# CALIFORNIA STATE SCIENCE FAIR
# 2004 PROJECT SUMMARY

| | |
|---|---|
| **Name(s)**<br>Aaron P. Gallagher | **Project Number**<br>J1207 |

**Project Title**

## Encryption: The Effect of Algorithm Type and Plaintext Length on Encryption, Decryption, and Force-Cracking Times

### Abstract

**Objectives/Goals**

The objective of this project was to find, with a method of scoring, which encryption algorithm was the "best."

**Methods/Materials**

Using REALbasic and C++, I wrote an implementation of each algorithm (RSA, Blowfish, and IDEA) and timed the number of milliseconds that it took to encrypt and decrypt a varying amount of data. I calculated the estimated time to force-crack, and awarded points to the quickest and strongest algorithms, where the best algorithm was the one with the most points.

**Results**

IDEA, which was the slowest algorithm, accumulated the most points, probably because it was strongest. RSA, second most seure and second quickest, almost beat IDEA because of speed, but did not win because of the weight of not being strongest. Blowfish, which was the least secure, but most likely the quickest algorithm, got the least amount of points.

**Conclusions/Discussion**

There was a lot of differentiation among the speeds of each algorithm. IDEA had times of over 600ms, while Blowfish had times around 4ms. Each algorithm was very secure and relatively speedy. I doubt that IDEA, the most secure out of the algorithms I tested with over 2.4· 10^40 years to force crack, is even the most secure algorithm that has been developed. If I were to design an encryption algorithm, I would combine the speed of Blowfish with the strength of IDEA.

**Summary Statement**

To see which encryption algorithm compared the best, where the best algorithm is the quickest and strongest, isolating factors such as length of plaintext.

**Help Received**

George Feineman helped with mathematical assistance and background information; Kathy Spoto helped type.