



Kutztown University of Pennsylvania
Department of Mathematics

COLLOQUIUM

9:00 A.M.

MARCH 20, 2009

LYTLE HALL 228

*Cracking Cryptography, Curves,
Card Tricks, and Kangaroos!*

DR. ERIC LANDQUIST

ASSISTANT PROFESSOR OF MATHEMATICS
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS

ABSTRACT

During a recent football season, Notre Dame's internet servers nearly crashed. Was it hype surrounding a Heisman Trophy candidate? Or could it have been a herd of wild kangaroos?

Modern communications rely on the secure transmission of sensitive data. We will give a brief overview of some of the methods used in cryptographic protocols and focus on the application of elliptic curves to cryptography. We will then give intuitive descriptions of the best known methods to crack cryptosystems based on algebraic curves, namely Pollard's Rho and Kangaroo algorithms.

Included in the talk will be unique problems for calculus students, a birthday game, a new card trick to dazzle your friends (with high probability), and open problems and challenges to play with in your (or your computer's) spare time.