Department of Mathematics and Statistics Colloquium

Effectiveness of Coppersmith's Attack on RSA Cryptography

Zachary Scherr

Bucknell University

Abstract: In 1977, mathematicians Rivest, Shamir and Adleman introduced a simple yet effective algorithm for achieving public key cryptography, allowing two parties who have never met to communicate securely over a channel which anybody can listen in on. While the RSA algorithm is unbreakable in theory, Coppersmith shocked the world in 1996 by discovering a series of efficient attacks on poorly implemented RSA schemes.
In this talk we will discuss the RSA algorithm, and motivate and demonstrate one of Coppersmith's methods of attack. At the end of the talk we will discuss recent work of the speaker and collaborators on proving just how effective Coppersmith's attacks are.

Monday, March 26 at 3:50 in Roop 103

Refreshments at 3:30