MASTER OF SCIENCE IN CYBER SECURITY AND DIGITALFORENSICS

SEMESTER1

SubjectCode	SubjectName	L	T	P	C
	FundamentalsofComputersandOperatingSystems	3	0	2	4
	IntroductiontoCyber&Network SecurityManagement	3	0	2	4
	ComputerNetworks	3	0	2	4
	FundamentalofDigitalForensic	3	0	2	4
	DataSecurityand Cryptography	3	0	2	4
	IntroductiontoProgramming	3	0	2	4
TotalHours/Credit					24

SEMESTER2

SubjectCode	SubjectName	L	T	P	C
	IntroductiontoServers	3	0	2	4
	Security Auditing, Risk andCompliance(ISO27001,GDPR, HIPPA,PCIDSSetc)	3	0	2	4
	Advanced Digital Forensic Analysis	3	0	2	4
	NetworksecurityandForensic Analysis	3	0	2	4
	Cyber Law and Intellectual PropertyRight	3	0	2	4
TotalHours/Credit					20

SEMESTER3

SubjectCode	SubjectName	L	T	P	C
	ReverseEngineeringandMalwareanalysis	**3**	**0**	**2**	**4**
	MachineLearningandArtificial Intelligence	**3**	**0**	**2**	**4**
	Introduction to Python Programming	**3**	**0**	**2**	**4**
	MiniProject(Phase1)				**12**
TotalHours/Credit					**24**

SEMESTER4

SubjectCode	SubjectName	L	T	P	C
	Project/Internship				**18**
TotalHours/Credit					**18**

SEMESTER1 **Duration:6months**

Fundamentsofcomputersystemsand operatingsystems

Unit No	**CourseContent**
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,CRC Press
2. AndrewSTanenbum,ModernOperatingSystems,Prentice-Hallof IndiaPvt.Ltd
3. RichardPetersen,Linux:TheCompleteReference,SixthEdition,McgrawHill

IntroductiontoCyberandNetworkSecurityManagement

UnitNo	CourseContent
01	IntroductiontoCybercrimeandCyberWorld,CyberSpaceDarkweb,Tor,DeepWeb, Network security Architecture, IDS, IPS, Firewall, DMZ, Types ofFirewall,UTM, etc.
02	BuildingCybersecurityenvironment Understanding Security Threats, Safe Work Station, Secure the Data, WorkingRemotely Windows - Workgroups and local accounts, active directory, trusts andgrouppolicy,LinuxSecurity-Dangerousservices,filesystempermissions,ownershipandsystemtools,Kali Linux-Overviewtothetools,updatingsoftware &OS,architectureofthesystem.
03	WebsitevulnerabilityandpenetrationtestingusingKalilinuxtools,andwindows tools,manualandautomatedVAPT
04	Web,server,applicationvulnerabilityandpenetration testing
05	NetworkandwirelessVAPTandreportwritingandcountermeasures,Scadasystemandd ata diode

Referencebook

1. NinaGodbole,SunitBelapure,CyberSecurity:UnderstandingCyberCrimes,ComputerForens icsAndLegal Perspectives,Willy'sIndia
2. AppliedNetworkSecurityMonitoring:Collection,Detection,andAnalysis– @ChrisSanders,@Jason Smith

ComputerNetworks

UnitNo	CourseContent
01	IntroductiontoNetworks
02	MediaAccessand InternetWorking
03	Routing,Networks andConnectingNetworks
04	CCNAV.3 Additions

ReferenceBook

1. JamesF.Kurose,KeithW.Ross,“ComputerNetworking–ATop-DownApproachFeaturingthe Internet”, Fifth Edition, Pearson Education, 2009.
2. Nader.F.Mir,“ComputerandCommunicationNetworks”,PearsonPrenticeHallPublishers,2010.
3. Ying-DarLin,Ren-HungHwang,FredBaker,“ComputerNetworks:AnOpenSourceApproach”,McGrawHill Publisher, 2011.
4. BehrouzA.Forouzan,“DatacommunicationandNetworking”,FourthEdition,TataMcGraw – Hill,2011.

FundamentalofDigitalForensics

UnitNo	CourseContent
01	Introduction to Digital Forensics, Goals of Digital forensics, e-discovery, Chain ofcustody, Forensics Investigation Techniques and process, Cyber Crime incidentResponse, Types of Evidence, Preparing for Forensic analysis, Data AcquisitionProcess,VolatileData,Cyber-attackcasestudyandforensics,natureofcybercrime,natureofdigitalevidence,Digitalcrimescenemanagementandincidentresponse, crimesceneрecording(video, photographyandsketching)
02	DeterminingLabRequirements,KeyComponentsofaForensicsLab,ForensicsTools: Open sourceandCommercial Tools
03	TechniquesofEvidenceCollection,SwitchedOffSystem,LiveSystem,The, MemoryCarvingProcess, probativevalueof evidence
04	EncryptionTypes,HashAlgorithm,FileSignatures,DigitalSignaturesVerification
05	Introduction to Network Forensics, Network Configuration, Common Protocols,NetworkDevices,LogAnalysis,CapturingTrafficFlowwithCommonTools, WiresharkGUIandCLI,FileExtractionwithNetworkMiner,CAPFilesAnalysis ,PackageStructureandAnalysis,InternetTrafficAnalyze,NetworkForensicsInvestigationProcess,AuditprocessandReportWriting,CDR, IPDR,Towerdump analysis

InformationSecurityandCryptography

Unit No.	CourseContents
1	CryptographicSystem,Classificationof Cryptographic System, Secret Key, Cryptography ,Substitution-PermutationNetwork,Feistelstructure,Block Ciphers:DES,DoubleDES,AES,StreamCiphers:LFSR,RC4.Modesof Operation:ECB,CBC,CFB,CTR,OFB.
2	Introductiontocryptocurrency. Block chaintechnologies,overviewofblockchainprocess andmethodologies,Transactions,Fork,Blockchainlimitationandmisconceptions
3	PublicKeyCryptography,OperationofPublicKeyCryptography,RSA, DiscreteLogarithmProblems,Diffie-Hellman,ElGamal,DSA.PKI,Conceptof SecurityModel, CPA.
4	DataIntegrity,Hash Functions:MD5,SHA,MessageAuthenticationCodes.
5	EmergingApplication:Kerberos,EmailSecurity, SSL/TLS,WebSecurity, AccessControls,Malwares,Firewalls,and Intruders.

ReferenceBook

1. IntroductiontoCryptographywithCodingTheory --Washington&Trappe[Pearson].
2. IntroductiontoModern Cryptography--Katz &Lindell,[CRCpress].
3. Cryptographyand Network Security--W. Stallings, [PrenticeHall].

Introductiontoprogramming

UnitNo	CourseContent
01	Introductiontoprogramminglanguage,differenttypeofprogramminglanguage, machinelanguageandassemblylanguage,introductiontoC,C++language
02	Fundamentalof webprogramming,HTML,XML,Javascript,css,jqueryetc
03	fundamentalsofphpandSQL,wordpress, buildingawebpageandhostinga website,phpmyadmin,CMS
04	IntroductiontoDBMS andSQLDDL,DML,DCL,TCL
05	IntroductiontoShellscripting,writinga script,shellcommands,decisionmaking,arithmeticoperation,loop,wildcards,conditionalexecutionandexecutingashell scriptinlinux environment.

SEMESTER2 **Duration:6months**

IntroductiontoServer

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

SecurityAuditing andCompliance(ISO27001,GDPR, HIPPA,PCIDSSetc)

Unit No	CourseContent
01	ITAuditandAssuranceStandards,GuidelinesandToolsandTechniques,CodeofProfessionalEthicsandotherapplicablestandards.Riskassessmentconceptsandtools &techniques used in planning,examination, reportingandfollow-up.
02	Fundamentalsofbusinessprocesses:Purchasing,Payroll,Accountspayable,accountsreceivable,RoleofISintheseprocesses.ControlPrinciplesrelatedtocontrolsin informationsystems.
03	Risk-basedauditplanningandauditprojectmanagementtechniques,includingfollow-up.Applicablelawsandregulationsthataffectthescope,evidencecollectionandpreservation,and frequencyof audits.
04	EvidenceCollectionTechniques:Observation,Inquiry,Inspection,Interview,Data Analysis,ForensicInvestigationTechniques,Computer-assistedaudittechniques[CAATs] used to gather,protect and preserveauditevidence.
05	Sampling methodologies and substantive/data analytical procedures. Reporting andCommunicationtechniques:Facilitation,Negotiation,ConflictResolution,Auditreportstructure,issuewriting,managementsummary,resultverification.AuditQualityassurance(QA)systemsandframeworks.Varioustypesofaudits:Internal, External, Financial, and methods for assessing and placing reliance on the work ofotherauditors and control entities.
06	Introduction to information auditing standards, ISO 27000, ISO 27001implementation,GDPR,HIPPA,PCIDSS,processofauditinginformationsystems, information security program development and incident management, Riskmanagementandcompliance,Introduction toDataprivacybillIndiaPDPA

AdvancedDigitalForensicsAnalysis

UnitNo	CourseContent
01	RAID -LevelsandDuplicating, HardDiskStructure, BootSequenceTypes ,FATFileSystem Types, NTFSInternals, HHDvs SSD,
02	Browsers and Internet Forensics, Windows Registry, Log Analysis Techniques,Open Source Tools, Recovering Deleted Files, Start-up Files, File system TimesAnalysis,Event LogAnalysis,WindowsRegistryAnalysis, InternetForensics
03	Anti-ForensicsTechniques,HashFunctions,FileSignaturesandCheck,PEAnalysis, Image Analysis, Steganography, Password Cracking , Hash Functions,FileSignaturesandCheck,PEAnalysis,ImageAnalysis,Steganography,PasswordCracking , Network Traffic Capture, Writing Professional Report, Anti forensicstechniques
04	Live response, Using netcat to minimize contamination, Collecting volatile data:Dateandtime,Networkinterfaces,Funnynetworks,Promiscuousmode?,Network connections,Openports,Programsassociatedwithports,Runningprocesses,Open files,Routingtables,Mountedfilesystems,Loadedkernelmodules
05	VolatileMemoryanalysis:MakingthedecisiontodumpRAM,Usingfmem,UsingLiME, Using /proc/kcore, Acquiring file system images, Analyzing file systemimages
06	LeveragingTheSleuthKit(TSK)andAutopsy,TimelineAnalysis,Diggingdeeper into Linux file systems, Linux file forensics , Memory Volatility, Reversing LinuxMalware,WritingtheReports: Autopsy, Dradis,OpenOffice
07	Mobileforensicstechniques,Android mobile file system,Forensiccopyof mobile device,LogicalandPhysicalanalysis,IoSanalysis,APFS

Network SecurityandForensicsAnalysis

UnitNo	CourseContent
01	Configuring Your Target Machines and Setup of Your Lab Environment, TheAbsoluteB,BasicsofPenetrationTesting,MetasploitBasics,IntelligenceGathering,VulnerabilityScanning,TheJoyofExploitation,Meterpreter,AvoidingDetection,ExploitationUsingClient-side Attacks
02	Metasploit Auxiliary Modules, The Social-Engineer Toolkit, Fast-Track, BuildingYourOwnModule,CreatingYourOwnExploits,PortingExploitstotheMetasploitFramework,MeterpreterScripting,SimulatedPenetrationTest,InformationGathering
03	Wirelessnetworkforensic,eventlogaggregation,correlationandanalysis,swiches,routers,webproxies,honepotsanalysis,TOR,Darkweb,VPNanalysis,FileTransferring (Tools & Payloads), Privilege Escalation, Backdoors, Data Transmit,AntiForensic
04	Introductionto IOTdevices, IOTnetworkloganalysis,IOTforensics
05	Introduction to Logs, Log Analysis Theory, Defining Log Data, System AuditPolices, Network Activity Logging,Log Sources,Log AnalysisProcess,LogAnalysisTools,Lab:SystemLogFiles,Network,LogCorrelation,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

UnitNo	**CourseContent**
01	FundamentalsofReverseEngineering,X86Architecture,Stack,Heap,Memory Registers,Bufferoverflow,StaticandDynamicCodeanalysis,GDB
02	Settingup aProtected MalwareAnalysis Environment,
03	BehavioralAnalysisof WindowsMalware,SandboxingWindowsMalware
04	StaticAnalysisMaliciousCodeAnalysis:depthMalwareAnalysis,RecognizingPackedMalware,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	Writingapythonprogram,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,UsingtheOSModuletoFindDeletedIte ms,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	**Practicals**

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,updationanddeletionusingthe referential integrityconstraints
10. Writethe queryfor creatingtheusers and theirrole.

CommunicationdeviceForensicsAnalysis

Communicationskills

UnitNo	CourseContent
01	**ConceptsofCommunications:** Definition,FormsofCommunication,ObjectivesofCommunication,CharacteristicsofCommunication,ProcessofCommunication,Communication, Roadblocks, Role of Verbal and Non-verbal Symbols inCommunication,BarrierstoEffectiveCommunication,Overcoming CommunicationBarriers.
02	**Nonverbalcommunication:** Body Language, Gestures, Postures, Facial Expressions, Dress codes; theCrossCulturalDimensionsofBusinessCommunication;ListeningandSpeaking, techniques of electing response, probing questions, Observation.Business and social etiquettes; Listening Skills: Definition, Anatomy ofpoor Listening, Features of a good Listener, Role Play, Group DiscussionandInterviews,Meetings:WaysandMeansofconductingmeetingseffectively,Mock Meetings andInterviews.
03	**Reading,Writing andlisting Ability:** The reading process, purpose, different kinds of texts, reference material,scientificandtechnicaltexts,activeandpassivereading,strategies-vocabulary skills, eye reading and visual perception, prediction techniques,scanning skills, distinguishing facts and opinions, drawing inferences andconclusions, comprehension of technical material - scientific and technicaltexts, instructions and technical manuals, graphic information. Forms ofCommunicationinWrittenmode:BasicsBodylanguageofBusinessLettersand Memos, Tone of writing, enquiries, orders and replying to them, salesletters, Job applications and resume, E-mail: How to make smart e-mail,WritingBusinessReportsandProposals,PracticeforWriting.HearingandListening,TypesofListening,barrierstoEffectiveListening,treatofagoodListening

Audio,VideoTechnologyForensicAnalysis

UnitNo	CourseContent
01	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 Tools,AuthenticityOfAudioEvidenceInCourtroom,BasicsofVoIPtechnology.
02	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.
03	Collecting voice samplefor analysis,Analysisof voice sample forauthentication, Speaker identification from sample, Video recording ofcrime scene,Videoanalysisandauthentication,Analysisof CCTVrecordings,Metadataanalysis of Audio/ Video file