Program Structure and Syllabus
for
M.Sc. Cybersecurity

2021-22 Onwards

ADIKAVI NANNAYA UNIVERSITY

RAJAMAHENDRAVARAM

ADIKAVI NANNAYA UNIVERSITY: RAJAMAHENDRAVARAM
BOARD OF STUDIES MEETING – FORENSIC SCIENCE
Date: 28-10-2021

AGENDA:

1. Eligibility and Entrance Examinations
2. Syllabus finalization
3. Syllabus for practicals
4. Number of teaching hours / Periods theory / Practicals
5. Model Question Papers
6. Credits / Evaluation
7. Scheme of Valuation
8. List of Examiners for paper setting
9. List of Practical Examiners

Members:

1. Dr. D. Kalyani, Asst. Prof.,
   Dept. of Zoology, AKNU, RJY, - **Chairman**

2. Mr.E.Mohan, Principal,
   Aditya Degree College, Surampalem - **Convener**

3. Dr. N. Kala Bhaskar, Asst. Prof.
   University of Madras, Chennai - **Member**

4. Dr. Komal Saini, Professor,
   Panjabi University - **Member**

5. Dr. P. Uma Maheshwara Rao, Prof. & Head,
   Forensic Medicine & Toxicology,
   Rangaraya Medical College, Kakinada - **Member**

6. Dr. Satyan, Scientist (Retd),
   CFSL Hyderabad - **Member**

RESOLUTIONS:

The common Board consisting of the above members have met on blended mode in the O/o Dean, Academic Affairs, Adikavi Nannaya University, Rajamahendravaram on 28/10/2021 and considered the enclosed agenda. After thorough deliberations and discussions, the Board members have resolved the following.

1. A B.Sc. graduate with “Chemistry or Forensic Science” as one of the subjects is eligible to apply for admission into M.Sc. Forensic Science-Questioned Documents and Fingerprints.

2. A B.Sc. graduate with “Chemistry or Forensic Science” as one of the subjects is eligible to apply for admission into M.Sc. Forensic Science - Chemistry and Toxicology.

3. A B.Sc. graduate with “Biology or Forensic Science” as one of the subjects is eligible to apply for admission into M. Sc. Forensic Science - DNA Finger Printing.

4. A B.Sc. graduate with “Computer Science or Forensic Science” as one of the subjects is eligible to apply for admission into M.Sc. Cyber Security.

5. A B.Sc. graduate with “Computer Science or Forensic Science” as one of the subjects is eligible to apply for admission into M.Sc. Digital Forensics and Information Security.

6. The members formulated the syllabus for M.Sc Forensic Science, a 2 year program on par with other Universities in the Country to be implemented from academic year 2021-22.

7. The syllabus for practicals of the above courses was formulated on par with UGC model curriculum.

8. There shall be 4 to 5 hours per week for each theory paper & 3 hrs for each practical.

9. I & II Semesters are common for M.Sc Forensic Science - Questioned Documents & Fingerprints, M.Sc Forensic Science - Chemistry and Toxicology, M.Sc Forensic Science - DNA Finger Printing

10. III Semester is having specialization i.e, Questioned Documents & Fingerprints in M.Sc Forensic Science - Questioned Documents & Fingerprints, Chemistry and Toxicology in M.Sc Forensic Science - Chemistry and Toxicology, DNA Finger Printing in M.Sc Forensic Science - DNA Finger Printing.

11. IV Semester will be project cum Internship for all M.Sc. Programs M.Sc Forensic Science - Questioned Documents & Fingerprints, M.Sc Forensic Science - Chemistry and Toxicology, M.Sc Forensic Science - DNA Finger Printing, M.Sc. Cyber Security, M.Sc. Digital Forensics and Information Security.

12. Marks and credits are allotted to theory & practical papers in each semester. There will be 100 marks for each theory, and 200 marks for 2 practicals each 100 marks and total marks for each semester 600 x 4 semester 2400 marks.

13. Examination pattern will be as follows.

a) Each theory paper will be evaluated for 100 marks out of which75% of marks, for Semester End Examination (SEE) while the remaining 25% marks for Continuous Internal Assessment (CIA)

Continuous Internal Assessment		
S. No	Scheme of Evaluation	Marks
1	Mid-Semester Examination	10M
2	Assignment/Seminar Presentation	5M
3	Attendance	5M
4	Swachhata Activity	5M
Total		25M

Details of Attendance Marks		
S.No	Attendance	Marks Allotted
1	95% above	5
2	85-94%	4
3	75-84%	3
4	65-74%	2
5	55-64%	1
6	< 54%	0
Total		25M

b) The Semester End Examination question paper comprises of two sections –Section A & B, Section A consists of 4 questions one question from each unit of syllabus with internal choice ‘a’ or ‘b’. Section-B consists of 8 short questions two from each unit of the syllabus, with internal choice out of which only 5 are to be attempted

c) Similarly, each practical will be evaluated for a total of 100 marks, out of which 75% of marks for Semester End Examination (75 Marks) and 25% (25 Marks) for Continuous Internal Assessment.

14. A comprehensive viva-voce will be conducted for students at the end of IV Semester for 100 marks carrying 4 credits.

15. IV Semester Students should do their project cum internship at Forensic Science Laboratories, Police Stations, Cyber cells, Fingerprint Bureau, National Crime Records Bureau, National Forensic Sciences University, Rashtriya Raksha University, Directorate of Forensic Science Services, Centre for Development of Advanced Computing (C-DAC), National Institute of Nutrition, Centre for DNA Fingerprinting and Diagnostics – CDFD, Council of Scientific And Industrial Research–Centre for Cellular and Molecular Biology (CSIR–CCMB), Indian Institute of Chemical Technology (CSIR-IICT), Central Detective Training Institute, etc. and thesis must be submitted to the college and University.

M.Sc. Forensic Science
SEMESTER END EXAMINATION
Theory Model Question Paper pattern

Time: 3 hrs **Max. Marks: 75**

Section-A

Answer all questions. Each question carries 15 marks. **4x15=60**

Q1. Unit-1

a or b

Q2. Unit-2

a or b

Q3. Unit-3

a or b

Q4. Unit-4

a or b

Section-B **5x3=15**

Q5. It contains 8 short questions with at least two from each unit, carrying 3 marks.

5 questions are to be answered.

M.Sc. Cybersecurity
Scheme of Examination

Code	Title of the Paper	L @	P #	Total (Hrs)/ Week	Duration of Exam (hrs)	External Marks	Internal Marks	Total Marks	Credits
I Semester									
MSFS101	Cyber Law and Intellectual Property Rights	4	3	7	3	75	25	100	4
MSFS102	Computer Fundamentals	4	3	7	3	75	25	100	4
MSFS103	Cybersecurity Essentials	4	3	7	3	75	25	100	4
MSFS104	Introduction to Programming	4	3	7	3	75	25	100	4
Lab Course									
MSFS105	Cybersecurity Essentials Lab				3	75	25	100	4
MSFS106	Introduction to Programming Lab				3	75	25	100	4
II Semester									
MSFS201	Cryptography & Network Security	4	3	7	3	75	25	100	4
MSFS202	Cyber Forensics	4	3	7	3	75	25	100	4
MSFS203	Database Management System	4	3	7	3	75	25	100	4
MSFS204	Vulnerability Assessment & Penetration testing	4	3	7	3	75	25	100	4
Lab Course									
MSFS205	Database Management System Lab				3	75	25	100	4
MSFS206	Vulnerability Assessment & Penetration Testing Lab				3	75	25	100	4
III Semester									
MSFS301	Reverse Engineering and Malware Analysis	4	3	7	3	75	25	100	4
MSFS302	Security Auditing, Risk and Compliance	4	3	7	3	75	25	100	4
MSFS303	Advanced Digital Forensic Analysis	4	3	7	3	75	25	100	4
MSFS304	Security in Cyber Physical Environment	4	3	7	3	75	25	100	4
Lab Course									
MSFS305	Reverse Engineering and Malware Analysis Lab				3	75	25	100	4
MSFS306	Advanced Digital Forensic Analysis Lab				3	75	25	100	4
IV Semester									
MSFS401	Comprehensive viva-voce							100	4
MSFS402	Project					500	100	600	24
Total								**2500**	**100**

@ Lectures
# Practicals

M.Sc. Cybersecurity

I Semester, Paper I

MSFS101- Cyber Law and Intellectual Property Rights

Aim and Objectives of Course: To Introduce fundamentals of Forensic Science, Concepts of Criminology, Laws pertaining to Criminal Justice System and Court Testimony.

Learning Outcomes:

1. To educate about the regulation of cyber space at national and international level.
2. To discuss the international legal regime related to cybercrimes.
3. To discuss about e- governance.
4. To discuss the offences and penalties under I.T. Act 2000 and its amendments.
5. To introduce the concept of cybercrimes.

Unit I- Introduction to Cyber Crimes

Introduction to Information technology & Cyber Law, Basics of E-commerce and Computer Fraud Techniques, Cyber Security Fundamentals Techniques and Core Principles, IT Rule 2011. Cyber Space, Technology & Issues, Regulating Cyber Space: International, National, E-contract & Electronic Data Interchange, Cyber security policy 2013, Stake Holders of Cyber Security (NPCA, CERT, NTRO, NCIIPC) Protection to critical Industries.

UNIT II- Cyber Laws

Introduction to cyber law, association of cyber law with IPC, IEA, CrPC, need of cyber law in country, IT – Act 2000, amendments in IT Act till Date, Right to Access Cyberspace – Access to Internet, Right to Privacy, Right to Data protection, Concept of Jurisdiction, Indian Context of Jurisdiction, International Law and Jurisdictional Issues in Cyberspace, Dispute Resolutions, Case studies, Introduction to CERT, working of CERT, Cyber Laws of EU – USA – Australia - Britain, other specific Cyber laws.

UNIT III- Significance of I.T. Act

E-signature and E-governance legality under I.T. Act, 2000, Cyber Contraventions, Compensation & Crimes under I.T. Act,2000. ISPs and Websites Legal Liability under I.T. Act, 2000.

Corporate Legal Liability, Adjudication Process for Recovery of Losses under I.T. Act,2000.

Policy, Law and Cyber Security community; Indian IT Act, Indian Penal Code, Income Tax Law; International Standards - IPR, COBIT, Security Audit.

UNIT IV- IPR

IPR & Cyber Space, Taxation Issues in Cyber Space, IT Act, and its relation with Income Tax Law. IT Act and its relation with Indian Penal Code, Case Studies and Case Laws, Relevant section of other Acts such as IPC, Indian Evidence ACT, etc.

Blocking websites, telephone tapping, packet sniffing, Dark web monitoring, social media monitoring.

Reference Books:

1. Cyber Security (with CD): Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole, Sunit Belapure.
2. Cyber Laws & Information Technology by Dr. Jyoti Rattan.
3. Cyber Crimes & laws by Taxman and Technology decoded by N.S.Nappani.

M.Sc. Cybersecurity

I Semester, Paper II

MSFS102- Computer Fundamentals

Aim and Objectives of Course: To give you a general understanding of how a computer works.

Learning Outcomes:

1. Basic Process AND Memory Management in Operating Systems.
2. Understanding of Linux operating system, Linux Flavors
3. Will be able to write a script
4. Will be able to execute shell commands

Unit I- Fundamentals of Computer

Hardware & Software, System Architecture, CPU organization, ALU, registers, memory, program execution at CPU and system level.

Data representation: Number systems, character representation codes, Binary, hex, octal codes and their inter conversions.

Basics of Operating Systems: Definition – Generations of Operating systems – Types of Operating Systems, OS Service, System Calls, OS structure: Layered, Monolithic, Microkernel.

Unit II- Operating Systems Concepts - I

Process Management: Processes: Definition, Process Relationship, Process states, Process State transitions, Process Control Block.

Context switching – Threads – Concept of multithreads, Benefits of threads – Types of threads Process Scheduling, Scheduling criteria, Scheduling algorithms.

Unit III- Operating Systems Concepts – II

Definition Logical and Physical address map, Memory allocation: Contiguous Memory allocation – Fixed and variable partition – Internal and External fragmentation and Compaction.

Paging: Principle of operation – Page allocation — Disadvantages of paging. Virtual Memory: Basics of Virtual Memory.

Unit IV- Linux Operating System

Basics of Linux, Basic commands of Linux, Creating and Removing Directories, Output Redirection, Running and managing processes in the background, Using SSH to connect to another machine, Default File Permissions, Password Files, Installing software packages, Console and Login security.

Understanding Wireshark, SUID Vulnerability, Firewall, Immutable Files, Forwarding X with OpenSSH, Syslog Basics, Dmesg, Log Rotation, Apache HTTP or Tomcat, Listing Open Files, Cracking the system with Bootloader, File Integrity check with Tripwire, Syslog-ng.

Reference Books:

1. Computer Fundamentals, by Anita Goel, PEARSON
2. Operating System Concepts by Abraham Silberschatz
3. Learning the UNIX Operating System, by Jerry Peek, Grace Todino-Gonguet, et al.
4. Linux System Programming Techniques: Become a proficient Linux system programmer using expert recipes and techniques, by Jack-Benny Persson, PACKT Publications
5. Hands-On System Programming with Linux: Explore Linux system programming interfaces, theory, and practice by Kaiwan N Billimoria, PACKT Publications

M.Sc. Cybersecurity

I Semester, Paper III

MSFS103- Cybersecurity Essentials

Aim and Objectives of Course: Understanding of cyberspace and cybersecurity, along with various Operating Systems Security.

Learning Outcomes:

1. Awareness about Cyberspace and countermeasures.
2. Building a Cybersecurity environment
3. Understanding of Windows Security Infrastructure
4. Securing Linux Services and knowing about various security features.

Tools: Kali Linux, AuditD, SIEM Tools, BitLocker, Microsoft Baseline Security Analyzer.

Unit I- Introduction to Cyber Security

Evolution of cyberspace, Elements of cyberspace, Actors, and actions in cyber security; Threats / Vulnerabilities / Attacks, Assessing the cyber threats; Countermeasures against threats, vulnerabilities, and attacks.

Cybersecurity and cyber warfare - overview from white-hat and black-hat hackers angles; Cyber Space Dark web, Tor, Deep Web, Network security Architecture, Network security and Défense mechanism - Firewall, SSL, VPN, IDS/IPS, UTM, DMZ etc; System security and Défense mechanism - OS and kernel level security and policy, malwares - updates and patches, virtualization;

Information/asset classification, Security policy, procedures, and practices; Resiliency and risk management; Cyber-crimes, Ethics, and best practices.

Unit II- Securing File Permissions

Securing Access with Permissions, Identifying Advanced NTFS Permissions, Enabling and Disabling Permission Inheritance, Exploring and Identifying Share Permissions, Combining NTFS and Share Permissions, Identifying Active Directory Permissions, Comparing NTFS and Active Directory Permissions, Assigning Registry Permissions.

Exploring Audit Policies and Object Access Auditing, Comparing Account Logon and Logon Events, Exploring Directory Service Access Auditing, Understanding Account Management Auditing, Enabling Auditing, Object Access Auditing, and Directory Service Access Auditing, Managing Security Logs, Auditing a Network with MBSA, Understanding User Account Control, Keeping Systems Updated, Updating Systems with WSUS or SCCM, Protecting Clients, Protecting Servers, Exploring DNS Security Issues.

Unit III - Windows Client Security

Securing your Windows clients, Introducing Windows Update for Business, Configuring Windows updates in Intune, Advanced Windows hardening configurations, Enabling Windows Hello for Business, Managing BitLocker encryption, Configuring Windows Defender AV, Enabling Microsoft Defender, SmartScreen, Preventing name resolution poisoning, Disabling the Web Proxy Autodiscovery Protocol (WPAD), Configuring Office security baselines, Hardening Google Chrome, Preventing user access to the registry, Windows Defender, Application Control, Windows 10 privacy, Controlling the privacy settings for each app, Additional privacy settings, Privacy settings for Microsoft Edge.

Unit IV - Linux Security Essentials

Differences between physical, virtual, and cloud setups, Creating a virtual machine snapshot with VirtualBox, Using Cygwin to connect to your virtual machines, Installing Cygwin on your Windows host, Using Windows 10 Pro Bash shell to interface with Linux virtual machines, Cygwin versus Windows Bash shell, Keeping the Linux systems updated, Securing User Accounts, The dangers of logging in as the root user, Setting up sudo privileges: for full administrative users, for users with only certain delegated privileges, Detecting and deleting default user accounts, Locking down users' home directories the Debian/Ubuntu way, Enforcing strong password criteria, Setting and enforcing password and account expiration, Preventing brute-force password attacks, Setting up security banners, Detecting compromised passwords, Understanding centralized user management.

Reference Books:

1. Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats by Mark Dunkerley and Matt Tumbarello, PACKT Publication.
2. Microsoft Windows Security Essentials by Darril Gibson, PACKT Publication.
3. Cybersecurity Ops with bash: Attack, Defend, and Analyze from the Command Line by Paul Troncone and Carl Albing Ph. D., O’Reilly.
4. Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy by Jordan Krause, PACKT Publication.
5. Mastering Linux Security and Hardening: Protect your Linux systems from intruders, malware attacks, and other cyber threats, 2nd Edition by Donald A. Tevault, PACKT Publication.

M.Sc. Cybersecurity

I Semester, Paper IV

MSFS104- Introduction to Programming

Aim and Objectives of Course: Understand various programming languages and their applications.

Learning Outcomes:

1. Will be able to write and execute C programs.
2. Will be able to write and execute C++ programs.
3. Will be able to write and execute Shell Scripts in Linux.
4. Will be able to write and execute Python Programs.

Tools: Anaconda, C compiler, C++ compiler, Visual Studio Code.

Unit-I- Introduction to programming language

Introduction to programming language, different type of programming language, machine language and assembly language, Introduction to C, C++ language.

UNIT II- Shell Scripting

Introduction to Shell scripting, writing a script, shell commands, decision making, arithmetic operation, loop, wildcards, conditional execution and executing a shell script in Linux environment.

UNIT III- Python Programming - I

Introduction to Python, the basic elements of python, Branching Programs, Control Structures.

Strings and Input, Iteration Functions, Scoping and Abstraction, Specifications, Recursion, Global variables, Modules, Files, System Functions and Parameters, Structured Types.

UNIT IV- Python Programming - II

Mutability and Higher-Order Functions, Strings, Tuples, Lists and Dictionaries, Lists and Mutability, Functions as Objects, Testing, Debugging, Handling Exceptions and Assertions.

Reference Books:

1. C Programming Language, by Brian W. Kernighan and Dennis M. Ritchie
2. The C++ Programming Language, by Bjarne Stroustrup
3. C and C++ Under the Hood by Anthony J. Dos Reis
4. Linux Shell Scripting with Bash by Ken O. Burtch.
5. Mastering Linux shell scripting a practical guide to Linux command- line, Bash scripting, and Shell programming by Mokhtar Ebrahim Andrew Mallett.
6. Python Object-Oriented Programming - Fourth Edition by Steven F. Lott, Dusty Phillips, Packt Publication

I SEMESTER PRACTICALS

MSFS105- Cybersecurity Essentials Lab

1. Implement the Windows Access Controls including NTFS Per missions, Shared Folder Permissions, Registry Key Permissions, Active Directory Permissions.
2. Hardening and Securing Linux Services: Starting services at boot time, Package control, Kernel security, Port control and port restriction, Monitoring and Attack Detection.
3. Logging with syslog and alternatives, parsing and filtering logs with grep, sed, awk, and cut.
4. Using built-in commands and security features, configure integrity, checkers, integrating host-based firewalls and managing them to provide security.
5. Setting up sudo privileges for full administrative users, users with only certain delegated privileges,
6. Detecting and deleting default user accounts.
7. Locking down users' home directories.
8. Using hardening scripts, deploying package management strategies.

MSFS106- Introduction to Programming Lab

1. Perform and Execute basic C programs.
2. Perform and Execute basic C++ programs.
3. Perform conditional execution in Linux environment.
4. Executing a shell script in Linux environment.
5. Perform and execute basic Python programs containing OOPs concepts.
6. Perform and execute programs using Tuples, Lists and Dictionaries.

M.Sc. Cybersecurity

II Semester, Paper I

MSFS201- Cryptography & Network Security

Aim and Objectives of Course: Understanding various Cryptographic concepts and emerging applications in Information Security.

Learning Outcomes:

1. Classification of Cryptographic System
2. Various Cryptographic Algorithms
3. Different concepts of Operating system security
4. Performing E-Mail Security

Unit I- CRYPTOGRAPHIC PROTOCOLS

Terminology, Steganography, Substitution and Transposition Ciphers, Simple XOR, One-Time Pads, Computer Algorithms, Large Numbers, Protocol Building Blocks, Communications Using Symmetric Cryptography, One-Way Functions, One-Way Hash Functions, Communications using Public-Key Cryptography, Digital Signatures, Digital Signatures with Encryption, Random and Pseudo-Random-Sequence Generation, Key Exchange, Authentication, Authentication and Key Exchange, Formal Analysis of Authentication and Key Exchange Protocols, Multiple-Key Public-Key Cryptography, Secret Splitting, Secret Sharing, Cryptographic protection of databases.

UNIT III- CRYPTOGRAPHIC TECHNIQUES

Key length, Symmetric key length, Public-Key Key Length, Comparing Symmetric and Public-Key's Key Length, Birthday Attacks Against One-Way Hash Functions, How Long Should a Key Be?, Caveat Emptor, Key Management, Algorithm Types and Modes, Electronic Codebook Mode, Block Replay, Cipher block chaining Mode, Stream Ciphers, Self-Synchronizing Stream Ciphers, Cipher-Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Modes, Counter Mode, Other Block-Cipher Modes, Choosing an Algorithm, Hardware Vs Software Encryption, Compression, Encoding, Encryption, Detecting Encryption, Hiding Ciphertext in Ciphertext, Destroying Information.

UNIT III- CRYPTOGRAPHIC ALGORITHMS

Mathematical Background, Information Theory, Complexity Theory, Number Theory, Factoring, Prime Number Generation, Discrete Logarithms in a Finite Field, Data Encryption Standard (DES), Description of DES, Security of DES, Differential and Linear Cryptanalysis, The real design criteria, DES Variants, How secure is DES Today? Pseudo-Random-Sequence Generators, Design and Analysis of stream ciphers, Stream Ciphers USING LFSRs, AS, HUGHES XPD/KPD, Nanoteq, Rambutan, Additive Generators, Gifford, Algorithm M, pkzip.

UNIT IV- PUBLIC-KEY ALGORITHMS

Knapsack Algorithms, RSA, POHLIG-HELLMAN, Rabin, Elgamal, McELIECE, Elliptic curve cryptosystems, LUC, Finite automation Public-Key cryptosystems, Digital signature algorithm (DSA), DSA Variants, GOST Digital signature algorithm, Discrete Logarithm Signature Schemes, ONG-SCHNORR-SHAMIR, ESIGN, Cellular Automata, Other Public-Key Algorithms.

Reference Books:

1. Cryptography and Network Security -- W. Stallings [Prentice Hall]
2. Introduction to Cryptography with Coding Theory -- Washington & Trappe [Pearson]
3. Introduction to Modern Cryptography -- Katz & Lindell [CRC press]
4. Applied Cryptography: Protocols, Algorithms, and Source Code in C -- Bruce Schneier, [Wiley].
5. Handbook of Applied Cryptography -- A. Menezes, P. van Oorschot and S. Vanstone [CRC press].

M.Sc. Cybersecurity

II Semester, Paper II

MSFS202- Cyber Forensics

Aim and Objectives of Course: Understanding Computer Forensics and Investigation Processes, Incident recovery and SIEM/Log Analysis.

Learning Outcomes:

1. Processing Crime and Incident Scenes
2. Learn about Network Forensics
3. Details related to Incident Response and Handling Process
4. Knowing about Incident Response Team Development
5. Hands-On with various Incident Response Investigation tools
6. Various features of Security information and event management

Tools: Kansa, Investigation Tools, IR Tools, Digital Incident Response Kit, SIEM Tools.

Unit I- Introduction to Cyber Forensics

Computer Forensics and Investigation Processes, Understanding Computing Investigations, The Investigator's Office and Laboratory, Data Acquisitions – file systems; disk imaging; programs traces; investigative tools; email trace, system audit trails; hard drive – access and recovery.

Processing Crime and Incident Scenes - Binary code analysis – evidence collection, preservation, and testimony. Working with Windows and DOS. Systems, Current Computer Forensics Tools, Macintosh and Linux Boot Processes and File Systems, Malware analysis.

Network Forensics - intrusion detection; attack trace-back; packet inspection; log analysis. Recovering Graphics Files, Virtual Machines, Network Forensics, and Live Acquisitions, E-mail Investigations, Device Forensics – phone calls analysis & trace; password cracking; anti-forensics techniques.

Unit II- Incident Response and Handling Process

Definitions of incident response need for Incidents Response, Goals for Incident Response, Challenges faced by Incident Responder & Team, relation of incident response to the rest of cybersecurity operations, indicators of compromise (IOC), forensic analysis as an incident response tool, cybersecurity forensics principles.

Incident Identification, Prioritization, Handling Reporting, Incident Reporting Organizations, Estimating Cost of an Incident, Vulnerability Resources.

Incident Response and Handling Process:

Step 1: Identification; Step 2: Incident Recording; Step 3: Initial Response; Step 4: Communicating the Incident; Step 5: Containment; Step 6: Formulating a Response Strategy; Step 7: Incident Classification; Step 8: Incident Investigation; Step 9: Data Collection; Step 10: Forensic Analysis, Step 11: Evidence Protection; Step 12: Notify External Agencies; Step 13: Eradication; Step 14: System Recovery; Step 15: Incident Documentation; Step 16: Incident Damage and Cause assessment; Step 17: Review and Update the Response Policies.

Unit III- Incident Recovery

Containment/Intelligence Development: Restricting access, monitoring, and learning about the adversary to develop threat intelligence, Eradication/Remediate, Determining and executing key steps that must be taken to help stop the current incident.

Recovery: Recording of the threat intelligence to be used in the event of a similar adversary returning to the enterprise, Avoiding "Whack-A-Mole"

Incident Response Team Development: Security Awareness and Training, Incident Management, Incident Management Team, Incident Response Team, Roles and Responsibilities, Developing Skills in, Dependencies, Incident Response and Hunting Endpoint Collection with Kansa.

Investigation Tools, e-discovery, EDRM Models, digital evidence collection and preservation, email investigation, email tracking, IP tracking, email recovery, Digital Incident Response kit (for IR role) and as support for cybercrime investigations.

Unit IV- SIEM/Log Management

High-level understanding of what logging is and why it is important, Logging Overview, Setting Up and Configuring Logging, Logging Analysis Basics, Key Logging Activity.

Practical related to Log parsing application / Security information and event management.

Introduction to IoT and Security issues, Intro Blockchain and it’s security issues, Introduction to Cloud and it’s threats along with security issues.

Report Writing for High-Tech Investigations, High-Tech crimes, Live demo of popular open source forensic tools.

Reference Books:

1. Incident Response & Computer Forensics, Third Edition by Jason T. Luttgens and Matthew Pepe
2. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response, by Leighton Johnson
3. Computer Forensics -- Robert C. Newman [Auerbach Publications]
4. Incident Response and Computer Forensics -- Chris Prosise and Kevin Mandia [McGraw-Hill].

5. NIST - Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim, Grance, Karen Scarfone.
6. Good Practice Guide for Incident Management, ENISA.
7. Handbook for Computer Security Incident Response Teams (CSIRTs) by Moira J. West-Brown, Don Stikvoort, Klaus-Peter, Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek.

M.Sc. Cybersecurity
II Semester, Paper III
MSFS203- Database Management System

Aim and Objectives of Course: Understanding Databases and their applications, vulnerabilities, and security policies.

Learning Outcomes:

1. Database Models
2. SQL Concepts
3. Threats & Physical Security
4. Database security risks
5. Maintenance Policies

Tools: MySQL Workbench.

Unit I- Introduction to DBMS

Introduction and applications of DBMS, Purpose of data base, Data, Independence, Database System architecture-levels, Structure of relational databases, Domains, Relations, Relational algebra – fundamental operators and syntax.

Entity Relationship model: Basic concepts, Design process, Overview of Query Processing; Query Optimization, Transaction Management,

Introduction to databases; ACID properties; database security lifecycle; data classification; data risk assessment; database security architecture; feedback mechanisms; database installation and configuration: profiles, passwords, privileges, and roles; databases security controls, security models, user Administration

Database application security models: Take-Grant Model; PN model; Bell and LaPadula Model, Biba Model, Clack-Wilson model; Lattice Model, Roll-based access control, XML databases.

Unit II- SQL Concepts

SQL Concepts: Basics of SQL, DDL, DML, DCL, structure – creation, alteration, defining constraints – Primary key, foreign key, unique, not null, check, IN operator,

Functions - aggregate functions, Built-in functions –numeric, date, string functions, set operations, sub-queries, correlated sub-queries, Use of group by, having, order by, join and its types, Exist, Any, All, view and its types. transaction control commands – Commit, Rollback, Savepoint.

Unit III- Database Vulnerabilities

Threats & Physical Security: external and internal database threats; flaws in perimeter security; database security hierarchy; security in distributed databases; evaluate database security; evaluate organization's asset; system event triggers; flaws fixes and security patches; managing USB ports and USB enabled devices; database obscurity; virtual private database; SQL injection; backup mechanisms.

Unit IV- Data security policy

Security: Introduction, Discretionary access control, Mandatory Access Control, Data Encryption.

Database security risks; database security testing; database auditing models and tools; user management strategies; maintenance policy, assessment, and countermeasures.

Reference Books:

1. Database Systems: Design, Implementation, & Management by Carlos Coronel and Steven Morris
2. Database Management Systems by Johannes Gehrke Raghu Ramakrishnan
3. Learning SQL: Generate, Manipulate, and Retrieve Data by Alan Beaulieu
4. Learn SQL Database Programming: Query and manipulate databases from popular relational database servers using SQL by Josephine Bush

M.Sc. Cybersecurity

II Semester, Paper IV

MSFS204- Vulnerability Assessment & Penetration Testing

Aim and Objectives of Course: Understanding of Web Fundamentals and OWASP top 10 Attacks along with Static and Dynamic Session Analysis.

Learning Outcomes:

1. Web Fundamentals
2. Windows server hardening
3. RFI and LFI (remote file inclusion; local file inclusion) vulnerability
4. Advanced session analysis, hijacking, and fixation techniques
5. Static and Dynamic Analysis for Mobile Applications

Tools: Metasploit, Wireshark, SQLmap, Nmap, Nikto, BeeF, Maltego, Shodan.io, Tenable.io, Lumin, Container Security, Burp Suite, MobSF, AndroBug, drozer.

Unit I- Web Fundamentals

Web Fundamentals – HTML, HTTP, Client-side scripting, Server-side scripting. Web server architecture - Windows & Linux, IIS and LAMP servers, Network topologies and DMZ. Web applications: Introduction to web applications, Web application hacking, Overview of browsers, extensions, cross-site scripting, and platforms.

Windows server hardening, Database security, Hijacking windows with using RAT and Trojan, Web Application Security, Burp suite tool, SQL injection.

Unit II- OWASP

OWASP top 10, Attacks, Detection evasion techniques, and countermeasures for the most popular web platforms, including IIS, Apache, and countermeasures for common web authentication mechanisms, including password-based, multifactor.

RFI and LFI (remote file inclusion; local file inclusion) vulnerability, Denial of service (DOS) and distributed denial of service (DDOS) attacks, Countermeasures of DoS, and DDoS.

Unit III- Advanced session analysis

Advanced session analysis, hijacking, and fixation techniques, SQL injection, classic categories of malicious input, Overlong input (like buffer overflows), canonicalization attacks (like the infamous dot-dot-slash), and meta characters, various SQL injection tools and techniques, stealth-encoding techniques and input validation/output- encoding countermeasures.

XSS Attack, The Defence mechanism of SQL Injection and XSS attack, Broken authentication and session hijacking, Security misconfiguration, Session Hijacking, Malicious file inclusion.

Unit IV- Static and Dynamic Analysis for Mobile Applications

Static and Dynamic Analysis for Mobile Applications, Requirements for: Architecture, Design and Threat Modelling, Data Storage and Privacy, Cryptography, Authentication and Session Management, Network Communication, Platform Interaction, Code Quality and Build Setting, Resilience. Insecure direct object reference, Information leakage and improper error handling, Failure to restrict URL access, Request forgery attack and countermeasures, Remote code execution, Vulnerability study.

Website code review and secure coding principles, Report writing.

Reference Books:

1. Learning Nessus for Penetration Testing, by Himanshu Kumar
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
3. 2nd Mastering Modern Web Penetration Testing by Prakhar Prasad
4. Burp Suite Essentials by Akash Mahajan
5. Rich Bowen, Ken Coar, “Apache Cookbook”, O’Reilly
6. Burp Suite Cookbook
7. Metasploit Penetration testing Cookbook

II SEMESTER PRACTICALS

MSFS205 – Database Management System Lab

1. Database installation and configuration: profiles, passwords, privileges, and roles; databases security controls, security models, user Administration.
2. Implement SQL Concepts by creation, alteration, defining constraints – Primary key, foreign key, unique, not null, check, IN operator.
3. Implement database auditing models and tools.

MSFS206 – Vulnerability Assessment & Penetration testing Lab

1. Client-side scripting programs
2. Server-side scripting programs
3. Hijacking windows with using RAT and Trojan
4. SQL Injection Techniques
5. Performing defense techniques on XSS Attacks
6. Request forgery attack, Remote code execution, and Vulnerability study.
7. How to configure Burp Suite and perform the following operations:
    - ♦ Spider
    - ♦ Intruder
    - ♦ Repeater
    - ♦ Sequencer
    - ♦ Decoder
    - ♦ Scanner

M.Sc. Cybersecurity

III Semester, Paper I

MSFS301- Reverse Engineering and Malware Analysis

Aim and Objectives of Course: Understanding Reverse Engineering, Kernel Debugging, Static and Dynamic Malware Analysis.

Learning Outcomes:

1. x86 and x64 Architecture.
2. Understanding processes, threads, ports, handles.
3. Malware and it's types.
4. Executing Malware Analysis in safe environment.
5. Debugging and Malware behavior.

Tools: OllyDbg/IDA Pro, WinDBG, Regshot, Wireshark, Netcat, Kali Linux, Santoku.

Unit 1- Introduction to Reverse Engineering

Introduction to x86 and x64 Architecture: The difference between source code and compiled code, Introduction to disassemblers and de-compilers, Register Set and Data Types, Data Movement, Canonical Address, Function Invocation, Self-Defending Malware, Malicious Documents, Analysis of File Formats, Setting up a Protected Malware Analysis Environment.

Unit 2- Reverse Engineering

Intro to Kernel – Kernel basics, understanding processes, threads, ports, handles etc. Identifying services and drivers, determining scheduled tasks, Windows Kernel API, Windows Drivers, Kernel Debugging, in- Process Dumping Tools & Imports Rebuilding Utilities, Rootkit Techniques- Hooking, Patching, Kernel Object Manipulation. Windows Kernel: Windows Fundamental, Kernel Debugging with WinDBG, Survey of Obfuscation techniques, Piracy and Copy Protection, Deep Web and Dark Net, Anti Reversing Techniques, JS Analysis Complications, Anti-Reverse Engineering.

Unit 3- Static Malware Analysis

Introduction to Malware, Types of malware – Virus, Worm, Trojan, Backdoor, Ransomware, The Goals of Malware Analysis, Malware Analysis Techniques, Basic Static Techniques: Hashing, Finding Strings, Packed and Obfuscated Malware, Portable Executable File Format, Linked Libraries and Functions, PE File Header and Sections, Non-PE files analysis, Virtual Machines for Malware Analysis, Anti-Virtual Machine Techniques.

Introduction to x86 Disassembly: Architecture, Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, Stack, Conditionals, Branching, introduction to sysinternal tools, sandboxes, Analyzing Malicious Windows Programs: Windows API, Windows Registry, Networking APIs, Code injection and API hooking, Kernel vs User Mode, Native API, Anti-Disassembly.

Unit 4- Dynamic Malware Analysis

Basic Dynamic Analysis: Executing Malware Analysis in safe environment, Monitoring with Process Monitor, Viewing Processes with Process Explorer, Comparing Registry Snapshots with Regshot, Faking a Network, Packet Sniffing with Wireshark, Malicious Websites Analysis, Rebuilding Utilities, DLL Analysis, Analysis of traces of malware.

Debugging: Source Level vs Assembly Level Debuggers, Kernel vs User mode Debugging, Using Debugger – OllyDbg/IDA Pro, Exceptions, Modifying execution with Debugger, Browser script De-Obfuscation using Debuggers, Malware Behaviour: Reverse Shell, RAT, Botnet, Covert Malware: Process Injection, Hook Injection, APC Injection, Memory Forensics, Working with Santoku, Cryptographic algorithms used by ransomware, Anti-Debugging.

Reference Books

1. Eldad Eilam: Reversing – Secrets of Reverse Engineering, Wiley Publishing
2. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Book by Andrew Honig and Michael Sikorski [NS press]
3. Hacking: The Art of Exploitation – J. Erickson [SPD]
4. Writing Secure Code -- David LeBlanc and Ben Howard [Microsoft Press]

M.Sc. Cybersecurity

III Semester, Paper II

MSFS302- Security Auditing, Risk and Compliance

Aim and Objectives of Course: Understanding of Audit and Assurance Standards with implementation of an IT Infrastructure Audit for compliance and Risk-based audit planning and audit project management.

Learning Outcomes:

1. IT security assessment and Compliance
2. IT Audit and Assurance Standards
3. Fundamentals of business processes
4. Risk-based audit planning and audit project management techniques
5. Compliance within LAN and WAN Domain
6. Compliance within Remote Access and Application Domain

Unit 1- IT Audit and Assurance Standards

The need for information system security compliance: What is IT security assessment?, What is IT security audit?, what is compliance? How does an audit differ from an assessment? Why are governance and compliance important? What if organization does not comply with compliance laws? What is the scope of an IT compliance audit?, what your organization do to be in compliance?, What are you auditing within the IT infrastructure?, Maintaining IT compliance. Introduction to information auditing standards: COSO, COBIT, ISO/IEC 27001/2, SOX, HIPAA, NIST 800 53, GDPR, PCIDSS, process of auditing information systems, information security program development and incident management

Risk management and compliance, Introduction to Data privacy bill India PDPA. Audit WRT Forensics: investigating website hacking, Data Breach Investigation.

IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics, and other applicable standards. Risk assessment concepts and tools & techniques used in planning, examination, reporting and follow-up.

Fundamentals of business processes: Purchasing, Payroll, Accounts payable, accounts receivable, Role of IS in these processes. Control Principles related to controls in information systems.

Unit 2- Planning and implementation of an IT Infrastructure Audit for compliance

Defining the scope for audit, Identifying critical requirements for the audit, assessing IT security, Obtaining Information, Documentation and Resources, Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure, Identifying and Testing Monitoring Requirements, Identifying critical security control points that must be verified throughout the IT infrastructure, Building a project plan. Conducting an IT infrastructure Audit for compliance: Identifying the maximum level of risk and appropriate security baseline definitions. Identifying all documented IT security policies, standards, procedures, and guidelines, reviewing configurations and implementations, verifying, and validating proper configuration and the implementation of security controls and countermeasures. Writing the IT infrastructure audit report: executive summary of audit report summery of findings, IT security assessment results, reporting on implementation of IT security controls and counter measures, IT security controls and countermeasures gap analysis, presenting compliance recommendations.

Unit 3- Risk-based audit planning and audit project management

Risk-based audit planning and audit project management techniques. Applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits.

Evidence Collection Techniques: Observation, Inquiry, Inspection, Interview, Data Analysis, Forensic Investigation Techniques, Computer-assisted audit techniques [CAATs] used to gather, protect, and preserve audit evidence.

Sampling methodologies and substantive/data analytical procedures. Reporting and Communication techniques: Facilitation, Negotiation, Conflict Resolution, Audit report structure, issue writing, management summary, result verification. Audit Quality assurance (QA) systems and frameworks.

Various types of audits: Internal, External, Financial, and methods for assessing and placing reliance on the work of other auditors and control entities.

Unit 4- Compliance within LAN and WAN Domain

Compliance within LAN and WAN Domain: Devices and Components Commonly Found in the Domain Routers; Switches; Firewall; Proxy Servers; Demilitarized Zones; Honeypots; ISP Connections; IDS IPS; Traffic Monitoring Devices, Traffic and Performance Monitoring and Analysis, Access Rights & Access Controls, Penetration Testing and Validating Configurations, External Attacks; Internal Attacks; Intrusive vs Nonintrusive Testing; Configuration Management Verification, CIA - Confidentiality; Integrity; Availability, Best Practices for LAN WAN Domain Compliance.

Compliance within Remote Access and Application Domain

Devices and Components Commonly Found in the Domain - Remote Users; Remote Workstations/ laptops; Authentication Servers; VPNs; Data Centre; Mainframe Computers; Source Code, VPN Tunnel Monitoring, Remote Access and Application Traffic & Performance Monitoring and Analysis, Remote Access Management Tools and Systems, Application Management Tools and Systems, Access rights and Access Control in Remote Access and Application Domain, Remote Access and Application Configuration Management, Remote Access Configuration Validation, Application Server Vulnerability Management - OS Patch Management; Application Patch Management, Best Practices for Remote Access and Application Domain Compliance.

Reference Books

1. Auditor’s Guide to IT Auditing by Richard E. Cascarino
2. IT Audit, Control, and Security by Robert R. Moeller
3. Human-Computer Interaction and Cybersecurity Handbook” edited by Abbas Moallem
4. IT Auditing Using Controls to Protect Information Assets, Third Edition by Mike Kegerreis, Mike Schiller, Chris Davis
5. Auditing IT Infrastructures for Compliance (Information Systems Security & Assurance) by Martin Weiss, Michael G. Solomon
6. The Information Audit: A Practical Guide, Susan Henczel, Information Services Management Series
7. The Basics of IT Audit: Purposes, Processes, and Practical Information, Stephen D. Gantz, Syngress, 2014

M.Sc. Cybersecurity

III Semester, Paper III

MSFS303 – Advanced Digital Forensic Analysis

Aim and Objectives of Course: Understanding the Digital forensic and Anti-Forensic Techniques along with various tools and Techniques.

Learning Outcomes:

1. Goals of Digital forensics
2. Anti-Forensics Techniques
3. Browsers and Internet Forensics
4. Memory Forensics Examinations
5. Registry analysis
6. Leveraging The Sleuth Kit (TSK) and Autopsy

Tools- The Sleuth Kit (TSK) and Autopsy, DRADIS, OpenOffice, Volatility, radare2, REMnux, fmem, LiME, Kali Linux, D.E.F.T., SANS SIFT workstation.

Unit 1- Introduction to Digital Forensics:

Goals of Digital forensics, e-discovery, Chain of custody, Forensics Investigation Techniques and process, Cyber Crime incident Response, Types of Evidence, Preparing for Forensic analysis, Data Acquisition Process, Volatile Data, Cyber-attack case study and forensics, nature of cybercrime, nature of digital evidence, Digital crime scene management and incident response, Dispute Settlement in the Law of the Sea, Memory Carving Process, probative value of evidence

Anti-Forensics Techniques, Hash Functions, File Signatures and Check, PE Analysis, Image Analysis, Steganography, Password Cracking , Hash Functions, File Signatures and Check, PE Analysis, Image Analysis, Steganography, Password Cracking , Network Traffic Capture, Writing Professional Report, Anti forensics techniques.

GNU and Unix Commands, Devices, Linux File systems, File system Hierarchy, Function of Kernel, Linux Kernel, Kernel Makefiles, Introduction to Netcat, Use of Netcat in forensics, Forensic tools in Linux, File System Imaging. RAID - Levels and Duplicating, Hard Disk Structure, Boot Sequence Types, FAT File System Types, NTFS Internals, HHD vs SSD.

Unit 2- Linux Installation and Package Management

Browsers and Internet Forensics, Windows Registry, Log Analysis Techniques, Open Source Tools, Recovering Deleted Files, Start-up Files, File system Times Analysis, Event Log Analysis, Windows Registry Analysis, Internet Forensics

Live response using Linux distributions, use of kali Linux, D.E.F.T., SANS SIFT work station, Using Netcat to minimize contamination, Collecting volatile data: Date and time, Network interfaces, Funny networks, Promiscuous mode?, Network connections, Open ports, Programs associated with ports, Running processes, Open files, Routing tables, Mounted file systems, Loaded kernel modules, Volatile Memory analysis: Making the decision to dump RAM, Using fmem, Using LiME, Using /proc/kcore, Acquiring file system images, Analyzing file system images.

Memory Forensics Examinations, Tools for memory acquisition, Identify Rogue Processes, DLLs and Handles , Review Network Artifacts, Look for Evidence of Code Injection, Check for Signs of a Rootkit, Acquire Suspicious Processes and Drivers, Memory Analysis Techniques with Redline, Advanced Memory Analysis with Volatility, Malware and Rootkit Hunting in Memory, Perform In-Memory Windows Registry Examinations, Extract Typed Adversary Command Lines, Investigate Windows Services, Hunting Malware using Comparison Baseline Systems, Dumping Hashes and Credentials from Memory, Prefetch and ShimCache Extraction via Memory.

Unit 3- Windows Forensics

Registry analysis, start-up files, log analysis, event log analysis, timestamp analysis, super timeline creation and analysis, use of log2timeline and Plaso, windows volume shadow copy analysis, password cracking techniques, MFT analysis, $Recycle bin forensics, $i30 analysis, other NTFS artifacts - $data, $UsnJrnl, ShimCache, Shellbags, lnk files, jump lists, USB and Bring Your Own Device (BYOD) Forensic Examinations, Incident response procedure, steganography, password cracking techniques, printer artifacts, browser forensics yellow dot concept in printer forensics

Unit 4- Digital Forensics Tools and Techniques

Leveraging The Sleuth Kit (TSK) and Autopsy, Timeline Analysis, digging deeper into Linux file systems, Linux file forensics, Memory Volatility, Reversing Linux Malware, Writing the Reports: Autopsy, DRADIS, OpenOffice.

Detecting use mode rootkits, file carving, file system image analysis, use of the sleuth kit, autopsy, bulk extractor, foremost, timeline analysis, reversing Linux malware, digging deeper into ELF.

Mobile forensics techniques, Android mobile file system, Forensic copy of mobile device, Logical and Physical analysis, iOS analysis, APFS. Computer Networks, Distributed System, Backup, Recovery & Replication, Types of Cloud Computing Models, Cloud Architecture-Layers, Introduction to VMWare Simulator, Cloud forensic techniques, reviewing cloud trail logs, data collection and analysis techniques.

Reference Books

1. Practical Guide to Digital Forensics Investigations, Pearson 2nd Edition by Darren Hayes
2. Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition by Gerard Johansen
3. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry 2nd Edition by Harlan Carvey
4. Guide to Computer Forensics and Investigations - Standalone Book by Bill Nelson, Amelia Phillips, et al.

M.Sc. Cybersecurity

III Semester, Paper IV

MSFS304- Security in Cyber Physical Environment

Aim and Objectives of Course: To introduce emerging technological options, platforms, and case studies of IoT implementation in home & city automation (smart homes and cities), Industrial Internet, healthcare, Govt., Mobile Cellular and other areas.

Learning Outcomes:

1. Embedded Systems
2. Embedded firmware design
3. Instruction Set
4. Internet of Things (IoT)

Tools: Arduino kit, Raspberry Pi, Soldering kit.

Unit 1- Introduction to Embedded Systems

Definition of embedded system, embedded systems vs. general computing systems, classification, application areas; Core of the embedded system: general purpose and domain specific processors, ASICs, PLDs, commercial Off-The-Shelf; Memory: ROM, RAM, memory shadowing, memory selection for embedded systems, sensors and actuators; communication interface: onboard and external communication interfaces.

Unit 2- Embedded firmware design

Embedded firmware design, timer, and other attributes; USB bus communication, USB states, USB interface; Ethernet basics; Exchanging messages using UDP and TCP.

Unit 3- Instruction Set

IA32 Instruction Set: application binary interface, exception and interrupt handling, interrupt latency, assemblers, assembler directives, macros, simulation and debugging tools; security algorithm implementation with FPGA.

Unit 4- Internet of Things (IoT)

Introduction, Sensing, Actuation, Basics of Networking, Communication Protocols, Sensor Networks, Machine-to-Machine Communications, Interoperability in IoT

Introduction to Arduino Programming, Integration of Sensors and Actuators with Arduino, Introduction to Raspberry Pi, Implementation of IoT with Raspberry Pi, Fog Computing, Smart Cities and Smart Homes, Connected Vehicles, Smart Grid, Industrial IoT Case Study: Agriculture, Healthcare, Activity Monitoring.

Reference Books

1. Introduction to Embedded Systems – K. V. Shibu [McGraw Hill]
2. Embedded Systems Security-- David Kleidermacher, Mike Kleidermacher [Elsevier]
3. Security in Embedded Devices – C. H. Gebotys [Springer]
4. The Internet of Things: Enabling Technologies, Platforms, and Use Cases", by PethuruRaj and Anupama C. Raman (CRCPress)
5. Internet of Things: A Hands-on Approach, by Arshdeep Bahgaand, Vijay Madisetti (Universities Press)
6. An Embedded Software Primer - David E. Simon [Pearson]
7. Practical Embedded Security – T. Stapko [Newnes]

SEMESTER – III PRACTICALS

MSFS305 – Reverse Engineering and Malware Analysis Lab

1. Set up a Protected Malware Analysis Environment.
2. Perform kernel Debugging with WinDBG.
3. Analyze malicious windows programs such as Windows API, Windows Registry, Networking APIs, etc.
4. Debugging using OllyDbg/IDA Pro and modifying execution with Debugger, Browser script De-Obfuscation.
5. Identifying Covert Malware and working with Santoku.

MSFS306 – Advanced Digital Forensic Analysis Lab

1. Live response using Linux distributions, use of kali Linux, D.E.F.T., SANS SIFT workstation.
2. Collecting volatile data such as Date and time, Network interfaces, Promiscuous mode.
3. Perform various operation on Memory Analysis using memory acquisition forensic tools.
4. Perform Registry analysis with different functions and windows volume shadow copy analysis.
5. Timeline Analysis and file carving, file system image analysis.
6. Forensic copy of mobile device, Logical and Physical analysis
7. Cloud forensic techniques, reviewing cloud trail logs, data collection and analysis techniques.

M.Sc. Cybersecurity

IV Semester, Paper I

MSFS401 – Comprehensive viva-voce

M.Sc. Cybersecurity

IV Semester, Paper II

MSFS402 – PROJECT

ADIKAVI NANNAYA UNIVERSITY: RAJAMAHENDRAVARAM
M.Sc. Cybersecurity
SEMESTER END EXAMINATION
Theory Model Question Paper Pattern: Paper I
MSFS101 Cyber Law and Intellectual Property Rights

Time: 3 hrs **Max. Marks: 75**

Answer all questions. Each question carries 15 marks. **4X15=60**

Section-A

1. a) Explain in detail about IT Rule 2011.

(OR)

b) Discuss the regulations in Cyber space in National and International Level.

2. a) Explain in detail about the Cybersecurity policy 2013.

(OR)

b) Explain about Indian Context of Jurisdiction and IT Act, 2000.

3. a) What does CERT mean? Explain in detail about working of CERT.

(OR)

b)Explain in detail about the Cyber Laws of EU – USA – Australia – Britain.

4. a) What is Corporate Legal Liability, Adjudication Process for Recovery of Losses under I.T. Act,2000

(OR)

b) Describe any one Case Study and Case Law.

Section-B **5X3=15**

5. Answer any FIVE of the following

a. Define the terms: IPC, IEA, CrPC.

b. Write about Indian Penal Code.

c. Explain IPR, COBIT.

d. What is Corporate Legal Liability.

e. What is ISP and describe it.

f. Explain about NPCA, NTRO, NCIIPC.

g. Write about telephone tapping, packet sniffing.

h. Explain about the basics of E-commerce.

M.Sc. Forensic Science

SEMESTER END EXAMINATION

Theory Model Question Paper pattern

MSFS102 Computer Fundamentals **Time: 3 hrs** **Max. Marks: 75**

Section-A

Answer all questions. Each question carries 15 marks. **4x15=60**

1.a) Explain about Data representation of Binary, hex, octal codes with examples.

(OR)

b) Explain the concept of multithreads, Benefits of threads and types of threads.

2. a) Explain about Process states, Process State transitions, Process Control Block.

(OR)

b) Explain Process Scheduling, Scheduling criteria, Scheduling algorithms.

3. a) Write about Paging: Principle of operation and Page allocation.

(OR)

b) Explain in detail about Virtual Memory with examples.

4. a) Explain about Memory allocation and its types.

(OR)

b) Explain about Running and managing processes in the background in Linux.

Section-B **5x3=15**

Answer any five questions

1.) Write about Wireshark.
2.) Explain Context switching.
3.) Explain about OS Structure: Layered, Monolithic, Microkernel.
4.) What is Firewall and Immutable Files.
5.) Write about CPU organization.
6.) Explain about Apache HTTP or Tomcat.
7.) Explain File Integrity check with Tripwire.
8.) What is program execution at CPU level.

M.Sc. Forensic Science
SEMESTER END EXAMINATION
Theory Model Question Paper pattern
MSFS103 Cybersecurity Essentials

Time: 3 hrs **Max. Marks: 75**

Answer all questions. Each question carries 15 marks. **4x15=60**

1.a) Explain about Setting up sudo privileges: for full administrative users, for users with only certain delegated privileges.

(OR)

b) Explain about Preventing name resolution poisoning, Disabling the Web Proxy Autodiscovery Protocol (WPAD)

2. a) Write about comparing Account Logon and Logon Events.

(OR)

b) Explain in detail about exploring DNS Security Issues.

3. a) Write about comparing NTFS and Active Directory Permissions, Assigning Registry Permissions.

(OR)

b) Explain in detail about Auditing a Network with MBSA.

4. a) Explain about Updating Systems with WSUS or SCCM.

(OR)

b) Explain about Cyber-crimes, Ethics, and best practices.

Section-B 5x3=15

Answer any five questions

1.) Write about SSL, VPN.
2.) Explain the dangers of logging in as the root user.
3.) Explain about setting and enforcing password and account expiration.
4.) What is kernel level security .
5.) Write about the differences between physical, virtual, and cloud setups.
6.) Explain about Identifying Active Directory Permissions.
7.) Explain about centralized user management.
8.) How do you manage BitLocker encryption.

M.Sc. Forensic Science
SEMESTER END EXAMINATION
Theory Model Question Paper pattern
MSFS104 Introduction to Programming

Time: 3 hrs **Max. Marks: 75**

Answer all questions. Each question carries 15 marks. **4x15=60**

1.a) Explain about Assembly Language with two example programs.

(OR)

b) Explain the concept of Inheritance and abstraction in C++ with programs.

2. a) Write about functions and recursion in general and explain its syntax with a program.

(OR)

b) Explain in detail about pointers in C with a program.

3. a) Write about arrays in C and C++ with two programs.

(OR)

b) Explain in detail about Object Oriented Programming with examples.

4. a) Explain about Tuples, Lists and Dictionaries with examples.

(OR)

b) Explain about conditional execution and execute a shell script in Linux environment..

Section-B **5x3=15**

Answer any five questions

1.) Write about strings.
2.) Explain the concept of dictionaries.
3.) Explain about conditional statements.
4.) What is a loop? Explain different types of loops.
5.) Write about polymorphism.
6.) Explain about procedural programming language.
7.) Explain about function overloading.
8.) How do you define a constructor.