FACULTY OF COMPUTER SCIENCE & IT

SYLLABUS

of

Master of Science (Information and Network Security)
(Semester - I & II)

(Under Continuous Evaluation System)

Session: 2019-20

The Heritage Institution

KANYA MAHA VIDYALAYA
JALANDHAR
(Autonomous)

PROGRAMME SPECIFIC OUTCOMES

Master of Science (Information and Network Security)

Students of this Post Graduation will be able to:

PSO1: Highlight the need of security architecture and its relevance to system, services, continuity and reliability.

PSO2: Understand the trade offs for functionality usability and security and to differentiate between controls to protect system availability and reliability: controls to protect information.

PSO2: Illustrate the use of standards to enhance security in the development process.

PSO3: Measure the performance of security systems within an enterprise-level information system and to troubleshoot, maintain and update an enterprise-level information security system.

PSO4: Evaluate the computer network and information security needs of an organization and to assess cyber security risk management policies in order to adequately protect an organization's critical information and assets.

PSO5: Prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.

PSO6: Understand the role of forensics, cyber incidents, intrusions and investigations in revealing how an attack was carried out and understand how to support investigation.

PSO7: Implement continuous network monitoring and provide real-time security solutions, formulate, update and communicate short- and long-term organizational cyber security strategies and policies.

Kanya Maha Vidyalaya, Jalandhar (Autonomous)

SCHEME AND CURRICULUMOF EXAMINATIONS OF TWO YEAR DEGREE PROGRAMME

Master of Science (Information and Network Security)

Session 2019-20

Master of Science (Information and Network Security) Semester - I							
COURSE CODE	**COURSE NAME**	**COURSE TYPE**	**Marks**				**Examination Time (in Hours)**
			Total	**Ext.**		**CA**	
				L	**P**		
MINL-1111	Computer Networks	C	100	80	-	20	3
MINL-1112	Network Protocols	C	100	80	-	20	3
MINL-1113	Network Operating System	C	100	80	-	20	3
MINL-1114	Information Security & Threats	C	100	80	-	20	3
MINL-1115	Java Programming	C	100	80	-	20	3
MINP-1116	Lab on NOS & Java Programming	C	100	-	80	20	3
		Total	600				

Note:

C - Compulsory

Kanya Maha Vidyalaya, Jalandhar (Autonomous)

SCHEME AND CURRICULUMOF EXAMINATIONS OF TWO YEAR DEGREE PROGRAMME

Master of Science (Information and Network Security)

Session 2019-20

Master of Science (Information and Network Security) Semester - II							
COURSE CODE	**COURSE NAME**	**COURSE TYPE**	**Marks**				**Examination Time (in Hours)**
			Total	**Ext.**		**CA**	
				L	**P**		
MINL-2111	Network Planning, Analysis & Performance	C	100	80	-	20	3
MINL-2112	Network Security Practices	C	100	80	-	20	3
MINL-2113	Computer Forensic Fundamentals	C	100	80	-	20	3
MINL-2114	Secure Code Development	C	100	80	-	20	3
MINL-2115	Mobile Application Development & Security	C	100	80	-	20	3
MINP-2116	Lab on Network Security Practice & Mobile Application Development & Security	C	100	-	80	20	3
			600				

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)

COMPUTER NETWORKS

COURSE CODE: MINL-1111

Course Outcomes:

CO1: The student will understand the fundamental concepts of computer networking and will be familiarized with the basic taxonomy and terminology of the computer networking area.

CO2: The student will be able to understand the physical and logical as well as the electrical characteristics of digital signals and the basic methods of data transmission.

CO3: To understand the organization of computer networks, factors influencing computer network development and the reasons for having variety of different types of networks.

CO4: To study the basic taxonomy and terminology of the computer networking and enumerate the layers of OSI model and TCP/IP model in order to have a good understanding of various Reference Models and protocols.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)

COMPUTER NETWORKS

COURSE CODE: MINL-1111

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80

CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction: Data Communication, Components, Protocols, Standard Organizations, Applications

Networks Basics & Various Types: Topology, Transmission Mode, Categories of Networks

OSI and TCP/IP Models: OSI Model Layers, Functions of the Layer, TCP/IP Layers and its functions, Comparison of TCP/IP and OSI Models

UNIT – II

Signals, Modulations and Multiplexing: Analog and Digital Signal, Digital to Digital Conversion, Analog to Digital Conversion, Digital to Analog Conversion

Transmission Media: Asynchronous and Synchronous Transmission, Modems, Guided (Twisted pair cable, Coaxial Cable and Optical Fibre) and Unguided Media (Terrestrial Microwave, Satellite and Cellular Telephony, Transmission Disturbance and Performance)

UNIT – III

Detection and Correction of Errors: Error types, Redundancy, Error Detection Methods: VRC, LRC, CRC and Checksum, Error Correction: Single Bit Error Correction, Hamming Code

Data Link Control and Protocols: Line Discipline, Flow Control, Error Control, Asynchronous Protocol, Synchronous Protocol, Character Oriented and Bit Oriented Protocols

UNIT – IV

Quality of Service in Routing & Signalling: Issues, importance, parameters like delay, jitter, end to end service, CoS.

Routing Algorithms: Distance Vector Routing, Link State Routing

Upper OSI Layers: Session Layer, Presentation Layer and Application Layer

References:

1) James F. Kuros and Keith W. Ross Computer Networking: A Top–Down Approach (2002).
2) Computer Networks Protocols, Standards and Interfaces: Uyless Black, PHI, 2006.
3) Data Communication and Networking, White, Cengage Learning, 2008.
4) Behrouz Frozen: Computer Network.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)

COURSE CODE:MINL-1112

NETWORK PROTOCOLS

Course Outcomes:

CO1: To get in depth knowledge about various networking protocols, their working, management and operations.

CO2: To understand the layered approach that makes design, implementation and operation of extensive networks possible.

CO3: Classify the routing protocols and analyze how to assign the IP addresses for the given network.

CO4: To understand the TCP/IP suite of protocols and the networked applications supported by it.

Master of Science (Information and Network Security) Semester – I
(Session 2019-20)

NETWORK PROTOCOLS
COURSE CODE:MINL-1112

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Review of networking Technologies & Internetworking Concepts and Architectural Model: Application level and Network level Interconnection, Properties of the Internet, Internet Architecture, Interconnection through IP Routers

Internet Addresses, Mapping internet addresses to Physical addresses (ARP) & Determining an internet addresses at Startup (RARP): Universal identifiers, three Primary classes of IP addresses, network and Broadcast Addresses, Limited Broadcast, Dotted decimal Notation, weakness in Internet addressing, Loopback addresses.

UNIT - II

Internet Addresses, Mapping internet addresses to Physical addresses (ARP) & Determining an internet addresses at Startup (RARP): Address resolution problem, two types of Physical addresses, resolution through Direct Mapping, Resolution through Dynamic Binding. address Resolution Cache, ARP to other Protocols. Reverse address resolution protocol, timing RARP transaction, Primary and backup RARP severs.

Internet Protocol Connectionless Data Gram Delivery & Internet Protocol: Routing IP Datagrams: The concepts of unreliable delivery, connectionless delivery system, purpose of the internet protocol. the internet datagram.

UNIT - III

Internet Protocol Connectionless Data Gram Delivery & Internet Protocol: Routing in an internet, direct and indirect delivery, table driven IP routing, next Hop Routing, default routes, host specific routes, The IP routing Algorithm, handling incoming datagrams, Establishing routing tables

Internet Protocol: Error and Control Message (ICMP) & Subnet and Supernet Address

Extension: The internet, control message protocols, Error reporting versus error detection. ICMP message format. Detecting and reporting various network problems through ICMP. Transparent Router, Proxy ARP, subset addressing, implementation of subnets with masks representation, Routing in the presence of subsets, a unified algorithm.

UNIT - IV

User Datagram Peotocol (UDP): Format of UDP message UDP pseudo header UDP encapsulation and Protocols layering and the UDP checksum computation. UDP multiplexing, De–multiplexing and Ports.

Reliable Stream Transport service (TCP): The Transmission control Protocol, pots, Connections and Endpoint, passive and active opens the TCP segment format. TCP implementation issues.

References:

1. Douglas E.Comer, Internetworking with TCP/IP: Principles, Protocols.
2. Forouzan, TCP–IP, Protocol Suit, TMH.
3. Comer, Internetworking with TCP–IP, Vol. 3.
4. Unix Network Programming, W. Richard Stevens.
5. SNMP, Stallings, Pearson.
6. TCP–IP Network Administration, Hunt Craig.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)
NETWORK OPERATING SYSTEM
COURSE CODE: MINL-1113

Course Outcomes:

A student will be able to do the following:

CO1: Understand the installation, configuration and administration of Network Operating Systems.

CO2: The student will gain and will improve the capabilities in:
• Installing, configuring and administering network operating system
• Remote administration using network operating systems
• Connecting client computers to the network
• Linux working

CO3: This course aims to provide an understanding of the general security concepts of windows and Linux systems, network security tools and implementation of organizational security.

CO4: To learn the fundamentals and gain knowledge of Operating Systems.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)
NETWORK OPERATING SYSTEM
COURSE CODE: MINL-1113

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction: Introduction to LINUX, Installing LINUX, Partitions, LILO, Installing software packages. Updating with Gnome, Updating with KDE, Command line installing.

File Structure: LINUX files, File structure, File & Directory permission, Operations on a file.

UNIT - II

Window 2003 File System, Active Directory, DHCP, IIS, DNS

Administering Linux: Creating a user A/C, modifying a user A/C, Deleting a user A/C, Checking Disk Quotas, System Initialization, System start–up & shutdown, Installing & managing H/W devices.

UNIT - III

Disk Management: Managing Basic & Dynamic Disks, Disk quotas, Disk Fragmentation, Remote Storage, RAID all levels

Administrating window 2003: User group & Computer Accounts, Creating & Managing Users and Groups

Backup & Disaster Recover: Concepts, Creating Backing Plan, Choosing & Managing Backup Media, Setting backup Options, Scheduling Backup.

UNIT - IV

Backup & Disaster Recover: Jobs, Disaster Recovery Plan, Assessing Threats, Restoring Data using Backup

Case & Comparative Studies: Windows 2003 Server & Linux Server

Troubleshooting : Troubleshooting LINUX in GRUB mode, Windows 2003 Server.

References:

1. Redhat Linux(10) Bible : Christopher Negus, 2003.
2. Linux Unleashed : Tim Parker, 2006.
3. Linux Administration Tools : Charles Fisher, 2007.
4. Window 2003 4 in 1: Dream Tech.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)
INFORMATION SECURITY & THREATS
COURSE CODE: MINL-1114

Course Outcomes:

CO1: To understand the network attacks (denial of service, flooding, sniffing and traffic redirection, inside attacks, etc.) and basic networking defense tools.

CO2: The student will be able to differentiate between organizational security policies and security mechanism and will be able to analyze the security needs of a small enterprise, design a strategic plan to address those security requirements and select the appropriate tools to implement the organizational policies.

CO3: To be able to explain various Information security threat and controls for it.

CO4: The student will be able to explain the mechanism to protect confidentiality and completeness of data.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)
INFORMATION SECURITY & THREATS
COURSE CODE: MINL-1114

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Essential terminology, Hardware, Software, Malware, Defining security, Need for security Cyber crime vs Computer based crime, Information Security statistics, Three pillars of Security,

UNIT - II

Security myths, Identity of a Web Site, http vs https, Operating System fingerprinting, Hardening operating system, updates, patches, CAN and CVEs, Host based firewall vs Network based firewall, deploying firewall, sniffing network traffic.

UNIT - III

Recognizing Security Threats and attacks, Phishing and its countermeasures, Virus, Trojan Horse, Worms, Spyware, Adware, Keylogger, Social engineering, Denial of Service, Spamming, Port Scanning, Password cracking, Security measures

UNIT - IV

Creating isolated network presence using virtualization, hosting different operating systems virtually and networking amongst these, Identify website's identity, Finding and understanding CVEs , deploying firewall, Understanding phishing, using NMAP, netcat, using tcpdump and

wireshark, generating digital certificates, understanding CAs.

Recommended Books:

1. Cryptography and Network Security, Atul Kahate, Second Edition, McGraw Hill, 2010.
2. Information Security Principles and Practices, Mark Merkow. Jim Briethaupt, Pearson, 2006.
3. Principles of Information Security, Michael E Whitman, Herbert J Mattord, Cengage Learning, 2010.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)

JAVA PROGRAMMING
COURSE CODE: MINL-1115

Course Outcomes:

CO1: To understand the fundamentals of object-oriented programming in Java, including defining classes, invoking methods, using class libraries, variables, conditional and iterative execution, methods, etc.

CO2: To be aware of the important topics and principles of software development and have the ability to write a computer program to solve specified problems in order to test, document and prepare a professional looking package for each business project.

CO3: To be able to use the Java SDK environment to create, debug and run simple Java programs and to model of object oriented programming: abstract data types, encapsulation, inheritance and polymorphism

CO4: To understand how to take the statement of a business problem and from this determine suitable logic for solving the problem; then be able to proceed to code that logic as a program written in Java.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)

JAVA PROGRAMMING

COURSE CODE: MINL-1115

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80

CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Java Fundamentals: Features, Objects Oriented Basis, Java Virtual Machine, Character Set, Operators, Data Types, Control Structures, Classes, Inheritance, Polymorphism, Packages & Interfaces, Abstract Classes, Stream IO Classes, Exception Handling.

Java I/O: I/O Basics, Streams, reading Console input and writing console output, Print Writer Class, Reading & Writing Files, Byte Streams, Character Streams & Serialization.

UNIT - II

Multithreading: Java Thread model, Thread Priorities, Synchronization, Interthread communication, Suspending, resuming & stopping thread.

Event Handling: The Delegation Event Model, Event Classes, Event Listener Interfaces

UNIT - III

AWT: Window Fundamentals, Working with Frame Windows, Graphics, Color and Fonts.

Swings: Basics of Swing, JButton class, JRadioButton, JTextArea class, JComboBox class JTable class. LayoutManagers BorderLayout, GridLayout, FlowLayout, CardLayout.

UNIT - IV

JDBC: JDBC Drivers, Steps to connect to the database, Connectivity with Oracle, DriverManager, Connection interface, Statement interface, ResultSet interface, PreparedStatement, ResultSetMetaData, DatabaseMetaData.

References

1. The Complete Reference – JAVA 2 by Ptrick Naughton & Herbert Schildt TMH Publications, 2007.

2. The Java Tutorial Continued by Compione, Walrath, Huml SUN JAVA Tutorial Team, Addison Wessley, 2007.

Master of Science (Information and Network Security) Semester – I

(Session 2019-20)

LAB ON NOS & JAVA PROGRAMMING

COURSE CODE: MINP-1116

Examination Time: 3 Hrs **Max. Marks: 100**

Practical: 80

CA:20

Lab on NOS: Installation & Configuration of NOS (Windows 2003, Linux) and their Administration. User account creation, group creation, DHCP settings, Backup & Recovery plan.

Lab on Java Programming

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

NETWORK PLANNING, ANALYSIS AND PERFORMANCE

COURSE CODE: MINL-2111

Course Outcomes:

CO1: To introduce analysis and design of computer and communication network.

CO2: To provide the student with knowledge of network planning and performance principals, including minimum cost and maximum flow methodologies.

CO3: To understand the introduction to planning and designing of a network.

CO4: Students will gain an understanding of the process used to plan network operations and performance characteristics.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

NETWORK PLANNING, ANALYSIS AND PERFORMANCE

COURSE CODE: MINL-2111

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80

CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Requirements, Planning & Choosing Technology: Business requirements, technical requirement user requirements, traffic sizing characteristics time & delay consideration

Traffic Engineering and Capacity Planning: Throughout calculation traffic characteristics & source models.

UNIT - II

Traffic Engineering and Capacity Planning: Traditional traffic engineering, queued data & packet switched traffic modeling, designing for peaks, delay or latency

Network Performance Modeling and Analysis: creating traffic matrix, design tools, components of design tools, types of design projects

UNIT - III

Technology Comparisons: Generic packet switching networks characteristics, private vs. public networking. Business aspects of packet, frame and cell switching services, High speed LAN protocols comparison, Application performance needs, Throughout, burstiness, response time and delay tolerance, selecting service provider, vendor, service levels, etc.

UNIT - IV

Access Network Design: N/W design layers, Access N/W design, access n/w capacity, Backbone n/w design, Backbone segments, backbone capacity, topologies, Tuning the network, securing the network.Design for network security

References:

1. James D McCabe, Network Analysis, Architecture and Design, 2nd Edition,

Morgan Kaufman Series in Networking, 2007.
2. Youeu Zheng, Shakil Akhtar, Network for Computer Scientists and Engineers, Oxford University Press, 2007.
3. Foruzan, Data Communications & Networking, Tata–Megraw Gill 2006.
4. Darren L. Spohn, Co–Authors: Tina L. Brawn and Scott G Rau.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

NETWORK SECURITY PRACTICES
COURSE CODE: MINL-2112

Course Outcomes:

After completing this course, a student will be able to:

CO1: Have a basic knowledge on the fundamentals of cryptography such as symmetric/asymmetric encryption, digital signatures, and hash functions.

CO2: Understand the current network authentication applications, PKI, Web security and their vulnerabilities that are exploited by intentional and unintentional attacks.

CO3: **D**evelop a basic understanding of cryptography, how it has evolved and some key encryption techniques.

CO4: Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

NETWORK SECURITY PRACTICES

COURSE CODE: MINL-2112

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80

CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT – I

Introduction: Overview, Security attacks (Interruption, Interception, Modification and Fabrication) and services (confidentiality, authentication, integrity, non–repudiation, access control and availability), types of attacks, model for network security.

Classical and Modern Cryptography Techniques: Conventional encryption model, classical encryption techniques.

UNIT - II

Classical and Modern Cryptography Techniques: Simplified DES, Principles of Block ciphers, DES and its strength, Triple DES, Blowfish, CAST – 128, linear and differential cryptanalysis, steganography.

Confidentiality: Traffic confidentiality, key distribution, random number generation

UNIT – III

Public Key Encryption Methods: Principles, RSA Algorithm, Key management, Diffie–Hellman key exchange, Elliptic curve cryptography

Authentication: Requirements, functions, Authentication codes, Hash functions

UNIT – IV

Digital Signatures: Basics, Digital signature standard, Authentication Protocols

Other Securities:

IP Security: overview and architecture, Authentication Header; Electronic Mail security: Pretty Good Privacy; Web security: overview.

References:

1. Cryptography and Network Security: Principles and Practice – William Stallings.
2. Introduction to Modern Cryptography by J. Katz and Y. Lindell.
3. Handbook of Applied Cryptography by A. Menezes, P. Van Oorshot, S. Vanstone.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

COMPUTER FORENSIC FUNDAMENTALS

COURSE CODE: MINL-2113

Course Outcomes:

CO1: The student will understand how to Interpret and appropriately apply the laws and procedures associated with identifying, acquiring, examining and presenting digital evidence.

CO2: The student will be able to apply the principles of effective digital forensics investigation techniques.

CO3: To be able to evaluate the effectiveness of available digital forensics tools and use them in a way that optimizes the efficiency and quality of digital forensics investigations.

CO4: To understand the role of digital forensics in the field of information assurance and cyber security and recognize the opportunities to benefit from and support the goals of those fields.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

COMPUTER FORENSIC FUNDAMENTALS

COURSE CODE: MINL-2113

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80

CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT – I

Computer Forensics Fundamentals: Introduction to Computer Forensics, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources, Employment Proceedings ,Computer Forensics Services ,Benefits of Professional Forensics Methodology ,Steps Taken by Computer Forensics Specialists ,Who Can Use Computer Forensic Evidence?

UNIT – II

Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised, Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls, Biometric Security Systems.

UNIT – III

Vendor and Computer Forensics Services: Occurrence of Cyber Crime, Cyber Detectives, Fighting Cyber Crime with Risk–Management Techniques, Computer Forensics Investigative Services, Forensic Process Improvement

Data Recovery: Data Recovery Defined, Data Backup and Recovery, The Role of Backup in Data Recovery, The Data–Recovery Solution, Hiding and Recovering Hidden Data

Evidence Collection and Data Seizure: Why Collect Evidence?, Collection Options, Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure

UNIT - IV

Computer Image Verification and Authentication: Special Needs of Evidential Authentication, Practical Considerations

Networks: Network Forensics Scenario, A Technical Approach, Destruction of Email, Damaging Computer Evidence, Tools Needed for Intrusion Response to the Destruction of Data, System Testing

References:

1. Computer Forensics: Computer Crime Scene Investigation, Second Edition, John R. Vacca.
2. Computer Forensics Evidence Collection and Preservation, EC – Council.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

SECURE CODE DEVELOPMENT

COURSE CODE: MINL-2114

Course Outcomes:

CO1: To have in depth knowledge about various software development techniques including agile and to have a brush up about various modeling techniques used in designing.

CO2: The student will understand about various attacks like buffer overrun, SQL injection and various principals concerning security.

CO3: To understand various securities related techniques and methodologies.

CO4: To learn about how to maintain the Confidentiality, Integrity and Availability of a data via secure coding practices.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

SECURE CODE DEVELOPMENT

COURSE CODE: MINL-2114

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80

CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Principles and Motivations: Software development process models waterfall, rapid prototyping, incremental development, spiral models, Agile Software Development.

UNIT - II

Software Development Methods: Formal, semi–formal and informal methods; Requirements elicitation, requirements specification; Data, function, and event–based modeling;

UNIT - III

The need for Secure Systems, Proactive Security development process: security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, SD3 (Secure by design, default and deployment), Security principles, Threat modelling.

UNIT - IV

Security Techniques, authentication, authorization, Buffer Overrun, Access control, least privilege, Input issues: database, web–specific, internationalization. Security testing, security code review, secure software installation, writing security documentation.

Recommended Books:

1. Writing Secure Code, Michael Howard and David LeBlanc, Microsoft Press, (2006).
2. Software Engineering – Security as A Process in the SDLC, Nithin Haridas, (2007).
3. Pressman, Roger, Software Engineering – A Practitioners Approach, McGraw

Hill (2008) 6th Ed.

4. Sommerville, Ian, Software Engineering, Addison–Wesley Publishing Company, (2006) 8th Ed.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

MOBILE APPLICATION DEVELOPMENT & SECURITY

COURSE CODE: MINL-2115

Course Outcomes:

CO1: To make the student aware about mobile devices, mobile platforms, mobile operating systems and their architecture.

CO2: The student will be able to recognize and setup a mobile device and application runtime environment.

CO3: The students will be exposed to technology and business trends impacting mobile applications in order to make the student competent with the characterization and architecture of mobile applications.

CO4: The student will be competent with designing and developing mobile applications using application development framework.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

MOBILE APPLICATION DEVELOPMENT & SECURITY

COURSE CODE: MINL-2115

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80

CA:20

Instructions for Paper Setter -

Eight questions of equal marks are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT – I

Introduction to Android: Android Introduction, History and Version, Android Architecture, Core Building Blocks, Android Emulator, Install Android, Setup Eclipse, Hello Android example, Internal Details, Dalvik VM, AndroidManifest.xml, R.java, Hide Title Bar, Screen Orientation

UNIT – II

Android Widgets: UI Widgets, Working with Button, Toast, Custom Toast, ToggleButton, CheckBox, Custom CheckBox, RadioButton, Dynamic RadioButton, Custom RadioButton, AlertDialog, Spinner, AutoCompleteTextView, ListView, Custom ListView, RatingBar, WebView, SeekBar, DatePicker, TimePicker, Analog and Digital, ProgressBar, Vertical ScrollView, Horizontal ScrollView

ImageSwitcher, ImageSlider, ViewStub, TabLayout, TabLayout with FrameLayout, searchView, SearchView on Toolbar, EditText with TextWatcher

UNIT – III

Activity and Intents: Activity LifeCycle, Implicit Intent, Explicit Intent, StartActivityForResult, Share App Data

Android Fragments

Android Menu: Option Menu, Context Menu, Popup Menu

UNIT – IV

Managing and Accessing Databases: SQLite.

Mobile Issues and Development Strategies: Issues facing Mobile devices, Securing mobile application development

Android Security: Android Securable IPC Mechanism, Android Security Model, Intents, Activities, Services, Android Security tools.

Recommended Books

1. Allen, Grant, Nikhil Gopal, and Michael Thomas. Beginning Android 4. Apress, 2012.
2. Horton, John. Android Programming for Beginners. Packt Publishing Ltd, 2015.
3. Hardy, Brian, and Bill Phillips. Android Programming: The Big Nerd Ranch Guide. Addison-Wesley Professional, 2013.
4. https://developer.android.com
5. 5. Mobile Application Security, HimanshuDwivedi, Chris Clark, David Thiel, Tata McGraw Hill, 1st Edition, 2010.
6. 6. Hacking Exposed Mobile Security Secrets & Solutions, Neil Bergman, Mike Stanfield, Jason, Rouse , Joel Scambray , SarathGeethakumar , SwapnilDeshmukh, Scott Matsumoto , John Steven , Mike Price, McGraw-Hill Osborne Media,1st Edition ,2013.

Master of Science (Information and Network Security) Semester – II

(Session 2019-20)

LAB ON N/W SECURITY PRACTICE & MOBILE APPLICATION DEVELOPMENT & SECURITY

COURSE CODE: MINP-2116

Examination Time: 3 Hrs

Max. Marks: 100

Practical: 80

CA:20

Lab on N/W Security Practices

Lab on Mobile Application Development & Security