California Science Center

CALIFORNIA STATE SCIENCE FAIR
2001 PROJECT SUMMARY

Your Name (List all student names if multiple authors.)
Julian S. Krause

Project Title (Limit: 120 characters. Those beyond 120 will be ignored. See pg. 9)
A New Game of Solitaire: Cryptanalysis

Science Fair Use Only

S1112

Division
_ Junior (6-8) X Senior (9-12)

Preferred Category (See page 5 for descriptions.)
11 - Mathematics & Software

Abstract (Include Objective, Methods, Results, Conclusion. See samples on page 14.)
Use no attachments. Only text inside these boxes will be used for category assignment or given to your judges.

Objective: To determine whether if you can decrypt messages done with a one-time pad (an encryption key using a randomizing algorithms which is designed to be used only once) if you have 2 messages sent with the same set of letters.
Materials: You will need one computer, a program to encrypt messages with a one-time pad (I used the Solitaire Algorithm), and 2 messages encrypted with the same key. I developed a program for file subtraction reasoning that I could use it to get the guessed key from one message, which would be tested, on the other message. That would enable me to decrypt the message
Results: You can decrypt messages sent with a one-time pad if the sender makes the mistake of using the one-time pad twice
Discussion: The most modern form of encryption, quantum cryptography, stems from the one-time pad. This is the most secure form of encryption because trying to test every key will generate every sensible message of the message#s length making it impossible to tell which is the right one. The total number of messages for 15 letters is 1*10^12 messages of which a third would probably be sensible to a computer screening program designed to detect the most frequent letters and digraphs, assuming you have the right language. However all of this work does not need to be done if the mistake is made of using the one time pad twice.

Summary Statement (In one sentence, state what your project is about.)
Using a one-time pad twice will allow someone to determine the encrypted message without knowing the key to the one-time pad.

Help Received in Doing Project (e.g. Mother helped type report; Neighbor helped wire board; Used lab equipment at university X under the supervision of Dr. Y; Participant in NSF Young Scholars Program) See Display Regulation #8 on page 4.
Parents helped make board; Teacher read reasearch paper and checked for spelling a grammer errors.