ICS 682: Cryptography and Computer Security

A. Course Description

Credits: 4

Lab Hours/Weeks: Lab Hours/Weeks: Corequisites: None

Lecture Hours/Week:

MnTC Goals: None

This course will discuss a broad range of computer security issues related to cryptography and networks. Students will study the design and use of cryptographic systems and analyze cryptanalytic attacks. A history of cryptographic systems and the mathematics behind them will be covered as well. Techniques of network security, including cryptographic techniques, will be covered.

B. Course Effective Dates: 05/10/2004 - Present

C. Outline of Major Content Areas:

See Course Description for major content areas.

D. Learning Outcomes (General)

1. Perform computations using key theorems of the mathematical underpinnings of contemporary cryptography, and prove related results.
2. Use the principles of substitution and transposition to perform encryptions and decryptions of historical pencil-and-paper ciphers.
3. Analyze the workings of modern cryptographic algorithms (both symmetric and public-key) manipulate simplified versions of modern algorithms, analyze the factors that determine the security of cryptographic algorithms, and evaluate security properties of such algorithms.
4. Explain the purpose and theory of cryptographic hash functions, do computations with simplified hash functions, analyze security properties of hash functions, and describe modern attacks against hash functions.
5. Analyze various forms of digital signature algorithm, explain security properties of digital signatures, and work with simplified digital signature algorithms.
6. Demonstrate expertise in reading peer-reviewed papers in computer security, and explain them in writing.

E. Learning Outcomes (MN Transfer Curriculum)

This contains no goal areas.

G. Special Information

Note: Graduate standing in the MSCS program or permission of the instructor. Students are responsible to both be aware of and abide by prerequisites for ICS courses for which they enroll, and will be administratively dropped from a course if they have not met prerequisites.