CSCE 4050 Applications of Cryptography  Spring 2019

Instructor: Kirill Morozov (Department of Computer Science and Engineering)

Course description: This course aims at introducing fundamentals of cryptography and their applications. The knowledge gained from this course will enable students to apply cryptographic algorithms as building blocks for designing security solutions.

Course schedule*

Lecture 1  (Jan 17): Introduction: Course overview, historical ciphers, mathematical background
Lecture 2  (Jan 24): Stream ciphers
Lecture 3  (Jan 31): Block ciphers
Lecture 4  (Feb 7):  Block cipher modes of operation
Lecture 5  (Feb 14): Message integrity, authentication codes, cryptographic hash functions
Lecture 6  (Feb 21): Authenticated encryption, key derivation, applications of block ciphers
Lecture 7  (Feb 28): Basic key exchange and elements of number theory
Lecture 8 (Mar 7): Summary of symmetric cryptography, Midterm Exam
------------ (Mar 14):  Spring Break
Lecture 9 (Mar 21): Public-key encryption
Lecture 10 (Mar 28): Digital signatures and identification schemes
Lecture 11 (Apr 4):  Public-key infrastructure and authenticated key exchange
Lecture 12 (Apr 11): Network security protocols and secure login
Lecture 13 (Apr 18): Quantum cryptanalysis and post-quantum cryptography
Lecture 14 (Apr 25): Homomorphic encryption, secret sharing, secure multi-party computation
Lecture 15 (May 2): Blockchain and cryptocurrencies
========  (May 9): Final Exam

* Subject to possible changes

Recommended literature:
- D. Boneh and V. Shoup: "A Graduate Course in Applied Cryptography" - Available as draft at: http://toc.cryptobook.us/

Grading:
- Take-home homeworks (some including programming assignments) – 50%
- Programming project (groups of 2-3 students or individual) – 10%
- Mid-term exam – 15%
- Final exam – 25%