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 16): Course overview, historical ciphers, mathematical background
Lecture 2 (Jan 23): Stream ciphers and pseudorandom generators
Lecture 3 (Jan 30): Block ciphers
Lecture 4 (Feb 6): Block cipher modes of operation; Message integrity I
Lecture 5 (Feb 13): Message integrity II, authentication codes, cryptographic hash functions
Lecture 6 (Feb 20): Authenticated encryption, key derivation, applications of block ciphers
Lecture 7 (Feb 27): Key exchange and elements of number theory
Lecture 8 (Mar 5): Review lecture; Midterm Exam
Lecture 9 (Mar 12): Spring Break
Lecture 10 (Mar 19): Public-key encryption
Lecture 11 (Mar 26): Digital signatures and identification schemes
Lecture 12 (Apr 2): Public-key infrastructure and authenticated key exchange
Lecture 13 (Apr 9): Network security protocols and secure login
Lecture 14 (Apr 16): Overview of quantum cryptanalysis and post-quantum cryptography
Lecture 15 (Apr 23): Blockchain and cryptocurrencies
Lecture 16 (Apr 30): Homomorphic encryption, secret sharing, secure multi-party computation

Recommended literature:

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


Grading:

- Homeworks (some including programming assignments) – 45%
- Programming project (individual or two-student teams) – 15%
- Mid-term exam – 15%
- Final exam – 25%