State-of-the-art Cryptography over the Whole Numbers

Lecturer: Prof. Claude Crépeau, McGill School of Computer Science

Cryptography is the science of secrecy and secret codes. We use cryptography in our everyday life when doing transactions via banking machines or communicating over the internet. It may seem that in order to get secrecy we should use very fancy and complicated calculations to obscure information as much as possible. On the contrary, it turns out that we are much better off with simple well-understood calculations like addition, subtraction, multiplication and division of large whole numbers properly combined with a source of randomness to obtain secrecy. If you understand how to perform addition, subtraction, multiplication and division of integers, you have all that is needed for this subject.

This course contains a small historical perspective of cryptography, as well as insights into the future of computing (via Quantum Computers).

This is a mainly theoretical course, but some practical exercises will be included. Concepts from probability and information theory will be introduced quite informally in relation to secrecy. This class will be of interest to anyone considering studies in mathematics, computer science, natural sciences, or engineering.

Lecturer Bio:

Prof. Claude Crepeau is an Associate Professor at McGill University. He received his Doctorate degree from M.I.T. in 1990 and later completed a Postdoc at the Université Paris-Sud and has been a CNRS researcher at the Ecole Normale Superieure, Paris, since 1991. He also previously served as Associate Editor for both the Journal of Cryptology and for Complexity and Cryptography of the IEEE Transactions on Information Theory. Prof. Crepeau has worked extensively at the design of cryptographic protocols, including Zero-knowledge protocols, Multiparty Computations, Two-Party Secure Function Evaluation. His major contribution has been to offer alternative (non-computational) assumptions under which such protocols may be implemented using noisy channels and quantum channels. In 1993, together with five international colleagues, he published a paper introducing the new concept of "quantum teleportation" which has been cited more than 12000 times in less than 25 years. The future of computing is most likely based on quantum teleportation.

INTRODUCTION TO QUANTUM MECHANICS

Lecturer: Dr. Rustam Khaliullin; Assistant Professor, Department of Chemistry

Since its inception a century ago, quantum mechanics — a probabilistic theory of the microscopic world with immense predictive power — has led a technological revolution that has created, to name just a few examples, modern electronics, lasers, solar cells, and MRI. At the same time, due to its bizarre predictions, quantum mechanics has become an integral part of popular culture while the surprising difficulty in interpreting its basic laws have revived philosophical questions like "What is the nature of reality?" and "What is the limit to our knowledge about the universe?".

Despite its counter intuitive predictions, quantum mechanics is based on a set of very simple assumptions. Using a series of elementary examples, this course explains why the fundamental axioms of quantum mechanics make sense and what mathematical tools are necessary to describe the behavior of microscopic objects like electrons and atomic nuclei. The course goes on to illustrate how the basic principles of quantum mechanics are used in quantum computing, quantum cryptography, and quantum teleportation — emerging technologies at the forefront of the second quantum revolution. Finally, the course briefly touches upon the history and interpretation of quantum mechanics, its most famous paradoxes, and philosophical questions — the answers to which are still illusive.

A good understanding of algebra and vectors is necessary. Basic knowledge of complex numbers, concepts of probability, and computer programming might be helpful but are not required. This class will be of interest to anyone considering studies in physical natural sciences, mathematics or engineering.

Lecturer Bio:

Following the completion of his PhD from the University of California at Berkeley, Dr. Khaliullin worked at ETH Zurich and the University of Mainz, before coming to McGill. The focus of Prof. Khaliullin's research is on the development of new theoretical methods and computational tools for solving difficult current problems in chemistry, solid-state physics, and materials science. His expertise extends from electronic structure methods and first-principle molecular dynamics to artificial intelligence methods and high performance massively-parallel computing for materials modeling. His research group contributes to the development of multiple software packages including such popular codes as Q-Chem (quantum chemistry) and CP2K (materials science). He is particularly known for his studies of quantum phenomena in the interactions between water molecules.

Toxicology: The Science of Poisons

Lecturer: Dr. Edith Zorychta, Faculty of Medicine, McGill University

In this course, we will examine some of the poisons that surround us in everyday life, and understand some of the mechanisms by which they alter the normal functioning of our cells and organ systems. As examples, we will consider some common plants that are found in our houses and gardens, some industrial chemicals in widespread use, and the pollutants that we breathe in our increasingly contaminated air. We will also look at the rising pollution of our oceans, and the challenges being faced by marine life from toxins in the water.

This course would be suitable for students wishing to study: medicine, biology, biochemistry, physiology, veterinary medicine or natural sciences.

Lecturer Bio:

Dr. Edith Zorychta is an Associate Professor in the Departments of Pathology, Pharmacology and Therapeutics at McGill University. She specializes in understanding disorders and drugs acting on the nervous system and she currently is the Director of Graduate Studies in a Pathology department that is focused on improving therapy for fatal diseases. She teaches extensively to undergraduate students in biomedical science programs, to medical students, and to graduate students in biomedical disciplines. She has been the recipient of teaching awards in both the Faculty of Science and the Faculty of Medicine, and currently chairs an awards committee on teaching excellence.

Medicines of the Future

Lecturer: Dr. Edith Zorychta, Faculty of Medicine, McGill University

In this course, we will examine the major changes that are taking place in the discovery and introduction of new drugs to treat or prevent some important diseases. No longer are we limited to simple chemical structures derived from plants or synthesized in a laboratory…we have entered the era of biological medicines that are made by living cells, and we are also experiencing personalized medicine, where we can test people ahead of time to find out which of several drugs will be best for them. As examples of these new approaches we will analyze a recent success in treating cancer, and a new strategy to prevent heart disease.

This course would be suitable for students wishing to study: medicine, biology, biochemistry, physiology, veterinary medicine or natural sciences.

Lecturer Bio:

Dr. Edith Zorychta is an Associate Professor in the Departments of Pathology, Pharmacology and Therapeutics at McGill University. She specializes in understanding disorders and drugs acting on the nervous system and she currently is the Director of Graduate Studies in a Pathology department that is focused on improving therapy for fatal diseases. She teaches extensively to undergraduate students in biomedical science programs, to medical students, and to graduate students in biomedical disciplines. She has been the recipient of teaching awards in both the Faculty of Science and the Faculty of Medicine, and currently chairs an awards committee on teaching excellence.

Reading, Writing & Thinking Across the Disciplines

Lecturer: Dr. Dianne Bateman, Lecturer, Faculty of Education, McGill University

This course examines the connection between thinking in a discipline and reading and writing in a discipline. Its premise is that each discipline has a unique framework for thinking that is required for successful learning. Making these frameworks for thinking explicit to the learner deepens their comprehension of the texts they are being asked to read and the course content they are being asked to learn. Students will learn how to choose generic and/or discipline-specific learning (cognitive) strategies that will increase their understanding of the content knowledge and thinking demands of any discipline.

This course is suitable for students who want to be prepared for the reading, writing and thinking challenges that they will face in their disciplines of choice when they start their postsecondary education. Thinking and learning in the Humanities, Social Science and Science will be highlighted.

Lecturer bio:

Dr. Bateman is a lecturer at McGill University where she is known for her courses on *Teaching & learning in Higher Education* and *Educational Measurement & Assessment*. She is also a well-known faculty member of Champlain St-Lambert College where she has taught for 36 years as a member of the English Department. Dr. Bateman has an M.A. in Educational Psychology and reading from Teachers College, Columbia University and a PhD in Educational Psychology, from McGill University. In 2014, Dr. Bateman was awarded entry into the 3M National Teaching Fellowship, Canada's most prestigious recognition of excellence in educational leadership and teaching at the university and college level.

Skills for Emerging leaders

Lecturer: Dr. Joseph Levitan, Assistant Professor, Faculty of Education McGill University

By the mid-21st century, leadership will look very different than it does today. With rapid innovation in technology, ever increasing globalization, and institutional structures constantly changing, youth will inherit a world that requires adaptive leadership skills. This course will take students through the different styles and theories of leadership that have emerged at the beginning of this century and provide an arena for students to practice different forms of leadership through studying and acting-out cases of current leadership issues.

This course is designed for students who are seeking to expand and develop their leadership skills in order to prepare for their future. No prerequisites are required.

Lecturer Bio: Dr. Joseph Levitan is an Assistant Professor in the Department of Integrated Studies of Education at McGill University. His research interests include leadership and policy for social justice in education, educational theory, responsive educational leadership, and intersectional analysis of culture, identity, and learning.

Dr. Levitan is an educational anthropologist who uses ethnography, collaborative inquiry, phenomenology, and other qualitative, mixed, and comparative methods to understand educational phenomena. He completed graduate studies at Columbia University Teachers College (MA) and the Pennsylvania State University (PhD), where he was awarded a U.S. Department of Education Funded Foreign Language and Area Studies Fellowship. He has performed research in Latin America, the United States, and Southeast Asia. Prior to joining the McGill Faculty, Dr. Levitan worked as an educational leader and researcher in the U.S. and Latin America for seven years.