A Novel Solution for Integer Factorization with Cryptographic Applications

Kirby, Evan (School: Aitchison College)

This project aims at challenging the underlying conjectures in many modern encryption systems. The problem of integer factorization, and its associated difficulty is solving, is essential to securing information. Algorithms such as RSA, Rabin, and Blum Blum Shub all rely directly on the near impossibility of efficiently solving integer factorization, other algorithms that do not directly rely on integer factorization can be significantly weakened as well. Factorization algorithms such as Dixions factorization, GNFS, QNFS, and the MPQNS are all general factorization methods, and all rely on sieving of numeric relations. This can be difficult to obtain, and sometimes may take trillions of iterations to complete. This project compares a developing algorithm called the Precision Sieve to many other effective factorization algorithms. The comparison takes place across a variety of semi-prime bit sizes, each semi-prime created securely, using a well seeded random number generator and ensuring both primes are unique and sufficiently selected in relation to each other. This method of testing creates the most difficult and most secure integers to factor, replicating a real world scenario.