL in 21 days, 2nd edition, Pearson Education, 2004.



PCS-220	Mobile & Wireless Network Security	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Recall fundamental concepts of wireless communication technologies, system types, and IEEE 802.11 standards	K1
CO2	Explain the architecture of infrastructure and ad hoc networks, including MAC and routing protocols in MANET	K2
CO3	Apply security mechanisms such as encryption, integrity checks, and anti-jamming methods to wireless communication scenarios	K3
CO4	Analyze advanced wireless threats like interception, spoofing, theft of service, and privacy concerns in modern wireless systems	K4
CO5	Evaluate wireless network security architectures in WLAN, WIMAX, MANETs, and sensor networks for secure communication	K5

K1 – Remember, K2 – Understand, K3 – Apply, K4 – Analyze, K5 – Evaluate, K6 – Create

COURSE CONTENTS:

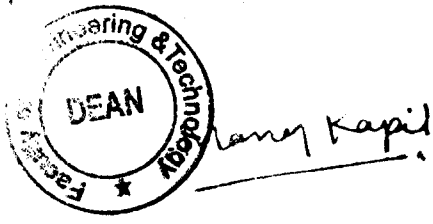
Content	Contact Hours
Unit-1:	**8**
Fundamental of Wireless Communication Technology, Wireless Network, Wireless Characteristics, Channels, Propagation. Types of wireless systems and their parameters, Satellite System, Cellular System, GSM, Wireless LAN, PAN, MAN and WANs, IEEE 802.11 Standards.	
Unit-2:	**8**
Infrastructure and Infrastructure less Network, Mobile Ad hoc Network (MANET), Wireless Sensor Network, Properties of MANET, MANET Applications, MAC (Hidden and Exposed terminal problems), MAC Protocol for MANET, Routing and various routing algorithms.	
Unit-3:	**8**
Security Definition, Services, Mechanisms, Spread spectrum, Frequency hopping, Encryption, Integrity check-sums, Assessment issues specifically related to wireless, Jamming, Interception, Spoofing, Fraud, Satellite Jamming, Theft of service – entertainment services on downlink, Hidden signals .	
Unit-4:	
Theft of service – uplink, Monitoring long distance communications, Low Probability of Intercept (LPI), Circular Error Probability (CEP), Confidentiality of information, Traffic analysis, Cellular Cloning of AMPs, Privacy issues in E911, Geo location WLAN, WEP issues, Managing a wireless LAN interconnected to wired LAN.	

Engineering & Technology DEAN Kapil

Unit-5:	**8**
Security in WLAN, Security in WMAX, Security in Ad Hoc Networks, Distributed Systems Security, Key Management, Secure Routing, Cooperation in MANETs, Security of Wireless Sensor Networks, Privacy and anonymity in MANETs, Intrusion Detection Systems in MANETs, Protocol Stack, Evaluation of Security Architectures for Mobile Broadband Access.	

Reference Books:

1. Ad Hoc Wireless Networks, Architecture and Protocols by C. Siva Ram Murthy
2. Wireless security handbook by Aron E. Earle.
3. Handbook of research on wireless security by Yan zhang jun zheng miao ma.



PCSE-222	Object Oriented Programming Using C++	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

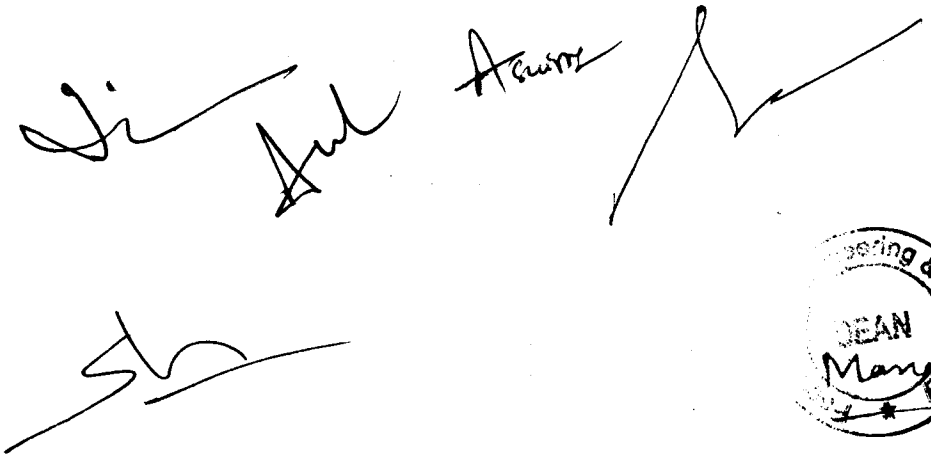
CO	CO Statement	Bloom's Level
CO1	Recall fundamental object-oriented concepts such as abstraction, encapsulation, inheritance, and polymorphism	K1
CO2	Understand the structure of C++ classes, constructors, destructors, and the basic idea of object behavior	K2
CO3	Apply C++ features like dynamic memory allocation, garbage collection, and inheritance to create class hierarchies	K3
CO4	Analyze different forms of polymorphism including function overloading, operator overloading, and templates	K4
CO5	Evaluate the use of advanced features like multiple inheritance, persistent objects, streams, and file handling	K5

COURSE CONTENTS:

Content	Contact Hours
Unit-1:	**8**
Objects, relating to other paradigms (functional, data decomposition),basic terms and ideas (abstraction, encapsulation, inheritance, polymorphism).	
Unit-2:	**8**
Overview of C, Encapsulation, information hiding, abstract data types, object & classes: attributes, methods. C++ class declaration, state identity and behavior of an object, constructors and destructors, instantiation of objects, default parameter value, object types.	
Unit-3:	**8**
C++ garbage collection, dynamic memory allocation, metaclass, Inheritance, Class hierarchy, derivation – public, private & protected, aggregation, omposition vs classification hierarchies.	
Unit-4:	**8**
polymorphism, operator overloading, parametric polymorphism, generic function – template function, function name overloading, overriding inheritance methods, run time polymorphism.	
Unit-5:	**8**
Standard C++ classes, using multiple inheritance, persistent objects, streams and files.	

References Books :

1. E. Balaguruswamy, "Objected Oriented Programming with C++", TMH.
2. D . Parasons, "Object Oriented Programming with C++",BPB Publication.
3. R. Lafore, "Object Oriented Programming using C++".
4. R. S. Pressman "Software Engineering", Mc Graw Hill



Open Elective II

PCSE-227	Cost Management of Engineering Projects	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand the fundamental concepts of project cost management and its significance in the successful execution of engineering projects.	K1,K2
CO2	Estimate project costs using various methods and techniquessuch as analogous, parametric, and bottom-up estimating.	K3, K5
CO3	Prepare and interpret project budgets, cash flow forecasts, and cost control reports for engineering projects.	K3, K_4
CO4	Apply techniques for cost planning, budgeting, and monitoring throughout the project lifecycle to manage project finances effectively.	K3, K_4

K1–Remember,K2–Understand,K3 –Apply,K4–Analyze,K5 –Evaluate,K6–Create

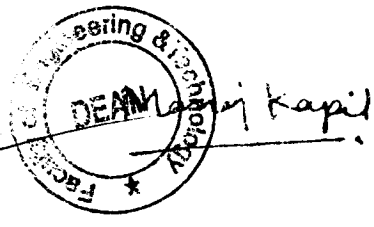
COURSE CONTENTS:

Content	Contact Hours
Unit 1	**8**
Cost concepts in decision-making; Relevant cost, Differential cost, Incremental cost and Opportunity cost. Objectives of a Costing System; Inventory valuation; Creation of a Database for operational control; Provision of data for Decision-Making.	
Unit-2:	**8**
Project: meaning, Different types, why to manage, cost overruns centres, various stages of project execution: conception to commissioning. Project execution as conglomeration of technical and non-technical activities. Detailed Engineering activities. Pre project execution main clearances and documents Project team: Role of each member. Importance Project site: Data required with significance. Project contracts. Types and contents. Project execution Project cost control. Bar charts and Network diagram. Project commissioning: mechanical and process	
Unit-3:	**8**
Cost Behavior and Profit Planning Marginal Costing; Distinction between Marginal Costing and Absorption Costing; Break-even Analysis, Cost-Volume-Profit Analysis. Various decision-making problems. Standard Costing and Variance Analysis. Pricing strategies: Pareto Analysis.	
Unit-4:	**8**

Target costing, Life Cycle Costing. Costing of service sector. Just-in-time approach, Material Requirement Planning, Enterprise Resource Planning, Total Quality Management and Theory of constraints. Activity-Based Cost Management, Bench Marking; Balanced Score Card and Value-Chain Analysis. Budgetary Control; Flexible Budgets; Performance budgets; Zero-based budgets. Measurement of Divisional profitability pricing decisions including transfer pricing.	
Unit-5:	**8**
Quantitative techniques for cost management, Linear Programming, PERT/CPM, Transportation problems, Assignment problems, Simulation, Learning Curve Theory.	

Reference Books:

1. Cost Accounting A Managerial Emphasis, Prentice Hall of India, New Delhi
2. Charles T. Horngren and George Foster, Advanced Management Accounting
3. Robert S Kaplan Anthony A. Alkinson, Management & Cost Accounting
4. Ashish K. Bhattacharya, Principles & Practices of Cost Accounting A. H. Wheeler publisher
5. N.D. Vohra, Quantitative Techniques in Management, Tata McGraw Hill Book Co. Ltd.



PCSE-228	Composite Materials	3L:1T:0P	4 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Understand the fundamental concepts, classification, and applications of composite materials in engineering industries.	K1,K2
CO2	Explain the properties and roles of matrix and reinforcement materialsin composite systems, including fibers, particulates, and laminates.	K3, K5
CO3	Analyze the mechanical behavior of composite materialsunder different loading conditions and environmental influences.	K3, K4
CO4	Select appropriate manufacturing processes for different types of composite materials, such as hand lay-up, filament winding, pultrusion, resin transfer molding, etc.	K3, K4

K1–Remember,K2–Understand,K3 –Apply,K4–Analyze,K5 –Evaluate,K6–Create

COURSE CONTENTS:

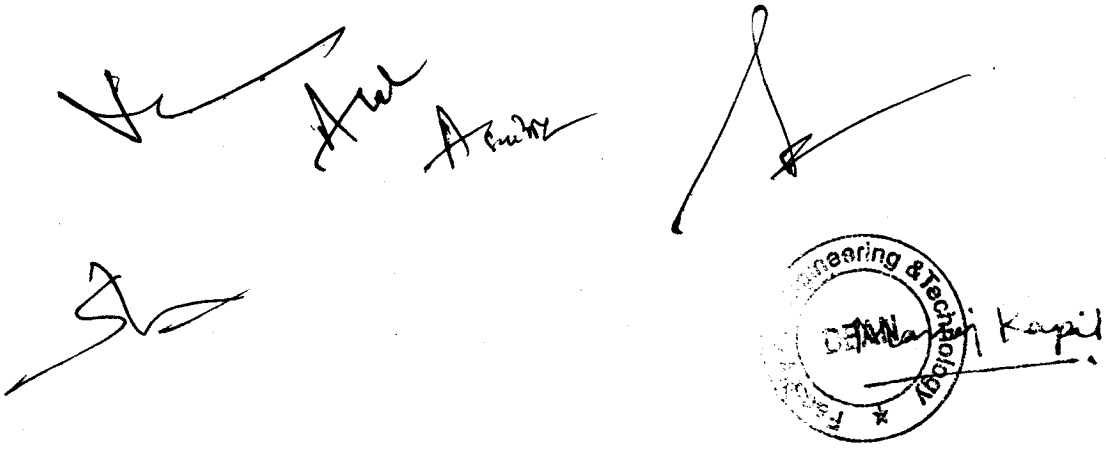
Content	Contact Hours
Unit 1	**8**
INTRODUCTION: Definition – Classification and characteristics of Composite materials. Advantages and application of composites. Functional requirements of reinforcement and matrix. Effect of reinforcement (size, shape, distribution, volume fraction) on overall composite performance.	
Unit-2:	**8**
REINFORCEMENTS: Preparation-layup, curing, properties and applications of glass fibers, carbon fibers, Kevlar fibers and Boron fibers. Properties and applications of whiskers, particle reinforcements. Mechanical Behavior of composites: Rule of mixtures, Inverse rule of mixtures. Isostrain and Isostress conditions.	
Unit-3:	**8**
Manufacturing of Metal Matrix Composites: Casting – Solid State diffusion technique, Cladding – Hot isostatic pressing. Properties and applications. Manufacturing of Ceramic Matrix Composites: Liquid Metal Infiltration – Liquid phase sintering. Manufacturing of Carbon – Carbon composites: Knitting, Braiding, Weaving. Properties and applications.	
Unit-4:	
Manufacturing of Polymer Matrix Composites: Preparation of Moulding compounds and prepregs – hand layup method – Autoclave method – Filament winding method – Compression moulding – Reaction injection moulding. Properties and applications.	

DEAN

Unit-5:	
Strength: Laminar Failure Criteria-strength ratio, maximum stress criteria, maximum strain criteria, interacting failure criteria, hygrothermal failure. Laminate first play failure-insight strength; Laminate strength-ply discount truncated maximum strain criterion; strength design using caplet plots; stress concentrations.	

Reference Books:

1. Hand Book of Composite Materials-ed-Lubin.
2. Composite Materials – K.K.Chawla.
3. Composite Materials Science and Applications – Deborah D.L. Chung.
4. Composite Materials Design and Applications – Danial Gay, Suong V. Hoa, and Stephen W. Tasi.



PCSE-229	Waste to Energy	3L:1T:0P	3 Credits

Course Outcomes:

On completion of course the students are able:

CO	CO Statement	Bloom's Level
CO1	Recall and explain the classification, characteristics, and energy potential of various types of waste	K1, K2
CO2	Understand the principles and technologies involved in waste-to-energy conversion processes	K2
CO3	Apply thermochemical and biochemical methods for energy extraction from waste (e.g., incineration, anaerobic digestion)	K3
CO4	Analyze technical, environmental, and economic feasibility of waste-to-energy systems	K4
CO5	Evaluate the performance, sustainability, and policy implications of existing waste-to-energy projects	K5
CO6	Design small-scale waste-to-energy systems suitable for local/community-level applications	K6

K1–Remember,K2–Understand,K3 –Apply,K4–Analyze,K5 –Evaluate,K6–Create

COURSE CONTENTS:

Content	Contact Hours
Unit 1	**8**
Introduction to Energy from Waste: Classification of waste as fuel – Agro based, Forest residue, Industrial waste - MSW – Conversion devices – Incinerators, gasifiers, digestors.	
Unit-2:	**8**
Biomass Pyrolysis: Pyrolysis – Types, slow fast – Manufacture of charcoal – Methods - Yields and application – Manufacture of pyrolytic oils and gases, yields and applications.	
Unit-3:	**8**
Biomass Gasification: Gasifiers – Fixed bed system – Downdraft and updraft gasifiers – Fluidized bed gasifiers – Design, construction and operation – Gasifier burner arrangement for thermal heating – Gasifier engine arrangement and electrical power – Equilibrium and kinetic consideration in gasifier operation.	
Unit-4:	**8**
Biomass Combustion: Biomass stoves – Improved chullahs, types, some exotic designs, Fixed bed combustors, Types, inclined grate combustors, Fluidized bed combustors, Design, construction and operation - Operation of all the above biomass combustors.	
Unit-5:	

Biogas: Properties of biogas (Calorific value and composition) - Biogas plant technology and status - Bio energy system - Design and constructional features - Biomass resources and their classification - Biomass conversion processes - Thermo chemical conversion - Direct combustion - biomass gasification - pyrolysis and liquefaction biochemical conversion - anaerobic digestion - Types of biogas Plants – Applications Alcohol production from biomass - Bio diesel production - Urban waste to energy conversion Biomass energy programme in India.	

Reference Books:

1. Non Conventional Energy, Desai, Ashok V., Wiley Eastern Ltd., 1990.
2. Biogas Technology - A Practical Hand Book - Khandelwal, K. C. and Mahdi, S. S., Vol. I & II, Tata McGraw Hill Publishing Co. Ltd., 1983.
3. Food, Feed and Fuel from Biomass, Challal, D. S., IBH Publishing Co. Pvt. Ltd., 1991.
4. Biomass Conversion and Technology, C. Y. WereKo-Brobby and E. B. Hagan, John Wiley & Sons, 1996.

DEAN