MACM 442
Cryptography

Fall 2019

Instructor: Dr. Petr Lisoněk (plisonek@sfu.ca)

Prerequisites: (CMPT 201 or 225) and one of (MATH 340 or 332 or 342); or CMPT 405

If you miss a prerequisite but you believe that you know the background material needed for taking the course, then please contact the instructor at the e-mail address given above.

Do you want to know how the remote lock for a car works? How are your on-line banking transactions and e-mail messages protected? Can anyone listen to your cell phone conversations or read your text messages? Do you want to break some historical ciphers, and learn how hard it would be to break the ciphers used nowadays? Then come to MACM 442!

The course is an introduction to the subject of modern cryptography. Topics include classical methods for cryptography and how to break them, the data encryption standard (DES), the advanced encryption standard (AES), the RSA and ElGamal public key cryptosystems, digital signatures, secure hash functions and pseudo-random number generation. The computational part of the course covers algorithms for computing with long integers including the use of probabilistic algorithms.