Hindi Vidya Prachar Samiti's

Ramniranjan Jhunjhunwala College

of Arts, Science & Commerce

(Empowered Autonomous College)

Affiliated to

UNIVERSITY OF MUMBAI

Program Code: RJCUCSDF

Syllabus for the

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

Course Codes: RJMAJCSDF111, RJMAJCSDF112, RJMAJCSDF121, RJMAJCSDF122

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

Preamble

The National Education Policy 2020 aims at imparting skill-based learning and caters to the multiple entry and exit facility for the students thus empowering them to acquire knowledge at their pace In the three-year UG program, the student has two exit options. Students also have the option for choosing the Honors program of four years study in a given discipline and later converting it to five year integrated PG degree program. As undergraduate student, he/she learns the core subject (Major), subject complementing the core subject (Minor), a course from other discipline (OEC or GEC) Vocational and Skill Enhancement course from the Major(VSEC). The remaining verticals under NEP 2020 are IKS (Indian Knowledge System), AEC (Ability Enhancement Course), VEC (Value Enhancement Course) and with progressive three years of UG, student also completes at different levels OJT (On Job Training), FP (Field Projects), CEP (Community Engagement Program) , RP (Research Project) which helps him/her in understanding their roots, application of the knowledge for the benefit of self and the society. Vertical CC (Co-curricular activities and activities related to yoga and human well-being) helps in preparing youth with good character and interpersonal relationships.

SEMESTER I

Major Core – Basics of Computer Networks

Course Code	Course Title	Course Type	Credits	Duration
RJMAJCSDF111	Basics of Computer Networks	Major Core (Theory)	2	30 Hours

Course Objectives

Sr. No.	Course Objective
1	Understand fundamentals of computer networks, network devices & topologies.
2	Explain OSI & TCP/IP models and the functionalities of each layer.
3	Learn network transmission media, switching & communication techniques.
4	Understand IP addressing, subnetting & routing basics.
5	Develop awareness of basic network security & troubleshooting commands.

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
I	**Fundamentals of Computer Networks** • Concept of Computer Networks: Need, advantages, applications in cybersecurity & digital forensics • Types of Networks: PAN, LAN, MAN, WAN, GAN, CAN • Network Topologies: Bus, Star, Ring, Mesh, Hybrid – Advantages & disadvantages • Networking Devices: Hub, Switch, Router, Bridge, Repeater, Gateway, NIC, Access Point • Transmission Media: Guided (Twisted pair, Coaxial, Fiber optic), Unguided (Microwave, Radio, Satellite) • Reference Models: OSI Model – Layer-wise functions, protocols & services • TCP/IP Model – Comparison with OSI, protocol stack mapping Introduction to WLAN, Wi-Fi security basics, SSID, MAC filtering	15
II	**IP Addressing, Routing & Basic Security Concepts** • IP Addressing: IPv4 structure, classes, private & public IP, subnet mask • Subnetting: FLSM, VLSM, CIDR, Supernetting • Routing: Static vs Dynamic routing, RIP & OSPF concept • Important Protocols: HTTP/HTTPS, ICMP, ARP, DHCP, DNS, FTP, SMTP, SNMP • Basic Network Security: Concept of firewall, IDS/IPS, proxy, VPN overview • Common Network Attacks: MITM, DNS spoofing, ARP poisoning, DoS • Basic Troubleshooting Commands: ping, tracert, ipconfig, netstat, nslookup	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Describe the fundamentals of computer networks, networking devices, and network topologies.	Remember (L1), Understand (L2)	PSO1, PSO5
CO2	Explain the functions of OSI and TCP/IP layers and compare their roles.	Understand (L2)	PSO1, PSO3, PSO5
CO3	Apply IP addressing, subnetting, and basic routing to small network configurations.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO4	Analyze common network problems and apply appropriate troubleshooting steps.	Apply (L3), Analyze (L4)	PSO1, PSO2, PSO3, PSO5
CO5	Identify fundamental network security concerns and methods to protect network infrastructure.	Understand (L2), Analyze (L4)	PSO1, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	Computer Networking: A Top-Down Approach (9th Ed., 2025)	James Kurose, Keith Ross / Pearson
2	Data Communications and Networking (6th Ed.)	Behrouz A. Forouzan / McGraw-Hill
3	Computer Networks (6th Ed.)	Andrew S. Tanenbaum, David J. Wetherall / Pearson
4	Network Security Essentials (6th Ed.)	William Stallings / Pearson
5	TCP/IP Illustrated, Vol. 1: The Protocols	W. Richard Stevens / Addison-Wesley

Major Core – Python Programming Fundamentals

Course Code	Course Title	Course Type	Credits	Duration
RJMAJCSDF112	Python Programming Fundamentals	Major Core (Theory)	2	30 Hours

Course Objectives

Sr. No.	Course Objective
1	Understand the basics of Python programming, including syntax, data types, and control structures, as per Coursera and SANS syllabi.
2	Learn object-oriented programming concepts and file handling in Python, aligned with Georgia Tech edX course.
3	Explore Python libraries relevant to cybersecurity, such as string manipulation and basic automation, from TCM Security syllabus.
4	Develop skills in writing simple scripts for data processing and error handling, incorporating MITRE ATT&CK examples.
5	Gain awareness of Python's role in digital forensics and cybersecurity scripting, encouraging reference to books for practical scripts.

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
I	**Introduction to Programming and Python Basics** • Overview of Programming: What is programming? Why Python? History, features, and installation (IDLE, PyCharm setup) • Algorithms and Flowcharts: Basic concepts of algorithms (step-by-step problem-solving), pseudocode examples; Introduction to flowcharts (symbols: start/end, input/output, decisions, loops) with simple problems like "Calculate average of three numbers" (Draw flowcharts manually and digitally using tools like draw.io) • Basic syntax: Variables (naming conventions), data types (int, float, str, bool with real-life analogies like "str as text messages"), operators (arithmetic, relational, logical with truth tables) • Input/output: print() for displaying results, input() for user interaction (error-proofing basics); Formatting strings (f-strings for simple reports) • Control structures: if-else (decision-making with everyday scenarios like "grade checker"), loops (for simple repetition like summing numbers, while for user menus), break/continue (with flowchart integration) • Lists and basic collections: Creation, indexing, slicing (analogies to shopping lists); Simple methods (append, pop); Applications in cybersecurity: Basic data parsing for log files (e.g., extracting IP addresses)	15

II	**Functions, Modules, and Advanced Beginner Concepts** • **Functions**: Why functions? Definition, parameters (positional/keyword), return values (simple math functions); Lambda functions (one-liners for quick tasks); Recursion (basic intro with factorial, avoiding deep dives) • **Modules**: Import statements, standard libraries (math for calculations, random for simulations, os/sys for file paths; cyber examples like random password generation) • **File handling:** Reading/writing text files (step-by-step with 'with' statements), exception handling (try-except-finally for file errors like "file not found"; log parsing exercises) • **Object-Oriented Programming:** Gentle intro to classes/objects (analogy to "blueprints for cars"), basic inheritance (parent-child classes for simple tools), encapsulation (private variables); No advanced polymorphism yet (Forensic classes like "LogAnalyzer") • **Strings and regular expressions:** Basic methods (split, join), regex module for simple pattern matching (e.g., email validation in forensic data; re.match basics) • **Error handling and debugging**: Common beginner errors (indentation, type mismatches), debugging techniques (print statements, pdb intro)	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Recall basic programming concepts, Python syntax, data types, algorithms, and flowcharts, using simple analogies.	Remember (L1), Understand (L2)	PSO1, PSO5
CO2	Explain functions, modules, and file handling mechanisms in Python, with step-by-step breakdowns for non-coders.	Understand (L2)	PSO1, PSO3, PSO5
CO3	Apply OOP concepts, control structures, and regular expressions to solve simple programming problems in security contexts.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO4	Analyze and debug Python scripts for common errors in cybersecurity contexts, drawing from beginner-friendly books.	Apply (L3), Analyze (L4)	PSO1, PSO2, PSO3, PSO5
CO5	Identify Python's utility in scripting for digital forensics tasks, building confidence through referenced texts.	Understand (L2), Analyze (L4)	PSO1, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	Python Crash Course (3rd Ed., 2023)	Eric Matthes / No Starch Press
2	Automate the Boring Stuff with Python (2nd Ed.)	Al Sweigart / No Starch Press
3	Black Hat Python (2nd Ed., 2021)	Justin Seitz, Tim Arnold / No Starch Press
4	Violent Python (2nd Ed.)	TJ O'Connor / Syngress
5	Python for Cybersecurity: Using Python for Cyber Offense and Defense	Heather Shannon, Alexey Soshin / Wiley

Major Practical – Python Programming & Networks Lab

Course Code	Course Title	Course Type	Credits	Duration
• RJMAJCSDFP111	Python Programming & Networks Lab	Major Practical	2	60 Hours

Course Objectives

Sr. No.	Objective
1	Implement basic Python programs to reinforce syntax, data types, control structures, and functions for cybersecurity data handling.
2	Develop simple scripts using loops, collections, modules, and file I/O to simulate network log parsing and error management.
3	Practice object-oriented basics and string patterns for introductory forensic scripting tasks.
4	Simulate network topologies, devices, and protocols using Cisco Packet Tracer to understand OSI/TCP/IP models and connectivity.

Practical Assignments

10 Python Labs (Using IDLE or Jupyter Notebook)

Practical No.	Task / Title	Description
1	Python: Hello World with Input	Write Python program to print "Hello, Cyber Security!" with user input for name.
2	Python: Variable Operations	Write Python program to declare variables for IP (str), port (int), status (bool); perform arithmetic and type conversions.
3	Python: Password Checker	Write Python program to check password strength using if-elif-else (length >8, has digit).
4	Python: Loops with Break	Write Python program using for/while loops to print ports 1-1024; add break/continue.
5	Python: List Operations	Write Python program to create IP list; append, slice, sort, and check membership.
6	Python: Function Validation	Write Python program to define function for email validation; use positional/keyword params and lambda.

7	Python: Module Usage	Write Python program to import math/random/os; generate random password and list directory.
8	Python: File Handling	Write Python program to read/write log file; use try-except for FileNotFoundError.
9	Python: String Regex	Write Python program to split/join strings; use re module for basic email pattern matching.
10	Python: OOP Class	Write Python program to define class NetworkDevice with attributes/methods; add inheritance and try-except for IP input.

10 Networking Labs (Using Cisco Packet Tracer)

1	Networks: Basic Connectivity	Using Cisco Packet Tracer, connect 2 PCs via switch; ping and observe PDU.
2	Networks: Bus Topology	Using Cisco Packet Tracer, build bus topology with 3 PCs; ping and note collisions.
3	Networks: Star Topology	Using Cisco Packet Tracer, build star topology with hub/switch; compare broadcasts.
4	Networks: HTTP Simulation	Using Cisco Packet Tracer, simulate PC-to-PC HTTP; trace OSI layers in simulation mode.
5	Networks: IP Assignment	Using Cisco Packet Tracer, assign IPv4 IPs to 3 PCs (192.168.1.0/26); ping and subnet.
6	Networks: Media Comparison	Using Cisco Packet Tracer, connect PCs with twisted pair/coaxial/wireless; compare pings.
7	Networks: Inter-LAN Routing	Using Cisco Packet Tracer, connect 2 LANs via router; add static routes and inter-ping.
8	Networks: ARP/ICMP Capture	Using Cisco Packet Tracer, ping between PCs; capture ARP/ICMP in simulation.
9	Networks: ACL Block	Using Cisco Packet Tracer, configure ACL on router to block one subnet's traffic.
10	Networks: Troubleshooting	Using Cisco Packet Tracer, build faulty network (IP mismatch); troubleshoot with ping/traceroute/show commands.

CO–PSO Mapping

CO	Outcome	Bloom's	PSO
CO1	Execute Python programs for data types, operators, and control structures in simple cyber scenarios.	Apply (L3)	PSO1, PSO5
CO2	Demonstrate loops, functions, and file handling for log analysis and automation scripts.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO3	Implement OOP classes and string/regex basics for network object simulations.	Apply (L3)	PSO1, PSO3, PSO5
CO4	Configure and test network topologies, devices, and protocols in Packet Tracer simulations.	Apply (L3), Analyze (L4)	PSO1, PSO2, PSO3, PSO5
CO5	Troubleshoot IP/subnetting, routing, and connectivity issues using virtual lab tools.	Apply (L3), Analyze (L4)	PSO1, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	Hands-On Python for Cybersecurity	Dr. Deepti Gupta / BPB Publications
2	Black Hat Python (2nd Ed., 2021)	Justin Seitz, Tim Arnold / No Starch Press
3	Python Network Programming Cookbook (2nd Ed.)	Pradeepta Mishra / Packt Publishing
4	Introduction to Networks Companion Guide (CCNAv7)	Cisco Networking Academy / Cisco Press
5	Lab Manual for Computer Networks (B.Sc. IT, Mumbai University)	Various / Internal Publication

SEMESTER II

Major Core (Theory) – Fundamentals of Cyber Security

Course Code	Course Title	Course Type	Credits	Hours
RJMAJCSDF121	Fundamentals of Cyber Security	Major Core (Theory)	2	30

Course Objectives

Sr. No.	Course Objective
1	Understand core principles of information security and the CIA triad.
2	Explain risk management frameworks and access control models.
3	Learn authentication mechanisms and AAA (Authentication, Authorization, Accounting).
4	Explore security policies, compliance standards, and basic governance.
5	Develop awareness of ethical hacking principles and secure development practices.

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
I	**Security Principles** • What is Cyber Security?; What is Digital Forensics?; Application and Role of Cyber Security & Digital Forensics. • CIA Triad: Detailed definitions with examples. • Threats and Vulnerabilities: Common threats (insider, external hackers), vulnerability types (software flaws, human error); threat modeling basics (e.g., STRIDE: Spoofing, Tampering, etc.); discussion on attack surfaces in networks/forensics. • Defense-in-Depth: Layered strategies (physical, technical, administrative); components like antivirus, firewalls; case study: Multi-layer defense in a corporate setup. • Security Models: Bell-LaPadula model (no read-up, no write-down for confidentiality); Biba model (no read-down, no write-up for integrity); simple flow diagrams and pros/cons.	15
II	Access Control and Compliance • AAA Frameworks: Authentication (something you know/have/are – passwords, tokens, biometrics); Authorization (DAC, MAC, RBAC models); Accounting (audit logs, SIEM basics); integration examples in OS like Linux PAM. • Risk Management: Identification (asset valuation), assessment (qualitative matrices, quantitative CVSS scoring); mitigation strategies (avoid, transfer, accept); tools like risk registers. • Policies and Compliance: Security policy lifecycle (development, implementation); standards (ISO 27001 controls, NIST framework, GDPR principles for PII); compliance audits and reporting.	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Describe security principles, models, and the CIA triad.	Remember (L1), Understand (L2)	PSO1, PSO5
CO2	Explain access control mechanisms and risk assessment techniques.	Understand (L2)	PSO1, PSO3, PSO5
CO3	Apply AAA concepts to basic security scenarios.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO4	Analyze compliance requirements and ethical implications in organizations.	Apply (L3), Analyze (L4)	PSO1, PSO2, PSO3, PSO5
CO5	Identify foundational practices for secure systems and hacking ethics.	Understand (L2), Analyze (L4)	PSO1, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	Fundamentals of Information Security (2011)	John A. Blackley / Wiley
2	Cyber Security Essentials (2018)	Charles J. Brooks et al. / Syngress
3	Principles of Information Security (7th Ed., 2023)	Michael E. Whitman, Herbert J. Mattord / Cengage Learning
4	Cybersecurity for Beginners (2017)	Raef Meeuwisse / Cyber Simplicity
5	The Fifth Domain (2019)	Richard A. Clarke, Robert K. Knake / Penguin Press

Major Core (Theory) – Basics of Cryptography

Course Code	Course Title	Course Type	Credits	Duration

RJMAJCSDF122	Basics of Cryptography	Major Core (Theory)	2	30 Hours

Course Objectives

Sr. No.	Course Objective
1	Understand symmetric encryption algorithms and modes.
2	Explain asymmetric key systems and key exchange.
3	Learn hash functions, digital signatures, and PKI.
4	Explore basic cryptanalysis and attack types.
5	Develop awareness of cryptography's role in secure communications.

Unit-wise Detailed Syllabus

Unit	Detailed Contents	Hours
I	• Introduction to Cryptography and Symmetric Systems • History of Cryptography: Classical ciphers (Caesar shift, substitution/transposition); monoalphabetic/polyalphabetic (Vigenère); Enigma machine in WWII; transition to computers (DES origin in 1970s). • Symmetric Encryption Basics: Secret key sharing problems; block vs. stream ciphers; DES (64-bit block, 56-bit key, Feistel structure with 16 rounds); weaknesses (differential cryptanalysis). • AES and Modes: AES (Rijndael algorithm, 128/192/256-bit keys, S-box substitution); modes (ECB for simplicity, CBC for chaining with IV, OFB/CTR for streaming); padding (PKCS#7). • Stream Ciphers: RC4 (state-based keystream, S-box permutation); IV usage and attacks (fluhrer-mantin-shamir on WEP).	15
II	• Asymmetric Cryptography and Applications • Asymmetric Foundations: Public/private key pairs; Diffie-Hellman key exchange (discrete log problem, g^a mod p); man-in-the-middle defenses. • RSA Algorithm: Prime generation, e/n/d computation (Euler's totient); encryption (c = m^e mod n); decryption; padding (OAEP for security). • ECC and Signatures: Elliptic curve cryptography (y^2 = x^3 + ax + b over finite fields); ECDSA for signatures (hash + curve point multiplication). • Hashes and PKI: Secure hash algorithms (SHA-1 flaws, SHA-256 Merkle-Damgård); digital signatures (sign(hash(m))); PKI (CAs, CRLs, certificates like X.509); attacks (birthday for collisions, timing for side-channel).	15

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level	PSO Mapped
CO1	Describe symmetric ciphers and modes.	Remember (L1), Understand (L2)	PSO1, PSO5
CO2	Explain asymmetric systems and key exchange.	Understand (L2)	PSO1, PSO3, PSO5
CO3	Apply hash/signature concepts.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO4	Analyze common attack vectors.	Apply (L3), Analyze (L4)	PSO1, PSO2, PSO3, PSO5
CO5	Identify cryptography in secure systems.	Understand (L2), Analyze (L4)	PSO1, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	Cryptography and Network Security (8th Ed., 2023)	William Stallings / Pearson
2	Introduction to Modern Cryptography (3rd Ed., 2020)	Jonathan Katz, Yehuda Lindell / Chapman & Hall
3	Handbook of Applied Cryptography (1996)	Alfred J. Menezes et al. / CRC Press
4	Serious Cryptography (2017)	Jean-Philippe Aumasson / No Starch Press
5	Understanding Cryptography (2010)	Christof Paar, Jan Pelzl / Springer

Major Practical – Cyber Security Fundamentals & Cryptography Lab

Course Code	Course Title	Course Type	Credits	Duration
RJMAJCSDFP121	Cyber Security Fundamentals & Cryptography Lab	Major Practical	2	60 Hours

Course Objectives

Sr. No.	Objective
1	Implement foundational security tools for encryption, logging, and traffic analysis.
2	Practice vulnerability detection and access restriction using simulation environments.
3	Simulate AAA processes and risk evaluation in virtual networks.
4	Apply ethical scanning and compliance checks with beginner-friendly tools.

Practical Assignments

10 Cyber Security Fundamentals Lab

Practical No.	Task / Title	Description
1	Traffic Capture	Using Wireshark, capture local traffic and filter for HTTP requests on port 80.
2	Firewall Configuration	Using Cisco Packet Tracer, configure a firewall rule on a router to block ICMP pings from a subnet.
3	2FA Setup	Using Google Workspace Admin Console, enable 2FA for a test user account.
4	SSL Decryption	Using Wireshark, decrypt a sample SSL/TLS session with known keys.
5	Password Policy	Using Cisco Packet Tracer, simulate password policy enforcement on a switch CLI.
6	ARP Analysis	Using Wireshark, analyze ARP traffic for spoofing indicators in a simulated network.
7	VLAN ACL	Using Cisco Packet Tracer, set up VLAN ACLs to restrict access between segments.
8	Audit Log Report	Using Google Workspace, create an audit log report for user sign-ins.
9	DNS Inspection	Using Wireshark, capture and inspect DNS queries for resolution patterns.
10	Static Routes with ACL	Using Cisco Packet Tracer, configure static routes with access lists for traffic control.

10 Cryptography Lab

1	Symmetric Encryption (AES)	Using Python (pycryptodome), implement AES-CBC encryption/decryption of a sample file; generate and verify IV.
2	Hash Function Verification	Using OpenSSL, compute SHA-256 hash of a document; compare with Python-generated hash for integrity check.
3	RSA Key Generation	Using OpenSSL, generate RSA public/private key pair; encrypt a message with public key and decrypt with private.
4	Diffie-Hellman Exchange	Using Python, simulate Diffie-Hellman key exchange between two parties; compute shared secret.
5	Digital Signature Creation	Using OpenSSL, create ECDSA signature on a file; verify signature integrity.
6	PKI Certificate Generation	Using OpenSSL, generate self-signed X.509 certificate; inspect details with openssl x509 command.
7	Stream Cipher (ChaCha20)	Using Python, encrypt/decrypt text with ChaCha20; test nonce reuse vulnerability.
8	Mode Comparison (ECB vs CBC)	Using OpenSSL, encrypt image with AES-ECB and AES-CBC; visually compare patterns for security flaws.
9	Hash Collision Demo	Using Python, demonstrate basic MD5 collision (pre-image attack simulation); discuss migration to SHA-3.
10	Hybrid Encryption	Using OpenSSL and Python, combine RSA for key wrap and AES for data encryption; decrypt full message.

CO–PSO Mapping

CO	Outcome	Bloom's	PSO
CO1	Execute tool-based configurations for firewalls, encryption, and logging.	Apply (L3)	PSO1, PSO5
CO2	Demonstrate scanning and access control in simulated scenarios.	Understand (L2), Apply (L3)	PSO1, PSO3, PSO5
CO3	Implement AAA and basic risk simulations.	Apply (L3)	PSO1, PSO3, PSO5
CO4	Analyze tool outputs for ethical and compliance insights.	Analyze (L4)	PSO1, PSO2, PSO3, PSO5

Textbooks & References

Sr. No.	Title	Author / Source
1	Cyber Security Essentials Lab Manual	Charles J. Brooks et al. / Syngress

2	Hands-On Cybersecurity with Wireshark	Chris Brenton / Packt
3	Cisco Networking Academy Labs	Cisco Press
4	Cryptography Labs for Beginners	William Stallings / Pearson
5	Practical Packet Analysis (3rd Ed.)	Chris Sanders / No Starch Press