# Elliptic curves and cryptography

**Alfred Menezes**
**Auburn University**

While elliptic curves have been intensively studied in number theory, it is only in the last 10 years that they have been shown to be useful in algorithmic number theory, specifically for designing efficient algorithms for factoring integers and for primality proving.

In this talk, I will describe how elliptic curves over finite fields are being used in designing secure and practical protocols for public-key encryption and digital signature schemes.