University of Florida
Mathematics Department
SECOND CENTER FOR APPLIED MATH COLLOQUIUM

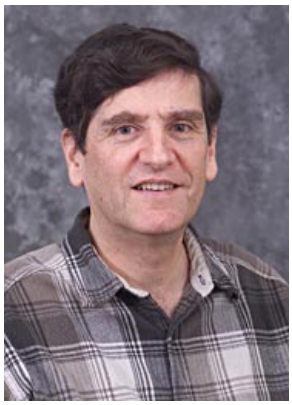
by

Carl Pomerance*

Dartmouth College

on

A New Primal Screen



Date and Time: 4:00 - 4:55pm, Thursday, March 10, 2005
Room: Little Hall 113
Refreshments: After the lecture in the Atrium (LIT 339)

OPENING REMARKS
by
Dr. Win Phillips
Vice-President for Research

Abstract: How fast can one determine if a given number is prime or composite? This question, which was first posed explicitly by Gauss in 1801, has been the subject of much attention in the computer age. In 2002, Agrawal, Kayal and Saxena announced a new and surprisingly simple deterministic algorithm that runs in polynomial time (within a fixed power of the number of digits of the number in question). We will discuss this algorithm as well as more recent developments.

* Carl Pomerance is a world famous number theorist and one of the pre-eminent authorities in the areas of primality testing and factoring of large integers which have applications to cryptography. One of his fundamental contributions is the quadratic sieve algorithm. After receiving his PhD from Harvard University, he joined the University of Georgia as an assistant professor and rose to the rank of Distinguished Professor there. Then he worked at Lucent Technologies for a few years and is currently a Distinguished Professor at Dartmouth.

University of Florida * Mathematics * Conltact Info