CSCE 5050.600

Applications of Cryptography

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

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 syllabus

Lecture 1 (Jan 18): Introduction: Course overview, history of cryptography, mathematical background

Lecture 2 (Jan 25): Stream ciphers

Lecture 3 (Feb 1): Block ciphers

Lecture 4 (Feb 8): Message Integrity, hash functions, authentication codes

Lecture 5 (Feb 15): Authenticated encryption and key derivation, **Mid-Term Exam 1**

Lecture 6 (Feb 22): Basic key exchange and elements of number theory

Lecture 7 (Mar 1): Public-key encryption

Lecture 8 (Mar 8): Digital signatures and identification schemes

---------- (Mar 15): **Spring Break**

Lecture 9 (Mar 22): Public-key infrastructure, authenticated key exchange

Lecture 10 (Mar 29): Network security protocols and secure login, quantum cryptanalysis and post-quantum crypto

Lecture 11 (Apr 5): Homomorphic encryption, **Mid-Term Exam 2**

Lecture 12 (Apr 12): Advanced protocols: Commitments, zero-knowledge proofs, secret sharing, secure multi-party computation

Lecture 13 (Apr 19): Advanced protocols: Visual cryptography, steganography, blockchain and cryptocurrencies

Lecture 14 (Apr 26): Topic presentations

Lecture 15 (May 3): Topic presentations

======== (May 10): **Final Exam**