Safer Security: A Novel Algorithm for Detecting Carmichael Numbers

Karnik, Sathwik

In an era of rapid growth in information technology, a significant danger threatens digital security: cyber-attacks. Public-key cryptosystems are used to overcome virtual vulnerabilities. The objective of this project was to find and prove a probabilistic algorithm for detecting Carmichael numbers, which endanger cryptosystems. An initial observation that many Carmichael numbers have a proportion of Fermat witnesses of less than 50% served as the motivation for the procedure followed in this project. These Carmichael numbers were first classified by deriving an equation involving a determined lower bound to the smallest prime factor and by using Newton's Method. Furthermore, an algorithm for distinguishing between Carmichael numbers and other composite numbers was developed and implemented in Python 3.5.2. This algorithm combined notions from the Fermat Primality Test and a Monte Carlo Simulation that randomly selected a sample of integers from 1 to n-1, where n represents the number that is tested. A second algorithm combined notions from the first algorithm and a highly accurate primality test to further differentiate between Carmichael numbers and prime numbers. In addition, the algorithms determined in this project were shown to be highly accurate through calculations involving Bayes' Rule in conditional probability. Both algorithms were also shown to be relatively efficient through theoretical big-O notation calculations. In this project, a novel algorithm was developed and proven to optimize the accuracy and efficiency in detecting Carmichael numbers with the ultimate goal of enhancing cyber security.

Awards Won:

Fourth Award of $500

Air Force Research Laboratory on behalf of the United States Air Force: First Award of $750 in each Intel ISEF Category