TEMPLE UNIVERSITY MATHEMATICS COLLOQUIUM

Ted Chinburg

University of Pennsylvania

will speak on

Crypto Capacity Theory

ABSTRACT: One of the applications often used to justify research in number theory to a skeptical public is its relevance in cryptography. This talk will be about the discovery last spring that adelic capacity theory is directly relevant in this way. Capacity theory quantifies when one can construct polynomials with certain boundedness properties on subsets of the complex plane and of the p-adic numbers. This pertains to cryptography because such polynomials can lead to polynomial time algorithms for factoring numbers given enough partial information about their factors. By the end of the talk I will describe some new work with Nadia Heninger and Zach Scherr on cryptographic capacity theory.

MONDAY, NOVEMBER 3
LECTURE AT 4:00 PM
COFFEE, TEA, AND REFRESHMENTS FROM 3:40 PM
ROOM 617, WACHMAN HALL
DEPARTMENT OF MATHEMATICS