CSCE 5050 Applications of Cryptography (Spring 2022)

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 20): Course overview, historical ciphers, mathematical background
Lecture 2 (Jan 27): One-time pad, stream ciphers and pseudorandom generators
Lecture 3 (Feb 3): Block ciphers
Lecture 4 (Feb 10): Block cipher modes of operation
Lecture 5 (Feb 17): Data integrity and message authentication codes (MACs)
Lecture 6 (Feb 24): Data integrity and cryptographic hash functions
Lecture 7 (Mar 3): Authenticated encryption;
                   Review of the material covered so far
Lecture 8 (Mar 10): Overview of practical implementations and their security (1st half);
                   Midterm Exam (2nd half)

---------- (Mar 17): Spring Break (no class)

Lecture 9 (Mar 24): Overview of key exchange, public-key encryption,
                   and their mathematical background
Lecture 10 (Mar 31): Public-key encryption
Lecture 11 (Apr 7): Digital signatures and identification schemes
Lecture 12 (Apr 14): Public-key infrastructure, authenticated key exchange, and TLS
Lecture 13 (Apr 21): Identification protocols and secure login;
                      Overview of quantum cryptanalysis and post-quantum cryptography
Lecture 14 (Apr 28): Blockchain and cryptocurrencies
Lecture 15 (May 5): Advanced cryptographic functionalities:
                      homomorphic encryption, secret sharing, and secure multi-party computation;
                      Review of the material covered in the course

---------- (May 12): Final Exam

Recommended literature:

[Graduate]: D. Boneh and V. Shoup: “A Graduate Course in Applied Cryptography”
           - Available as draft at: http://toc.cryptobook.us/
[Undergraduate]: M. Rosulek: “The Joy of Cryptography”
                - Available as draft at: https://web.engr.oregonstate.edu/~rosulekm/crypto/
[Supplementary reading]:


**Grading:**

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