Master of Science in Cybersecurity 2025

Program Components

Course Type	CRD
Major Requirement (MR)	16
Major Elective (ME)[1]	8
Other type of courses (MSc Thesis)	9
Total Credit (CRD)	

[1] Student must select two (6XX) courses from Major Elective (ME) List.

Detailed Study Plan

Year 1 - Semester 1

Course Code	Course Title	Course Hours			Course Type	Pre requisite	Major CGPA
		LEC	PRAC	CRD			
ITCY610	Network and Information Security Management	4	0	4	MR	-	Yes
ITCY614	Applied Cryptography	4	0	4	MR	-	Yes
ITCY615	Research Methodology	4	0	4	MR	-	Yes

Year 1 - Semester 2

Course Code	Course Title	Course Hours			Course Type	Pre requisite	Major CGPA
		LEC	PRAC	CRD			
ITCY620	Incident Response and Penetration Testing	4	0	4	MR	-	Yes
ITCY6xx	Elective 1	4	0	4	ME	-	Yes
ITCY6xx	Elective 2	4	0	4	ME	-	Yes

Year 2 - Semester 3

Course Code	Course Title	Course Hours			Course Type	Pre requisite	Major CGPA
		LEC	PRAC	CRD			
ITCY690	M.Sc. Thesis	0	27	9	MSc Thesis	Pass 20 Credit Hours	Yes

Major Elective Courses

Course Code	Course Title	Course Hours			Course Type	Pre requisite	Major GPA
		LEC	PRAC	CRD			
ITCY622	Cloud Security	4	0	4	ME	-	Yes
ITCY623	Threats, Exploits and Countermeasures	4	0	4	ME	-	Yes
ITCY624	Security Aspects of Internet of Things	4	0	4	ME	-	Yes
ITCY625	Machine Learning	4	0	4	ME	-	Yes
ITCY626	Cyber Security Architecture and Design	4	0	4	ME	-	Yes
ITCY627	Selected Topics in Cyber-Security	4	0	4	ME	-	Yes

Course Description

Course Code: ITCY 610   **Course Title: Network and Information System Security**
The course covers essential topics ranging from threat analysis and information classification to encryption standards like AES and public-key cryptography algorithms such as RSA. Topics include hashing algorithms, authentication mechanisms, system security principles, protocols like SSL, IPSec, and SSH for secure communication, email security, web security, VPN technologies, and secure system architectures including firewalls and intrusion detection systems.

Course Code: ITCY 614   **Course Title: Applied Cryptography**
This course covers advanced concepts and principles of cryptography. Topics include historical ciphers and their significance in the evaluation of science of hiding techniques, modern cryptographic algorithms and protocols, popular applications of cryptography and cryptographic designs, symmetric and asymmetric encryptions, block and stream ciphers, cryptographic hash functions and digital signatures.

Course Code: ITCY 615   **Course Title: Research Methodology**
This course provides critical understanding of major research paradigms, research methodology and professional issues. Topics include all aspects related to the process of developing new research questions/solutions through literature survey, planning, proposing scientific methodologies, collecting experimental results, materials related to scientific publishing, legal IT & cybersecurity issues and regulations, code of ethics and plagiarism, AI ethics, article critique, writing scientific proposal, writing research papers, writing master level thesis, and presenting research papers to audience.

Course Code: ITCY 620   **Course Title: Incident Response and Penetration Testing**
This course aims to equip learners with advanced knowledge in managing cybersecurity incidents and conducting penetration testing. Topics include various methods and techniques to assess the effectiveness of various incident response strategies, develop comprehensive incident response plans, critique the impact of penetration testing methodologies, formulate strategies for continuous improvement in cybersecurity management, and appraise the ethical and legal considerations in conducting penetration testing and incident response.

Course Code: ITCY622   **Course Title: Cloud Security**
The course covers principles, emerging trends, and advanced techniques in securing cloud environments. Topics include cloud infrastructure security, access management, data security, monitoring, incident response, application security, and governance in the context of cloud computing.

Course Code: ITCY 623   **Course Title: Threats, Exploits and Countermeasures**

This course covers industry-standard methods, techniques and tools for mitigating security threats. Topics include attacks and defense basics, secure coding techniques, format abuses, race conditions, vulnerability discovery, fuzzing techniques for finding security flaws in protocols and program input, limits of network discovery, writing exploits and shellcodes, encapsulating the payloads, reversing exploits and protectors/packers and Rootkits for OS and execution environments.

Course Code: ITCY 624   **Course Title: Security Aspects of Internet of Things**

This course covers advanced concepts of Internet of Thing (IoT) security. Topics include vulnerabilities, threats, and attacks in the entire protocol stack for the IoT, aspects of IoT software and hardware security, IoT security architecture, IoT privacy authentication, authorization, attacks and mitigation strategies, and techniques for IoT communication and applications.

Course Code: ITCY 625   **Course Title: Machine Learning**

This course focuses on machine learning techniques related to supervised learning, unsupervised learning, semi supervised learning and reinforcement learning. Topics include regression such as linear regression and logistic regression, classification such as KNN, SVM, neural networks, decision trees, and Naïve Bayes. Clustering such as K-means and SOM. Reinforcement learning such as Q-learning. Simulation techniques such as genetic algorithms and PSO. Ensemble learning, boosting and bagging.

Course Code: ITCY 626   **Course Title: Cybersecurity Architecture and Design**

The course explores the building blocks needed to implement a life-cycle security system. Topics include analysis of internal applications, computing platforms/network infrastructure, corporate objectives with an eye toward designing flexible security architecture that is best suited for the enterprise, case studies illustrating key security architecture concepts and methods and the latest challenges and the new default expectations of enterprise security.

Course Code: ITCY 690   **Course Title: M.Sc. Thesis**

The M.Sc. Thesis course is designed to guide students through the process of conducting original research in their field of study. Students will formulate research questions, conduct a literature review, design and implement a research methodology, analyze data, and present their findings in a well-structured thesis. The course will emphasize critical thinking, scientific writing, and the ethical considerations of research. Students will work closely with a faculty supervisor and participate in regular seminars to discuss progress, challenges, and methodologies.