Fundamentals of Information Security
ECE 5560 / CS 5560

I. Catalog Description

Principles of information security and relevant mathematical concepts. Classical ciphers, relevant abstract algebra and number theory, symmetric-key ciphers, cipher modes of operation, and asymmetric-key ciphers. Cryptographic hash functions and message authentication codes. Elliptic curve cryptography and cryptosystems. Applications and standards relevant to network and computer security. Pre: Graduate standing. (3H, 3C)

Course Number: 5560 / CS 5560

ADP Title: Fundamentals of Info Security

II. Learning Objectives

Having successfully completed this course, the student will be able to:

- Formulate information security objectives of privacy (confidentiality), data integrity, authentication, and non-repudiation.
- Describe the fundamental axioms and concepts in abstract algebra and number theory that form the foundation of network and computer security solutions.
- Design and implement cryptosystems based on the design principles of symmetric-key and asymmetric-key algorithms.
- Design and implement cryptosystems based the design principles of elliptic curve cryptography-based factorization methods.
- Explain how cryptographic algorithms and protocols have been employed in various security solutions and standards.

III. Justification

Reasons for teaching the course: Past experiences have shown us that security mechanisms of a given system or network must be properly designed from the very beginning, and not added on as an afterthought. If the required security mechanisms are not carefully integrated into the target system/network *a priori* to deployment, potential security breaches can inflict enormous damage. This issue is becoming more critical than ever as we see an increase in the exchange of sensitive information (e.g., medical records, financial data, etc.) over insecure network links. The design, deployment, and management of secure systems or networks require the ability to understand core security concepts, analyze the security vulnerabilities of a target system, and design necessary cryptosystems for the target system. This course

provides requisite knowledge of fundamental security concepts and a brief introduction to their applications that are needed by students who are conducting research in security-related topics.

Level Justification: This course builds on the base of knowledge developed in relevant undergraduate programs, including understanding of the fundamentals of computer systems, networking, and probability. The course also requires an understanding of system-level issues and an ability to undertake independent, self-directed projects.

IV. Prerequisites and Corequisites

Pre: Graduate standing.

V. Texts and Special Teaching Aids

Required Texts: William Stallings, Cryptography and Network Security – Principles and Practice, 6th Ed., Prentice Hall, 2013, 752 pp.

VI. Syllabus

	Percent of Course
Introduction to basic security concepts	5%
Classical ciphers	5%
Abstract algebra	10%
Groups, rings, fields, and finite fields	
Modular arithmetic and arithmetic in finite fields	
The Euclidean algorithm	
Symmetric-key cryptosystems and Advanced Encryption Standard (AES)	20%
Cipher modes of operation	5%
Number theory	10%
Primality testing algorithms, the Chinese remainder theorem	
Fermat's little theorem, Euler's theorem	
Euler's totient function, the discrete logarithm problem	
Asymmetric-key cryptosystems	20%
Cryptographic hash functions and message authentication codes	5%
Elliptic Curve Cryptography (ECC) and ECC-based cryptosystems	5%
Applications of cryptographic algorithms and protocols	15%
Total	100%

VII. Old (Current) Syllabus

	Percent of Course
Introduction to basic concepts	5%
Authorization and access control	10%
Cryptography and its applications	20%
Authentication systems	20%
Security issues in e-commerce	15%
Sensor network security	15%
Other security topics: Intrusion detection, Denial of service attacks	10%
Legal and ethical issues	5%
Total	100%

IX. ECE is the Home Department