CSCE 4050 Applications of Cryptography (Spring 2024)

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 secure solutions.

Course schedule

Lecture 1 (Jan 18): Course overview, historical ciphers, mathematical background
Lecture 2 (Jan 25): One-time pad and stream ciphers
Lecture 3 (Feb 1): Pseudorandom generators
Lecture 4 (Feb 8): Block ciphers
Lecture 5 (Feb 15): Block cipher modes of operation
Lecture 6 (Feb 22): Data integrity, message authentication codes (MACs), and cryptographic hash functions
Lecture 7 (Feb 29): Authenticated encryption
Lecture 8 (Mar 7): Midterm Exam (1st half)
                    Review of the course material (2nd half)
------------- (Mar 14): Spring Break (no class)
Lecture 9 (Mar 21): Overview of key exchange, public-key encryption, and their mathematical background
Lecture 10 (Mar 28): Public-key encryption
Lecture 11 (Apr 4): Digital signatures and identification schemes
Lecture 12 (Apr 11): Public-key infrastructure, authenticated key exchange and TLS
Lecture 13 (Apr 18): Identification protocols and secure login
                    Overview of quantum cryptanalysis and post-quantum cryptography
Lecture 14 (Apr 25): Blockchain and cryptocurrencies
Lecture 15 (May 2): Advanced cryptographic functionalities:
                    homomorphic encryption, secret sharing, and secure multi-party computation
                    Review of the material covered in the course
------------- (May 9): Final Exam

Recommended literature:
[Graduate]: D. Boneh and V. Shoup: “A Graduate Course in Applied Cryptography”
            - Available online at: http://toc.cryptobook.us/
[Undergraduate]: M. Rosulek: “The Joy of Cryptography”
            - Available online at: https://joyofcryptography.com/
[Supplementary reading]:

Grading:
- Homeworks – 40%
- Programming projects – 15%
- Mid-term exam – 20%
- Final exam – 25%