Brock University
Department of Mathematics & Statistics

Math 5P99 Masters Project Presentation

February 7th at 4pm

Permutation Polynomials over Finite Fields and their application to Cryptography

Katia Benseba

Abstract

The aim of the paper is the study of Permutation Polynomials over finite fields and their application to cryptography. In my talk, I will begin by a brief review of finite fields, define permutation polynomials over finite fields and their properties. I will present old results such as Hermite-Dickson's Theorem as well as some most recent ones. After introducing cryptography, I will give a historical overview, by explaining some cryptosystems such as RSA and ElGamal. Finally, I will present some cryptographical protocols based on Permutation Polynomials over Finite Fields.

Keywords*: Permutation Polynomials, Cryptography, Hermite's Theorem.*

Examination Committee Members:

Supervisor: Dr. Omar Kihel.

Supervisory Committee Members: Dr. Pouria Ramazi.

Presentation will be held in MCG310