COURSE TITLE: Cryptography: Algorithms and Applications

COURSE NUMBER: SEC 310

Minimum Grade Policy
The Computer & Network Security program has set a minimum passing grade of "C-" for program core courses. Students receiving a grade lower than "C-" in any required core course must retake that course.

I. RATIONALE:

This course provides an in-depth knowledge of network security problems and discusses potential solutions to these issues. Emphasis will be placed upon the analysis and design of network security. The course will cover a wide range of security concepts, including cryptography, network security, authentication, DDOS attacks, and network protection... Management of telecommunications networks, cost-benefit analysis, and evaluation of security options are also covered. Students learn to evaluate, select, and implement different security options within an organization.

II. MAJOR INSTRUCTIONAL GOALS:

During this course, students should improve their understanding of:

The goals of this course are to discuss and dissect the fundamental concepts of modern cryptography with emphasis on mathematical background and practical execution. Topics include:

- How did we get here: The history of cryptography and cryptanalysis
- Ciphers – What ones are available? Which ones are best for you
- Public and private key cryptography
- Digital Signatures
- Application of Cryptography in the modern workforce.
- Network Security (viruses, worms, Trojan horses)

III. CLASS PARTICIPATION:

Students are expected to attend class and participate actively and in a positive way. Questions and relevant observations are encouraged and enrich the experience of the entire class.

Computers in the classrooms are intended to be used as tools to enhance the students' learning experience. Instant messaging, gaming, emailing, and surfing the web are
distractions to the student, the surrounding students, and the instructor and constitute inappropriate behavior. Students are ethically obliged to avoid these and similar practices.