

Integral University, Lucknow
Department of Computer Application
STUDY & EVALUATION SCHEME

Choice Based Credit System

Post Graduate Diploma in Cyber Security and Law (PGDCSL)

w.e.f Session 2019-20

Total Credits = 30

Year Ist, Semester Ist

S. No.	Course Category	Subject Code	Name of the Subject	Periods				Evaluation Scheme				Subject Total
								Sessional (CA)			End Sem Exam	
				L	T	P	C	UE	TA	Total	ESE	
1.	Core	CAE401	Fundamentals of Computer Security and Cryptography	3	1	0	4	40	20	60	40	100
2.	Core	CAE402	Intellectual Property Rights	3	1	0	4	40	20	60	40	100
3.	Core	CAE403	Fundamentals of Web Designing and Application Security	3	1	0	4	40	20	60	40	100
4.	Core	CAE404	Web Application and Security Lab	0	0	3	3	40	20	60	40	100
Total				9	3	3	15					400

L- Lecture **T-** Tutorial **P-** Practical **C-** Credit **UE-** Unit Exam **TA-** Teacher Assessment

Sessional Total (CA) = Unit Exam + Teacher Assessment

Subject Total = Sessional Total (CA) + End Semester Examination (ESE)

CAE401 FUNDAMENTALS OF COMPUTER SECURITY & CRYPTOGRAPHY

w.e.f Session 2019-20

PREREQUISITE: NONE

COREQUISITE: NONE

L T P

3 1 0

UNIT-I

Computer Security: Computer Security Concepts, OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Network Security Model

Introduction to Cryptography: Plain Text and Cipher Text, Substitution Ciphers and Transposition Ciphers, Cryptanalysis, Steganography, Rotor Machines, Stream and Block Ciphers

[8]

UNIT-II

Modern Block Ciphers: Block Ciphers Principles, Data Encryption Standard (DES), Strength of DES, Idea of Differential Cryptanalysis, Block Cipher Design Principles, Triple DES, DES Security, Block Cipher Modes of Operations

Advanced Encryption Standard (AES): Origin, Structure, Round Functions, AES Key Expansion, AES Implementation

[8]

UNIT-III

Asymmetric Key Cryptography: Introduction to Asymmetric Key Cryptography, RSA Algorithm, Rabin Cryptosystem, Elgamal Cryptosystem, Elliptic Curve Cryptosystems

Key Management and Distribution: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Public Key Distribution, X.509 Certificates, Public Key Infrastructure

[8]

UNIT-IV

Message Authentication Codes: Message Authentication Requirements, Authentication Functions, Authentication Codes, Security of MACs, MACs Based on Hash Functions: HMAC, MACs Based on Block Ciphers: DAA and CMAC, Secure Hash Algorithm (SHA), Kerberos

Digital Signatures: Comparison, Process and Services, RSA Digital Signature Scheme, Elgamal Digital Signature Scheme, Digital Signature Standard (DSS), Applications of Digital Signature

[8]

UNIT-V

Transport-Level Security: Web Security Issues, Secure Sockets Layer (SSL), Transport Layer Security (TLS), HTTPS, Secure Shell (SSH)

IP Security: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange, Cryptographic Suites

Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME

[8]

References:

1. Charles P. Pfleeger “Security in computing”, Pearson Education
2. William Stallings, “Cryptography and Network Security: Principals and Practice”, Pearson Education.
3. Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw Hill
4. AtulKahate, “Cryptography and Network Security”, Tata McGraw Hill

CA 452 INTELLECTUAL PROPERTY RIGHTS (IPR)

w.e.f Session 2019-20

PREREQUISITE: NONE

COREQUISITE: NONE

L T P
3 1 0

UNIT-I

Introduction to Intellectual Property Law, Evolutionary past of IPR, IPR Tool Kit, Legal Tasks in Intellectual Property Law- Ethical obligations in Legal Tasks in Intellectual Property Law, Innovations and Inventions Trade related Intellectual Property Right

[8]

UNIT-II

Introduction to Trade mark Registration Process, Post registration Procedures, Trade mark Maintenance, Transfer of Rights, Inter Parties Proceedings, Infringement, Dilution, Ownership of Trade Mark, Like hood of confusion, Trademarks claims, Trademarks Litigations, International Trade mark Law

[8]

UNIT-III

Introduction to Copyrights: Principles of Copyright, Subjects Matter of Copyright, Rights Afforded by Copyright Law, Copy right Ownership, Transfer and duration, Right to prepare Derivative works, Rights of Distribution, Rights to Perform the work, Publicity Copyright, Formalities and Registrations, Limitations, Copyright disputes and International Copyright Law, Semiconductor Chip Protection Act

[8]

UNIT-IV

Law of Patents: Patent searches, Patent ownership and transfer, Patent Infringement, International Patent Law
Geographical Indications: Overview of Geographical Indications, Importance of Geographical Indication Protection
Introduction to Industrial Designs, Industrial designs protection

[8]

UNIT-V

Plant Variety Protection: Meaning and Benefit, Sharing and Farmers' Rights.
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.

[8]

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
5. J Martin and C Turner: "Intellectual Property" CRC Press
6. Richard Stmm :Intellctual Property Cengage Learning"

CAE403 FUNDAMENTALS OF WEB DESIGNING AND APPLICATION SECURITY

w.e.f. Session 2019-2020

PREREQUISITE: NONE

COREQUISITE: CAE404

**L T P
3 1 0**

UNIT- I

Web Development: Introduction and Web Development Strategies, History of Web and Internet, Protocols governing Web, Writing Web Projects, Connecting to Internet, Introduction to Internet services and tools, Introduction to client-server computing.

[8]

UNIT -II

Web Designing: HTML: List, Table, Images, Frames, Forms, CSS, Document Type Definition, XML: DTD, XML Schemes, Object Models, Presenting and using XML, Using XML Processors: DOM and SAX, Dynamic HTML.

[8]

UNIT- III

Scripting: Java script: Introduction, Documents, Forms, Statements, Functions, Objects; Introduction to AJAX, VB Script, Introduction to Java Beans, Advantage, Properties, BDK, Introduction to EJB, Java Beans API, Introduction to Server Site Programming.

PHP (Hypertext Pre-processor) : Introduction, Syntax, Variables, Strings, Operators, If-Else, Loop, Switch, Array, Function, Form, Mail, File Upload, Session, Error, Exception, Filter, PHP-ODBC.

[8]

UNIT- IV

Web Security Fundamentals: Security, Threats and OWASP Principles, Introduction to Secure Design, typical Attack Models (MITM, MITB) and Other Attacks (DOS, ARP Cache Poisoning, DNS Cache Poisoning etc.), Secure Authentication, Session Management, and Access Control, Avoiding Malicious Input Control, Secure Error Handling and Logging, Data Protection, Communication Security, HTTP Security, Malicious Controls, Business Logic Security.

[8]

UNIT- V

Web Application Security Vulnerabilities: Cross Site Scripting (XSS), SQL Injection (SQi) , Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS), Path Disclosure, Arbitrary Code Execution, Memory Corruption, Cross-Site Request Forgery.

Mitigate Vulnerabilities: Web Application Firewall (WAF), WAF - Protection against Application Layer Attacks, DDoS Mitigation, DNS Amplification DDoS, DNS Security, Bot Filtering.

[8]

References:

1. Ramesh Bangia, "Internet and Web Design" , New Age International
2. Ivan Bayross," HTML, DHTML, Java Script, Perl & CGI", BPB Publication
3. Deitel, "Java for programmers", Pearson Education
4. Joel Sklar , "Principal of web Design" Vikash and Thomas Learning5.
- 5.Merkov, Breithaupt, "Information Security", Pearson Education.

CAE404 WEB APPLICATION AND SECURITY LAB

w.e.f. Session 2019-20

PREREQUISITE: NONE

COREQUISITE: CAE403

L T P
0 0 3

1. Design a web page to display your CV.
2. Design a HTML page using links, list, and table tag etc.
3. Design a HTML form for user registration.
4. Write a JavaScript to prompt for username and display a welcome message and username.
5. Write a code in XML for creating DTD, which specifies set of rules.
6. Create style sheets in CSS/XSL and display the document in Browser.
7. Basic programs based on PHP.
8. Basic programs based on AJAX.
9. Develop a web portal using HTML, CSS & Java Script.
10. Study of different types of Vulnerabilities for hacking a website.
11. Analyze the security Vulnerabilities Email/E-commerce service.

Integral University, Lucknow
Department of Computer Application
STUDY & EVALUATION SCHEME

Choice Based Credit System

Post Graduate Diploma in Cyber Security and Law (PGDCSL)

Year Ist, Semester IInd

S. No.	Course Category	Subject Code	Name of the Subject	Periods				Evaluation Scheme				Subject Total
								Sessional (CA)			End Sem Exam	
				L	T	P	C	UE	TA	Total	ESE	
1.	Core	CAE405	National - International Cyber Law and GDPR	3	1	0	4	40	20	60	40	100
2.	Core	CAE406	Cyber Crime Investigations and Digital Forensic	3	1	0	4	40	20	60	40	100
3.	Elective-1			3	1	0	4	40	20	60	40	100
4.	Core	CAE409	Project Lab	0	0	3	3	40	20	60	40	100
Total				9	3	3	15					400

L- Lecture **T-** Tutorial **P-** Practical **C-** Credit **UE-** Unit Exam **TA-** Teacher Assessment

Sessional Total (CA) = Unit Exam + Teacher Assessment

Subject Total = Sessional Total (CA) + End Semester Examination (ESE)

Elective-1

CAE407 SCADA and Mobile Eco System Security*

CAE408 Cyber Security in Education

*GDPR General Data Protection Regulation
 SCADA Supervisory Control and Data Acquisition

CAE405 National - International Cyber Law and GDPR

w.e.f. Session 2019-20

PREREQUISITE: NONE

COREQUISITE: NONE

L T P
3 1 0

UNIT-I

Basic of Computer and Cyber Security

History of Computers, Areas of Application, Introduction to Operating System, Basics of Networks and Internet, Types of Network, Definition of Cyber Security, Search Engines, E –mails and WWW, Cryptography, Digital Signatures and Electronic Signatures, Electronic Payment System and Taxation, Computer & Cyber Security, Email Security: Web Authentication, SSL and SET, Database Security, E – Commerce & M – Commerce System Security, Advance Computers, Network & Mobile Security Techniques.

[8]

UNIT-II

Information Technology Law

Evolution of the IT Act, Genesis and Necessity, Salient features of the IT Act, 2000, Various Authorities under IT Act and their Powers: Penalties & Offences, Amendments, Impact on other related Acts (Amendments): Amendments to Indian Penal Code, Amendments to Indian Evidence Act, Amendments to Bankers Book Evidence Act, and Amendments to Reserve Bank of India Act.

[8]

UNIT-III

Cyber Space Jurisdiction

Jurisdiction Issues under IT Act, 2000, Traditional Principals of Jurisdiction, Extra-terrestrial Jurisdiction, and Case Laws on Cyber Space Jurisdiction.

E – Commerce and Laws in India

Digital / Electronic Signature in Indian Laws, E – Commerce: Issues and Provisions in Indian Law, E – Governance: Concept and Practicality in India, E – Taxation Issues in Cyberspace, E – Contracts and its Validity in India, Cyber Tribunal & Appellate Tribunal and Cyber Regulations.

[8]

UNIT-IV

Intellectual Property Rights, Domain Names and Trademark Disputes

Concept of Trademarks / in Internet Era, Cyber Squatting, Reverse Hijacking, Jurisdiction in Trademark Disputes, Copyright in the Digital Medium, Copyright in Computer Programmes, Copyright and WIPO Treaties, Concept of Patent Right, and Relevant Provisions of Patent Act 1970.

Sensitive Personal Data or Information (SPDI) in Cyber Law, Cloud Computing & Law and Cyber Law: International Perspective, EDI: Concept and legal Issues, UNCITRAL Model Law, Electronic Signature Law's of Major Countries, Cryptography Laws, Cyber Law's of Major Countries, and EU Convention on Cyber Crime.

[8]

UNIT-V

General Data Protection Regulation (GDPR)

General principles and Basic Concepts of the GDPR, Key Actors under the GDPR and their Role, Rights of Data Subjects, Obligations of Data Controllers and Processors and Law Compliance Measures, Enforcement and Compliance Mechanisms and Liabilities and Sanctions.

[8]

REFERENCES:

1. Guide to Cyber and E – Commerce Laws by P.M. Bukshi and R.K. Suri; Bharat LawHouse, New Delhi.
2. Guide to Cyber Laws by Rodney D. Ryder; Wadhwa and Company, Nagpur.
3. Computer Forensics: Principals and Practices by Linda Volonino, Reynaldo Anzalduaand Jana Godwin; Pearson Prentice – Hall 2007.
4. The Regulation of Cyberspace by Andrew Murray, 2006; Rutledge – Cavendish.
5. Security and Incident Response by Keith J. Jones, Richard Bejtloich and Curtis W.Rose.
6. GDPR: How To Achieve and Maintain Compliance by Mark Foulsham, Brian Hitchen, Andrew Denley, Routledge 2019.
7. GDPR: Guiding Your Business To Compliance: A practical guide to meeting GDPR regulations. (Edition 2), byMark Foulsham, Brian Hitchen, Independently published, 2017.

CAE406 Cyber Crime Investigations and Digital Forensic

w.e.f. Session 2019-20

PREREQUISITE: NONE

COREQUISITE: NONE

L T P
3 1 0

UNIT-I

Cyber Forensic and Computer Crimes, Crimes Targeting Computers: Definition of Cyber Crime & Computer Related Crimes, Classification & Differentiation between Traditional Crimes.

Cyber Crimes: Data Theft, Hacking ,Spreading Virus & Worms, Phishing, Cyber Stalking/Bullying, Identity Theft & Impersonation, Credit Card & Online Banking Frauds, Obscenity, Pornography & Child Pornography, Cyber Defamation, Defacement, Illegal Online Selling & Gambling, Denial of Service Attacks, Cyber Terrorism, Software Piracy & Illegal Downloading.

[8]

UNIT-II

Reasons for Cyber Crimes, Cyber Criminal Mode and Manner of Committing Cyber Crime, Prevention of Cyber Crimes & Frauds Critical Analysis & Loop Holes of The IT Act-2000 and IT Act Amendments, Cyber Crimes: Freedom of Speech in Cyber Space & Human Right Issues.

[8]

UNIT-III

Investigation of Cyber Crimes, Investigation of Malicious Applications, Agencies for Investigation in India: their Powers and Constitution as per Indian Laws, Procedures followed by First Responders, Search and Seizure Procedures of Digital Evidence, Securing the Scene, Documenting the Scene, Evidence Collection and Transportation: Data Acquisition, Data Analysis, and Reporting.

[8]

UNIT-IV

Digital Forensics: Computer Forensics, Mobile Forensics, Forensic Tools, Anti-Forensics.

Network Forensic: Collecting and Analyzing Network-Based Evidence, Reconstructing Web Browsing, Email Activity, and Windows Registry Changes, Intrusion Detection, Tracking Offenders, etc.

Mobile Network Forensic: Introduction, Mobile Network Technology, Investigations, Collecting Evidence, Where to seek Digital Data for Further Investigations, Interpretation of Digital Evidence on Mobile Network.

[8]

UNIT-V

Electronic/Digital Evidence laws & case Laws ,International Organizations and Their Roles: ICANN , URDP , WTO and TRIPS , Interpol & Europol , Impact of Cyber warfare on Privacy Identity , Net Neutrality and EU Electronic communication Regulatory framework , WCAG ,Social Networking sites and Human Right, Case Laws : Indian & International Cases.

[8]

Books:

- 1.Cyber Law & Cyber Crimes By Advocate Prashant Mali; Snow White Publications, Mumbai
- 2.Cyber Law in India by Farooq Ahmad; Pioneer Books
- 3.The Information technology Act, 2000; Bare Act- Professional Book Publishers, New Delhi.
- 4.Computer Forensics: Principles and Practices by Linda Volonino, Reynaldo Anzaldua and Jana Godwin; Pearson Prentice-Hall 2007.
- 5.First Responder's Guide to Computer Forensics by Richard Nolan et al; Carnegie Mellon, 2005
- 6.Digital Evidence and Computer Crime, 2nd Ed. By Eoghan Casey; Academic Press, 2004.

CAE407 SCADA AND MOBILE ECO SYSTEM SECURITY

w.e.f. Session 2019-20

PREREQUISITE: NONE

COREQUISITE: NONE

L T P
3 1 0

UNIT-I

Introduction and Overview

SCADA: Introduction, SCADA Architecture, Different Communication Protocols, Common System Components, Supervision and Control, HMI, RTU and Supervisory Stations, Trends in SCADA, Security Issues.

DCS: Introduction, DCS Architecture, Local Control (LCU) architecture, LCU languages, LCU - Process interfacing issues, communication facilities, configuration of DCS, displays, redundancy concept - case studies in DCS.

[8]

UNIT-II

Real Time Systems

Real time systems- Real time specifications and design techniques- Real time kernels- Inter task communication and synchronization- Real time memory management- Supervisory control- direct digital control- Distributed control- PC based automation. SCADA Architecture: Various SCADA architectures, advantages and disadvantages of each system - Single Unified Standard Architecture - IEC 61850 SCADA Communication: various Industrial Communication Technologies - Wired and Wireless methods and Fiber Optics, Open standard Communication Protocols.

[8]

UNIT-III

Introduction to Industrial Networks

SCADA networks - Remote Terminal Unit (RTU), Intelligent Electronic Devices (IED) - Communication Network, SCADA Server, SCADA/HMI Systems - single unified standard architecture -IEC 61850 - SCADA Communication: various industrial communication technologies -wired and wireless methods and fiber optics, open standard communication protocols, SCADA Applications: Utility applications- Transmission and Distribution sector -operations, monitoring, analysis and improvement. Industries - Oil, Gas and Water. Case Studies, Implementation, Simulation Exercises.

[8]

UNIT-IV

Mobile Ecosystem Technology

Mobile Devices - Features and Security Concerns, Enterprise Mobility Program, File Synchronization and Sharing, Cellular Network – baseband processor and SIM card, GSM encryption and authentication and other attacks. Mobile Platform and Operating System Security Model: Android Software Stack, APK: Android Application Package, APK Internals, Android Application Components, Introduction to Rooted Android Devices,

Android Security Model: IOS Security Model, Windows Mobile Security, BlackBerry Security, Java Mobile Edition Security, Symbian OS Security, Web OS Security.

[8]

UNIT-V

Enterprise Security on the Mobile OS

Device Security Options, Secure Local Storage, Security Policy Enforcement, Need of Cryptography and its applications in Mobile Ecosystem, Secure Crypto Algorithms(Confidentiality, Integrity, Authenticity), Application and implementation of symmetric encryption algorithms, asymmetric encryption algorithms, Hashing Algorithm and MAC Algorithms (HMAC), Full Disk Encryption, E-mail Encryption and File Encryption, Application Sandboxing, Signing, and Permissions, Buffer Overflow Protection, Security of Mobile VoIP Communications, Emerging Trends in Mobile Security.

[8]

REFERENCES:

1. Stuart A. Boyer: SCADA-Supervisory Control and Data Acquisition, Instrument Society of America Publications,USA,2004.
2. Gordon Clarke, Deon Reynders: Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, Newnes Publications, Oxford, UK,2004.
3. William T. Shaw, Cybersecurity for SCADA systems, PennWell Books, 2006.
4. David Bailey, Edwin Wright, Practical SCADA for industry, Newnes, 2003.
5. Michael Wiebe, A guide to utility automation: AMR, SCADA, and IT systems for electric power, PennWell 1999.
6. Mobile Application Security, Himanshu Dviwedi, Chris Clark and David Thiel, 1st Edition. Security of Mobile Communications, Nouredine Boudriga, 2009.

CAE408 CYBER SECURITY IN EDUCATION

w.e.f Session 2019-20

PREREQUISITE: NONE

COREQUISITE: NONE

L T P
3 1 0

UNIT-I

Cyber Security Fundamentals and Cyberoffenses: Introduction, Cybercrime and Information Security, Classification of Cybercrimes, Cybercrime Perspectives, Cyber-Attacks, Social Engineering, Cyberstalking, Botnets, Attack Vector, Cybercrime and Cloud Computing.

Cybercrimes on Mobile and Wireless Devices: Trends in Mobility, Credit Card Frauds, Authentication Service Security, Attacks on Mobile Phones, Security Implications

[8]

UNIT-II

Tools and Methods: Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers, Spywares, Virus, Worms, Trojan Horses and Backdoors, Phishing and Identity Theft, DoS and DDoS Attacks, SQL Injection

Phishing and Identity Theft: Phishing Methods and Techniques, Spear Phishing, Phishing Scam Types, Personal Identifiable Information (PII), Types of ID Theft, Identification Theft Techniques

[8]

UNIT-III

Legal Perspective for Cybercrimes: Needs for Cyber laws, Indian IT Act, Challenges, Digital Signatures and Indian IT Act, Amendments to Indian IT Act, Web Threats for Organizations, Social Computing and associated Challenges for Organizations, Cybercrime and Punishment

Security Policies: Why Policies should be developed, WWW Policies, Email Security Policies, Policy Review Process-Corporate policies, Sample Security Policies, Publishing and Notification Requirement of the Policies

[8]

UNIT-IV

Computer Forensics: Background, Need for Forensics, Digital Evidence, Digital Forensics Life Cycle, Network Forensics, Computer Forensics Investigation, Computer Forensics and Steganography, OSI Model relevance to Forensics, Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing

[8]

UNIT-V

Organizational Implications: Introduction, Cost of Cybercrimes and IPR Issues, Security and Privacy Implications, Computer Usage Policy, Incident Handling, Forensics Best Practices

Social, Ethical and Psychological Dimensions: Intellectual Property in Cyberspace, Ethical Dimension, Hackers and Cybercriminals, Cybercriminals Sociology, Information Warfare

[8]

References:

1. Nina Godbole, SunitBelapure, "Cyber Security", Wiley India.
2. James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", CRC Press, Taylor & Francis Group
3. Dr. K. K. Goyal, AmitGarg, "Cyber Security", University Science Press.
4. Chander, Harish, "Cyber Laws and IT Protection", PHI Learning Private Limited, Delhi, India

CAE409 PROJECT LAB

w.e.f Session 2019-20

PREREQUISITE: NONE

COREQUISITE: NONE

L T P
0 0 3

Students are required to build a project as per schedule. The final evaluation will be based on the application developed. Students will be required to submit their original work in the form of hard & soft copies as well as make presentations for their examination.