


UNIVERSITY OF MADRAS
INSTITUTE OF DISTANCE EDUCATION
DIPLOMA IN INFORMATION SECURITY AND CYBER LAW
(With effect from the Academic Year 2023-2024)
SCHEME OF EXAMINATION

- a) Candidates who have qualified for a Degree (Regular) of this University or any other University recognized by UGC/AIU accepted as equivalent thereto by this University under **10 + 2 + 3 (or) 11 + 1 + 3 (or) 11 + 2 + 2** pattern are eligible for admission to the Diploma Courses other than Sanskrit/ French/ German.
- b) The duration of the course is one year with Semester pattern examination.
- c) Admission is open to the students of Postgraduate Course in the Colleges/ Distance Education Institutions (Regular)/university Departments of the University of Madras or any other University recognized by UGC/AIU accepted as equivalent thereto by this University are eligible for admission to any one of the Diploma Course provided that they should submit the application form for admission together with bonafide certificate and Photostat copies of all the certificates duly attested by the principal from the institution where they are studying post-Graduate Degree Course concerned.
- d) A student can additionally enroll for one Diploma Course only at a time.
- e) Course of study and scheme of Examination:

| Paper | Subjects | Credit | Max Marks | | Total |
|--------------------|-----------------------------------------------------------------|--------|-----------|------|-------|
| | | | Int. | Ext. | |
| I Semester | | | | | |
| Paper – I | Introduction to Criminology and Criminal Justice Administration | 5 | 25 | 75 | 100 |
| Paper-II | Forms of Cyber Crimes | 5 | 25 | 75 | 100 |
| Paper-III | Fundamentals of Information Security | 5 | 25 | 75 | 100 |
| Paper-IV | Cyber Laws | 5 | 25 | 75 | 100 |
| II Semester | | | | | |
| Paper-V | Intellectual Property Rights | 5 | 25 | 75 | 100 |
| Paper-VI | Advanced Information Security | 5 | 25 | 75 | 100 |
| Paper-VII | Digital Frauds | 5 | 25 | 75 | 100 |
| Paper-VIII | Critical Infrastructure Security Management | 5 | 25 | 75 | 100 |

Center for Cyber Forensics & Information Security
 University of Madras
 Chennai 600 005


 Director i/c,
 Center for Cyber Forensics & Information Security
 University of Madras
 Chennai 600 005

**INTRODUCTION TO CRIMINOLOGY AND CRIMINAL JUSTICE
ADMINISTRATION**

Unit 1: Criminology Concepts:

Definition and scope – Definition of Crime & Juvenile Delinquency: social and Legal – relation of criminology with correctional administration, Forensic Science, Criminal Law and other disciplines – Characteristics of Crime – Mensrea, Actusreus.

Unit 2: Schools of Criminology:

Classical, Neo-classical– Positive Schools of Criminology.

Unit 3: Causes of Crime: Sociological Explanations of Criminal behavior:

Sociological theories – Anomie, Differential Association theory, Opportunity Structure, Social Disorganization, Subculture and Gang Delinquency, Containment, Social Bond, Labelling, Multiple factor approach- Radical Criminology – Other Factors- Family peer group, Neighbourhood and Mass media.

Unit 4: Crime and its contemporary forms:

White collar crimes, Economic Offences, Organized Crimes, Terrorism, Crime and Media, Cyber Crime & Pornography.

Unit 5: Criminal Justice System.

- a. Police – Organizational structure of Police in India – Different wings in the states and Districts and their functions – Police & Law Enforcement – F.I.R.- Cognizable and non-cognizable offences, bailable and non-bailable offence – arrest, search, seizure –Interrogation of suspects and witnesses – Charge sheet – Cyber-crime Cells – Structure & Investigations of Cyber-crime cases.
- b. Judiciary – Different types of courts – powers – Proceedings in the court before trial, after trial, Plea of guilty, Sentencing, Cyber Appellate Tribunals.

Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005


M. S. Srinivasan

Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

References:

1. Hagan, F. (2017). Introduction to Criminology (9th ed.) Los Angeles: SAGE
2. Sutherland, E.H., & Cressey, D.R. (1974) Principles of Criminology. Philadelphia, PA: Lippincott.
3. Lab,S. (2013), Crime prevention (8th ed.). Elsevier.
4. Ahuja Ram, (2000), Criminology, Rawat Publications, New Delhi.
5. Paranjape N.V (2013) Criminology and Penology, Central Law Publications, Allahabad.
6. Srivastava S. S (2002) – Criminology and Criminal Administration, Central Law Agency, Allahabad.

Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005


Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

FORMS OF CYBER CRIMES

Unit 1: Cyber Crime – Introduction – History and Development – Definition, Nature and Extent of Cyber Crimes in India and other countries - Classification of Cyber Crimes - Trends in Cyber Crimes across the world.

Unit 2: Forms of Cyber Crimes – Hacking, Cracking, DoS – Viruses, Worms, Bombs, Logical Bombs, Time Bombs, Email Bombing, Data Diddling, Salami Attacks, Phishing, Steganography, Cyber Stalking, Spoofing, Pornography, Defamation, Computer Vandalism, Cyber Terrorism, Cyber Warfare, Crimes in Social Media, Malwares, Adware, Scareware, Ransomware, Social Engineering, Cloud based crimes -Understanding Fraudulent Behaviour, Fraud Triangle, Fraud Detection Techniques, Intellectual Property Rights and Violation of Intellectual Property Rights, Ecommerce Frauds and Other Forms.


Unit 3: Modus Operandi of Various Cybercrimes and Frauds – Definition of Various Types of Cyber Frauds – Modus Operandi - Fraud Triangle – Fraud Detection Techniques Including Data Mining and Statistical References - Countermeasures.

Unit 4: Profile of Cyber criminals – Cyber Crime Psychology – Psychological theories dealing with cyber criminals


Unit 5: Impact of cybercrimes – to the Individual, to the Corporate and Companies, to Government and the Nation.

References:

1. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats by Will Gragido, John Pirc, 1st edition, Syngress, 7 January 2011
2. Cyber Crime & Warfare: All That Matters by Peter Warren, Michael Streeter, Kindle Edition, Hodder & Stoughton, 26 July 2013
3. Digital Evidence and computer crime by Eoghan Casey, 3rd Edition, Academic Press Publication, 17 June 2011


Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

4. The Psychology of Cyber Crime: Concepts and Principles by Grainne Kirwan, Andrew Power, 1 edition, Business Science Reference, 15 March 2012
5. The basics of Cloud Computing – Understanding the fundamentals of cloud computing in theory and practice by Derrick Rountree, Ileana Castrilo, Illustrated Edition, Syngress Publication, 01 Nov 2013


Director/IC,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

Director/IC,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

FUNDAMENTALS OF INFORMATION SECURITY

Unit 1: Information security

Information - Definition, Valuation and Place in Corporate Strategic Competitive Advantage – Information Security vs. Cybersecurity – CIA Triad – Active vs. Passive Attacks – OSI Model – Authentication – Authorization – Access Control. Managerial vs. Technological Paradigms -- Six-Pronged Approach -- Logical vs. Physical Security -- Networked Information System Security -- Open vs. Closed Networks – Threats – Vulnerabilities — Countermeasures -- Operational Controls -- Managerial Controls -- Physical Controls – Information Security Policy -- Information Security and Data Protection Laws.

Unit 2: Perimeter Security

Firewalls – Planning for Types and Design -- Firewall Configuration Strategies -- Proxy Servers -- Packet Filtering -- Application-Level Firewalls -- User Authentication -- Creating and Managing Rule Base -- Bastion Host -- Demilitarized Zone -- Logs, Audit and Administration of Firewalls – Security Protocols – Benefits of Firewall – Application

Unit 3: Architecting Secured Data Transmission

Data transmission architecture -- TCP/IP structure -- Security issues in the internet protocols and structure -- Models and approaches to security in data transmission -- Virtual Private Networks -- Remote Access -- Intrusion Detection and Honeypots- Concepts only. Detailed discussions in the Paper on Forensics -- Logging and monitoring of open network traffic -- Cryptographic applications -- Symmetric vs. Asymmetric protocols -- DES, Diffie-Hellman protocols -- E-Commerce and Cryptography -- E- Business models -- Trusted Third Party Services -- Public Key Infrastructure – CHAP, Kerberos, Single Sign On -Digital Signature -- Digital Time- Stamping – Steganography

Unit 4: Legal Framework for E-Commerce Transactions & Assurance Services

Legal implications of Information Security Infractions and breaches -- Issues in trans-border cybercrimes -- Problems in investigating cybercrimes -- UNCITRAL initiative in combating cyber crimes -- Information Technology Act,2000 and the Rules framed there under -- Discussion on select reported International and National cases


M. M. M.
Director, I/C,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

Unit 5: Security Assurance Services

Concept of security assurance -- Corporate IT Scorecard -- Information Technology Governance -- Information Security Governance -- The IA3paradigm leading to security assurance

References:

1. Security Technologies for the World Wide Web, Rolf Oppliger, Artech House, 2000
2. Internet and Intranet Security, Rolf Oppliger, Artech House, 1998
3. Building Internet Firewalls, Brent Chapman and Elizabeth Zwicky, O'Reilly and Associates, 1995


Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

Director
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

CYBER LAWS

Unit 1: Fundamentals of Cyber Law

Introduction on cyber space- Jurisprudence of cyber Law- Scope of Cyber Law – Cyber law in India with special reference to Information Technology Act, 2000 with amendments

Unit 2: E- Governance and E- Commerce

Electronic Governance – Procedures in India – Essentials & System of Digital Signatures – the Role and Function of Certifying Authorities – Digital contracts – UNCITRAL Model law on Electronic Commerce Cryptography – Encryption and decryption

Unit 3: Cyber Crimes

Introduction to Cyber Crimes – Kinds of Cyber Crimes – Investigation Related issues – issues relating to Jurisdiction - Relevant provisions under Information Technology act, Evidence Act, Indian Penal Code –Cyber Forensics –Case studies


Unit 4: Legal Issues and Courtroom skills

Key legal aspects of computer crime – IT Act of 2000 (discussed above) – Evidence act – Terrorism issues – Overseas Co-operation – Seizure of backups and data Disclosure – Dealing with third party and confidential and Privileged material – Selected comparative law overseas – Virtual Drives, Virtual Connectivity – Emergent Issues – Civil Issues and General Enforcement _ Potential defamation –Intellectual Property Infringement – Confidentiality Obligations – Internal Boardroom Disclosure and the traps – Duties of Disclosure – Data Preservation and Retention –Seizure of Records – proceeds of crime - Damages – the domain of the instrument of fraud –Evidential aspects of computer material – Planning operations – Admissibility – Discovery – Civil and Criminal – particular Devices – Best Practice – preparation of Material for Court –Review of selected real- world case examples – challenges and suggested solutions – Court Room Environments – Evidential Presentation and Explanation – Key players in the courtroom – Role, Obligation and Expectations of 'Expert witness'

Unit 5: Practices in cyber Jurisprudence – Regional and Global – Important Case Laws.

References:

1. Saurabh Sharma, "Information Security and Cyber Law", Vikas publication, 2010
2. Peggy E Chaudhary, "Protecting Your Intellectual Property Rights: Understanding the Role of Management, Governments, Consumers and Pirates", Springer, 2013
3. Brain Craig, "Cyber Law: The Law of Internet and IT", Prentice Hall, 2012


Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

Handwritten text, possibly a date or reference number, located at the bottom left of the page.

SEMESTER – II

PAPER – V

CREDITS: 5

INTELLECTUAL PROPERTY RIGHTS

Introduction to Intellectual Property

I. Copyright – Basics- Infringement – Liability- Defenses- Case studies and Internet Applications

II. Trademark - Basics - Traditional Infringement and Dilution – Defenses - Case Studies and Internet Application

III. Trade Secrets - Efforts to Maintain Secrecy, Including Confidentially Agreements- Remedies for Trade Secret Misappropriation


IV. Patent Law - Basics - Infringement –Defenses - Business Method Patents

V. Additional Topics - “where is the internet?- The Digital Marketplace

VI. Intellectual Property Rights – Global Scenario with Case Laws

References:

1. Neeraj Pandey, Khushdeep Dharni, “Intellectual Property Rights”, PHI Learning; 1st edition.
2. Dr. B.L. Wadehra, “Law relating to patents, trademarks, copyright, design and geographical indications”, 5th edition, Universal law Publication.
3. Dr. S.R. Myneni, “Law of Intellectual Property”, 6 th Edition, Asia Law House Publication.
4. David I. Bainbridge, “International Property”, 9th Edition, Pearson Education Publication.
5. W.R. Cornish, D Llewelyn, “Intellectual Property, Patents, Copyright, trademarks and allied rights”, sweet and Maxwell Publication.


Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

PAPER – VI

CREDITS: 5

ADVANCED INFORMATION SECURITY

Unit 1: Advanced Cryptography and Secure Protocols

Advanced Cryptographic Algorithms – AES & RSA - Elliptic Curve Cryptography -- Cryptographic Hash Functions and Message Authentication Codes (MACs) -- Post-Quantum Cryptography -- Blockchain and Cryptocurrency Security -- Secure Multiparty Computation and Homomorphic Encryption -- Cryptanalysis Techniques (Side-Channel Attacks, Fault Injection Attacks) -- Blockchain Security Considerations (Consensus Mechanisms, Smart Contract Security).

Unit 2: Network Security and Defense

Advanced Firewall Technologies (Next-Generation Firewalls) -- Intrusion Detection and Prevention Systems (IDPS) -- Network Traffic Analysis and Packet Forensics -- Zero Trust Network Architecture -- Software-Defined Networking (SDN) Security -- Network Access Control (NAC) and Network Segmentation Strategies – DNSSEC, DNS filtering – Network Based Malware Analysis and Sandboxing

Unit 3: Secure Cloud and Container Environments

Cloud Security Architecture and Design -- Container Security (Docker, Kubernetes) -- Cloud Access Security Brokers (CASBs) -- DevSecOps and Continuous Security in Cloud Environments Cloud Compliance and Governance (GDPR, HIPAA, SOC 2) -- Container Orchestration Security Best Practices -- Cloud Workload Protection Platforms (CWPP) and Cloud Security Posture Management (CSPM).

Unit 4: Threat Intelligence and Cyber Threat Hunting

Cyber Threat Landscape Analysis -- Threat Intelligence Platforms (TIPs) and Feeds -- Cyber Threat Hunting Methodologies -- Advanced Persistent Threats (APTs) and Nation-State Actors -- Dark Web Monitoring and Analysis Threat Modeling Methodologies (STRIDE, DREAD, PASTA) -- Machine Learning and AI in Threat Intelligence -- Cyber Deception Techniques and Honeytokens -- Threat Hunting Using Open-Source Tools and Platforms -- Incident Response Planning and Cyber Crisis Management.

AP/10/2021
AP/10/2021
AP/10/2021
AP/10/2021



Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

Unit 5: Offensive Security Techniques and Red Teaming

Penetration Testing Methodologies (White, Grey, Black Box)-- Social Engineering and Phishing Attacks -- Red Team Operations and Adversarial Simulation -- Exploit Development and Reverse Engineering -- Legal and Ethical Considerations in Offensive Security-- Post-Exploitation Strategies and Privilege Escalation -- Hardware Hacking and Embedded System Exploitation -- Adversary Simulation Methodologies (MITRE ATTACK Framework, Purple Teaming)

References:

1. "Understanding Cryptography: A Textbook for Students and Practitioners" by Christof Paar and Jan Pelzl
2. "Network Security Essentials: Applications and Standards" by William Stallings
3. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif
4. "The Hacker Playbook 3: Practical Guide To Penetration Testing" by Peter Kim


Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

20/10/2020
10:10:30 AM
600 005 Chennai

DIGITAL FRAUDS

1. **Introduction:** Fraud introduction and overview - “Standard” fraud types - recent fraud types - The next generation of fraud – Fraud Detection – Fraud opportunities - Countermeasures
2. **Banking Fraud:** Banking Concepts – Forms of Banking Fraud - Core Banking Solution - Security mechanisms to secure network and devices – Internet Banking - Mobile banking - Cyber Security Attacks On Banks – Fraud Detection – Fraud opportunities
3. **Corporate Fraud:** Nature of Fraud – Forms of Corporate Fraud - Elements of crimes of theft and fraud – Role of ethics in fighting fraud – Controlling fraud – fraud risk management – Investigating fraud – Computer fraud and countermeasures
4. **Financial Fraud:** The Origin of Financial Fraud – Forms of Financial Fraud - Treadway to Sarbanes-Oxley - The Sarbanes-Oxley Act - The Audit Committee - Detection and Its Aftermath - Investigating Financial Fraud - Finding the False Numbers - Getting a New Audit Report on the Financial Statements - The Securities and Exchange Commission - The Future of Financial Reporting
5. **Trends in e-commerce & digital fraud:** Introduction-Methods of payment fraud - Decoding the methods of online or e-commerce fraud - The financial impact of online or E-commerce fraud - E-commerce fraud prevention capabilities - Use of technology

REFERENCE BOOKS:

1. Richard E. Cascarino, Corporate Fraud and Internal Control Workbook: A Framework for Prevention, Wiley, Dec 2012
2. Michael R. Young, Financial Fraud Prevention and Detection: Governance and Effective Practices, Wiley, Oct 2013
3. Zabihollah Rezaee, Richard Riley, Financial Statement Fraud: Prevention and Detection, Wiley, 2nd edition, 2009

4. Managing the risk of fraud and misconduct by Richard H Girgenti, and Timothy P Hedley, first edition, Mc Graw Hill Education Publication, 09 Mar 2011
5. Detecting Accounting Fraud: Analysis and Ethics by Cecil W Jackson, 1st Edition, Pearson Education Publication, 26 Jan 2014
6. Anatomy of a fraud investigation by Stephen Peddeault, 1st Edition, John Wiley & Sons Publication, 2010
7. Telecom and Network Security: Toll Fraud and Telabuse update by Jan Wilson, 2nd Edition, Telecommunications reports International Publication, 22 April 2010



Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

Director i/c,
Center for Cyber Forensics & Information Security
University of Madras
Chennai 600 005

PAPER VIII

CREDITS: 5

CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT

Unit 1: Risk Assessment and Management

Supply Chain Risk Management -- Business Impact Analysis (BIA) -- Security Governance and Compliance -- Threat Intelligence and Information Sharing -- Resilience Planning

Unit 2: Cybersecurity for Critical Infrastructure

Securing Industrial IoT (IIoT) Devices -- Zero Trust Architecture -- Threat Hunting and Incident Detection -- Cryptographic Control -- Cybersecurity Training and Awareness

Unit 3: Physical Security Measures

Perimeter Security Technologies -- Security Guards and Personnel Training -- Emergency Response Planning -- Security Through Environmental Design (CPTED) -- Biometric Access Control Systems

Unit 4: Incident Response and Business Continuity Planning

Crisis Communication Strategies -- Cloud-Based Disaster Recovery Solutions -- Cross-Sector Collaboration -- Post-Incident Analysis and Lessons Learned -- Regulatory Reporting and Compliance

Unit 5: Regulatory Compliance and Legal Considerations

Data Privacy and Protection Laws -- Critical Infrastructure Protection (CIP) Standards -- International Standards and Frameworks -- Litigation and Legal Liability -- Ethical and Legal Considerations in Incident Response

References:

1. A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance by Julia Graham, David Kaye and Philip Jan Rothstein, Illustrated edition, Rothstein Associates Publication, 31 Jan2006
2. Allen, B., Loyear, R. (2016). The Manager's Guide to Enterprise Security Risk
3. Management: Essentials of Risk-Based Security. United States: Rothstein Publishing.
4. Anson, S. (2020). Applied Incident Response. United Kingdom: Wiley.