MATH 4809/5300 (Fall 2022)

Mathematical Cryptography (Crypto II)

Instructor: Yuly Billig

Office: Herzberg 4221

Phone: 520-2600 ext. 4310

e-mail: billig@math.carleton.ca

Office Hours: To be determined

Course platform: BrightSpace

Textbook (optional): J. Hoffstein, J. Pipher, J. Silverman, An Introduction to Mathematical Cryptography, 2nd edition.

Method of Evaluation:

Home Assignments	25%
Midterm	25%
Final Exam	50%

Midterm Date: Thursday October 20, in class.

Prerequisite: Number Theory and Cryptography (Crypto I) MATH 3809 (or permission of instructor)

Topics Covered:

Elliptic curves
Finite Fields
Discrete logarithm cryptography
ElGamal cryptosystem
Index Calculus Method
Factoring large integers
Hyperelliptic curves
Additional selected topics

Home assignments will include implementations of various cryptosystems in C/C++.