

## UNDERGRADUATE MATHEMATICS SEMINAR

The next meeting of the seminar will be this coming **Monday, March 3<sup>rd</sup>**, with refreshments beginning at **4:00** in the Math Common Room, **Bailey 204**, and the lecture following at **4:15** in **Bailey 207**.

In this seminar, Union College's own **Professor Kathryn Lesh** will be presenting the talk below.

### TITLE: Low exponent Attacks on the RSA Cryptosystem

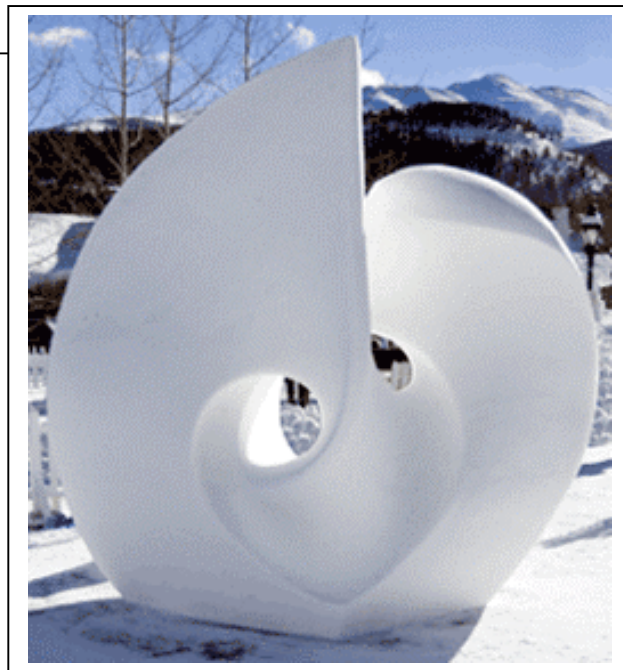
**ABSTRACT:** The RSA cryptosystem is widely used today to protect the secrecy of data transmitted over the Internet, such as credit card numbers. Encryption and decryption in RSA both involve computing an exponentiation, which is computationally intensive, so there is a temptation to shorten computations by using small exponents. (Computing  $17^3$  is so much easier than computing  $17^{501}$ .) In this talk, we'll discuss "low exponent attacks" on RSA such as those devised in the 1990s by Weiner, Boneh and Durfee, and Coppersmith. It turns out that using small exponents is a really bad idea for security!

### What to Do with all of this Snow?

As winter recently reminded us that it is still around, you might be thinking about what you can do with all of this snow (besides sledding on cafeteria trays!). For inspiration, you might look to **Stan Wagon**.

Wagon, a Professor of Mathematics and Computer Science at Macalester College in Minnesota (who will likely be holding an undergraduate seminar this coming spring term), has been a participant in the International Snow Sculpture Championships in Breckenridge, Colorado. As part of Team Minnesota, Wagon has helped sculpt geometric objects, such as "Cold Hands, Warm Heart" pictured below and to the right.

For more information, visit the website <http://www.maa.org/news/013008snow.html>.



If snow sculpting isn't for you, how about thinking about the mathematics of snowflakes? From <http://mathgateway.maa.org/do/ViewMathNews?id=251> we have the following lead paragraph:

"Snowflakes have puzzled mathematicians from the time Johannes Kepler predicted that the six-pointed structure reflects an underlying crystal structure. Now--four hundred years later--mathematicians claim to be able to model three-dimensional snowflakes via a computer program. More important, being able to model the process of creation might explain why no snowflakes are alike, according to Janko Gravner (UC Davis)."

## Opportunity in Finance

(A nonpaid advertisement) Are you interested in pursuing challenging professional business careers? The MS/Finance program in Washington University's Olin Business School can be just the right way for your students to prepare for an exciting future. Graduates of Washington University's 10-month MS/Finance program have accepted positions at many top firms in the U.S. and around the world.

Detailed information about the Olin Business School's MS/Finance program can be found at <http://www.olin.wustl.edu/prospective/msfin.cfm>.

Interested students are encouraged to contact Gary Hochberg directly at [Hochberg@wustl.edu](mailto:Hochberg@wustl.edu) or by telephone at (314) 935-6380. Our published application deadline is March 14, 2008 for students wanting to enroll with us in Fall 2008, but we can be flexible with this deadline for the right students.

## Fishy Math

by  
Shawn Bartok &  
Richie Bonventre



## Problem of the Newsletter: February 29, 2008

Congratulations to **Brandon Bartell** for submitting a correct solution to last week's problem. You can view last week's question with a winning solution on the first floor bulletin board in Bailey Hall.

This week's problem was suggested to this column by Professor Karl Zimmermann, inspired by a question from his daughter.

**Here is this week's problem:** Consider a triangle with side lengths  $a$ ,  $b$ , and  $c$ . In this triangle, draw three parallel lines, one parallel to each side of the triangle, so that these three parallel lines are of the same length,  $x$ , and intersect at a common point. (See the picture.) Find the length,  $x$ , of these parallel lines.

Professor Friedman will accept solutions to this problem until 12:00 noon Thursday, March 6<sup>th</sup>. Email your solution to him ([friedmap@union.edu](mailto:friedmap@union.edu)) or put it in his mailbox in the Math Department's office on the second floor of Bailey Hall.

