M.Sc. CS & DF Major Syllabus

Hindi Vidya Prachar Samiti's

Ramniranjan Jhunjhunwala College

of Arts, Science & Commerce

(Empowered Autonomous College)

Affiliated to

UNIVERSITY OF MUMBAI

Program Code: RJSPGCSDF

Syllabus for the

M.Sc Cyber Security & Digital Forensics (under NEP)

New Program to be started from the academic year 2026-2027

M.Sc. CS & DF Major Syllabus

PREAMBLE

1. Why M.Sc. Cyber Security & Digital Forensics?

Cyber Security & Digital Forensics has evolved from an operational discipline into a highly specialized and research-driven domain due to the exponential growth of digital infrastructure, cloud computing, artificial intelligence, Internet of Things (IoT), and cyber–physical systems. Modern societies increasingly rely on complex digital ecosystems, making them vulnerable to sophisticated cyber threats, advanced persistent attacks, digital espionage, cyber warfare, and large-scale data breaches.

At the postgraduate level, Cyber Security focuses on the **design, evaluation, and optimization of advanced security architectures**, cryptographic systems, threat intelligence frameworks, and resilient infrastructures. Digital Forensics, in parallel, emphasizes **scientific investigation**, evidence correlation, incident reconstruction, malware analysis, cloud and mobile forensics, and legal admissibility of digital evidence in complex cyber crime scenarios.

The M.Sc. Cyber Security & Digital Forensics program addresses the growing need for **highly skilled professionals and researchers** who can go beyond tool-based operations to understand attacker behaviour, adversarial techniques, forensic artefacts, and system-level vulnerabilities. The discipline requires advanced analytical reasoning, research aptitude, ethical judgment, and a strong understanding of legal and regulatory frameworks.

With the rapid escalation of ransomware campaigns, nation-state cyber operations, financial cyber-crimes, and digital frauds, organizations increasingly demand **postgraduate-level expertise** capable of handling advanced investigations, security strategy formulation, and innovation-driven problem solving. The M.Sc. program is therefore designed to produce graduates who can operate effectively in **industry, government, law enforcement, research laboratories, and doctoral research environments**.

2. Why M.Sc. Cyber Security & Digital Forensics at R J College?

The introduction of the **M.Sc. Cyber Security & Digital Forensics** program at **Hindi Vidya Prachar Samiti's Ramniranjan Jhunjhunwala College of Arts, Science & Commerce (Empowered Autonomous College)** reflects a strategic academic initiative to address the evolving demands of advanced cyber education and research.

As an empowered autonomous institution, the college possesses the academic freedom to design a **rigorous, contemporary, and industry-aligned postgraduate curriculum**, fully compliant with **NEP 2020**. The program is conceptualized with a strong emphasis on **advanced specialization, research orientation, and industry relevance**, ensuring that graduates acquire both depth and breadth in cyber security and digital forensics.

The department is being developed with a focus on:

- Advanced cyber security and digital forensics laboratories equipped with modern computing infrastructure and professional-grade tools
- Emphasis on **hands-on experimentation, simulations, forensic investigations, and adversarial analysis**
- Integration of **research methodology, case studies, incident simulations, and real-world cyber-crime scenarios**
- Strong grounding in **ethical conduct, cyber laws, digital evidence handling, and professional responsibility**
- Alignment with **industry certifications, higher education pathways, and doctoral research preparation**

Being a newly established postgraduate program allows the curriculum to be developed without legacy limitations, ensuring that course content, laboratory design, assessment strategies, and internship components reflect **current global practices** in cyber security, DFIR, malware analysis, and forensic science.

3. Our Curriculum, Our Strength

The **M.Sc. Cyber Security & Digital Forensics curriculum**, structured under **NEP 2020**, is designed to deliver **advanced theoretical knowledge, applied technical skills, and research competence** across four semesters.

In the initial phase, the curriculum focuses on strengthening students' expertise in **advanced cryptographic systems, digital forensic methodologies, network threat detection, adversarial tactics, and research methodology**. As students' progress, the program introduces specialized domains such as **malware reverse engineering, incident response and DFIR, cloud security and forensics, AI-driven threat detection, blockchain forensics, IoT and mobile forensics, and post-quantum cryptography**.

A defining strength of the curriculum lies in its **tight integration of advanced theory, laboratory-intensive practice, research exposure, and industry engagement**. Each semester incorporates substantial practical components, enabling students to apply theoretical concepts to realistic cyber incidents, forensic investigations, and security challenges. The inclusion of **on-job training / industry internship** further strengthens professional readiness and experiential learning.

The curriculum also emphasizes **research skills, academic writing, ethics, legal compliance, and societal responsibility**, ensuring that graduates are not only technically competent but also ethically grounded and legally aware. By the completion of the program, students are expected to demonstrate **advanced problem-solving ability, investigative rigor, research aptitude, and professional confidence**, enabling them to excel in cyber security operations, digital forensic investigations, research roles, policy formulation, or doctoral studies.

PROGRAM OUTCOMES OF GENERAL POST GRADUATE DEGREE PROGRAMS

Students of all Post graduate degree program on completion of the program will be able to –

Convey the concept clearly

Students would have clarity and complete domain knowledge. Shall be able to analyze solve, innovate and convey the concept clearly by utilizing effective communication skills

Social Interaction

Respect each other and should be able to resolve conflicts and help in reaching an amicable solution. They should be able to work in diverse teams. They should be able to distinguish when and what is socially acceptable. Students would perform functions that demand higher competence in national/international organizations with positive spirit and cooperate with peer. Provide leadership and be mentors.

Responsible citizen

Contribute to Nation development through social service. Being empathetic and sympathetic to fellow beings.

Honesty and Integrity, Ethics

Recognize different values and systems and respect them. In decision making moral values should be given prime importance. Students should be aware of ethical issues and regulatory considerations while addressing society needs for growth with honesty.

Environmental and Sustainability

Environmental issues would be considered and problem solving with sustainable development would be chosen.

Lifelong learning and Global thinking

Enjoy learning in every situation and should have skills for adapting in any part of the world and contribute to nation building globally.

PROGRAM SPECIFIC OUTCOMES (PSO)

PSO1 – Advanced Cyber Security Expertise

Graduates will be able to design, analyze, and evaluate advanced cyber security mechanisms, cryptographic systems, forensic methodologies, and secure infrastructures to solve complex real-world security problems.

PSO2 – Digital Forensics & Incident Investigation Skills

Graduates will demonstrate professional competence in digital evidence acquisition, forensic analysis, incident response, cyber-crime investigation, and legal admissibility of digital evidence.

PSO3 – Industry & Research Readiness

Graduates will apply research methods, tools, and emerging technologies to innovate, adapt, and contribute effectively in industry, government, law enforcement, or doctoral research environments.

PSO4 – Ethical, Legal & Social Responsibility

Graduates will practice cyber security and digital forensics with integrity, ethical responsibility, legal compliance, and sensitivity to societal, environmental, and global concerns.

M.Sc. CS & DF Major Syllabus

CREDIT STRUCTURE

Credit Structure for M.Sc. Semester-I as per NEP 2020 To be implemented from the academic year 2026-2027

Papers	Number of Papers	Credits	Total Credits
Major Mandatory Theory	2	3	6
	1	2	2
Major Mandatory Practical	3	2	6
Major Elective Theory	1 – Elective I or Elective II	2	2
Major Elective Practical	1 – Elective I or Elective II	2	2
Other Elective	1	4	4
Total			22

Credit Structure for M.Sc. Semester-II as per NEP 2020 To be implemented from the academic year 2026-2027

Papers	Number of Papers	Credits	Total Credits
Major Mandatory Theory	2	3	6
	1	2	2
Major Mandatory Practical	3	2	6
Major Elective Theory	1 – Elective I or Elective II	2	2
Major Elective Practical	1 – Elective I or Elective II	2	2
On-Job Training	1	4	4
Total			22

M.Sc. CS & DF Major Syllabus

Semester I – Course Titles & Codes

Course Code	Course Title	Credits
RJSPGCSDF101	Advanced Cryptographic Systems & Secure Protocols (Major Mandatory Theory)	3
RJSPGCSDF102	Advanced Digital Forensics Techniques & Evidence Correlation (Major Mandatory Theory)	3
RJSPGCSDF103	Network Threat Detection, Attack Surface & Adversarial Tactics (Major Mandatory Theory)	2
RJSPGCSDF101P	Cryptographic Systems Implementation & Analysis Lab	2
RJSPGCSDF102P	Advanced Digital Forensics & Evidence Analysis Lab	2
RJSPGCSDF103P	Network Threat Detection & Security Analytics Lab	2
RJSPGCSDFE101	Blockchain Security & Distributed Ledger Forensics (Major Elective Theory – I)	2
RJSPGCSDFE101P	Blockchain Forensics & Smart Contract Analysis Lab	2
OR		
RJSPGCSDFE102	AI & Machine Learning for Cyber Threat Detection (Major Elective Theory – II)	2
RJSPGCSDFE102P	AI-Driven Threat Detection & Modelling Lab	2
RJSPGCSDFOEC101	Research Methodology, Academic Writing & Research Ethics	4
Total		22

Semester II – Course Titles & Codes

Course Code	Course Title	Credits
RJSPGCSDF201	Malware Reverse Engineering & Exploit Analysis (Major Mandatory Theory)	3
RJSPGCSDF202	Incident Response, DFIR & Cyber Crime Investigation (Major Mandatory Theory)	3
RJSPGCSDF203	Cloud Security Architecture & Cloud Forensics (Major Mandatory Theory)	2
RJSPGCSDF201P	Malware Analysis, Debugging & Reverse Engineering Lab	2
RJSPGCSDF202P	Incident Response & Digital Investigation Simulation Lab	2
RJSPGCSDF203P	Cloud Security & Cloud Forensics Lab	2
RJSPGCSDFE201	IoT & Mobile Device Forensics (Major Elective Theory – I)	2
RJSPGCSDFE201P	IoT & Mobile Forensics Lab	2
OR		
RJSPGCSDFE202	Post-Quantum & Quantum Cryptography (Major Elective Theory – II)	2
RJSPGCSDFE202P	Quantum-Resistant Cryptography & Security Lab	2
RJSPGCSDFOJT201	Industry Internship in Cyber Security / DFIR / SOC Operations	4
Total		22

Syllabus Grid – M.Sc. Cyber Security & Digital Forensics (Part I)

Level	Semester	Major (Mandatory)	Major (Elective)	Minor	OE	VSC / SEC	AEC, VEC, IKS	OJT/ FP/ CEP/ CC/ RP	Cum. Credits per Semester	Degree / Cum. Credits
PG	I	Advanced Cryptographic Systems & Secure Protocols (3+2) Advanced Digital Forensics Techniques & Evidence Correlation (3+2) Network Threat Detection, Attack Surface & Adversarial Tactics (2+2)	Elective I: Blockchain Security & Distributed Ledger Forensics (2+2) OR AI & Machine Learning for Cyber Threat Detection (2+2)	—	Research Methodology, Academic Writing & Research Ethics (4)	—	—	—	22	
PG	II	Malware Reverse Engineering & Exploit Analysis (3) Incident Response, DFIR & Cyber Crime Investigation (3) Cloud Security Architecture & Cloud Forensics (2)	Elective II: IoT & Mobile Device Forensics (2) OR Post-Quantum & Quantum Cryptography (2)	—	—	—	—	OJT	22	
										44

SEMESTER I

Course Code	RJSPGCSDF101
Course Title	Cryptographic Algorithms & Applications
Credits	3
Duration	45 Hours

Course Objectives

Sr. No.	Course Objective
1	To understand modern cryptographic algorithms used in secure systems
2	To study public key cryptography and digital trust infrastructures
3	To analyze cryptographic protocols used in real-world applications
4	To evaluate cryptographic vulnerabilities and security issues
5	To apply cryptographic techniques in network and cloud environments

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Symmetric Key Cryptography & Key Management: AES algorithm structure, AES key sizes (128/192/256), block cipher modes (ECB limitations, CBC, CTR, GCM), authenticated encryption, stream ciphers overview (ChaCha20), key generation methods (true random number generators – TRNG, cryptographically secure pseudo-random number generators – CSPRNG), key derivation functions (PBKDF2, bcrypt, scrypt), key management techniques (key storage, key rotation, key escrow, key destruction), introduction to Hardware Security Modules (HSM) and Trusted Platform Module (TPM)	15
Unit II	Public Key Cryptography & Trust Models: RSA key generation and security considerations, elliptic curve cryptography (ECC) fundamentals, Diffie–Hellman and ECDH key exchange, digital signature schemes (RSA, ECDSA), cryptographic hash functions (SHA-2, SHA-3), Message Authentication Codes (HMAC), Public Key Infrastructure (PKI), X.509 certificate structure, certificate issuance, revocation (CRL, OCSP), enterprise trust models	15
Unit III	Applied Cryptography & Secure Protocols: TLS/SSL architecture and handshake process, cipher suite selection, cryptographic failures and misconfigurations, secure email mechanisms (PGP, S/MIME), cryptography in cloud security (encryption at rest and in transit), key management services (KMS – conceptual overview), cryptographic compliance standards (NIST, ISO/IEC 27001 controls)	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain modern cryptographic algorithms and key management concepts	Understand	PSO1
CO2	Analyze public key systems and digital trust models	Analyze	PSO1
CO3	Apply cryptographic mechanisms in secure communications	Apply	PSO1, PSO3
CO4	Evaluate cryptographic protocols and security issues	Evaluate	PSO1
CO5	Select appropriate cryptographic solutions for enterprise applications	Create	PSO1, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Cryptography and Network Security	William Stallings
2	Serious Cryptography	Jean-Philippe Aumasson
3	Applied Cryptography	Bruce Schneier
4	NIST SP 800-56, 800-57, 800-132	NIST Publications
5	IEEE Security & Privacy Journal	IEEE

Course Code	RJSPGCSDF102
Course Title	Advanced Digital Forensics Techniques
Credits	3
Duration	45 Hours

Course Objectives

Sr. No.	Course Objective
1	To develop advanced understanding of digital forensic investigation processes
2	To study file system, memory, and log-based forensic analysis techniques
3	To correlate digital evidence from multiple sources
4	To understand legal admissibility and forensic reporting standards
5	To apply forensic techniques to complex cyber crime investigations

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Advanced Forensic Foundations & File System Analysis: Digital forensic investigation models, forensic readiness, evidence identification and classification, forensic imaging methods (bit-stream imaging, live vs dead acquisition), hashing algorithms for integrity verification (MD5, SHA-1, SHA-256 – usage only), advanced file system forensics (NTFS, EXT4 structures, metadata, timestamps, journaling), deleted file recovery concepts, slack space and unallocated space analysis	15
Unit II	Memory, Log & System Artifact Forensics: Volatile memory forensics concepts, memory acquisition techniques, analysis of running processes and loaded modules, Windows Registry forensics (hives, keys, artifacts), system log analysis (event logs, application logs), browser and email artifact analysis, introduction to anti-forensics techniques (data hiding, timestamp manipulation, secure deletion)	15
Unit III	Evidence Correlation, Timeline Analysis & Legal Aspects: Timeline creation and event reconstruction, multi-source evidence correlation (disk, memory, logs, network), forensic case documentation, chain of custody, forensic reporting structure, expert witness responsibilities, legal admissibility of digital evidence (Indian IT Act overview), challenges in cloud and distributed forensic investigations	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain advanced digital forensic investigation processes	Understand	PSO2
CO2	Analyze file systems, memory, and system artifacts	Analyze	PSO2
CO3	Apply forensic techniques to investigate cyber incidents	Apply	PSO2, PSO3
CO4	Evaluate digital evidence for legal admissibility	Evaluate	PSO4
CO5	Prepare structured forensic reports for investigations	Create	PSO2, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Digital Evidence and Computer Crime	Eoghan Casey
2	File System Forensic Analysis	Brian Carrier
3	The Practice of Network Security Monitoring (selected forensic chapters)	Richard Bejtlich
4	NIST SP 800-86 – Guide to Integrating Forensic Techniques	NIST
5	Journal of Digital Forensics, Security & Law	Standard Journal

Course Code	**RJSPGCSDF103**
Course Title	**Network Threat Detection & Attack Surface Analysis**
Credits	**2**
Duration	**30 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand modern network-based cyber threats and attack patterns
2	To study methods for identifying and analyzing attack surfaces
3	To analyze network traffic for threat detection
4	To understand threat modeling frameworks used in industry
5	To apply network threat detection concepts in enterprise environments

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Network Threat Landscape & Attack Surface Analysis: Modern network threat landscape, types of network-based attacks (scanning, sniffing, spoofing, DoS/DDoS, lateral movement), concept of attack surface, internal vs external attack surface, asset identification and classification, network exposure points, introduction to threat modeling, STRIDE threat model, MITRE ATT&CK framework (network-related techniques), mapping threats to attack surfaces	15
Unit II	Network Threat Detection Techniques: Network traffic fundamentals for security analysis, signature-based detection concepts, anomaly-based detection concepts, intrusion detection and prevention systems (IDS/IPS), flow-based monitoring, behavioral analysis, basics of detection engineering, log and alert correlation concepts, limitations of network-based detection, ethical and legal considerations in network monitoring	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain modern network threats and attack surfaces	Understand	PSO1
CO2	Analyze network attack patterns using threat models	Analyze	PSO1
CO3	Apply network threat detection concepts to enterprise networks	Apply	PSO1, PSO3
CO4	Evaluate effectiveness of different detection techniques	Evaluate	PSO1
CO5	Identify and document attack surfaces for given network scenarios	Create	PSO1, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Network Security Essentials	William Stallings
2	The Practice of Network Security Monitoring	Richard Bejtlich
3	MITRE ATT&CK Framework Documentation	MITRE
4	NIST SP 800-94 – Intrusion Detection and Prevention Systems	NIST
5	IEEE Security & Privacy Journal	IEEE

Course Code	**RJSPGCSDF101P**
Course Title	**Cryptographic Systems Implementation & Analysis Lab**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To implement cryptographic algorithms using standard libraries and tools
2	To analyze the behavior and security of cryptographic systems
3	To understand practical aspects of key generation and management
4	To evaluate cryptographic protocols through experimentation
5	To develop secure cryptographic solutions for real-world applications

Practical Assignments

Indicative Tools (not restrictive):
OpenSSL, Python (cryptography / PyCrypto), Wireshark, Hash utilities

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Symmetric Encryption – AES	Implement AES encryption and decryption using different key sizes; observe output
2	AES Modes of Operation	Compare CBC, CTR, and GCM modes with respect to security and performance
3	Secure Random Number Generation	Generate cryptographic keys using CSPRNG; analyze randomness
4	Key Derivation Functions	Implement PBKDF2 / bcrypt for password-based key derivation
5	Asymmetric Key Generation	Generate RSA and ECC key pairs; compare key sizes and strength

6	Digital Signatures	Create and verify digital signatures using RSA/ECDSA
7	Hash Functions	Implement SHA-256 and SHA-3 for data integrity verification
8	Message Authentication Codes	Implement HMAC for message authentication
9	Public Key Infrastructure	Create a simple CA, issue and verify digital certificates
10	TLS Traffic Analysis	Capture and analyze TLS handshake using Wireshark
11	Secure File Storage	Design encrypted file storage using symmetric encryption
12	Key Management Practices	Demonstrate key storage, rotation, and revocation concepts
13	Cryptographic Attack Demo	Demonstrate replay or weak-key attack (controlled setup)
14	Case Study Analysis	Analyze a real-world cryptographic failure scenario
15	Mini Project	Design and implement a secure cryptographic communication module

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Implement cryptographic algorithms using standard tools	Apply	PSO1
CO2	Analyze cryptographic behavior and security properties	Analyze	PSO1
CO3	Apply key generation and management techniques	Apply	PSO1, PSO3
CO4	Evaluate cryptographic protocols through experimentation	Evaluate	PSO1
CO5	Develop secure cryptographic solutions for applications		

Course Code	**RJSPGCSDF102P**
Course Title	**Advanced Digital Forensics & Evidence Analysis Lab**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To perform advanced digital evidence acquisition and analysis

2	To analyze file system, memory, and system artifacts using forensic tools
3	To correlate digital evidence from multiple forensic sources
4	To maintain forensic integrity and legal admissibility of evidence
5	To prepare professional forensic analysis reports

Practical Assignments

Indicative Tools (not restrictive):
Autopsy, FTK Imager, EnCase (demo), Volatility, Registry Explorer, Plaso, HashCalc

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Forensic Image Acquisition	Create forensic disk images using FTK Imager; generate and verify hashes
2	Evidence Integrity Verification	Verify integrity of acquired images using MD5/SHA-256
3	File System Artifact Analysis	Analyze NTFS/EXT file system metadata and timestamps
4	Deleted Data Recovery	Recover deleted files and document findings
5	Unallocated & Slack Space Analysis	Identify artifacts in unallocated and slack space
6	Memory Acquisition	Acquire volatile memory image in a controlled environment
7	Memory Analysis	Analyze processes and loaded modules using Volatility
8	Windows Registry Analysis	Examine registry hives for user and system activity
9	System Log Analysis	Analyze event logs and application logs
10	Browser Forensics	Extract and analyze browser artifacts
11	Email Evidence Analysis	Examine email headers and message content
12	Timeline Construction	Build a system activity timeline using Plaso
13	Anti-Forensics Detection	Detect signs of wiping, obfuscation, or timestamp tampering
14	Evidence Correlation	Correlate disk, memory, and log artifacts
15	Forensic Case Report	Prepare a structured, court-admissible forensic report

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Perform forensic acquisition while preserving evidence integrity	Apply	PSO2
CO2	Analyze digital artifacts using advanced forensic tools	Analyze	PSO2
CO3	Correlate evidence from multiple forensic sources	Analyze	PSO2, PSO3
CO4	Evaluate forensic findings for investigative relevance	Evaluate	PSO2

CO5	Produce professional forensic analysis reports	Create	PSO2, PSO4

Course Code	**RJSPGCSDF103P**
Course Title	**Network Security Lab**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To develop practical skills in network traffic analysis for security purposes
2	To identify and analyze network-based attacks
3	To apply threat detection techniques in simulated environments
4	To understand IDS/IPS deployment and alert analysis
5	To correlate network events with attack scenarios

Practical Assignments

Indicative Tools:
Wireshark, tcpdump, Snort / Suricata, Zeek, Nmap, OpenVAS (demo), SIEM (conceptual)

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Network Traffic Capture	Capture live network traffic using Wireshark/tcpdump and identify basic protocols
2	Packet Analysis	Analyze TCP, UDP, ICMP packets and identify anomalies
3	Network Scanning	Perform network scanning using Nmap and document exposed services
4	Attack Surface Identification	Identify internal and external attack surfaces from scan results
5	ARP & Spoofing Analysis	Observe and analyze ARP spoofing behavior in a controlled setup
6	DoS/DDoS Traffic Analysis	Analyze traffic patterns of DoS/DDoS attacks (pcap-based)
7	IDS Setup	Install and configure Snort/Suricata with basic rules
8	Signature-Based Detection	Detect known attacks using IDS signatures
9	Anomaly Detection	Identify abnormal traffic behavior using flow statistics
10	MITRE ATT&CK Mapping	Map detected network attacks to MITRE ATT&CK techniques
11	Log Analysis	Analyze Zeek logs for suspicious activity
12	Alert Correlation	Correlate IDS alerts with traffic captures

13	False Positive Analysis	Identify and explain false positives in IDS alerts
14	Case-Based Network Incident	Analyze a given network breach scenario
15	Mini Project	End-to-end network threat detection report with findings

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Capture and analyze network traffic for security analysis	Apply	PSO1
CO2	Identify network-based attacks using practical tools	Analyze	PSO1
CO3	Deploy and evaluate IDS for threat detection	Apply	PSO1, PSO3
CO4	Correlate network events with attack techniques	Analyze	PSO1
CO5	Prepare structured reports for network security incidents	Create	PSO1, PSO4

Course Code	**RJSPGCSDFE101**
Course Title	**Blockchain Security & Forensics**
Credits	**2**
Duration	**30 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand blockchain architecture from a security perspective
2	To study security mechanisms used in blockchain systems
3	To analyze vulnerabilities and attacks on blockchain platforms
4	To understand forensic investigation techniques for blockchain-based crimes
5	To apply blockchain forensic concepts in cyber crime investigation

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Blockchain Architecture & Security Foundations: Distributed ledger concepts, blockchain data structures (blocks, hashes, Merkle trees), consensus mechanisms (PoW, PoS – security view), cryptographic primitives in blockchain (hashing, digital signatures), wallet security (hot vs cold wallets), identity and key management in blockchain systems, overview of popular blockchain platforms (Bitcoin, Ethereum)	15

Unit II	Blockchain Attacks, Security Issues & Forensics: Blockchain threat landscape, double-spending attacks, 51% attack, Sybil attack, smart contract vulnerabilities (reentrancy, integer overflow – concept level), transaction analysis and tracing, blockchain forensic methodologies, evidence collection from blockchain explorers, legal and regulatory challenges in blockchain investigations	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain blockchain architecture and security mechanisms	Understand	PSO1
CO2	Analyze vulnerabilities and attacks in blockchain systems	Analyze	PSO1
CO3	Apply forensic techniques to investigate blockchain transactions	Apply	PSO2, PSO3
CO4	Evaluate blockchain security incidents from a forensic perspective	Evaluate	PSO2
CO5	Identify legal and regulatory issues in blockchain investigations	Create	PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Blockchain Basics	Daniel Drescher
2	Mastering Blockchain	Imran Bashir
3	Hands-On Smart Contract Development	Zubin Shah
4	NIST IR 8425 – Blockchain Technology Overview	NIST
5	IEEE Blockchain, ACM Distributed Ledger Journals	Journals

Course Code	**RJSPGCSDFE101P**
Course Title	**Blockchain Forensics Lab**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To analyze blockchain transactions using forensic techniques
2	To trace cryptocurrency movement and identify suspicious activity
3	To understand wallet, address, and smart contract analysis
4	To collect and preserve blockchain-based digital evidence
5	To prepare forensic reports for blockchain-related cyber crimes

Practical Assignments

Indicative Tools (not restrictive):
Blockchain Explorers (Bitcoin, Ethereum), Remix IDE, Ganache, MetaMask, Blockchair, Etherscan

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Blockchain Explorer Familiarization	Explore Bitcoin/Ethereum blockchain using public explorers; understand blocks and transactions
2	Transaction Analysis	Analyze a given blockchain transaction: inputs, outputs, fees, confirmations
3	Address & Wallet Analysis	Examine wallet addresses and transaction history
4	Cryptocurrency Flow Tracing	Trace fund movement across multiple addresses
5	Identification of Suspicious Patterns	Identify mixing, repeated transfers, or abnormal transaction behavior
6	Smart Contract Deployment	Deploy a basic smart contract using Remix and Ganache
7	Smart Contract Interaction	Invoke smart contract functions and analyze transactions
8	Smart Contract Vulnerability Observation	Observe reentrancy or logic flaw using sample vulnerable contracts
9	Token Transaction Analysis	Analyze ERC-20 token transfers using Etherscan
10	NFT Transaction Analysis	Examine NFT minting and ownership transfer records
11	Evidence Collection	Collect transaction data and screenshots as forensic evidence
12	Timestamp & Block Analysis	Analyze timestamps and block confirmations
13	Case Study – Crypto Scam	Investigate a simulated cryptocurrency scam scenario
14	Legal Documentation	Document findings suitable for legal or investigative use
15	Mini Project	End-to-end blockchain forensic investigation and report

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Analyze blockchain transactions using forensic tools	Analyze	PSO2
CO2	Trace cryptocurrency movement across addresses	Apply	PSO2, PSO3
CO3	Examine smart contract activity for forensic evidence	Analyze	PSO2

CO4	Collect and preserve blockchain-based digital evidence	Apply	PSO2, PSO4
CO5	Prepare structured forensic reports for blockchain cases	Create	PSO2, PSO4

Course Code	**RJSPGCSDFE102**
Course Title	**AI in Cyber Threat Detection**
Credits	**2**
Duration	**30 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand the role of Artificial Intelligence in cyber security
2	To study machine learning techniques used for threat detection
3	To analyze AI-based detection of network and system anomalies
4	To evaluate advantages and limitations of AI-driven security systems
5	To apply AI concepts to real-world cyber threat detection scenarios

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Foundations of AI for Cyber Security: Overview of AI and machine learning in cyber security, supervised vs unsupervised learning (security context), feature extraction for cyber data, datasets used in cyber security (network traffic, logs, malware features), anomaly detection concepts, classification vs clustering for threat detection, evaluation metrics (accuracy, precision, recall, false positives/negatives), challenges of applying AI in security	15
Unit II	AI-based Threat Detection Techniques & Applications: Machine learning algorithms for intrusion detection (decision trees, SVM, k-NN – concept level), anomaly detection using clustering and statistical methods, AI-based malware detection overview, behavior-based threat detection, AI for phishing and spam detection, limitations of AI systems (adversarial ML, data poisoning), ethical and legal considerations in AI-driven security systems	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain AI and ML concepts used in cyber threat detection	Understand	PSO1
CO2	Analyze cyber threats using AI-based detection approaches	Analyze	PSO1

CO3	Apply AI concepts to detect anomalies and attacks	Apply	PSO1, PSO3
CO4	Evaluate effectiveness and limitations of AI-driven security systems	Evaluate	PSO1
CO5	Select suitable AI techniques for cyber threat detection problems	Create	PSO1, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Machine Learning and Security	Clarence Chio, David Freeman
2	Hands-On Machine Learning for Cybersecurity	Sundaramurthy et al.
3	Artificial Intelligence for Cybersecurity	Chaudhary & Saxena
4	NIST AI Risk Management Framework	NIST
5	IEEE Transactions on Information Forensics & Security	Journal

Course Code	**RJSPGCSDFE102P**
Course Title	**AI Threat Modeling Lab**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To apply AI and machine learning concepts for cyber threat detection
2	To perform feature extraction from cyber security datasets
3	To implement basic AI models for anomaly and attack detection
4	To analyze performance of AI-based security models
5	To understand ethical and practical limitations of AI in cyber security

Practical Assignments

Indicative Tools (not restrictive):
Python, Scikit-learn, Pandas, Jupyter Notebook, CICIDS Dataset / NSL-KDD (sampled), basic SIEM logs (CSV)

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Cyber Security Dataset Exploration	Explore network/log dataset; understand features and labels
2	Data Preprocessing	Handle missing values, normalization, and encoding
3	Feature Selection	Identify relevant features for threat detection

4	Supervised Learning – Classification	Implement a basic classifier (Decision Tree / k-NN)
5	Model Evaluation	Evaluate model using accuracy, precision, recall
6	Unsupervised Learning – Anomaly Detection	Apply clustering or statistical anomaly detection
7	Intrusion Detection Simulation	Detect malicious vs normal traffic in dataset
8	Malware Feature Analysis	Analyze malware feature dataset (conceptual)
9	Behavioral Analysis	Detect abnormal user or system behavior
10	False Positive Analysis	Analyze causes of false alerts
11	Adversarial Awareness	Observe impact of noisy or poisoned data
12	Ethical Considerations	Discuss bias, privacy, and transparency issues
13	Threat Modeling with AI	Map AI detection results to threat scenarios
14	Case Study	Analyze a real-world AI-based security solution
15	Mini Project	Design a basic AI-driven threat detection model and report

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Prepare and preprocess cyber security datasets	Apply	PSO1
CO2	Implement AI models for threat detection	Apply	PSO1, PSO3
CO3	Analyze AI-based detection results	Analyze	PSO1
CO4	Evaluate performance and limitations of AI models	Evaluate	PSO1, PSO4
CO5	Design a basic AI-driven threat detection solution	Create	PSO1, PSO3

Course Code	**RJSPGCSDFOEC101**
Course Title	**Research Methodology & Academic Writing**
Credits	**4**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand the fundamentals of research methodology and scientific inquiry
2	To develop skills in problem identification and research design

3	To train students in literature review and academic writing
4	To prepare students for research paper writing and publication
5	To familiarize students with modern digital tools and AI for research and presentation

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Introduction to Research: Meaning and definition of research, purpose of research, scientific method, positivist and post-positivist approaches to research, types of research, beginning stages of research process, problem definition, qualitative research, quantitative research, primary and secondary data research. Business Research: Role of business research, information systems and knowledge management, theory building, organizational ethics and issues in research.	15
Unit II	Research Methods and Data Collection: Survey research, communicating with respondents, observation methods, descriptive and experimental research types, inductive and deductive approach, action research, steps in research process. Formulation of Research Problem: Problem selection, literature review, formulation of hypothesis. Variables: Dependent, independent, and intervening variables.	15
Unit III	Data Collection and Sampling: Probability sampling, non-probability sampling, survey method, contact methods, questionnaire design. Selection of Project Domain: Publication ethics, research tools and evaluation. Literature Survey: Selection of tentative project area, literature survey components and procedures. Research Paper Basics: Components of a research paper, journal types, indexing databases (Scopus, Web of Science, Science Citation Index), H-index, Google Scholar citations.	15
Unit IV	Research Paper Writing, Publishing & Presentation (Enhanced Unit): Title selection, paragraph writing, report and paper structure, methodology and result presentation, conclusion writing, diagrams, tables and equations, citation styles, plagiarism and similarity index, paper formatting as per journal/conference guidelines, scopus indexed journals vs predatory journals, DOI/ISBN and publication process, research ethics. Modern Tools & Technologies: Use of digital libraries, reference managers (Mendeley, Zotero), plagiarism detection tools, LaTeX for paper writing, AI tools for literature summarization, grammar support and reference assistance (ethical use only). Research Presentation: Preparation of research paper presentation (PPT/poster), oral presentation techniques, seminar presentation on selected project proposal, attending invited expert talks, practical orientation in searching and collecting literature using online tools and libraries.	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped

CO1	Explain research concepts, methodologies, and ethics	Understand	PSO3
CO2	Analyze research problems using appropriate methods	Analyze	PSO3
CO3	Apply literature review and academic writing techniques	Apply	PSO3
CO4	Evaluate journals, conferences, and publication practices	Evaluate	PSO4
CO5	Prepare, present, and submit a research paper using modern tools responsibly	Create	PSO3, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Research Methodology: Methods and Techniques	C. R. Kothari
2	How to Write and Publish a Scientific Paper	Robert A. Day
3	Writing for Computer Science	Justin Zobel
4	IEEE Author Guidelines & Publication Ethics	IEEE
5	Elsevier Researcher Academy / Springer Author Resources	Online

SEMESTER II

Course Code	**RJSPGCSDF201**
Course Title	**Malware Reverse Engineering**
Credits	**3**
Duration	**45 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand the structure and behavior of modern malware
2	To study static and dynamic malware analysis techniques
3	To analyze malware execution, persistence, and evasion mechanisms
4	To understand reverse engineering tools and methodologies
5	To develop analytical skills for malware investigation and reporting

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Malware Fundamentals & Classification: Malware definition and evolution, malware lifecycle, classification of malware (viruses, worms, Trojans, ransomware, spyware, rootkits), malware delivery mechanisms, command-and-control (C2) concepts, indicators of compromise (IOC), ethical and legal considerations in malware analysis	15

Unit II	Static Malware Analysis Techniques: Static analysis methodology, malware file formats (PE file structure overview), hashing and signature-based detection, string analysis, entropy analysis, disassembly concepts, use of static analysis tools, limitations of static analysis, packed and obfuscated malware (conceptual understanding)	15
Unit III	Dynamic & Behavioral Malware Analysis: Dynamic analysis environment setup (sandbox concepts), monitoring system calls and processes, registry and file system changes, network behavior analysis, malware persistence techniques, evasion and anti-analysis techniques, documenting malware behavior and analysis findings	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain malware types, lifecycle, and infection mechanisms	Understand	PSO1
CO2	Analyze malware using static analysis techniques	Analyze	PSO1
CO3	Analyze malware behavior using dynamic analysis	Analyze	PSO1, PSO3
CO4	Evaluate malware persistence and evasion techniques	Evaluate	PSO1
CO5	Document and report malware analysis findings professionally	Create	PSO3, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Practical Malware Analysis	Michael Sikorski & Andrew Honig
2	Malware Analyst's Cookbook	Michael Hale Ligh et al.
3	The Art of Memory Forensics (selected chapters)	Michael Hale Ligh
4	NIST SP 800-83 – Malware Incident Prevention	NIST
5	Journal of Computer Virology & Hacking Techniques	Journal

Course Code: RJSPGCSDF202

Course Title: Incident Response & Digital Investigation

Credits: 3

Duration: 45 Hours

Course Objectives

M.Sc. CS & DF Major Syllabus

Sr. No.	Course Objective
1	To understand structured incident response processes used in industry
2	To study techniques for detecting, containing, and eradicating cyber incidents
3	To integrate digital forensic methods into incident response
4	To analyze cyber crime incidents from investigation and legal perspectives
5	To prepare professional incident response and investigation reports

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Incident Response Foundations & Frameworks: Definition and types of cyber incidents, incident response lifecycle (preparation, identification, containment, eradication, recovery, lessons learned), roles and responsibilities of incident response teams, incident classification and prioritization, incident response policies and playbooks, coordination with management and stakeholders, overview of industry frameworks (NIST Incident Response Lifecycle, ISO/IEC 27035)	15
Unit II	Incident Detection, Analysis & Containment: Incident detection sources (logs, alerts, IDS/IPS, SIEM), triage and incident validation, evidence preservation during incidents, short-term and long-term containment strategies, system isolation techniques, root cause analysis, integrating forensic data during live incidents, challenges in handling large-scale and cloud-based incidents	15
Unit III	Digital Investigation, Reporting & Legal Aspects: Cyber crime investigation process, integration of digital forensics with incident response, timeline reconstruction during investigations, documentation and incident reporting standards, communication with law enforcement and legal teams, overview of cyber laws relevant to incident investigation (Indian IT Act – conceptual), post-incident review and improvement, ethical considerations in incident handling	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain incident response processes and frameworks	Understand	PSO2
CO2	Analyze cyber incidents using structured response techniques	Analyze	PSO2
CO3	Apply digital investigation methods during incident handling	Apply	PSO2, PSO3
CO4	Evaluate incident response effectiveness and legal implications	Evaluate	PSO4
CO5	Prepare professional incident response and investigation reports	Create	PSO3, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Incident Response & Computer Forensics	Jason T. Luttgens et al.
2	The Practice of Incident Response	O'Reilly Media
3	Computer Security Incident Handling Guide (SP 800-61)	NIST
4	ISO/IEC 27035 – Information Security Incident Management	ISO
5	CERT-In Incident Handling Guidelines	Government of India

Course Code	**RJSPGCSDF203**
Course Title	**Cloud Security Architectures**
Credits	**2**
Duration	**30 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand cloud computing architectures from a security perspective
2	To study security models and shared responsibility in cloud environments
3	To analyze threats, risks, and controls specific to cloud platforms
4	To understand data protection, identity, and access management in the cloud
5	To apply cloud security concepts in enterprise and forensic contexts

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Cloud Architecture & Security Foundations: Cloud service models (IaaS, PaaS, SaaS) from a security viewpoint, cloud deployment models (public, private, hybrid, multi-cloud), shared responsibility model, cloud threat landscape, virtualization and container security concepts, identity and access management (IAM) fundamentals, authentication and authorization in cloud environments, security considerations in cloud networking	15
Unit II	Cloud Security Controls, Data Protection & Compliance: Data security in the cloud (encryption at rest and in transit), key management concepts and cloud KMS overview, secure storage and backup strategies, logging and monitoring in cloud environments, incident response in cloud platforms (conceptual), compliance and regulatory requirements (ISO 27001, GDPR – overview), challenges in cloud forensics and investigations	15

M.Sc. CS & DF Major Syllabus

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain cloud architectures and shared responsibility model	Understand	PSO1
CO2	Analyze cloud-specific threats and security challenges	Analyze	PSO1
CO3	Apply cloud security controls for data and identity protection	Apply	PSO1, PSO3
CO4	Evaluate compliance and risk issues in cloud environments	Evaluate	PSO4
CO5	Identify security considerations for cloud-based investigations	Create	PSO2, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Cloud Security and Privacy	Tim Mather, Subra Kumaraswamy
2	Practical Cloud Security	Chris Dotson
3	Security Guidance for Critical Areas of Cloud Computing	Cloud Security Alliance
4	NIST SP 800-53 / 800-210 (Cloud Security Guidance)	NIST
5	AWS / Azure / Google Cloud Security Whitepapers	Official Documentation

Course Code	**RJSPGCSDF201P**
Course Title	**Malware Analysis Lab**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To perform safe and structured malware analysis
2	To apply static and dynamic malware analysis techniques
3	To observe malware behavior and persistence mechanisms
4	To analyze network activity generated by malware
5	To document malware analysis findings professionally

Practical Assignments

Indicative Tools (not restrictive):
VirtualBox / VMware, PEview, Strings, IDA Free / Ghidra (intro), Process Monitor, Process Explorer, Wireshark, FakeNet-NG, Cuckoo Sandbox (demo)

M.Sc. CS & DF Major Syllabus

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Malware Analysis Environment Setup	Configure isolated VM and snapshot environment for malware analysis
2	Malware Sample Handling	Safe handling and hashing of malware samples
3	Basic Static Analysis	Identify file type, strings, and imports of malware sample
4	PE File Structure Analysis	Analyze PE headers and sections
5	Signature-Based Detection	Compare malware hashes using signature databases
6	Dynamic Analysis Setup	Execute malware in sandboxed environment
7	Process Behavior Analysis	Monitor processes and system calls during execution
8	File System Changes	Observe file creation, deletion, and modification
9	Registry Activity Analysis	Identify persistence-related registry changes
10	Network Behavior Analysis	Capture and analyze malware-generated network traffic
11	Command-and-Control Observation	Identify potential C2 communication patterns
12	Anti-Analysis Awareness	Observe evasion or anti-debugging behavior
13	IOC Extraction	Extract Indicators of Compromise (hashes, IPs, domains)
14	Case-Based Malware Investigation	Analyze a given malware incident scenario
15	Malware Analysis Report	Prepare a structured malware analysis report

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Configure a secure malware analysis environment	Apply	PSO1
CO2	Perform static and dynamic malware analysis	Apply	PSO1, PSO3
CO3	Analyze malware behavior and persistence mechanisms	Analyze	PSO1
CO4	Identify and document malware indicators of compromise	Evaluate	PSO2
CO5	Prepare professional malware analysis reports	Create	PSO3, PSO4

Course Code	**RJSPGCSDF202P**
Course Title	**Incident Response Simulation Lab**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To apply structured incident response processes in simulated environments
2	To perform incident detection, triage, and containment
3	To integrate digital forensic techniques during incident handling
4	To analyze and document cyber incidents systematically
5	To prepare professional incident response and investigation reports

Practical Assignments

Indicative Tools (not restrictive):
SIEM (demo logs), Wireshark, Zeek logs, Windows Event Viewer, Volatility (conceptual use), Case documentation templates

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Incident Response Environment Setup	Understand lab setup, roles, IR workflow, and documentation templates
2	Incident Identification	Identify indicators of a cyber incident from given logs and alerts
3	Incident Classification & Prioritization	Classify incidents based on severity and business impact
4	Incident Triage	Perform initial triage and validate incident authenticity
5	Evidence Preservation	Preserve volatile and non-volatile evidence without contamination
6	Short-Term Containment	Apply immediate containment actions (system isolation, access control)
7	Long-Term Containment	Plan long-term containment and remediation strategies
8	Root Cause Analysis	Analyze logs and artifacts to identify root cause
9	Timeline Reconstruction	Construct an incident timeline from multiple data sources
10	Forensic Integration	Integrate forensic findings into incident analysis
11	Communication & Escalation	Draft incident notifications for management and stakeholders
12	Legal & Compliance Considerations	Identify legal, regulatory, and reporting requirements
13	Post-Incident Review	Conduct lessons-learned and improvement analysis
14	Case-Based Incident Handling	Handle a full incident scenario end-to-end
15	Incident Response Report	Prepare a professional IR and investigation report

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Identify and classify cyber security incidents	Apply	PSO2
CO2	Perform containment and evidence preservation	Apply	PSO2
CO3	Analyze incidents using forensic and log data	Analyze	PSO2, PSO3
CO4	Evaluate incident response effectiveness	Evaluate	PSO4
CO5	Prepare structured incident response reports	Create	PSO3, PSO4

Course Code	**RJSPGCSDF203P**
Course Title	**Cloud Forensics Lab**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand forensic challenges in cloud environments
2	To collect and analyze cloud-based logs and artifacts
3	To apply cloud security monitoring and investigation techniques
4	To perform incident analysis in cloud-hosted systems
5	To prepare cloud forensic investigation reports

Practical Assignments

Indicative Tools (not restrictive):
AWS CloudTrail / Azure Monitor (free tier or simulated logs), Google Cloud Logs (sample), Cloud Storage logs, SIEM sample datasets, Linux tools

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Introduction to Cloud Forensics	Understand cloud service models, forensic challenges, and shared responsibility
2	Cloud Log Familiarization	Explore cloud audit logs and activity logs
3	Identity & Access Log Analysis	Analyze IAM logs for unauthorized access attempts
4	Cloud Storage Forensics	Examine object access, deletion, and modification logs
5	Virtual Machine Log Analysis	Analyze VM/system logs from cloud-hosted instances
6	Network Activity Analysis	Analyze cloud network flow logs for suspicious traffic
7	Timeline Construction	Build activity timeline from cloud logs
8	Incident Detection in Cloud	Identify indicators of compromise from cloud audit data

9	Evidence Collection Strategy	Plan evidence acquisition under cloud constraints
10	Data Integrity Verification	Verify integrity of collected cloud forensic data
11	Cloud Incident Response	Simulate containment and remediation actions
12	Compliance & Legal Considerations	Identify compliance and jurisdictional issues in cloud investigations
13	Case Study – Cloud Breach	Analyze a real or simulated cloud security incident
14	Evidence Correlation	Correlate cloud logs with host and network evidence
15	Cloud Forensic Report	Prepare a structured cloud forensic investigation report

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain forensic challenges in cloud environments	Understand	PSO2
CO2	Analyze cloud logs and audit trails for investigations	Analyze	PSO2
CO3	Apply forensic techniques to cloud-based incidents	Apply	PSO2, PSO3
CO4	Evaluate cloud security incidents and compliance issues	Evaluate	PSO4
CO5	Prepare professional cloud forensic investigation reports	Create	PSO3, PSO4

Course Code	**RJSPGCSDFE201**
Course Title	**Ethical Hacking & Exploitation**
Credits	**2**
Duration	**30 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand ethical hacking principles and legal boundaries
2	To study structured penetration testing methodologies
3	To analyze common vulnerabilities and exploitation techniques
4	To understand post-exploitation and privilege escalation concepts
5	To prepare students for ethical hacking roles in industry

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Ethical Hacking Foundations & Vulnerability Discovery: Ethical hacking concepts and scope, difference between ethical hacking and cyber crime, legal and ethical considerations, penetration testing lifecycle, reconnaissance and	15

	footprinting techniques, scanning and enumeration concepts, vulnerability assessment methodologies, common vulnerability categories (OWASP Top 10 – overview), reporting and responsible disclosure	
Unit II	Exploitation & Post-Exploitation Techniques: Exploitation concepts and objectives, client-side and server-side exploitation (conceptual), web application exploitation techniques (authentication flaws, injection, misconfiguration), privilege escalation concepts, lateral movement basics, persistence mechanisms, post-exploitation documentation, ethical limitations and real-world constraints	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain ethical hacking principles and legal constraints	Understand	PSO1
CO2	Analyze vulnerabilities using structured methodologies	Analyze	PSO1
CO3	Apply ethical hacking concepts to penetration testing scenarios	Apply	PSO1, PSO3
CO4	Evaluate exploitation outcomes and security risks	Evaluate	PSO1
CO5	Prepare professional ethical hacking and vulnerability reports	Create	PSO3, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	The Web Application Hacker's Handbook	Dafydd Stuttard
2	Metasploit: The Penetration Tester's Guide	Kennedy et al.
3	OWASP Testing Guide	OWASP Foundation
4	Penetration Testing: A Hands-On Introduction	Georgia Weidman
5	CEH v12 Official Courseware (Reference)	EC-Council

Course Code	**RJSPGCSDFE201P**
Course Title	**Ethical Hacking Practical**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To apply ethical hacking methodologies in controlled environments
2	To perform vulnerability identification and exploitation safely
3	To understand post-exploitation and risk assessment techniques
4	To follow legal, ethical, and professional guidelines during testing
5	To document penetration testing findings in a professional manner

Practical Assignments

Indicative Tools (not restrictive):
Kali Linux, Nmap, Nikto, Burp Suite (Community), Metasploit (demo), OWASP Juice Shop, DVWA, OpenVAS (demo)

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Ethical Hacking Lab Setup	Configure Kali Linux and target VMs; understand scope & rules of engagement
2	Reconnaissance & Footprinting	Perform passive and active reconnaissance on target systems
3	Network Scanning	Use Nmap to identify open ports, services, and OS fingerprints
4	Vulnerability Scanning	Conduct vulnerability scans and analyze scan results
5	Web Application Mapping	Map web application structure and inputs
6	Authentication Testing	Identify weak authentication and session issues
7	Injection Attack Observation	Demonstrate SQL injection in a vulnerable application
8	Client-Side Vulnerabilities	Observe XSS and input validation flaws
9	Exploitation Framework Usage	Use Metasploit modules in a controlled scenario
10	Privilege Escalation Concepts	Identify privilege escalation opportunities (conceptual)
11	Post-Exploitation Observation	Observe system changes after exploitation
12	Password Security Testing	Perform password strength and brute-force analysis (controlled)
13	Risk & Impact Analysis	Assess impact of discovered vulnerabilities
14	Penetration Test Case Study	Conduct a guided end-to-end penetration test
15	Penetration Test Report	Prepare a professional ethical hacking report

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Perform reconnaissance and scanning ethically	Apply	PSO1
CO2	Identify vulnerabilities using ethical hacking tools	Analyze	PSO1
CO3	Apply controlled exploitation techniques	Apply	PSO1, PSO3
CO4	Evaluate security risks and impacts	Evaluate	PSO4
CO5	Prepare professional penetration testing reports	Create	PSO3, PSO4

Course Code	**RJSPGCSDFE202**
Course Title	**Blockchain Security**
Credits	**2**
Duration	**30 Hours**

Course Objectives

Sr. No.	Course Objective
1	To understand blockchain systems from a security perspective
2	To study security mechanisms used in public and permissioned blockchains
3	To analyze vulnerabilities and attacks on blockchain platforms
4	To understand smart contract security issues
5	To apply blockchain security concepts in real-world applications

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
Unit I	Blockchain Architecture & Security Mechanisms: Review of blockchain fundamentals (brief), block structure and Merkle trees, cryptographic primitives used in blockchain (hashing, digital signatures), consensus mechanisms (PoW, PoS, PBFT – security comparison), node security, wallet and private key security, permissioned vs permissionless blockchain security considerations, overview of major platforms (Bitcoin, Ethereum, Hyperledger)	15
Unit II	Blockchain Threats, Attacks & Smart Contract Security: Blockchain threat landscape, double-spending attacks, 51% attacks, Sybil attacks, eclipse attacks, smart contract vulnerabilities (reentrancy, integer overflow, access control flaws – concept level), security auditing basics for smart contracts, regulatory and legal challenges in blockchain security, security best practices for blockchain deployments	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Explain blockchain architecture and security mechanisms	Understand	PSO1
CO2	Analyze blockchain-specific threats and attacks	Analyze	PSO1
CO3	Apply security concepts to blockchain platforms	Apply	PSO1, PSO3
CO4	Evaluate smart contract security risks	Evaluate	PSO1
CO5	Recommend security best practices for blockchain systems	Create	PSO3, PSO4

Textbooks & References

Sr. No.	Title	Author / Source
1	Mastering Blockchain	Imran Bashir
2	Blockchain Basics	Daniel Drescher
3	Hands-On Smart Contract Development	Zubin Shah
4	NIST IR 8425 – Blockchain Technology Overview	NIST
5	Ethereum Smart Contract Security Best Practices	Ethereum Foundation

Course Code	**RJSPGCSDFE202P**
Course Title	**Blockchain Security Practical**
Credits	**2**
Duration	**60 Hours**

Course Objectives

Sr. No.	Course Objective
1	To analyze blockchain security mechanisms through hands-on exercises
2	To identify and study common blockchain attacks and vulnerabilities
3	To perform basic smart contract security analysis
4	To understand blockchain transaction tracing and audit techniques
5	To prepare security and forensic reports for blockchain systems

Practical Assignments

Indicative Tools (not restrictive):
Bitcoin / Ethereum Testnet, Etherscan, Blockchair, Remix IDE, Ganache, MetaMask, Solidity (basic), Truffle (demo)

Practical No.	Task / Title	Description (Key Tools & Deliverables)
1	Blockchain Environment Setup	Configure local blockchain using Ganache and connect via MetaMask
2	Block & Transaction Analysis	Analyze blocks, transactions, gas, and confirmations using Etherscan
3	Wallet & Key Security	Study wallet generation, private key handling, and recovery mechanisms
4	Consensus Observation	Observe block creation and validation in test networks
5	Double-Spending Simulation	Demonstrate concept of double spending in controlled environment
6	Smart Contract Deployment	Deploy a basic Solidity smart contract using Remix

7	Smart Contract Interaction	Invoke contract functions and analyze transaction logs
8	Access Control Vulnerability	Observe access control flaws in sample smart contracts
9	Reentrancy Observation	Demonstrate reentrancy vulnerability using vulnerable contract
10	Smart Contract Audit Basics	Identify security issues in given smart contract code
11	Transaction Tracing	Trace fund movement across multiple addresses
12	Blockchain Log Evidence Collection	Collect and document blockchain transaction evidence
13	Regulatory & Compliance Mapping	Map blockchain activities to legal and compliance considerations
14	Case Study – Blockchain Breach	Analyze a real or simulated blockchain security incident
15	Security & Forensic Report	Prepare structured blockchain security/forensic report

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Analyze blockchain transactions and blocks	Analyze	PSO1
CO2	Identify blockchain security vulnerabilities	Analyze	PSO1
CO3	Apply smart contract security analysis techniques	Apply	PSO1, PSO3
CO4	Trace and document blockchain-based evidence	Evaluate	PSO2
CO5	Prepare professional blockchain security reports	Create	PSO3, PSO4

Course Code	**RJSPGCSDFOJT201**
Course Title	**Internship / On-Job Training in Cyber Security & Digital Forensics**
Credits	**4**
Duration	**Minimum 8–10 Weeks / 240 Hours**

(Industry / Government / Research Organization)

Course Code	**RJSPGCSDFOJT201**
Course Title	**Internship / On-Job Training in Cyber Security & Digital Forensics**
Credits	**4**
Duration	**Minimum 8–10 Weeks / 240 Hours**

(Industry / Government / Research Organization)

Course Objectives

Sr. No.	Course Objective
1	To provide real-world exposure to cyber security and digital forensics practices
2	To apply theoretical and practical knowledge in professional environments
3	To develop industry-relevant technical, analytical, and communication skills
4	To understand professional ethics, teamwork, and organizational practices
5	To prepare students for industry roles, research, or higher studies

Assessment of On-Job Training (OJT)

a) On-Job Training: Internship / Apprenticeship Assessment

Maximum Marks: 100

The assessment of On-Job Training (Internship / Apprenticeship) shall be carried out based on the student's performance during the training period, the internship report submitted, and the presentation/viva-voce conducted by the department.

Internship Report Format

- **Name of the Department:** _____
- **Course Code:** _____
- **Course Name:** _____
- **Date:** _____
- **Roll No.:** _____
- **UID No.:** _____
- **Marks:** _____ / 60
- **Name of the Student:** _____
- **Title of the Project:** _____

Report Contents:
As specified in the respective course syllabus.

Assessment Grid – Internship / Apprenticeship

OJT Parameters	Marks	Excellent (81–100%)	Good (61–80%)	Satisfactory (41–60%)	Average (20–40%)
Work done at OJT (including attendance)	50	41–50 / 50	31–40 / 50	21–30 / 50	10–20 / 50

Report Writing and Conclusions	30	25–30 / 30	19–24 / 30	13–18 / 30	6–12 / 30
Presentation and Communication	20	17–20 / 20	13–16 / 20	7–12 / 20	4–6 / 20
Total	100				

b) On-Job Training: Field Project Assessment / Project Assessment (wherever applicable)

In cases where a **Field Project / Project Work** is prescribed in lieu of or in addition to the internship, the assessment shall be carried out as per the following scheme.

Maximum Marks: 100

Project Report Format

- **Name of the Department:** _____
- **Course Code:** _____
- **Course Name:** _____
- **Date:** _____
- **Roll No.:** _____
- **UID No.:** _____
- **Marks:** _____ / 60
- **Name of the Student:** _____
- **Title of the Project:** _____

Report Contents: As specified in the respective course syllabus.

Assessment Grid – Field Project / Project Work

Project Work / Report Parameters	Marks	Excellent (81–100%)	Good (61–80%)	Satisfactory (41–60%)	Average (20–40%)
Project Work Done	50	41–50 / 50	31–40 / 50	21–30 / 50	10–20 / 50
Report Writing and Conclusions	30	25–30 / 30	19–24 / 30	13–18 / 30	6–12 / 30
Presentation and Communication	20	17–20 / 20	13–16 / 20	7–12 / 20	4–6 / 20
Total	100				

M.Sc. CS & DF Major Syllabus

General Guidelines

1. The On-Job Training / Internship / Field Project shall be undertaken only after approval by the Department.
2. The student shall submit the internship/project report within the stipulated time.
3. The assessment shall be conducted by a panel appointed by the Head of the Department.
4. Students shall adhere strictly to ethical practices and confidentiality norms of the organization.

Scheme of Examination

M.Sc. Cyber Security & Digital Forensics

Semester I

Sr. No.	Course Code	Course Name	Internal	External	Total	Credits
1	RJSPGCSDF101	Advanced Cryptographic Systems & Secure Protocols	40	60	100	3
2	RJSPGCSDF101P	Cryptographic Systems Implementation & Analysis Lab	–	50	50	2
3	RJSPGCSDF102	Advanced Digital Forensics Techniques & Evidence Correlation	40	60	100	3
4	RJSPGCSDF102P	Advanced Digital Forensics & Evidence Analysis Lab	–	50	50	2
5	RJSPGCSDF103	Network Threat Detection, Attack Surface & Adversarial Tactics	40	60	100	2

6	RJSPGCSDF103P	Network Threat Detection & Security Analytics Lab	–	50	50	2
7	RJSPGCSDFE101	Blockchain Security & Distributed Ledger Forensics *(Elective – I)*	40	60	100	2
8	RJSPGCSDFE101P	Blockchain Forensics & Smart Contract Analysis Lab	–	50	50	2
9	RJSPGCSDFE102	AI & Machine Learning for Cyber Threat Detection	40	60	100	2
10	RJSPGCSDFE102P	AI-Driven Threat Detection & Modelling Lab	–	50	50	2
11	RJSPGCSDFOEC101	Research Methodology, Academic Writing & Research Ethics	40	60	100	4
		Total			**700**	**22**

Semester II

Sr. No.	Course Code	Course Name	Internal	External	Total	Credits
1	RJSPGCSDF201	Malware Reverse Engineering & Exploit Analysis	40	60	100	3
2	RJSPGCSDF201P	Malware Analysis, Debugging	–	50	50	2

		& Reverse Engineering Lab				
3	RJSPGCSDF202	Incident Response, DFIR & Cyber Crime Investigation	40	60	100	3
4	RJSPGCSDF202P	Incident Response & Digital Investigation Simulation Lab	–	50	50	2
5	RJSPGCSDF203	Cloud Security Architecture & Cloud Forensics	40	60	100	2
6	RJSPGCSDF203P	Cloud Security & Cloud Forensics Lab	–	50	50	2
7	RJSPGCSDFE201	IoT & Mobile Device Forensics *(Elective – I)*	40	60	100	2
8	RJSPGCSDFE201P	IoT & Mobile Forensics Lab	–	50	50	2

9	RJSPGCSDFE202	Post-Quantum & Quantum Cryptography	40	60	100	2
10	RJSPGCSDFE202P	Quantum-Resistant Cryptography & Security Lab	–	50	50	2
11	RJSPGCSDFOJT201	Industry Internship in Cyber Security / DFIR / SOC Operations	40	60	100	4
		Total			**700**	**22**

Evaluation and Assessment

M.Sc. Cyber Security & Digital Forensics (Part I)

(As per NEP 2020 Guidelines)

1. Evaluation – Theory

Total Marks per Theory Course: 100

- **Internal Assessment:** 40 Marks
- **Semester End Examination (SEE):** 60 Marks

a. Internal Assessment – 40 Marks

The internal assessment shall be awarded as follows:

I. 25 Marks (Any ONE of the following):

i. Written Test / Case Study / Presentation

OR

ii. SWAYAM / NPTEL **Advanced Course** of minimum **20 hours** with

successful certification

OR

iii. Valid **International Certification** (Prometric, Pearson, Certiport, Coursera, Udemy, edX or equivalent platforms)

Note:

- One certification shall be considered for **one course only**.
- For four theory courses, the student must complete **four distinct certifications**.

II. 15 Marks – Mini Project / Assignment

Mini project or assignment shall be aligned with the course curriculum and evaluated based on:

- Conceptual clarity
- Technical depth
- Analysis and interpretation
- Documentation and presentation

III. Special Provision – Research Methodology

For **Research Methodology, Academic Writing & Research Ethics (RJSPGCSDFOEC101)**, the **entire 40 internal marks** shall be awarded for:

- Presentation and review of **classic and recent research papers**, **or**
- Research-based case study relevant to Cyber Security & Digital Forensics.

2. Semester End Examination (SEE) – 60 Marks

- Question paper shall cover **all units**, unless otherwise specified.

Applicable Courses

Semester I:

RJSPGCSDF101, RJSPGCSDF102, RJSPGCSDF103, RJSPGCSDFE101 / RJSPGCSDFE102, RJSPGCSDFOEC101

Semester II:
RJSPGCSDF201, RJSPGCSDF202, RJSPGCSDF203,
RJSPGCSDFE201 / RJSPGCSDFE202

SEE Question Paper Blueprint (60 Marks)

Unit / Component	**Knowledge**	**Understanding**	**Application & Analysis**	**Total Marks**
Unit I	06	02	04	12
Unit II	06	02	04	12
Unit III	06	02	04	12
Unit IV	06	02	04	12
Short Notes *(covering all units)*	04	04	04	12
Total per Objective	**28**	**12**	**20**	**60**

Weightage (%)

Cognitive Level	**Percentage**
Knowledge	46%
Understanding	20%
Application & Analysis	34%
Total	**100%**

3. Assessment of Practicals – 50 Marks

Applicable Practical Courses

Semester I:
RJSPGCSDF101P, RJSPGCSDF102P, RJSPGCSDF103P,
RJSPGCSDFE101P / RJSPGCSDFE102P

Semester II:
RJSPGCSDF201P, RJSPGCSDF202P, RJSPGCSDF203P,
RJSPGCSDFE201P / RJSPGCSDFE202P

Sample Practical Examination Pattern

Option I

Component	**Marks**
Practical Question 1	15
Practical Question 2	15
e-Journal & Continuous Evaluation	15
Viva-Voce	05
Total	**50**

OR

Option II

Component	**Marks**
Practical Question	30
e-Journal & Continuous Evaluation	15
Viva-Voce	05
Total	**50**

4. Assessment of On-Job Training (OJT)

a. Internship / Apprenticeship Assessment – 100 Marks

Course Code: RJSPGCSDFOJT201

Internship Report Format

- Name of Department: _____

- Course Code: _____ Course Name: _____ Date: _____
- Roll No.: _____ UID No.: _____ Marks: ____ / 60
- Name of Student: _____
- Title of Project: _____
- Report Contents: As specified in the course syllabus

OJT Assessment Grid

Parameter	**Marks**	**Excellent (81–100%)**	**Good (61–80%)**	**Satisfactory (41–60%)**	**Average (20–40%)**
Work done at OJT *(including attendance)*	50	41–50	31–40	21–30	10–20
Report writing & conclusions	30	25–30	19–24	13–18	6–12
Presentation & communication	20	17–20	13–16	7–12	4–6
Total	**100**				

b. Field Project / Project Assessment (Where Applicable)

Assessment Grid

Parameter	**Marks**	**Excellent**	**Good**	**Satisfactory**	**Average**
Project work done	50	41–50	31–40	21–30	10–20
Report writing & conclusions	30	25–30	19–24	13–18	6–12

Presentation & communication	20	17–20	13–16	7–12	4–6

Teaching–Learning Process

The teaching–learning process for the **M.Sc. Cyber Security & Digital Forensics** program is designed under a **learning-outcomes–based framework**, emphasizing **advanced analytical skills, investigative competence, and research orientation**.

The program adopts a balanced mix of **theoretical instruction, laboratory-intensive learning, case studies, simulations, and industry exposure**, enabling students to handle real-world cyber security and digital forensic challenges.

Teaching–Learning Methods Include:

- Classroom lectures
- Hands-on laboratory sessions
- Case studies and cyber incident simulations
- Research paper reviews and presentations
- Group discussions, workshops, and seminars
- Peer learning and collaborative projects
- Flipped classroom and project-based learning
- Practical experiment design, analysis, interpretation, and application
- On-Job Training / Industry Internship
- Technology-enabled self-learning
- Learning Management Systems (e.g., Google Classroom)
- Online cyber security and forensic tools

At the postgraduate level, **self-learning and independent inquiry are strongly encouraged**, with emphasis on **higher-order cognitive skills, ethical responsibility, and professional competence**. The program aims to develop

graduates capable of contributing effectively to **industry, law enforcement, research, and doctoral studies** in Cyber Security and Digital Forensics.

Mapping of Courses to Employability / Entrepreneurship / Skill Development

M.Sc. Cyber Security & Digital Forensics (Part I)

Semester I

Course Name	Course Code	Topic Focusing on Employability / Entrepreneurship / Skill Development	Employability / Entrepreneurship / Skill Development	Specific Activity
Advanced Cryptographic Systems & Secure Protocols	RJSPGCSDF101	**Skill Development Unit I:** Cryptographic primitives, symmetric & asymmetric algorithms **Unit II:** PKI, digital signatures, authentication protocols **Unit III:** Secure communication protocols (TLS, IPSec) **Unit IV:**	1. Technical skills in designing and evaluating cryptographic mechanisms for secure systems. 2. Employability skills in analysing cryptographic protocols used in finance, cloud, and enterprise security.	Experiential learning enhances skills in threat modelling, cryptographic evaluation, and secure protocol design.

		Cryptographic attacks, protocol analysis		
Advanced Cryptographic Systems Implementation & Analysis Lab	RJSPGCSDF101P	Implementation of encryption algorithms, hashing, digital signatures, key exchange mechanisms	Technical skills in implementing and analysing cryptographic systems using industry-grade libraries and tools	Hands-on lab work on encryption, secure communication, and cryptographic attack simulation
Advanced Digital Forensics Techniques & Evidence Correlation	RJSPGCSDF102	**Skill Development**		
		Unit I: Advanced forensic acquisition & evidence handling **Unit II:** File system & memory forensics **Unit III:** Evidence correlation, timeline reconstruction **Unit IV:** Legal	1. Technical skills in forensic investigation and evidence correlation. 2. Employability skills for DFIR teams, law enforcement, and cyber crime investigation units.	Experiential learning through forensic case analysis and digital evidence correlation.

		admissibility, reporting		
Advanced Digital Forensics & Evidence Analysis Lab	RJSPGCSDF102P	Disk, memory, log analysis, timeline reconstruction, forensic reporting	Technical skills in handling forensic tools and conducting investigations	Practical forensic investigations using real-world datasets
Network Threat Detection, Attack Surface & Adversarial Tactics	RJSPGCSDF103	**Skill Development Unit I:** Network threat landscape & attack surface analysis **Unit II:** Adversarial tactics, techniques & procedures (TTPs) **Unit III:** Threat detection & intrusion analysis **Unit IV:** Security analytics & mitigation	1. Technical skills in identifying and analysing network-based cyber attacks. 2. Employability skills for SOC, threat hunting, and security monitoring roles.	Experiential learning enhances skills in threat simulation and network traffic analysis.
Network Threat Detection & Security	RJSPGCSDF103P	Network traffic analysis, IDS/IPS configuration,	Practical skills for SOC operations and real-time	Hands-on exercises using security analytics

Analytics Lab		anomaly detection	threat detection	and monitoring tools
Blockchain Security & Distributed Ledger Forensics *(Elective – I)*	RJSPGCSDFE101	**Skill Development** Blockchain security architecture, smart contract vulnerabilities, ledger forensics	Employability skills for blockchain security analyst and forensic investigator roles	Case studies on blockchain fraud and smart contract analysis
Blockchain Forensics & Smart Contract Analysis Lab	RJSPGCSDFE101P	Smart contract analysis, blockchain transaction tracing	Practical skills in blockchain forensic investigation	Hands-on smart contract auditing and forensic analysis
OR				
AI & Machine Learning for Cyber Threat Detection *(Elective – II)*	RJSPGCSDFE102	**Skill Development** ML-based anomaly detection, threat prediction models	Employability skills for AI-driven cyber defence roles	ML-based threat detection projects
AI-Driven Threat Detection & Modelling Lab	RJSPGCSDFE102P	ML model development for threat detection	Practical skills in AI-based security analytics	Hands-on ML model implementation

Research Methodology, Academic Writing & Research Ethics	RJSPGCSDFOEC101	**Skill Development** Research methods, academic writing, ethics, proposal development	1. Research and analytical skills for higher studies and R&D roles. 2. Technical skills in research documentation and reporting.	Experiential learning through research paper reviews and proposal writing

Semester II

Course Name	Course Code	Topic Focusing on Employability / Entrepreneurship / Skill Development	Employability / Entrepreneurship / Skill Development	Specific Activity
Malware Reverse Engineering & Exploit Analysis	RJSPGCSDF201	**Skill Development** Malware analysis, reverse engineering, exploit techniques	Technical skills for malware analyst and reverse engineering roles	Hands-on malware dissection and exploit analysis
Malware Analysis, Debugging & Reverse	RJSPGCSDF201P	Static and dynamic malware	Practical skills in reverse engineering malware	Real-world malware analysis exercises

Engineering Lab		analysis, debugging		
Incident Response, DFIR & Cyber Crime Investigation	RJSPGCSDF202	**Skill Development** Incident response lifecycle, digital investigation	Employability skills for DFIR, SOC lead, and cyber crime investigation roles	Incident response simulations and forensic investigations
Incident Response & Digital Investigation Simulation Lab	RJSPGCSDF202P	Incident handling, evidence collection, reporting	Practical DFIR skills	Simulation-based incident response exercises
Cloud Security Architecture & Cloud Forensics	RJSPGCSDF203	**Skill Development** Secure cloud design, cloud forensic investigation	Employability skills for cloud security and forensic analyst roles	Case studies and cloud forensic simulations
Cloud Security & Cloud Forensics Lab	RJSPGCSDF203P	Cloud log analysis, forensic investigation	Practical skills in cloud security operations	Hands-on cloud forensic analysis
IoT & Mobile Device Forensics *(Elective – I)*	RJSPGCSDFE201	**Skill Development** Mobile & IoT forensic techniques	Employability skills in emerging forensic domains	Device-level forensic investigations

OR				
Post-Quantum & Quantum Cryptography *(Elective – II)*	RJSPGCSDFE202	**Skill Development** Quantum-resistant cryptographic systems	Research and advanced cryptography skills	Cryptographic analysis projects
Industry Internship / On-Job Training	RJSPGCSDFOJT201	**Employability / Entrepreneurship** Industry exposure in cyber security & DFIR	Professional, technical, and workplace readiness	Real-world industry problem solving