



**Centurion**  
**UNIVERSITY**

*Shaping Lives...  
Empowering Communities...*

## M.Sc Cyber Security & Cyber Forensics

### SEMESTER1

SubjectCode	SubjectName	L	T	P	C
	Fundamentals of Computers and Operating Systems	3	0	2	4
	Introduction to Cyber & Network Security Management	3	0	2	4
	Computer Networks	3	0	2	4
	Fundamentals of Digital Forensics	3	0	2	4
	Data Security and Cryptography	3	0	2	4
	Introduction to Programming	3	0	2	4
<b>Total Hours/Credit</b>					<b>24</b>

### SEMESTER2

SubjectCode	SubjectName	L	T	P	C
	Introduction to Servers	3	0	2	4
	Security Auditing, Risk and Compliance (ISO 27001, GDPR, HIPPA, PCIDSS etc)	3	0	2	4
	Advanced Digital Forensic Analysis	3	0	2	4
	Network Security and Forensic Analysis	3	0	2	4
	Cyber Law and Intellectual Property Right	3	0	2	4
<b>Total Hours/Credit</b>					<b>20</b>

**SEMESTER3**

<b>SubjectCode</b>	<b>SubjectName</b>	<b>L</b>	<b>T</b>	<b>P</b>	<b>C</b>
	ReverseEngineeringandMalwareanalysis	<b>3</b>	<b>0</b>	<b>2</b>	<b>4</b>
	MachineLearningandArtificialIntelligence	<b>3</b>	<b>0</b>	<b>2</b>	<b>4</b>
	Introduction to Python Programming	<b>3</b>	<b>0</b>	<b>2</b>	<b>4</b>
	MiniProject(Phase1)				<b>12</b>
<b>TotalHours/Credit</b>					<b>24</b>

**SEMESTER4**

<b>SubjectCode</b>	<b>SubjectName</b>	<b>L</b>	<b>T</b>	<b>P</b>	<b>C</b>
	Project/Internship				<b>18</b>
<b>TotalHours/Credit</b>					<b>18</b>

**SEMESTER1****Duration:6months****Fundamentsofcomputersystemsand operatingsystems**

<b>Unit No</b>	<b>CourseContent</b>
01	FundamentalsofComputerHardware&Software,SystemArchitecture,IntroductiontoCloud, CloudComputing, Client servermodel.
02	OverviewofLinuxoperatingsystem,LinuxFlavors(DebianandRPM),LinuxInstallation and Package Management, GNU and Unix Commands, Devices, LinuxFilesystems,FilesystemHierarchyStandard,CapacityPlanning,LinuxKernel,Linux architecture,LinuxandUnixFirewall,Iptable,UFW
03	SystemStartup,FilesystemandDevices,AdvancedStorageDeviceAdministration, SystemMaintenance,
04	NetworkConfiguration,DomainNameServer,WebServices,FileSharing,NetworkClient Management, Email Services and SystemSecurity
05	FundamentalsofOperatingsystem,basicsofmemorymanagementandprocessmanagement. Interrupts, RPC, Deadlock, semaphore, fundamentals of file managementetc

## ReferenceBook

1. JosephD.DumasII,ComputerArchitecture:FundamentalsandPrinciplesofcomputerdesign,C RC Press
2. AndrewSTanenbum,ModernOperatingSystems,Prentice-Hallof IndiaPvt.Ltd
3. RichardPetersen,Linux:TheCompleteReference,SixthEdition,McgrawHill

## Introduction to Cyber and Network Security Management

Unit No	Course Content
01	Introduction to Cybercrime and Cyber World, CyberSpace Darkweb, Tor, Deep Web, Network security Architecture, IDS, IPS, Firewall, DMZ, Types of Firewall, UTM, etc.
02	Building Cybersecurity environment Understanding Security Threats, Safe Work Station, Secure the Data, Working Remotely Windows - Workgroups and local accounts, active directory, trusts and group policy, Linux Security- Dangerous services, file system permissions, ownership and system tools, Kali Linux- Overview to the tools, updating software & OS, architecture of the system.
03	Website vulnerability and penetration testing using Kali Linux tools, and windows tools, manual and automated VAPT
04	Web, server, application vulnerability and penetration testing
05	Network and wireless VAPT and report writing and countermeasures, Scada system and data diode

### Reference book

1. Nina Godbole, Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives, Willy's India
2. Applied Network Security Monitoring: Collection, Detection, and Analysis – @Chris Sanders, @Jason Smith

## Computer Networks

UnitNo	CourseContent
01	Introduction to Networks
02	Media Access and Internet Working
03	Routing, Networks and Connecting Networks
04	CCNA V.3 Additions

### Reference Book

1. James F. Kurose, Keith W. Ross, "Computer Networking – A Top-Down Approach Featuring the Internet", Fifth Edition, Pearson Education, 2009.
2. Nader F. Mir, "Computer and Communication Networks", Pearson Prentice Hall Publishers, 2010.
3. Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, "Computer Networks: An Open Source Approach", McGraw Hill Publisher, 2011.
4. Behrouz A. Forouzan, "Data Communication and Networking", Fourth Edition, Tata McGraw – Hill, 2011.

## Fundamental of Digital Forensics

UnitNo	CourseContent
01	Introduction to Digital Forensics, Goals of Digital forensics, e-discovery, Chain of custody, Forensics Investigation Techniques and process, Cyber Crime incident Response, Types of Evidence, Preparing for Forensic analysis, Data Acquisition Process, Volatile Data, Cyber-attack case study and forensics, nature of cybercrime, nature of digital evidence, Digital crime scene management and incident response, crime scene recording (video, photography and sketching)
02	Determining Lab Requirements, Key Components of a Forensics Lab, Forensics Tools: Open source and Commercial Tools
03	Techniques of Evidence Collection, Switched Off System, Live System, The Memory Carving Process, probative value of evidence
04	Encryption Types, Hash Algorithm, File Signatures, Digital Signatures Verification
05	Introduction to Network Forensics, Network Configuration, Common Protocols, Network Devices, Log Analysis, Capturing Traffic Flow with Common Tools, Wireshark GUI and CLI, File Extraction with Network Miner, CAP Files Analysis, Package Structure and Analysis, Internet Traffic Analyze, Network Forensics Investigation Process, Audit process and Report Writing, CDR, IPDR, Tower dump analysis

## Information Security and Cryptography

Unit No.	Course Contents
1	Cryptographic System, Classification of Cryptographic System, Secret Key, Cryptography, Substitution-Permutation Network, Feistel structure, Block Ciphers: DES, Double DES, AES, Stream Ciphers: LFSR, RC4. Modes of Operation: ECB, CBC, CFB, CTR, OFB.
2	Introduction to cryptocurrency. Block chain technologies, overview of blockchain process and methodologies, Transactions, Fork, Blockchain limitation and misconceptions
3	Public Key Cryptography, Operation of Public Key Cryptography, RSA, Discrete Logarithm Problems, Diffie-Hellman, ElGamal, DSA. PKI, Concept of Security Model, CPA.
4	Data Integrity, Hash Functions: MD5, SHA, Message Authentication Codes.
5	Emerging Application: Kerberos, Email Security, SSL/TLS, Web Security, Access Controls, Malwares, Firewalls, and Intruders.

### Reference Book

1. Introduction to Cryptography with Coding Theory -- Washington & Trappe [Pearson].
2. Introduction to Modern Cryptography -- Katz & Lindell, [CRC press].
3. Cryptography and Network Security -- W. Stallings, [Prentice Hall].

## Introduction to programming

UnitNo	CourseContent
01	Introduction to programming language, different types of programming language, machine language and assembly language, introduction to C, C++ language
02	Fundamentals of web programming, HTML, XML, Javascript, CSS, jQuery etc
03	Fundamentals of PHP and SQL, WordPress, building a webpage and hosting a website, phpMyAdmin, CMS
04	Introduction to DBMS and SQL DDL, DML, DCL, TCL
05	Introduction to Shell scripting, writing a script, shell commands, decision making, arithmetic operation, loop, wildcards, conditional execution and executing a shell script in Linux environment.

**SEMESTER2****Duration:6months****IntroductiontoServer**

<b>UnitNo</b>	<b>CourseContent</b>
01	InstallandConfigureServers,ConfigureServerRoleandFeatures,ConfigureHyper-V,DeployandConfigureCoreNetworkServices,InstallandAdministerActiveDirectory,CreateandManage GroupPolicy
02	Deploy,Manage,andMaintainServers,ConfigureFileandPrintServices,ConfigureNetworkServicesandAccess,ConfigureandManageActiveDirectory,Configureand ManageGroupPolicy
03	ConfigureandManageHighAvailability,ConfigureFileandStorageSolutions,ImplementBusinessContinuityandDisasterManagement
04	ConfigureNetworkServices,ConfiguretheActiveDirectoryInfrastructure,Configure IdentityandAccessSolutions
05	IntroductiontoRAIDserverandCloudServerManagementand application

## Security Auditing and Compliance (ISO 27001, GDPR, HIPPA, PCIDSS etc)

Unit No	Course Content
01	IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards. Risk assessment concepts and tools & techniques used in planning, examination, reporting and follow-up.
02	Fundamentals of business processes: Purchasing, Payroll, Accounts payable, accounts receivable, Role of IS in these processes. Control Principles related to controls in information systems.
03	Risk-based audit planning and audit project management techniques, including follow-up. Applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits.
04	Evidence Collection Techniques: Observation, Inquiry, Inspection, Interview, Data Analysis, Forensic Investigation Techniques, Computer-assisted audit techniques [CAATs] used to gather, protect and preserve audit evidence.
05	Sampling methodologies and substantive/data analytical procedures. Reporting and Communication techniques: Facilitation, Negotiation, Conflict Resolution, Audit report structure, issue writing, management summary, result verification. Audit Quality assurance (QA) systems and frameworks. Various types of audits: Internal, External, Financial, and methods for assessing and placing reliance on the work of other auditors and control entities.
06	Introduction to information auditing standards, ISO 27000, ISO 27001 implementation, GDPR, HIPPA, PCIDSS, process of auditing in information systems, information security program development and incident management, Risk management and compliance, Introduction to Data privacy bill India PDPA

## Advanced Digital Forensics Analysis

UnitNo	CourseContent
01	RAID -Levels and Duplicating, Hard Disk Structure, Boot Sequence Types, FAT File System Types, NTFS Internals, HDD vs SSD,
02	Browsers and Internet Forensics, Windows Registry, Log Analysis Techniques, Open Source Tools, Recovering Deleted Files, Start-up Files, File system Times Analysis, Event Log Analysis, Windows Registry Analysis, Internet Forensics
03	Anti-Forensics Techniques, Hash Functions, File Signatures and Check, PE Analysis, Image Analysis, Steganography, Password Cracking, Hash Functions, File Signatures and Check, PE Analysis, Image Analysis, Steganography, Password Cracking, Network Traffic Capture, Writing Professional Report, Anti forensic techniques
04	Live response, Using netcat to minimize contamination, Collecting volatile data: Date and time, Network interfaces, Funny networks, Promiscuous mode?, Network connections, Open ports, Programs associated with ports, Running processes, Open files, Routing tables, Mounted file systems, Loaded kernel modules
05	Volatile Memory analysis: Making the decision to dump RAM, Using fmem, Using LiME, Using /proc/kcore, Acquiring file system images, Analyzing file system images
06	Leveraging The Sleuth Kit (TSK) and Autopsy, Timeline Analysis, Digging deeper into Linux file systems, Linux file forensics, Memory Volatility, Reversing Linux Malware, Writing the Reports: Autopsy, Dradis, OpenOffice
07	Mobile forensic techniques, Android mobile file system, Forensic copy of mobile device, Logical and Physical analysis, IoS analysis, APFS

## Network Security and Forensics Analysis

UnitNo	CourseContent
01	Configuring Your Target Machines and Setup of Your Lab Environment, The Absolute Beginner's Guide to Penetration Testing, Metasploit Basics, Intelligence Gathering, Vulnerability Scanning, The Joy of Exploitation, Meterpreter, Avoiding Detection, Exploitation Using Client-side Attacks
02	Metasploit Auxiliary Modules, The Social-Engineer Toolkit, Fast-Track, Building Your Own Module, Creating Your Own Exploits, Porting Exploits to the Metasploit Framework, Meterpreter Scripting, Simulated Penetration Test, Information Gathering
03	Wireless network forensics, event log aggregation, correlation and analysis, switches, routers, web proxies, honeypots analysis, TOR, Darkweb, VPN analysis, File Transferring (Tools & Payloads), Privilege Escalation, Backdoors, Data Transmit, Anti-Forensic
04	Introduction to IOT devices, IOT network log analysis, IOT forensics
05	Introduction to Logs, Log Analysis Theory, Defining Log Data, System Audit Policies, Network Activity Logging, Log Sources, Log Analysis Process, Log Analysis Tools, Lab: System Log Files, Network, Log Correlation, Log Manipulation

## CyberLawandIntellectualPropertyRight

UnitNo	CourseContent
01	IntroductiontoInformationtechnology&CyberLaw,BasicsofE-commerceandComputerFraudTechniquesCyberSecurityFundaments,TechniquesandCore Principles,ITRule2011
02	CyberSpace,Technology&Issues,RegulatingCyberSpace:International,National, E-contract & Electronic Data Interchange, Cyber security policy 2013,StakeHoldersofCyberSecurity(NPCA,CERT,NTRO,DefenseCERT, Protectiontocritical Industries.
03	E-signatureandE-governancelegalityunder I.T.Act,2000 CyberContraventions,Compensation&CrimesunderI.T.Act,2000ISP sand WebsitesLegalLiabilityunder I.T.Act,2000 CorporateLegalLiability,AdjudicationProcessForRecoveryofLossesunderI.T.Act,2000
04	IPR&CyberSpace,TaxationIssuesinCyberSpace,ITActanditsrelationwithIncomeTax Law, ITActanditsrelationwithIndianPenalCode,CaseStudiesand CaseLaws
05	Relevantsectionof other ActssuchasIPC,CrPC,Indian EvidenceACTetc.Blockingwebsites,telephonetapping,packetsniffing,Darkwebmonitoring,social mediamonitoring

**SEMESTER3****Duration:6months****ReverseEngineeringandMalwareanalysis**

<b>UnitNo</b>	<b>CourseContent</b>
01	FundamentalsofReverseEngineering,X86Architecture,Stack,Heap,Memory Registers,Bufferoverflow,StaticandDynamicCodeanalysis,GDB
02	Settingup aProtected MalwareAnalysis Environment,
03	BehavioralAnalysisof WindowsMalware,SandboxingWindowsMalware
04	StaticAnalysisMaliciousCodeAnalysis:depthMalwareAnalysis,RecognizingPacke dMalware,MalwareUnpackingApproaches&Tools.ManualUnpacking usingOllyDbg,
05	DynamicMalwareAnalysis:MaliciousCodeAnalysis:In- ProcessDumpingTools&Imports RebuildingUtilities, DLL Analysis,WindowsInternals,MaliciousWebsites Analysis, Browser script DE obfuscation using Debuggers , JS AnalysisComplications,Self-DefendingMalware,MaliciousDocuments&Memory Forensics

## MachinelearningandArtificialIntelligence

UnitNo	CourseContent
01	Introductiontomachinelearning,Decisiontree,,supervisedlearning,unsupervised learning,neuralnetworks,
02	Applicationofmachinelearningincybersecurityandcyberforensics,machine learningalgorithmsandapplications
03	Dataanalysisusingmachinelearningforforensicexpert,socialmediaandmachine learning,malwareanalysisusingML, HIDS,NIPSbasedanalysis

## Introductiontopythonprogrammingforforensic

UnitNo	CourseContent
01	IntroductiontoPythonProgramming, OOPconcepts, Installingpython,pycharm Settingupenvironment
02	Writingpythonprogram, Variables,datatype,libraries,functions,classobjects, list,tuples,strings,methods,inheritance
03	NetworkTrafficanalysisusingPython UsingPyGeoIPtoCorrelateIPtoPhysicalLocations,UsingDpkttoParsePackets,Using PythontoBuildaGoogleMap,IsAnonymousReallyAnonymous?Analyzing LOIC Traffic, Using Dpkt to Find the LOIC Download, Parsing IRCCommandstotheHive,IdentifyingtheDDoSAttackinProgress,UsingScapyto ParseDNS,TCP SequencePrediction
04	Python forNetwork Forensics Analysis of Wireless Access Points in the Registry, Using WinReg to Read theWindowsRegistry,UsingMechanizetoSubmittheMACAddresstoWigle,UsingPy thontoRecoverDeletedItemsintheRecycleBin,UsingtheOSModuletoFindDeletedItems,UsingPyPDFtoParsePDFMetadata,UnderstandingExifMetadata,DownloadingI mageswithBeautifulSoup,Investigating ApplicationArtifacts with Python, Understanding the Skype Sqlite3 Database, Using PythonandSqlite3 to AutomateSkypeDatabaseQueries

### MiniProjectphase1

**SEMESTER4**

**Duration:6months**

**ProjectinternshipPhase2**

## Electivesubjects

### DatabaseManagementSystem

UnitNo	CourseContent
01	IntroductionandapplicationsofDBMS,Purposeofdatabase,Data,Independence, Database System architecture-levels, Structure of relationaldatabases, Domains, Relations, Relational algebra – fundamental operatorsand syntax, Entity-Relationship model : Basic concepts, Design process,Overview of Query Processing & Query Optimization, TransactionManagement,Security:Introduction,Discretionaryaccesscontrol, MandatoryAccess Control, Data Encryption
02	SQL Concepts : Basics of SQL, DDL,DML,DCL, structure–creation,alteration,definingconstraints– Primarykey,foreignkey,unique,notnull,check,INoperator, Functions - aggregate functions, Built-in functions –numeric, date, stringfunctions, set operations, sub-queries, correlated sub-queries, Use of groupby, having, order by, join and its types, Exist, Any, All , view and its types.transactioncontrol commands – Commit, Rollback,Savepoint
03	<b>Practicals</b>

#### Unit–3Practical

1. Design aDatabase and createrequiredtables. Fore.g.Bank,CollegeDatabase,
2. Applythe constraintslikePrimaryKey,Foreignkey,NOTNULLtothetables.,
3. Writeasql statementforimplementingALTER,UPDATE andDELETE
4. Writethequeries toimplement thejoins
5. Write the query for implementing the following functions:MAX(),MIN(),AVG(),COUNT()
6. Writethe queryto implementthe conceptofIntegrityconstrains
7. Writethe queryto create theviews
8. Performthequeriesfortriggers
9. Performthefollowingoperationfordemonstratingtheinsertion,updatationanddeletionusingt he referential integrityconstraints
10. Writethe queryfor creatingtheusers and theirrole.

Communication device Forensics Analysis

**Communications skills**

Unit No	Course Content
01	<p><b>Concepts of Communications:</b>            Definition, Forms of Communication, Objectives of Communication, Characteristics of Communication, Process of Communication, Communication, Roadblocks, Role of Verbal and Non-verbal Symbols in Communication, Barriers to Effective Communication, Overcoming Communication Barriers.</p>
02	<p><b>Nonverbal communication:</b>            Body Language, Gestures, Postures, Facial Expressions, Dress codes; the Cross Cultural Dimensions of Business Communication; Listening and Speaking, techniques of eliciting response, probing questions, Observation. Business and social etiquettes; Listening Skills: Definition, Anatomy of poor Listening, Features of a good Listener, Role Play, Group Discussion and Interviews, Meetings: Ways and Means of conducting meetings effectively, Mock Meetings and Interviews.</p>
03	<p><b>Reading, Writing and listening Ability:</b>            The reading process, purpose, different kinds of texts, reference material, scientific and technical texts, active and passive reading, strategies- vocabulary skills, eye reading and visual perception, prediction techniques, scanning skills, distinguishing facts and opinions, drawing inferences and conclusions, comprehension of technical material - scientific and technical texts, instructions and technical manuals, graphic information. Forms of Communication in Written mode: Basics Body language of Business Letters and Memos, Tone of writing, enquiries, orders and replying to them, sales letters, Job applications and resume, E-mail: How to make smart e-mail, Writing Business Reports and Proposals, Practice for Writing. Hearing and Listening, Types of Listening, barriers to Effective Listening, traits of a good Listener</p>

## Audio, Video Technology Forensic Analysis

UnitNo	CourseContent
01	<p>Physics Of Sound: Waves And Sound, AnalysisAndSynthesis OfComplex Waves, Human And Non-Human Utterances, Anatomy OfVocal Tract, Speech And Noise Characteristics, Audio ClarificationPrinciples, Difference Between Language And Speech, Collection OfVoice Sample, Various Approaches In Forensic Speaker Identification,InstrumentalAnalysisOfSpeechSample,InterpretationOfResult,Speech Recognition And Speaker Identification, Voice Authentication,Tools And Software Used In Audio Analysis, Noise Reduction</p> <p>Tools,AuthenticityOfAudioEvidenceInCourtroom,BasicsofVoIPtechnology.</p>
02	<p>Introductiontovideotechnology,differentvideoformats,videorecordingdevices,LegalconceptsregardingDigitalMulti-MediaEvidence,Scientificmethodologyofforensicvideoanalysis:Bestpracticesofcollection,recovery,enhancement,analysisandinterpretationofvideoevidence,Authenticationofvideoasanevidence,basics of CCTV and DVR, best practices of CCTV evidence retrievaland storage at scene of crime and laboratory, challenges and precautionatthesceneofcrime,evidencehandlingprocedure,legal issues.</p>
03	<p>Collecting voice samplefor analysis,Analysisof voice sample forauthentication, Speaker identification from sample, Video recording ofcrime scene,Videoanalysisandauthentication,Analysisof CCTVrecordings,Metadataanalysis of Audio/ Video file</p>