University of Lethbridge

FIAT LUX

FALL 2019 COURSE OFFERING

MATH 4460

MATHEMATICS OF PUBLIC KEY CRYPTOGRAPHY

CRN 30931 | Tues & Thurs 10:50AM -12:05PM | Instructor: Andrew Fiori

Public key cryptography is the foundation on which our modern digital world is built, with fundamental roles in ensuring our privacy and the security of e-commerce among others. The most widely used public key crypto-systems are based on the computational complexity of certain mathematical problems, many from Number Theory.

This course will discuss mathematical aspects of cryptosystems including RSA, Diffie-Hellman style key agreement schemes, and lattice based systems. The number theoretic applications will include algorithms for primality testing as well as factoring of integers.

The course is intended for both Mathematics and Computer Science students, some programming experience may be useful, but it will not be assumed.