Concentration in Cryptography

Objective

This concentration is offered as an area of specialization within the Majors or Honours program in Pure Mathematics. The goal of this concentration is to provide students with a comprehensive education in cryptography, including basic cryptographic primitives, modern cryptographic algorithms and their underlying mathematics, models of cryptographic security, mathematical techniques for attacking cryptosystems, and selected applications of cryptography. This concentration is unique in Canada and prepares students for either a career or graduate school in cryptography.

For the exact course requirements, students are advised to consult the University calendar. Brief descriptions of the courses that are particularly relevant to the concentration are provided below. Students should also note that the course PMAT 427 (Number Theory) can be used to satisfy a requirement of either the major program or the concentration, but not both; in other words, it cannot be "double-counted".

Concentration-Relevant Courses

- CPSC 329 Explorations in Information Security and Privacy
- PMAT 418 Introduction to Cryptography
- PMAT 419 Information Theory and Error Control Codes
- PMAT 427 Number Theory
- PMAT 429 Cryptography – Design and Analysis of Cryptosystems
- PMAT 511 Rings and Modules
- PMAT 527 Computational Number Theory
- PMAT 529 Advanced Cryptography and Cryptanalysis
- CPSC 530 Information Theoretic Security

Description and Rationale

CPSC 329 is a broad survey of topics in information security and privacy, with the purpose of cultivating an appropriate mind set for approaching security and privacy issues. Topics will be motivated by recreational puzzles, possibly stemming from real-life problems, with time allocated for students to attempt to solve these puzzles. Historical background behind the puzzle, together with a technical solution, will be presented afterward. This course is open to all students who have taken a first year programming course.

PMAT 418 provides an introduction to cryptography, with emphasis on attaining well-defined and practical notions of security. The course discusses basic cryptographic primitives, including symmetric and public-key cryptosystems, one-way and trapdoor functions, mechanisms for data integrity, digital signatures, key management, and applications to the design of cryptographic schemes. Assessment will be conducted through homework assignments, exams, and a term paper. Additional application programming exercises may be available for extra credit. Lectures run concurrently with the course CPSC 418 of the same title.

PMAT 419 discusses information theory and coding theory, both topics that are relevant and closely related to cryptography. Information theory assesses the amount of meaningful information contained in — and potentially revealed by — data. While coding theory is often used in conjunction with cryptography, the two fields aim to achieve almost opposite goals. In essence, coding theory is about making data easy to read, while cryptography aims to make it hard to read. For example, an error-correcting code could be applied to a signal from a military satellite in order to detect and possibly correct errors incurred during transmission. At the same time, the signal could be encrypted to make it unreadable to unauthorized parties.

PMAT 427 is a first course in number theory that is not only a standard ingredient of most undergraduate programs, but is also highly beneficial to a well-rounded eduction in cryptography. Number Theory is fundamental to the understanding of modern cryptosystems. Many such schemes use modular arithmetic, greatest common divisor computations, group theory, prime numbers, and other elements from number theory. In addition, cryptanalytic attack algorithms are frequently based on number theory.

PMAT 429, the second cryptography course, explores mathematical techiques for designing, implementing and analyzing cryptographic systems. Beginning with a review of basic algorithms and complexity, the course investigates how to design and attack public key cryptosystems based on number theory. Topics include basic techniques for primality testing, factoring and extracting discrete logarithms, as well as elliptic curve cryptography. Additional topics may include knapsack systems, zero knowledge, attacks on hash functions, identity based cryptography, and quantum cryptography.

PMAT 511 investigates advanced algebraic structures beyond those covered in lower level algebra courses such as PMAT 315 and PMAT 431. While this course is not as directly relevant to the concentration as some of the other courses described here, it is included as an additional 500 level option.

PMAT 527 is a second number theory course that investigates major problems in computational number theory, with emphasis on practical techniques and their computational complexity. Many of these methods are crucial ingredients in the design and efficient implementation of public key cryptographic schemes, and may also represent tools for attacking these systems. Topics of this course include algorithms for basic integer arithmetic, finite fields, primality proving, factoring methods, and algorithms in algebraic number fields. In addition to assignments and exams, course requirements will generally include a project of the student's own choosing (subject to instructor approval) which consists of a potential proposal, a term paper, and possibly an oral presentation.

PMAT 529, the third and last in the sequence of cryptography courses, focuses on advanced mathematical techniques for designing and attacking modern cryptosystems, such as cryptography based on quadratic residuacity, advanced techniques for factoring and extracting discrete logarithms, hyperelliptic curve cryptography, as well as pairings and their applications to cryptography. The course also investigates post-quantum cryptosystems based on algebraic codes and lattices. Additional topics may include provable security, secret sharing, more post-quantum cryptography, and new developments in cryptography. Assessment mechanisms are similar to PMAT 527.

CPSC 530 explores information theoretic concepts and their applications to cryptography in information theoretic settings. The course discusses formal models of security and efficiency of cryptographic primitives, as well as techniques for analyzing such primitives in these models. Constructions of cryptographic primitives when there is no bound on an adversarys computational resources are also introduced.

Additional Courses of Potential Interest

- PMAT 431 Groups, Rings and Fields
- CPSC 519 Introduction to Quantum Computation
- CPSC 525 Principles of Computer Security
- CPSC 526 Network Systems Security
- CPSC 527 Computer Viruses and Malware
- CPSC 528 Spam and Spyware

These courses provide further background in areas related to cryptography. Any of them would be beneficial to a student taking this concentration. A number of the Computer Science courses constitute a portion of a *Concentration in Information Security* that is offered as part of the Bachelor's degree in Computer Science. They provide more in-depth instruction in fields such as applied cryptography as well as information and computer security. Students are advised that these courses have their own pre-requisite requirements.