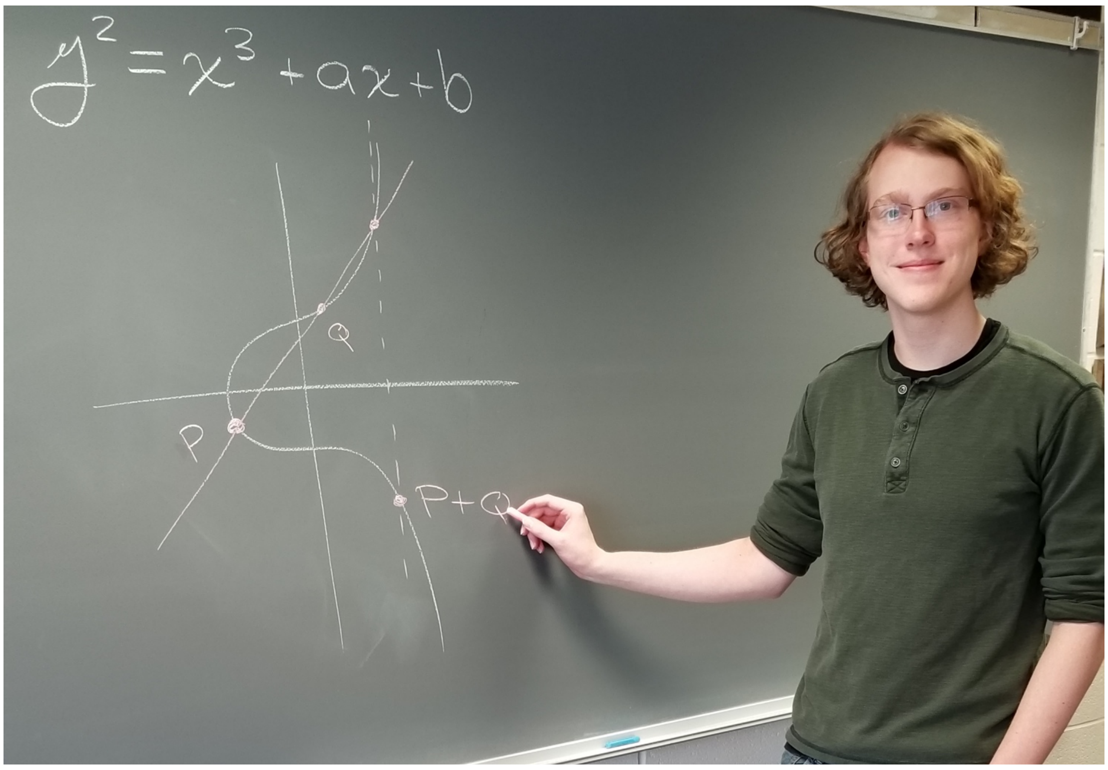
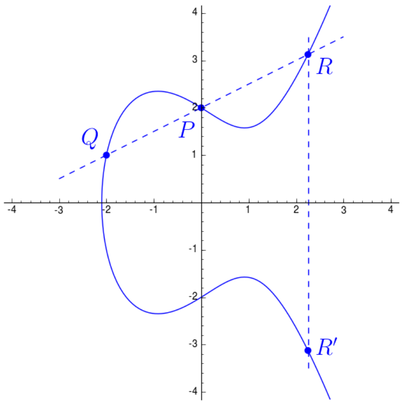
# The MATHEMATICS Honors Lecture Series



## Nicholas Wilcox '18

**Monday, May 7**
**Reception 4:00, King 203**
**Lecture 4:30, King 239**

## Elliptic Curve Cryptography: A Computational Introduction



At its core, cryptography relies on problems that are simple to construct but difficult to solve unless certain information (the key") is known. One such problem is that of computing the discrete logarithm in finite groups. In order to implement cryptographic protocols based on the discrete logarithm problem, we must obtain very large groups that have an easily computable operation. Fortunately, we can derive groups from the set of points on an algebraic curve, that is, the set of points *(x; y)* satisfying a polynomial equation *p(x; y)* = 0, where *p* is a polynomial in *x* and *y*.

This presentation will describe the basic algebra behind fundamental cryptographic protocols, such as Diffie-Hellman Key Exchange, and then show how a certain class of algebraic curves, elliptic curves, can be used to implement those protocols.