BAMA Bay Area Mathematical Adventures

# BAMA 5

School Year 2016—2017

Join us for a free talk...

# Jeffrey Hoffstein

## *Public Key Cryptography:*

### *A Behind-the-Scenes Look at a 20-Year Roller Coaster Ride*

Santa Clara University

**Santa Clara University, Daly Science 206**

**Friday, March 3, 2017, 7:30 pm**

I'll discuss the history of cryptography, what public key cryptography is, and the amazing mathematical advances after the mid-1970s, when this completely new concept was first introduced. In 1996, I and two of my colleagues from Brown University, Jill Pipher and Joe Silverman, introduced some new ideas, started a company, and embarked on a 20 year journey that changed cryptography and our lives. I'll explain these ideas, their connection to the present, and a future that may include quantum computers.

***Jeffrey Hoffstein*** is a Professor at Brown University, and an ICERM Associate Director. He received his PhD in mathematics from MIT in 1978. After postdoctoral positions at the Institute for Advanced Study, Cambridge University, and Brown University, Hoffstein served as Assistant and Associate Professor at University of Rochester. He came to Brown as a full professor in 1989. His research interests are number theory, automorphic forms, and cryptography. Hoffstein has written over seventy papers in these fields, co-authored an undergraduate textbook in cryptography, and jointly holds eleven patents for his cryptographic inventions. He was a co-founder of Ntru Cryptosystems, Inc., now merged with Security Innovation, Inc

*** See back for map and directions.**

**Visit the Bay Area Mathematical Adventures (BAMA) at http://mathematicaladventures.org**

**To receive email notifications about BAMA talks, please contact Frank Farris at ffarris@scu.edu .**

# BAMA

## Bay Area Mathematical Adventures

**A series of presentations on diverse topics by remarkable mathematicians. All talks are free and open to the public.**

## WHY?

BAMA aims to challenge and motivate students to think mathematically. Speakers will present real mathematics, and will share with the audience modern views of mathematics. Some talks will provide students with related problems, or will enable teachers to expand later on the topics with their students.

## WHO?

BAMA is aimed at bright high-school age students. However, all are welcome: younger or older students, teachers, parents, and the general public.

## WHEN?

Evening talks will be given approximately once a month between September and April. Each talk will be self-contained (speakers will not assume their audiences have attended previous talks).

## WHERE?

### Santa Clara University
### Daly Science, rm. 206

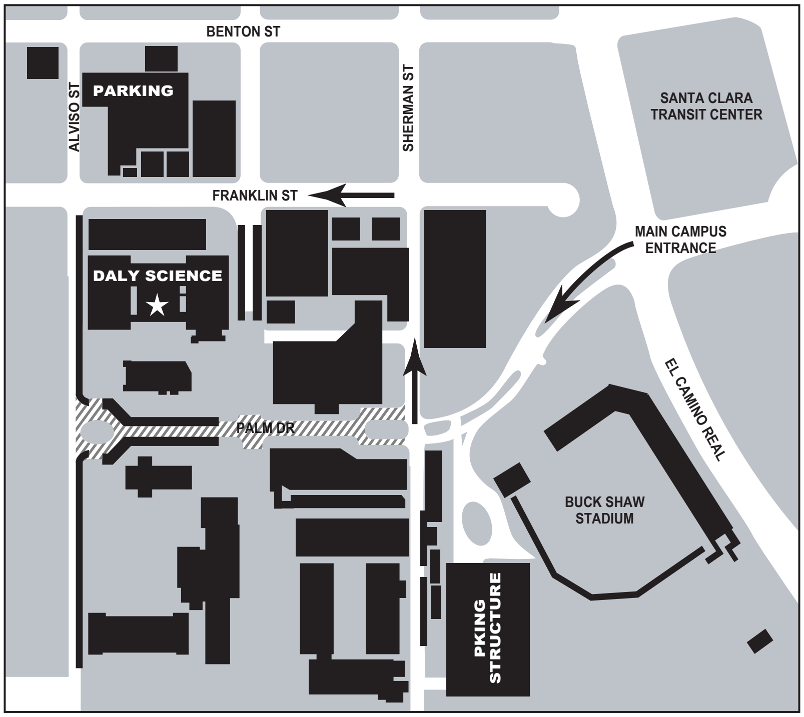
- From US Highway 101, take the De La Cruz Blvd/Santa Clara exit and follow the signs to El Camino real and main campus entrance.

- From I-280, take I-880 north toward Oakland to The Alameda exit. Turn left onto The Alameda (which becomes El Camino Real) to main campus entrance.

- From I-880, take The Alameda exit, travel north (The Alameda becomes El Camino Real) to main campus entrance.

***Note:*** If you arrive by car, you can go directly to the parking garage at Franklin and Alviso and purchase a permit at a self-serve kiosk. Alternatively, it is usually possible to find free street parking within a couple of blocks.
The parking garage is free after 7 pm on Fridays.

- If you have a disability and require reasonable accommodation, please call anyone on the steering committee, or 1-800-735-2929 (TTY—California Relay) 24 hours in advance.



## SPONSORS:

**San Jose State University**
Departments of Mathematics and Computer Science
College of Engineering

**Santa Clara University**
Department of Mathematics and Computer Science

American Institute of Mathematics

Mathematical Sciences Research Institute

## FOR MORE INFO:

**http://www.mathematicaladventures.org**

BAMA Steering Committee:

| | |
|---|---|
| Tatiana Shubin | SJSU 408-924-5146 |
| Frank Farris | SCU 408-554-4430 |
| Bradley Jackson | SJSU 408-924-5100 |
| Gerald L. Alexanderson | SCU 408-554-6894 |