

CAS705 Fall 2009
Computational Complexity

<http://www.cas.mcmaster.ca/~soltys/cas705-f09>

Michael Soltys
soltys@mcmaster.ca

Lectures: Tu, Th, Fr, 11:30-12:30, in ITB-222.

The background for this course is basic undergraduate discrete mathematics, and some rudimentary number theory and linear algebra (the latter two for the cryptography part of the course). The course will be self-contained, with all the necessary background presented in the lectures.

There are two parts to the course; the second part builds on the first:

Part I Computational Complexity:

- Turing machines and lower bounds illustrated with crossing sequences
- the classes P and NP
- completeness & reducibility
- space bounded computations, inductive counting, and interactive proofs
- circuits and randomized complexity classes.

Part II Cryptography:

- Rabin-Miller primality testing
- Diffie-Hellman, ElGamal, and RSA protocols
- elliptic curve cryptography
- lattice-based cryptography

Textbook: *An Introduction to Computational Complexity*, by Michael Soltys, published by the Jagiellonian University Press, 2009. Preprints will be distributed in class at a small cost.

Marking scheme:

- 4 assignments, where best 3 will be selected, each worth 20%,
- take home exam, worth 20%,
- class attendance and participation, worth 20%

Important Note: The instructor and university reserve the right to modify elements of the course during the term. The university may change the dates and deadlines for any or all courses in extreme circumstances. If either type of modification becomes necessary, reasonable notice and communication with the students will be given with explanation and the opportunity to comment on changes. It is the responsibility of the student to check their McMaster email and course websites weekly during the term and to note any changes.