

Graduate Certificate in Cyber Security

Cybersecurity skills are necessary for many industrial and governmental organizations. With an increasing number of network-connected and smart devices, malicious activities threatening data security and personal privacy are at an all-time high. The purpose of this graduate certificate is to prepare students and working professionals to understand the fundamentals and obtain practical skills in cybersecurity to meet growing demands for a highly trained cybersecurity workforce.

At the conclusion of this graduate certificate, students will have learned state-of-the-art cybersecurity tools and techniques, obtained a comprehensive understanding of both classic and modern cryptographic concepts and their mathematical principles, established the ability to detect and defend against cyber-attacks, and developed a strong ability to effectively communicate cybersecurity concepts and solutions and their importance to a broad audience.

Requirements

The Graduate Certificate in Cyber Security requires a total of 15 credit hours with core and elective courses selected as follows.

Core Courses

Two core courses (6 credit hours) are required from below:

CMP_SC 7420	Software Security	3
CMP_SC 7460	Introduction to Cryptography	3
CMP_SC 7550	Cyber Defense	3

Elective Courses

Three elective courses (9 credit hours) are required from below:

CMP_SC 7530	Cloud Computing	3
CMP_SC 7910	Digital Forensics	3
CMP_SC 8001	Advanced Topics in Computer Science	3
CMP_SC 8440	Information Security: A Language-Based Approach	3
CMP_SC 8450	Formal Engineering Methods for Software and Security	3
CMP_SC 8460	Cryptographic Protocols and Formal Proofs	3