

# MSCS



# Mess

Access the Mess anytime online at [http://www.stolaf.edu/depts/mscs/MSCS\\_Mess](http://www.stolaf.edu/depts/mscs/MSCS_Mess)

Department of Mathematics, Statistics and Computer Science  
St. Olaf College, Northfield, MN 55057

April 4<sup>th</sup>, 2008  
Volume 36, No 19

## This Week's Colloquium

Title:	The Birthday Attack in Cryptography
Presenter:	Josh Gower
Date:	Tuesday April 8 <sup>th</sup>
Time:	1:30pm (Treats 1:15)
Location:	SC 188

**Abstract:** In its most common form, the birthday paradox states that among 23 randomly chosen people the probability of two of these people sharing the same birthday is approximately 1/2. Though not actually a paradox, presumably most people would guess that the probability would be much lower (or, equivalently, that many more people would be needed for such odds). In this talk we will explain this result, derive a formula for the birthday paradox in a more general setting, and then discuss its impact on the design of digital encryption and signature schemes.

**Bio:** Jason Gower is currently a postdoctoral fellow at the Institute for Mathematics and its Applications. Before coming to the Twin Cities, Jason majored in mathematics and physics at Truman State University and earned his Ph.D. in computational number theory at Purdue University.

## CS summer work opportunities

The CS program plans to hire two full-time summer workers (pending funding approval). Highlights of these two positions:

- **Web and wiki master.** This person would help update wiki software used by the program, work with department-related web sites, and explore and implement new ways of using these technologies in teaching and projects. Training provided.  
*Qualifications:* One or more CS courses; experience with PHP and/or web-related technologies a plus, CS major a plus.
- **Cluster system administrator.** This person will learn how to manage the CS Beowulf clusters from others with experience at this job, and will develop and implement new applications of the clusters, often involving other fields of study. Potential for ongoing cluster-related work in the future.  
*Qualifications:* CS 251 minimum; operating systems (CS 273), other relevant courses, or prior system management experience is a plus, CS major is a plus.

Prof. Brown also knows of some off-campus internships. To apply or for more information, contact Dick Brown ([rab@stolaf.edu](mailto:rab@stolaf.edu), x3860) or see the CS website ([www.cs.stolaf.edu](http://www.cs.stolaf.edu)).

## Carlson Problem Solving Contest

It's time for the annual Carlson Problem Solving Contest. You can win the largest cash prize ever awarded!

**Format:** The exam is an individual 75 minute exam that is taken at St. Olaf on the honor system. The exam may be picked up beginning Apr. 10 outside Old Music 304 and must be completed by Apr. 14. If you plan to take the exam, please inform Prof. Smith in Old Music 209, or Prof. Weimer in Old Music 304, or send an e-mail to [weimer@stolaf.edu](mailto:weimer@stolaf.edu).

**Prize Format:** There are two categories, first year students in one category, upper-class in the other. Prize money will be awarded in each category as follows:

*First Place = \$60*

*Second Place = \$50*

*Third Place = \$40*

*Fourth Place = \$30*

*Fifth Place = \$20*

*Sixth Place = \$10*

## Interested in learning more about Actuarial Science?

Two St. Olaf alumni from St. Paul-based Travelers Companies are coming to campus on Thursday, April 17th during community time (11:30-12:30) to speak with students interested in learning more about the actuarial science field. Hear more about internships and jobs, the exams you'll need to take, and what a real-world role using your MSCS background might entail. (Science Center 186)

For more information on Travelers, visit: <http://www.travelers.com/SPT03PortalMain.asp?startpage=/corporate/careers/index.html>

## Reminder: Math Recital This week!

Wednesday evening, April 9th at 7:00pm in Ytterboe Lounge.

Who's invited: anyone who has taken a math, stats or CS class, or knows someone who has taken an MSCS class.

Potential performers should contact Steve McKelvey ([mckelvey@stolaf.edu](mailto:mckelvey@stolaf.edu), x3421)

## Problem of the Week

Each of the letters {D,E,M,N,O,R,S,Y} is to be replaced with a base-10 digit {0,1,2,3,4,5,6,7,8,9} to make the following addition correct.

$$\text{SEND} + \text{MORE} = \text{MONEY}$$

## Joke of the week

Submitted by Ben Clifford

**Question:** Why was 6 afraid of 7?

*Answer:* Because 7 8 9.

Editor-in-Chief:	Kate Tummers
Faculty Advisor:	Katie Ziegler-Graham
MM Czar:	Donna Brakke
Problems Editor:	Mike Weimerskirch

*If you would like to submit an article or math event to be published in the Math Mess, e-mail [tummers@stolaf.edu](mailto:tummers@stolaf.edu).*