Elliptic Curve Cryptography

Dissertation

Integrated Masters of Science
In
Applied Mathematics

Submitted by
Harsh Kumar Chourasia

supervised by
Dr. Ram Krishna Panday

Department of Mathematics
Indian Institute of Technology, Roorkee
Department of Mathematics
Roorkee-247667

Declaration

Abstract

Acknowledgments

I would like to thank my supervisor, Ram Krishna Panday,Department of Mathematics, Indian Institute of Technology Roorkee for his guidance through each stage of the process.

Contents

Chapter 1

Introduction to Cryptography

1.1 Introduction

Intorduction

Chapter 2

Discrete Logarithms and Diffie–Hellman

2.1 Discrete Logarithms and Diffie–Hellman

chapter 2

Chapter 3

Elliptic Curves and Cryptography

3.1 Elliptic Curves

3.2 Elliptic Curves over Finite Field

3.3 The elliptic curve discrete logarithm problem

3.4 Elliptic curve cryptography