(Annexure A-2)

FACULTY OF COMPUTER SCIENCE & IT

SYLLABUS

of

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

(Under Credit Based Continuous Evaluation Grading System)

Session: 2024-25

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

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

PSO5: Apply skills gained for evaluation and protection of computer networks and security system.

Kanya Maha Vidyalaya, Jalandhar (Autonomous)

SCHEME AND CURRICULUMOF EXAMINATIONS OF TWO YEAR DEGREE PROGRAMME

Master of Science (Information and Network Security)

Credit Based Continuous Evaluation Grading System (CBCEGS)

(Session 2024-25 -- Batch 2024-26)

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

Course Code	Course Title	Course Type	Hours Per Week	Credit		Marks				Examination Time (in Hours)
			L-T-P	L-T-P	Total	Total	Ext.		CA	
							L	P		
MINL-1111	Computer Networks	C	4-0-0	4-0-0	4	100	80	-	20	3
MINL-1112	Network Protocols	C	3-1-0	3-1-0	4	100	80	-	20	3
MINL-1113	Network Operating System	C	4-0-0	4-0-0	4	100	80	-	20	3
MINL-1114	Information Security and Threats	C	4-0-0	4-0-0	4	100	80	-	20	3
MINL-1115	Object Oriented Programming	C	4-0-0	4-0-0	4	100	80	-	20	3
MINP-1116	Lab on NOS and Object Oriented Programming	C	0-0-4	0-0-2	2	50	-	40	10	3
	** Student can opt any one of the following Interdisciplinary courses	IDE			4	100	80	-	20	3
	Total				22	550				

**** List of Interdisciplinary Courses**

Option 1 - Effective Communication Skills (IDEC-1101)

Option 2 – Basics of Music (Vocal) (IDEM-1362)

Option 3 - Human Rights and Constitutional Duties (IDEH-1313)

Option 4 - Indian Heritage: Contribution to the world (IDEW-1275)

Note:

C – Compulsory, IDE-Interdisciplinary Elective Courses

****Grade points of these courses will not be included in the SGPA/CGPA of Semester/ Programme.**

Kanya Maha Vidyalaya, Jalandhar (Autonomous)

SCHEME AND CURRICULUMOF EXAMINATIONS OF TWO YEAR DEGREE PROGRAMME

Master of Science (Information and Network Security)

Credit Based Continuous Evaluation Grading System (CBCEGS)

(Session 2024-25 -- Batch 2024-26)

Master of Science (Information and Network Security) Semester – II										
Course Code	**Course Title**	**Course Type**	**Hours per week**	**Credit**		**Marks**				**Examination Time (in Hours)**
			L-T-P	**L-T-P**	**Total**	**Total**	**Ext.**		**CA**	
							L	**P**		
MINL-2111	Network Planning, Analysis and Performance	C	4-0-0	4-0-0	4	100	80	-	20	3
MINL-2112	Network Security Practices	C	3-1-0	3-1-0	4	100	80	-	20	3
MINL-2113	Computer Forensic Fundamentals	C	4-0-0	4-0-0	4	100	80	-	20	3
MINL-2114	Secure Code Development	C	3-1-0	3-1-0	4	100	80	-	20	3
MINL-2115	Mobile Application Development and Security	C	4-0-0	4-0-0	4	100	80	-	20	3
MINP-2116	Lab on Mobile Application Development and Security	C	0-0-4	0-0-2	2	50	-	40	10	3
	Total				22	550				

Note:

C - Compulsory

Master of Science (Information and Network Security) Semester – I
(Session 2024-25)
COURSE CODE: MINL-1111
COMPUTER NETWORKS

Course Outcomes:

After passing course the student will be able to:

CO1: Comprehend basics of networks and network reference models.

CO2: Comprehend signal conversion and network transmission media.

CO3: Implement error detection and correction techniques on data.

CO4: Identify routing patterns in different routing algorithm and various QoS parameters.

Master of Science (Information and Network Security) Semester – I
(Session 2024-25)
COURSE CODE: MINL-1111
COMPUTER NETWORKS

L-T-P: 4-0-0 **Max. Marks: 100**
Credits: 4
Examination Time: 3 Hours **Theory: 80**
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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 Fiber) 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 &Signaling: 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 / Textbooks:

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 Forouzan, Data Communications and networking, McGraw Hill, 2007.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – I
(Session 2024-25)
COURSE CODE: MINL-1112
NETWORK PROTOCOLS

Course Outcomes:

After passing course the student will be able to:

CO1: Comprehend about various networking protocols, their working, management and operations.

CO2: Comprehend about working of address resolution and datagram protocol.

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

CO4: Identify the working of TCP and UDP at transport layer.

Master of Science (Information and Network Security) Semester – I
(Session 2024-25)
COURSE CODE: MINL - 1112
NETWORK PROTOCOLS

L-T-P: 3-1-0 **Max. Marks: 100**
Credits: 4
Examination Time: 3 Hours **Theory: 80**
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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 Protocol (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 / Textbooks:

1. Douglas E.Comer, Internetworking with TCP/IP, Pearson Prentice Hall, 2006.
2. Behrouz A. Forouzan, TCP/IP Protocol Suite, McGraw Hill Education, 2010.
3. Douglas E. Comer, David L. Stevens, Internetworking with TCP/IP, Vol. III: Client-Server Programming and Applications, Linux/Posix Sockets Version, Pearson, 2000.
4. W. Richard Stevens, Unix Network Programming, PHI, 1998.
5. William Stallings, SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Addison-Wesley, 1999.
6. Craig Hunt, TCP/IP Network Administration, O'Reilly & Associates, 2002.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – I
(Session 2024-25)
COURSE CODE: MINL - 1113
NETWORK OPERATING SYSTEM

Course Outcomes:

After passing course the student will be able to:

CO1: Comprehend installation and file structure of Linux operating system.

CO2: Administer user accounts in Linux.

CO3: Identify disk structure and different RAID levels.

CO4: Comprehend backup, recovery and troubleshooting of network operating system.

Master of Science (Information and Network Security) Semester – I
(Session 2024-25)
COURSE CODE: MINL - 1113
NETWORK OPERATING SYSTEM

L-T-P: 4-0-0 **Max. Marks: 100**
Credits: 4
Examination Time: 3 Hours **Theory: 80**
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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 / Textbooks:

1. Christopher Negus, Red Hat Linux(10) Bible, Wiley, 2003.
2. Tim Parker, Linux Unleashed, Sams, 2006.
3. Charles Fisher, Red Hat Linux Administration Tools, 2007.
4. Kathy Ivens, Windows Server 2003: The Complete Reference, McGraw-Hill, 2003.
5. William R. Stanek, Microsoft Windows Server 2003 Inside Out, Microsoft Press, 2004.

Note: The latest editions of the books should be followed.

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

(Session 2024-25)

COURSE CODE: MINL - 1114

INFORMATION SECURITY AND THREATS

Course Outcomes:

After passing course the student will be able to:

CO1: Comprehend essential terminology of cyber security and its importance.

CO2: Comprehend various security measures for security at web and operating system level.

CO3: Identify various Information security threat and its countermeasures.

CO4: comprehend hosting at different platforms, virtualization, firewall deployment and digital certificates.

Master of Science (Information and Network Security) Semester – I
(Session 2024-25)
COURSE CODE: MINL - 1114
INFORMATION SECURITY AND THREATS

L-T-P: 4-0-0 **Max. Marks: 100**
Credits: 4
Examination Time: 3 Hours **Theory: 80**
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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 Cybercrime 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.

References / Textbooks:

1. Atul Kahate, Cryptography and Network Security, McGraw Hill, 2010.
2. Mark S. Merkow, Jim Breithaupt, Information Security: Principles and Practices, Pearson Prentice Hall, 2006.
3. Michael E Whitman, Herbert J Mattord, Principles of Information Security, Cengage Learning, 2018.
4. Christopher T. Carlson, How to Manage Cybersecurity Risk, Universal-Publishers, 2019.

Note: The latest editions of the books should be followed.

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

(Session 2024-25)
COURSE CODE: MINL-1115
OBJECT ORIENTED PROGRAMMING

Course Outcomes:

After passing course the student will be able to:

CO1: Comprehend fundamentals of Java programming and OOPs concepts.

CO2: Apply event handling and multithreading in Java.

CO3: Work with Graphical User Interface through Swings and AWT.

CO4: Connect Java application with an existing database and access it through JDBC.

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

(Session 2024-25)
COURSE CODE: MINL-1115
OBJECT ORIENTED PROGRAMMING

L-T-P: 4-0-0 **Max. Marks: 100**
Credits: 4
Examination Time: 3 Hours **Theory: 80**
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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, JRadio Button, JTextArea class, JCombo Box class JTable class. Layout Managers Border Layout, Grid Layout, Flow Layout, Card Layout.

UNIT - IV

JDBC: JDBC Drivers, Steps to connect to the database, Connectivity with Oracle, Driver Manager, Connection interface, Statement interface, ResultSet interface, Prepared Statement, ResultSet MetaData, Database MetaData.

References / Textbooks:

1. Patrick Naughton& Herbert Schildt, JAVA 2: The Complete Reference, McGraw-Hill Education, 1999.
2. Mary Campione, Kathy Walrath, Alison Huml, The Java Tutorial Continued: The Rest of the JDK, Addison Wesley, 1998.
3. Bruce Eckel, Thinking in Java, Prentice Hall, 2006.
4. D.T. Editorial Services, Java 8 Programming Black Book, Dreamtech Press, 2015.
5. Cay S. Horstmann, Core Java Vol I & II, Prentice Hall, 2013.

Note: The latest editions of the books should be followed.

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

(Session 2024-25)

COURSE CODE: MINP-1116

LAB ON NOS ANDOBJECT ORIENTED PROGRAMMING

L-T-P: 0-0-2 **Max. Marks: 50**

Credits: 2

Examination Time: 3 Hours **Practical: 40**

CA:10

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 Object Oriented Programming.

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

(Session 2024-25)

COURSE CODE: MINL-2111
NETWORK PLANNING, ANALYSIS AND PERFORMANCE

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend planning requirements for building a network.

CO2: Analyze network performance through design tools, traffic matrix, etc.

CO3: Analyze various network technologies available for data transmission against different parameters such as throughput, delay, response time, etc.

CO4: Comprehend and tune various network design.

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

(Session 2024-25)
COURSE CODE: MINL-2111
NETWORK PLANNING, ANALYSIS AND PERFORMANCE

L-T-P: 4-0-0 **Max. Marks: 100**
Credits: 4
Examination Time: 3 Hours **Theory: 80**
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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 / Textbooks:

1. Piet Van Mieghem, Performance Analysis of Complex Networks and Systems, Cambridge University Press (2014), 2nd Edition.
2. James D McCabe, Network Analysis, Architecture and Design, Morgan Kaufman Series in Networking (2007), 2nd Edition.
3. Youeu Zheng, Shakil Akhtar, Network for Computer Scientists and Engineers, Oxford University Press (2007)
4. Foruzan, Data Communications & Networking, Tata–McGraw Hill (2006).
5. Darren L. Spohn, Co–Authors: Tina L. Brawn and Scott G Rau.

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

(Session 2024-25)
COURSE CODE: MINL-2112
NETWORK SECURITY PRACTICES

Course Outcomes:

After passing this course the student will be able to:

CO1: Demonstrate various security attacks like Interruption, Interception, Modification, integrity, non–repudiation, etc.

CO2: Analyze the performance of various Classical and Modern Cryptography Techniques.

CO3: Comprehend authentication and different public key cryptography mechanism.

CO4: Comprehend various security protocols implemented at application level.

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

(Session 2024-25)
COURSE CODE: MINL-2112
NETWORK SECURITY PRACTICES

L-T-P: 3-1-0 **Max. Marks: 100**
Credits: 4
Examination Time: 3 Hours **Theory: 80**
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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 (AH) and Encryption Security Payload (ESP); Electronic Mail security: Pretty Good Privacy (PGP); Web security: overview.

References / Textbooks:

1. Forouzan, Cryptography and Network Security, McGraw Hill Education (2015).
2. William Stallings and Lawrie Brown, Computer Security: Principles and Practice, Pearson Education (2019), 4th Edition
3. Richard Bejtlich, The Practice of Network Security Monitoring, No Starch Press (2013), 1st Edition
4. Atul Kahate, Network Security Practices, McGraw Hill Education (2019), 4th Edition

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

(Session 2024-25)
COURSE CODE: MINL-2113
COMPUTER FORENSIC FUNDAMENTALS

Course Outcomes:
After passing this course the student will be able to:
CO1: Comprehend the role of digital forensics and techniques used by attackers to trigger cyberattacks.
CO2: Apply various principles of effective digital forensics investigation techniques.
CO3: Identify housing, hardware and software requirements for Computer Forensics and sampling of forensic software.
CO4: Comprehend processing of evidence and report preparation.

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

(Session 2024-25)

COURSE CODE: MINL-2113

COMPUTER FORENSIC FUNDAMENTALS

L-T-P: 4-0-0 **Max. Marks: 100**

Credits: 4

Examination Time: 3 Hours **Theory: 80**

CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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, Cyberspace and Criminal Behavior, Traditional Problems Associated with Computer Crime.

Web-Based Criminal Activity, Malware: Viruses and Worms, DoS and DDoS Attacks, Botnets and Zombie Armies, Spam, Ransomware. Theft of Information, Data Manipulation, and Web Encroachment.

UNIT- II

Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources, Employment Proceedings.
Computer Forensics: Traditional Problems in Computer Investigations, Disk Structure and Digital Evidence, Developing Computer Forensic Science Capabilities.

UNIT- III

Requirements: Housing, Hardware and software requirements.
Sampling of Forensic Software. Searching and Seizing Computer-Related Evidence, Pre-search Activities, On-scene Activities.

UNIT- IV

Processing of Evidence and Report Preparation: Aspects of Data Analysis, Smart Phones and GPS Forensics, Smart Phones and GPS Forensics.
Report Preparation and Final Documentation.

References / Textbooks:

1. Britz, Computer Forensics and Cyber Crime: An Introduction, Pearson Education India (2011), 2nd Edition
2. Jason Luttgens and Matthew Pepe, Incident Response and Computer Forensics, McGraw-Hill Education (2014), 3rd Edition
3. Akash Kamal Mishra, Computer Crime Investigation and Computer Forensics, Notion Press (2020), 1st Edition
4. Christopher Steuart, Bill Nelson, Guide to Computer Forensics and Investigations, Cengage (2013), 4th Edition
5. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications (2015), 1st Edition

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

(Session 2024-25)

COURSE CODE: MINL-2114

SECURE CODE DEVELOPMENT

Course Outcomes:

After passing this course the student will be able to:

CO1: Identify and evaluate various process model used for development of software.

CO2: Comprehend the incorporation of security requirements at different phases of secure system development.

CO3: Comprehend various securities related techniques and methodologies.

CO4: Apply security testing, secure code review and installation along with preparation of security document.

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

(Session 2024-25)

COURSE CODE: MINL-2114

SECURE CODE DEVELOPMENT

L-T-P: 3-1-0 **Max. Marks: 100**

Credits: 4

Examination Time: 3 Hours **Theory: 80**

CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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, RAD model, prototyping, incremental development, spiral models, Agile Software Development.

Software Development Methods: Formal and informal methods; Requirement selicitation, requirements specification; Data, function, and event–based modeling;

UNIT – II

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

UNIT III

Security Techniques, authentication, authorization, Buffer Overrun, Access control list, least privilege, Cryptographic Foibles, Protecting Secret Data

Input issues: database, web–specific, internationalization.

UNIT – IV

Socket Security, Securing RPC, Protecting Against Denial of Service Attacks.

Security testing, security code review, secure software installation, writing security documentation.

References / Textbooks:

1. Michael Howard and David LeBlanc, Writing Secure Code, Microsoft Press, (2006).
2. Nithin Haridas, Software Engineering – Security as A Process in the SDLC, Startch Publisher (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.
5. J.D. Glaser, Secure Code Development for Mobile Apps, Auerbach Publications (2017), 1st Edition

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

(Session 2024-25)
COURSE CODE: MINL-2115
MOBILE APPLICATION DEVELOPMENT AND SECURITY

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend Integrated Development Environment and project structure for developing and configuring mobile applications.

CO2: Apply various UI widgets and components for designing User Interface of application.

CO3: Manage view and navigation in mobile application through intents, activities, fragments, etc.

CO4: Link android application to SQLite database and implement security in the application.

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

(Session 2024-25)

COURSE CODE: MINL-2115

MOBILE APPLICATION DEVELOPMENT AND SECURITY

L-T-P: 4-0-0 **Max. Marks: 100**

Credits: 4

Examination Time: 3 Hours **Theory: 80**

CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) 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, Android Project Folder Structure, Hide Title Bar, Screen Orientation.

UNIT – II

Android Widgets: UI Widgets, Working with Button, Toast, Custom Toast, Toggle Button, Check Box, Custom Check Box, Radio Button, Dynamic Radio Button, Custom Radio Button, Alert Dialog, Spinner, Auto Complete Text View, List View, Custom List View, Rating Bar, WebView, Seek Bar, Date Picker, Time Picker, Analog and Digital, Progress Bar, Vertical Scroll View, Horizontal Scroll View.

Image Switcher, Image Slider, View Stub, Tab Layout, Tab Layout with Frame Layout, search View, Search View on Toolbar, Edit Text with Text Watcher.

UNIT – III

Activity and Intents: Activity Life Cycle, Implicit Intent, Explicit Intent, Start Activity for Result, 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.

References / Textbooks:

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. Himanshu Dwivedi, Chris Clark, David Thiel, Mobile Application Security, Tata McGraw Hill, 1st Edition, 2010.
5. Neil Bergman, Mike Stanfield, Jason, Rouse , Joel Scambray , Sarath Geethakumar , Swapnil Deshmukh, Scott Matsumoto , John Steven , Mike Price, Hacking Exposed Mobile Security Secrets & Solutions, McGraw-Hill Osborne Media,1st Edition ,2013.
6. https://developer.android.com

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

(Session 2024-25)

COURSE CODE: MINP-2116

LAB ON MOBILE APPLICATION DEVELOPMENT AND SECURITY

L-T-P: 0-0-2 **Max. Marks: 50**

Credits: 2

Examination Time: 3 Hours **Practical: 40**

CA:10

Lab on Mobile Application Development and Security.