CALIFORNIA STATE SCIENCE FAIR
2004 PROJECT SUMMARY

Name(s)
Joshua A. Kroll

Project Number
S1214

Project Title
Security Through Chaos: Encryption as a Source for Information Entropy

Abstract

Objectives/Goals
The need for a reliable method of encryption has persisted throughout history; encryption applications range from military and intelligence uses to daily commercial activities. As technology has improved to allow for easier and better encryption and transmission, so has it allowed improvements in interception and message processing. Codes have become more advanced, progressing from simple character-replacement ciphers to today's algorithms of large pseudoprimes, exponents, and modular congruences. But the concept has remained simple; it is desirable to be able to send information from one point to another without anyone being able to understand it in the middle. Ideally, the encrypted information should contain no shadows of the original message, which could be identified by careful observation. That is, the ideal code would encrypt a message so that it would be indistinguishable from random noise during transmission. The aim of this project is to determine just how random the messages encrypted by various algorithms really are by comparing large empirical tests to an ideal, random set.

Methods/Materials
The internal complexity, or randomness, of each message was tested using Shannon's measure of information entropy. A Chi-square test was then used to determine how close to the ideal of random noise the encrypted form comes. Data were encrypted using the DES, 3DES, and AES strong encryption methods.

Results
While all three encryption algorithms effectively randomized the set with respect to one-character strings, only AES performed well at higher orders of entropy and approximated the random condition well in all tests. 3DES outperformed DES on all tests.

Conclusions/Discussion
The results strongly indicate that AES is more secure than other algorithms tested. It is highly unlikely that any cryptanalytic attack could be developed for use against AES-encrypted messages which takes advantage of internal patterning. Also, though no such attack has yet been developed, it is likely that one exists in DES and 3DES systems. Additionally, results demonstrate that it is possible to develop a secure communication system using AES in which it would be impossible for an adversary eavesdropping on the communication channel to determine whether a message was being transmitted or simply random data.

Summary Statement
This project is designed to determine the effectiveness of various encryption algorithms at increasing the entropy of, or randomizing, sets of several internal complexities.

Help Received
Dr. Rose Rey assisted in reviewing the project idea and developing the Chi-squared test.; Hans and Eric Nielson assisted in coding the entropy computation program; Mr. Eric Fink reviewed some written material related to the project.