Annexure-2

BACHELOR OF COMPUTER APPLICATIONS (BCA)
Specialization in Cyber Security (Cyber Dojo)
Academic Curriculum (2025 – 26 onwards)

First Year
Curriculum Component

Component	Credit (BCA)
1. University core (3 courses)	6
2. University Elective (2courses)	6
3. Basic Science (2 courses)	6
4. Program Core (26 courses)	77
5. Program Elective (4 courses)	-
6.Project/Seminar (2 courses)	22
7. Proficiency (Non Credit/Non Graded)	-
Total	**117**

	Course Type	Course Title	Contact Hrs Per Week			Credits	ETE Duration Hours	Weightage %			
			L	T	P			CW	MTE	PBL	ETE
Autumn Semester	UC 23.101	Human Values & Professional Ethics	2	0	0	2	3	10	40		50
	CA 25.102	Cyber Security Fundamentals	3	-	-	3	3	10	40		50
	CA 23.103	C Programming	3	-	-	3	3	10	40		50
	CA 23.107	Foundation Course in Mathematics	3	1	-	4	3	10	40		50
	CY23.102	Environmental Studies	2	0	0	2	3	10	40		50
	FL	Foreign Language*(Non Grade)	3	-	-	3	3	25	25		50
	CA 25.133	Operating Systems Fundamentals	2	-	2	3	3	10	40		50
	CA 23.135	C Programming Laboratory	-	-	4	2	2	20	20	20	40
	SF 101	Personal Grooming and Fine Dining (Non Grade)	0	0	1	1	2	50			50
		Sub Total	**16**	**1**	**07**	**19**					

	Course Type	Course Title	Contact Hrs per Week			Credits	ETE Duration Hour	Weightage %			
			L	T	P			CW*	MTE	PBL	ETE
Spring Semest	UC 23.102	Pragmatic English Communication	2	0	0	2	3	10	40		50
	UE	University Elective-I	3	-	-	3	3	10	40		50
	CA 25.106	Networking from Security Perspective	4	-	-	4	3	10	40		50
	CA 23.104	Data Structures	3	-	-	3	3	10	40		50
	FL	Foreign Language*(Non Grade)	3	-	-	3	3	25	25		50
	CA 23.134	Data Structures Laboratory	-	-	4	2	2	20	20	20	40
	CA 23.136	Python Programming Laboratory	-	-	4	2	2	20	20	20	40

BACHELOR OF COMPUTER APPLICATIONS (BCA)
Specialization in Cyber Security (Cyber Dojo)
Academic Curriculum (2025 – 26 onwards)

	CA 25.138	Networking from Security Perspective Lab			4	2		20	20	20	40
	SF 102	Social Grooming, Home & Decor and Business Communication (Non Grade)	0	0	2	1	2	50			50
		Sub Total	**18**	**1**	**14**	**18**					

Second Year
Curriculum Component

	Course Type	Course Title	Contact Hrs per Week			Credits	ETE Duration Hours	Weightage %			
			L	T	P			CW	MTE	PBL	ETE
Autumn Semester	CA 23.201	Computer Organization	3	1	-	4	3	10	40		50
	CA 23.203	Database Management System	3	-	-	3	3	10	40		50
	CA 25.205	**Network Defence and Network Analysis**	4	-	-	4	3	10	40		50
	CA 25.207	**End Point Security**	3	-	-	3	3	10	40		50
	FL	Foreign Language*(Non Grade)	3	-	-	3	3	25			50
	CA 23.233	Database Management System Laboratory	-	-	4	2	3	20	20	20	40
	CA 25.235	**Network Defence and Network Analysis** Laboratory	-	-	4	2	3	20	20	20	40
	CA 25.237	**End Point Security Lab**			4	2	3				
	SF 201	Personal Grooming Fine Dining and Home Safety (Non Grade)	0	0	2	1	2	50			50
		Sub Total	**16**	**1**	**14**	**20**					

	Course Type	Course Title	Contact Hrs per Week			Credits	ETE Duration Hours	Weightage %			
			L	T	P			CW	MTE	PBL	ETE
Spring Semester	UC 25.201	Management and Entrepreneurship	2	0	0	2	3	10	40		50
	UE	University Elective-2	3	-	-	3	3	10	40		50
	CA 25.204	**Network & Systems VA /PT**	3	0	-	3	3	10	40		50
	CA 25.206	**Post Exploitation and Advanced Techniques**	3	0	-	3	3	10	40		50
	CA 23.210	Java Programming	3	-	-	3	3	10	40		50
	FL	Foreign Language*(Non Grade)	3	-	-	3	3	25	25		50
	CA 25.234	**Network & Systems VA /PT Lab**	0	0	4	2	2	20	20	20	40
	CA 25.238	**Post Exploitation and Advanced Techniques Lab**	0	0	4	2	2	20	20	20	40

BACHELOR OF COMPUTER APPLICATIONS (BCA)
Specialization in Cyber Security (Cyber Dojo)
Academic Curriculum (2025 – 26 onwards)

	CA 23.236	Java Programming Laboratory	-	-	4	2	2	20	20	20	40
	SF 202	Social Grooming and Professional Skills(Non Grade)	0	0	2	1	2	50			50
		Sub Total	**17**	**0**	**14**	**20**					

BACHELOR OF COMPUTER APPLICATIONS (BCA)
Specialization in Cyber Security (Cyber Dojo)
Academic Curriculum (2025 – 26 onwards)
Third Year
Curriculum Component

	Course Type	Course Title	Contact Hrs per L	T	P	Credits	ETE Duration Hours	Weightage % CW	MTE	ETE
Autumn Semester	CA23.303	**Software Engineering**	3	0	0	3	3	10	40	50
	CA 25.305	**Web Application Security**	3	-	-	3	3	10	40	50
	CA 25.307	**Threat Analysis and Advanced Security Operations**	3	0	0	3	3	10	40	50
	CA 25.309	**Incident Response & Redressal**	3	-	0	3	3	10	40	50
	CA 25.351	**Threat Analysis and Advanced Security Operations Lab**	0	0	4	2	2	20	20	20
	CA 25.353	**Incident Response & Redressal lab**	0	0	4	2	2	20	20	20
	CA 25.355	**Web Application Security Lab**	0	0	4	2	4	20	20	20
	FL	Foreign Language*(Non Grade)	3	-	-	3	3	25	25	
	CA 25.339	Minor Project	-	-	-	7	-			100
		Sub Total	**15**	**0**	**12**	**25**				

	Course Type	Course Title	Contact Hrs per Week L	T	P	Credits	ETE Duration Hours	CW Weightage %	MTE	ETE
Spring Semester	CA 23.312	Major Project*	-	-	-	15	-			100
		Sub Total				**15**				

Total Credits = 37+40+40=117

MTE : *Mid Term Examination*

ETE : *End Term Examination*

·Major Project: Spring Semester of third year will be exclusively for project training in an organization in which student shall be required to work on a project assigned by such organizations in consultation with the concerned Internal Supervisor allotted to her from the faculty members of the department. However, In exceptional conditions HOD may allow any student to undergo the project training in the campus under the supervision of faculty member assigned to her. At the end of the semester the student shall be required to submit a Project Report based on the project given to her. A committee of the Internal Supervisor & External Examiner will evaluate the report & conduct viva- voce.

BACHELOR OF COMPUTER APPLICATIONS (BCA)
Specialization in Cyber Security (Cyber Dojo)
Academic Curriculum (2025 – 26 onwards)

***Choose any one which shall remain in all six semesters**

Semester- I

FL 20.101	French Language & Grammar-I
GL 20.101	German Language & Grammar-I
JL 20.101	Japanese Language & Grammar-I
SL 20.101	Spanish Language & Grammar-I

Semester-II

FL 20.102	French Language & Grammar-II
GL 20.102	German Language & Grammar-II
JL 20.102	Japanese Language & Grammar-II
SL 20.102	Spanish Language & Grammar-II

Semester- III

FL 20.201	French Language & Grammar-III
GL 20.201	German Language & Grammar-III
JL 20.201	Japanese Language & Grammar-III
SL 20.201	Spanish Language & Grammar-III

Semester- IV

FL 20.202	French Language & Grammar-IV
GL 20.202	German Language & Grammar-IV
JL 20.202	Japanese Language & Grammar-IV
SL 20.202	Spanish Language & Grammar-IV

Semester- V

FL 20.301	French Language & Grammar-V
GL 20.301	German Language & Grammar-V
JL 20.301	Japanese Language & Grammar-V
SL 20.301	Spanish Language & Grammar-V

**MOOC courses will be approved by Department.

Credit Distribution across all Components

Semester		UC	UE	BS	ES	PC	PE/SE	MOOC	Proj/Seminar	Total
First		2	-	6	-	11	-	-		19
Second		2	3	-	-	13				18
Third		0		-		20				20
Fourth		2	3			15	0			20
Fifth						18		-	7	25
Sixth									15	15
BCA	**Total**	**6**	**6**	**6**		**77**	**0**	**-**	**22**	**117**

Exit Options:

I. After II Semester - Exit option with Certificate in Computer Applications (with a minimum of 40 credits)
II. After IV Semester - Exit option with Diploma in Computer Applications (with a minimum of 86 credits)
III. After VI Semester - Exit Option with Bachelor of Computer Applications Degree, BCA Degree (with aminimum of 108 credits)

BCA -(2025-28) Batch Onwards

CA 25.133 **Operating Systems Fundamentals** **Total Lectures: 40**
Credit: 2-0-2-3

Prerequisite(s): Basic Computer Knowledge

Objective(s):

- The objective of this course is to provide learners with a foundational understanding of operating systems, including their structure, functionality, and role in managing computer hardware and software resources.
- Grasp key concepts such as process management, memory management, file systems, input/output control, and basic security mechanisms.
- This course lays the groundwork for further studies in computer science, systems administration, and cyber security.

1	**Introduction to OS** What is OS, components of OS, types of OS : distributed, multi-user, network etc, Working of an OS - from hardware & software perspective, Services in an OS, Processes in an OS, Process Scheduling, Scheduling Algorithms - FCFS, SJN/F, RR, Priority, Multilevel Queue Scheduling, Multilevel Feedback Queue Scheduling, Types/ Classification of scheduling algorithms, Multi-threading - What, benefits & types, Multi-processing - What, benefits & types, Multi-threading vs Multi-processing, Instruction Streams & Data Streams, SISD, SIMD, MISD, MIMD, Memory Management, Virtual Memory, I/O Hardware, I/O Software, File Systems, Platform Agnostic Security Mechanisms in an OS, Microsoft Windows OS, Linux OS, UNIX OS.	[5]
2	**Working on the OS** Introduction to OS Security - Windows - user management, user account creation & management, user account privilege management, user account access control, user account control panel, local security policy, group policy editor, windows firewall, remote desktop, service management, disk management, file system, application installation.	[10]
3	**Linux and Windows Basics** Linus file systems structure, terminal commands, practical use of Ubuntu, kali and virtual machine etc. Windows Interface & Settings, Control panel Vs Settings, Task Manager , Service registry basics	[10]
4	**Windows & Linux Security** Windows - understanding virtual memory, physical memory, paging & page files, memory protection, introduction to concepts of group administration, tools for group administration like Active directory, LDAP etc. Advantages of group policies, main terminologies & components, domain controller Introduction to types of users and groups like privileged accounts/users, security groups, general user etc., Introduction to RAID on Linux, RAID levels (0, 1 and 5), Resizing the Partition using LVM,.	[15]
5	**Modern Trends and Case Studies** Mobile OS vs. Desktop OS, Containerization and OS virtualization (Docker, VMs),Cloud-based OS and micro services, Case study: Linux vs. Windows internals, Emerging OS technologies (e.g., uni kernels)	[5]

BCA -(2025-28) Batch Onwards

Outcome(s):

- Understand the role and purpose of operating systems
- Analyze and describe OS architecture and core components
- Explain and manage processes and threads
- Understand concurrency and synchronization
- Apply memory management techniques.
- Explain and evaluate file systems and storage management
- Understand I/O management and device communication
- Identify OS-level security and protection mechanisms
- Perform basic OS installation, configuration, and troubleshooting

Text Books: CyberDojo Content through LMS

Reference Books:

1. Trent Jaeger ,"Operating System Security" Morgan & Claypool Publishers,2010,
2. Kyle Rankin , "Linux Hardening in Hostile Networks: Server Security from TLS to Tor" Addison-Wesley Professional , ISBN: 978-0134173269 ,2017

BCA (2025-28) Batch Onwards

CS 25.106 **Networking from Security Perspective** **Total Lectures: 40**
Credit: 3-0-0-3

Prerequisite(s): Basic Computer Knowledge

Objective(s): Designed to provide learners with a comprehensive understanding of computer networking concepts through the lens of cybersecurity.

The primary objective is to equip students with the foundational knowledge of network architectures, protocols, and operations, while emphasizing how these components are targeted, exploited, and secured in modern network environments.

1	**Basics of data communication & network protocols** Basic Terminologies - Sender, Receiver, Message, etc, Digital Communication - What, Types, etc, Networks - Based on topology, Based on geography, OSI Model & its layers, TCP/IP Model & its layers, TCP/IP & its layer protocols, TCP/IP Network Devices - based on the layers, Protocols - DHCP, DNS, ICMP, SSL, MIME, S/MIME, SMTP, IMAP, POP, PGP, DNS Sec, TLS, HTTP, HTTPS, SSH, Telnet, FTP, SFTP..	[5]
2	**Working on network devices** Internet Protocol (IP), IP addressing, Classful vs Classless IP addressing, Subnetting vs Supernetting, Switching - phases, benefits etc, Routing - basics, process, protocols & advantages, VLAN, VLAN tagging & IDs, ACLs - types, rules, configuration, purposes, Network topology in detail - bus, ring, star, mesh, tree, hybrid etc.	[15]
3	**Advanced Windows Networking** Quick Recap: networking-infrastructure components, such as cabling, routers, hubs, and switches & Protocols, Planning & Implementing IPv4 & IPv6 : addressing, configuring hosts, implementing IPv4 & IPv6 coexistence etc, Implementing DHCP : deploy, manage & troubleshoot DHCP, Implement DNS : implement servers, configure - zones, name resolution between DNS zones, DNS integration with Active Directory Domain Services (AD DS) & advanced DNS settings, Implement & manage IPAM : deploy IPAM, manage IP address spaces using IPAM.	[7]
4	**Implement remote access** : remote access options, managing remote access, installing remote access server role, configuring routing and NAT, WAP, configuring WAP, DAS - components, configuration & deployment options, Networking features and considerations for branch offices, Implementing Distributed File System (DFS) for branch offices, Implementing BranchCache for branch offices, Overview of high performance networking features, Configuring advanced Microsoft Hyper-V networking features, Overview of SDN, Implementing network virtualization, Implementing Network Controller	[8]
5	**Advanced Linux Networking** Quick Recap: linux networking commands - ipfconfig, traceroute, ping, scp command, etc, UFW & System Firewall, Network Configuration : configuring IPv6 address & performing basic IPv6 troubleshooting in linux, routing IP traffic and creating static routes, Configuring NAT (in linux) - Masquerade &	[15]

port forwarding, Configuring systems as iSCSI target & initiator, Use procsys & sysctl to modify/set kernel runtime parameters, produce and deliver reports on system utilization, Configure SELinux & use it for port labelling to allow services to use non-standard ports, Configure Apache virtual host, access restrictions on directories, group managed content, configure TLS security, Configure a caching-only name server, provide network shares to specific clients-client installation & configuration, Use Kerberos to control access to NFS network shares - configure Kerberos & NFS server.

Outcome(s):

1. Explain Core Networking Concepts**.**
2. Identify and Analyze Network Protocols
3. Design and Evaluate Secure Network Architectures
4. Explain and manage Advance windows & Linux networking concepts like IPAM. Domain Controller, IPV4 & IPV6, Firewall, NAT Extra

Text Books:

CyberDojo Content through LMS

Reference Books:

1. James F. Kurose and Keith W. Ross Computer Networking: A Top-Down Approach" by, 7th ed.,Pearson, 2020
2. Darril Gibson "Microsoft Windows Networking Essentials",Sybex, ISBN: 978-1118016855, 2011
3. Carla Schroder, "Linux Networking Cookbook", O'Relly,2007.

BCA 2025-29) Batch Onwards

CA 25.102 **Cyber Security Fundamentals** **Total Lectures: 40**
Credit: 3-0-0-3

Prerequisite(s): Nil

Objective(s):

- The objective of this course is to introduce learners to the foundational principles, practices, and technologies of cybersecurity.
- By the end of the course, participants will have a solid understanding of core cybersecurity concepts, common threat types, basic defense mechanisms, and the importance of securing information systems.
- The course is designed to equip learners with the knowledge needed to identify risks, understand attack vectors, and apply basic security controls in real-world environments, serving as a stepping stone for more advanced cybersecurity study or careers.

1	**Understanding Of IT Concepts:** Understand the basics of hardware and operating systems, Networking Fundamentals, types of software, basics of software installation & maintenance, Develop Basic problem solving skills,	[5]
2	**Introduction to Cyber Security:** What is Cyber Security & Its importance, definition and challenges in Cyber Security, Key terminologies in Cyber Security, Cyber threats, vulnerability and risk, types of attack: active attacks, passive attacks, motives of attackers, layers of security, CIA Triad, types of security attacks, security services and mechanisms.	[5]
3	**Basic Cyberspace Concepts:** Cyberspace, importance, definition and challenges in Cyber Security, Cyber threats, vulnerability and risk, Introduction to types of attack: active attacks, passive attacks, motives of attackers, layers of security, CIA Triad, types of security attacks, security services and mechanisms. Introduction to key terminologies used in Cyber Security like proxy servers and anonymizers, phishing, password cracking, keyloggers and spywares, virus and worms, Trojan horses and backdoors, steganography, DoS and DDoS attacks, SQL injection, buffer overflow, attacks on wireless networks, phishing . and identity theft.	[10]
4	**Stay Safe Online:** Best practices to stay safe online, introduction to concepts like strong password, MFA, Safe browsing, identifying fake web sites and avoiding scams Use of personal security tools like Antivirus, personal firewall, secure USN drives, Basic security on home routers. .	[10]
5	**Basics of How are websites hacked, Key precautions & What happens during an attack:** How can websites be hacked, what developers do to protect Aaps. Basics of How to test security of App & Websites, basic understanding of what happens durng an attack, how companies respond and what role does a security team play and importance of logs and alerts	[10]

Outcome(s): On successful completion of this course, students will be able to

- Understand IT Fundamentals, cyberspace, cybersecurity fundamentals, threats, and risks.
- Basic Understanding of cyber-attacks, motives, and layered security.
- Basic Understanding of cybercrime types and tools including malware, phishing, and keyloggers.
- Understanding of real world cyber threats and attacks
- Understanding on career opportunities and skill requirements in Cyber Security

BCA 2025-29) Batch Onwards

Text Books:

1. CyberDojo Content Through LMS

Reference Books:

1. Bhushan, Rathore et al. Fundamental of Cyber Security (Principles, Theory & Practices), BPB Publications, I ed. New Delhi. ISBN 978-9386551559

2. Anand Shinde , Introduction to Cyber Security : Guide to the World of Cyber Security Paperback. Notion Press, I ed. ISBN 978-163781642

BCA (2025-28) Batch Onwards

CA 25.138 **Networking from Security Perspective Laboratory**

Total Hours: 26

Credit: 0-0-2-2

Prerequisite: Basic Security Knowledge, Basic Command-Line Skills, Basic Understanding of Computer Networks, Familiarity with Networking Protocols

Objectives: The objective of this course is to:

- To gain hands-on experience in configuring and securing operating systems, including user permissions, access controls, and patch management on Linux and Windows platforms.
- To analyze and monitor network traffic using tools like Wireshark and tcpdump for identifying suspicious activities and understanding protocol vulnerabilities.
- To implement network security mechanisms such as firewall rules, VPNs, and secure communication protocols (e.g., SSL/TLS) in a controlled lab environment.
- To simulate common operating system and network attacks (e.g., privilege escalation, ARP spoofing, man-in-the-middle) and develop appropriate defense strategies.
- To understand the process of system hardening and baseline security configuration on different OS and network devices.

Contents:

- Introduction to Active Directory & Lab Environment Setup
- Installing Active Directory Domain Services (AD DS)
- Domain Controller Deep Dive & AD Structure
- Advanced Group Policy Objects (GPOs) and Basic OS Commands
- Advanced Security and Windows OS Commands
- Adding Windows Client to AD Domain
- User and Group Management
- Installing and Configuring DNS in AD
- Installing and Configuring DHCP in AD Environment
- Troubleshooting & Security Hardening in AD
- Packet Analysis with Wireshark – Capturing and Analyzing Traffic
- Network Scanning with Nmap – Host Discovery and Port Scanning
- Banner Grabbing and Service Fingerprinting (Netcat, Nmap scripts)
- Protocol-Level Attacks: ARP Spoofing and MITM (Using Ettercap/Bettercap)
- DNS Attacks and DNS Monitoring using Packet Capture
- Network Segmentation and VLAN Security Concepts (Simulation with Cisco Packet
- or GNS3)
- Simulating DoS and Recon Attacks – Detection and Mitigation Strategies
- Incident Simulation: Analyzing PCAPs and Building a Network Defense Report

Outcomes: Upon completion of this course, students are able to:

- Demonstrate the ability to configure secure user accounts, permissions, and access controls on Linux and Windows operating systems.
- Effectively capture and analyze network traffic to detect anomalies and understand common network protocol vulnerabilities.
- Simulate real-world OS and network attacks and apply mitigation techniques to prevent or minimize their impact.
- Perform system hardening tasks to improve the security posture of operating systems and network devices.