Encryption

New Mexico Adventures in
Supercomputing Challenge
Final Report
April 7, 2004

Team Number 10
Aztec High School

Team Members
Matt Roufberg
Ralf Meyer

Teacher
John Frazzini

Project Mentor
James Jacobs

Executive Summary

The goal of our project was to create a small, fast and efficient encryption program to run on Ti calculators. After deciding to use matrices as a mode of encryption, we proceeded to program using Ti-Basic. By multiplying two matrices together, we have an encrypted message. By using the inverse of the code matrix, we can decode the coded message. Upon completion of the code, we discovered that program would be too inefficient to run in a real world scenario.

Introduction

In today's modernized world, a secure mode of communication is essential. The advances made in today's technology have demanded even more secure modes. Our goal was to test out a small program (less than 1kb) to be able to encrypt messages. Our program fell below this coming in around 600 bytes.

Method

By multiplying a message turned into a matrix (a=1, b=2, c=3, etc.) by another matrix, one can produce an encrypted message. This matrix was then multiplied by a random number (generated by the calculator). This matrix can then be deciphered by multiplying the original "message" matrix by the inverse of the "code" matrix and dividing by the random number.

Results

Although we were not able to achieve a full level of testing, we decided through other people that it provided a secure method of communication. By using a link cable, two calculators can easily transfer the information. This information can be deciphered then by using the random number and the original matrix.

Conclusion

In conclusion, we can determine that matrices are less secure than the current 256 bit encryption keys, and therefore not practical for use outside of a school environment.

Significant Achievement

I believe that our significant achievement was to actually get the program to recognize the characters and turn them into numbers and vice versa. After this was completed, the rest flowed quite easily.