CSCI 2101: Foundations of Cryptography

A. COURSE DESCRIPTION

Credits: 4
Lecture Hours/Week: 4
Lab Hours/Week: 0
OJT Hours/Week: *.*
Prerequisites: None
Corequisites: None
MnTC Goals: None

This is a foundational course in cryptography covering systems of secure communication relevant to the field of Cyber Security and to Computer Science in general.

Topics include theories and applications of encryption of both historical and modern methods, and techniques for creating systems of secure communication. Programming is undertaken to encode and decode information using industry standard cryptographic algorithms. The C programming language is emphasized due to its ubiquity in both the field of applied cryptography and in operating systems.

While this is not a course to study techniques for breaking cryptographic systems (cryptanalysis), considerations are given to the probability that weaknesses in a cryptographic cipher can be exploited and that data confidentiality, integrity, and availability can be potentially lost.

B. COURSE EFFECTIVE DATES: 05/08/2024 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

D. LEARNING OUTCOMES (General)

1. Argue the importance and limitations of randomness in encryption. (ELOs 1, 2a, 2d)
2. Evaluate use-case scenarios of cryptographic systems (e.g., public versus private networks). (ELOs 1, 2a, 2d)
3. Assess the security of cryptographic protocols and underlying algorithms. (ELOs 1, 2a, 2d)
4. Outline and demonstrate the application and implementation of hash functions. (ELOs 1, 2a, 2b, 2d)
5. Outline, implement, and evaluate cryptographic functions. (ELOs 1, 2a, 2b, 2d)
6. Examine and apply cryptographic algorithms. (ELOs 1, 2a, 2b, 2d)
7. Examine and demonstrate cryptographic software. (ELOs 1, 2a, 2b, 2d)
8. Execute coded (written) encryption techniques and ciphers in historical context and describe. (ELOs 1, 2a, 2b, 2d)
9. Examine, analyze, and apply the mathematics of cryptography. (ELOs 1, 2a, 2d)
10. Examine and demonstrate the use of source code for private and public key technologies, (ELOs 1, 2a, 2b, 2d)

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus
G. SPECIAL INFORMATION
   None noted