**COLLOQUIUM**

Chris Monico

**“**The Number Field Sieve for Integer Factorization**”**

Tuesday, October 7, 2008 at 3:30 p.m. in CH 107

Refreshments will be served in Math 238 at 3:00 p.m.

**Abstract**

The problem of factoring integers is a difficult one, with direct consequences for cryptography. The Number Field Sieve (NFS) represents the current state-of-the-art for integer factorization. It has its roots in a 1988 paper by John Pollard, but has been brought into current practical form by dozens of people over the last 20 years.

In this talk, I will briefly recall the relevance of integer factorization to cryptography and then describe the algorithm.

I will conclude by describing some open problems whose resolutions could lead to meaningful efficiency improvements.