FACULTY OF COMPUTER SCIENCE & IT

SYLLABUS

of

Master of Science (Information and Network Security)
(Semester III - IV)

(Under Continuous Evaluation System)

Session: 2022-23

कन्या महा विद्यालय जालन्धर

असतो मा सद् गमय

स्था. 1886

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)

Session 2022-23

Master of Science (Information and Network Security) Semester - III							
COURSE CODE	**COURSE NAME**	**COURSE TYPE**	**Marks**				**Examination Time (in Hours)**
			Total	**Ext.**		**CA**	
				L	**P**		
MINL-3111	Cyber Incident Handling and Reporting	C	100	80	-	20	3
MINL-3112	Cloud Computing and its Security	C	100	80	-	20	3
MINL-3113	Proactive Security Tools and Technology	C	100	80	-	20	3
MINL-3114	Penetration Testing and Auditing	C	100	80	-	20	3
MINL-3115	Cryptography and Network Security	C	100	80	-	20	3
MINP-3116	Lab on Penetration Testing and Virtualization	C	100	-	80	20	3
			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 2022-23

Master of Science (Information and Network Security) Semester - IV							
COURSE CODE	**COURSE NAME**	**COURSE TYPE**	**Marks**				**Examination Time (in Hours)**
			Total	**Ext.**		**CA**	
				L	**P**		
MINL-4111	Intrusion Detection System	C	100	80	-	20	3
MINL-4112	Reverse Engineering and Malware	C	100	80	-	20	3
MINL-4113	Ethical Hacking	C	100	80	-	20	3
MINL-4114	Blockchain for Enterprise Applications	C	100	80	-	20	3
MIND-4115	Major Project / Dissertation	C	200	-	160	40	6
	Total		600				

Note:

C - Compulsory

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

(Session 2022-23)

COURSE CODE: MINL - 3111

CYBER INCIDENT HANDLING AND REPORTING

Course Outcomes:

CO1: Comprehend handling of system security related incidents.
CO2: Analyze compromised systems through the utilization of tools and common processes.
CO3: Identify Denial-of-Service attacks and its appropriate countermeasures.
CO4: Apply different incident handling tools.

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

(Session 2022-23)
COURSE CODE: MINL - 3111
CYBER INCIDENT HANDLING AND REPORTING

Examination Time: 3 Hrs **Max. Marks: 100**
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: Concept of Computer security Incident, Types of Incident-denial of service-malicious code, unauthorized access, Inappropriate Usage. Need for incident Response, Policies, Plans and Procedure related to incident Response, Incident reporting organization.

UNIT - II

Incident Detection and Analysis: Profiling, Behaviors, Centralized logging , Event Correlation, Diagnosis matrix , Incident Analysis – Incident Documentation ,incident Prioritization, Incident Response SLA Matrix , Incident Notification.

UNIT - III

Handling denial of Service Incident: DoS attacks, Concept of DDoS, Types of DDoS- Reflector Attacks, Amplifier Attacks and Floods, Prevention of DDoS-Incident Handling Preparation, Containment Strategy, Handling Unauthorized Access Incidents, Malicious Code Incidents.

UNIT - IV

Incident Handling Tools: Disk Digger, NTFS Walker, LOG Auditing

References / Textbooks:

1. Barbara Guttman, Edward Roback, An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12, 1995.
2. Julie Lucas, Brian Moeller, The Effective Incident Response Team, Addison-Wesley Professional, 2004.
3. Michael E. Whitman, Herbert J. Mattord, Principles of Incident Response and Disaster Recovery, Thomson Course Technology, 2007.
4. E. Eugene Schultz, Russell Shumway, Incident Response: A Strategic Guide to Handling System and Network Security Breaches, New Rider Publishing, 2002.
5. Chris Prosise, Kevin Mandia, Incident Response & Computer Forensics, Tata McGraw-Hill Education, 2003.

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

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

(Session 2022-23)

COURSE CODE: MINL - 3112

CLOUD COMPUTING AND ITS SECURITY

Course Outcomes:

CO1: Comprehend cloud reference model, associated threats and security requirements.
CO2: Analyze the Virtualization concept and cloud security model.
CO3: Identify different cloud service provider and mini variations of cloud computing.
CO4: Identify the application of different security tools and technologies for trustworthiness of cloud.

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

(Session 2022-23)
COURSE CODE: MINL - 3112
CLOUD COMPUTING AND ITS SECURITY

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

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: Cloud Computing, Advantage & Disadvantage, History of Cloud, Cloud Computing Architecture, Cloud Computing Technologies, Cloud Computing vs Grid Computing, working of Cloud, Cloud Computing Applications, Security Risks of Cloud Computing, Essential Characteristics of Cloud Computing, Cloud deployment model.

Cloud Computing: Cloud Service Models, cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing.

UNIT - II

Virtualization: What is Virtualization, Data Virtualization, Hardware Virtualization, Software virtualization, Server Virtualization, Storage Virtualization, OS Virtualization, Linux Virtualization, Windows virtualization

Cloud security: Cloud Security challenge, Principal Characteristics of Cloud Computing security, Data center security Recommendations, Encryption and key management in the cloud, identity and access management, trust models for cloud, Cloud forensics, traditional security, business continuity and disaster recovery.

UNIT - III

Cloud Service providers: Cloud Service Provider Companies, Amazon EC2, AWS vs Azure vs GCP. Different Clouds - Mobile Cloud Computing, Fog Computing, Green cloud, Sensor Cloud Computing, IoT cloud.

UNIT - IV

Data security tools and techniques for the cloud: Understanding the cloud architecture, Governance and enterprise risk management, design of customized cloud security measures, application security, targets of cybercrime.

Trustworthy cloud infrastructures, Secure computations, Cloud related regulatory and compliance issues,

References / Textbooks:

1. Jim Smith, Ravi Nair, and Virtual Machines: Versatile Platforms for Systems and Processes, Morgan Kaufmann, 2005.
2. John Ritting house and James F.Ransome, Cloud Computing: Implementation, Management, and Security, CRC Press Taylor and Francis Group, 2010.
3. Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010.
4. John R. Vacca, Cloud Computing Security, CRC Press, 2016.

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

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

(Session 2022-23)
COURSE CODE: MINL - 3113
PROACTIVE SECURITY TOOLS AND TECHNOLOGY

Course Outcomes:

CO1: Comprehend the taxonomy of security tools.
CO2: Identify the working of different honeypots.
CO3: Articulate various commands used in the implementation of proactive security.
CO4: Analyze and track botnets, malware and client honeypots.

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

(Session 2022-23)
COURSE CODE: MINL - 3113
PROACTIVE SECURITY TOOLS AND TECHNOLOGY

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

Network Security tool taxonomy: Reconnaissance tools, attack and penetration tools, defensive tools, Security planning, Security Strategies, Security threats.

UNIT - II

High interaction honeypots, Medium interaction honeypots, Low interactions honeypots and Virtual honeypots, Netcat (Sniff army knife), NMAP (Active scanning), Nessus (Penetration testing), TCPDUMP, Wireshark (passive traffic sniffing)

UNIT - III

NSLOOKUP, DIG (DNS information retrieval), Firewalling (iptables), Reverse firewalling, securing honeypots, sebek, Argos, Honeywall, Network traffic visualization.

UNIT - IV

Hybrid systems, client honeypots, Botnets, tracking botnets, analysing malware, Hacking channel jargon and interpretation.

References / Textbooks:

1. Niels Provos, Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison-Wesley, 2007.
2. The Honeynet Project, Know Your Enemy: Learning about Security Threats, Addison-Wesley Professional, 2004.
3. Mike Schiffman, Building Open Source Network Security Tools: Components and Techniques, Wiley, 2002.
4. Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg, Network Security: The Complete Reference, McGraw Hill Education, 2017.

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

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

(Session 2022-23)
COURSE CODE: MINL - 3114
PENETRATION TESTING AND AUDITING

Course Outcomes:

CO1: Comprehend risk management and penetration testing.
CO2: Implement penetration testing in routers, firewalls and IDS.
CO3: comprehend penetration testing for social engineering and password cracking.
CO4: Write penetration testing report.

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

(Session 2022-23)
COURSE CODE: MINL - 3114
PENETRATION TESTING AND AUDITING

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

Identify Risk, Manage Risk, Risk mitigation, Customers and legal agreements, Penetration testing planning and scheduling, Information gathering.

UNIT – II

External and internal network penetration testing. Router penetration testing, Firewalls penetration testing, Intrusion detection system penetration testing

UNIT – III

Wireless networks penetration testing, Password cracking penetration testing, social engineering penetration testing.

UNIT – IV

Application penetration testing, Policies and controls testing. Penetration testing report and documentation writing

References / Textbooks:

1. T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Hack I.T.: Security Through Penetration Testing, Addison-Wesley, 2002.
2. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, Metasploit: The Penetration Tester's Guide, No Starch Press, 2011.
3. Thomas Wilhelm, Professional Penetration Testing: Creating and Learning in a Hacking Lab, Syngress, 2013.
4. William Chuck Easttom II, Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits, Pearson, 2018.

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

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

(Session 2022-23)
COURSE CODE: MINL - 3115
CRYPTOGRAPHY AND NETWORK SECURITY

Course Outcomes:

CO1: Analyze the performance of various Classical Cryptography Techniques.
CO2: Comprehend various symmetric and public key cryptography techniques.
CO3: Evaluate the authentication and hash algorithms.
CO4: Comprehend concepts of cryptanalysis and internetwork security.

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

(Session 2022-23)
COURSE CODE: MINL - 3115
CRYPTOGRAPHY AND NETWORK SECURITY

Examination Time: 3 Hrs **Max. Marks: 100**
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 cryptography, Classical Cryptosystem, Cryptanalysis on Substitution Cipher (Frequency Analysis), Play fair Cipher, Block Cipher. Data Encryption Standard (DES), DES (Contd.), Triple DES, Modes of Operation, Stream Cipher, Pseudorandom Sequence. LFSR based Stream Cipher, Abstract algebra, Number Theory.

UNIT - II

Modular Inverse, Extended Euclid Algorithm, Fermat's Little Theorem, Eular Phi-Function, Eular's theorem, Quadratic Residue, Polynomial Arithmetic. Advanced Encryption Standard (AES), Introduction to Public Key Cryptosystem, Dife-eellman Key Exchange, Knapsack Cryptosystem, RSA Cryptosystem. Primarily Testing, Ellamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime.

UNIT - III

Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function, Universal hashing, Cryptographic hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS), More on Key Exchange Protocol.

UNIT - IV

Cryptanalysis, Time-Memory Trade-of Attack, Differential Cryptanalysis, Linear Cryptanalysis. Cryptanalysis on Stream Cipher. Internetwork Security, SSL, PGP, Cloud Security, Introduction to Blockchain and Bitcoin.

References / Textbooks:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2003.
2. Behrouz A. Forouzan, Cryptography & Network Security, McGraw Hill Education, 2010.
3. S.Bose, P.Vijayakumar, Cryptography and Network Security, Pearson, 2016.
4. Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill, 2003.
5. Bruce Schneier, Applied Cryptography, John Wiley & Sons, 2015.

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

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

(Session 2022-23)
COURSE CODE: MINP - 3116
LAB ON PENETRATION TESTING AND VIRTUALIZATION

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

Lab on Penetration Testing and Virtualization.

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

(Session 2022-23)
COURSE CODE: MINL-4111
INTRUSION DETECTION SYSTEM

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend the importance of intrusion detection.
CO2: Identify various Intrusion Detection systems and methodologies associated with them.
CO3: Evaluate the impact of Intrusion Detection Systems through its capabilities.
CO4: Identify the integration of multiple IDS.

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

(Session 2022-23)
COURSE CODE: MINL-4111
INTRUSION DETECTION SYSTEM

Examination Time: 3 Hrs **Max. Marks: 100**
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 and an Overview of Intrusion Detection Systems: Introduction about intrusion detection systems, Purpose and Scope of intrusion detection systems, Need of intrusion detection systems, applications of intrusion detection systems, Firewalls and intrusion detection systems.

UNIT - II

Intrusion Detection Systems and Associated Methodologies: Uses of Intrusion detection technologies, Key Functions of Intrusion detection systems, Common Detection Methodologies, Signature-Based Detection, Anomaly-Based Detection, stateful protocol analysis, Types of Intrusion detection technologies

UNIT - III

Intrusion detection Technologies and Components: Components and Architecture, Typical Components Network Architectures, Security capabilities, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities Prevention Capabilities and its implementation, Deploying IDS.

UNIT - IV

Using and Integrating Multiple Intrusion Detection Systems Technologies The Need for Multiple IDS technologies, Integrating Different IDS Technologies, Direct IDS Integration Indirect IDS Integration, Other Technologies with IDS Capabilities, Network Forensic Analysis Anti-Malware Technologies, Honeypots

References / Textbooks:

1. Tim Crothers, Implementing Intrusion Detection Systems: A Hands–On Guide for Securing the Network, John Wiley and Sons.
2. Christopher Kruegel, Fedrick Valeur, Intrusion Detection and Correlation: Challenges and Solutions, Springer.
3. Chris Sanders, Intrusion Detection Honeypots: Detection through Deception (2020).

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

(Session 2022-23)
COURSE CODE: MINL-4112
REVERSE ENGINEERING AND MALWARE

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend complete taxonomy of malware.
CO2: Comprehend the Reverse Engineering Malware Methodology and associated tools.
CO3: Comprehend various resources utilized for detection of malware.
CO4: Apply tools for examination, analysis and mitigation of malware attack.

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

(Session 2022-23)
COURSE CODE: MINL-4112
REVERSE ENGINEERING AND MALWARE

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

Malware, Analysis, and Trends, Malware taxonomy and characteristics: Understanding Malware Threats: Malware indicators, Malware Classification, Examining Clam AV Signatures, Creating Custom Clam AV Databases.

UNIT - II

Malware Analysis (MA): Reverse Engineering Malware (REM) Methodology, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis.

UNIT - III

Resources for Reverse-Engineering Malware (REM): Initial Infection Vectors and Malware Discovery, Sandboxing Executables and Gathering Information From Runtime Analysis, The Portable Executable (PE32) File Format, Identifying Executable Metadata, Executable Packers and Compression, and Obfuscation, Techniques.

UNIT - IV

Utilizing Software Debuggers to Examine Malware, Analyzing Malicious Microsoft Office and Adobe PDF Documents, Analyzing Malicious Browser-based Exploits, Automating the Reverse Engineering Process.

References / Textbooks:

1. Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard “Malware Analyst’s Cookbook and DVD: Tools and Techniques for Fighting Malic ious Code”, First Edition (2010), Wiley Publications.
2. Ed Skoudis and Lenny Zeltser, “Malware: Fighting Malicious Code” (2003). Prentice Hall Publications.
3. Cameron H. Malin, Eoghan Casey, and James M. Aquilina “Malware Forensics: Investigating and Analyzing Malicious Code” (2008), Syngress Publications.
4. Eldad Eilam, “Reversing: Secrets of Reverse Engineering” (2005), Wiley.
5. Blokdyk, Gerardus, “Reverse Engineering Malware: The Ultimate Step-By-Step Guide” (2018).

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

(Session 2022-23)
COURSE CODE: MINL-4113
ETHICAL HACKING

Course Outcomes:

After passing this course the student will be able to:

CO1: Articulate the concept of security and phases involved in hacking.
CO2: Comprehend various hacking techniques Sniffing Traffic, DNS and IP Sniffing, HTTPS Sniffing, WLAN Sniffers, etc.
CO3: Comprehend session hijacking along with its types and tools for implementation.
CO4: Comprehend the process of hacking wireless networks.

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

(Session 2022-23)
COURSE CODE: MINL-4113
ETHICAL HACKING

Examination Time: 3 Hrs **Max. Marks: 100**
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: Understanding the importance of security, Concept of ethical hacking and essential Terminologies-Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking

UNIT - II

Foot Printing: Introduction to foot printing, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase.

System Hacking: Aspect of remote password guessing, Role of eavesdropping ,Various methods of password cracking, Keystroke Loggers, Understanding Sniffers ,Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing.

UNIT - III

Session Hijacking: Understanding Session Hijacking, Phases involved in Session Hijacking, Types of Session Hijacking, Session Hijacking Tools.

UNIT - IV

Hacking Wireless Networks: IEEE 802.11a and IEEE 802.11b standards, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing Wireless Networks.

References / Textbooks:

1. Network Security and Ethical Hacking, Rajat Khare, Luniver Press,(2006).
2. Ethical Hacking, Thomas Mathew, OSB Publisher, (2003).
3. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and George Kurtz, McGraw-Hill, (2005).
4. Ethical Hacking and Network defense, Simpson, Cengage Learning, (2009).

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

(Session 2022-23)
COURSE CODE: MINL-4114
BLOCKCHAIN FOR ENTERPRISE APPLICATIONS

Course Outcomes:

After passing this course the student will be able to:

CO1: Identify elements, working and role of Blockchain.
CO2: Comprehend implementation of Blockchain in bitcoin.
CO3: Comprehend about setup of bitcoin node and development of alternative cryptocurrencies.
CO4: Comprehend the networking and components of Ethereum.

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

(Session 2022-23)
COURSE CODE: MINL-4114
BLOCKCHAIN FOR ENTERPRISE APPLICATIONS

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

Blockchain : Introduction, History, Elements of Blockchain, Working of a blockchain, tiers, features, Types, Benefits and Limitations, Consensus.

Decentralization: Use of Blockchain in Decentralization, Methods of Decentralization, Routes, Smart Contracts, Decentralized Organizations, Requirements of Decentralized Application, Platforms for Decentralization, Symmetric Cryptography, Private Key Cryptography

UNIT - II

BitCoin: Introduction, Digital Key and address, Transaction, Blockchain Structure, Mining

Bitcoin Network Wallets, Bitcoin Payments

UNIT - III

Bitcoin Clients and APIs: Bitcoin Installation, Type of Clients, setting up a bitcoin node

Bitcoin Limitations, Development of altcoins, Namecoin, Primecoin, Zcash

UNIT - IV

Ethereum: Introduction, Ethereum network, Components, Development Environment, Alternative Blockchains – Kadena, Ripple, Stellar, Rootstack, Quorum, BigchainDB

References / Textbooks:

1. Ambadas Tulajadas Choudhari, MR Sharn, Blockchain for Enterprise Applications, Wiley (2020)
2. Tiana Laurence, Blockchain for Dummies, Wiley (2017)
3. Daniel Drescher, Blockchain Basics, Apress (2017), 1st Edition
4. David Shrier, Basic Blockchain: What it is and How it will transform the way we work and live, Robinson Publishers (2020)

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

(Session 2022-23)
COURSE CODE: MIND-4115
MAJOR PROJECT / DISSERTATION

Course Outcomes:

After passing course the student will be able to:

CO1: Apply the tools and techniques learnt to frame problems and their corresponding solutions.

CO2: Develop skills necessary to structure, manage and execute projects.

CO3: Learn to work as a member of a cohesive unit.

CO4: Develop presentation skills.

CO5: Perform documentation related to development of the project.

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

(Session 2022-23)
COURSE CODE: MIND-4115
MAJOT PROJECT / DISSERTATION

Examination Time: 6 Hrs | **Max. Marks: 200**
Practical: 160
CA:40

1. Candidates have to submit one hard copy and two CDs/DVDs of documentation which shall be kept with the HoD in the college only. Further, supervisor/guide shall forward one copy of DVD/CD containing all the documentation files of the students (file name to be saved as Rollno_of_the_ student.pdf) to the COE Office. The Covering letter (duly signed by the guide and Head of the department) should contain the following information. Candidate name, Candidate Roll no, Project Title of the student and .pdf file name of her dissertation documentation.

2. The assignment shall be evaluated by a board of three examiners (one (01) External examiner as approved by the BOS, one (01) internal examiner and HoD) .

3. The dissertation is to be submitted as per the common ordinances for P.G. courses under semester system.