UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS
Department of Combinatorics and Optimization

C&O Comprehensive Exam Syllabus for Cryptography

Cryptography is a broad subject and can be approached from many angles. The primary focus of this exam is mathematical and public key cryptography, though it does provide some coverage of the core components of symmetric key cryptography as well. The primary reference is [SP], which covers all areas of cryptography on the exam. [K] goes into mathematical cryptography in greater depth. [KL] covers much of the same material as [SP], but proceeds from the "reductionist security" methodology, which is widely used in cryptography research.

Suggested References and Outline of Topics:

- D. Stinson and and M. Paterson, *Cryptography: Theory and Practice*, CRC Press, fourth edition, 2019.
  - Introduction (1)
  - Block Ciphers and Stream Ciphers (4, omit Sections 4.3, 4.4)
  - Hash Functions and Message Authentication (5, omit Section 5.6)
  - The RSA Cryptosystem and Factoring Integers (6)
  - Public-Key Cryptography and Discrete Logarithms (7)
  - Signature Schemes (8)
  - Post-Quantum Cryptography (9, omit Section 9.4)
  - Identification Schemes (10, omit Section 10.5)
  - Key Agreement (12, omit Sections 12.4-12.7)
- N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, Second edition, 1994.
  - Some Topics in Elementary Number Theory (1)
  - Finite Fields and Quadratic Residues (2)
  - Elliptic Curves (6)
- J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC Press, 2nd edition, 2015.
  - Public-Key Encryption (11, omit Sections 11.5.3-11.5.5)
  - Digital Signature Schemes (12, omit Sections 12.6-12.9)