Introduction

Our team consists of Alexander Agruso and Brandon Howell. Our research intends to explore and possibly improve existing methods of cracking RSA encryption, as well as suggest avenues of research that might yield more progress in the field of elliptic curve encryption. Specific methods of cracking RSA encryption that we will explore include brute force approaches and Shor's algorithm, while for elliptic curve encryption we will explore what makes it so strong, and what would be necessary to break it.

Existing Approaches for Cracking RSA

While performing our research, we will study existing methods of breaking RSA encryption, including but not limited to brute-force prime-factorization methods and Shor's algorithm for quantum computers. Along the way, we will look for ways in which these algorithms can be improved, either through code optimizations or mathematical insights that reduce the computation power required.

Overview of Elliptic Curve Encryption

We intend to provide a fairly rigorous overview of elliptic curve encryption, but also aim to make it accessible to an audience with a limited math background. We will explore why mathematicians are so interested in elliptic curves, as well as how they are used in encryption. Finally, we will discuss what makes elliptic curve encryption so powerful, the immense computational requirements that are needed to break it, and what advancements, if any, have recently been made in the field.

Our Approaches to Research

Our research will be conducted through experimentation with actual implementations of RSA cracking algorithms. While observing the algorithms function, we will be looking for ways to optimize them. We also intend on reading existing literature on elliptic curve encryption to see if there are any recent advances in the field. If there are, we will explore what progress they have made, as well as look for ways to improve upon their methods.