

Department of Mathematical and Physical Sciences Presents

The 2008 Colloquium

Thursday, April 10, 5:00-6:00pm

LBV Room 219, TAMIU

Free Refreshment Starts at 4:30pm

Mr. Thomas Rodriguez

Graduate Student of Mathematics in TAMIU

Cryptography with an Emphasis on Elliptic Curves

Abstract

The following is an independent study of Cryptography and Cryptanalysis under the guidance of Dr. Abe and Dr. Khosraviyani. This project was originally created to serve as an advanced Mathematical elective during the Spring 2007 semester. This independent study applies a heuristic method to the study of Cryptography with an emphasis on Elliptic Curves. The presentation will give a summary of the concepts learned during the study, but will focus on the application of Elliptic curves in the field of Cryptography. Elliptic curve cryptosystems provide a comparable level of security as other strong cryptosystems such as RSA public-key cryptography, but provide the advantage of requiring less memory allocation. Hence, elliptic curve cryptosystems are suitable for devices with limited memory.

Refreshment Starts at 4:30pm

For additional Information, contact Dr. T. Jin. (tjin@tamiu.edu) or (956)326-2582 (office)