ICS 483: Cryptography for Cybersecurity Practitioners

A. Course Description

Credits: 4

ICS 382 Computer Security
OR
MATH 215 Discrete Mathematics OR Instructor approval.

Lab Hours/ Weeks:

Corequisites: None

Lecture Hours/ Week:

MnTC Goals: None

This course provides students with a thorough foundation of applied cryptography for cybersecurity practitioners. As encryption technologies continue to integrate into everyday culture, the importance of cryptography and encryption knowledge of cybersecurity practitioners continues to increase. Students will learn and be able to apply and analyze: the history of cryptography from the earliest ciphers to current encryption methodology, mathematical foundations for cryptography, symmetric and asymmetric algorithms, and applied cryptography pertaining to Virtual Private Networks (VPNs), SSL/TLS, strategies for defense utilizing encryption and cryptography, military applications, steganography, cryptanalysis, and more. Additionally, students will look to the future of cryptography and encryption including a look into quantum cryptography and encryption in cloud environments.

B. Course Effective Dates: 12/15/2017 - Present

C. Outline of Major Content Areas:

See Course Description for major content areas.

D. Learning Outcomes (General)

1. Analyze the evolution of cryptography from the earliest known ciphers to present day encryption techniques
2. Apply mathematical foundations of cryptography
3. Interpret and use symmetric cryptography principles and encryption techniques such as Feistel networks, Substitution-Permutation Networks, S-Box design, and Cryptographic Hashes
4. Interpret and use asymmetric cryptography principles and encryption techniques such as Elliptic Curve Cryptography and common Asymmetric algorithms such as RSA, Diffie-Hellman, and Digital Certificates
5. Dissect applied cryptography in military applications, SSL/TLS, Virtual Private Networks (VPNs), Steganography, Cryptanalysis, Cryptographic backdoors
6. Examine, compare, and architect defense strategies using encryption and cryptography principles
7. Identify and make sense of attacks on encryption and how they impact the principles of Confidentiality, Integrity, and Availability
8. Model how malicious threat actors use encryption to bypass common defense techniques
9. Illustrate the most likely future of cryptography including quantum cryptography and cryptography in cloud environments

E. Learning Outcomes (MN Transfer Curriculum)

This contains no goal areas.

G. Special Information
Note: 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.