

Pratibha College of Commerce & Computer Studies

M. Sc. (Cyber Security) (NEP 2020 Pattern)

Programme Outcomes

After successfully completing **M. Sc. (Cyber Security)** Programme students will be able to:

PO1	In today's IT environment, recognize and apply wireless security.
PO2	Protect and defend computer systems and networks from Cyber security threats.
PO3	Learn innovative abilities to tackle modern cyber security tasks like Vulnerability assessment and penetration testing.
PO4	Understand advanced malware analysis, IT laws, digital payments, and Security concepts.
PO5	Students are able to present information security solutions to both technical And non-technical decision-makers both orally and in writing.
PO6	Students are able to recognize and evaluate the dangers, threats, and Weaknesses related to technological devices.
PO7	Understand new tools and technologies which are trending
PO8	Understand the working of Virtualization & Security Audit.
PO9	Students can create reports summarizing their research and providing Concept proof.
PO10	Students can understand cloud services, applications, and security.

Course Outcomes

F. Y. M. Sc. (Cyber Security)

SEMESTER- I

MCS-501MJ: Malware Analysis II

After successfully completing this course, students will be able to:

CO1	Learn to analyze various malicious file types
CO2	Apply various tools to Identify the vulnerabilities and to perform Malware analysis
CO3	Apply malware classification and functionality & anti-reverse engineering techniques.
CO4	Deploy and Configure Linux Operating Systems Network-wide

MCS-502MJ: Intrusion Detection and Prevention System

After successfully completing this course, students will be able to:

CO1	Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise
CO2	Analyze intrusion detection alerts and logs to distinguish attack types from false alarms.
CO3	Use various protocol analyzers and Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.
CO4	Explain the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets

MCS-503MJ: Digital Image Processing

After successfully completing this course, students will be able to:

CO1	To learn and understand various image compression and Segmentation used in digital image processing
CO2	To learn and understand various image enhancement technique used in digital image processing.
CO3	Develop and implement algorithms for digital image processing.
CO4	Apply image processing algorithms for practical object recognition applications.

Semester II

MCS-551-MJ Mobile Application and Service

After successfully completing this course, students will be able to:

CO1	Creating robust mobile applications and learn how to integrate them with other services
CO2	Explain and use key Android programming concepts
CO3	Understand both the basic and advanced concepts Android Programming Platforms

MCS-552-MJ: Incident Handling

After successfully completing this course, students will be able to:

CO1	Have an understanding of the fundamentals of computer forensics and forensic readiness
CO2	Apply the right techniques to different types of cyber security incidents in a systematic manner (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents) Master all incident handling and response best practices, standards, cyber security frameworks, laws, acts, and regulations.
CO3	The student has general knowledge of planning for incident response readiness and managing the operational aspects of the incident response team
CO4	The student understands cyber incident response and its components. The student has a good overview of known frameworks and tools for incident response

MCS-553-MJ Cyber Security Architecture

After successfully completing this course, students will be able to:

CO1	To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks
CO2	To develop graduates that can plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets
CO3	Be able to use cyber security, information assurance, and cyber/computer forensics software/tools
CO4	Design and develop a security architecture for an organization
CO5	Design operational and strategic cyber security strategies and policies