Atlantic Association for Research in the Mathematical Sciences

Memorial University of Newfoundland

Atlantic Algebra Centre

February 26 - March 3, 2012

AAC Mini Course

Non-commutative cryptography

will be delivered by

Professor Vladimir Shpilrain

Department of Mathematics
The City College of New York
New York, USA

Vladimir Shpilrain received his PhD in 1992 from Moscow State University. He held postdoctoral positions at the Technion in Israel and at the Ruhr University (Bochum) in Germany. Currently he is a Professor at the City College of New York. He also held visiting positions at various institutions, including the University of California at Santa Barbara, the University of Hong Kong, the Max-Planck-Institut (Bonn), MSRI (Berkeley), CRM (Barcelona), CRM (Montreal), and other institutions. He has authored and coauthored over 80 papers and 3 monographs.Professor Shpilrain's current research focuses on the complexity of algorithms in Group Theory and on applications of Non-commutative Algebra in Cryptography. He is a managing editor of the "Groups, Complexity, and Cryptology" journal published by Walter de Gruyter.

Abstract of the mini course

The object of this minicourse is threefold. First, we discuss how non-commutative groups which are typically studied in combinatorial group theory can be used in *public key cryptography*. Second, we show that there is a remarkable feedback from cryptography to combinatorial group theory because some of the problems motivated by cryptography appear to be new to group theory, and they open many interesting research avenues within group theory. In particular, we put a lot of emphasis on studying *search problems*, as compared to *decision problems* traditionally studied in combinatorial group theory. We also briefly survey a rapidly emerging area of group theory that studies complexity of various algorithmic problems. This includes generic properties of groups, subgroups and elements, generic- and average-case complexity of group-theoretic algorithms, asymptotically dominant properties, etc.

Applications of group theory to cryptography that we will discuss focus on public-key (or asymmetric) cryptography. The basic idea of public-key cryptography involves the use of a so-called one-way function to encrypt messages. Very informally, a one-way function f is a function such that it is easy to compute the value of $f(x)$ for each argument x in the domain of f, but it is very hard to compute the value of $f^{-1}(y)$ for "most" y in the range of f. The most celebrated one-way function, due to Rivest, Shamir and Adleman, gives rise to the protocol called RSA, which is the most common public-key cryptosystem in use today. It depends in its efficacy, as do many of other cryptosystems, on the complexity of finite abelian (or commutative) groups. Such algebraic structures are very special examples of *finitely generated groups*. Finitely generated groups have been intensively studied for over 100 years and they exhibit extraordinary complexity. Although the security of the Internet does not appear to be threatened at this time because of the weaknesses of the existing protocols such as RSA, it seems prudent to explore possible enhancements and replacements of such protocols which depend on finite abelian groups. This is one of the basic objectives of this minicourse.

Everybody is invited! A limited support is available for the mathematics students in Atlantic Canada. Please provide a recommendation letter from your supervisor. Send applications to aac at mun.ca. *Please also visit the website of AAC at* www.mun.ca/aac.