Public Abstract
First Name:Michael
Middle Name:Paul
Last Name:Pemberton
Adviser's First Name:William
Adviser's Last Name:Banks
Co-Adviser's First Name:
Co-Adviser's Last Name:
Graduation Term:FS 2009
Department:Mathematics
Degree:MS
Title:Elliptic Curves and Their Applications in Cryptography

In 1985, Koblitz and Miller proposed elliptic curves to be used for public key cryptosystems. This present thesis examines the role of elliptic curves on cryptography and basic problems involving implementation and security of some elliptic curve cryptosystems. Some of the aspects we are concerned with include: 1. methods to determine the number of points on an elliptic curve over a finite field; 2. implementation of cryptosystems based on the discrete logarithm problem for elliptic curves defined over a finite field; 3. examine an elliptic curve analogue of the RSA cryptosystem. We provide answers to these and discuss a number of applications for number theory, such as factorization and primality testing.