Time: Wednesday May 4th, 2011 5:00pm
Location: Buchanan A203

Constructing curves with prescribed automorphisim group for cryptographic porpuses

Syd Lasavani, University of Calgary

Automorphisms have been always a great help to mathematicians to understand the structure of geometric and algebraic objects.

Specifically, the group of automorphisms of a curve, i.e. the set of invertible maps from a curve to itself, is of a great computational value.

In this talk, we will discuss how finding curves with specific automorphism groups can be used in mounting cryptographic attacks. Then we present different methods of constructing curves which have the desired automorphism groups for a specific attack.