CMPT 404 - D100 Cryptography and Cryptographic Protocols

**Instructor(s):** Antonina Kolokolova

**SFU Burnaby**

**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:**
This course focuses on cryptographic primitives and cryptosystems underlying secure communication and information protection. We will study private-key and public-key encryption, authentication, digital signatures, and commitment schemes, and see how they are used in practice, analyse what it means for them to be secure, and look at why widely-used schemes such as SSL may be insecure. We will cover a range of cryptographic applications from wifi protocols to electronic voting and blockchains.

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

**Topics:**
- Basic cryptographic primitives and respective computational assumptions
- Private-key encryption, block ciphers
- Public-key encryption, certificates and certificate authorities
- Message authentication, digital signatures and hashing
- Secure communication protocols
- Commitment schemes, blockchains
- Time permitting: post-quantum cryptography

**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).