# IB Extended Essay

Jacob Bruner

August 15, 2022

## Contents

# 1 Introduction and Aim

## 1.1 Motivating Problem

# 2 What is 'Public-Key' Cryptography

The first protocol developed to address this motivating problem was RSA encryption. Leveraging intuitive properties of numbers, RSA establishes our idea of 'one-way operations' using simple multiplication of large, highly prime (minimal divisors), numbers.

# 3 How can we formalize this: An Introduction to Groups

Group theory provides us a way to generalize certain, often intuitive, properties of number systems, by using axiomatic structure to classify groups 'up to isomorphism' and to prove various properties about their structures. A 'Group' boils down to a set, infinite or finite, and an operation that takes two elements and maps it to another while maintaining some structure. It's common to think that this structure is too vague, or broad, but, in fact, it's enough to prove sweeping conjectures and determine non-trivial properties, thereby making itself a staple of modern mathematics.

$$A_b = \int_{x_1}^{x_2} y \, dx$$