CALIFORNIA STATE SCIENCE FAIR
2007 PROJECT SUMMARY

Name(s)
Bryce H. Kobrin

Project Number
J1307

Project Title
If Robert E. Lee Had a PC: Cracking the Vigenere Cipher

Abstract

Objectives/Goals
The Vigenere cipher is a substitution cipher used during the Civil War to encrypt messages with a keyword. The objective of this project is to determine how much text for a given key length is required to crack the Vigenere cipher.

Methods/Materials
I created a Visual Basic computer program to crack the Vigenere cipher using two different procedures, index of coincidence and frequency analysis. Index of coincidence identifies the key length and frequency analysis uses the key length to identify the key. Both procedures are based on the standard English letter frequencies. I tested both procedures on 10 different texts and 100 different keys with key lengths from 1 to 20 letters.

Results
The results for frequency analysis averaged 30 letters in the text for each letter in the key. The results for index of coincidence were more scattered than frequency analysis and averaged 400 letters of text regardless of key length.

Conclusions/Discussion
The results for index of coincidence did not follow any particular trend. I believe this is because index of coincidence is highly key and algorithm dependent. Once the key length is known, then frequency analysis can determine the key if the text is at least 30 letters long for each letter in the key.

Summary Statement
My project demonstrates how the Vigenere cipher can be cracked using a computer program.

Help Received
Father helped me debug the computer program; Mother showed me tricks in Excel.