ELLIPTIC CURVES AND THEIR APPLICATIONS IN CRYPTOGRAPHY

Michael Pemberton

Dr. William Banks, Thesis Supervisor

ABSTRACT

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:

- Methods to determine the number of points on an elliptic curve over a finite field
- Implementation of cryptosystems based on the discrete logarithm problem for elliptic curves defined over a finite field
- 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.