CMPT 404 - D100 Cryptography and Cryptographic Protocols

Instructor(s): Andrei Bulatov

Calendar Objective/Description:
The main cryptographic tools and primitives, their use in cryptographic applications; security and weaknesses of the current protocols. The notion of security, standard encryption schemes, digital signatures, zero-knowledge, selected other topics.

Instructor's Objectives:
The course focuses on foundations of modern cryptography. It rigorously defines the basic requirements to cryptographic schemes, privacy and authenticity. It introduces required constructions and results from complexity theory, and shows how these results are used to built provably secure cryptographic schemes. We also consider how these principles are used in the existing systems, and see why many of the widely used schemes such as SSL and SSH may be insecure.

Prerequisites:
MACM 201. CMPT 307 and 308 are recommended.

Topics:
- Basics of probability, cryptography, and complexity. Historical remarks
- Concepts of privacy and authenticity: perfect, statistical, and computational
- Pseudo-random generators and functions
- One-way functions
- Private-key encryption: constructions
- Private-key encryption in practice: block ciphers
- Trapdoor functions and public-key encryption
- Message authentication, digital signatures, and hashing
- Zero-knowledge proofs
- Survey of the cryptographic components of the existing protocols

Grading:
Will be discussed in the first week of classes.
Students must attain an overall passing grade on the weighted average of exams in the course in order to obtain a clear pass (C- or better).

Recommended Books:
**Academic Honesty Statement:**

Academic honesty plays a key role in our efforts to maintain a high standard of academic excellence and integrity. Students are advised that ALL acts of intellectual dishonesty will be handled in accordance with the SFU Academic Honesty and Student Conduct Policies (http://www.sfu.ca/policies/gazette/student.html).