The Conjugacy Problem:
Cryptoanalytic approaches to a problem of Dehn

(Boaz Tsaban)

The ultimate goal in the field of noncommutative-algebraic cryptography is to devise key exchange protocols (KEPs) based on computationally hard problems in noncommutative groups. Such KEPs, if found, would be substantially different than all present-day KEPs, may have better trade-off between security and efficiency, and may even (unlike all widely-adopted KEPs) resist attacks by quantum computers. Strikingly, the security of essentially all group theory based KEPs boils down to variantions of Dehn's Conjugacy Problem (usually, in Artin's braid group).

While classical mathematics was concerned with decidability/computability aspects of the Conjugacy Problem, the introduction of cryptography based on this problem spurred a cryptoanalytic approach to this problem, where efficiency and heuristic shortcuts play key roles.

This minicourse will cover (as far as time permits) the following topics:

* Introduction to Key Exchange Protocols (KEPs);

* The main schemes for KEPs based on noncommutative groups;

* The variations of the Conjugacy Problem on which these KEPs are based;

* Introduction to Artin's Braid Group;

* Two cryptanalytic approaches to the Conjugacy Problem in the Braid Group:

- Length-based algorithms; - Complete-invariants-based algorithms.

We will argue that the two mentioned approaches are conceptually similar, and describe a simple distribution on the braid group where a new length-based algorithm outperforms the best Complete-Invariants-based algorithm. We will challenge the prevalent opinion, that the Conjugacy Problem in the braid group is "easy on random instances" when the distribution is simple.

If time permits, we will also describe our Complete invariant for Multiple Conjugacy in Garside groups, and a provable reduction of the Decomposition (aka Double Coset) Problem in the braid group to the Multiple Conjugacy Problem in that group.

The new results presented in this course are based on joint works with (various subsets of):

David Garber, Arkadius Kalka, Mina Teicher and Gary Vinokur.