

Jharkhand Raksha Shakti University

Meur's Road SKIPA Premises, Ranchi



Course Framework

of

M.Sc. Programme

in

Computer Application and Cyber Security (Two Year)

(W.e.f. from Academic Year 2026-27)

DEPARTMENT OF CYBER DEFENCE

SSK
Dhawan
Shuchi Arora
Kishan
Rang

1. Introduction of the Programme:

Computer Application and Cyber Security is a multidisciplinary domain that plays a pivotal role in safeguarding digital ecosystems, ensuring data protection, and maintaining the integrity and resilience of information systems. The field integrates core concepts from computer science, information technology, mathematics, statistics, cybersecurity, and data analytics to address the complex and evolving challenges of the modern digital world.

The M.Sc. Programme in Computer Application and Cyber Security (Two-Year) is designed to provide advanced knowledge and specialized skills aligned with current industry requirements and technological advancements. The programme emphasizes both theoretical foundations and practical competencies, enabling students to develop a comprehensive understanding of secure computing environments.

The curriculum encompasses a wide range of contemporary and emerging areas, including:

- Advanced Network Security and Cryptography
- Operating Systems and Secure System Administration
- Programming, Software Engineering, and Secure Coding Practices
- Database Management Systems and Data Security
- Ethical Hacking, Penetration Testing, and Digital Forensics
- Cyber Law, Digital Ethics, and Governance
- Cloud Computing, Virtualization, and Security
- Artificial Intelligence and Machine Learning Applications in Cybersecurity

In addition to classroom learning, the programme incorporates hands-on laboratory sessions, real-world case studies, internships, and project work to ensure practical exposure to modern tools and technologies used in cybersecurity and IT industries.

This programme equips post graduates with the ability to identify vulnerabilities, design secure systems, detect and mitigate cyber threats, and respond effectively to security incidents. With the rapid digital transformation across sectors such as banking, healthcare, governance, defense, and education, there is a significant and growing demand for skilled cybersecurity professionals.

Post Graduates of the programme are well-prepared for diverse career roles, including:

- Cybersecurity Analyst
- Network Security Engineer / Administrator
- Information Security Officer
- Ethical Hacker / Penetration Tester
- Digital Forensics Expert
- Software Developer (Secure Systems)
- IT Security Consultant

SSB *[Signature]* Shuchi Bains *[Signature]* *[Signature]* *[Signature]*

Employment opportunities are available in government organizations, defense and intelligence agencies, IT and cybersecurity firms, financial institutions, multinational corporations, and research organizations.

Furthermore, the programme fosters critical thinking, analytical reasoning, and decision-making abilities, enabling students to take on leadership roles in the cybersecurity domain. As digital technologies continue to evolve, professionals trained in Computer Application and Cyber Security will remain indispensable in ensuring secure, reliable, and sustainable digital infrastructures.

2. Programme Objectives (POs)

Programme Objectives describe the advanced knowledge, skills, research capabilities, and professional competencies that students acquire during the course of the programme. The following Programme Objectives are endorsed for the M.Sc. Programme in Computer Application and Cyber Security:

➤ **Advanced Domain Knowledge**

To develop in-depth and advanced knowledge of computer science, cybersecurity, mathematics, and data analytics, enabling learners to address complex and emerging challenges in areas such as secure system design, advanced network security, cryptography, digital forensics, and intelligent cybersecurity systems.

➤ **Critical Problem Analysis**

To critically analyze, model, and solve complex and real-world problems in computing and cybersecurity using advanced mathematical, statistical, and computational techniques, fostering innovation and analytical reasoning.

➤ **Research and Innovation**

To design and develop innovative, research-oriented solutions using scientific methodologies, experimental design, and data-driven approaches in areas such as cybersecurity, artificial intelligence, digital forensics, and secure software systems.

➤ **Modern Tools and Technologies**

To effectively select, evaluate, and utilize advanced tools, platforms, and technologies including cloud computing, virtualization, AI/ML frameworks, cybersecurity tools, and simulation environments—for designing, implementing, and analyzing secure and scalable systems.

➤ **Secure System Design and Development**

To design, implement, and evaluate secure, reliable, and efficient computing systems and applications by integrating principles of secure coding, system architecture, risk assessment, and vulnerability management.

Handwritten signatures:
Shuchi Arora
Rajiv
SSK
Arjun
[Signature]

➤ **Effective Technical Communication**

To communicate complex technical ideas, research outcomes, and cybersecurity solutions clearly and professionally through technical reports, research publications, presentations, and digital media for diverse audiences.

➤ **Societal, Legal, and Global Perspective**

To assess the societal, ethical, and legal implications of cybersecurity practices, including cyber laws, digital rights, data protection regulations, and global security standards, contributing responsibly to digital governance and national security.

➤ **Leadership and Teamwork**

To demonstrate leadership, project management, and collaborative skills in multidisciplinary and multicultural environments, managing cybersecurity projects and teams effectively in professional settings.

➤ **Professional Ethics and Responsibility**

To uphold the highest standards of professional ethics, integrity, and accountability in cybersecurity practices, including responsible disclosure, data privacy, compliance with legal frameworks, and adherence to industry standards.

➤ **Lifelong Learning and Adaptability**

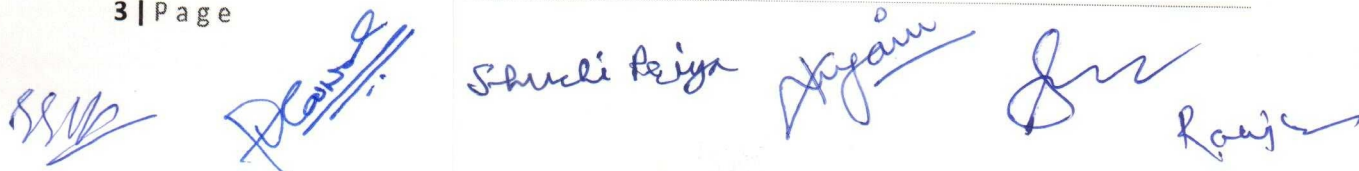
To cultivate a mindset of continuous learning and adaptability, enabling graduates to stay abreast of rapidly evolving technologies, cyber threats, and research advancements in computing and cybersecurity domains.

3. Programme Outcomes

Programme outcomes are defined by the National Assessment and Accreditation Council (NAAC) to ensure that educational programmes meet specific quality standards. The National Assessment and Accreditation Council (NAAC) designs these outcomes to measure students' achievements at the end of a programme, with a focus on the knowledge, skills, and attitudes they acquire. Outcomes for students include attaining profound expertise in their discipline, acquiring the ability to function in multidisciplinary domains, exercising research intelligence in investigations and innovations, and learning ethical principles.

The POs for M.Sc. Programme in Computer Application and Cyber Security (Two year) are as follows:

PO-1	To develop a deep understanding of both fundamental and advanced topics within the fields of Computer Science and Cyber Security.
PO-2	To build a strong foundation in computing principles, including programming, algorithms, system design, and secure computing practices.
PO-3	To develop critical thinking and problem-solving abilities for addressing complex computational and cyber security challenges using modern tools and techniques.



PO-4	To cultivate evidence-based decision-making skills by integrating mathematical foundations with computing and cyber security, while adhering to ethical, legal, and professional standards.
PO-5	To prepare competent professionals in Computer Application and Cyber Security capable of contributing effectively to industry, research, cyber security agencies, and societal well-being.
PO-6	To design and develop innovative, research-oriented solutions to contemporary challenges and promote lifelong learning in emerging areas of cyber security and computing.

Devi

Shuchi Priya

Arjun

Dr

Raj

8816

Course Structure

FIRST SEMESTER

Course Code	Course Title	Teaching Scheme			Examination Scheme			
		L	T	P	MS	ES	Total Marks	Total Credits
MCACS-101	Mathematical Foundation for Machine Learning	3	0	1	25	75	100	4
MCACS-102	Advanced Artificial Intelligence	3	0	1	25	75	100	4
MCACS-103	Advanced Operating System and Shell Programming	3	0	1	25	75	100	4
MCACS-104	Cryptography for Cyber Security	3	0	1	25	75	100	4
MCACS-105	Advanced Digital Forensic	3	0	1	25	75	100	4
		Total Credit			Total Marks		500	20

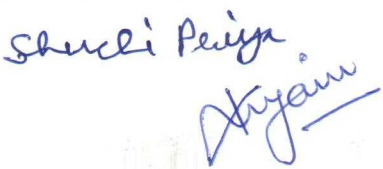
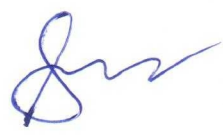
L: Lecture; T: Tutorial; P: Practical; MS: Mid-Semester; ES: End-Semester

SECOND SEMESTER

Course Code	Course Title	Teaching Scheme			Examination Scheme			
		L	T	P	MS	ES	Total Marks	Total Credits
MCACS-201	Advanced Java Programming	3	0	1	25	75	100	4
MCACS-202	Advanced Machine Learning and Data Analytics	3	0	1	25	75	100	4
MCACS-203	Database and Network Security	3	0	1	25	75	100	4
MCACS-204	Deep Learning for Computer Vision	3	0	1	25	75	100	4
MCACS-205	Internship	0	0	4	0	100	100	4
		Total Credit			Total Marks		500	20

L: Lecture; T: Tutorial; P: Practical; MS: Mid-Semester; ES: End-Semester




THIRD SEMESTER

Course Code	Course Title	Teaching Scheme			Examination Scheme			
		L	T	P	MS	ES	Total Marks	Total Credits
MCACS-301	Advanced Web Development	3	0	1	25	75	100	4
MCACS-302	Foundation of Natural Language Processing	3	0	1	25	75	100	4
MCACS-303	Elective-I	3	0	1	25	75	100	4
MCACS-304	Cloud Security	3	0	1	25	75	100	4
MCACS-305	Research Methodology	2	0	0	0	50	50	2
MCACS-306	Minor Project	0	0	2	0	50	50	2
		Total Credit			Total Marks		500	20

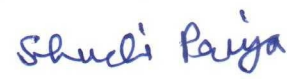
L: Lecture; T: Tutorial; P: Practical; MS: Mid-Semester; ES: End-Semester

FOURTH SEMESTER

Course Code	Course Title	Teaching Scheme			Examination Scheme			
		L	T	P	MS	ES	Total Marks	Total Credits
MCACS-401	Malware Analysis and Penetration Testing	3	0	1	25	75	100	4
MCACS-402	Blockchain Technologies	3	0	1	25	75	100	4
MCACS-403	Elective-II	3	0	1	25	75	100	4
MCACS-404	Quantum Technology	3	0	1	25	75	100	4
MCACS-405	Dissertation	0	0	4	0	100	100	4
		Total Credit			Total Marks		500	20

L: Lecture; T: Tutorial; P: Practical; MS: Mid-Semester; ES: End-Semester








ELECTIVE-1

Course Code	Course Title	Teaching Scheme			Examination Scheme			
		L	T	P	MS	ES	Total Marks	Total Credits
ELC-1	Advanced Computer Architecture	3	0	1	25	75	100	4
ELC-2	Pattern Recognition and Classification	3	0	1	25	75	100	4
ELC-3	Advanced Computer Network	3	0	1	25	75	100	4
ELC-4	Data Warehousing and Data Mining	3	0	1	25	75	100	4

L: Lecture; T: Tutorial; P: Practical; MS: Mid-Semester; ES: End-Semester

ELECTIVE-II

Course Code	Course Title	Teaching Scheme			Examination Scheme			
		L	T	P	MS	ES	Total Marks	Total Credits
ELC-5	Embedded System	3	0	1	25	75	100	4
ELC-6	Optimization Techniques	3	0	1	25	75	100	4
ELC-7	Mobile and Network Forensics	3	0	1	25	75	100	4
ELC-8	Threat Intelligence and Cyber Defense Strategies	3	0	1	25	75	100	4

L: Lecture; T: Tutorial; P: Practical; MS: Mid-Semester; ES: End-Semester

8813

Shuchi Anuja

Signature

Signature

Signature

Marks Distribution Scheme

Course	Credits	FM	MS		ES	
			T	P	T	P
Course (With Practical)	2	50	-	-	50	-
Course (With Practical)	4	100	15 (10+5) *	10	50	25
Core (Without Practical)	4	100	25 (20+5) *	-	75	-
Internship	4	100	-		Grade Point awarded and validated by concerned authorities	
Research						
i. Research Methodology	2	50	-		50	
ii. Thesis/Dissertation/Project	4	100	-		100	

T: Theory; P: Practical; MS: Mid Semester; ES: End Semester; FM: Full Marks

Note:

* - Internal assessment (15 marks) comprises 10 marks for mid-sem/internal evaluation (based on exams, assignments, quizzes, etc.) and 5 marks for attendance and overall performance.

** - Internal assessment (25 marks) comprises 20 marks for mid-sem/internal evaluation (based on exams, assignments, quizzes, etc.), and 5 marks for attendance and overall performance.

8819

Dr. P. S. Singh

Seni. Asst.

Again

Dr. P. S. Singh

Dr. P. S. Singh