Undergraduate Certificate in Cybersecurity
Course Plan

Students must earn 13-15 credit hours by taking these courses:

1. EE 576 - Cybersecurity

2. Two out of the following three courses:

CS 378 - Introduction to Cryptology
CS 564 - Computer Security (new course)
CS 572 - Network Security (new course)

3. One course from the following list, or a course approved by the certificate director/co-director:

CS 371 - Introduction to Computer Networking
CS 505 - Intermediate Topics in Database Systems
CS 570 - Modern Operating Systems
CS 571 - Computer Networks
EE 380 - Microcomputer Organization
EE 480 - Computer Architecture
EE 586 - Communication and Switching Networks
ICT351 - Technology Security
ICT550 - Security Informatics
ICT552 - Cybercrime and Digital Law Enforcement

4. Finally, CS395 or EE395 for 1 to 3 credit hours with the certificate director/co-director or a designated faculty. As part of the course requirements, every student will submit a final report on a selected topic in cybersecurity, to be approved by the certificate director or co-director, and will make an oral presentation (taken as final exam) to a group of members of the faculty of record. The number of credit hours depends on the complexity of the topic and will be determined by the certificate director/co-director.