University of Florida, Mathematics Department
Fifth Ulam Colloquium

by

Gerhard Frey*

Institute for Experimental Mathematics in Essen (Germany)

on

Fermat's Last Theorem and Data Security

Date and Time: 4:00 - 4:55pm, Thursday, March 6, 2003
Room: 105 Fine Arts Building B
Refreshments: After the lecture in the Atrium (LIT 339)

OPENING REMARKS
by
Dean Pramod Khargonekar
(Engineering)

Abstract: One of the greatest achievements in pure mathematics is Wiles' proof of Fermat's Last Theorem in 1994. One of the biggest challenges in applied mathematics is to provide tools for secure data storage and transmission.

It is very remarkable that for both problems one can use methods from a very active field of contemporary research called Arithmetical Geometry. In this area one combines methods from Algebraic Number Theory, Algebraic Geometry and Algebra to obtain results for diophantine problems. The key ingredient is Galois theory and so group theory and representation theory play an important role. In the lecture we shall explain how one can transform Fermat's Last Theorem and an important part of cryptography to questions about Galois representations and discuss methods used to solve these questions.

* Professor Gerhard Frey is an authority on Number Theory, Algebraic Geometry and Cryptography. He is world-renowned for his contribution to the proof of Fermat's Last Theorem, one of the most celebrated problems in mathematics, for which he was awarded the Gauss Medal in 1996. Currently he is head of the cryptography group at the Institute for Experimental Mathematics in Essen (Germany).

This years Ulam Colloquium is part of the Computational Algebra Workshop and the Special Year in Algebra.

Ulam Colloquium * University of Florida * Mathematics * Conltact Info