CMPT 789 - G100 Applied Cryptography

**Instructor(s):** Andrei Bulatov

**Calendar Objective/Description:**
Applied Cryptography

**Instructor's Objectives:**
The course focuses on foundations of modern cryptography. It introduces the basic requirements to cryptographic schemes, privacy and authenticity. The course then describes the main cryptographic primitives and demonstrates how they are used to construct private and public cryptosystems. We also consider how these constructions are used in the existing systems, and survey a number of modern applications of cryptography.

**Prerequisites:**
see go.sfu.ca

**Topics:**
- Basics of probability, cryptography, and complexity. Historical remarks
- Concepts of privacy and authenticity
- Cryptographic primitives
  - Private-key encryption: stream ciphers and block ciphers
  - Public-key encryption
- Message authentication, digital signatures, and hashing
- Selected topics: zero-knowledge proof, post-quantum cryptography, etc.
- 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).