CYBERSECURITY

(Department of Computer Science)

Cybersecurity is a computing-based discipline that involves the creation, operation, analysis, and testing of secure systems, networks, and applications to protect against a variety of digital threats. The cybersecurity curriculum is based on national standards and builds on a computer science foundation. The curriculum emphasizes four main areas of cybersecurity: information security, software security, network security, and system security. Mindful of the rapid changes in technology, the curriculum seeks to prepare students for lifelong learning to enable them to meet future challenges. A student expecting to major in cybersecurity should complete CSCI 111 and CSCI 112 in the first year.

Capstone experiences offered by the Department of Computer Science include CSCI 401, CSCI 403, and CSCI 485, all of which are available to majors in cybersecurity.

- Cybersecurity Major (https://rmc.courseleaf.com/programs/cybersecurity/cybersecurity-major/)
- Cybersecurity Minor (https://rmc.courseleaf.com/programs/cybersecurity/cybersecurity-minor/)

CSEC 121 - Privacy and Security (3 Hours)
This course explores how the concepts of privacy and security have changed with the emergence of personal computers, tablets, and smart phones. Students will learn to leverage the benefits of emerging technologies and applications while understanding the impacts to their personal security and privacy. Students will also develop a working knowledge of the ethical issues related to emerging technologies and social media applications and research issues related to personal privacy, freedom of expression, and respecting and protecting intellectual property. C21:CL,NS,WA.
Curriculum: CL,NS,WA

CSEC 321 - Cryptography (3 Hours)
Cryptography is the study of secure communication and has become essential to protecting sensitive information in a world with constant data transfer. This course covers classical cryptography which focuses on encryption, and modern cryptography which relies on computationally difficult problems to make systems unbreakable in practice. Topics include stream and block ciphers, the Advanced Encryption Standard, public-key cryptosystems, digital signatures, and known attacks for the algorithms covered. C21:CC.
Prerequisite(s): CSCI 112, CSCI 212 and ENGL185 or CSCI 112, CSCI 213 and ENGL185 or permission of instructor

CSEC 322 - System Security (3 Hours)
This course explores techniques and best practices for securing hardware and software systems and detecting and recovering from digital attacks. Topics include authentication and authorization models, access control, monitoring, penetration testing, intrusion detection, attacks and defenses, malware, system recovery, and tools for assessing system vulnerabilities.
Prerequisite(s): CSCI 330 and CSEC 121

CSEC 323 - Software Security (3 Hours)
This course introduces the fundamentals of designing and developing secure software that reliably protects the information it stores and the systems on which it is used. Topics include open design, least privilege, static and dynamic testing, integration testing, specification of security requirements, validating input, use of security features, patching, and assurance documentation.
Prerequisite(s): CSEC 121, CSEC 321 and CSCI 212

CSEC 381 - Special Topics in Cybersecurity (3 Hours)

CSEC 382 - Special Topics in Cybersecurity (3 Hours)