# CALIFORNIA STATE SCIENCE FAIR
# 2011 PROJECT SUMMARY

**Name(s)**

**Ben F. Hannel**

**Project Number**

**J1403**

**Project Title**

## Cracking the Code: The Effect of Key Length on the Security of a Public Key Encryption

**Abstract**

**Objectives/Goals**

The objective is to determine how the length of the key used to encrypt a code affects how long it takes to decipher the code, and how codes can be deciphered faster using different algorithms.

**Methods/Materials**

Programs were written in Java to crack codes with key lengths between 15 and 70 bits (5 to 23 digits). The test machine had an Athlon II X4 635 processor and 4 gigabytes of OCZ RAM. Three versions of the program were used. The first cracked the key by trying every possibility. The second tested only certain possibilities that were the most likely, and the third tested the most likely possibilities on all four cores of the processor using multi-threading.

**Results**

Each bit added to the key length increased the time to decipher the code by about 40 percent. The second version of the program used to decipher the code, which eliminated testing of unlikely keys, was three times faster than the first version. The third version, which used multi-threading, was four times faster than the second version.

**Conclusions/Discussion**

The time to decipher the code went up exponentially with key length, making keys beyond 85 bits essentially undecipherable. The deciphering time decreased by testing only the most likely keys and using all four cores of the processor. Keys used for online bank accounts and other online transactions are usually between 512 to 1024 bits long, so bank accounts are safe from anyone without a large supercomputing budget and thorough knowledge of the general number field sieve.

**Summary Statement**

This experiment tested the difficulty of deciphering an encrypted code by varying the length of the key used to encrypt the code and by increasing the efficiency of the algorithm used to decipher the code.

**Help Received**

My mother helped me edit the report, debug code, and fill out this application.