# SPECIAL MATH CLUB LECTURE

## 3:40 PM, 22 April 2008, 239 Lockett

# Braids and Cryptography


## Professor Tara E. Brendle

## LSU Department of Mathematics

## http://www.math.lsu.edu/∼brendle/



**Abstract:** In the late 1990s Anshel, Anshel and Goldfeld proposed a new cryptosystem based on Dehn's famous "Decision Problems" in combinatorial group theory. Their paper sparked a great debate about the effectiveness of such a cryptosystem which continues today. In this talk, we will take no sides in this debate! We will describe the particular group which Anshel, Anshel and Goldfeld suggested for use in their cryptosystem, known as the *braid group*. This group is widely studied by topologists because of its close connections with knots and surfaces. We will also show how to implement the Anshel-Anshel-Goldfeld cryptoscheme using braid groups.


**All undergrads and first year grads invited.**
**Refreshments will be provided.**